

## Security Audit Framework

# Security Audit Report

Target: https://vickkykruzprogramming.dev/admin/page/home

Scan Mode: full

Generated: 2026-02-24T00:03:00.679602Z

## Executive Summary

# Grade

Score

12.5%

Passed

3 / 24

High Risk

8

### AI-GENERATED ASSESSMENT

The current security posture is Grade.F with 3 of 24 checks passing (12.5% overall). There are 8 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	33.3% (2/6)	■	HIGH
Web Server	16.7% (1/6)	■	HIGH
Container	0.0% (0/6)	■	HIGH
Host	0.0% (0/6)	■	HIGH

## Configuration Drift vs Hardened Flask LMS

Grade Delta	Grade.F vs A
Pass Delta	-19 checks vs baseline
Improved Checks	None

<b>Regressed Checks</b>	APP-COOKIE-001, APP-CSRF-001, APP-RATE-001, APP-PASS-001, 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-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	Severity.HIGH	No obvious debug/traceback content in root response.
APP-COOKIE-001	Secure session cookies	WARN	Severity.HIGH	No cookies observed on root response; cannot assess session cookie security.
APP-CSRF-001	CSRF protection enabled	FAIL	Severity.MEDIUM	CSRF patterns missing.
APP-ADMIN-001	No exposed admin endpoints	PASS	Severity.MEDIUM	Admin paths none found.
APP-RATE-001	Rate limiting configured	WARN	Severity.MEDIUM	Rate limiting not evident.
APP-PASS-001	Strong password policy	WARN	Severity.LOW	Password hints: 0/5 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: ['Server', 'Date', 'Content-Type', 'Content-Length', 'Connection']
WS-TLS-001	TLS 1.2+ with strong ciphers	WARN	Severity.HIGH	TLS details unavailable or legacy cipher detected
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: 141

## CONTAINER Layer Findings

ID	Check	Status	Severity	Details
CONT-USER-001	Non-root container user	WARN	Severity.HIGH	Pending Docker API - requires 'docker inspect' to check USER directive
CONT-PORT-001	Minimal ports exposed	WARN	Severity.MEDIUM	Pending Docker API - requires 'docker ps' to check port bindings
CONT-RES-001	Resource limits configured	WARN	Severity.MEDIUM	Pending Docker API - requires docker-compose.yml CPU/memory limits check
CONT-HEALTH-001	Health checks configured	WARN	Severity.LOW	Pending Docker API - requires Dockerfile HEALTHCHECK directive
CONT-REG-001	Trusted image registry	WARN	Severity.MEDIUM	Pending Docker API - requires image source validation
CONT-SEC-001	No hardcoded secrets	WARN	Severity.CRITICAL	Pending file parsing - requires docker-compose.yml secret scanning

## HOST Layer Findings

ID	Check	Status	Severity	Details
HOST-SSH-001	SSH hardened configuration	WARN	Severity.HIGH	Pending SSH connection - requires 'cat /etc/ssh/sshd_config   grep PermitRootLogin' (should be 'no')
HOST-SVC-001	No unnecessary services	WARN	Severity.MEDIUM	Pending SSH - requires 'systemctl list-units --type=service --state=running' to check for risky services
HOST-UPDATE-001	Automatic security updates	WARN	Severity.MEDIUM	Pending SSH - requires 'systemctl is-enabled unattended-upgrades' (should be 'enabled')
HOST-PERM-001	Correct file permissions	WARN	Severity.HIGH	Pending SSH - requires 'find /etc -perm -o+w -ls 2>/dev/null' (no world-writable files)
HOST-FW-001	Firewall configured	WARN	Severity.HIGH	Pending SSH - requires 'ufw status' or 'iptables -L' (firewall should be active)
HOST-LOG-001	Logging and monitoring	WARN	Severity.MEDIUM	Pending SSH - requires 'systemctl is-active rsyslog' and '/var/log/auth.log' writable

## 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 Harden session cookies (set Secure, HttpOnly and SameSite attributes).
- 3 Update TLS configuration to disable weak protocols/ciphers and prefer TLS 1.2+.

4	Harden SSH by disabling root login and password authentication, and using key-based access.
5	Review container images to ensure non-root users, minimal exposed ports, and no secrets baked into images.

## Server Fingerprint

---

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