

■■ Security Audit Framework Report

Target: <https://vickkykruzprogramming.dev>

Scan Mode: full

Generated: 2026-02-22T21:26:35.619161Z

■ EXECUTIVE SUMMARY

OVERALL GRADE	Grade.F (25.0%)
Total Checks	24
Passed	6
High Risk Issues	7

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 response.
APP-COOKIE-001	Secure session cookies	█ Status.PASS	Severity.HIGH	At least one cookie appears to use both Secure and HttpOnly flags.
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.WARN	Severity.MEDIUM	Rate limiting not evident.
APP-PASS-001	Strong password policy	█ Status.PASS	Severity.LOW	Password hints: 3/5 complexity requirements met.

■ WEB SERVER 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', 'Content-Type', 'Content-Security-Policy']
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-Length header checked.

■ 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 check.
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.yml file.
CONT-HEALTH-001	Health checks configured	█ Status.WARN	Severity.LOW	Pending Docker API - requires Dockerfile HEALTHCHECK command.
CONT-REG-001	Trusted image registry	█ Status.WARN	Severity.MEDIUM	Pending Docker API - requires image source validation.
CONT-SEC-001	No hardcoded secrets	█ Status.WARN	Severity.CRITICAL	Pending file parsing - requires docker-compose.yml file.

■ 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/sshd_config' to check.
HOST-SVC-001	No unnecessary services	█ Status.WARN	Severity.MEDIUM	Pending SSH - requires 'systemctl list-units --type=service' to check.
HOST-UPDATE-001	Automatic security updates	█ Status.WARN	Severity.MEDIUM	Pending SSH - requires 'systemctl is-enabled unattended-upgrades' to check.
HOST-PERM-001	Correct file permissions	█ Status.WARN	Severity.HIGH	Pending SSH - requires 'find /etc -perm -o+w -ls 2>/dev/null' to check.
HOST-FW-001	Firewall configured	█ Status.WARN	Severity.HIGH	Pending SSH - requires 'ufw status' or 'iptables -L' to check.
HOST-LOG-001	Logging and monitoring	█ Status.WARN	Severity.MEDIUM	Pending SSH - requires 'systemctl is-active rsyslog' to check.

■ PRIORITY REMEDIATION

Priority	Issue	Recommended Fix
#1	WS-HSTS-001: HSTS header enabled	Strict-Transport-Security header is missing.
#2	WS-SEC-001: Security headers present	0/4 security headers present: ['Server', 'Date', 'Content-Type', 'Content-Security-Policy']

#3	WS-TLS-001: TLS 1.2+ with strong ciphers	TLS details unavailable or legacy cipher detected
#4	CONT-USER-001: Non-root container user	Pending Docker API - requires 'docker inspect' to check USER directory
#5	HOST-SSH-001: SSH hardened configuration	Pending SSH connection - requires 'cat /etc/ssh/sshd_config grep'
#6	HOST-PERM-001: Correct file permissions	Pending SSH - requires 'find /etc -perm -o+w -ls 2>/dev/null' (no warning)
#7	HOST-FW-001: Firewall configured	Pending SSH - requires 'ufw status' or 'iptables -L' (firewall should be active)

■ SERVER FINGERPRINT

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

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