SCAN SUMMARY · 2026-05-04

Vulnerability findings for juice-shop.github.io

https://juice-shop.github.io/ · 185.199.110.153

The latest scan identified 17 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: 6, Informational: 7.

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	4	6	7

REPORT	SCAN	TOOLS
2742e806	09:16 UTC	httpx · nmap · zap

Medium severity

4 FINDINGS

M-01 **Content Security Policy (CSP) Header Not Set** MEDIUM
— · 5 instance(s)

M-02 **Cross-Domain Misconfiguration** MEDIUM
— · 5 instance(s)

M-03 **Missing Anti-clickjacking Header** MEDIUM
— · 5 instance(s)

M-04 **Sub Resource Integrity Attribute Missing** MEDIUM
— · 5 instance(s)

Low severity

6 FINDINGS

L-01 **Cross-Domain JavaScript Source File Inclusion** LOW
— · 5 instance(s)

L-02 **Cross-Origin-Embedder-Policy Header Missing or Invalid** LOW
— · 5 instance(s)

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

L-04 **Permissions Policy Header Not Set** LOW
— · 5 instance(s)

L-05 **Strict-Transport-Security Header Not Set** LOW
— · 5 instance(s)

L-06 **X-Content-Type-Options Header Missing** LOW
— · 5 instance(s)

Informational

7 FINDINGS

2 network observation(s) on 185.199.110.153: 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.