Ahmed Nouralla's Org

Scan Report

juice-shop
Development

Completed On
Nov 23, 2022 at 19:12 MSK

juice-shop

Development

Scan Date: Nov 23, 2022 at 19:12 MSK | Paths Scanned: 83 | Scan Duration: 1 minute and 25 seconds

High	Medium	Low	New	Assigned	Risk Accepted	False Positive
0	28	9	37	0	0	0

Findings

Criticality	Finding	New	Assigned	Risk Accepted	False Positive
Medium	Cross-Domain Misconfiguration	13	0	0	0
Medium	Content Security Policy (CSP) Header Not Set	15	0	0	0
Low	Private IP Disclosure	1	0	0	0

Low	Cross-Domain JavaScript Source File Inclusion	7	0	0	0
Low	Application Error Disclosure	1	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
/juice-shop/build/routes/assets/public/favicon_js.ico	GET	New
/juice-shop/build/routes/polyfills.js	GET	New
/juice-shop/node_modules/graceful-fs/vendor.js	GET	New
/juice-shop/build/routes/main.js	GET	New
/juice-shop/build/routes/userProfile.js:69:22	GET	New
/juice-shop/node_modules/graceful-fs/styles.css	GET	New
/juice-shop/node_modules/graceful-fs/graceful-fs.js:123:16	GET	New
/juice-shop/build/routes/vendor.js	GET	New
[root]	GET	New
/juice-shop/build/routes/runtime.js	GET	New
/juice-shop/node_modules/graceful-fs/assets/public/favicon_js.ico	GET	New
/profile	GET	New
/juice-shop/build/routes/styles.css	GET	New
/sitemap.xml	GET	New
/juice-shop/node_modules/graceful-fs/runtime.js	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
/main.js	GET	New
/assets/public/favicon_js.ico	GET	New
/vendor.js	GET	New
/runtime.js	GET	New
/sitemap.xml	GET	New
/polyfills.js	GET	New
/profile	GET	New
/juice-shop/node_modules/graceful-fs/assets/public/favicon_js.ico	GET	New
/styles.css	GET	New
/robots.txt	GET	New
[root]	GET	New
/juice-shop/node_modules/graceful-fs/graceful-fs.js:123:16	GET	New
/juice-shop/build/routes/userProfile.js:69:22	GET	New

Private IP Disclosure

Criticality: LOW

Category: Information Leakage

Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

Path	Method	Status
/profile	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
/juice-shop/node_modules/graceful-fs/graceful-fs.js:123:16	GET	New
/juice-shop/build/routes/assets/public/favicon_js.ico	GET	New
/juice-shop/build/routes/userProfile.js:69:22	GET	New
/juice-shop/node_modules/graceful-fs/assets/public/favicon_js.ico	GET	New
/juice-shop/node_modules/graceful-fs/styles.css	GET	New
[root]	GET	New
/sitemap.xml	GET	New

Application Error Disclosure

Criticality: `LOW`

Category: Information Leakage

Description: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Path	Method	Status
/profile	GET	New