

ZAP_{by} Checkmar× ZAP by Checkmarx Scanning Report

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

Generated on Wed, 15 Oct 2025 16:08:44

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	74
Cross-Domain Misconfiguration	Medium	100
Missing Anti-clickjacking Header	Medium	16
Session ID in URL Rewrite	Medium	71
Vulnerable JS Library	Medium	1
Cross-Domain JavaScript Source File Inclusion	Low	98
Private IP Disclosure	Low	1
<u>Timestamp Disclosure - Unix</u>	Low	162
X-Content-Type-Options Header Missing	Low	71
Information Disclosure - Suspicious Comments	Informational	4
Modern Web Application	Informational	50
Retrieved from Cache	Informational	9
User Agent Fuzzer	Informational	112

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	
IIIIO	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13 GET
URL Method Attack	
URL Method Attack Evidence	
URL Method Attack	
URL Method Attack Evidence Other	
URL Method Attack Evidence Other Info	GET
URL Method Attack Evidence Other Info URL	GET http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
URL Method Attack Evidence Other Info URL Method Attack Evidence	GET http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
URL Method Attack Evidence Other Info URL Method Attack	GET http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
URL Method Attack Evidence Other Info URL Method Attack Evidence Other	GET http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 GET
URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL URL URL Method Attack URL URL URL URL URL URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 GET http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 GET http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Attack Evidence Other Info URL Method Attack	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 GET http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
URL Method Attack Evidence Other Info URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 GET http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
URL Method Attack Evidence Other Info	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 GET http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14 GET
URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack URL URL URL URL URL URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14 GET http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14 GET http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3

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	

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=PdfSbl2&sid=k8EZRNNfT3-tQELHAAAW
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfScwn&sid=TYafPcUf8ifUG5cyAAAY

Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfShK9&sid=GY9M8mCaCjAbyyWZAAAa
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSiL1&sid=O-RgKKEE5zgL2X87AAAc
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSj5x&sid=RikHJG_PnMgkz8hEAAAe
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSnXl&sid=yfgGVPJteWWbJDRpAAAg
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSon5&sid=DxErFLCztc9zPOn8AAAi
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSoxT&sid=oAr-kxL10IHMT7zHAAAj
Method	POST
Attack	
Evidence	
Other Info	

URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSsfM&sid=7SQ4v8wodprjukxkAAAm
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfStI9&sid=c5v6lx_4YAzmKpbIAAAo
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSu6C&sid=LioAEUTo_jxaC4i4AAAq
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSuxI&sid=OPAOmz5AmC732BPmAAAs
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSv6S&sid=MnANeJyZYe5FsmS0AAAt
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSvyS&sid=p-NWnqV_UNwNVvDfAAAw
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwap&sid=Bw9anqxtgpXYGUTzAAAy
Method	POST
Attack	

Evidence	
Other	
Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0
Method	POST
Attack	
Evidence	
Other Info	
Instances	74
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	<u>693</u>
WASC Id	15
Plugin Id	10038
Medium	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
	(o o r o o r o o o o o o o o o o o o o
URL	http://cdnis.cloudflare.com/ajax/libs/cookjeconsent2/3.1.0/cookjeconsent.min.css
URL Method	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css GET
Method	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css GET
Method Attack	GET
Method	
Method Attack Evidence Other	Access-Control-Allow-Origin: * The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but
Method Attack Evidence Other Info	Access-Control-Allow-Origin: * The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Method Attack Evidence Other Info	Access-Control-Allow-Origin: * The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing. http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Method Attack Evidence Other Info URL Method	Access-Control-Allow-Origin: * The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing. http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Method Attack Evidence Other Info URL Method Attack	Access-Control-Allow-Origin: * The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing. http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js GET
Method Attack Evidence Other Info URL Method Attack Evidence	Access-Control-Allow-Origin: * The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing. http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js GET Access-Control-Allow-Origin: * The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but

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

	The CORS misconfiguration on the web server permits cross demain read requests from
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that 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: *
	The 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/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/order_b642-1a5e5bf04f20db68.pdf
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that 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 Central Allow Origin: *
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that 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: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that 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: *
	The 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/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	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from
3.10.	

