

## (Executive Summary)

This report presents the results of a web application vulnerability assessment performed on the target application hosted at http://localhost:3000 using OWASP ZAP, a leading open-source security scanning tool. The assessment was conducted to identify and analyze potential security flaws that could be exploited by malicious actors. During the evaluation, multiple vulnerabilities were discovered that align with the OWASP Top 10 Web Application Security Risks, including a critical SQL Injection vulnerability via the q parameter, which triggered backend SQLite errors. This confirmed a lack of proper input validation and a high risk of unauthorized data access or manipulation. Additional findings included the absence of essential security headers such as Content Security Policy (CSP) and X-Frame-Options, exposing the application to clickjacking and content injection attacks. The application was also observed to expose session IDs in the URL, increasing the risk of session hijacking through shared links or browser history.

Furthermore, the use of an outdated and vulnerable JavaScript library and cross-domain misconfigurations were noted, which may lead to unauthorized cross-origin access or data leakage.

All findings were identified and verified using OWASP ZAP, and this report outlines each vulnerability in detail along with its potential impact and suggested mitigation strategies. The results reflect a need for improved secure coding practices and enhanced server configuration to safeguard the application against common web-based threats.

Sites: http://cdnjs.cloudflare.com http://localhost:3000

Generated on Sat, 21 Jun 2025 10:33:26

ZAP Version: 2.16.1

ZAP by Checkmarx

## **Summary of Alerts**

Risk Level	Number of Alerts
High	1
Medium	5
Low	4
Informational	4

## **Alerts**

Name	Risk Level	Number of Instances
SQL Injection - SQLite	High	1
Content Security Policy (CSP) Header Not Set	Medium	61
Cross-Domain Misconfiguration	Medium	97
Missing Anti-clickjacking Header	Medium	3
Session ID in URL Rewrite	Medium	17
Vulnerable JS Library	Medium	1
Cross-Domain JavaScript Source File Inclusion	Low	98

Private IP Disclosure	Low	1
<u>Timestamp Disclosure - Unix</u>	Low	162
X-Content-Type-Options Header Missing	Low	17
Information Disclosure - Suspicious Comments	Informational	3
Modern Web Application	Informational	50
Retrieved from Cache	Informational	3
User Agent Fuzzer	Informational	120

## **Alert Detail**

High	SQL Injection - SQLite
Description	SQL injection may be possible.
URL	http://localhost:3000/rest/products/search?q=%27%28
Method	GET
Attack	)'
Evidence	SQLITE_ERROR
Other Info	RDBMS [SQLite] likely, given error message regular expression [SQLITE_ERROR] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
Instances	1
Solution	Do not trust client side input, even if there is client side validation in place.  In general, type check all data on the server side.  If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'  If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries.  If database Stored Procedures can be used, use them.  Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality!  Do not create dynamic SQL queries using simple string concatenation.  Escape all data received from the client.  Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input.  Apply the principle of least privilege by using the least privileged database user possible.  In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL
	injection, but minimizes its impact.  Grant the minimum database access that is necessary for the application.  https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.
Reference	html
CWE Id	89
WASC Id	19
Plugin Id	40018
Medium	Content Security Policy (CSP) Header Not Set

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.
URL	http://localhost:3000
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/coupons_2013.md.bak
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/eastere.gg
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/encrypt.pyc
Method	GET

Attack	
Evidence	
Other	
Info	
URL	http://localhost:3000/ftp/package-lock.json.bak
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/package.json.bak
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/quarantine
Method	GET
Attack	
Evidence	
Other	
Info	
URL	http://localhost:3000/ftp/suspicious_errors.yml
	http://localhost:3000/ftp/suspicious_errors.yml GET
URL	
URL Method	
URL Method Attack	
URL Method Attack Evidence Other	
URL Method Attack Evidence Other Info	GET
URL  Method  Attack  Evidence  Other Info  URL	GET  http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico
URL  Method  Attack  Evidence  Other Info  URL  Method	GET  http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack	GET  http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other	GET  http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico  GET
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  URL  URL  Method  Attack  URL  URL  URL  URL  URL  URL	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico  GET  http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico  GET  http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Attack  Evidence  Other Info  URL  Method  Attack	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico  GET  http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico
URL  Method  Attack  Evidence  Other Info	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico  GET  http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico
URL  Method  Attack  Evidence  Other Info	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico  GET  http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico  GET
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  URL  URL  URL  URL  URL  URL	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico  GET  http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico  GET  http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico

Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/polyfills.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/runtime.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:43:13
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/main.js
Method	GET
Attack	
Evidence	
Other Info	

URL	http://localhost:3000/juice-shop/build/routes/polyfills.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/runtime.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/main.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/polyfills.js

Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/runtime.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	

Evidence	
Other	
Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/main.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node modules/express/lib/router/runtime.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/styles.css
Method	GET
Attack	
Evidence	

Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/main.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/polyfills.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/runtime.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/styles.css
Method	GET
Attack	
Evidence	
Other Info	

Method GET  Attack Evidence Other Info  URL Method GET  Attack Evidence Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/index_is:145:39  Method GET  Attack Evidence Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/main_is  Method GET  Attack Evidence Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/polyfills_is  Method GET  Attack Evidence Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/runtime.js  Method GET  Attack Evidence Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/runtime.js  Method GET  Attack Evidence Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/vendor.js  Method GET	URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/vendor.js
Evidence Other Info URL bttp://localhost.3000/juice-shop/node_modules/serve-index/index.js:145:39  Method GET Attack Evidence Other Info URL bttp://localhost.3000/juice-shop/node_modules/serve-index/main.js  Method GET Attack Evidence Other Info URL bttp://localhost.3000/juice-shop/node_modules/serve-index/polyfills.js  Method GET  Attack Evidence Other Info URL bttp://localhost.3000/juice-shop/node_modules/serve-index/runtime.js  Method GET  Attack Evidence Other Info URL bttp://localhost.3000/juice-shop/node_modules/serve-index/runtime.js  Method GET  Attack Evidence Other Info URL bttp://localhost.3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info URL bttp://localhost.3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info URL bttp://localhost.3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info URL bttp://localhost.3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info URL bttp://localhost.3000/juice-shop/node_modules/serve-index/vendor.js	Method	GET
Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/index_is:145:39  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/main.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info	Attack	
Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/index.js:145:39  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/main.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info	Evidence	
Method GET Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/main.js  Method GET Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js  Method GET Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js  Method GET Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js  Method GET Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css Method GET Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET Attack Evidence Other Info		
Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/main.js  Method GET Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/polyfills.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/runtime.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info	URL	http://localhost:3000/juice-shop/node_modules/serve-index/index.js:145:39
Evidence Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/main.js  Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js Method GET Attack Evidence Other Info	Method	GET
Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/main.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info	Attack	
Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/main.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/funtime.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info	Evidence	
Method GET  Attack  Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js  Method GET  Attack  Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js  Method GET  Attack  Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js  Method GET  Attack  Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack  Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack  Evidence Other Info  Other Info  Other Info		
Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js  Method GET Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js  Method GET Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js  Method GET Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info  Other Info	URL	http://localhost:3000/juice-shop/node_modules/serve-index/main.js
Evidence Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/polyfills.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/runtime.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info	Method	GET
Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info  Other Info  Other Info  Other Info	Attack	
Info URL http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js  Method GET  Attack  Evidence Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js  Method GET  Attack  Evidence Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack  Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack  Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack  Evidence Other Info  Other Info  Other Info  Other Info	Evidence	
Method GET  Attack  Evidence  Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/runtime.js  Method GET  Attack  Evidence  Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/styles.css  Method GET  Attack  Evidence  Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/styles.css  Method GET  Attack  Evidence  Other Info  URL http://localhost:3000/juice-shop/node modules/serve-index/vendor.js  Method GET  Attack  Evidence  Other Info  Other Info		
Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info  Other Info	URL	http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js
Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js  Method GET Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info	Method	GET
Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info	Attack	
Info URL http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js  Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js Method GET Attack Evidence Other Info	Evidence	
Method GET  Attack  Evidence  Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack  Evidence  Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack  Evidence  Other Info  GET  Attack  Evidence  Other Info		
Attack Evidence  Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info  Other Info  Other Info  Other Info	URL	http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js
Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info	Method	GET
Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack  Evidence  Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack  Evidence  Other Info  Other Info	Attack	
Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence  Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence  Other Info	Evidence	
Method GET  Attack Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info		
Attack Evidence  Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info	URL	http://localhost:3000/juice-shop/node_modules/serve-index/styles.css
Evidence Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence Other Info	Method	GET
Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack  Evidence  Other Info	Attack	
Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack  Evidence  Other Info	Evidence	
Method GET  Attack  Evidence  Other Info		
Attack Evidence Other Info	URL	http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js
Evidence Other Info	Method	GET
Other Info	Attack	
Info	Evidence	
URL <a href="http://localhost:3000/sitemap.xml">http://localhost:3000/sitemap.xml</a>		
	URL	http://localhost:3000/sitemap.xml

