

Security Audit Framework

Security Audit Report

Target: https://admin.vickykruzprogramming.dev/dashboard

Scan Mode: full

Generated: 2026-03-31T10:56:11.400848Z

Executive Summary

F

Score

Passed

High Risk

18.2%

4 / 22

8

AI-GENERATED ASSESSMENT

Learning Context: You're building foundational security knowledge. The current grade (F) reflects common beginner gaps. Focus on Security Misconfiguration and Cryptographic Failures—these are textbook vulnerabilities often tested in academic assessments. Use this report to map theory (OWASP framework) to practice (actual misconfigurations).

Attack Surface Heatmap

Layer	Pass Rate	Status	Risk
Web App	16.7% (1/6)	FAIL	HIGH
Web Server	50.0% (3/6)	WARN	MEDIUM
Host	0.0% (0/10)	FAIL	HIGH

Top 5 Priority Fixes

#	Check ID	Fix	Severity / Status	Layer
1	APP-COOKIE-001	<div>Secure session cookies</div> <div>No cookies observed on root response; cannot assess session cookie security.</div>	<div>HIGH</div> <div>WARN</div>	app

2	WS-TLS-001	TLS 1.2+ with strong ciphers TLS details unavailable or cipher does not look clearly modern (heuristic).	HIGH WARN	webserver
3	HOST-SSH-001	SSH hardening Authentication failed.	HIGH WARN	host
4	HOST-FW-001	Firewall enabled Authentication failed.	HIGH WARN	host
5	HOST-SVC-GUNICORN	Gunicorn runs as non-root Authentication failed.	HIGH WARN	host

Prioritised Hardening Plan (Day 1 / Day 7 / Day 30)

Bucket	Check ID	Layer	Severity	Priority	Recommended Fix
Day 1 (Immediate)	APP-COOKIE-001	app	HIGH	6.0	Configure session cookies with secure flags in framework settings.
Day 1 (Immediate)	HOST-SSH-001	host	HIGH	6.0	Set 'PermitRootLogin no' in sshd_config and restart the SSH service.
Day 1 (Immediate)	APP-ADMIN-001	app	MEDIUM	3.4	Disable or protect admin/debug endpoints with authentication.
Day 1 (Immediate)	HOST-FW-001	host	HIGH	3.0	Enable and configure a host firewall (e.g. ufw enable, or nftables/iptables rules).
Day 1 (Immediate)	WS-SRV-001	webserver	MEDIUM	2.8	Set 'server_tokens off' in Nginx or ServerTokens Prod in Apache.
Day 7 (Short-term)	WS-TLS-001	webserver	HIGH	2.0	Disable TLS 1.0/1.1. Use only strong ciphers (ECDHE + AES-GCM).
Day 7 (Short-term)	HOST-SVC-GUNICORN	host	HIGH	2.0	Run Gunicorn under a dedicated non-root account via systemd or a process manager.
Day 7 (Short-term)	HOST-SVC-UWSGI	host	HIGH	2.0	Run uWSGI under a non-root service account in its service configuration.
Day 7 (Short-term)	HOST-SVC-MYSQL	host	HIGH	2.0	Ensure the MySQL daemon runs under the 'mysql' user account and not as root.
Day 7 (Short-term)	HOST-SVC-REDIS	host	HIGH	2.0	Run Redis as the 'redis' user (or another non-root user) in the service configuration.
Day 7 (Short-term)	APP-CSRF-001	app	MEDIUM	1.7	Enable CSRF middleware in Flask/Django. Validate tokens on state-changing requests.

Bucket	Check ID	Layer	Severity	Priority	Recommended Fix
Day 7 (Short-term)	HOST-PERM-001	host	MEDIUM	1.7	Tighten permissions in /etc/ssh so that only root can modify SSH configuration files.

OWASP Top 5 Risk Summary (2025)

OWASP Category	Failed Checks	Fail Rate
A01:2025 – Broken Access Control	3	100.0%
A02:2025 – Security Misconfiguration	11	78.6%
A04:2025 – Cryptographic Failures	3	75.0%
A09:2025 – Security Logging & Alerting Failures	1	100.0%

Learning Context: You're building foundational security knowledge. The current grade (F) reflects common beginner gaps. Focus on Security Misconfiguration and Cryptographic Failures—these are textbook vulnerabilities often tested in academic assessments. Use this report to map theory (OWASP framework) to practice (actual misconfigurations).