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

	authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from

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

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

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

LIDI	hum Maralla ask 0000 fining also also also also also also also also
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/tutorial.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/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	100
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet. html5_overly_permissive_cors_policy
CWE Id	<u>264</u>
WASC Id	14
Plugin Id	10098
Medium	Missing Anti-clicking Hooder
	Missing Anti-clickjacking Header The response does not protect against 'ClickJacking' attacks. It should include either
Description	Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbl2&sid=k8EZRNNfT3-tQELHAAAW
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfScwn&sid=TYafPcUf8ifUG5cyAAAY
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfShK9&sid=GY9M8mCaCjAbyyWZAAAa
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSiL1&sid=O-RgKKEE5zgL2X87AAAc
Method	POST
Attack	
Evidence	
Other	

Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSj5x&sid=RikHJG_PnMgkz8hEAAAe
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSnXl&sid=yfgGVPJteWWbJDRpAAAg
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSon5&sid=DxErFLCztc9zPOn8AAAi
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSoxT&sid=oAr-kxL10IHMT7zHAAAj
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSsfM&sid=7SQ4y8wodprjukxkAAAm
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfStl9&sid=c5v6lx_4YAzmKpblAAAo
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSu6C&sid=LioAEUTo_jxaC4i4AAAq
Method	POST
Attack	

Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSuxI&sid=OPAOmz5AmC732BPmAAAs
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSv6S&sid=MnANeJyZYe5FsmS0AAAt
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSvyS&sid=p-NWnqV_UNwNVvDfAAAw
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwap&sid=Bw9anqxtgpXYGUTzAAAy
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0
Method	POST
Attack	
Evidence	
Other Info	
Instances	16
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=PdfSbl3&sid=k8EZRNNfT3-tQELHAAAW
Method	GET
Attack	
Evidence	k8EZRNNfT3-tQELHAAAW
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbpR&sid=k8EZRNNfT3-tQELHAAAW
Method	GET
Attack	
Evidence	k8EZRNNfT3-tQELHAAAW
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfScwq&sid=TYafPcUf8ifUG5cyAAAY
Method	GET
Attack	
Evidence	TYafPcUf8ifUG5cyAAAY
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSd7x&sid=TYafPcUf8ifUG5cyAAAY
Method	GET
Attack	
Evidence	TYafPcUf8ifUG5cyAAAY
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfShKA&sid=GY9M8mCaCjAbyyWZAAAa
Method	GET
Attack	
Evidence	GY9M8mCaCjAbyyWZAAAa
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfShP- &sid=GY9M8mCaCjAbyyWZAAAa
Method	GET
Attack	
Evidence	GY9M8mCaCjAbyyWZAAAa

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSiaN&sid=O-RgKKEE5zgL2X87AAAc
Method	GET
Attack	
Evidence	O-RgKKEE5zgL2X87AAAc
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSiL2&sid=O-RgKKEE5zgL2X87AAAc
Method	GET
Attack	
Evidence	O-RgKKEE5zgL2X87AAAc
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSj61&sid=RikHJG_PnMgkz8hEAAAe
Method	GET
Attack	
Evidence	RikHJG_PnMgkz8hEAAAe
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSjDV&sid=RikHJG_PnMgkz8hEAAAe
Method	GET
Attack	
Evidence	RikHJG_PnMgkz8hEAAAe
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSnxn&sid=yfgGVPJteWWbJDRpAAAg
Method	GET
Attack	
Evidence	yfgGVPJteWWbJDRpAAAg
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSnXo&sid=yfgGVPJteWWbJDRpAAAg
Method	GET
Attack	
Evidence	yfgGVPJteWWbJDRpAAAg
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSonE&sid=DxErFLCztc9zPOn8AAAi
Method	GET