Method	GET
Attack	
Evidence	
Other	
Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr2iZ&sid=Rw-fonf5fS-soOyqAAAC
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	
Evidence	
Other Info	
Instances	61
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
	https://developer.mozilla.org/en-US/docs/Web/Security/CSP /Introducing Content Security Policy
	https://cheatsheetseries.owasp.org/cheatsheets/Content Security Policy Cheat Sheet.html
Reference	https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/
	https://web.dev/articles/csp
	https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	<del>693</del>
WASC Id	15
Plugin Id	10038
Medium	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Method	GET
Attack	
, maon	

Access-Control-Allow-Origin: \*

Evidence

Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/api/Challenges/?name=Score%20Board
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
	The CORS misconfiguration on the web server permits cross-domain read requests from
	arbitrary third party domains, using unauthenticated APIs on this domain. Web browser

Other Info		
Method GET  Attack  Evidence  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  http://localhost.3000/assets/i18n/en.json  GET  Attack  Evidence  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  http://localhost.3000/assets/public/favicon_js.ico  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to rea		authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but
Attack Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third party dos somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  http://localhost.3000/assets/it8n/en.json  Method  GET  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  http://localhost.3000/assets/public/ravicon_is.ioo  GET  Attack  Evidence  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  http://localhost.3000/assets/public/images/luiceShop_Logo.png  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this doma	URL	http://localhost:3000/api/Quantitys/
Evidence  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  Method  GET  Attack  Evidence  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third party decuces the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  http://localhost.3000/assets/public/favicon_is.ico  Other  Info  Other  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third party comains. Web browser implementations do not permit arbitrary third party to read the response from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  http://localhost.3000/assets/public/images/products/apple_juice.jpg  The CORS misconfiguration on the web se	Method	GET
The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  Method  GET  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  http://localhost.3000/assets/public/favicon_js.ico  GET  Attack  Evidence  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  http://localhost.3000/assets/public/images/JuiceShop_Logo.png  Method  GET  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconf	Attack	
Other Info Info Info Info Info Info Info Info	Evidence	Access-Control-Allow-Origin: *
Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauuthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/lavicon_js.ico  GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/JuiceShop_Logo.png  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/products/apple_juice.jpg  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third		arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but
Attack  Evidence  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  http://localhost:3000/assets/public/favicon_is.ico  Method  GET  Attack  Evidence  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  http://localhost:3000/assets/public/images/JuiceShop_Logo.png  Method  GET  Attack  Evidence  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other from of security, such as IP address white-listing.  URL  http://localhost:3000/assets/public/images/products/apple_juice.jpg  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. W	URL	http://localhost:3000/assets/i18n/en.json
Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/favicon_is.ico  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, nowever. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/JuiceShop_Logo.png  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from arbitrary third parties to read the response from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from the which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/i	Method	GET
The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  http://localhost:3000/assets/public/lavicon_js.ico  Method  GET  Attack  Evidence  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  http://localhost:3000/assets/public/images/JuiceShop_Logo.png  Method  GET  Attack  Evidence  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs in domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL  http://localhost:3000/assets/public/images/products/apple_juice.jpg  Method  GET  Attack  Evidence  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third parties to read the response from arbitrary third p	Attack	
arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/favicon_js.ico  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs in this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/JuiceShop_Logo.png  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs in domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/products/apple_juice.jpg  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third parties to read the response from lathenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read t	Evidence	Access-Control-Allow-Origin: *
Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/JuiceShop_Logo.png  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/products/apple_juice.jpg  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from		arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but
Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/JuiceShop_Logo.png  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/products/apple_juice.jpg  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from	URL	http://localhost:3000/assets/public/favicon_js.ico
Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/JuiceShop_Logo.png  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/products/apple_juice.jpg  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from	Method	GET
The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/JuiceShop_Logo.png  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/products/apple_juice.jpg  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from	Attack	
Other Info authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/JuiceShop_Logo.png  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/products/apple_juice.jpg  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from	Evidence	Access-Control-Allow-Origin: *
Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/products/apple_juice.jpg  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from		arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but
Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/products/apple_juice.jpg  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from	URL	http://localhost:3000/assets/public/images/JuiceShop_Logo.png
Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL http://localhost:3000/assets/public/images/products/apple_juice.jpg  Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from	Method	GET
The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL <a href="http://localhost:3000/assets/public/images/products/apple_juice.jpg">http://localhost:3000/assets/public/images/products/apple_juice.jpg</a> Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from	Attack	
Other Info authenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  URL <a href="http://localhost:3000/assets/public/images/products/apple_juice.jpg">http://localhost:3000/assets/public/images/products/apple_juice.jpg</a> Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from	Evidence	Access-Control-Allow-Origin: *
Method GET  Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from		arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but
Attack  Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser other implementations do not permit arbitrary third parties to read the response from	URL	http://localhost:3000/assets/public/images/products/apple_juice.jpg
Evidence Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser other implementations do not permit arbitrary third parties to read the response from	Method	GET
The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser other implementations do not permit arbitrary third parties to read the response from	Attack	
Other arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from	Evidence	Access-Control-Allow-Origin: *
		arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from

	be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/products/apple_pressings.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/products/artwork2.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/products/banana_juice.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/products/carrot_juice.jpeg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/products/eggfruit_juice.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

1101	1
URL	http://localhost:3000/assets/public/images/products/fan_facemask.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/products/fruit_press.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/products/green_smoothie.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/products/lemon_juice.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/products/melon_bike.jpeg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/products/permafrost.jpg

Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/acquisitions.md
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/announcement_encrypted.md
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/coupons 2013.md.bak
Method	GET

Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/eastere.gg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/encrypt.pyc
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/incident-support.kdbx
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/legal.md
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/package-lock.json.bak
Method	GET
Attack	

Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/package.json.bak
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/quarantine
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/quarantine/juicy_malware_linux_amd_64.url
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/quarantine/juicy_malware_linux_arm_64.url
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/quarantine/juicy_malware_macos_64.url
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *

Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/quarantine/juicy_malware_windows_64.exe.url
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/suspicious_errors.yml
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/main.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
	-
	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser

Other Info	implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/polyfills.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/runtime.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/styles.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/vendor.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:43:13
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could

	he wood by an attacker to access data that is available in an authorities to be as
	be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/main.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/polyfills.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/runtime.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/styles.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

URL	http://localhost:3000/juice-shop/build/routes/vendor.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	$\underline{\text{http://localhost:3000/juice-shop/node modules/express/lib/router/assets/public/favicon\_js.ico}$
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node modules/express/lib/router/assets/public/main.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/polyfills.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/runtime.js

Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/styles.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET

Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/main.js
Method	GET
Attack	

Evidence	
	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/runtime.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/styles.css
Method	GET
Attack	
Attack Evidence	Access-Control-Allow-Origin: *
	Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Evidence Other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but
Evidence Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Evidence Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  http://localhost:3000/juice-shop/node_modules/express/lib/router/vendor.js
Other Info  URL  Method	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  http://localhost:3000/juice-shop/node_modules/express/lib/router/vendor.js
Other Info  URL  Method  Attack	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing. <a href="http://localhost:3000/juice-shop/node_modules/express/lib/router/vendor.js">http://localhost:3000/juice-shop/node_modules/express/lib/router/vendor.js</a> GET
Other Info  URL  Method  Attack  Evidence	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  http://localhost:3000/juice-shop/node_modules/express/lib/router/vendor.js  GET  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but
Other Info  URL  Method  Attack  Evidence  Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  http://localhost:3000/juice-shop/node modules/express/lib/router/vendor.js  GET  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  http://localhost:3000/juice-shop/node modules/serve-index/assets/public/assets/public
Other Info  URL  Method  Attack  Evidence  Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  http://localhost:3000/juice-shop/node modules/express/lib/router/vendor.js  GET  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  http://localhost:3000/juice-shop/node modules/serve-index/assets/public/assets/public/favicon_js.ico
Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  http://localhost:3000/juice-shop/node modules/express/lib/router/vendor.js  GET  Access-Control-Allow-Origin: *  The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.  http://localhost:3000/juice-shop/node modules/serve-index/assets/public/assets/public/favicon_js.ico

	Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
UR	L	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/favicon_js.ico
	Method	GET
	Attack	
	Evidence	Access-Control-Allow-Origin: *
	Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
UR	L	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/main.js
	Method	GET
	Attack	
	Evidence	Access-Control-Allow-Origin: *
	Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
UR	L	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/polyfills.js
	Method	GET
	Attack	
	Evidence	Access-Control-Allow-Origin: *
	Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
UR	L	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/runtime.js
	Method	GET
	Attack	
	Evidence	Access-Control-Allow-Origin: *
	Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
UR	L	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/styles.css
	Method	GET
	Attack	
	Evidence	Access-Control-Allow-Origin: *
		The CORS misconfiguration on the web server permits cross-domain read requests from
		arbitrary third party domains, using unauthenticated APIs on this domain. Web browser

Other Info	implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/vendor.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/index.js:145:39
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/main.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could

	be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/styles.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/main.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/Materiallcons-Regular.woff2
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/polyfills.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

URL	http://localhost:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/rest/admin/application-version
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/rest/languages
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/rest/products/search?q=
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/robots.txt
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/runtime.js

Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/vendor.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	97
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).  Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet. html5_overly_permissive_cors_policy
CWE Id	<u>264</u>
WASC Id	14
Plugin Id	10098
Medium	Missing Anti-clickjacking Header

Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr2iZ&sid=Rw-fonf5fS-soOyqAAAC
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8bl&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	
Evidence	
Other Info	
Instances	3
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.  If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	<u>1021</u>
WASC Id	15
Plugin Id	10020
Madium	Section ID in LIDI. Powrite
Medium  Description	URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site referer header. In addition, the session ID might be stored in browser history or server logs.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr2jl&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	Rw-fonf5fS-soOyqAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr3GH&sid=Rw-fonf5fS-soOyqAAAC

Method	GET
Attack	OL!
Evidence	Rw-fonf5fS-soOyqAAAC
Other Info	IXW-IUIII3I3-SUOYYAAAC
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr424&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	Rw-fonf5fS-soOyqAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr43V&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	Rw-fonf5fS-soOyqAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr452&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	Rw-fonf5fS-soOyqAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr47B&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	Rw-fonf5fS-soOyqAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr48L&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	Rw-fonf5fS-soOyqAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr4AU&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	Rw-fonf5fS-soOyqAAAC
Other Info	

URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr4Bk&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	Rw-fonf5fS-soOyqAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr4DU&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	Rw-fonf5fS-soOyqAAAC
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8cA&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	
Evidence	bbnwfd9qOchbbDn-AAAE
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9Qp&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	
Evidence	bbnwfd9qOchbbDn-AAAE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	
Evidence	bbnwfd9qOchbbDn-AAAE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	Rw-fonf5fS-soOyqAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr2iZ&sid=Rw-fonf5fS-soOyqAAAC
Method	POST
Attack	
Evidence	Rw-fonf5fS-soOyqAAAC

Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8bl&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	
Evidence	bbnwfd9qOchbbDn-AAAE
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	
Evidence	bbnwfd9qOchbbDn-AAAE
Other Info	
Instances	17
Solution	For secure content, put session ID in a cookie. To be even more secure consider using a combination of cookie and URL rewrite.
Reference	https://seclists.org/webappsec/2002/q4/111
CWE Id	<u>598</u>
WASC Id	13
Plugin Id	3
Medium	Vulnerable JS Library
Medium  Description	Vulnerable JS Library  The identified library appears to be vulnerable.
	•
Description	The identified library appears to be vulnerable.
Description URL	The identified library appears to be vulnerable. <a href="http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js</a>
Description URL Method	The identified library appears to be vulnerable. <a href="http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js</a>
Description  URL  Method  Attack	The identified library appears to be vulnerable.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET
Description  URL  Method  Attack  Evidence	The identified library appears to be vulnerable.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  /2.2.4/jquery.min.js  The identified library jquery, version 2.2.4 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://github.com/jquery/jquery.com/issues/162 https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-
Description  URL  Method  Attack  Evidence  Other Info	The identified library appears to be vulnerable.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  /2.2.4/jquery.min.js  The identified library jquery, version 2.2.4 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://github.com/jquery/jquery.com/issues/162 https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
Description  URL  Method  Attack  Evidence  Other Info	The identified library appears to be vulnerable.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  /2.2.4/jquery.min.js  The identified library jquery, version 2.2.4 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://github.com/jquery/jquery.com/issues/162 https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
Description  URL  Method  Attack  Evidence  Other Info  Instances  Solution	The identified library appears to be vulnerable.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  /2.2.4/jquery.min.js  The identified library jquery, version 2.2.4 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://github.com/jquery/jquery.com/issues/162 https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/  Upgrade to the latest version of the affected library.
Description URL Method Attack Evidence  Other Info  Instances Solution Reference	The identified library appears to be vulnerable.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  /2.2.4/jquery.min.js  The identified library jquery, version 2.2.4 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://nvl.nist.gov/uln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://github.com/jquery/jquery.com/issues/162 https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/  1  Upgrade to the latest version of the affected library. https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
Description  URL  Method  Attack  Evidence  Other Info  Instances  Solution  Reference  CWE Id	The identified library appears to be vulnerable.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  /2.2.4/jquery.min.js  The identified library jquery, version 2.2.4 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://nvl.nist.gov/uln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://github.com/jquery/jquery.com/issues/162 https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/  1  Upgrade to the latest version of the affected library. https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
Description  URL  Method  Attack  Evidence  Other Info  Instances  Solution  Reference  CWE Id  WASC Id	The identified library appears to be vulnerable.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  /2.2.4/jquery.min.js  The identified library jquery, version 2.2.4 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://github.com/jquery/jquery.com/issues/162 https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/  1 Upgrade to the latest version of the affected library.  https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
Description  URL  Method  Attack  Evidence  Other Info  Instances  Solution  Reference  CWE Id  WASC Id  Plugin Id	The identified library appears to be vulnerable.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  /2.2.4/jquery.min.js  The identified library jquery, version 2.2.4 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://github.com/jquery/jquery.com/issues/162 https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/  1  Upgrade to the latest version of the affected library. https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/1395
Description  URL  Method  Attack  Evidence  Other Info  Instances  Solution  Reference  CWE Id  WASC Id  Plugin Id  Low	The identified library appears to be vulnerable.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  /2.2.4/jquery.min.js  The identified library jquery, version 2.2.4 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p88 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://github.com/jquery/jquery.com/issues/162 https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/  1 Upgrade to the latest version of the affected library. https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/ 1395  10003  Cross-Domain JavaScript Source File Inclusion

Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico</td></tr><tr><td></td><td></td></tr></tbody></table></script></pre>

Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/main.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/main.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/polyfills.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/polyfills.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/runtime.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/runtime.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/styles.css

<b>5.6</b> (1) 1	OFT
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/styles.css</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/vendor.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/vendor.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:43:13
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/fileServer.js:43:13</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td></td><td></td></tr></tbody></table></script></pre>

URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/main.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/main.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/polyfills.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/polyfills.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/runtime.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/runtime.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	

URL	http://localhost:3000/juice-shop/build/routes/styles.css
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/styles.css</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/vendor.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/vendor.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	$\underline{http://localhost:3000/juice-shop/node\_modules/express/lib/router/assets/public/favicon\_js.ico}$
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr></tbody></table></script></pre>

Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/main.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/main.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/polyfills.js
Method	GET
Attack	
Evidence	$<\!$
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/polyfills.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/runtime.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/runtime.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>

Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/styles.css
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/styles.css</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr></tbody></table></script></pre>

Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>

Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/main.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/main.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js
Method	GET
Attack	
	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</pre></td></tr></tbody></table></script></pre>

Cvidonos	/novint
Evidence	/script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/runtime.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/runtime.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/styles.css
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/styles.css</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/vendor.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/vendor.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td></td><td></td></tr></tbody></table></script></pre>

Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node modules/serve-index/assets/public/assets/public/favicon_js.ico</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/favicon_js.ico</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/main.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/main.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/polyfills.js
Method	GET

Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></pre></td></tr><tr><td>Other</td><td>/script></td></tr><tr><td>Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/polyfills.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/runtime.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/runtime.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/styles.css
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/styles.css</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/vendor.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/vendor.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td></td><td></td></tr></tbody></table></script></pre>

Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node modules/serve-index/index.js:145:39
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/index.js:145:39</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/main.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/main.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js
Method	GET

Script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">   Script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">   Script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">   Script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">   Without script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">   Without script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">   Without script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">   Without script src="//cdnjs.cloudflare.com/ajax/libs/spuery/2.2.4/jquery.min.js">   Without script script src="//cdnjs.cloudflare.com/ajax/libs/spuery/2.2.4/jquery.min.js">   Without script	Attack	
Info URL Method GET Attack Evidence Other Info URL Method GET Attack Evidence Other Info URL Method GET Attack  Evidence  Script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"> Other Info URL Mttp://localhost.3000/juice-shop/node_modules/serve-index/styles.css  Method GET Attack Evidence  Script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script> Other Info URL Mttp://localhost.3000/juice-shop/node_modules/serve-index/styles.css  Method GET Attack Evidence  script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"> Other Info URL Mttp://localhost.3000/juice-shop/node_modules/serve-index/serve-index/seript> Other Info URL Mttp://localhost.3000/juice-shop/node_modules/serve-index/vendor.js  Method GET Attack Evidence  script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script> Other Info URL Mttp://localhost.3000/juice-shop/node_modules/serve-index/vendor.js  Method GET Attack Evidence  script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< Other Info URL Mttp://localhost.3000/juice-shop/node_modules/serve-index/vendor.js  Method GET Attack Evidence  script src="//cdnjs.cloudflare.com/ajax/libs/guery/2.2.4/jquery.min.js"> Other Info URL Mttp://localhost.3000/sitemap.xml Method GET Attack Evidence  script src="//cdnjs.cloudflare.com/ajax/libs/guery/2.2.4/jquery.min.js"> Other Info Other Info Other Info Other Info	Evidence	
Method GET  Attack Evidence <script src="//odnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence <script src="//odnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script> Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack Evidence <script src="//odnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence <script src="//odnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script> Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence <script src="//odnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script> Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence <script src="//odnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info  URL http://localhost.3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack Evidence <script src="//odnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info  URL http://localhost.3000/sitemap.xml  Method GET  Attack Evidence <script src="//odnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</script> Other Info  Other Info  Attack Evidence <script src="//odnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</script> Other Info		
Attack Evidence	URL	http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js
Evidence	Method	GET
Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack  Evidence	Attack	
Info URL http://localhost.3000/juice-shop/node_modules/serve-index/styles.css  Method GET Attack  Evidence	Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Method GET Attack  Evidence		
Attack  Evidence  /script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><  Other Info  URL  http://localhost.3000/juice-shop/node_modules/serve-index/styles.css  Method  GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info  URL  http://localhost.3000/juice-shop/node_modules/serve-index/vendor.js  Method  GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><  Other Info  Other Info  URL  http://localhost.3000/juice-shop/node_modules/serve-index/vendor.js  Method  GET  Attack  Evidence  <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><  Other Info  URL  http://localhost.3000/juice-shop/node_modules/serve-index/vendor.js  Method  GET  Attack  Evidence  <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info  URL  http://localhost.3000/sitemap.xml  Method  GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</script> Other Info  Other Info  Other Info  Other Info	URL	http://localhost:3000/juice-shop/node_modules/serve-index/styles.css
Evidence /script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><	Method	GET
Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< //rrccookieconsent.min.js"><</rr> Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info  URL http://localhost:3000/sitemap.xml  Method GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</script> <>  Other Info	Attack	
Info  URL  http://localhost:3000/juice-shop/node_modules/serve-index/styles.css  Method  GET  Attack  Evidence <pre></pre>	Evidence	
Method GET  Attack  Evidence		
Attack Evidence	URL	http://localhost:3000/juice-shop/node_modules/serve-index/styles.css
Evidence	Method	GET
Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><  Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info  URL http://localhost:3000/sitemap.xml  Method GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><  Certain Stript src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><  Certain Stript src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><  Certain Stript src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</a>  Other Info</td><td>Attack</td><td></td></tr><tr><td>Info  URL  http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method  GET  Attack  Evidence  Script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /pre>  Other Info  URL  http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method  GET  Attack  Evidence  Script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">  Other Info  URL  http://localhost:3000/sitemap.xml  Method  GET  Attack  Evidence  Script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /pre>  Other Info  Other Info  Other Info</td><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>		
Method GET  Attack  Evidence		
Attack  Evidence	URL	http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js
Evidence /script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack  Evidence /script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">  Other Info  URL http://localhost:3000/sitemap.xml  Method GET  Attack  Evidence /script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< Other Info  Other Info  Other Info	Method	GET
Other Info  URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info  URL http://localhost:3000/sitemap.xml  Method GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</script> Other Info  Other Info	Attack	
Info  URL  http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js  Method  GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info  URL  http://localhost:3000/sitemap.xml  Method  GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</script> Other Info  Other Info	Evidence	
Method GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info  URL http://localhost:3000/sitemap.xml  Method GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< Other Info  Other Info</td><td></td><td></td></tr><tr><td>Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info  URL http://localhost:3000/sitemap.xml  Method GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< Other Info  Other Info</td><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js</td></tr><tr><td>Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info  URL http://localhost:3000/sitemap.xml  Method GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< Other Info</td><td>Method</td><td>GET</td></tr><tr><td>Other Info  URL http://localhost:3000/sitemap.xml  Method GET  Attack  Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< Other Info</td><td>Attack</td><td></td></tr><tr><td>Info  URL <a href="http://localhost:3000/sitemap.xml">http://localhost:3000/sitemap.xml</a>  Method GET  Attack  Evidence <a href="secont-seco</td><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>		
Method GET  Attack  Evidence		
Attack  Evidence	URL	http://localhost:3000/sitemap.xml
Evidence	Method	GET
Other Info	Attack	
Info	Evidence	
URL <a href="http://localhost:3000/sitemap.xml">http://localhost:3000/sitemap.xml</a>		
	URL	http://localhost:3000/sitemap.xml

Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other	Compt of a mount of the manufacture of the manufact
Info	
Instances	98
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017
Low	Private IP Disclosure
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.
URL	http://localhost:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	192.168.99.100:3000
Other Info	192.168.99.100:3000 192.168.99.100:4200
Instances	1
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP /PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Reference	https://tools.ietf.org/html/rfc1918
CWE Id	497
WASC Id	13
Plugin Id	2
-	
Low	Timestamp Disclosure - Unix
<b>Low</b> Description	Timestamp Disclosure - Unix  A timestamp was disclosed by the application/web server Unix
Low Description URL	Timestamp Disclosure - Unix  A timestamp was disclosed by the application/web server Unix <a href="http://localhost:3000">http://localhost:3000</a>
Low Description URL Method	Timestamp Disclosure - Unix  A timestamp was disclosed by the application/web server Unix
Low Description URL Method Attack	Timestamp Disclosure - Unix  A timestamp was disclosed by the application/web server Unix <a href="http://localhost:3000">http://localhost:3000</a>
Low Description URL Method	Timestamp Disclosure - Unix  A timestamp was disclosed by the application/web server Unix <a href="http://localhost:3000">http://localhost:3000</a> GET
Low  Description  URL  Method  Attack  Evidence  Other	Timestamp Disclosure - Unix  A timestamp was disclosed by the application/web server Unix <a href="http://localhost:3000">http://localhost:3000</a> GET  1650485437
Low  Description  URL  Method  Attack  Evidence  Other Info	Timestamp Disclosure - Unix  A timestamp was disclosed by the application/web server Unix  http://localhost:3000  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.
Low  Description  URL  Method  Attack  Evidence  Other Info  URL	Timestamp Disclosure - Unix  A timestamp was disclosed by the application/web server Unix  http://localhost:3000  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000
Low  Description  URL  Method  Attack  Evidence  Other Info  URL  Method	Timestamp Disclosure - Unix  A timestamp was disclosed by the application/web server Unix  http://localhost:3000  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000
Low  Description  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack	Timestamp Disclosure - Unix  A timestamp was disclosed by the application/web server Unix  http://localhost:3000  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000  GET
Low  Description  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other	Timestamp Disclosure - Unix  A timestamp was disclosed by the application/web server Unix  http://localhost:3000  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000  GET  1981395349

Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico
Method	GET
Attack	

Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/main.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/main.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/main.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1981395349

Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/polyfills.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL <u>I</u>	http://localhost:3000/juice-shop/build/routes/assets/public/runtime.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL <u>I</u>	http://localhost:3000/juice-shop/build/routes/assets/public/runtime.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL <u>I</u>	http://localhost:3000/juice-shop/build/routes/assets/public/runtime.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL <u>I</u>	http://localhost:3000/juice-shop/build/routes/assets/public/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL <u>I</u>	http://localhost:3000/juice-shop/build/routes/assets/public/styles.css
Method	GET
Attack	
Evidence 2	2038834951
Other /	2038834951, which evaluates to: 2034-08-10 11:02:31.

URL	http://localhost:3000/juice-shop/build/routes/assets/public/vendor.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/vendor.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/vendor.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:43:13
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:43:13
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:43:13
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET

Attack	
Evidence	1981395349
Other	
Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/build/routes/main.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/build/routes/main.js
Method	GET
Attack	
Evidence	1981395349
Other	1981395349, which evaluates to: 2032-10-14 15:35:49.
Info	
Info URL	http://localhost:3000/juice-shop/build/routes/main.js
URL	http://localhost:3000/juice-shop/build/routes/main.js
URL Method	http://localhost:3000/juice-shop/build/routes/main.js
URL Method Attack	http://localhost:3000/juice-shop/build/routes/main.js GET
URL Method Attack Evidence Other	http://localhost:3000/juice-shop/build/routes/main.js  GET  2038834951
URL Method Attack Evidence Other Info	http://localhost:3000/juice-shop/build/routes/main.js GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.
URL  Method  Attack  Evidence  Other Info  URL	http://localhost:3000/juice-shop/build/routes/main.js  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/build/routes/polyfills.js
URL  Method  Attack  Evidence  Other Info  URL  Method	http://localhost:3000/juice-shop/build/routes/main.js  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/build/routes/polyfills.js
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack	http://localhost:3000/juice-shop/build/routes/main.js  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/build/routes/polyfills.js  GET
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other	http://localhost:3000/juice-shop/build/routes/main.js  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/build/routes/polyfills.js  GET  1650485437
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info	http://localhost:3000/juice-shop/build/routes/main.js  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/build/routes/polyfills.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  URL  URL  URL  URL  URL  URL  UR	http://localhost:3000/juice-shop/build/routes/main.js  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/build/routes/polyfills.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/build/routes/polyfills.js
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method	http://localhost:3000/juice-shop/build/routes/main.js  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/build/routes/polyfills.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/build/routes/polyfills.js
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Attack	http://localhost:3000/juice-shop/build/routes/main.js  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/build/routes/polyfills.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/build/routes/polyfills.js  GET
URL  Method  Attack  Evidence  Other Info  URL	http://localhost:3000/juice-shop/build/routes/main.js  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/build/routes/polyfills.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/build/routes/polyfills.js  GET  1981395349
URL  Method  Attack  Evidence  Other Info	http://localhost:3000/juice-shop/build/routes/main.js  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/build/routes/polyfills.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/build/routes/polyfills.js  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.
URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  URL  Method  Attack  URL  Method  Attack  URL  Method  Attack  URL  URL  URL  URL  URL	http://localhost:3000/juice-shop/build/routes/main.js  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/build/routes/polyfills.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/build/routes/polyfills.js  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.  http://localhost:3000/juice-shop/build/routes/polyfills.js

Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/build/routes/runtime.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/build/routes/runtime.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/build/routes/runtime.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/build/routes/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/build/routes/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/build/routes/styles.css
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/build/routes/vendor.js
Method	GET
Attack	
Evidence	1650485437
Other	

Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/build/routes/vendor.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/build/routes/vendor.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1981395349
Other	

Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/main.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/main.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/main.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/polyfills.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/runtime.js

Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/runtime.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/runtime.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node modules/express/lib/router/assets/public/styles.css
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node modules/express/lib/router/assets/public/vendor.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node modules/express/lib/router/assets/public/vendor.js
Method	GET

Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	1981395349
Other	
Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
	1981395349, which evaluates to: 2032-10-14 15:35:49. <a href="http://localhost:3000/juice-shop/node">http://localhost:3000/juice-shop/node</a> modules/express/lib/router/index.js:280:10
Info	
Info URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10
Info URL Method	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10
Info URL Method Attack	http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:280:10 GET
Info URL Method Attack Evidence Other	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10  GET  2038834951
Info URL Method Attack Evidence Other Info	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.
Info URL Method Attack Evidence Other Info URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9
Info URL Method Attack Evidence Other Info URL Method	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack	http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:280:10  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:286:9  GET
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9  GET  1650485437
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  URL  URL  Method  Attack  URL  URL  URL  URL  URL  URL  URL  UR	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9  GET
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Other Info  URL  Method  Attack  Evidence  Other Info	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10 GET  2038834951 2038834951, which evaluates to: 2034-08-10 11:02:31. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9 GET  1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9 GET  1981395349
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Other Info  URL  Method  Attack  Evidence  Other Info	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10 GET  2038834951 2038834951, which evaluates to: 2034-08-10 11:02:31. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9 GET  1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9 GET  1981395349 1981395349, which evaluates to: 2032-10-14 15:35:49.
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  URL  URL  URL  URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.  http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9

Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.

URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.is:376:14
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5
Method	GET

Attack	
Evidence	2038834951
Other	2030034931
Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node modules/express/lib/router/main.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/main.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/main.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js
	GET
Method	GET
Method Attack	OL I
	1650485437
Attack	
Attack Evidence Other	1650485437
Attack Evidence Other Info	1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37.
Attack Evidence Other Info URL	1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js
Attack Evidence Other Info URL Method	1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js
Attack Evidence Other Info URL Method Attack	1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js  GET
Attack Evidence Other Info URL Method Attack Evidence Other	1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js  GET  1981395349
Attack Evidence Other Info URL Method Attack Evidence Other Info	1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.
Attack Evidence Other Info URL Method Attack Evidence Other Info URL	1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node modules/express/lib/router/polyfills.js  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.  http://localhost:3000/juice-shop/node modules/express/lib/router/polyfills.js
Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method	1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node modules/express/lib/router/polyfills.js  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.  http://localhost:3000/juice-shop/node modules/express/lib/router/polyfills.js
Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack	1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.  http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js  GET
Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other	1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.  http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js  GET  2038834951
Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info	1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js  GET  1981395349 1981395349, which evaluates to: 2032-10-14 15:35:49.  http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js  GET  2038834951 2038834951, which evaluates to: 2034-08-10 11:02:31.
Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence URL Method Attack Evidence Other Info URL	1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.  http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/node_modules/express/lib/router/runtime.js

Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/runtime.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/runtime.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/styles.css
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/vendor.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/vendor.js
Method	GET
Attack	
Evidence	1981395349
Other	

Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/vendor.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node modules/serve-index/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node modules/serve-index/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1981395349
	4004007040 111 1 4 4 00004044470740
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/favicon_js.ico
Info	
Info URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/favicon_js.ico
Info URL Method	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/favicon_js.ico

Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/main.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/main.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/main.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/polyfills.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/runtime.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/runtime.js

NA-4bI	OFT
Method	GET
Attack	4004007040
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/runtime.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/styles.css
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/vendor.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/vendor.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/vendor.js
Method	GET

Attack	
Evidence	2038834951
Other	
Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/index.js:145:39
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/index.js:145:39
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/index.js:145:39
Method	GET
Attack	
Evidence	2038834951
Other	2038834951, which evaluates to: 2034-08-10 11:02:31.
Info	2030034931, William evaluates to: 2034-00-10 11.02.31.
	http://localhost:3000/juice-shop/node_modules/serve-index/main.js
Info	
Info URL Method Attack	http://localhost:3000/juice-shop/node_modules/serve-index/main.js GET
Info URL Method Attack Evidence	http://localhost:3000/juice-shop/node_modules/serve-index/main.js
Info URL Method Attack	http://localhost:3000/juice-shop/node_modules/serve-index/main.js GET
Info URL Method Attack Evidence Other	http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1650485437
Info URL Method Attack Evidence Other Info	http://localhost:3000/juice-shop/node_modules/serve-index/main.js GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.
Info URL  Method  Attack  Evidence  Other Info  URL	http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js
Info URL Method Attack Evidence Other Info URL Method	http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js
Info URL Method Attack Evidence Other Info URL Method Attack	http://localhost:3000/juice-shop/node modules/serve-index/main.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node modules/serve-index/main.js  GET
Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other	http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1981395349
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info	http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.
Info URL  Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL	http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js
Info URL  Method Attack Evidence Other Info URL  Method Attack Evidence Other Info URL  Method Attack URL  Method  Method  Method  Method  Method  Method  Method  URL	http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack	http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other	http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  2038834951
Info URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info	http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.
Info URL  Method Attack Evidence Other Info URL  Method Attack Evidence Other Info URL  Method Attack Evidence Other Info URL  Method Attack URL  URL	http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1650485437  1650485437, which evaluates to: 2022-04-20 16:10:37.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  1981395349  1981395349, which evaluates to: 2032-10-14 15:35:49.  http://localhost:3000/juice-shop/node_modules/serve-index/main.js  GET  2038834951  2038834951, which evaluates to: 2034-08-10 11:02:31.  http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js

Other	46E049E497, which evaluates to 2009 04 00 4040-97
Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.

URL	http://localhost:3000/juice-shop/node_modules/serve-index/styles.css
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/main.js
Method	GET
Attack	
Evidence	1734944650
Other Info	1734944650, which evaluates to: 2024-12-23 04:04:10.
URL	http://localhost:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1969196030
Other Info	1969196030, which evaluates to: 2032-05-26 10:53:50.
URL	http://localhost:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1970691216
Other Info	1970691216, which evaluates to: 2032-06-12 18:13:36.
URL	http://localhost:3000/rest/products/search?q=
Method	GET

Attack	
Evidence	1969196030
Other Info	1969196030, which evaluates to: 2032-05-26 10:53:50.
URL	http://localhost:3000/rest/products/search?q=
Method	GET
Attack	
Evidence	1970691216
Other Info	1970691216, which evaluates to: 2032-06-12 18:13:36.
URL	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1680327869
Other Info	1680327869, which evaluates to: 2023-04-01 01:44:29.
URL	http://localhost:3000/styles.css
Method	GET
Attack	

Evidence	1701244813
Other	
Info	1701244813, which evaluates to: 2023-11-29 03:00:13.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	18181818
Other Info	18181818, which evaluates to: 2027-08-13 14:30:18.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1839622642
Other Info	1839622642, which evaluates to: 2028-04-17 18:17:22.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1863874346
Other Info	1863874346, which evaluates to: 2029-01-23 09:52:26.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1917098446
Other Info	1917098446, which evaluates to: 2030-10-01 11:20:46.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	2033195021
Other Info	2033195021, which evaluates to: 2034-06-06 04:23:41.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	2038834951
Other	

Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
Instances	162
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096
Low	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr1zx
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr2jI&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr3GH&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr424&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

LIDI	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr43V&sid=Rw-fonf5fS-
URL	<u>soOyqAAAC</u>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr452&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr47B&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr48L&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr4AU&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr4Bk&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr4DU&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr7jA
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8cA&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9Qp&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr2iZ&sid=Rw-fonf5fS-soOyqAAAC
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8bl&sid=bbnwfd9qOchbbDn-AAAE
Method	POST

