

Security Audit Framework

Security Audit Report

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

Scan Mode: full

Generated: 2026-04-11T01:46:29.951610Z

Executive Summary

C

Score

Passed

High Risk

72.7%

16 / 22

1

AI-GENERATED ASSESSMENT

The current security posture is Grade.C with 16 of 22 checks passing (72.7% overall). There are 1 high-severity issues, mainly concentrated in the application layer, which significantly increases the likelihood of successful attacks in that area. No multi-step attack paths were found, which reduces the chance of chained exploitation across layers.

Attack Surface Heatmap

Layer	Pass Rate	Status	Risk
Web App	16.7% (1/6)	FAIL	HIGH
Web Server	100.0% (6/6)	PASS	LOW
Host	90.0% (9/10)	PASS	LOW

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	APP-PASS-001	Strong password policy Password hints: 0/5 complexity requirements mentioned.	LOW WARN	app
3	APP-CSRF-001	CSRF protection enabled No CSRF protection detected. No form tokens, CSRF headers, or XSRF cookies found. Enable CSRF middleware.	MEDIUM FAIL	app
4	APP-ADMIN-001	No exposed admin endpoints Admin path(s) return 200 with SPA shell content (/admin, /admin/index.php, /debug, /test, /wp-admin, /wp-login.php, /administrator, /phpmyadmin, /pma, /cpanel). Likely a login wall — verify these paths are properly authenticated.	MEDIUM WARN	app
5	APP-RATE-001	Rate limiting configured Rate limiting not evident.	MEDIUM WARN	app

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 7 (Short-term)	APP-ADMIN-001	app	MEDIUM	3.4	Disable or protect admin/debug endpoints with authentication.
Day 7 (Short-term)	APP-CSRF-001	app	MEDIUM	1.7	Enable CSRF middleware in Flask/Django. Validate tokens on state-changing requests.
Day 7 (Short-term)	APP-RATE-001	app	MEDIUM	1.4	Implement rate limiting at application level (Flask-Limiter, Django-ratelimit).
Day 30 (Medium-term)	HOST-SVC-001	host	MEDIUM	1.4	Review running services with systemctl and disable those not required for the web stack.
Day 30 (Medium-term)	APP-PASS-001	app	LOW	0.5	Enforce minimum 12 chars, mixed case, numbers, symbols in password policy.

OWASP Top 5 Risk Summary (2025)

OWASP Category	Failed Checks	Fail Rate
A01:2025 – Broken Access Control	3	100.0%
A02:2025 – Security Misconfiguration	1	7.1%

A04:2025 – Cryptographic Failures	2	50.0%
A09:2025 – Security Logging & Alerting Failures	0	0.0%

Security Assessment: Overall grade C. Primary concerns: Broken Access Control. Review the prioritized hardening plan and address Day 1 items first. OWASP alignment ensures industry-standard risk categorization.

30-Day Hardening Roadmap Simulation

Phase	Fixes	Grade	Score	Attack Paths
Current	0	C	72.7%	0
Day 1	1	C	77.3%	0
Day 7	4	A	90.9%	0
Day 30	6	A	100.0%	0

Configuration Drift vs Hardened Flask LMS

Grade Delta	C vs A
Pass Delta	-6 checks vs baseline
Improved Checks	None
Regressed Checks	APP-COOKIE-001, APP-CSRF-001, APP-ADMIN-001, APP-RATE-001, APP-PASS-001, HOST-SVC-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	No CSRF protection detected. No form tokens, CSRF headers, or XSRF cookies found. Enable CSRF middleware.
APP-ADMIN-001	No exposed admin endpoints	WARN	MEDIUM	Admin path(s) return 200 with SPA shell content (/admin, /admin/index.php, /debug, /test, /wp-admin, /wp-login.php, /administrator, /phpmyadmin, /pma, /cpanel). Likely a login wall — verify these paths are properly authenticated.
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	PASS	HIGH	Site served over HTTPS (cipher details unavailable via HTTP client). Verify manually: openssl s_client -connect admin.vickkykruzprogramming.dev:443
WS-SRV-001	No server version disclosure	PASS	MEDIUM	Server: nginx. Version hidden — good practice.
WS-DIR-001	Directory listing disabled	PASS	MEDIUM	Directory listing disabled on tested paths.
WS-LIMIT-001	Request size limits	PASS	LOW	Request size limit enforced (413 or reset on oversized POST).

HOST Layer Findings

ID	Check	Status	Severity	Details
HOST-SSH-001	SSH hardening	PASS	HIGH	SSH root login disabled ✓ (PermitRootLogin prohibit-password)
HOST-FW-001	Firewall enabled	PASS	HIGH	Firewall appears active ✓
HOST-SVC-001	Minimal services running	WARN	MEDIUM	34 services running. Review with: systemctl list-units
HOST-UPDATE-001	Automatic updates configured	PASS	MEDIUM	Unattended upgrades enabled ✓
HOST-PERM-001	Secure SSH file permissions	PASS	MEDIUM	No world-writable files detected in /etc/ssh ✓
HOST-LOG-001	Logging service active	PASS	LOW	rsyslog logging service active ✓
HOST-SVC-GUNICORN	Gunicorn runs as non-root	PASS	HIGH	Gunicorn runs as non-root user 'www-data' ✓
HOST-SVC-UWSGI	uWSGI runs as non-root	PASS	HIGH	uWSGI process not found (not in use) ✓
HOST-SVC-MYSQL	MySQL runs as non-root	PASS	HIGH	MySQL process not found (not in use) ✓
HOST-SVC-REDIS	Redis runs as non-root	PASS	HIGH	Redis runs as non-root user 'redis' ✓

Critical Attack Paths

No multi-layer attack paths detected.

Recommended Next Actions

1	Harden session cookies (set Secure, HttpOnly and SameSite attributes).
2	Restrict admin endpoints behind authentication and, ideally, IP allowlists or VPN.
3	Review host OS hardening: firewall rules, automatic security updates, logging and file permissions.

Security Posture History

Trend	IMPROVED
Grade change	F → C (+13.6%)
Previous scan	2026-04-11 01:23:40
Time elapsed	0.0 day(s)
Regressions	None
Improvements	WS-LIMIT-001, WS-SRV-001, WS-TLS-001
Persistent failures	APP-CSRF-001
Summary	Grade improved from F to C (+13.6%) over 0 days. 3 checks improved (WS-LIMIT-001, WS-SRV-001, WS-TLS-001).

Server Fingerprint

OS	Ubuntu 24.04.3 LTS
Docker	N/A
Web Server	nginx
App	N/A