Security Audit Framework Report

Target: https://vickkykruzprogramming.dev
Scan Mode: full
Generated: 2026-02-23T16:25:15.216220Z

■ EXECUTIVE SUMMARY

OVERALL GRADE	Grade.F (29.2%)
Total Checks	24
Passed	7
High Risk Issues	7

■ CONFIGURATION DRIFT (vs Hardened Flask LMS)

Grade: Grade.F vs A
Pass delta: -15 checks vs baseline
Improved checks: None
Regressed checks: WS-HSTS-001, WS-SEC-001, WS-TLS-001, WS-SRV-001, WS-LIMIT-001

Risk Level: ■ HIGH RISK

■ APP LAYER FINDINGS

ID	Check	Status	Severity	Details
APP-DEBUG-001	Debug mode disabled	■ Status.PASS	Severity.HIGH	No obvious debug/traceback content in root respo
APP-COOKIE-001	Secure session cookies	■ Status.PASS	Severity.HIGH	At least one cookie appears to use both Secure ar
APP-CSRF-001	CSRF protection enabled	■ Status.PASS	Severity.MEDIUM	CSRF patterns detected.
APP-ADMIN-001	No exposed admin endpoints	■ Status.PASS	Severity.MEDIUM	Admin paths none found.
APP-RATE-001	Rate limiting configured	■ Status.PASS	Severity.MEDIUM	Rate limiting detected (429).
APP-PASS-001	Strong password policy	■ Status.PASS	Severity.LOW	Password hints: 2/5 complexity requirements ment

■ WEBSERVER LAYER FINDINGS

ID	Check	Status	Severity	Details
WS-HSTS-001	HSTS header enabled	■ Status.FAIL	Severity.HIGH	Strict-Transport-Security header is missing.
WS-SEC-001	Security headers present	■ Status.FAIL	Severity.HIGH	0/4 security headers present: ['Server', 'Date', 'Cor
WS-TLS-001	TLS 1.2+ with strong ciphers	■■ Status.WARN	Severity.HIGH	TLS details unavailable or legacy cipher detected
WS-SRV-001	No server version disclosure	■ Status.FAIL	Severity.MEDIUM	Server: nginx/1.24.0 (Ubuntu). Version exposed.
WS-DIR-001	Directory listing disabled	■ Status.PASS	Severity.MEDIUM	Directory listing disabled
WS-LIMIT-001	Request size limits	■■ Status.WARN	Severity.LOW	No direct request limit test available. Content-Leng

■ CONTAINER LAYER FINDINGS

ID	Check	Status	Severity	Details
CONT-USER-001	Non-root container user	■■ Status.WARN	Severity.HIGH	Pending Docker API - requires 'docker inspect' to c
CONT-PORT-001	Minimal ports exposed	■■ Status.WARN	Severity.MEDIUM	Pending Docker API - requires 'docker ps' to check
CONT-RES-001	Resource limits configured	■■ Status.WARN	Severity.MEDIUM	Pending Docker API - requires docker-compose.yr
CONT-HEALTH-001	Health checks configured	■■ Status.WARN	Severity.LOW	Pending Docker API - requires Dockerfile HEALTH
CONT-REG-001	Trusted image registry	■■ Status.WARN	Severity.MEDIUM	Pending Docker API - requires image source valid
CONT-SEC-001	No hardcoded secrets	■■ Status.WARN	Severity.CRITICAL	Pending file parsing - requires docker-compose.ym

■ HOST LAYER FINDINGS

ID	Check	Status	Severity	Details
HOST-SSH-001	SSH hardened configuration	■■ Status.WARN	Severity.HIGH	Pending SSH connection - requires 'cat /etc/ssh/ss
HOST-SVC-001	No unnecessary services	■■ Status.WARN	Severity.MEDIUM	Pending SSH - requires 'systemctl list-units --type=
HOST-UPDATE-001	Automatic security updates	■■ Status.WARN	Severity.MEDIUM	Pending SSH - requires 'systemctl is-enabled unat
HOST-PERM-001	Correct file permissions	■■ Status.WARN	Severity.HIGH	Pending SSH - requires 'find /etc -perm -o+w -ls 2>
HOST-FW-001	Firewall configured	■■ Status.WARN	Severity.HIGH	Pending SSH - requires 'ufw status' or 'iptables -L'
HOST-LOG-001	Logging and monitoring	■■ Status.WARN	Severity.MEDIUM	Pending SSH - requires 'systemctl is-active rsyslog

■ 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. Fix highest-risk paths first.

■ SERVER FINGERPRINT

Detected stack: **Nginx + Docker + Ubuntu**

This fingerprint is inferred from HTTP headers, framework-specific behaviours, and container/host findings where available.