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	17
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	<u>693</u>
WASC Id	15
WACC IU	15
Plugin Id	10021
Plugin Id	10021
Plugin Id  Informational	10021 Information Disclosure - Suspicious Comments
Plugin Id  Informational  Description	Information Disclosure - Suspicious Comments  The response appears to contain suspicious comments which may help an attacker.
Plugin Id  Informational  Description  URL	Information Disclosure - Suspicious Comments  The response appears to contain suspicious comments which may help an attacker.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Plugin Id  Informational  Description  URL  Method	Information Disclosure - Suspicious Comments  The response appears to contain suspicious comments which may help an attacker.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Plugin Id  Informational  Description  URL  Method  Attack	Information Disclosure - Suspicious Comments  The response appears to contain suspicious comments which may help an attacker.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET
Plugin Id  Informational  Description  URL  Method  Attack  Evidence  Other	Information Disclosure - Suspicious Comments  The response appears to contain suspicious comments which may help an attacker.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  Db  The following pattern was used: \bDB\b and was detected in likely comment: "//,sb={},tb={}, ub="*/".concat("*"),vb=d.createElement("a");vb.href=jb.href;function wb(a){return function(b,
Plugin Id  Informational  Description  URL  Method  Attack  Evidence  Other Info	Information Disclosure - Suspicious Comments  The response appears to contain suspicious comments which may help an attacker.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  Db  The following pattern was used: \bDB\b and was detected in likely comment: "//,sb={},tb={}, ub="*/".concat("*"),vb=d.createElement("a");vb.href=jb.href;function wb(a){return function(b, c){"string"!=typeof", see evidence field for the suspicious comment/snippet.
Plugin Id  Informational  Description  URL  Method  Attack  Evidence  Other Info  URL	Information Disclosure - Suspicious Comments  The response appears to contain suspicious comments which may help an attacker.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  Db  The following pattern was used: \bDB\b and was detected in likely comment: "//,sb={},tb={}, ub="*/".concat("*"),vb=d.createElement("a");vb.href=jb.href;function wb(a){return function(b, c){"string"!=typeof", see evidence field for the suspicious comment/snippet.  http://localhost:3000/main.js
Plugin Id  Informational  Description  URL  Method  Attack  Evidence  Other Info  URL  Method	Information Disclosure - Suspicious Comments  The response appears to contain suspicious comments which may help an attacker.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  Db  The following pattern was used: \bDB\b and was detected in likely comment: "//,sb={},tb={}, ub="*/".concat("*"),vb=d.createElement("a");vb.href=jb.href;function wb(a){return function(b, c){"string"!=typeof", see evidence field for the suspicious comment/snippet.  http://localhost:3000/main.js
Plugin Id  Informational  Description  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack	Information Disclosure - Suspicious Comments  The response appears to contain suspicious comments which may help an attacker.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  Db  The following pattern was used: \bDB\b and was detected in likely comment: "//,sb={},tb={}, ub="*/".concat("*"),vb=d.createElement("a");vb.href=jb.href;function wb(a){return function(b, c){"string"!=typeof", see evidence field for the suspicious comment/snippet.  http://localhost:3000/main.js  GET
Plugin Id  Informational  Description  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Other  Info  URL  Method  Attack  Evidence  Other	Information Disclosure - Suspicious Comments  The response appears to contain suspicious comments which may help an attacker.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  Db  The following pattern was used: \bDB\b and was detected in likely comment: "//,sb={},tb={}, ub="*/".concat("*"),vb=d.createElement("a");vb.href=jb.href;function wb(a){return function(b, c){"string"!=typeof ", see evidence field for the suspicious comment/snippet.  http://localhost:3000/main.js  GET  query  The following pattern was used: \bQUERY\b and was detected in likely comment: "//owasp. org' target='_blank'>Open Worldwide Application Security Project (OWASP)/a> and is developed and maintained by voluntee", see evidence field for the suspicious comment
Plugin Id  Informational  Description  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info	Information Disclosure - Suspicious Comments  The response appears to contain suspicious comments which may help an attacker.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  Db  The following pattern was used: \bDB\b and was detected in likely comment: "//,sb={},tb={}, ub="*/".concat("*"),vb=d.createElement("a");vb.href=jb.href;function wb(a){return function(b, c){"string"!=typeof", see evidence field for the suspicious comment/snippet.  http://localhost:3000/main.js  GET  query  The following pattern was used: \bQUERY\b and was detected in likely comment: "//owasp. org' target='_blank'>Open Worldwide Application Security Project (OWASP)/a> and is developed and maintained by voluntee", see evidence field for the suspicious comment /snippet.
Plugin Id  Informational  Description  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  Evidence  Other Info  URL  Method  Attack  URL  Method  Attack  URL  URL  URL  URL  URL  URL  URL  UR	Information Disclosure - Suspicious Comments  The response appears to contain suspicious comments which may help an attacker.  http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js  GET  Db  The following pattern was used: \bDB\b and was detected in likely comment: "//,sb={},tb={}, ub="*/".concat("*"),vb=d.createElement("a");vb.href=jb.href;function wb(a){return function(b, c){"string"!=typeof ", see evidence field for the suspicious comment/snippet.  http://localhost:3000/main.js  GET  query  The following pattern was used: \bQUERY\b and was detected in likely comment: "//owasp. org' target='_blank'>Open Worldwide Application Security Project (OWASP)/a> and is developed and maintained by voluntee", see evidence field for the suspicious comment /snippet.  http://localhost:3000/vendor.js

Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//www. w3.org/2000/svg" viewBox="0 0 512 512"> <path ,="" comment="" d="M0 256C0 397.4 114.6 512 256 512s256-114.6 256-256S397.4 0 256 0S0 114.6 0" evidence="" field="" for="" see="" snippet.<="" suspicious="" th="" the=""></path>
Instances	3
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	<u>615</u>
WASC Id	13
Plugin Id	10027

Informational	Modern Web Application
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	http://localhost:3000
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/ftp/</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><a href="">ftp</a></td></tr><tr><td>Other Info</td><td>Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr></tbody></table></script></pre>

Other Info	No links have been found while there are scripts, which is an indication that this is a moder web application.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/main.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a moder web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/polyfills.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a model web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/runtime.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a model web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/styles.css</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a model web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/vendor.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a mode web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/fileServer.js:43:13</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a mode web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/fileServer.js:59:18</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr></tbody></table></script></pre>

Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/main.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/polyfills.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/runtime.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/styles.css</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/vendor.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td></td><td></td></tr></tbody></table></script></pre>

URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/main.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node modules/express/lib/router/assets/public/polyfills.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/runtime.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/styles.css</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td></td><td></td></tr></tbody></table></script></pre>

Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/main.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td></td><td></td></tr></tbody></table></script></pre>

Attack	
Allack	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</pre></td></tr><tr><td>Evidence</td><td>/script></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/runtime.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/styles.css</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/vendor.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node modules/serve-index/assets/public/assets/public/favicon_js.ico</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/favicon_js.ico</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td></td><td></td></tr></tbody></table></script></pre>

URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/main.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/polyfills.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/runtime.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/styles.css</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/vendor.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/index.js:145:39</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/main.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td></td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</pre></td></tr><tr><td></td><td><Script Src= //curijs.cloudilare.com/ajax/iibs/cookieconsentz/s.1.0/cookieconsent.miir.js ></td></tr></tbody></table></script></pre>

Evidence	/script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/styles.css</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/sitemap.xml</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>Instances</td><td>50</td></tr><tr><td>Solution</td><td>This is an informational alert and so no changes are required.</td></tr><tr><td>Reference</td><td></td></tr><tr><td>CWE Id</td><td></td></tr><tr><td>WASC Id</td><td></td></tr><tr><td>Plugin Id</td><td>10109</td></tr><tr><td>Informational</td><td>Retrieved from Cache</td></tr></tbody></table></script></pre>

Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Method	GET
Attack	
Evidence	Age: 237933
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Method	GET
Attack	
Evidence	Age: 25591
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	Age: 442510
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	3
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:  Cache-Control: no-cache, no-store, must-revalidate, private  Pragma: no-cache  Expires: 0  This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	
WASC Id	
Plugin Id	10050
Informational	User Agent Fuzzer
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	http://localhost:3000/assets

Method

**GET** 

Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
	http://localhost:3000/assets
Info	http://localhost:3000/assets GET

Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

Evidence	
Other	
Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
A 1	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML,
Attack	like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4

Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/assets/i18n
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/assets/public
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	