Attack	
Evidence	DxErFLCztc9zPOn8AAAi
Other	DALIT EGZIGGZI GITOAAAI
Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSos0&sid=DxErFLCztc9zPOn8AAAi
Method	GET
Attack	
Evidence	DxErFLCztc9zPOn8AAAi
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSoxd&sid=oAr-kxL10IHMT7zHAAAj
Method	GET
Attack	
Evidence	oAr-kxL10IHMT7zHAAAj
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSp7X&sid=oAr-kxL10IHMT7zHAAAj
Method	GET
Attack	
Evidence	oAr-kxL10IHMT7zHAAAj
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSpBu&sid=DxErFLCztc9zPOn8AAAi
Method	GET
Attack	
Evidence	DxErFLCztc9zPOn8AAAi
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSsfZ&sid=7SQ4y8wodprjukxkAAAm
Method	GET
Attack	
Evidence	7SQ4y8wodprjukxkAAAm
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSsmr&sid=7SQ4y8wodprjukxkAAAm
Method	GET
Attack	
Evidence	7SQ4y8wodprjukxkAAAm
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PdfStIG&sid=c5v6Ix_4YAzmKpbIAAAo
Method	GET
Attack	
Evidence	c5v6lx_4YAzmKpblAAAo
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfStWm&sid=c5v6lx_4YAzmKpbIAAAo
Method	GET
Attack	
Evidence	c5v6lx_4YAzmKpblAAAo
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSu6S&sid=LioAEUTo_jxaC4i4AAAq
Method	GET
Attack	
Evidence	LioAEUTo_jxaC4i4AAAq
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSuOM&sid=LioAEUTo_jxaC4i4AAAq
Method	GET
Attack	
Evidence	LioAEUTo_jxaC4i4AAAq
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSuVF&sid=LioAEUTo_jxaC4i4AAAq
Method	GET
Attack	
Evidence	LioAEUTo_jxaC4i4AAAq
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSuxK&sid=OPAOmz5AmC732BPmAAAs
Method	GET
Attack	
Evidence	OPAOmz5AmC732BPmAAAs
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSv6T&sid=MnANeJyZYe5FsmS0AAAt
Method	GET
Attack	
Evidence	MnANeJyZYe5FsmS0AAAt

