

SCAN SUMMARY · 2026-05-24

Vulnerability findings for facebook.com

https://www.facebook.com/ · 102.132.99.35

The latest scan identified 24 findings across the public-facing infrastructure. No critical or high-severity issues were observed in this run. 4 medium-severity item(s) should be scheduled for the next change window. Low: 7, Informational: 13.

CRITICAL 0	HIGH 0	MEDIUM 4	LOW 7	INFO 13
REPORT 0cace22c	SCAN 23:08 UTC	TOOLS httpx · nmap · subfinder · zap		

Medium severity

4 FINDINGS

M-01	CSP: Failure to Define Directive with No Fallback — · 5 instance(s)	MEDIUM
M-02	CSP: script-src unsafe-eval — · 5 instance(s)	MEDIUM
M-03	CSP: style-src unsafe-inline — · 5 instance(s)	MEDIUM
M-04	Sub Resource Integrity Attribute Missing — · 5 instance(s)	MEDIUM

Low severity

7 FINDINGS

L-01	Cookie No HttpOnly Flag — · 1 instance(s)	LOW
L-02	Cookie without SameSite Attribute — · 2 instance(s)	LOW
L-03	Cross-Domain JavaScript Source File Inclusion — · 2 instance(s)	LOW
L-04	Cross-Origin-Embedder-Policy Header Missing or Invalid — · 2 instance(s)	LOW
L-05	Cross-Origin-Opener-Policy Header Missing or Invalid — · 2 instance(s)	LOW
L-06	Permissions Policy Header Not Set — · 5 instance(s)	LOW
L-07	Timestamp Disclosure - Unix — · 2 instance(s)	LOW

Informational

13 FINDINGS

2 network observation(s) on 102.132.99.35: http/80, https/443 plus httpx (1) plus subfinder (6).

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

This message contains confidential security information.
Do not forward outside the intended recipient list.

REPORT 0cace22c
2026-05-24

Facebook · Automated security scan summary