SECURITY AUDIT REPORT

Export PDF

Generated 6 de abril de 2026 às 11:02 · 112 findings analyzed

01 EXECUTIVE SUMMARY

/100

Critical

Overall Risk Score

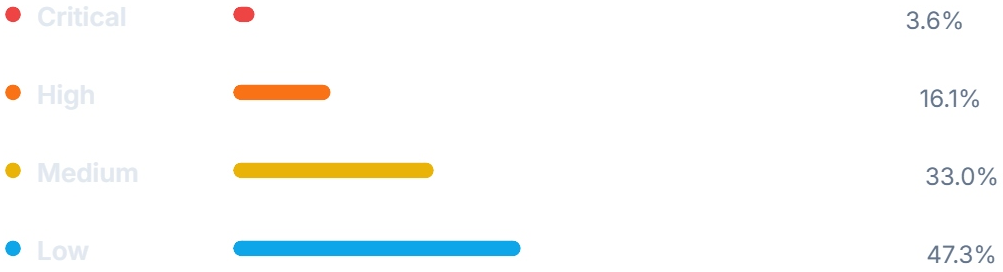
TOTAL FINDINGS

PENDING TRIAGE

CRITICAL + HIGH

22

02 SEVERITY DISTRIBUTION



Critical	4	3.6%
High	18	16.1%
Medium	37	33.0%
Low	53	47.3%

03 COVERAGE BY SOURCE

FORTIFY SAST

55.4% of total

SONATYPE SCA

33.9% of total

PENTEST

8.0% of total

MANUAL REVIEW

2.7% of total

04 TOP VULNERABILITIES

#	FINDING	SEVERITY	SOURCE
01	SQL Injection in UserRepository.findByEmail()	CRITICAL	FORTIFY_SAST
02	Hardcoded AWS Secret Key in CloudStorageConfig	CRITICAL	FORTIFY_SAST
03	Broken Access Control — IDOR on /api/v1/users/{id}/profile	CRITICAL	PENTEST
04	CVE-2026-21345 — Remote Code Execution in log4j-core 2.17.0	CRITICAL	SONATYPE_SCA
05	Cross-Site Scripting (Reflected) in SearchController	HIGH	FORTIFY_SAST
06	CVE-2025-48271 — Deserialization of Untrusted Data in jackson	HIGH	SONATYPE_SCA
07	Path Traversal in FileUploadService.store()	HIGH	FORTIFY_SAST
08	Server-Side Request Forgery via PDF Generation Endpoint	HIGH	PENTEST
09	CVE-2026-10892 — Prototype Pollution in lodash 4.17.21	MEDIUM	SONATYPE_SCA
10	Missing CSRF Token Validation on /api/v1/settings	MEDIUM	FORTIFY_SAST

05 METHODOLOGY & SCOPE

All applications and repositories connected through the Security Hub platform, including SAST (Static Analysis), SCA (Software Composition Analysis), and manual pentest findings.

Findings are ingested from configured connectors including Fortify SSC (SAST), Sonatype IQ (SCA), and manual imports. Each finding is normalized to a unified severity scale.

Risk scores are calculated using a weighted severity model: Critical findings carry a 25-point penalty, High findings 10 points, and Medium findings 3 points against a base score of 100.

CONFIDENTIAL — This report contains sensitive security information and should be shared only with authorized personnel.