30-Day Hardening Roadmap Simulation

Phase	Fixes	Grade	Score	Attack Paths
Current	0	F	18.2%	1
Day 1	5	F	40.9%	1
Day 7	12	C	72.7%	0
Day 30	18	A	100.0%	0

Configuration Drift vs Hardened Flask LMS

Grade Delta	F vs A
Pass Delta	-18 checks vs baseline
Improved Checks	None

Regressed Checks	APP-COOKIE-001, APP-CSRF-001, APP-ADMIN-001, APP-RATE-001, APP-PASS-001, WS-TLS-001, WS-SRV-001, WS-LIMIT-001, HOST-SSH-001, HOST-SVC-001, HOST-UPDATE-001, HOST-PERM-001, HOST-FW-001, HOST-LOG-001
------------------	--

APP Layer Findings

ID	Check	Status	Severity	Details
APP-DEBUG-001	Debug mode disabled	PASS	HIGH	No obvious debug/traceback content in root response.
APP-COOKIE-001	Secure session cookies	WARN	HIGH	No cookies observed on root response; cannot assess session cookie security.
APP-CSRF-001	CSRF protection enabled	FAIL	MEDIUM	CSRF patterns missing.
APP-ADMIN-001	No exposed admin endpoints	FAIL	MEDIUM	Admin paths exposed: /admin, /debug, /test, /wp-admin.
APP-RATE-001	Rate limiting configured	WARN	MEDIUM	Rate limiting not evident.
APP-PASS-001	Strong password policy	WARN	LOW	Password hints: 0/5 complexity requirements mentioned.

WEBSERVER Layer Findings

ID	Check	Status	Severity	Details
WS-HSTS-001	HSTS header enabled	PASS	HIGH	HSTS present with strong max-age=31536000.
WS-SEC-001	Security headers present	PASS	HIGH	3/4 security headers present: ['X-Frame-Options', 'X-Content-Type-Options', 'Referrer-Policy']
WS-TLS-001	TLS 1.2+ with strong ciphers	WARN	HIGH	TLS details unavailable or cipher does not look clearly modern (heuristic).
WS-SRV-001	No server version disclosure	WARN	MEDIUM	Server: nginx. Version hidden.
WS-DIR-001	Directory listing disabled	PASS	MEDIUM	Directory listing disabled
WS-LIMIT-001	Request size limits	WARN	LOW	No direct request limit test available. Content-Length: 0

HOST Layer Findings

ID	Check	Status	Severity	Details
HOST-SSH-001	SSH hardening	WARN	HIGH	Authentication failed.
HOST-FW-001	Firewall enabled	WARN	HIGH	Authentication failed.
HOST-SVC-001	Minimal services running	WARN	MEDIUM	Authentication failed.
HOST-UPDATE-001	Automatic updates configured	WARN	MEDIUM	Authentication failed.
HOST-PERM-001	Secure SSH file permissions	WARN	MEDIUM	Authentication failed.
HOST-LOG-001	Logging service active	WARN	LOW	Authentication failed.
HOST-SVC-GUNICORN	Gunicorn runs as non-root	WARN	HIGH	Authentication failed.
HOST-SVC-UWSGI	uWSGI runs as non-root	WARN	HIGH	Authentication failed.
HOST-SVC-MYSQL	MySQL runs as non-root	WARN	HIGH	Error reading SSH protocol banner
HOST-SVC-REDIS	Redis runs as non-root	WARN	HIGH	Authentication failed.

Critical Attack Paths

#	Attack Path	Risk	Score
1	Server → Internal Services	MEDIUM	6.5

1 attack path(s) identified. Remediate highest-score paths first.

Recommended Next Actions

1	Harden session cookies (set Secure, HttpOnly and SameSite attributes).
2	Update TLS configuration to disable weak protocols/ciphers and prefer TLS 1.2+.
3	Restrict admin endpoints behind authentication and, ideally, IP allowlists or VPN.

4	Harden SSH by disabling root login and password authentication, and using key-based access.
5	Review host OS hardening: firewall rules, automatic security updates, logging and file permissions.

Security Posture History

Trend	STABLE
Grade change	F → F (-31.8%)
Previous scan	2026-03-31 10:49:56
Time elapsed	0.0 day(s)
Regressions	HOST-LOG-001, HOST-PERM-001, HOST-SVC-GUNICORN, HOST-SVC-MYSQL, HOST-SVC-REDIS, HOST-SVC-UWSGI, HOST-UPDATE-001
Improvements	None
Persistent failures	APP-ADMIN-001, APP-CSRF-001
Summary	Grade unchanged at F (-31.8% score change) over 0 days. 7 checks regressed (HOST-LOG-001, HOST-PERM-001, HOST-SVC-GUNICORN...).

Server Fingerprint

OS	N/A
Docker	N/A
Web Server	nginx
App	N/A