Other Info  URL http://localhost.3000/assets/public  Method GET  Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36  Evidence Other Info  URL http://localhost.3000/assets/public  Method GET  Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv-93.0) Gecko/20100101 Firefox/91.0  Evidence Other Info  URL http://localhost.3000/assets/public  Method GET  Attack Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)  Evidence Other Info  URL http://localhost.3000/assets/public  Evidence Other Info  URL http://localhost.3000/assets/public  Method GET  Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info  URL http://localhost.3000/assets/public  Evidence Other Info  URL http://localhost.3000/assets/public  URL http://localhost.3000/assets/public  URL http://localhost.3000/assets/public  URL http://localhost.3000/assets/public  URL http://localhost.3000/assets/public  Wethod GET  Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8.0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info  URL http://localhost.3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gacko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost.3000/assets/public  Method GET  Attack Method GET		
Method GET Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36  Evidence Other Info URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv-93.0) Gecko/20100101 Firefox/91.0  Evidence Other Info URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)  Evidence Other Info URL http://localhost:3000/assets/public Wethod GET Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info URL http://localhost:3000/assets/public Wethod GET Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  URL http://localhost:3000/assets/public  Wethod GET Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8.0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info URL http://localhost:3000/assets/public  Method GET Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3.0 like Mac OS X; en-us) AppleWebKit/528.18  (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info URL http://localhost:3000/assets/public  Method GET Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3.0 like Mac OS X; en-us) AppleWebKit/528.18  (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info URL http://localhost:3000/assets/public  Method GET Attack Method GET		
Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36  Evidence Other Info  URL http://localhost.3000/assets/public  Method GET  Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64; n:93.0) Gecko/20100101 Firefox/91.0  Evidence Other Info  URL http://localhost.3000/assets/public  Method GET  Attack Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)  Evidence Other Info  URL http://localhost.3000/assets/public  Method GET  Attack Mozilla/5.0 (compatible; Yahool Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info  URL http://localhost.3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8, 0, 2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info  URL http://localhost.3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3, 0 like Mac OS X; en-us) AppleWebKit/528.18  (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost.3000/assets/public  Method GET  Attack Method GET	URL	http://localhost:3000/assets/public
Evidence Other Info URL http://localhost:3000/assets/public Evidence Other Info URL http://localhost:3000/assets/public Evidence Other Info URL http://localhost:3000/assets/public  Evidence Other Info URL http://localhost:3000/assets/public  Method GET Attack Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)  Evidence Other Info URL http://localhost:3000/assets/public  Evidence Other Info URL http://localhost:3000/assets/public  Method GET Attack Mozilla/5.0 (compatible; Yahool Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info URL http://localhost:3000/assets/public  Evidence Other Info URL http://localhost:3000/assets/public  Evidence Other Info URL http://localhost:3000/assets/public  Method GET Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info URL http://localhost:3000/assets/public  Method GET Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18  Evidence Other Info URL http://localhost:3000/assets/public  Method GET Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18  Evidence Other Info URL http://localhost:3000/assets/public  Method GET Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18  Evidence Other Info URL http://localhost:3000/assets/public  Method GET Method GET Method GET Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18  Evidence Other Info URL http://localhost:3000/assets/public  Method GET Method GET Method GET	Method	GET
Other Info  URL http://localhost-3000/assets/public  Method GET  Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0  Evidence Other Info  URL http://localhost-3000/assets/public  Method GET  Attack Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)  Evidence Other Info  URL http://localhost-3000/assets/public  Method GET  Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info  URL http://localhost-3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info  URL http://localhost-3000/assets/public  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18  K(HTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost-3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18  KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost-3000/assets/public  Method GET  Method GET  Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)	Attack	
Info URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0 Evidence Other Info URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) Evidence Other Info URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (compatible; Yahool Slurp; http://help.yahoo.com/help/us/ysearch/slurp) Evidence Other Info URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4 Evidence Other Info URL http://localhost:3000/assets/public GET Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info URL http://localhost:3000/assets/public	Evidence	
Method GET Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0  Evidence Other Info  URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)  Evidence Other Info  URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)		
Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64; nv:93.0) Gecko/20100101 Firefox/91.0  Evidence Other Info URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)  Evidence Other Info URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info URL http://localhost:3000/assets/public  Evidence Other Info URL http://localhost:3000/assets/public  Method GET Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info URL http://localhost:3000/assets/public  Evidence Other Info URL http://localhost:3000/assets/public Method GET Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)	URL	http://localhost:3000/assets/public
Evidence Other Info  URL http://localhost:3000/assets/public  Method GET Attack Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)  Evidence Other Info  URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info  URL http://localhost:3000/assets/public  Wethod GET Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info  URL http://localhost:3000/assets/public  Wethod GET Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18  KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)	Method	GET
Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18  (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public  Evidence Other Info  URL http://localhost:3000/assets/public  Evidence Other Info  Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18  KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16	Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)  Evidence Other Info  URL http://localhost:3000/assets/public Method GET  Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public Method GET	Evidence	
Method GET Attack Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)  Evidence Other Info  URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info  URL http://localhost:3000/assets/public Method GET  Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public Method GET  Method GET  Method GET  Method GET  Method GET  Matack msnbot/1.1 (+http://search.msn.com/msnbot.htm)		
Attack Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)  Evidence Other Info URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18  (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info URL http://localhost:3000/assets/public	URL	http://localhost:3000/assets/public
Evidence Other Info  URL http://localhost:3000/assets/public  Method GET Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info  URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info  URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET	Method	GET
Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info  URL http://localhost:3000/assets/public Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET	Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info  URL http://localhost:3000/assets/public Method GET  Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info  URL http://localhost:3000/assets/public Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)	Evidence	
Method GET  Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info  URL http://localhost:3000/assets/public Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Method Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16		
Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)  Evidence Other Info  URL http://localhost:3000/assets/public Method GET  Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info  URL http://localhost:3000/assets/public Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public Method GET  Method Method GET	URL	http://localhost:3000/assets/public
Evidence Other Info  URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info  URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)	Method	GET
Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence  Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence  Other Info  URL http://localhost:3000/assets/public  Method GET  Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)	Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Info URL http://localhost:3000/assets/public  Method GET Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info URL http://localhost:3000/assets/public Method GET Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info URL http://localhost:3000/assets/public  Method GET Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)	Evidence	
Method GET  Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)		
Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4  Evidence Other Info   URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info   URL http://localhost:3000/assets/public  Method GET  Attack Method GET  Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)	URL	http://localhost:3000/assets/public
Evidence Other Info  URL http://localhost:3000/assets/public Method GET Attack (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  URL http://localhost:3000/assets/public  Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public Method GET Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)	Method	GET
Other Info  URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)	Attack	
URL http://localhost:3000/assets/public  Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)	Evidence	
Method GET  Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public  Method GET  Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)		
Attack  Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence  Other Info  URL  http://localhost:3000/assets/public  Method  GET  Attack  msnbot/1.1 (+http://search.msn.com/msnbot.htm)	URL	http://localhost:3000/assets/public
Attack (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16  Evidence Other Info  URL http://localhost:3000/assets/public Method GET Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)	Method	
Other Info  URL http://localhost:3000/assets/public  Method GET  Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)	Attack	
URL <a href="http://localhost:3000/assets/public">http://localhost:3000/assets/public</a> Method GET  Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)	Evidence	
Method GET  Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)		
Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)	URL	http://localhost:3000/assets/public
	Method	GET
Evidence	Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
	Evidence	

Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	

Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	

URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	

LIDI	http://localhoot/2000/socoto/p.uhlin/imparco/products
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/products
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr7jA
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr7jA
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr7jA
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr7jA
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr7jA

Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr7jA
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr7jA
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr7jA
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr7jA
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr7jA
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr7jA
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	

URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr7jA
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9Qp&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9Qp&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9Qp&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9Qp&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9Qp&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9Qp&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9Qp&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9Qp&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9Qp&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9Qp&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9Qp&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9Qp&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=bbnwfd9qOchbbDn-AAAE

Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	$\underline{http://localhost:3000/socket.io/?EIO=4\&transport=websocket\&sid=bbnwfd9qOchbbDn-AAAE}$
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost: 3000/socket.io/? EIO=4&transport=websocket&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost: 3000/socket.io/? EIO=4&transport=websocket&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=bbnwfd9qOchbbDn-AAAE

Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	$\underline{http://localhost:3000/socket.io/?EIO=4\&transport=websocket\&sid=bbnwfd9qOchbbDn-AAAE}$
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	$\underline{http://localhost:3000/socket.io/?EIO=4\&transport=websocket\&sid=bbnwfd9qOchbbDn-AAAE}$
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	$\underline{http://localhost:3000/socket.io/?EIO=4\&transport=websocket\&sid=bbnwfd9qOchbbDn-AAAE}$
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PUHr8bl&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8bl&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8bl&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8bl&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8bl&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8bl&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8bl&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)

Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9gOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	WOZINA/3.0 (WINDOWS WT 10.0, THURSTIP 1.0, TV. 11.0) IING GEORG
Other	
Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4

Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	120
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	<u>10104</u>