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

Generated on Sun, 3 Aug 2025 05:32:16

ZAP Version: 2.16.1

ZAP by **Checkmarx**

Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	5
Low	4
Informational	3

Alerts

Name	Risk Level	Number of Instances
Open Redirect	High	1
SQL Injection - SQLite	High	1
Content Security Policy (CSP) Header Not Set	Medium	102
Cross-Domain Misconfiguration	Medium	167
Missing Anti-clickjacking Header	Medium	42
Session ID in URL Rewrite	Medium	188
Vulnerable JS Library	Medium	1
Cross-Domain JavaScript Source File Inclusion	Low	102
Private IP Disclosure	Low	1
<u>Timestamp Disclosure - Unix</u>	Low	168
X-Content-Type-Options Header Missing	Low	188
Information Disclosure - Suspicious Comments	Informational	4
Modern Web Application	Informational	52
Retrieved from Cache	Informational	6

Alert Detail

High	Open Redirect
	Open redirects are one of the OWASP 2010 Top Ten vulnerabilities. This check looks at user-supplied input in query string parameters and POST data to identify where open

Description	redirects might be possible. Open redirects occur when an application allows user-supplied input (e.g. https://nottrusted.com) to control an offsite redirect. This is generally a pretty accurate way to find where 301 or 302 redirects could be exploited by spammers or phishing attacks. For example an attacker could supply a user with the following link: https://example.com/example.php?url=https://malicious.example.com.
URL	http://localhost:3000/redirect?to=https://github.com/juice-shop/juice-shop
Method	GET
Attack	
Evidence	
Other Info	The 301 or 302 response to a request for the following URL appeared to contain user input in the location header: http://localhost:3000/redirect?to=https://github.com/juice-shop/juice-shop/juice-shop The user input found was: to=https://github.com/juice-shop/juice
Instances	1
Solution	To avoid the open redirect vulnerability, parameters of the application script/program must be validated before sending 302 HTTP code (redirect) to the client browser. Implement safe redirect functionality that only redirects to relative URI's, or a list of trusted domains
Reference	https://cheatsheetseries.owasp.org/cheatsheets /Unvalidated Redirects and Forwards Cheat Sheet.html https://cwe.mitre.org/data/definitions/601.html
CWE Id	<u>601</u>
WASC Id	38
Plugin Id	10028

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.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL Injection Prevention Cheat Sheet. 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/assets/public/images/uploads/%E1%93%9A%E1%98%8F%E1%97%A2-
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/favicon.ico
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	
IIIIO	
URL	http://localhost:3000/ftp/encrypt.pyc
	http://localhost:3000/ftp/encrypt.pyc 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/ftp/package-lock.json.bak
URL Method Attack Evidence Other Info URL Method	GET http://localhost:3000/ftp/package-lock.json.bak
URL Method Attack Evidence Other Info URL Method Attack	GET http://localhost:3000/ftp/package-lock.json.bak
URL Method Attack Evidence Other Info URL Method Attack Evidence Other	GET http://localhost:3000/ftp/package-lock.json.bak
URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info	http://localhost:3000/ftp/package-lock.json.bak 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/ftp/package-lock.json.bak GET http://localhost:3000/ftp/package.json.bak
URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Method Attack Evidence Other Info URL Method	http://localhost:3000/ftp/package-lock.json.bak GET http://localhost:3000/ftp/package.json.bak
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/ftp/package-lock.json.bak GET http://localhost:3000/ftp/package.json.bak
URL Method Attack Evidence Other Info URL	http://localhost:3000/ftp/package-lock.json.bak GET http://localhost:3000/ftp/package.json.bak
URL Method Attack Evidence Other Info	http://localhost:3000/ftp/package-lock.json.bak GET http://localhost:3000/ftp/package.json.bak GET
URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence URL Method Attack URL Method Attack URL Method Attack URL Method Attack URL URL URL URL URL	http://localhost:3000/ftp/package-lock.json.bak GET http://localhost:3000/ftp/package.json.bak GET http://localhost:3000/ftp/package.json.bak GET

Info URL http://localhost:3000/ftp/suspicious_errors.yml Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/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/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/styles.css Method GET	Other	
Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico Wethod GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/polyfills.js Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/tuntime.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/styles.css Method GET Attack Evidence Other Info Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/styles.css Method GET	Info	
Attack Evidence Other Info URL http://localhost.3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost.3000/juice-shop/build/routes/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost.3000/juice-shop/build/routes/assets/public/favicon_js.ico Other Info URL http://localhost.3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/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/styles.css Method GET Attack Evidence Other Info URL http://localhost.3000/juice-shop/build/routes/assets/public/styles.css Method GET Attack Evidence Other Other		
Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/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/styles.css Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/styles.css Method GET Attack Evidence Other Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/styles.css Method GET Attack Evidence Other Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/styles.css		GET
Other Info URL http://localhost.3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost.3000/juice-shop/build/routes/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost.3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/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/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/styles.css 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/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/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/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/styles.css Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/styles.css Method GET Attack Evidence Other		
Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/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/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 Other Info		
Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/styles.css Method GET Attack Evidence Other	URL	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico
Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/favicon_is.ico Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/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/styles.css Method GET Attack Evidence Other Info	Method	GET
Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/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/styles.css Method GET Attack Evidence Other Info	Attack	
Info URL http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/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/styles.css Method GET Attack Evidence Other	Evidence	
Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/routime.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 Attack Evidence Other Other		
Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/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 Attack Evidence Other	URL	http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico
Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/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/styles.css Method GET Attack Evidence Other	Method	GET
Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/routime.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/styles.css Method GET Attack Evidence Other	Attack	
Info URL http://localhost:3000/juice-shop/build/routes/assets/public/main.js Method GET Attack Evidence 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/rout/fills.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/styles.css Method GET Attack Evidence Other	Evidence	
Method GET Attack Evidence 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/styles.css Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/styles.css Method GET Attack Evidence Other		
Attack Evidence 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/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	URL	http://localhost:3000/juice-shop/build/routes/assets/public/main.js
Evidence 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/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	Method	GET
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/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	Attack	
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/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	Evidence	
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 Attack Evidence Other		
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 GET Attack Evidence Other	URL	http://localhost:3000/juice-shop/build/routes/assets/public/polyfills.js
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 Other	Method	GET
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 Other	Attack	
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 Other	Evidence	
Method GET Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/styles.css Method GET Attack Evidence Other		
Attack Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/styles.css Method GET Attack Evidence Other	URL	http://localhost:3000/juice-shop/build/routes/assets/public/runtime.js
Evidence Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/styles.css Method GET Attack Evidence Other	Method	GET
Other Info URL http://localhost:3000/juice-shop/build/routes/assets/public/styles.css Method GET Attack Evidence Other	Attack	
Info URL http://localhost:3000/juice-shop/build/routes/assets/public/styles.css Method GET Attack Evidence Other	Evidence	
Method GET Attack Evidence Other		
Attack Evidence Other	URL	http://localhost:3000/juice-shop/build/routes/assets/public/styles.css
Evidence Other	Method	GET
Other	Attack	
	Evidence	

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	
	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/assets/public
URL	/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	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/vendor.js
Method	GET
Attack	
Evidence	
Other 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

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/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost.3000/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost.3000/socket.io/? EIO-s&transport=polling&t=PXINgoe&sid=2f5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost.3000/socket.io/? EIO-s&transport=polling&t=PXINgoe&sid=2f5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost.3000/socket.io/? EIO-s&transport=polling&t=PXINgoe&sid=2f5bMp82Z9dUQqfVAAAC DOTHER Info URL http://localhost.3000/socket.io/? EIO-s&transport=polling&t=PXINgoe&sid=7K5VpH6acNpSwKXeAAAG Method POST Method POST	Attack	
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/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost:3000/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO—48transport=polling&t=PXINgoe&sid=2l5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=48transport=polling&t=PXINjrf&sid=-miNhTFpgRS7F4AAAE Evidence Other Info URL http://localhost:3000/socket.io/?EIO=48transport=polling&t=PXINjrf&sid=-miNhTFpgRS7F4AAAE Evidence Other Info		
Info URL Method GET Attack Evidence Other Info URL Method POST Attack Evidence Other Info URL Method POST Attack Evidence Other Info URL Attack Evidence Other Info URL Attac		
Method GET Attack Evidence Other Info Info URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css Method GET Attack Evidence Other Info http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js Method GET Attack Evidence Other Info http://localhost:3000/sitemap.xml Wethod GET Attack Evidence Other Info http://localhost:3000/socket.io/? URL http://localhost:3000/socket.io/? ElO=4&transport=polling&t=PXINgoe&sid=2!5bMp82Z9dUQqfVAAAC POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrt&sid=-miNhTFEpgRS7FH4AAAE Method POST Attack Evidence Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjvax&sid=7K5VpH6acNpSwKXeAAAG		
Attack	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 URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js Method GET Attack Evidence Other Info URL http://localhost:3000/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost:3000/socket.io/? ElO=4&transport=polling&t=PXINgoe&sid=2l5bMp82Z9dUOqtVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?ElO=4&transport=polling&t=PXINjrf&sid=-mlVnTFFp8RS7FI4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?ElO=4&transport=polling&t=PXINjrf&sid=-mlVnTFFp8RS7FI4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?ElO=4&transport=polling&t=PXINjrf&sid=-mlVnTFFp8RS7FI4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?ElO=4&transport=polling&t=PXINjrf&sid=-mlVnTFFp8RS7FI4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?ElO=4&transport=polling&t=PXINjrf&sid=-mlVnTFFp8RS7FI4AAAE Method POST Attack Evidence Other Info	Method	GET
Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/styles.css Method Attack Evidence Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js Method Attack Evidence Other Info URL http://localhost:3000/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost:3000/socket.io/? ElO=4&transport=polling&t=PXINjqoe&sid=215bMp82Z9dUQqtVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?ElO=4&transport=polling&t=PXINjrf&sid=mIVnTFFp9RS7F14AAAE Method POST	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 URL http://localhost:3000/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=2I5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=2I5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=-mVhTFFp9RS7F4AAAE Method POST Attack Evidence Other Info Attack Evidence Other Info DITL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=-mVhTFFp9RS7F4AAAE Method POST Attack Evidence Other Info LIRL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=-mVhTFFp9RS7F4AAAE Method POST Attack Evidence Other Info LIRL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINma&sid=7K5VpH6acNpSwKXeAAAG	Evidence	
Method GET Attack Evidence Other Info Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js Method GET Attack Evidence Other Info Other Attack Evidence Other Info Other Info URL http://localhost:3000/socket.io/? ElO=4&transport=polling&t=PXINgoe&sid=2l5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=-mIVhTEFp9RS7Fl4AAAE Method POST Attack Evidence Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=-mIVhTEFp9RS7Fl4AAAE Wethod POST Attack Evidence Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG		
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/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost:3000/socket.io/? ElO=4&transport=polling&t=PXINgoe&sid=2l5bMp82Z9dUOqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?ElO=4&transport=polling&t=PXINjrf&sid=-mt/hTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?ElO=4&transport=polling&t=PXINjrf&sid=-mt/hTFFp9RS7Ff4AAAE Method POST 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 URL http://localhost:3000/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost:3000/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=2l5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlvhTFFp9RS7FI4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlvhTFFp9RS7FI4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlvhTFFp9RS7FI4AAAE Method POST Attack Evidence Other Info Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlvhTFFp9RS7FI4AAAE Method POST Attack Evidence Other Info Info	Method	GET
Other Info URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js Method GET Attack Evidence Other Info URL http://localhost:3000/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=2!5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlVnTFFp9RS7Ft4AAAE	Attack	
Info URL http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js Method GET Attack Evidence Other Info URL http://localhost:3000/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=215bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=215bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=-miVhTFEp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=-miVhTFEp9RS7Ff4AAAE Wethod POST Attack Evidence Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=-miVhTFEp9RS7Ff4AAAE Hethod POST Attack Evidence Other Info http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG	Evidence	
Method GET Attack Evidence Other Info URL http://localhost:3000/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=2I5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?FIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS/FI4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?FIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS/FI4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PXINpra&sid=7K5VpH6acNpSwKXeAAAG		
Attack Evidence Other Info URL http://localhost:3000/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=2I5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?FIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS/FI4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?FIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS/FI4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PXINjrf&sid=-TK5VpH6acNpSwKXeAAAG	URL	http://localhost:3000/juice-shop/node modules/serve-index/vendor.js
Evidence Other Info URL http://localhost:3000/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=2I5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=miVhTFEp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=miVhTFEp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=miVhTEp9RS7Ff4AAAE Wethod POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINpra&sid=7KSVpH6acNpSwKXeAAAG	Method	GET
Other Info URL http://localhost:3000/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=2l5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? FIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS7F14AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?FIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS7F14AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS7F14AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS7F14AAAE	Attack	
Info URL http://localhost:3000/sitemap.xml Method GET Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=2I5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlvhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlvhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlvhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG	Evidence	
Method GET Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=2I5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG		
Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=2I5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG	URL	http://localhost:3000/sitemap.xml
Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=2l5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=-mlVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=-mlVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG	Method	GET
Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=2I5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG	Attack	
Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=2I5bMp82Z9dUQqfVAAAC Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mIVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mIVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINtrwa&sid=7K5VpH6acNpSwKXeAAAG	Evidence	
Method POST Attack Evidence Other Info URL Method POST http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG		
Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINjrf&sid=mlVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info	URL	
Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=mIVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINjrf&sid=mIVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info	Method	POST
Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=-mIVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG	Attack	
Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=-mlVhTFFp9RS7Ff4AAAE Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG	Evidence	
Method POST Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG		
Attack Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG	URL	
Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG	Method	POST
Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG	Attack	
URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG	Evidence	
EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG		
Method POST	URL	
	Mathaal	POST

Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINsZs&sid=Zi_Slhms1STDM57iAAAH
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINwFT&sid=fX51XeedI4pt4YQJAAAK
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINy3a&sid=Kwa8OeOh2pxuMSaVAAAM
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIO-IB&sid=UeL35-cfUjXzywO9AAAw
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIO2D2&sid=bdeyXpKNMNcBpQAbAAAO
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIO5At&sid=kA4CWjF19xGageFyAAAQ
Method	POST
Attack	
Evidence	
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXIObAs&sid=r0Gyydx5_nXCEI3-AAAi
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOBZA&sid=06f47PLdT2QjJRdRAAAS
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIOEhG&sid=-rRTtWVV6yEWZkqNAAAU
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOhIU&sid=YsqTY6ctxcuAcjvwAAAk
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOiVN&sid=0BngYOnC9ZPURbtcAAAI
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOJih&sid=c8KluezYgHSr0yHGAAAW
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOmD9&sid=a9JjFEvJao43zt6CAAAo
Method	POST
Attack	
Evidence	

Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOMeM&sid=i6bdX8p1D0EFVnupAAAY
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOP46&sid=ruBBrVn9fE_F1wM-AAAa
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOqDD&sid=JC1ekD_Zh9n659q9AAAq
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIOQFF&sid=k6F6sgkqu7-F3mdHAAAc
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOSVu&sid=SdCA5TaV_EE9dy19AAAe
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOVCY&sid=L4knAU540ljVTjTFAAAg
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOw_E&sid=E8bG5H88ZZu6x7DXAAAs
Method	POST