URL http://localhost-3000/socket.io/? EIO=48transport=poling&l=PdfSvae&sid=OPAOmz5AmC732BPmAAAs Method GET Attack Evidence OPAOmz5AmC732BPmAAAs Other Info URL http://localhost-3000/socket.io/? EIO=48transport=poling&l=PdfSvOv&sid=OPAOmz5AmC732BPmAAAs Method GET Attack Evidence OPAOmz5AmC732BPmAAAs Other Info URL http://localhost-3000/socket.io/? EiO=48transport=poling&l=PdfSvOv&sid=OPAOmz5AmC732BPmAAAs Other Info URL http://localhost-3000/socket.io/? EiO=48transport=poling&l=PdfSvYi&sid=MnANe_JyZYe5FsmS0AAAt Method GET Attack Evidence MnANe_JyZYe5FsmS0AAAt Other Info URL http://localhost-3000/socket.io/?EIO=48transport=polling&l=PdfSvyU&sid=p-NVmqV_UNwNVvDfAAAw Other Info URL http://localhost-3000/socket.io/?EIO=48transport=polling&l=PdfSw6_&sid=p-NVmqV_UNwNVvDfAAAw Other Info URL http://localhost-3000/socket.io/?EIO=48transport=polling&l=PdfSw6_&sid=p-NVmqV_UNwNVvDfAAAw Other Info URL http://localhost-3000/socket.io/?EIO=48transport=polling&l=PdfSw6_&sid=p-NVmqV_UNwNVvDfAAAw Other Info URL http://localhost-3000/socket.io/? EIO=48transport=polling&l=PdfSwb3&sid=Bw9anoxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost-3000/socket.io/? EIO=48transport=polling&l=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost-3000/socket.io/? EIO=48transport=polling&l=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy Method GET	Other Info	
Attack Evidence OPAOmz5AmC732BPmAAAs Other Info URL http://localhost:3000/socket.io/? EIC=#&transport=polling&t=PdfSvOv&sid=OPAOmz5AmC732BPmAAAs Method GET Attack Evidence OPAOmz5AmC732BPmAAAs Other Info URL http://localhost:3000/socket.io/? EIC=#&transport=polling&t=PdfSvYi&sid=MnANe.lyZYe5FsmS0AAAt Method GET Attack Evidence MnANe.lyZYe5FsmS0AAAt Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSvyU&sid=p- MVnqV_UNwNVvDfAAAw Method GET Attack Evidence P-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSvyU&sid=p- MVnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6_&sid=p- MVnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6_&sid=p- MVnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6_&sid=p- MVnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info	URL	
Evidence OPAOmz5AmC732BPmAAAs Other Info URL http://localhost:3000/socket.io/? EIO=48transport=polling&t=PdfSvOv&sid=OPAOmz5AmC732BPmAAAs Method GET Attack Evidence OPAOmz5AmC732BPmAAAs Other Info URL http://localhost:3000/socket.io/? EIO=48transport=polling&t=PdfSvYi&sid=MnANeJyZYe5FsmS0AAAt Method GET Attack Evidence MnANeJyZYe5FsmS0AAat Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSvyU&sid=p-NVmqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6.&sid=p-NVmqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6.&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6.&sid=Bw9anqxtgpXYGUTzAAAy Other Info	Method	GET
Other Info URL http://localhost.3000/socket.io/? EIG=8&transport=polling&t=PdfSvOv&sid=OPAOmz5AmC732BPmAAAs Method GET Attack Evidence OPAOmz5AmC732BPmAAAs Other Info URL http://localhost.3000/socket.io/? EIG=8&transport=polling&t=PdfSvYi&sid=MnANeJyZYe5EsmS0AAAt Method GET Attack Evidence MnANeJyZYe5FsmS0AAAt Other Info URL http://localhost.3000/socket.io/?EIG=4&transport=polling&t=PdfSvyU&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost.3000/socket.io/?EIG=4&transport=polling&t=PdfSw6.&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost.3000/socket.io/?EIG=4&transport=polling&t=PdfSw6.&sid=p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost.3000/socket.io/?EIG=4&transport=polling&t=PdfSw6.&sid=p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost.3000/socket.io/? EIG=4&transport=polling&t=PdfSw5.&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost.3000/socket.io/? EIG=4&transport=polling&t=PdfSw5.Q&sid=Bw9anqxtgpXYGUTzAAAy Other Info	Attack	
URL http://localhost:3000/socket.io/? EIO-48transport=polling&t=PdfSvOv&sid=OPAOmz5AmC732BPmAAAs Method GET Attack Evidence OPAOmz5AmC732BPmAAAs Other Info URL http://localhost:3000/socket.io/? EIO-48transport=polling&t=PdfSvYi&sid=MnANeJyZYe5FsmS0AAAt Method GET Attack Evidence MnANeJyZYe5FsmS0AAAt Other Info URL http://localhost:3000/socket.io/?EIO-4&transport=polling&t=PdfSvyU&sid=p-NWnqV_UNwNIvvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO-4&transport=polling&t=PdfSw6-&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO-4&transport=polling&t=PdfSw6-&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO-4&transport=polling&t=PdfSw5-&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy	Evidence	OPAOmz5AmC732BPmAAAs
Method GET Attack Evidence OPAOmz5AmC732BPmAAAs Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PdfSvVji&sid=MnANeJyZYe5FsmS0AAt Method GET Attack Evidence MnANeJyZYe5FsmS0AAt Method GET Attack Evidence MnANeJyZYe5FsmS0AAAt Other Info URL http://localhost:3000/socket.io/?EiO=4&transport=polling&t=PdfSvyU&sid=p-NV/nqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNvVDfAAAw Other Info URL http://localhost:3000/socket.io/?EiO=4&transport=polling&t=PdfSw6_&sid=p-NV/nqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EiO=4&transport=polling&t=PdfSw6_&sid=p-NV/nqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy		
