Ahmed Nouralla's Org

Scan Report

juice-shop
Development

Completed On
Nov 23, 2022 at 18:21 MSK

juice-shop

Development

Scan Date: Nov 23, 2022 at 18:21 MSK | Paths Scanned: 11 | Scan Duration: 1 minute

High	Medium	Low	New	Assigned	Risk Accepted	False Positive
0	11	2	13	0	0	0

Findings

Criticality	Finding	New	Assigned	Risk Accepted	False Positive
Medium	Content Security Policy (CSP) Header Not Set	2	0	0	0
Medium	Cross-Domain Misconfiguration	9	0	0	0
Low	Cross-Domain JavaScript Source File Inclusion	2	0	0	0

Finding Details

Content Security Policy (CSP) Header Not Set

Criticality: MEDIUM

Category: Information Leakage

Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Path	Method	Status
/sitemap.xml	GET	New
[root]	GET	New

Cross-Domain Misconfiguration

Criticality: MEDIUM

Category: Information Leakage

Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server

Path	Method	Status
/sitemap.xml	GET	New
/polyfills.js	GET	New
[root]	GET	New
/runtime.js	GET	New
/robots.txt	GET	New
/styles.css	GET	New
/main.js	GET	New
/assets/public/favicon_js.ico	GET	New
/vendor.js	GET	New

Cross-Domain JavaScript Source File Inclusion

Criticality: LOW

Category: Information Leakage

Description: The page includes one or more script files from a third-party domain.

Path	Method	Status
[root]	GET	New
/sitemap.xml	GET	New