Attack	
Evidence	
Other	
Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOwJC&sid=drxMb855dSnsb3-0AAAt
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIP1nf&sid=4tMqpwECVd3QYn6LAAAy
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIP7wO&sid=B- VwlotrGvt_zZJgAAA0
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIP9px&sid=RSMsBj2nWSvCnbDbAAA2
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPg7v&sid=IOUKVOyvWg9SAcXBAABE
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPh0v&sid=F2Wh9nt7bXo9pSIVAABG
Method	POST
Attack	
Evidence	
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXIPhzC&sid=LHJ6ah5Z_SHnhYOIAABI
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPItZ&sid=NWf5_adIRpq6XRiUAAA5
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPJAr&sid=7DdeBruF0OwBhp67AAA4
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPjw3&sid=rgfE_I7RPI1LHFbFAABK
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPIVT&sid=1Lt6h3A3eZVMp7NrAABM
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmMd&sid=pQdzAuDtIJRC4tKRAABO
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnB8&sid=gtGYScX-WJR9eBWLAABQ
Method	POST
Attack	
Evidence	

Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPNP8&sid=t3jFQ_asoWrzfGkgAAA8
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPo1v&sid=RHZWQ0DPD1TDDq8oAABS
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPokU&sid=4sp63Er9EkvPF6aPAABU
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPPdM&sid=Me_bKGbJk93GH-fYAAA-
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPWZx&sid=lng5-c-rNyDCFS5CAABA
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPYQE&sid=BVad5NVM2JIZA8g9AABC
Method	POST
Attack	
Evidence	
Other Info	
Instances	102
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Reference	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 https://www.w3.org/TR/CSP/
	https://www.ws.org/TK/CSF/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	<u>693</u>
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	
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/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: *
	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/
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/ae.svg
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: *
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/Feedbacks/
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/Quantitys/
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/i18n/en.json
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/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/assets/public/images/carousel/1.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/carousel/2.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/carousel/3.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/carousel/4.jpg
Method	GET
Attack	
Evidence	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://localhost:3000/assets/public/images/carousel/5.png
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/carousel/6.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/carousel/7.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/hackingInstructor.png
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/JuiceShop_Logo.png

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/apple_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/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.
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	

F '.	A
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/no-results.png
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/assets/public/images/uploads/%E1%93%9A%E1%98%8F%E1%97%A2-
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/uploads/BeeHaven.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
LVIGETICE	Access Control Amon Chight.

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/uploads/building-something-literally-bottom-up-1721152342603.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/uploads/everything-up-and-running! -1721152385146.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/uploads/favorite-hiking-place.png
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/uploads/IMG_4253.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/uploads/magn(et)ificent!-1571814229653.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
URL	which uses some other form of security, such as IP address white-listing. http://localhost:3000/assets/public/images/uploads/my-rare-collectors-item!-%5B%CC%B2%CC%85\$%CC%B2%CC%85(%CC%B2%CC%85-%CD%A1%C2%B0-%CD%9C%CA%96-%CD%A1%C2%B0%CC%B2%CC%85)%CC%B2%CC%85\$%CC%B2%CC%85%5D-1572603645543.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/uploads/putting-in-the-hardware-1721152366854.
	<u>ipg</u>
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/uploads/sorted-the-pieces,-starting-assembly-process-1721152307290.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/az.svg
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/bd.svg
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/bg.svg
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/br.svg
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/ch.svg
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/cn.svg
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/cz.svg
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/de.svg
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/dk.svg
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/ee.svg
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/es-ct.svg
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/es.svg
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/favicon.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/fi.svg
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/font-mfizz.woff
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/fr.svg
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: *
	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/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/gb.svg
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/ge.svg
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/gr.svg
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/hk.svg
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/hu.svg
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/id.svg
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/ie.svg
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/il.svg
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/in.svg
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/it.svg
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/jp.svg
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: *
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/polyfills.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *

	The CORS misconfiguration on the web server permits cross-domain read requests from
Other Info	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 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: *
	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 arbitriary third panies 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/julce-shop/build/routes/main_is Evidence Access-Control-Allow-Origin: * The CORS misconfiguration on the web server permits cross-domain read requests from attributed APIs and the server permits cross-domain read requests from authenticated APIs on the server permits cross-domain read requests from this domain. Web browser in the server permits cross-domain read requests 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/julce-shop/build/routes/polyfills_is 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 domains. Use 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/julce-shop/build/routes/runtime_is 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 domains, using unauthenticated APIs on this domain. Web brow		
Method Access-Control-Allow-Origin: * The CORS misconliguration 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 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/juice-shop/build/routes/runtime.js 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 is somewhat. This misconfiguration could be used by an attacker to access date that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing. Hethod 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		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. Well 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/juice-shop/build/routes/runtime.js 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 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 party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the	URL	http://localhost:3000/juice-shop/build/routes/main.js
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 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://localhosti.3000/juice-shop/build/routes/runtime.js 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 contains, 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 Full Permit P	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 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/juice-shop/build/routes/runtime is 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/juice-shop/build/routes/styles.css 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 but which uses some other form	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/juice-shop/build/routes/runtime_is 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/juice-shop/build/routes/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 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/eyendor.js 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 i		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 of 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: * 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: * 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 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 re	URL	http://localhost:3000/juice-shop/build/routes/polyfills.js
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/juice-shop/build/routes/runtime.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 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: * 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 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 party to read the response from arbit	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/juice-shop/build/routes/runtime.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 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/juice-shop/build/routes/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 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: * The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web	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/juice-shop/build/routes/runtime.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 in domain. Web browser implementations do not permit arbitrary bird 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: * 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 bird 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: * 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 th	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/juice-shop/build/routes/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 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: * 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/juice-shop/build/routes/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 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: * 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/juice-shop/build/routes/runtime.js
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/juice-shop/build/routes/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 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: * 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/juice-shop/build/routes/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 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: * 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 Info Info Info Info Info Info Info	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/juice-shop/build/routes/vendor.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 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/juice-shop/build/routes/vendor.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 implementations do not permit arbitrary third parties to read the response from	URL	http://localhost:3000/juice-shop/build/routes/styles.css
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/juice-shop/build/routes/vendor.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 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/juice-shop/build/routes/vendor.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 implementations do not permit arbitrary third parties to read the response from	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 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/juice-shop/build/routes/vendor.js
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/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	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	
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/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/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/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.
URL	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.
URL	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.
URL	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.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/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.

LIDI	http://leastleast.0000/juice.shap/gade.goods/leastleastleastleastleastleastleastleast
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/kr.svg
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/lv.svg
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/MaterialIcons-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/mm.svg
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/nl.svg
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/no.svg
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/pl.svg
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/pt.svg
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/redirect?to=https://github.com/juice-shop/juice-shop
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/captcha/
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/memories/
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/rest/user/whoami
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/ro.svg
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/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/ru.svg
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/se.svg
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/si.svg
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/th.svg
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/tn.svg
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/tr.svg
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/tutorial.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/tw.svg
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/ua.svg
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/us.svg
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	167

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	<u>10098</u>
Medium	Missing Anti-clickjacking Header

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=PXINgoe&sid=2I5bMp82Z9dUQqfVAAAC
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=-mIVhTFFp9RS7Ff4AAAE
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINsZs&sid=Zi_Slhms1STDM57iAAAH
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINwFT&sid=fX51XeedI4pt4YQJAAAK
Method	POST
Attack	
Evidence	
Other	

Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINy3a&sid=Kwa8OeOh2pxuMSaVAAAM
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIO-IB&sid=UeL35-cfUjXzywO9AAAw
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIO2D2&sid=bdeyXpKNMNcBpQAbAAAO
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIO5At&sid=kA4CWjF19xGageFyAAAQ
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIObAs&sid=r0Gyydx5_nXCEI3-AAAi
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOBZA&sid=06f47PLdT2QjJRdRAAAS
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIOEhG&sid=-rRTtWVV6yEWZkqNAAAU
Method	POST
Attack	

Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOhIU&sid=YsqTY6ctxcuAcjvwAAAk
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOiVN&sid=0BngYOnC9ZPURbtcAAAI
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOJih&sid=c8KluezYgHSr0yHGAAAW
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOmD9&sid=a9JjFEvJao43zt6CAAAo
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOMeM&sid=i6bdX8p1D0EFVnupAAAY
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOP46&sid=ruBBrVn9fE_F1wM-AAAa
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOqDD&sid=JC1ekD_Zh9n659q9AAAq

Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIOQFF&sid=k6F6sgkqu7-F3mdHAAAc
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOSVu&sid=SdCA5TaV_EE9dy19AAAe
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOVCY&sid=L4knAU540ljVTjTFAAAg
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOw_E&sid=E8bG5H88ZZu6x7DXAAAs
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOwJC&sid=drxMb855dSnsb3-0AAAt
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIP1nf&sid=4tMqpwECVd3QYn6LAAAy
Method	POST
Attack	
Evidence	
Other	

Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIP7wO&sid=B- VwlotrGvt_zZJgAAA0
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIP9px&sid=RSMsBj2nWSvCnbDbAAA2
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPg7v&sid=IOUKVOyvWg9SAcXBAABE
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPh0v&sid=F2Wh9nt7bXo9pSIVAABG
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPhzC&sid=LHJ6ah5Z_SHnhYOIAABI
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPItZ&sid=NWf5_adIRpq6XRiUAAA5
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPJAr&sid=7DdeBruF0OwBhp67AAA4
Method	POST
Attack	

Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPjw3&sid=rgfE_I7RPI1LHFbFAABK
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPIVT&sid=1Lt6h3A3eZVMp7NrAABM
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmMd&sid=pQdzAuDtIJRC4tKRAABO
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnB8&sid=gtGYScX-WJR9eBWLAABQ
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPNP8&sid=t3jFQ_asoWrzfGkqAAA8
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPo1v&sid=RHZWQ0DPD1TDDq8oAABS
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPokU&sid=4sp63Er9EkvPF6aPAABU

Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPPdM&sid=Me_bKGbJk93GH-fYAAA-
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPWZx&sid=lng5-c-rNyDCFS5CAABA
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPYQE&sid=BVad5NVM2JIZA8g9AABC
Method	POST
Attack	
Evidence	
Other Info	
Instances	42
	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.
Solution	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	1021
WASC Id	15
Plugin Id	10020
Medium	Session ID in URL Rewrite
Wedium	
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=PXINgog&sid=2I5bMp82Z9dUQqfVAAAC
Method	GET
Attack	
Evidence	2I5bMp82Z9dUQqfVAAAC

Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINhTs&sid=2I5bMp82Z9dUQqfVAAAC
Method	GET
Attack	
Evidence	2I5bMp82Z9dUQqfVAAAC
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINhYn&sid=2I5bMp82Z9dUQqfVAAAC
Method	GET
Attack	
Evidence	2I5bMp82Z9dUQqfVAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjtH&sid=-mIVhTFFp9RS7Ff4AAAE
Method	GET
Attack	
Evidence	-mIVhTFFp9RS7Ff4AAAE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINkJJ&sid=-mIVhTFFp9RS7Ff4AAAE
Method	GET
Attack	
Evidence	-mIVhTFFp9RS7Ff4AAAE
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINrx1&sid=7K5VpH6acNpSwKXeAAAG
Method	GET
Attack	
Evidence	7K5VpH6acNpSwKXeAAAG
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINsac&sid=Zi_SIhms1STDM57iAAAH
Method	GET
Attack	
Evidence	Zi_Slhms1STDM57iAAAH
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINsmJ&sid=7K5VpH6acNpSwKXeAAAG
Method	GET

Attack	
Evidence	7K5VpH6acNpSwKXeAAAG
Other	The vipinous spewrote, with
Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINteT&sid=Zi_Slhms1STDM57iAAAH
Method	GET
Attack	
Evidence	Zi_Slhms1STDM57iAAAH
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINtMP&sid=7K5VpH6acNpSwKXeAAAG
Method	GET
Attack	
Evidence	7K5VpH6acNpSwKXeAAAG
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINtOO&sid=Zi_Slhms1STDM57iAAAH
Method	GET
Attack	
Evidence	Zi_Slhms1STDM57iAAAH
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINw-b&sid=fX51XeedI4pt4YQJAAAK
Method	GET
Attack	
Evidence	fX51XeedI4pt4YQJAAAK
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINwep&sid=fX51XeedI4pt4YQJAAAK
Method	GET
Attack	
Evidence	fX51XeedI4pt4YQJAAAK
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINwG5&sid=fX51XeedI4pt4YQJAAAK
Method	GET
Attack	
Evidence	fX51Xeedl4pt4YQJAAAK
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXINy3z&sid=Kwa8OeOh2pxuMSaVAAAM
Method	GET
Attack	
Evidence	Kwa8OeOh2pxuMSaVAAAM
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINyTN&sid=Kwa8OeOh2pxuMSaVAAAM
Method	GET
Attack	
Evidence	Kwa8OeOh2pxuMSaVAAAM
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIO-IP&sid=UeL35-cfUjXzywO9AAAw
Method	GET
Attack	
Evidence	UeL35-cfUjXzywO9AAAw
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIO-YT&sid=UeL35-cfUjXzywO9AAAw
Method	GET
Attack	
Evidence	UeL35-cfUjXzywO9AAAw
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIO2-k&sid=bdeyXpKNMNcBpQAbAAAO
Method	GET
Attack	
Evidence	bdeyXpKNMNcBpQAbAAAO
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIO2Dq&sid=bdeyXpKNMNcBpQAbAAAO
Method	GET
Attack	
Evidence	bdeyXpKNMNcBpQAbAAAO
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIO3Hw&sid=bdeyXpKNMNcBpQAbAAAO
Method	GET
Attack	
Evidence	bdeyXpKNMNcBpQAbAAAO

0 .11	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIO5Az&sid=kA4CWjF19xGageFyAAAQ
Method	GET
Attack	
Evidence	kA4CWjF19xGageFyAAAQ
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIO5cR&sid=kA4CWjF19xGageFyAAAQ
Method	GET
Attack	
Evidence	kA4CWjF19xGageFyAAAQ
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIO5s9&sid=kA4CWjF19xGageFyAAAQ
Method	GET
Attack	
Evidence	kA4CWjF19xGageFyAAAQ
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIO_5g&sid=UeL35-cfUjXzywO9AAAw
Method	GET
Attack	
Evidence	UeL35-cfUjXzywO9AAAw
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIObB3&sid=r0Gyydx5_nXCEI3-AAAi
Method	GET
Attack	
Evidence	r0Gyydx5_nXCEI3-AAAi
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIObll&sid=r0Gyydx5_nXCEI3-AAAi
Method	GET
Attack	
Evidence	r0Gyydx5_nXCEI3-AAAi
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIObWa&sid=r0Gyydx5_nXCEI3-AAAi
Method	GET

