SCAN SUMMARY · 2026-05-01

Vulnerability findings for github.com

https://github.com/ · 20.87.245.0

The latest scan identified 23 findings across the public-facing infrastructure. No critical or high-severity issues were observed in this run. 3 medium-severity item(s) should be scheduled for the next change window. Low: 9, Informational: 11.

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	3	9	11

REPORT	SCAN	TOOLS
5c6aa6e9	16:43 UTC	httpx · nmap · zap

Medium severity

3 FINDINGS

M-01 **CSP: style-src unsafe-inline** MEDIUM
— · 5 instance(s)

M-02 **Source Code Disclosure - SQL** MEDIUM
— · 1 instance(s)

M-03 **Sub Resource Integrity Attribute Missing** MEDIUM
— · 5 instance(s)

Low severity

9 FINDINGS

L-01 **Cookie No HttpOnly Flag** LOW
— · 3 instance(s)

L-02 **Cross-Domain JavaScript Source File Inclusion** LOW
— · 5 instance(s)

L-03 **Cross-Origin-Embedder-Policy Header Missing or Invalid** LOW
— · 3 instance(s)

L-04 **Cross-Origin-Opener-Policy Header Missing or Invalid** LOW
— · 3 instance(s)

L-05 **Cross-Origin-Resource-Policy Header Missing or Invalid** LOW
— · 4 instance(s)

L-06 **Information Disclosure - Debug Error Messages** LOW
— · 1 instance(s)

L-07 **Permissions Policy Header Not Set** LOW
— · 5 instance(s)

L-08 **Timestamp Disclosure - Unix** LOW
— · 5 instance(s)

L-09 **X-Content-Type-Options Header Missing** LOW

— · 3 instance(s)

Informational

11 FINDINGS

3 network observation(s) on 20.87.245.0: ssh/22, http/80, https/443 plus httpx (1).

The detailed HTML report (full_vulnerable_reports) lists evidence, endpoints, and remediation text where the scanner provided it.

REPORT 5c6aa6e9
2026-05-01