Web Application Vulnerability Assessment Report on OWASP Juice Shop using OWASP ZAP

(Executive Summary)

This report presents the results of a web application vulnerability assessment performed on the target application hosted at http://localhost:3000 using OWASP ZAP, a leading open-source security scanning tool. The assessment was conducted to identify and analyze potential security flaws that could be exploited by malicious actors.

During the evaluation, multiple vulnerabilities were discovered that align with the OWASP Top 10 Web Application Security Risks, including a critical SQL Injection vulnerability via the q parameter, which triggered backend SQLite errors. This confirmed a lack of proper input validation and a high risk of unauthorized data access or manipulation.

Additional findings included the absence of essential security headers such as Content Security Policy (CSP) and X-Frame-Options, exposing the application to clickjacking and content injection attacks. The application was also observed to expose session IDs in the URL, increasing the risk of session hijacking through shared links or browser history.

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

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

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

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

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

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

Alerts

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

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

Alert Detail

High	**SQL Injection - SQLite**
Description	SQL injection may be possible.
URL	http://localhost:3000/rest/products/search?q=%27%28
Method	GET
Attack	'(
Evidence	SQLITE_ERROR
Other Info	RDBMS [SQLite] likely, given error message regular expression [SQLITE_ERROR] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
Instances	1
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
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/ftp
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/coupons_2013.md.bak
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/eastere.gg
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/encrypt.pyc
Method	GET

Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/package-lock.json.bak
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/package.json.bak
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/quarantine
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp/suspicious_errors.yml
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/runtime.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:43:13
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/main.js
Method	GET
Attack	
Evidence	
Other Info	

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

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

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

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

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
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/sitemap.xml

Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr2iZ&sid=Rw-fonf5fS-soOyqAAAC
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	
Evidence	
Other Info	
Instances	61
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
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://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
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: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/api/Challenges/?name=Score%20Board
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser

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

Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/acquisitions.md
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/announcement_encrypted.md
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/coupons_2013.md.bak
Method	GET

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

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

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

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

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

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

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

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

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

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

Medium	Missing Anti-clickjacking Header

Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr2iZ&sid=Rw-fonf5fS-soOyqAAAC
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	
Evidence	
Other Info	
Instances	3
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Medium	**Session ID in URL Rewrite**
Description	URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site referer header. In addition, the session ID might be stored in browser history or server logs.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr2jl&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	Rw-fonf5fS-soOyqAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr3GH&sid=Rw-fonf5fS-soOyqAAAC

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

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

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	
Evidence	bbnwfd9qOchbbDn-AAAE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	
Evidence	bbnwfd9qOchbbDn-AAAE
Other Info	
Instances	17
Solution	For secure content, put session ID in a cookie. To be even more secure consider using a combination of cookie and URL rewrite.
Reference	https://seclists.org/webappsec/2002/q4/111
CWE Id	598
WASC Id	13
Plugin Id	3

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	1395
WASC Id	
Plugin Id	10003

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	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	
URL	http://localhost:3000
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/
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/
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/assets/public/assets/public/favicon_js.ico
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/assets/public/assets/public/favicon_js.ico
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/assets/public/favicon_js.ico
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/assets/public/favicon_js.ico

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/assets/public/main.js
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/assets/public/main.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/assets/public/polyfills.js
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/assets/public/polyfills.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/assets/public/runtime.js
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/assets/public/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/assets/public/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/assets/public/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/assets/public/vendor.js
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/assets/public/vendor.js
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:43:13
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/fileServer.js:43:13
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/fileServer.js:59:18
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/fileServer.js:59:18
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/main.js
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/main.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/polyfills.js
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/polyfills.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/runtime.js
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/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/vendor.js
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/vendor.js
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
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/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/favicon_js.ico
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/node_modules/express/lib/router/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/main.js
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/node_modules/express/lib/router/assets/public/main.js
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/polyfills.js
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/node_modules/express/lib/router/assets/public/polyfills.js
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/runtime.js
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/node_modules/express/lib/router/assets/public/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/node_modules/express/lib/router/assets/public/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/node_modules/express/lib/router/assets/public/styles.css
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js
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/node_modules/express/lib/router/assets/public/vendor.js
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10
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/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9
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/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
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/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
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/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
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/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>

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

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

Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
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/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/favicon_js.ico
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/node_modules/serve-index/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/main.js
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/node_modules/serve-index/assets/public/main.js
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/polyfills.js
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/node_modules/serve-index/assets/public/polyfills.js
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/runtime.js
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/node_modules/serve-index/assets/public/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/node_modules/serve-index/assets/public/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/node_modules/serve-index/assets/public/styles.css
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/vendor.js
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/node_modules/serve-index/assets/public/vendor.js
Method	GET

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

Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
Instances	98
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

Low	**Private IP Disclosure**
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	http://localhost:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	192.168.99.100:3000
Other Info	192.168.99.100:3000 192.168.99.100:4200
Instances	1
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP /PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Reference	https://tools.ietf.org/html/rfc1918
CWE Id	497
WASC Id	13
Plugin Id	2

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	http://localhost:3000
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Evidence	1701244813
Other Info	1701244813, which evaluates to: 2023-11-29 03:00:13.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1818181818
Other Info	1818181818, which evaluates to: 2027-08-13 14:30:18.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1839622642
Other Info	1839622642, which evaluates to: 2028-04-17 18:17:22.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1863874346
Other Info	1863874346, which evaluates to: 2029-01-23 09:52:26.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1917098446
Other Info	1917098446, which evaluates to: 2030-10-01 11:20:46.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	2033195021
Other Info	2033195021, which evaluates to: 2034-06-06 04:23:41.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	2038834951
Other	

Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
Instances	162
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr1zx
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr2jI&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr3GH&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr424&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

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

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr4DU&sid=Rw-fonf5fS-soOyqAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr7jA
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr8cA&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr9Qp&sid=bbnwfd9qOchbbDn-AAAE
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr2iZ&sid=Rw-fonf5fS-soOyqAAAC
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr9oQ&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	17
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
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)</a> and is developed and maintained by voluntee", see evidence field for the suspicious comment /snippet.
URL	http://localhost:3000/vendor.js
Method	GET
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 d="M0 256C0 397.4 114.6 512 256 512s256-114.6 256-256S397.4 0 256 0S0 114.6 0", see evidence field for the suspicious comment/snippet.
Instances	3
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	[615](615)
WASC Id	13
Plugin Id	[10027](10027)

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	http://localhost:3000
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/ftp/
Method	GET
Attack	
Evidence	<a href="">ftp</a>
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	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>

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

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

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

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

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

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

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

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: 237933
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Method	GET
Attack	
Evidence	Age: 25591
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	Age: 442510
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	3
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	
WASC Id	
Plugin Id	10050

Informational	User Agent Fuzzer
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	http://localhost:3000/assets
Method	GET

Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/assets
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

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

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

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

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

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

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

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

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

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

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

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

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

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

URL	EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PUHr8bI&sid=bbnwfd9qOchbbDn-AAAE
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)

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

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

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