A tto als	
Attack	
Evidence	r0Gyydx5_nXCEI3-AAAi
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOBZd&sid=06f47PLdT2QjJRdRAAAS
Method	GET
Attack	
Evidence	06f47PLdT2QjJRdRAAAS
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOCGk&sid=06f47PLdT2QjJRdRAAAS
Method	GET
Attack	
Evidence	06f47PLdT2QjJRdRAAAS
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIOEiH&sid=-rRTtWVV6yEWZkqNAAAU
Method	GET
Attack	
Evidence	-rRTtWVV6yEWZkqNAAAU
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIOFYU&sid=-rRTtWVV6yEWZkqNAAAU
Method	GET
Attack	
Evidence	-rRTtWVV6yEWZkqNAAAU
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOhla&sid=YsqTY6ctxcuAcjvwAAAk
Method	GET
Attack	
Evidence	YsqTY6ctxcuAcjvwAAAk
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOiEA&sid=YsqTY6ctxcuAcjvwAAAk
Method	GET
Attack	
Evidence	YsqTY6ctxcuAcjvwAAAk
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXIOiQ2&sid=YsqTY6ctxcuAcjvwAAAk
Method	GET
Attack	
Evidence	YsqTY6ctxcuAcjvwAAAk
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOiq_&sid=0BngYOnC9ZPURbtcAAAI
Method	GET
Attack	
Evidence	0BngYOnC9ZPURbtcAAAI
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOiVo&sid=0BngYOnC9ZPURbtcAAAI
Method	GET
Attack	
Evidence	0BngYOnC9ZPURbtcAAAI
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOJjH&sid=c8KluezYgHSr0yHGAAAW
Method	GET
Attack	
Evidence	c8KluezYgHSr0yHGAAAW
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOK4P&sid=c8KluezYgHSr0yHGAAAW
Method	GET
Attack	
Evidence	c8KluezYgHSr0yHGAAAW
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOKHI&sid=c8KluezYgHSr0yHGAAAW
Method	GET
Attack	
Evidence	c8KluezYgHSr0yHGAAAW
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOmDk&sid=a9JjFEvJao43zt6CAAAo
Method	GET
Attack	
Evidence	a9JjFEvJao43zt6CAAAo

Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOMeb&sid=i6bdX8p1D0EFVnupAAAY
Method	GET
Attack	
Evidence	i6bdX8p1D0EFVnupAAAY
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOmlv&sid=a9JjFEvJao43zt6CAAAo
Method	GET
Attack	
Evidence	a9JjFEvJao43zt6CAAAo
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOMvp&sid=i6bdX8p1D0EFVnupAAAY
Method	GET
Attack	
Evidence	i6bdX8p1D0EFVnupAAAY
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIONAQ&sid=i6bdX8p1D0EFVnupAAAY
Method	GET
Attack	
Evidence	i6bdX8p1D0EFVnupAAAY
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOP4X&sid=ruBBrVn9fE_F1wM-AAAa
Method	GET
Attack	
Evidence	ruBBrVn9fE_F1wM-AAAa
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOPXD&sid=ruBBrVn9fE_F1wM-AAAa
Method	GET
Attack	
Evidence	ruBBrVn9fE_F1wM-AAAa
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOqE2&sid=JC1ekD_Zh9n659q9AAAq
Method	GET

Attoole	
Attack	
Evidence	JC1ekD_Zh9n659q9AAAq
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIOQFx&sid=k6F6sgkqu7-F3mdHAAAc
Method	GET
Attack	
Evidence	k6F6sgkqu7-F3mdHAAAc
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIOQpI&sid=k6F6sgkqu7-F3mdHAAAc
Method	GET
Attack	
Evidence	k6F6sgkqu7-F3mdHAAAc
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOqVu&sid=JC1ekD_Zh9n659q9AAAq
Method	GET
Attack	
Evidence	JC1ekD_Zh9n659q9AAAq
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOSVw&sid=SdCA5TaV_EE9dy19AAAe
Method	GET
Attack	
Evidence	SdCA5TaV_EE9dy19AAAe
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOT8H&sid=SdCA5TaV_EE9dy19AAAe
Method	GET
Attack	
Evidence	SdCA5TaV_EE9dy19AAAe
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOVDz&sid=L4knAU540ljVTjTFAAAg
Method	GET
Attack	
Evidence	L4knAU540ljVTjTFAAAg
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXIOw M&sid=E8bG5H88ZZu6x7DXAAAs
Method	GET
Attack	
Evidence	E8bG5H88ZZu6x7DXAAAs
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOWjT&sid=L4knAU540ljVTjTFAAAg
Method	GET
Attack	
Evidence	L4knAU540ljVTjTFAAAg
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOwKB&sid=drxMb855dSnsb3-0AAAt
Method	GET
Attack	
Evidence	drxMb855dSnsb3-0AAAt
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOwun&sid=drxMb855dSnsb3-0AAAt
Method	GET
Attack	
Evidence	drxMb855dSnsb3-0AAAt
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOxBv&sid=E8bG5H88ZZu6x7DXAAAs
Method	GET
Attack	
Evidence	E8bG5H88ZZu6x7DXAAAs
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOxJF&sid=E8bG5H88ZZu6x7DXAAAs
Method	GET
Attack	
Evidence	E8bG5H88ZZu6x7DXAAAs
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIP1np&sid=4tMqpwECVd3QYn6LAAAy
Method	GET
Attack	
Evidence	4tMqpwECVd3QYn6LAAAy

Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIP2Eg&sid=4tMqpwECVd3QYn6LAAAy
Method	GET
Attack	
Evidence	4tMqpwECVd3QYn6LAAAy
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIP7we&sid=B- VwlotrGvt_zZJgAAA0
Method	GET
Attack	
Evidence	B-VwlotrGvt_zZJgAAA0
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIP8mH&sid=B- VwlotrGvt_zZJgAAA0
Method	GET
Attack	
Evidence	B-VwlotrGvt_zZJgAAA0
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIP8R5&sid=B- VwlotrGvt_zZJgAAA0
Method	GET
Attack	
Evidence	B-VwlotrGvt_zZJgAAA0
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIP8vQ&sid=B- VwlotrGvt_zZJgAAA0
Method	GET
Attack	
Evidence	B-VwlotrGvt_zZJgAAA0
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIP9q0&sid=RSMsBj2nWSvCnbDbAAA2
Method	GET
Attack	
Evidence	RSMsBj2nWSvCnbDbAAA2
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPAM8&sid=RSMsBj2nWSvCnbDbAAA2
Method	GET

Attack	
Evidence	RSMsBj2nWSvCnbDbAAA2
Other	NONSEJENVOVONSESSI V V VE
Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPAS4&sid=RSMsBj2nWSvCnbDbAAA2
Method	GET
Attack	
Evidence	RSMsBj2nWSvCnbDbAAA2
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPg89&sid=IOUKVOyvWg9SAcXBAABE
Method	GET
Attack	
Evidence	IOUKVOyvWg9SAcXBAABE
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPghg&sid=IOUKVOyvWg9SAcXBAABE
Method	GET
Attack	
Evidence	IOUKVOyvWg9SAcXBAABE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPh0- &sid=F2Wh9nt7bXo9pSIVAABG
Method	GET
Attack	
Evidence	F2Wh9nt7bXo9pSIVAABG
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPhE0&sid=F2Wh9nt7bXo9pSIVAABG
Method	GET
Attack	
Evidence	F2Wh9nt7bXo9pSIVAABG
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPhzH&sid=LHJ6ah5Z_SHnhYOIAABI
Method	GET
Attack	
Evidence	LHJ6ah5Z_SHnhYOIAABI
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXIPilj&sid=LHJ6ah5Z_SHnhYOIAABI
Method	GET
Attack	
Evidence	LHJ6ah5Z_SHnhYOIAABI
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPIta&sid=NWf5_adIRpq6XRiUAAA5
Method	GET
Attack	
Evidence	NWf5_adIRpq6XRiUAAA5
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPJAU&sid=NWf5_adIRpq6XRiUAAA5
Method	GET
Attack	
Evidence	NWf5_adIRpq6XRiUAAA5
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPJBH&sid=7DdeBruF0OwBhp67AAA4
Method	GET
Attack	
Evidence	7DdeBruF0OwBhp67AAA4
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPJIx&sid=NWf5_adIRpq6XRiUAAA5
Method	GET
Attack	
Evidence	NWf5_adIRpq6XRiUAAA5
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPJSH&sid=7DdeBruF0OwBhp67AAA4
Method	GET
Attack	
Evidence	7DdeBruF0OwBhp67AAA4
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPjwO&sid=rgfE_I7RPI1LHFbFAABK
Method	GET
Attack	
Evidence	rgfE_I7RPI1LHFbFAABK

URL http://localhosts3000/socket.io/? FIG-48transport-polling&t=PXIPk5V&sid=rgfE_I7RP11LHFbFAABK Method GET Attack Evidence rgfE_I7RP11LHFbFAABK Other Info URL http://localhosts3000/socket.io/? FIG-48transport-polling&t=PXIPIml&sid=1L16h3A3eZVMp7NrAABM Method GET Attack Evidence 1L16h3A3eZVMp7NrAABM Other Info URL http://localhosts3000/socket.io/? FIG-48transport-polling&t=PXIPIml&sid=1L16h3A3eZVMp7NrAABM Method GET Attack Evidence 1L16h3A3eZVMp7NrAABM Method GET Attack Evidence 1L16h3A3eZVMp7NrAABM Other Info URL http://localhosts3000/socket.io/? FIG-48transport-polling&t=PXIPIMS&sid=1L16h3A3eZVMp7NrAABM Other Info URL http://localhosts3000/socket.io/? FIG-48transport-polling&t=PXIPmOQ&sid=pQdzAuDtURC4tKRAABO Other Info URL http://localhosts3000/socket.io/? FIG-48transport-polling&t=PXIPmSo&sid=pQdzAuDtURC4tKRAABO Other Info URL http://localhosts3000/socket.io/? FIG-48transport-polling&t=PXIPmSo&sid=pQdzAuDtURC4tKRAABO Other Info URL http://localhosts3000/socket.io/? FIG-48transport-polling&t=PXIPmSo&sid=spQdzAuDtURC4tKRAABO Other Info URL http://localhosts3000/socket.io/? FIG-48transport-polling&t=PXIPN_X&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence 13jFQ_asoWrzfGkqAAA8 Other Info URL http://localhosts3000/socket.io/?EIO=4&transport-polling&t=PXIPnBR&sid=gtGYSox-WuRSgBWtAABQ Other Info In	Other Info	
Attack Evidence rgfE_17RPI1LHFbFAABK Other Info URL http://localhost.3000/socket.io/? EIO=48transport=polling&t=PXIPImI&sid=1Li6h3A3eZVMp7NrAABM Method GET Attack Evidence 1Li6h3A3eZVMp7NrAABM Other Info URL http://localhost.3000/socket.io/? EIO=48transport=polling&t=PXIPIv8&sid=1Li6h3A3eZVMp7NrAABM Method GET Attack Evidence 1Li6h3A3eZVMp7NrAABM Other Info URL http://localhost.3000/socket.io/? EIO=48transport=polling&t=PXIPMOQ&sid=pQdzAuDitJRC4tKRAABQ Method GET Attack Evidence pQdzAuDitJRC4tKRAABQ Method GET Attack Evidence pQdzAuDitJRC4tKRAABQ Other Info URL http://localhost.3000/socket.io/? EIO=48transport=polling&t=PXIPMSo&sid=pQdzAuDitJRC4tKRAABQ Method GET Attack Evidence pQdzAuDitJRC4tKRAABQ Other Info URL http://localhost.3000/socket.io/? EIO=48transport=polling&t=PXIPMSo&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAAB Other Info Dter Info Nttp://localhost.3000/socket.io/?EIO=48transport=polling&t=PXIPnBR&sid=gtGYScX-	URL	
Evidence rgfE_17RP/1LHFbFAABK Other Info URL bttp://localhost.3000/socket.io/? EIO=4&transport=polling&t=PXIPIml&sid=1Lt6h3A3eZVMp7NrAABM Method GET Attack Evidence 1Lt6h3A3eZVMp7NrAABM Other Info URL bttp://localhost.3000/socket.io/? EIO=4&transport=polling&t=PXIPIVs&sid=1Lt6h3A3eZVMp7NrAABM Method GET Attack Evidence 1Lt6h3A3eZVMp7NrAABM Other Info URL bttp://localhost.3000/socket.io/? EIO=4&transport=polling&t=PXIPIMOQ&sid=pOdzAuDtUJRC4tKRAABQ Method GET Attack Evidence pOdzAuDtUJRC4tKRAABQ Other Info URL http://localhost.3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pOdzAuDtUJRC4tKRAABQ Method GET Attack Evidence pOdzAuDtUJRC4tKRAABQ Other Info URL http://localhost.3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDtUJRC4tKRAABQ Method GET Attack Evidence pOdzAuDtUJRC4tKRAABO Other Info URL http://localhost.3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info Attack Evidence t3jFQ_asoWrzfGkqAAA8	Method	GET
Other Info URL http://localhost:3000/socket.io/? EIO=48transport=polling&t=PXIPIml&sid=1Li6h3A3eZVMp7NrAABM Method GET Attack Evidence 1Li6h3A3eZVMp7NrAABM Other Info URL http://localhost:3000/socket.io/? EIO=48transport=polling&t=PXIPIVs&sid=1Li6h3A3eZVMp7NrAABM Method GET Attack Evidence 1Li6h3A3eZVMp7NrAABM Other Info URL http://localhost:3000/socket.io/? EIO=48transport=polling&t=PXIPIVoQ&sid=pQdzAuDtUJRC4tKRAABO Method GET Attack Evidence pQdzAuDtUJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=48transport=polling&t=PXIPmSo&sid=pQdzAuDtUJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=48transport=polling&t=PXIPmSo&sid=pQdzAuDtUJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=48transport=polling&t=PXIPmSo&sid=pQdzAuDtUJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=48transport=polling&t=PXIPnX&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	Attack	
Info URL http://localhost:3000/socket.io/? EIO=48transport=polling&t=PXIPIml&sid=1Lt6h3A3eZVMp7NrAABM Method GET Attack Evidence 1Lt6h3A3eZVMp7NrAABM Other Info URL http://localhost:3000/socket.io/? EIO=48transport=polling&t=PXIPIvs&sid=1Lt6h3A3eZVMp7NrAABM Method GET Attack Evidence 1Lt6h3A3eZVMp7NrAABM Other Info URL http://localhost:3000/socket.io/? EIO=48transport=polling&t=PXIPIvs&sid=1Lt6h3A3eZVMp7NrAABM Wethod GET Attack Evidence QdzAuDttJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=48transport=polling&t=PXIPmSo&sid=pQdzAuDttJRC4tKRAABO Method GET Attack Evidence pQdzAuDttJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=48transport=polling&t=PXIPmSo&sid=pQdzAuDttJRC4tKRAABO Method GET Attack Evidence pQdzAuDttJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=48transport=polling&t=PXIPnSo&sid=3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence 13jFQ_asoWrzfGkqAAA8 Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	Evidence	rgfE_I7RPI1LHFbFAABK
Method GET Attack Evidence 1Lt6h3A3eZVMp7NrAABM Other Info URL bttp://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPIvs&sid=1Lt6h3A3eZVMp7NrAABM Method GET Attack Evidence 1Lt6h3A3eZVMp7NrAABM Method GET Attack Evidence 1Lt6h3A3eZVMp7NrAABM Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPIvs&sid=1Lt6h3A3eZVMp7NrAABM Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmOQ&sid=pQdzAuDtJJRC4tKRAABO Method GET Attack Evidence pQdzAuDtJJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDtJJRC4tKRAABO Method GET Attack Evidence pQdzAuDtJJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info		
Attack Evidence 1Lt6h3A3eZVMp7NrAABM Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPIVs&sid=1Lt6h3A3eZVMp7NrAABM Method GET Attack Evidence 1Lt6h3A3eZVMp7NrAABM Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmOQ&sid=pQdzAuDtIJRC4tKRAABO Method GET Attack Evidence pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPMSo&sid=pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPN X&sid=t3jFQ_asoWrztGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrztGkqAAA8 Other Info Info Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	URL	
Evidence 1Lt6h3A3eZVMp7NrAABM Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPIVs&sid=1Lt6h3A3eZVMp7NrAABM Method GET Attack Evidence 1Lt6h3A3eZVMp7NrAABM Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmOQ&sid=pQdzAuDttJRC4tKRAABO Method GET Attack Evidence pQdzAuDttJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDttJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDttJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPN X&sid=t3jFQ_asoWrzfGkqAAA& Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA& Other Info Other Info INFO Other Info INFO Other Info INFO Other Info I	Method	GET
Other Info URL http://localhost.3000/socket.io/? EIO=4&transport=polling&t=PXIPIVs&sid=1Lt6h3A3eZVMp7NrAABM Method GET Attack Evidence 1Lt6h3A3eZVMp7NrAABM Other Info URL http://localhost.3000/socket.io/? EIO=4&transport=polling&t=PXIPmOQ&sid=pQdzAuDttJRC4tKRAABO Method GET Attack Evidence pQdzAuDttJRC4tKRAABO Other Info URL http://localhost.3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDttJRC4tKRAABO Other Info URL http://localhost.3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDttJRC4tKRAABO Other Info URL http://localhost.3000/socket.io/? EIO=4&transport=polling&t=PXIPN X&sid=t3jFQ_asoWrzfGkqAAA& Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA& Other Info Other Info Other Info	Attack	
Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPIVs&sid=1Lt6h3A3eZVMp7NrAABM Method GET Attack Evidence 1Lt6h3A3eZVMp7NrAABM Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmOQ&sid=pQdzAuDttJRC4tKRAABO Method GET Attack Evidence pQdzAuDttJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDttJRC4tKRAABO Method GET Attack Evidence pQdzAuDttJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDttJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPN X&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info LURL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	Evidence	1Lt6h3A3eZVMp7NrAABM
Method GET Attack Evidence 1Lt6h3A3eZVMp7NrAABM Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PXIPmOQ&sid=pQdzAuDtIJRC4tKRAABO Method GET Attack Evidence pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDtIJRC4tKRAABO Other Info URL pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PXIPN_X&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-		
Attack Evidence 1Lt6h3A3eZVMp7NrAABM Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PXIPmOQ&sid=pQdzAuDtIJRC4tKRAABQ Method GET Attack Evidence pQdzAuDtIJRC4tKRAABQ Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDtIJRC4tKRAABQ Method GET Attack Evidence pQdzAuDtIJRC4tKRAABQ Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PXIPmSo&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PXIPN_X&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8	URL	
Evidence 1Lt6h3A3eZVMp7NrAABM Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmOQ&sid=pQdzAuDttJRC4tKRAABQ Method GET Attack Evidence pQdzAuDttJRC4tKRAABQ Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDttJRC4tKRAABQ Method GET Attack Evidence pQdzAuDttJRC4tKRAABQ Method GET Attack Evidence pQdzAuDttJRC4tKRAABQ Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPMSo&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info LIRL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-bttp.	Method	GET
Other Info URL http://localhost;3000/socket.io/? EIO=4&transport=polling&t=PXIPmOQ&sid=pQdzAuDtIJRC4tKRAABO Method GET Attack Evidence pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost;3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDtIJRC4tKRAABO Method GET Attack Evidence pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost;3000/socket.io/? EIO=4&transport=polling&t=PXIPN_X&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8	Attack	
Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmOQ&sid=pQdzAuDtIJRC4tKRAABO Method GET Attack Evidence pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDtIJRC4tKRAABO Method GET Attack Evidence pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPN_X&sid=t3jFQ_asoWrzfGkqAAA& Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA& Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	Evidence	1Lt6h3A3eZVMp7NrAABM
Method GET Attack Evidence pQdzAuDttJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? Evidence pQdzAuDttJRC4tKRAABO Method GET Attack Evidence pQdzAuDttJRC4tKRAABO Method GET Attack Evidence pQdzAuDttJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? ElO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDttJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? ElO=4&transport=polling&t=PXIPN X&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info LIDI http://localhost:3000/socket.io/?ElO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-		
Attack Evidence pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDtIJRC4tKRAABO Method GET Attack Evidence pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPN X&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info IIDI http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	URL	
Evidence pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDtIJRC4tKRAABO Method GET Attack Evidence pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPN_X&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	Method	GET
Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDtIJRC4tKRAABO Method GET Attack Evidence pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPN X&sid=t3jFQ asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	Attack	
Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmSo&sid=pQdzAuDttJRC4tKRAABO Method GET Attack Evidence pQdzAuDttJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPN_X&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	Evidence	pQdzAuDtlJRC4tKRAABO
Method GET Attack Evidence pQdzAuDtlJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? ElO=4&transport=polling&t=PXIPN X&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info http://localhost:3000/socket.io/?ElO=4&transport=polling&t=PXIPN X&sid=t3jFQ_asoWrzfGkqAAA8		
Attack Evidence pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPN X&sid=t3jFQ asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	URL	
Evidence pQdzAuDtIJRC4tKRAABO Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPN X&sid=t3jFQ asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	Method	GET
Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPN_X&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	Attack	
Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPN_X&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	Evidence	pQdzAuDtIJRC4tKRAABO
Method GET Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-		
Attack Evidence t3jFQ_asoWrzfGkqAAA8 Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	URL	
Evidence t3jFQ_asoWrzfGkqAAA8 Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	Method	GET
Other Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	Attack	
Info http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-	Evidence	t3jFQ_asoWrzfGkqAAA8
	URL	
Method GET	Method	GET

