

Security Audit Framework

Security Audit Report

Target: https://vickkykruzprogramming.dev

Scan Mode: full

Generated: 2026-02-27T17:38:02.486491Z

Executive Summary

Grade.F

Score

Passed

High Risk

50.0%

14 / 28

6

AI-GENERATED ASSESSMENT

The current security posture is Grade.F with 14 of 28 checks passing (50.0% overall). There are 6 high-severity issues, mainly concentrated in the container layer, which significantly increases the likelihood of successful attacks in that area. The analysis also identified 2 multi-step attack path(s), showing how an attacker could chain misconfigurations to escalate impact.

Attack Surface Heatmap

Layer	Pass Rate	Status	Risk
Web App	100.0% (6/6)	■	LOW
Web Server	16.7% (1/6)	■	HIGH
Container	0.0% (0/6)	■	HIGH
Host	70.0% (7/10)	■	MEDIUM

Configuration Drift vs Hardened Flask LMS

Grade Delta	Grade.F vs A
Pass Delta	-8 checks vs baseline
Improved Checks	None

Regressed Checks	WS-HSTS-001, WS-SEC-001, WS-TLS-001, WS-SRV-001, WS-LIMIT-001, CONT-USER-001, CONT-PORT-001, CONT-RES-001, CONT-HEALTH-001, CONT-REG-001, CONT-SEC-001, HOST-UPDATE-001, HOST-FW-001, HOST-LOG-001
------------------	--

APP Layer Findings

ID	Check	Status	Severity	Details
APP-DEBUG-001	Debug mode disabled	PASS	Severity.HIGH	No obvious debug/traceback content in root response.
APP-COOKIE-001	Secure session cookies	PASS	Severity.HIGH	At least one cookie appears to use both Secure and HttpOnly flags.
APP-CSRF-001	CSRF protection enabled	PASS	Severity.MEDIUM	CSRF patterns detected.
APP-ADMIN-001	No exposed admin endpoints	PASS	Severity.MEDIUM	Admin paths none found.
APP-RATE-001	Rate limiting configured	PASS	Severity.MEDIUM	Rate limiting detected (429).
APP-PASS-001	Strong password policy	PASS	Severity.LOW	Password hints: 3/5 complexity requirements mentioned.

WEBSERVER Layer Findings

ID	Check	Status	Severity	Details
WS-HSTS-001	HSTS header enabled	FAIL	Severity.HIGH	Strict-Transport-Security header is missing.
WS-SEC-001	Security headers present	FAIL	Severity.HIGH	0/4 security headers present: []
WS-TLS-001	TLS 1.2+ with strong ciphers	WARN	Severity.HIGH	TLS details unavailable or cipher does not look clearly modern (heuristic).
WS-SRV-001	No server version disclosure	FAIL	Severity.MEDIUM	Server: nginx/1.24.0 (Ubuntu). Version exposed.
WS-DIR-001	Directory listing disabled	PASS	Severity.MEDIUM	Directory listing disabled
WS-LIMIT-001	Request size limits	WARN	Severity.LOW	No direct request limit test available. Content-Length: 117

CONTAINER Layer Findings

ID	Check	Status	Severity	Details
CONT-USER-001	Non-root container user	WARN	Severity.HIGH	Docker error while checking container user: Docker daemon not accessible (Error while fetching server API version: (2, 'CreateFile', 'The system cannot find the file specified.'))
CONT-PORT-001	Minimal exposed ports	WARN	Severity.MEDIUM	Docker error while checking ports: Docker daemon not accessible (Error while fetching server API version: (2, 'CreateFile', 'The system cannot find the file specified.'))
CONT-RES-001	Resource limits configured	WARN	Severity.MEDIUM	Docker error while checking resource limits: Docker daemon not accessible (Error while fetching server API version: (2, 'CreateFile', 'The system cannot find the file specified.')).
CONT-HEALTH-001	Healthcheck configured	WARN	Severity.MEDIUM	Docker error while checking healthcheck: Docker daemon not accessible (Error while fetching server API version: (2, 'CreateFile', 'The system cannot find the file specified.')).
CONT-REG-001	Trusted image registry	WARN	Severity.MEDIUM	Docker error while checking image registry: Docker daemon not accessible (Error while fetching server API version: (2, 'CreateFile', 'The system cannot find the file specified.')).
CONT-SEC-001	No secrets in environment	WARN	Severity.HIGH	Docker error while checking environment secrets: Docker daemon not accessible (Error while fetching server API version: (2, 'CreateFile', 'The system cannot find the file specified.')).

HOST Layer Findings

ID	Check	Status	Severity	Details
HOST-SSH-001	SSH hardening	PASS	Severity.HIGH	SSH root login disabled ✓ (PermitRootLogin yes)
HOST-FW-001	Firewall enabled	WARN	Severity.HIGH	Could not confirm active firewall (ufw not found). Review iptables/nftables rules.
HOST-SVC-001	Minimal services running	PASS	Severity.MEDIUM	31 services: acceptable
HOST-UPDATE-001	Automatic updates configured	WARN	Severity.MEDIUM	Install: apt install unattended-upgrades && systemctl enable
HOST-PERM-001	Secure SSH file permissions	PASS	Severity.MEDIUM	No insecure permissions detected
HOST-LOG-001	Logging service active	WARN	Severity.LOW	Install logging: apt install rsyslog
HOST-SVC-GUNICORN	Gunicorn runs as non-root	PASS	Severity.HIGH	Gunicorn runs as non-root user 'www-data' ✓
HOST-SVC-UWSGI	uWSGI runs as non-root	PASS	Severity.HIGH	uWSGI runs as non-root user "" ✓
HOST-SVC-MYSQL	MySQL runs as non-root	PASS	Severity.HIGH	MySQL runs as non-root user "" ✓
HOST-SVC-REDIS	Redis runs as non-root	PASS	Severity.HIGH	Redis runs as non-root user 'redis' ✓

Critical Attack Paths

#	Attack Path	Risk	Score
1	Web → Container Escape	HIGH	8.5
2	Server → Internal Services	MEDIUM	6.5

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

Recommended Next Actions

1	Enable HSTS (Strict-Transport-Security) to enforce HTTPS on all responses.
2	Update TLS configuration to disable weak protocols/ciphers and prefer TLS 1.2+.

3	Review container images to ensure non-root users, minimal exposed ports, and no secrets baked into images.
4	Review host OS hardening: firewall rules, automatic security updates, logging and file permissions.

Server Fingerprint

Detected Stack	Nginx + Docker + Ubuntu
Inference Method	HTTP headers, framework behaviours, container/host findings