Security Audit Framework

Security Audit Report

Target: https://vickkykruzprogramming.dev

Scan Mode: full

Generated: 2026-02-25T20:07:06.086556Z

Executive Summary

Grade.F

Score	50.0%
Passed	6 / 24
High Risk	3

AI-GENERATED ASSESSMENT

The current security posture is Grade.F with 6 of 24 checks passing (50.0% overall). There are 3 high-severity issues, mainly concentrated in the infrastructure, which significantly increases the likelihood of successful attacks in that area. The analysis also identified 1 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	83.3% (5/6)	■	LOW
Web Server	16.7% (1/6)	■	HIGH

Configuration Drift vs Hardened Flask LMS

Grade Delta	Grade.F vs A
Pass Delta	-16 checks vs baseline
Improved Checks	None
Regressed Checks	APP-RATE-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	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	WARN	Severity.MEDIUM	Rate limiting not evident.
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: ['Server', 'Date', 'Content-Type', 'Transfer-Encoding', 'Connection', 'Vary', 'Content-Encoding']
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: 0

NON-ROOT CONTAINER USER Layer Findings

ID	Check	Status	Severity	Details
CONT-USER-001	Container	**HIGH**	Status.WARN	Docker host not specified (--docker-host required for full mode)

MINIMAL EXPOSED PORTS Layer Findings

ID	Check	Status	Severity	Details
CONT-PORT-001	Container	**MEDIUM**	Status.WARN	Docker host not specified

RESOURCE LIMITS CONFIGURED Layer Findings

ID	Check	Status	Severity	Details
CONT-RES-001	Container	**MEDIUM**	Status.WARN	Docker host not specified

HEALTHCHECK CONFIGURED Layer Findings

ID	Check	Status	Severity	Details
CONT-HEALTH-001	Container	**MEDIUM**	Status.WARN	Docker host not specified

TRUSTED IMAGE REGISTRY Layer Findings

ID	Check	Status	Severity	Details
CONT-REG-001	Container	**MEDIUM**	Status.WARN	Docker host not specified

NO SECRETS IN ENVIRONMENT Layer Findings

ID	Check	Status	Severity	Details
CONT-SEC-001	Container	**HIGH**	Status.WARN	Docker host not specified

SSH HARDENING Layer Findings

ID	Check	Status	Severity	Details
HOST-SSH-001	Host	**HIGH**	Status.WARN	Authentication failed.

FIREWALL ENABLED Layer Findings

ID	Check	Status	Severity	Details
HOST-FW-001	Host	**HIGH**	Status.WARN	Authentication failed.

MINIMAL SERVICES Layer Findings

ID	Check	Status	Severity	Details
HOST-SVC-001	Host	**MEDIUM**	Status.WARN	Authentication failed.

AUTO-UPDATES ENABLED Layer Findings

ID	Check	Status	Severity	Details
HOST-UPDATE-001	Host	**MEDIUM**	Status.WARN	Authentication failed.

SECURE PERMISSIONS Layer Findings

ID	Check	Status	Severity	Details
HOST-PERM-001	Host	**MEDIUM**	Status.WARN	Authentication failed.

LOGGING CONFIGURED Layer Findings

ID	Check	Status	Severity	Details
HOST-LOG-001	Host	**LOW**	Status.WARN	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	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	Harden SSH by disabling root login and password authentication, and using key-based access.

Server Fingerprint

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