Attack	
Evidence	OFCVSOV MAIDOODIMA A DO
	gtGYScX-WJR9eBWLAABQ
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPndt&sid=gtGYScX-WJR9eBWLAABQ
Method	GET
Attack	
Evidence	gtGYScX-WJR9eBWLAABQ
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnLw&sid=gtGYScX-WJR9eBWLAABQ
Method	GET
Attack	
Evidence	gtGYScX-WJR9eBWLAABQ
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPNQI&sid=t3jFQ_asoWrzfGkqAAA8
Method	GET
Attack	
Evidence	t3jFQ_asoWrzfGkqAAA8
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPo25&sid=RHZWQ0DPD1TDDq8oAABS
Method	GET
Attack	
Evidence	RHZWQ0DPD1TDDq8oAABS
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPoCP&sid=RHZWQ0DPD1TDDq8oAABS
Method	GET
Attack	
Evidence	RHZWQ0DPD1TDDq8oAABS
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPolS&sid=4sp63Er9EkvPF6aPAABU
Method	GET
Attack	
Evidence	4sp63Er9EkvPF6aPAABU
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXIPOXI&sid=t3jFQ_asoWrzfGkqAAA8
Method	GET
Attack	
Evidence	t3jFQ_asoWrzfGkqAAA8
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPoxn&sid=4sp63Er9EkvPF6aPAABU
Method	GET
Attack	
Evidence	4sp63Er9EkvPF6aPAABU
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPPdb&sid=Me_bKGbJk93GH-fYAAA-
Method	GET
Attack	
Evidence	Me_bKGbJk93GH-fYAAA-
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPPrc&sid=Me_bKGbJk93GH-fYAAA-
Method	GET
Attack	
Evidence	Me_bKGbJk93GH-fYAAA-
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPWa5&sid=Ing5-c-rNyDCFS5CAABA
Method	GET
Attack	
Evidence	Ing5-c-rNyDCFS5CAABA
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPY3-&sid=Ing5-c-rNyDCFS5CAABA
Method	GET
Attack	
Evidence	Ing5-c-rNyDCFS5CAABA
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPY f&sid=BVad5NVM2JIZA8g9AABC
Method	GET
Attack	
Evidence	BVad5NVM2JIZA8g9AABC

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPYA4&sid=lng5-c-rNyDCFS5CAABA
Method	GET
Attack	
Evidence	Ing5-c-rNyDCFS5CAABA
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPYmv&sid=BVad5NVM2JIZA8g9AABC
Method	GET
Attack	
Evidence	BVad5NVM2JIZA8g9AABC
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPYQH&sid=BVad5NVM2JIZA8g9AABC
Method	GET
Attack	
Evidence	BVad5NVM2JIZA8g9AABC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=-mlVhTFFp9RS7Ff4AAAE
Method	GET
Attack	
Evidence	-mlVhTFFp9RS7Ff4AAAE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=-rRTtWVV6yEWZkqNAAAU
Method	GET
Attack	
Evidence	-rRTtWVV6yEWZkqNAAAU
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=06f47PLdT2QjJRdRAAAS
Method	GET
Attack	
Evidence	06f47PLdT2QjJRdRAAAS
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=0BngYOnC9ZPURbtcAAAI
Method	GET
Attack	

Evidence	0BngYOnC9ZPURbtcAAAI
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=1Lt6h3A3eZVMp7NrAABM
Method	GET
Attack	
Evidence	1Lt6h3A3eZVMp7NrAABM
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=2I5bMp82Z9dUQqfVAAAC
Method	GET
Attack	
Evidence	2I5bMp82Z9dUQqfVAAAC
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=4sp63Er9EkvPF6aPAABU
Method	GET
Attack	
Evidence	4sp63Er9EkvPF6aPAABU
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=4tMqpwECVd3QYn6LAAAy
Method	GET
Attack	
Evidence	4tMqpwECVd3QYn6LAAAy
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=7DdeBruF0OwBhp67AAA4
Method	GET
Attack	
Evidence	7DdeBruF0OwBhp67AAA4
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=7K5VpH6acNpSwKXeAAAG
Method	GET
Attack	
Evidence	7K5VpH6acNpSwKXeAAAG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=a9JjFEvJao43zt6CAAAo
Method	GET

Attack	
Evidence	a9JjFEvJao43zt6CAAAo
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=B-VwlotrGvt_zZJgAAA0
Method	GET
Attack	
Evidence	B-VwlotrGvt_zZJgAAA0
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=bdeyXpKNMNcBpQAbAAAO
Method	GET
Attack	
Evidence	bdeyXpKNMNcBpQAbAAAO
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=BVad5NVM2JIZA8g9AABC
Method	GET
Attack	
Evidence	BVad5NVM2JIZA8g9AABC
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=c8KluezYgHSr0yHGAAAW
Method	GET
Attack	
Evidence	c8KluezYgHSr0yHGAAAW
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=drxMb855dSnsb3-0AAAt
Method	GET
Attack	
Evidence	drxMb855dSnsb3-0AAAt
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=E8bG5H88ZZu6x7DXAAAs
Method	GET
Attack	
Evidence	E8bG5H88ZZu6x7DXAAAs
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=F2Wh9nt7bXo9pSIVAABG

	0.00
Method	GET
Attack	
Evidence	F2Wh9nt7bXo9pSIVAABG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=fX51XeedI4pt4YQJAAAK
Method	GET
Attack	
Evidence	fX51XeedI4pt4YQJAAAK
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=gtGYScX-WJR9eBWLAABQ
Method	GET
Attack	
Evidence	gtGYScX-WJR9eBWLAABQ
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=i6bdX8p1D0EFVnupAAAY
Method	GET
Attack	
Evidence	i6bdX8p1D0EFVnupAAAY
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=JC1ekD_Zh9n659q9AAAq
Method	GET
Attack	
Evidence	JC1ekD_Zh9n659q9AAAq
Other Info	
URL	$\underline{http://localhost:3000/socket.io/?EIO=4\&transport=websocket\&sid=k6F6sgkqu7-F3mdHAAAc}\\$
Method	GET
Attack	
Evidence	k6F6sgkqu7-F3mdHAAAc
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=kA4CWjF19xGageFyAAAQ
Method	GET
Attack	
Evidence	kA4CWjF19xGageFyAAAQ
Other Info	

URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=Kwa8OeOh2pxuMSaVAAAM
Method	GET
Attack	
Evidence	Kwa8OeOh2pxuMSaVAAAM
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=L4knAU540ljVTjTFAAAg
Method	GET
Attack	
Evidence	L4knAU540ljVTjTFAAAg
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=LHJ6ah5Z_SHnhYOIAABI
Method	GET
Attack	
Evidence	LHJ6ah5Z_SHnhYOIAABI
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=Ing5-c-rNyDCFS5CAABA
Method	GET
Attack	
Evidence	Ing5-c-rNyDCFS5CAABA
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=lOUKVOyvWg9SAcXBAABE
Method	GET
Attack	
Evidence	IOUKVOyvWg9SAcXBAABE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=Me_bKGbJk93GH-fYAAA-
Method	GET
Attack	
Evidence	Me_bKGbJk93GH-fYAAA-
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=NWf5_adIRpq6XRiUAAA5
Method	GET
Attack	
Evidence	NWf5_adIRpq6XRiUAAA5
Other	

Info	
URL	http://localhost:3000/socket.io/?
	EIO=4&transport=websocket&sid=pQdzAuDtlJRC4tKRAABO
Method	GET
Attack	
Evidence	pQdzAuDtIJRC4tKRAABO
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=r0Gyydx5_nXCEI3-AAAi
Method	GET
Attack	
Evidence	r0Gyydx5_nXCEI3-AAAi
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=rgfE_I7RPI1LHFbFAABK
Method	GET
Attack	
Evidence	rgfE_I7RPI1LHFbFAABK
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=RHZWQ0DPD1TDDq8oAABS
Method	GET
Attack	
Evidence	RHZWQ0DPD1TDDq8oAABS
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=RSMsBj2nWSvCnbDbAAA2
Method	GET
Attack	
Evidence	RSMsBj2nWSvCnbDbAAA2
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=ruBBrVn9fE_F1wM-AAAa
Method	GET
Attack	
Evidence	ruBBrVn9fE_F1wM-AAAa
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=SdCA5TaV_EE9dy19AAAe
Method	GET
Attack	
Evidence	SdCA5TaV_EE9dy19AAAe

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=t3jFQ_asoWrzfGkqAAA8
Method	GET
Attack	
Evidence	t3jFQ_asoWrzfGkqAAA8
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=UeL35-cfUjXzywO9AAAw
Method	GET
Attack	
Evidence	UeL35-cfUjXzywO9AAAw
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=YsqTY6ctxcuAcjvwAAAk
Method	GET
Attack	
Evidence	YsqTY6ctxcuAcjvwAAAk
Other Info	
URL	$\underline{http://localhost:3000/socket.io/?EIO=4\&transport=websocket\&sid=Zi_Slhms1STDM57iAAAH}$
Method	GET
Attack	
Evidence	Zi_Slhms1STDM57iAAAH
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINgoe&sid=2I5bMp82Z9dUQqfVAAAC
Method	POST
Attack	
Evidence	2I5bMp82Z9dUQqfVAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXINjrf&sid=-mlVhTFFp9RS7Ff4AAAE
Method	POST
Attack	
Evidence	-mIVhTFFp9RS7Ff4AAAE
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINrwa&sid=7K5VpH6acNpSwKXeAAAG
Method	POST
Attack	
Evidence	7K5VpH6acNpSwKXeAAAG

Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINsZs&sid=Zi_Slhms1STDM57iAAAH
Method	POST
Attack	
Evidence	Zi_Slhms1STDM57iAAAH
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINwFT&sid=fX51XeedI4pt4YQJAAAK
Method	POST
Attack	
Evidence	fX51XeedI4pt4YQJAAAK
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXINy3a&sid=Kwa8OeOh2pxuMSaVAAAM
Method	POST
Attack	
Evidence	Kwa8OeOh2pxuMSaVAAAM
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIO-IB&sid=UeL35-cfUjXzywO9AAAw
Method	POST
Attack	
Evidence	UeL35-cfUjXzywO9AAAw
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIO2D2&sid=bdeyXpKNMNcBpQAbAAAO
Method	POST
Attack	
Evidence	bdeyXpKNMNcBpQAbAAAO
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIO5At&sid=kA4CWjF19xGageFyAAAQ
Method	POST
Attack	
Evidence	kA4CWjF19xGageFyAAAQ
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIObAs&sid=r0Gyydx5_nXCEI3-AAAi
Method	POST

Attack	
Evidence	TOO In this To VOCIO AAA:
	r0Gyydx5_nXCEI3-AAAi
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOBZA&sid=06f47PLdT2QjJRdRAAAS
Method	POST
Attack	
Evidence	06f47PLdT2QjJRdRAAAS
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIOEhG&sid=-rRTtWVV6yEWZkqNAAAU
Method	POST
Attack	
Evidence	-rRTtWVV6yEWZkqNAAAU
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOhIU&sid=YsqTY6ctxcuAcjvwAAAk
Method	POST
Attack	
Evidence	YsqTY6ctxcuAcjvwAAAk
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOiVN&sid=0BngYOnC9ZPURbtcAAAl
Method	POST
Attack	
Evidence	0BngYOnC9ZPURbtcAAAI
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOJih&sid=c8KluezYgHSr0yHGAAAW
Method	POST
Attack	
Evidence	c8KluezYgHSr0yHGAAAW
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOmD9&sid=a9JjFEvJao43zt6CAAAo
Method	POST
Attack	
Evidence	a9JjFEvJao43zt6CAAAo
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXIOMeM&sid=i6bdX8p1D0EFVnupAAAY
Method	POST
Attack	
Evidence	i6bdX8p1D0EFVnupAAAY
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOP46&sid=ruBBrVn9fE_F1wM-AAAa
Method	POST
Attack	
Evidence	ruBBrVn9fE_F1wM-AAAa
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOqDD&sid=JC1ekD_Zh9n659q9AAAq
Method	POST
Attack	
Evidence	JC1ekD_Zh9n659q9AAAq
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIOQFF&sid=k6F6sgkqu7-F3mdHAAAc
Method	POST
Attack	
Evidence	k6F6sgkqu7-F3mdHAAAc
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOSVu&sid=SdCA5TaV_EE9dy19AAAe
Method	POST
Attack	
Evidence	SdCA5TaV_EE9dy19AAAe
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOVCY&sid=L4knAU540ljVTjTFAAAg
Method	POST
Attack	
Evidence	L4knAU540ljVTjTFAAAg
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOw E&sid=E8bG5H88ZZu6x7DXAAAs
Method	POST
Attack	
Evidence	E8bG5H88ZZu6x7DXAAAs

Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOwJC&sid=drxMb855dSnsb3-0AAAt
Method	POST
Attack	F001
Evidence	drxMb855dSnsb3-0AAAt
Other Info	UIXIVIDOS GOTISDO-OAAR
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIP1nf&sid=4tMgpwECVd3QYn6LAAAy
Method	POST
Attack	
Evidence	4tMqpwECVd3QYn6LAAAy
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIP7wO&sid=B- VwlotrGvt_zZJgAAA0
Method	POST
Attack	
Evidence	B-VwlotrGvt_zZJgAAA0
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIP9px&sid=RSMsBj2nWSvCnbDbAAA2
Method	POST
Attack	
Evidence	RSMsBj2nWSvCnbDbAAA2
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPg7v&sid=IOUKVOyvWg9SAcXBAABE
Method	POST
Attack	
Evidence	IOUKVOyvWg9SAcXBAABE
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPh0v&sid=F2Wh9nt7bXo9pSIVAABG
Method	POST
Attack	
Evidence	F2Wh9nt7bXo9pSIVAABG
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPhzC&sid=LHJ6ah5Z_SHnhYOIAABI
Method	POST

Attack	
	LILICODET CLICAVOIAADI
Evidence Other	LHJ6ah5Z_SHnhYOIAABI
Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPItZ&sid=NWf5_adIRpq6XRiUAAA5
Method	POST
Attack	
Evidence	NWf5_adIRpq6XRiUAAA5
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPJAr&sid=7DdeBruF0OwBhp67AAA4
Method	POST
Attack	
Evidence	7DdeBruF0OwBhp67AAA4
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPjw3&sid=rgfE_I7RPI1LHFbFAABK
Method	POST
Attack	
Evidence	rgfE_I7RPI1LHFbFAABK
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPIVT&sid=1Lt6h3A3eZVMp7NrAABM
Method	POST
Attack	
Evidence	1Lt6h3A3eZVMp7NrAABM
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPmMd&sid=pQdzAuDtIJRC4tKRAABO
Method	POST
Attack	
Evidence	pQdzAuDtlJRC4tKRAABO
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnB8&sid=gtGYScX-WJR9eBWLAABQ
Method	POST
Attack	
Evidence	gtGYScX-WJR9eBWLAABQ
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXIPNP8&sid=t3jFQ_asoWrzfGkqAAA8
Method	POST
Attack	
Evidence	t3jFQ_asoWrzfGkqAAA8
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPo1v&sid=RHZWQ0DPD1TDDq8oAABS
Method	POST
Attack	
Evidence	RHZWQ0DPD1TDDq8oAABS
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPokU&sid=4sp63Er9EkvPF6aPAABU
Method	POST
Attack	
Evidence	4sp63Er9EkvPF6aPAABU
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPPdM&sid=Me_bKGbJk93GH-fYAAA-
Method	POST
Attack	
Evidence	Me_bKGbJk93GH-fYAAA-
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPWZx&sid=lng5-c-rNyDCFS5CAABA
Method	POST
Attack	
Evidence	Ing5-c-rNyDCFS5CAABA
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIPYQE&sid=BVad5NVM2JIZA8g9AABC
Method	POST
Attack	
Evidence	BVad5NVM2JIZA8g9AABC
Other Info	
Instances	188
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	<u>3</u>
Medium	Vulnerable JS Library
Description	The identified library appears to be vulnerable.
URL	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	/2.2.4/jquery.min.js
Other Info	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/
Instances	1
Solution	Upgrade to the latest version of the affected library.
Reference	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
CWE Id	<u>1395</u>
WASC Id	
Plugin Id	<u>10003</u>
Low	Cross-Domain JavaScript Source File Inclusion
Description	The page includes one or more script files from a third-party domain.
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/
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></td><td></td></tr></tbody></table></script></pre>

Method	CET
	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/assets/public/images/uploads/%E1%93%9A%E1%98%8F%E1%97%A2-
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/assets/public/images/uploads/%E1%93%9A%E1%98%8F%E1%97%A2-</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/favicon.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/favicon.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/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>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/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></td><td></td></tr></tbody></table></script></pre>

URL	http://localhost:3000/juice-shop/build/routes/assets/public/runtime.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/build/routes/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/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>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><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/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</td><td></td></tr></tbody></table></script></pre>

URL http://localhost:3000/juice-shop/build/routes/runtime.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/build/routes/styles.css Method GET Attack Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"> /script> Other Info URL http://localhost:3000/juice-shop/build/routes/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/build/routes/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/build/routes/vendor.js Method GET Attack Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"> /scripts src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"> /scripts src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"> /scripts</th><th>Method Attack Evidence Other Info Method Attack Evidence Other Info Method Attack Evidence Other Info Method Attack Evidence Other Info</th></tr><tr><td>Attack Evidence</td><td>Attack Evidence Other Info Method Attack Evidence Other Info Method Attack Evidence Other Info Method Attack Evidence Other Info</td></tr><tr><td>Evidence</td><td>Evidence Other Info Method Attack Evidence Other Info Method Attack Evidence Other Info Other Info Other Info Other Info</td></tr><tr><td>Other Info URL http://localhost:3000/juice-shop/build/routes/styles.css Method GET Attack Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"> /script> Other Info URL http://localhost:3000/juice-shop/build/routes/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/build/routes/vendor.js Method GET Attack Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"> /script> Method GET Attack Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"> /script> Other Other</td><td>Other Info L Method Attack Evidence Other Info L Method Attack Evidence Other Info Other Info</td></tr><tr><td>Info URL http://localhost:3000/juice-shop/build/routes/styles.css Method GET Attack Evidence /script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">/script> Other Info URL http://localhost:3000/juice-shop/build/routes/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/build/routes/vendor.js Method GET Attack Evidence /script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"> Other Attack Evidence /script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">/script> Other <td>Info L Method Attack Evidence Other Info L Method Attack Evidence Other Other</td>	Info L Method Attack Evidence Other Info L Method Attack Evidence Other Other
Method GET Attack Evidence	Method Attack Evidence Other Info Method Attack Evidence Other Info
Attack Evidence	Attack Evidence Other Info L Method Attack Evidence Other Info
Evidence	Evidence Other Info Method Attack Evidence Other Info
Other Info URL http://localhost:3000/juice-shop/build/routes/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/build/routes/vendor.js Method GET Attack Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script> Other Other Other	Other Info L Method Attack Evidence Other Info
Info URL http://localhost:3000/juice-shop/build/routes/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/build/routes/vendor.js Method GET Attack Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script> Other	Info L Method Attack Evidence Other Info
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/build/routes/vendor.js Method GET Attack Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script> Other	Method Attack Evidence Other Info
Attack Evidence	Attack Evidence Other Info
Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info URL http://localhost:3000/juice-shop/build/routes/vendor.js Method GET Attack Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script> Other	Evidence Other Info
Other Info URL http://localhost:3000/juice-shop/build/routes/vendor.js Method GET Attack Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></td><td>Other Info</td></tr><tr><td>Info URL http://localhost:3000/juice-shop/build/routes/vendor.js Method GET Attack Evidence Script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"> Cookieconsent.min.js"> Cookieconsent.min.js" Cookieconsent.min.js" Cookieconsent.min.js" Cookieconsent.min.js</td><td>Info</td></tr><tr><td>Method GET Attack Evidence</td><td></td></tr><tr><td>Attack Evidence</td><td>-</td></tr><tr><td>Evidence <pre></td><td>Method</td></tr><tr><td>Other /script></td><td>Attack</td></tr><tr><td></td><td>Evidence</td></tr><tr><td>THO STATE OF THE S</td><td>Other Info</td></tr><tr><td>URL http://localhost:3000/juice-shop/build/routes/vendor.js</td><td>_</td></tr><tr><td>Method GET</td><td>Method</td></tr><tr><td>Attack</td><td>Attack</td></tr><tr><td>Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>	Evidence
Other Info	
URL <a 3.1.0="" ajax="" cdnjs.cloudflare.com="" cookieconsent.min.js"="" cookieconsent2="" href="http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/assets/p</td><td>_</td></tr><tr><td>Method GET</td><td>Method</td></tr><tr><td>Attack</td><td>Attack</td></tr><tr><td>Evidence <pre><script src=" libs="">	Evidence
Other Info	
URL <a 2.2.4="" ajax="" cdnjs.cloudflare.com="" href="http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/assets/p</td><td></td></tr><tr><td>Method GET</td><td>Method</td></tr><tr><td>Attack</td><td>Attack</td></tr><tr><td>Evidence <script src=" jquery="" jquery.min.js"="" libs="">	

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/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>$\underline{http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/favicon_js.ico}$</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/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	<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/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/express/lib/router/assets/public/runtime.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>

Evidence	/script>
Other	73CHpt2
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/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></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/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></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9</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: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></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>URL Method</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13 GET</td></tr><tr><td></td><td></td></tr><tr><td>Method</td><td></td></tr><tr><td>Method Attack</td><td>GET</td></tr><tr><td>Method Attack Evidence Other</td><td>GET</td></tr><tr><td>Method Attack Evidence Other Info</td><td><pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Method Attack Evidence Other Info URL	<pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14</pre>
Method Attack Evidence Other Info URL Method	<pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14</pre>
Method Attack Evidence Other Info URL Method Attack	GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</script> <<<<<<<<<<<<<<<<<< http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</script> <<<<<<<<<<<<<<<<<< http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL URL URL URL URL URL	<pre> <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script> http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 </pre>
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL URL Method	<pre> <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script> http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 </pre>
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Attack	<pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:365:14 GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script> http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:365:14 GET</pre>
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other	<pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:365:14 GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script> http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:365:14 GET</pre>
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info	<pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:365:14 GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script> http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:365:14 GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack URL Method Attack Evidence URL Method Attack Evidence Other Info URL URL URL URL URL URL	<pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script> http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14</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></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><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	
	http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5
Info	http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5 GET
Info URL	
Info URL Method	
Info URL Method Attack	GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</script> <<<<<<<<<<<<<<<<<< /script>
Info URL Method Attack Evidence Other Info URL	<pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script> http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5</pre></td></tr><tr><td>Info URL Method Attack Evidence Other Info URL Method</td><td><pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script> http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5</pre></td></tr><tr><td>Info URL Method Attack Evidence Other Info URL Method Attack</td><td><pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script> http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5</pre> GET</td></tr><tr><td>Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other</td><td><pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script> http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5</pre> GET</td></tr><tr><td>Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other</td><td><pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script> http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5 GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
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	<pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script> http://localhost:3000/juice-shop/node modules/express/lib/router/layer.js:95:5 GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> http://localhost:3000/juice-shop/node modules/express/lib/router/main.js</pre>
Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method	<pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script> http://localhost:3000/juice-shop/node modules/express/lib/router/layer.js:95:5 GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> http://localhost:3000/juice-shop/node modules/express/lib/router/main.js</pre>
Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Attack Evidence Other Info URL Method Attack	<pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script> http://localhost:3000/juice-shop/node modules/express/lib/router/layer.js:95:5 GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> http://localhost:3000/juice-shop/node_modules/express/lib/router/main.js GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</script></pre>
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 Other	<pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script> http://localhost:3000/juice-shop/node modules/express/lib/router/layer.js:95:5 GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> http://localhost:3000/juice-shop/node_modules/express/lib/router/main.js GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</script></pre>
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	<pre>GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script> http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5 GET <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> http://localhost:3000/juice-shop/node_modules/express/lib/router/main.js GET <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></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/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><tr><td>Evidence</td><td>/script></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/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/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>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/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></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/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">< /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/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	$<\!$
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/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>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/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></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/node_modules/serve-index/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/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/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/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/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/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/sitemap.xml