Attack Evidence OPAOmz5AmC732BPmAAAs Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSvYi&sid=MnANe_JyZYe5FsmS0AAAt Method GET Attack Evidence MnANeJyZYe5FsmS0AAAt Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSvyU&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6-&sid=p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6-&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNvvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Dither Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy	URL	
Evidence Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSvYi&sid=MnANe_JyZYe5FsmS0AAAt Method GET Attack Evidence MnANeJyZYe5FsmS0AAAt Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSvyU&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6-&sid=p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6-&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Drher Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy Drher Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy	Method	GET
Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=Pdf\$vYi&sid=MnANeJyZYe5Fsm\$0AAAt Method GET Attack Evidence MnANeJyZYe5Fsm\$0AAAt Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=Pdf\$vyU&sid=p-NV/nqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=Pdf\$wyU&sid=p-NV/nqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=Pdf\$w6 &sid=p-NV/nqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=Pdf\$wb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=Pdf\$wsQ&sid=Bw9anqxtgpXYGUTzAAAy	Attack	
Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSvYi&sid=MnANeJyZYe5FsmS0AAAt Method GET Attack Evidence MnANeJyZYe5FsmS0AAAt Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSvyU&sid=p-NVmqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6-&sid=p-NVmqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy	Evidence	OPAOmz5AmC732BPmAAAs
Method GET Attack Evidence MnANeJyZYe5FsmS0AAAt Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSvyU&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSvyU&sid=p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6_&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy		
Attack Evidence MnANeJyZYe5FsmS0AAAt Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSvyU&sid=p-NW/nqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6 &sid=p-NW/nqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6 &sid=p-NW/nqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy	URL	
Evidence MnANeJyZYe5FsmS0AAAt Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSvyU&sid=p-NV/nqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6_&sid=p-NV/nqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6_&sid=p-NV/nqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy	Method	GET
Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSvyU&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6_&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy	Attack	
Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSvyU&sid=p-NW/nqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6_&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSw6_&sid=p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy	Evidence	MnANeJyZYe5FsmS0AAAt
Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6_&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EVIDENCE p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy. Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EVIDENCE Bw9anqxtgpXYGUTzAAAy		
Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6_&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy	URL	
Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost;3000/socket.io/?EIO=4&transport=polling&t=PdfSw6 &sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost;3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost;3000/socket.io/? EiO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy	Method	GET
Other Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6_&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EiO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy	Attack	
Info URL http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSw6_&sid=p-NWnqV_UNwNVvDfAAAw Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? ElO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy	Evidence	p-NWnqV_UNwNVvDfAAAw
Method GET Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy		
Attack Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy	URL	
Evidence p-NWnqV_UNwNVvDfAAAw Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy	Method	GET
Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy	Attack	
Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy	Evidence	p-NWnqV_UNwNVvDfAAAw
Method GET Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy		
Attack Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy	URL	
Evidence Bw9anqxtgpXYGUTzAAAy Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy	Method	GET
Other Info URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy	Attack	
URL http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy	Evidence	Bw9anqxtgpXYGUTzAAAy
EIO=4&transport=polling&t=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy		
Method GET	URL	
	Method	GET