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/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/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
Instances	102
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	
Attack Evidence	192.168.99.100:3000
	192.168.99.100:3000 192.168.99.100:3000 192.168.99.100:4200
Evidence Other	
Evidence Other Info	192.168.99.100:3000 192.168.99.100:4200
Evidence Other Info Instances	192.168.99.100:3000 192.168.99.100:4200 1 Remove the private IP address from the HTTP response body. For comments, use JSP/ASP
Evidence Other Info Instances Solution	192.168.99.100:3000 192.168.99.100:4200 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.
Evidence Other Info Instances Solution Reference	192.168.99.100:3000 192.168.99.100:4200 1 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. https://tools.ietf.org/html/rfc1918
Evidence Other Info Instances Solution Reference CWE Id	192.168.99.100:3000 192.168.99.100:4200 1 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. https://tools.ietf.org/html/rfc1918 497
Evidence Other Info Instances Solution Reference CWE Id WASC Id	192.168.99.100:3000 192.168.99.100:4200 1 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. https://tools.ietf.org/html/rfc1918 497 13
Evidence Other Info Instances Solution Reference CWE Id WASC Id Plugin Id	1 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. https://tools.ietf.org/html/rfc1918 497 13
Evidence Other Info Instances Solution Reference CWE Id WASC Id Plugin Id Low	192.168.99.100:3000 192.168.99.100:4200 1 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. https://tools.ietf.org/html/rfc1918 497 13 2 Timestamp Disclosure - Unix
Evidence Other Info Instances Solution Reference CWE Id WASC Id Plugin Id Low Description	192.168.99.100:3000 192.168.99.100:4200 1 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. https://tools.ietf.org/html/rfc1918 497 13 2 Timestamp Disclosure - Unix A timestamp was disclosed by the application/web server Unix
Evidence Other Info Instances Solution Reference CWE Id WASC Id Plugin Id Low Description URL	192.168.99.100:3000 192.168.99.100:4200 1 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. https://tools.ietf.org/html/rfc1918 497 13 2 Timestamp Disclosure - Unix A timestamp was disclosed by the application/web server Unix http://localhost:3000
Evidence Other Info Instances Solution Reference CWE Id WASC Id Plugin Id Low Description URL Method	192.168.99.100:3000 192.168.99.100:4200 1 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. https://tools.ietf.org/html/rfc1918 497 13 2 Timestamp Disclosure - Unix A timestamp was disclosed by the application/web server Unix http://localhost:3000
Evidence Other Info Instances Solution Reference CWE Id WASC Id Plugin Id Low Description URL Method Attack	192.168.99.100:3000 192.168.99.100:4200 1 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. https://tools.ietf.org/html/rfc1918 497 13 2 Timestamp Disclosure - Unix A timestamp was disclosed by the application/web server Unix http://localhost:3000 GET
Evidence Other Info Instances Solution Reference CWE Id WASC Id Plugin Id Low Description URL Method Attack Evidence Other	192.168.99.100:3000 192.168.99.100:4200 1 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. https://tools.ietf.org/html/rfc1918 497 13 2 Timestamp Disclosure - Unix A timestamp was disclosed by the application/web server Unix http://localhost:3000 GET 1650485437

Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 14:35:49.
URL	http://localhost:3000
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 10:02:31.
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 15:10:37.
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 14:35:49.
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 10:02:31.
URL	http://localhost:3000/assets/public/images/uploads/%E1%93%9A%E1%98%8F%E1%97%A2-
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 15:10:37.
URL	http://localhost:3000/assets/public/images/uploads/%E1%93%9A%E1%98%8F%E1%97%A2-
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 14:35:49.
URL	http://localhost:3000/assets/public/images/uploads/%E1%93%9A%E1%98%8F%E1%97%A2-

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

Fuidanaa	4650495427
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1981395349

URL http://localhost:3000/juice-shop/build/routes/assets/public/polyfills.js Method GET Attack Evidence 2038834951	
Attack	
Evidence 2038834951	
Other Info 2038834951, which evaluates to: 2034-08-10 10:02:31.	
URL 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 15:10:37.	
URL 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 14:35:49.	
URL 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 10:02:31.	
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 15:10:37.	
URL http://localhost:3000/juice-shop/build/routes/assets/public/styles.css	
Method GET	
Attack	
Evidence 1981395349	
Other 1981395349, which evaluates to: 2032-10-14 14:35:49.	
URL http://localhost:3000/juice-shop/build/routes/assets/public/styles.css	
Method GET	
Attack	
Evidence 2038834951	
Other Info 2038834951, which evaluates to: 2034-08-10 10:02:31.	

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

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

Info	1650485437, which evaluates to: 2022-04-20 15:10:37.
URL	http://localhost:3000/juice-shop/build/routes/vendor.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 14:35:49.
URL	http://localhost:3000/juice-shop/build/routes/vendor.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
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 14:35:49.
	1981395349, which evaluates to: 2032-10-14 14:35:49. http://localhost:3000/juice-shop/node 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 10:02:31.
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 10:02:31. 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 10:02:31. 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 10:02:31. 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 10:02:31. 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 10:02:31. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9 GET 1650485437 1650485437, which evaluates to: 2022-04-20 15:10:37.
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 10:02:31. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9 GET 1650485437 1650485437, which evaluates to: 2022-04-20 15:10:37. 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 10:02:31. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9 GET 1650485437 1650485437, which evaluates to: 2022-04-20 15:10:37. 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 10:02:31. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9 GET 1650485437 1650485437, which evaluates to: 2022-04-20 15:10:37. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9 GET
Info URL Method Attack Evidence Other Info URL	http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:280:10 GET 2038834951 2038834951, which evaluates to: 2034-08-10 10:02:31. http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:286:9 GET 1650485437 1650485437, which evaluates to: 2022-04-20 15:10:37. http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:286:9 GET 1981395349
Info URL Method Attack Evidence Other Info	http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:280:10 GET 2038834951 2038834951, which evaluates to: 2034-08-10 10:02:31. http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:286:9 GET 1650485437 1650485437, which evaluates to: 2022-04-20 15:10:37. http://localhost:3000/juice-shop/node modules/express/lib/router/index.js:286:9 GET 1981395349 1981395349, which evaluates to: 2032-10-14 14:35:49.
Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index_js:280:10 GET 2038834951 2038834951, which evaluates to: 2034-08-10 10:02:31. http://localhost:3000/juice-shop/node_modules/express/lib/router/index_js:286:9 GET 1650485437 1650485437, which evaluates to: 2022-04-20 15:10:37. http://localhost:3000/juice-shop/node_modules/express/lib/router/index_js:286:9 GET 1981395349 1981395349, which evaluates to: 2032-10-14 14:35:49. http://localhost:3000/juice-shop/node_modules/express/lib/router/index_js:286:9

Other Info	2038834951, which evaluates to: 2034-08-10 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.

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

Evidence	1650485437
Other	1650485437, which evaluates to: 2022-04-20 15:10:37.
Info	
URL Mathad	http://localhost:3000/juice-shop/node_modules/express/lib/router/runtime.js
Method Attack	GET
Evidence	1981395349
Other	
Info	1981395349, which evaluates to: 2032-10-14 14:35:49.
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 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
URL	http://localhost:3000/juice-shop/node modules/serve-index/assets/public/favicon js.ico
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 14:35:49.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/favicon_js.ico
Method	GET
	GET
Method	GET 2038834951

Info	2038834951, which evaluates to: 2034-08-10 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/runtime.js

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

Other	4650495427 which evaluates to 2002 04 00 45.40.07
Info	1650485437, which evaluates to: 2022-04-20 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
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 15:10:37.
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 14:35:49.

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 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
URL	http://localhost:3000/main.js
Method	GET
Attack	
Evidence	1734944650
Other Info	1734944650, which evaluates to: 2024-12-23 03:04:10.
URL	http://localhost:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1969196030
Other Info	1969196030, which evaluates to: 2032-05-26 09:53:50.
URL	http://localhost:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1970691216
Other Info	1970691216, which evaluates to: 2032-06-12 17:13:36.
URL	http://localhost:3000/rest/products/search?q=
Method	GET

Attack	
Evidence	1969196030
Other Info	1969196030, which evaluates to: 2032-05-26 09:53:50.
URL	http://localhost:3000/rest/products/search?q=
Method	GET
Attack	
Evidence	1970691216
Other Info	1970691216, which evaluates to: 2032-06-12 17:13:36.
URL	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 15:10:37.
URL	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 14:35:49.
URL	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 10:02:31.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 15:10:37.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1680327869
Other Info	1680327869, which evaluates to: 2023-04-01 00:44:29.
URL	http://localhost:3000/styles.css
Method	GET
Attack	

Evidence	1701244813
Other	1701244813, which evaluates to: 2023-11-29 02:00:13.
Info	
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	18181818
Other Info	18181818, which evaluates to: 2027-08-13 13:30:18.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1839622642
Other Info	1839622642, which evaluates to: 2028-04-17 17:17:22.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1863874346
Other Info	1863874346, which evaluates to: 2029-01-23 08:52:26.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1917098446
Other Info	1917098446, which evaluates to: 2030-10-01 10:20:46.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 14:35:49.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	2033195021
Other Info	2033195021, which evaluates to: 2034-06-06 03:23:41.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	2038834951
Other	

1	0000004054 which confusion to 0004 00 40 40 0004
Info	2038834951, which evaluates to: 2034-08-10 10:02:31.
Instances	168
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=PXINg0y
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=PXINgog&sid=2I5bMp82Z9dUQqfVAAAC
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=PXINhTs&sid=2I5bMp82Z9dUQqfVAAAC
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=PXINhYn&sid=2I5bMp82Z9dUQqfVAAAC
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=PXINjG-
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=PXINjtH&sid=-mIVhTFFp9RS7Ff4AAAE
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=PXINkJJ&sid=-mIVhTFFp9RS7Ff4AAAE
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=PXINrAU
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=PXINrfx
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=PXINrx1&sid=7K5VpH6acNpSwKXeAAAG
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=PXINsac&sid=Zi_Slhms1STDM57iAAAH
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=PXINsmJ&sid=7K5VpH6acNpSwKXeAAAG
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=PXINteT&sid=Zi_Slhms1STDM57iAAAH
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=PXINtMP&sid=7K5VpH6acNpSwKXeAAAG
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=PXINtOO&sid=Zi_Slhms1STDM57iAAAH
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=PXINvy4
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=PXINw-b&sid=fX51XeedI4pt4YQJAAAK
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=PXINwep&sid=fX51XeedI4pt4YQJAAAK
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=PXINwG5&sid=fX51XeedI4pt4YQJAAAK
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=PXINxRe
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=PXINy3z&sid=Kwa8OeOh2pxuMSaVAAAM
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=PXINyTN&sid=Kwa8OeOh2pxuMSaVAAAM
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=PXIO-IP&sid=UeL35-cfUjXzywO9AAAw
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=PXIO-YT&sid=UeL35-cfUjXzywO9AAAw
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=PXIO0b-
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=PXIO2-k&sid=bdeyXpKNMNcBpQAbAAAO
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=PXIO2Dq&sid=bdeyXpKNMNcBpQAbAAAO
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=PXIO3Hw&sid=bdeyXpKNMNcBpQAbAAAO
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=PXIO4R8
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=PXIO5Az&sid=kA4CWjF19xGageFyAAAQ
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=PXIO5cR&sid=kA4CWjF19xGageFyAAAQ
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=PXIO5s9&sid=kA4CWjF19xGageFyAAAQ
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=PXIO_5g&sid=UeL35-cfUjXzywO9AAAw
Method	GET
Attack	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	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=PXIOAjk
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=PXIObB3&sid=r0Gyydx5_nXCEI3-AAAi
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=PXIObll&sid=r0Gyydx5_nXCEI3-AAAi
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=PXIObWa&sid=r0Gyydx5_nXCEI3-AAAi
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=PXIOBZd&sid=06f47PLdT2QjJRdRAAAS
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=PXIOCGk&sid=06f47PLdT2QjJRdRAAAS
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=PXIODjg
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=PXIOEiH&sid=-rRTtWVV6yEWZkqNAAAU
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=PXIOFYU&sid=-rRTtWVV6yEWZkqNAAAU
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=PXIOhd1
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=PXIOhla&sid=YsqTY6ctxcuAcjvwAAAk
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=PXIOhPj

Attack Evidence 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 alort on client or server error responses. URL http://localhost/3000/socket.io/? ElO-48/transport-polling&t=PXIOIEA&sid=YsqTY&ctxcuAcjvwAAAk Method GET 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/1000/socket.io/? ElO-48/transport-polling&t=PXIOIQ2&aidsYsqTY&ctxcuAcjvwAAAk Method GET 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/? ElO-48/transport-polling&t=PXIOIQ &sid=OBngYOnC9ZPURbtcAAAl GET Attack Evidence Other Info Other Info Other Info Other Info 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/? ElO-48/transport-polling&t=PXIOIy0&sid=OBngYOnC9ZPURbtcAAAl GET Attack Evidence 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 t	Method	GET
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://localabots.1000/socket.io/? EIO=4&transport=polling&t=PXIOIEA&sid=YsqTYSctxcuAcjowAAAk Method GET Attack Evidence 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://localabots.1000/socket.io/? EIO=4&transport=polling&t=PXIOiQ2&sid=YsqTYSctxcuAcjowAAAk Method GET Attack Evidence 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://localabots.1000/socket.io/? EIO=4&transport=polling&t=PXIOiq. &sid=OBngYOnC9ZPURbicAAAI GET Attack Evidence 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://localabots.1000/socket.io/? EIO=4&transport=polling&t=PXIOivOs&sid=OBngYOnC9ZPURbicAAAI GET Attack Evidence 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 are often still affected by injection issues, in which case there is still concer	Attack	
Other Info 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://localhosts.3000/socket.io/? EID=8kItansport=polling&EPXIOIEA&sid=YsqTY6clxcuAcjvwAAAk Method GET Attack Evidence 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://localhosts.3000/socket.io/? EIO=4&transport=polling&EPXIOIQ2&sid=YsqTY6ctxcuAcjvwAAAk Method GET Attack Evidence 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://localhosts.3000/socket.io/? EIO=4&transport=polling&EPXIOIq_&sid=0BngYOnC9ZPURbtcAAAl Method GET Attack Evidence Other 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://localhosts.3000/socket.io/? EIO=4&transport=polling&EPXIOIvo&sid=0BngYOnC9ZPURbtcAAAl GET 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=	Evidence	
Method Attack Evidence 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/? ElO-4&transport=polling&t=PXIOiQ2&sid=YsqTY6ctxcuAcjvwAAAk Method GET Attack Evidence 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/? ElO-4&transport=polling&t=PXIOiq &sid=0BngYOnC9ZPURbtcAAAl GET Attack Evidence 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/? ElO-4&transport=polling&t=PXIOivo&sid=0BngYOnC9ZPURbtcAAAl Method GET Attack Evidence 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/? ElO-4&transport=polling&t=PXIOivo&sid=0BngYOnC9ZPURbtcAAAl Method GET 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		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
Attack Evidence 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://localhosts300/scoket.io/? ElO=48transport=poiling&t=PXIOIQ2&sid=YsgTV6ctxcuAcjvwAAAk Method GET 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://localhost3000/socket.io/? ElO=48transport=poiling&t=PXIOiq_&sid=0BngYOnC9ZPURbtcAAAl Method GET Attack Evidence 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://localhost3000/socket.io/? ElO=48transport=poiling&t=PXIOIvo&sid=0BngYOnC9ZPURbtcAAAl Method GET Attack Evidence 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://localhost3000/socket.io/? ElO=48transport=poiling&t=PXIOIvo&sid=0BngYOnC9ZPURbtcAAAl Method GET 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	URL	
Other Info	Method	GET
Other Info Other Info Other Info Other Info Other Info Info Other Info Info Other Info Info Info Info Info Info Info Info	Attack	
Other Info 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=PXIOIQ2&sid=YsqTY6ctxcuAcjvwAAAk Method GET Attack Evidence 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=PXIOiq. &sid=0BngYOnC9ZPURbtcAAAl Method GET Attack Evidence 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=PXIOiVo&sid=0BngYOnC9ZPURbtcAAAl Method GET Attack Evidence 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 are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often server error responses. URL http://localhost.3000/socket.io/?EIO=4&transport=polling&t=PXIOIVX Method GET Attack Evidence 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 are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection	Evidence	
Method GET Attack Evidence 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://localhosti.3000/socket.io/? EIO=4&transport=polling&t=PXIOiq_&sid=0BngYOnC9ZPURbtcAAAI Method GET Attack Evidence 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://localhosti.3000/socket.io/? EIO=4&transport=polling&t=PXIOiVo&sid=0BngYOnC9ZPURbtcAAAI Method GET Attack Evidence 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://localhosti.3000/socket.io/?EIO=4&transport=polling&t=PXIOIWX Method GET Attack Evidence 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 are greated three is the still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is 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
Attack Evidence 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=48transport=polling&t=PXIOiq_&sid=0BngYOnC9ZPURbtcAAAI Method GET Attack Evidence 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=48transport=polling&t=PXIOiVo&sid=0BngYOnC9ZPURbtcAAAI Method GET Attack Evidence 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=48transport=polling&t=PXIOiwX Method GET Attack Evidence 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 affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case	URL	
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=PXIOiq &sid=0BngYOnC9ZPURbtcAAAI Method GET Attack Evidence 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=PXIOiVo&sid=0BngYOnC9ZPURbtcAAAI Method GET Attack Evidence 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=PXIOIWX Method GET Attack Evidence 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 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 affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages	Method	GET
Other Info	Attack	
Other Info 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=PXIOiq &sid=0BngYOnC9ZPURbtcAAAI Method GET Attack Evidence 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=PXIOIVo&sid=0BngYOnC9ZPURbtcAAAI Method GET Attack Evidence 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=PXIOIwX Method GET Attack Evidence 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 in the page of the page of the 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 affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues	Evidence	
Method GET Attack Evidence 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=PXIOiVo&sid=0BngYOnC9ZPURbtcAAAI Method GET Attack Evidence 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=PXIOIwX Method GET Attack Evidence 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 are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages.		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
Attack Evidence 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=PXIOiVo&sid=0BngYOnC9ZPURbtcAAAI Method GET Attack Evidence 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=PXIOIwX Method GET Attack Evidence 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 are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still conce	URL	
Evidence 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=PXIOiVo&sid=0BngYOnC9ZPURbtcAAAI Method GET Attack Evidence 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=PXIOlwX Method GET Attack Evidence 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 is supported by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages is supported by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers and the page of the page of t	Method	GET
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=PXIOiVo&sid=0BngYOnC9ZPURbtcAAAI Method GET Attack Evidence 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=PXIOIwX Method GET Attack Evidence 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 affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are of	Attack	
Other Info 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=PXIOiVo&sid=0BngYOnC9ZPURbtcAAAI Method GET Attack Evidence 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=PXIOIwX Method GET Attack Evidence 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 are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often the pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often the page are often there is still concern for browsers sniffing pages are often there is still concern for browsers sniffing pages are often there is still concern for browsers sniffing pages are often there is still concern for browsers sniffing pages are often the page are often the pa	Evidence	
Method GET Attack Evidence 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=PXIOIwX Method GET Attack Evidence 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 affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers are often still affected by injection issues, in which case there is still concern for browsers are often still affected by injection issues, in which case there is still concern for browsers are often still aff		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
Attack Evidence 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=PXIOIwX Method GET Attack Evidence 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 are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still affected by injection issues, in which case there is still affected by injection issues, in which case there is still affected by injection issues, in which case there is still affected by injection issues, in which case there i	URL	
Evidence 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=PXIOIwX Method GET Attack Evidence 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 are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers and the page of the still affected by injection issues, in which case there is still concern for browsers and the page of the still affected by injection issues, in which case there is still concern for browsers and the page of the still affected by injection issues, in which case there is still concern for browsers and the page of the still affected by injection issues, in which case there is still concern for browsers and the page of the still affected by injection issues, in which case there is still affected by injection issues, in which case there is still affected by injection issues.	Method	GET
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 affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers and pages are often still affected by injection issues, in which case there is still concern for browsers and pages are often still affected by injection issues, in which case there is still concern for browsers and pages are often still affected by injection issues, in which case there is still concern for browsers and pages are often still affected by injection issues.	Attack	
Other Info Info Info Info Info Info Info Info	Evidence	
Method Attack Evidence 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 are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages.		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
Attack Evidence 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 are often still affected by injection issues, in which case there is still concern for browsers sniffing pages.	URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIOIwX
Other 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 are often still concern for browsers sniffing pages.	Method	GET
Other 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 are often still concern for browsers sniffing pages.	Attack	
Other affected by injection issues, in which case there is still concern for browsers sniffing pages	Evidence	
		affected by injection issues, in which case there is still concern for browsers sniffing pages

	or server error responses.
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOJjH&sid=c8KluezYgHSr0yHGAAAW
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=PXIOK4P&sid=c8KluezYgHSr0yHGAAAW
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=PXIOKHI&sid=c8KluezYgHSr0yHGAAAW
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=PXIOIL5
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=PXIOmDk&sid=a9JjFEvJao43zt6CAAAo
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=PXIOMeb&sid=i6bdX8p1D0EFVnupAAAY
Method	GET
Attack	
Evidence	

	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still
Other Info	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=PXIOMEq
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=PXIOmlv&sid=a9JjFEvJao43zt6CAAAo
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=PXIOMvp&sid=i6bdX8p1D0EFVnupAAAY
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=PXIONAQ&sid=i6bdX8p1D0EFVnupAAAY
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=PXIOOJa
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=PXIOP4X&sid=ruBBrVn9fE_F1wM-AAAa
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=PXIOpal
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=PXIOPgI
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=PXIOPXD&sid=ruBBrVn9fE_F1wM-AAAa
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=PXIOqE2&sid=JC1ekD_Zh9n659q9AAAq
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=PXIOQFx&sid=k6F6sgkqu7-F3mdHAAAc
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.
	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIOQpI&sid=k6F6sgkqu7-

URL	F3mdHAAAc
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=PXIOqVu&sid=JC1ekD_Zh9n659q9AAAq
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=PXIORuQ
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=PXIOSVw&sid=SdCA5TaV_EE9dy19AAAe
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=PXIOT8H&sid=SdCA5TaV_EE9dy19AAAe
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=PXIOUoX
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
11110	· · · · · · · · · · · · · · · · · · ·

	or server error responses.
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIOVDz&sid=L4knAU540ljVTjTFAAAg
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=PXIOvOC
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=PXIOvU0
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=PXIOw_M&sid=E8bG5H88ZZu6x7DXAAAs
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=PXIOWjT&sid=L4knAU540ljVTjTFAAAg
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=PXIOwKB&sid=drxMb855dSnsb3-0AAAt
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=PXIOwun&sid=drxMb855dSnsb3-0AAAt
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=PXIOxBv&sid=E8bG5H88ZZu6x7DXAAAs
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=PXIOxJF&sid=E8bG5H88ZZu6x7DXAAAs
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=PXIOzbf
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=PXIOZUF
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=PXIP1A2
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=PXIP1np&sid=4tMqpwECVd3QYn6LAAAy
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=PXIP2Eg&sid=4tMqpwECVd3QYn6LAAAy
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=PXIP7UK
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=PXIP7we&sid=B- VwlotrGvt_zZJgAAA0
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=PXIP8mH&sid=B- VwlotrGvt_zZJgAAA0
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=PXIP8R5&sid=B- VwlotrGvt_zZJgAAA0

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=PXIP8vQ&sid=B- VwlotrGvt_zZJgAAA0
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=PXIP9A0
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=PXIP9q0&sid=RSMsBj2nWSvCnbDbAAA2
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=PXIPAM8&sid=RSMsBj2nWSvCnbDbAAA2
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=PXIPAS4&sid=RSMsBj2nWSvCnbDbAAA2
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=PXIPfY3
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=PXIPg89&sid=IOUKVOyvWg9SAcXBAABE
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=PXIPghg&sid=IOUKVOyvWg9SAcXBAABE
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=PXIPgia
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=PXIPh0- &sid=F2Wh9nt7bXo9pSIVAABG
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=PXIPhE0&sid=F2Wh9nt7bXo9pSIVAABG
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=PXIPhhu
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=PXIPhzH&sid=LHJ6ah5Z_SHnhYOIAABI
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=PXIPilj&sid=LHJ6ah5Z_SHnhYOIAABI
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=PXIPIKC
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=PXIPIMS
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=PXIPIta&sid=NWf5_adIRpq6XRiUAAA5
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=PXIPJAU&sid=NWf5_adIRpq6XRiUAAA5
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=PXIPJBH&sid=7DdeBruF0OwBhp67AAA4
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=PXIPjFy
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=PXIPJIx&sid=NWf5_adIRpq6XRiUAAA5
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=PXIPJSH&sid=7DdeBruF0OwBhp67AAA4
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=PXIPjwO&sid=rgfE_I7RPI1LHFbFAABK

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=PXIPk5V&sid=rgfE_I7RPI1LHFbFAABK
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=PXIPI8R
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=PXIPImI&sid=1Lt6h3A3eZVMp7NrAABM
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=PXIPluw
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=PXIPIVs&sid=1Lt6h3A3eZVMp7NrAABM
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.

Method GET 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/? EID=4&transport=polling&t=PXIPmSo&sid=pQdzAuDtIJRC4tKRAABQ GET Attack Evidence Other additional 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=PXIPMQ GET Attack Evidence Other additional 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=PXIPMQ GET Attack Evidence 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=PXIPn1u Method GET Attack Evidence Other 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=PXIPn1u Method GET Attack Evidence Other 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=PXIPn1u Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are oft	URL	http://localhost:3000/socket.io/?
Attack Evidence 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/? EIC=4&transport=polling&t=PXIPmSo&sid=pOdrAuDitJRC4tkRAABQ Method GET Attack Evidence Other 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/?EIQ=4&transport=polling&t=PXIPMQ Method GET Attack Evidence Other 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/?EIQ=4&transport=polling&t=PXIPMQ Other 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/?EIQ=4&transport=polling&t=PXIPhTu Method GET Attack Evidence Other 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/?EIQ=4&transport=polling&t=PXIPhTu Attack Evidence 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/?EIQ=4&transport=polling&t=PXIPnBR&sid=gIGYSoX-WiReebyiLABBQ	Mathad	i i i i i i i i i i i i i i i i i i i
Evidence 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. All "High" threshold this scan rule will not alert on client or server error responses. URL #### Intervisional State (107) ### ElD-4&transport=polling&t=PXIPmSo&sid=pOdzAuDtLIRC4tKRAABO ### GET Attack Evidence Other 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 #################################		GET
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which ease 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://localhosts.3000/socket.io/? EIO=48transport=polling&t=PXIPmSo&sid=pQdzAuDitJRC4tKRAABO Method GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which ease 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://localhosts.3000/socket.io/?EIO=4&transport=polling&t=PXIPMfQ Other Info Ot		
Other Info Info Info Info Info Info Info Info	Evidence	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still
Method GET Attack Evidence 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=PXIPMIQ Other affected by injection issues, in which case there is still concern for browsers sniffing 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=PXIPn1u Method GET Attack Evidence 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=PXIPn1u Attack Evidence 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=PXIPnBR&sid=gtGYScX-WiReBWILAABQ Method GET Attack Evidence 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:/		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
Attack Evidence 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 allert on client or server error responses. URL http://localhost.3000/socket.io/?FIO=4&transport=polling&t=PXIPMtQ GET Attack Evidence 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 allert on client or server error responses. URL http://localhost.3000/socket.io/?EIO=4&transport=polling&t=PXIPn1u Method GET Attack Evidence 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 allert on client or server error responses. URL http://localhost.3000/socket.io/? EIO=4&transport=polling&t=PXIPN X&sid=t3jFQ asoWrztGkqAAA8 GET Attack Evidence 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 allert on client or server error responses. URL http://localhost.3000/socket.io/? EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-WJR9aBWI.AABQ Method GET Attack Evidence 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 allert on client or server err	URL	
Evidence Other Info O	Method	GET
Other Info	Attack	
Other Info 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=PXIPMtQ Method GET Attack Evidence 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=PXIPn1u Method GET Attack Evidence 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=PXIPN X&sid=13jFQ asoWrzfGkqAAA8 Method GET 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence 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 are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are oft	Evidence	
Method GET Attack Evidence 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=PXIPn1u Method GET Attack Evidence 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=PXIPN X&sid=t3jFQ asoWrzfGkqAAA8 Method GET Attack Evidence 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=PXIPnBR&sid=gtGYScX-WJR9sBWLAABQ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still attack Evidence		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
Attack Evidence 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=PXIPn1u Method GET Attack Evidence 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=PXIPN X&sid=t3jFQ asoWrzfGkqAAA8 Method GET Attack Evidence Other 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=PXIPn X&sid=t3jFQ asoWrzfGkqAAA8 URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPnBR&sid=gtGYScX-WJRgeBWLAABQ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still applies to error type pages (401, 403, 500, etc.) as those pages are often still attack Evidence	URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPMtQ
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=PXIPn1u Method GET Attack Evidence Other 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=PXIPn X&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence Other Info away from their actual content 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still evidence	Method	GET
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=PXIPn1u Method GET Attack Evidence 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=PXIPN X&sid=13jEQ asoWrzfGkqAAA8 Method GET Attack Evidence 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence 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.	Attack	
Other Info 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=PXIPn1u Method GET Attack Evidence 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=PXIPN_X&sid=t3jFQ_asoWrzfGkqAAA& Method GET Attack Evidence 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still aftected 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still applies to error type pages (401, 403, 500, etc.) as those pages are often still applies to error type pages (401, 403, 500, etc.) as those pages are often still applies to error type pages (401, 403, 500, etc.) as those pages are often still applies to error type pages (401, 403, 500, etc.) as tho	Evidence	
Method GET Attack Evidence Other Info 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/? ElO=4&transport=polling&t=PXIPN X&sid=t3jFQ asoWrzfGkqAAA8 Method GET Attack Evidence Other Info away from their actual content 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence 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
Attack Evidence 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=PXIPN_X&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still explications.	URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPn1u
Evidence 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=PXIPN X&sid=t3jFQ asoWrzfGkqAAA8 Method GET Attack Evidence 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still	Method	GET
Other Info Info Other Info Other Info 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=PXIPN X&sid=t3jFQ asoWrzfGkqAAA8 Method GET Attack Evidence Other Info 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still	Attack	
Other Info 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=PXIPN_X&sid=t3jFQ_asoWrzfGkqAAA8 Method GET Attack Evidence Other Info 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still this issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still this issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still this issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still this issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still this issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still this issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still this issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still this issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still applies to error type pages (401, 403, 500, etc.)	Evidence	
Method GET Attack Evidence 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence 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
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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still	URL	
Evidence 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still	Method	GET
Other Info Other Info Other Info 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still	Attack	
Other Info 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=PXIPnBR&sid=gtGYScX-WJR9eBWLAABQ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still	Evidence	
Method GET Attack Evidence 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
Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still	URL	
Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still	Method	GET
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still	Attack	
	Evidence	
	Other	