Attack	
Evidence	Bw9anqxtgpXYGUTzAAAy
Other Info	DwodingxigpX10012/wwy
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSwTS&sid=p-NWngV_UNwNVvDfAAAw
Method	GET
Attack	
Evidence	p-NWnqV_UNwNVvDfAAAw
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSxbl&sid=Bw9anqxtgpXYGUTzAAAy
Method	GET
Attack	
Evidence	Bw9anqxtgpXYGUTzAAAy
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSxct&sid=Bw9anqxtgpXYGUTzAAAy
Method	GET
Attack	
Evidence	Bw9anqxtgpXYGUTzAAAy
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSxwW&sid=MJRB9uC6lgB6g_JaAAA0
Method	GET
Attack	
Evidence	MJRB9uC6lgB6g_JaAAA0
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSxXk&sid=MJRB9uC6lgB6g_JaAAA0
Method	GET
Attack	
Evidence	MJRB9uC6lgB6g_JaAAA0
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSxY5&sid=Bw9anqxtgpXYGUTzAAAy
Method	GET
Attack	
Evidence	Bw9anqxtgpXYGUTzAAAy
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=7SQ4y8wodprjukxkAAAm

Method	GET
Attack	
Evidence	7SQ4y8wodprjukxkAAAm
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=Bw9anqxtgpXYGUTzAAAy
Method	GET
Attack	
Evidence	Bw9anqxtgpXYGUTzAAAy
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=c5v6lx_4YAzmKpblAAAo
Method	GET
Attack	
Evidence	c5v6lx_4YAzmKpblAAAo
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=DxErFLCztc9zPOn8AAAi
Method	GET
Attack	
Evidence	DxErFLCztc9zPOn8AAAi
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=GY9M8mCaCjAbyyWZAAAa
Method	GET
Attack	
Evidence	GY9M8mCaCjAbyyWZAAAa
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=k8EZRNNfT3-tQELHAAAW
Method	GET
Attack	
Evidence	k8EZRNNfT3-tQELHAAAW
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=LioAEUTo_jxaC4i4AAAq
Method	GET
Attack	
Evidence	LioAEUTo_jxaC4i4AAAq
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=websocket&sid=MJRB9uC6lgB6g_JaAAA0
Method	GET
Attack	
Evidence	MJRB9uC6lgB6g_JaAAA0
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=MnANeJyZYe5FsmS0AAAt
Method	GET
Attack	
Evidence	MnANeJyZYe5FsmS0AAAt
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=O- RgKKEE5zgL2X87AAAc
Method	GET
Attack	
Evidence	O-RgKKEE5zgL2X87AAAc
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=oAr-kxL10IHMT7zHAAAj
Method	GET
Attack	
Evidence	oAr-kxL10IHMT7zHAAAj
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=OPAOmz5AmC732BPmAAAs
Method	GET
Attack	
Evidence	OPAOmz5AmC732BPmAAAs
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=p- NWnqV_UNwNVvDfAAAw
Method	GET
Attack	
Evidence	p-NWnqV_UNwNVvDfAAAw
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=RikHJG_PnMgkz8hEAAAe
Method	GET
Attack	
Evidence	RikHJG_PnMgkz8hEAAAe
Other	

Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=TYafPcUf8ifUG5cyAAAY
Method	GET
Attack	
Evidence	TYafPcUf8ifUG5cyAAAY
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=websocket&sid=yfgGVPJteWWbJDRpAAAg
Method	GET
Attack	
Evidence	yfgGVPJteWWbJDRpAAAg
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbl2&sid=k8EZRNNfT3-tQELHAAAW
Method	POST
Attack	
Evidence	k8EZRNNfT3-tQELHAAAW
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfScwn&sid=TYafPcUf8ifUG5cyAAAY
Method	POST
Attack	
Evidence	TYafPcUf8ifUG5cyAAAY
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfShK9&sid=GY9M8mCaCjAbyyWZAAAa
Method	POST
Attack	
Evidence	GY9M8mCaCjAbyyWZAAAa
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSiL1&sid=O-RgKKEE5zgL2X87AAAc
Method	POST
Attack	
Evidence	O-RgKKEE5zgL2X87AAAc
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSj5x&sid=RikHJG_PnMgkz8hEAAAe
Method	POST
Attack	

Evidence	RikHJG_PnMgkz8hEAAAe
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSnXl&sid=yfgGVPJteWWbJDRpAAAg
Method	POST
Attack	
Evidence	yfgGVPJteWWbJDRpAAAg
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSon5&sid=DxErFLCztc9zPOn8AAAi
Method	POST
Attack	
Evidence	DxErFLCztc9zPOn8AAAi
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSoxT&sid=oAr-kxL10IHMT7zHAAAj
Method	POST
Attack	
Evidence	oAr-kxL10IHMT7zHAAAj
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSsfM&sid=7SQ4y8wodprjukxkAAAm
Method	POST
Attack	
Evidence	7SQ4y8wodprjukxkAAAm
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfStl9&sid=c5v6lx_4YAzmKpbIAAAo
Method	POST
Attack	
Evidence	c5v6lx_4YAzmKpbIAAAo
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSu6C&sid=LioAEUTo_jxaC4i4AAAq
Method	POST
Attack	
Evidence	LioAEUTo_jxaC4i4AAAq
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSuxI&sid=OPAOmz5AmC732BPmAAAs

Method	POST
Attack	
Evidence	OPAOmz5AmC732BPmAAAs
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSv6S&sid=MnANeJyZYe5FsmS0AAAt
Method	POST
Attack	
Evidence	MnANeJyZYe5FsmS0AAAt
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSvyS&sid=p- NWnqV_UNwNVvDfAAAw
Method	POST
Attack	
Evidence	p-NWnqV_UNwNVvDfAAAw
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSwap&sid=Bw9anqxtgpXYGUTzAAAy
Method	POST
Attack	
Evidence	Bw9anqxtgpXYGUTzAAAy
Other Info	
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0
Method	POST
Attack	
Evidence	MJRB9uC6lgB6g_JaAAA0
Other Info	
Instances	71
Solution	For secure content, put session ID in a cookie. To be even more secure consider using a combination of cookie and URL rewrite.
Reference	https://seclists.org/webappsec/2002/q4/111
CWE Id	<u>598</u>
WASC Id	13
Plugin Id	3
Medium	Vulnerable JS Library
Description	The identified library appears to be vulnerable.
URL	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	