Info	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=PXIPndt&sid=gtGYScX-WJR9eBWLAABQ
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=PXIPnLw&sid=gtGYScX-WJR9eBWLAABQ
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=PXIPNQI&sid=t3jFQ_asoWrzfGkqAAA8
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=PXIPnrh
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=PXIPo25&sid=RHZWQ0DPD1TDDq8oAABS
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=PXIPob2
Method	GET
Attack	

Othe Info	er	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=PXIPoCP&sid=RHZWQ0DPD1TDDq8oAABS
Meth	hod	GET
Atta	ck	
Evid	lence	
Othe Info	ər	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=PXIPolS&sid=4sp63Er9EkvPF6aPAABU
Meth	hod	GET
Atta	ck	
Evid	lence	
Othe Info	er	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=PXIPOXI&sid=t3jFQ_asoWrzfGkqAAA8
Meth	hod	GET
Atta	ck	
Evid	lence	
Othe 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=PXIPoxn&sid=4sp63Er9EkvPF6aPAABU
Meth	hod	GET
Atta	ck	
Evid	lence	
Othe Info	ər	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=PXIPOxq
Meth	hod	GET
Atta	ck	
Evid	lence	
Othe Info	er	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=PXIPPdb&sid=Me_bKGbJk93GH-fYAAA-
Meth	hod	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=PXIPPrc&sid=Me_bKGbJk93GH-fYAAA-
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=PXIPWa5&sid=Ing5-c-rNyDCFS5CAABA
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=PXIPWJD
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=PXIPY3-&sid=Ing5-c-rNyDCFS5CAABA
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=PXIPY5y
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.
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXIPY_f&sid=BVad5NVM2JIZA8g9AABC
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=PXIPYA4&sid=Ing5-c-rNyDCFS5CAABA
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=PXIPYmv&sid=BVad5NVM2JIZA8g9AABC
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=PXIPYQH&sid=BVad5NVM2JIZA8g9AABC
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=PXINgoe&sid=2I5bMp82Z9dUQqfVAAAC
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=PXINjrf&sid=-mIVhTFFp9RS7Ff4AAAE
Method	POST
Attack	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Method	Other Info	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.
Evidence 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/? EIC=4&transport=polling&t=PXINsZs&sid=ZI. Sihms1STDM57iAAAH Method POST Attack Evidence 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/? EIC=4&transport=polling&t=PXINwFT&sid=X51Xsedi4pt4YQJAAAK POST Attack Evidence 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/? EIC=4&transport=polling&t=PXINy3a&sid=KwaBOeOh2pxuMSaVAAAM POST Attack Evidence 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/?EIC=4&transport=polling&t=PXIO-IB&sid=Usl.35-ctUJXzywOgAAAW Method POST Attack Evidence 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 in a fected by injection issues, in which case there is still concern	URL	
Evidence 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://localhos.sia.900/socket.io/? EIO=4&transport=polling&t=PXINsZs&sid=ZL.Shms1STDM57iAAAH POST Attack Evidence 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. Http://localhoss.3000/socket.io/? EIO=3&transport=polling&t=PXINvET&sid=IX51XeedI4pt4YQJAAAK POST Attack Evidence Other Info of server error responses. URL http://localhoss.3000/socket.io/? EIO=4&transport=polling&t=PXINvJaa&sid=Kwa8OeOh2pxuMSaVAAAM Method POST Attack Evidence 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://localhoss.3000/socket.io/? EIO=4&transport=polling&t=PXINy3a&sid=Kwa8OeOh2pxuMSaVAAAM Method Other Info or server error responses. URL http://localhoss.3000/socket.io/?EIO=4&transport=polling&t=PXIO-IB&sid=Usl_35-ctUJX;yyyO9AAAW Method Other Info Attack Evidence 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://localhoss.3000/socket.io/?EIO=4&transport=polling&t=P	Method	POST
Other Info	Attack	
Other Info 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_4Atransport=polling&t=PXINsZs&sid=ZI. Sihms1STDM57iAAAH Method POST Attack Evidence 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_4Atransport=polling&t=PXINwFT&sid=fX51XeedI4pt4YQJAAAK POST Attack Evidence 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_4Atransport=polling&t=PXINy3a&sid=Kwa8OeOh2pxuMSaVAAAM Method POST Attack Evidence 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_4Atransport=polling&t=PXIO_4B&transport=polling&t=PXIO_1B&sid=DXIO_1BASid=DXIO_1BASid=DXIO_1BASid=DXIO_1BASid=DXIO_1	Evidence	
Method POST Attack Evidence 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 allert on client or server error responses. URL http://localhost:3000/socket.io/? ElO=a&transport=polling&t=PXINwFT&sid=fX51XeedI4pt4YQJAAAK Method POST Attack Evidence 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 allert on client or server error responses. Http://localhost:3000/socket.io/? ElO=a&transport=polling&t=PXINy3a&sid=Kwa8QeOh2pxuMSaVAAAM Method POST Attack Evidence 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 allert on client or server error responses. URL http://localhost:3000/socket.io/?ElO=4&transport=polling&t=PXIO-IB&sid=LeL35-ctUJX:zyyvOgAAAW Method POST Attack Evidence 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 are often still affected by injection issues, in which case there is still concern for browsers sniffing 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 allert on client or server error responses. LILL		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
Attack Evidence 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-48transport=polling&t=PXINwFT&sid=IX51XeedI4pt4YQJAAAK Method POST Attack Evidence 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-48transport=polling&t=PXINy3a&sid=Kwa8QeOh2pxuMSaVAAAM Method POST Attack Evidence 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=PXIO-IB&sid=UeL35-ctUjXzywOgAAAW Method POST Attack Evidence 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=PXIO-IB&sid=bdeyXpKNMNcBpQAbAAAO	URL	
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. URL http://localhost.3000/socket.io/? EIO=48transport=polling&t=PXINwFT&sid=fX51XeedI4pt4YQJAAAK Method POST Attack Evidence 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=48transport=polling&t=PXINy.3a&sid=Kwa&QeOh2pxuMSaYAAAM Method POST Attack Evidence 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 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=PXIO-IB&sid=UeL35-ctUbZywOgAAAW Method POST Attack Evidence 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.	Method	POST
Other Info	Attack	
Other Info 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=PXINwFT&sid=fX51Xeedl4pt4YOJAAAK Method POST Attack Evidence 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=PXINy3a&sid=Kwa8OeOh2pxuMSaVAAAM POST Attack Evidence 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=PXIO-IB&sid=Uel.35-ctUiXzywOgAAAW Method POST Attack Evidence 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. Other Info 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.	Evidence	
Method POST Attack Evidence Other Info 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=PXIO-IB&sid=UeL.35-ctUjXzywOgAAAw Method POST Attack Evidence 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=PXINy3a&sid=Kwa8OeOh2pxuMSaVAAAM POST Attack Evidence URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIO-IB&sid=UeL.35-ctUjXzywOgAAAw Method POST Attack Evidence 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 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=PXIO-IB&sid=UeL.35-ctUjXzywOgAAAw Method POST Attack Evidence 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.		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
Attack Evidence 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=PXINy3a&sid=Kwa8QeOh2pxuMSaVAAAM POST Attack Evidence 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=PXIO-IB&sid=UeL35-cfUjXzywOgAAAw POST Attack Evidence 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=PXIO2D2&sid=bdeyXpKNMNcBpQAbAAAO	URL	
Evidence 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=PXINy3a&sid=Kwa8OeOh2pxuMSaVAAAM POST Attack Evidence 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=PXIO-IB&sid=UeL35-cfUjXzywOgAAAW POST Attack Evidence 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 in the page of t	Method	POST
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=PXINy3a&sid=Kwa8OeOh2pxuMSaVAAAM Method POST Attack Evidence 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=PXIO-IB&sid=UeL35-cfUjXzywOgAAAw POST Attack Evidence 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 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=PXIO2D2&sid=bdeyXpKNMNcBpQAbAAAO	Attack	
Other Info Info Info Info Info Info Info Info	Evidence	
Method POST Attack Evidence 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=PXIO-IB&sid=UeL.35-cfUjXzywO9AAAw Method POST Attack Evidence 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=PXIO2D2&sid=bdeyXpKNMNcBpQAbAAAO		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
Attack Evidence 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=PXIO-IB&sid=UeL35-cfUjXzywO9AAAw Method POST Attack Evidence 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=PXIO2D2&sid=bdeyXpKNMNcBpQAbAAAO	URL	
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=PXIO-IB&sid=UeL35-cfUjXzywO9AAAW Method POST Attack Evidence 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=PXIO2D2&sid=bdeyXpKNMNcBpQAbAAAO	Method	POST
Other Info Other Info Other Info Other Info Other Info 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=PXIO-IB&sid=UeL.35-cfUjXzywO9AAAw Method POST Attack Evidence 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=PXIO2D2&sid=bdeyXpKNMNcBpQAbAAAO	Attack	
Other Info 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=PXIO-IB&sid=UeL35-cfUjXzywO9AAAw Method POST Attack Evidence 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=PXIO2D2&sid=bdeyXpKNMNcBpQAbAAAO	Evidence	
Method POST Attack Evidence 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=PXIO2D2&sid=bdeyXpKNMNcBpQAbAAAO		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
Attack Evidence 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=PXIO2D2&sid=bdeyXpKNMNcBpQAbAAAO	URL	
Description of the proof of the	Method	POST
Other Info Other Info Other Info URL 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. http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PXIO2D2&sid=bdeyXpKNMNcBpQAbAAAO	Attack	
Other Info 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=PXIO2D2&sid=bdeyXpKNMNcBpQAbAAAO	Evidence	
EIO=4&transport=polling&t=PXIO2D2&sid=bdeyXpKNMNcBpQAbAAAO		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.
Method POST	URL	
	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=PXIO5At&sid=kA4CWjF19xGageFyAAAQ
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=PXIObAs&sid=r0Gyydx5_nXCEI3-AAAi
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=PXIOBZA&sid=06f47PLdT2QjJRdRAAAS
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=PXIOEhG&sid=-rRTtWVV6yEWZkqNAAAU
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=PXIOhIU&sid=YsqTY6ctxcuAcjvwAAAk
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=PXIOiVN&sid=0BngYOnC9ZPURbtcAAAI
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=PXIOJih&sid=c8KluezYgHSr0yHGAAAW
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=PXIOmD9&sid=a9JjFEvJao43zt6CAAAo
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=PXIOMeM&sid=i6bdX8p1D0EFVnupAAAY
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=PXIOP46&sid=ruBBrVn9fE_F1wM-AAAa
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=PXIOqDD&sid=JC1ekD_Zh9n659q9AAAq
Method	POST
Attack	
Evidence	

Other	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
Info	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=PXIOQFF&sid=k6F6sgkqu7-F3mdHAAAc
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=PXIOSVu&sid=SdCA5TaV_EE9dy19AAAe
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=PXIOVCY&sid=L4knAU540ljVTjTFAAAg
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=PXIOw E&sid=E8bG5H88ZZu6x7DXAAAs
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=PXIOwJC&sid=drxMb855dSnsb3-0AAAt
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=PXIP1nf&sid=4tMqpwECVd3QYn6LAAAy

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=PXIP7wO&sid=B- VwlotrGvt_zZJgAAA0
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=PXIP9px&sid=RSMsBj2nWSvCnbDbAAA2
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=PXIPg7v&sid=IOUKVOyvWg9SAcXBAABE
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=PXIPh0v&sid=F2Wh9nt7bXo9pSIVAABG
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=PXIPhzC&sid=LHJ6ah5Z_SHnhYOIAABI
Method	POST
Attack	
Evidence	
Other	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

Info	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=PXIPItZ&sid=NWf5_adIRpq6XRiUAAA5
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=PXIPJAr&sid=7DdeBruF0OwBhp67AAA4
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=PXIPjw3&sid=rgfE_I7RPI1LHFbFAABK
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=PXIPIVT&sid=1Lt6h3A3eZVMp7NrAABM
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=PXIPmMd&sid=pQdzAuDtIJRC4tKRAABO
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=PXIPnB8&sid=gtGYScX-WJR9eBWLAABQ
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=PXIPNP8&sid=t3jFQ_asoWrzfGkqAAA8
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=PXIPo1v&sid=RHZWQ0DPD1TDDq8oAABS
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=PXIPokU&sid=4sp63Er9EkvPF6aPAABU
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=PXIPPdM&sid=Me_bKGbJk93GH-fYAAA-
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=PXIPWZx&sid=Ing5-c-rNyDCFS5CAABA
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.
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXIPYQE&sid=BVad5NVM2JIZA8g9AABC
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	188
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
Plugin Id	10021

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker.
URL	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	Db
Other Info	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.
URL	http://localhost:3000/main.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//owasp. org' target='_blank'>Open Worldwide Application Security Project (OWASP) and is developed and maintained by voluntee", see evidence field for the suspicious comment /snippet.
URL	http://localhost:3000/tutorial.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//w. soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076& color=%23ff5500&auto_play=true&h", see evidence field for the suspicious comment/snippet.
URL	http://localhost:3000/vendor.js
Method	GET

A tto old	
Attack	
Evidence	Query
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="" td="" the=""></path>
Instances	4
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	<u>10027</u>
Informational	Modern Web Application
iniormational	***
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/assets/public/images/uploads/%E1%93%9A%E1%98%8F%E1%97% A2-</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/favicon.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/ftp/</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td></td><td></td></tr></tbody></table></script></pre>

Attack	
Evidence	ftp
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
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>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><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/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/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/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 modern 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 modern web application.</td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/vendor.js</td></tr></tbody></table></script></pre>

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

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/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>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:286:9</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: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></td><td></td></tr></tbody></table></script></pre>

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>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>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/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></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/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>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>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/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></td><td></td></tr></tbody></table></script></pre>

A., 1	
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/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>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/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/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></td><td></td></tr></tbody></table></script></pre>

URL	http://localhost:3000/sitemap.xml
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>Instances</td><td>52</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></td><td></td></tr></tbody></table></script></pre>

Informational	Retrieved from Cache
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: 869750
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.css
Method	GET
Attack	
Evidence	Age: 869796
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: 269082
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: 269129
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: 2321820
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: 2321866
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	6
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