Evidence	/2.2.4/jquery.min.js
Other Info	The identified library jquery, version 2.2.4 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 https://github.com/jquery/jquery/issues/2432 http://blog. jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org /jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov /vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit /753d591aea698e57d6db58c9f722cd0808619b1b https://github.com/jquery/jquery.com /issues/162 https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
Instances	1
Solution	Upgrade to the latest version of the affected library.
Reference	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
CWE Id	<u>1395</u>
WASC Id	
Plugin Id	<u>10003</u>
Low	Cross-Domain JavaScript Source File Inclusion
Description	The page includes one or more script files from a third-party domain.
URL	http://localhost:3000
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	

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

Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other	,
Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/runtime.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/runtime.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/styles.css
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/styles.css</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/vendor.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/assets/public/vendor.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:43:13
Method	GET

Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/fileServer.js:43:13</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/fileServer.js:59:18</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/main.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/main.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/polyfills.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/build/routes/polyfills.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td></td><td></td></tr></tbody></table></script></pre>

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

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

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

URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td></td><td></td></tr></tbody></table></script></pre>

URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	

Method GET Attack Evidence	URL	http://localheat/2000/jujec.ahap/pada_madulas/ovpress/lib/router/main.is
Attack Evidence //scripts rc=*//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js*> //scripts Other Info URL http://localhost.3000/juice-shop/node_modules/express/lib/router/main.js //scripts Attack Evidence Secript src=*//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js*> //scripts Wethod GET Attack Evidence Secript src=*//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js*> //scripts Wethod GET Attack Evidence Secript src=*//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js*> //scripts URL http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js Method GET Attack Evidence Secript src=*//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js*> //scripts URL http://localhost:3000/juice-shop/node_modules/express/lib/router/nuntime.js Method GET Attack Evidence Secript src=*//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js*> //scripts Other Info URL http://localhost:3000/juice-shop/node_modules/express/lib/router/nuntime.js Method GET Attack Evidence Secript src=*//cdnjs.cloudflare.com/ajax/libs/guery/2.2.4/jquery.min.js*> //scripts Method GET Attack Evidence Secript src=*//cdnjs.cloudflare.com/ajax/libs/guery/2.2.4/jquery.min.js*> //scripts Other Info URL http://localhost:3000/juice-shop/node_modules/express/lib/router/nuntime.js Method GET Attack Evidence Secript src=*//cdnjs.cloudflare.com/ajax/libs/guery/2.2.4/jquery.min.js*> //scripts URL http://localhost:3000/juice-shop/node_modules/express/lib/router/styles.css Method GET Attack Evidence Secript src=*//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js*> //scripts		
Evidence script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"> Other Info 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"> 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/cookieconsent2/3.1.0/cookieconsent.min.js"> Other Info 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"> Other Info http://localhost:3000/juice-shop/node_modules/express/lib/router/runtime.js Wethod GET Attack Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"> Other Info URL http://localhost:3000/juice-shop/node_modules/express/lib/router/runtime.js Other Info GET Attack Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"> URL http://localhost:3000/juice-shop/node_modules/express/lib/router/runtime.js 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"><</td> URL http://localhost:3000/juic</td><td></td><td>GET</td></tr><tr><td>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 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/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/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> 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/jquery/2.2.4/jquery.min.js"></script> Method GET Attack Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"><<script></script> Method GET Attack Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</script>	Attack	
Info URL Method GET Attack Evidence Other Info URL Method GET Attack Evidence Script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"> Other Info URL Method GET Attack Evidence Script src="/cdnjs.cloudflare.com/ajax/libs/govery2.2.4/jquery.min.js"> Other Info URL 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/polyfills.js Method GET Attack Evidence Script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"> Other Info URL http://localhost:3000/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/cookieconsent2/3.1.0/cookieconsent.min.js"> Method GET Attack Evidence Script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"> Other Info URL http://localhost:3000/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"> 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/gookieconsent2/3.1.0/cookieconsent.min.js"> Other Info URL http://localhost:3000/juice-shop/node_modules/express/lib/router/syles.css Method GET Attack Evidence Script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"> Scripts	Evidence	
Method GET Attack Evidence		
Attack Evidence	URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/main.js
Evidence	Method	GET
Other Info URL http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js Method GET Attack Evidence	Attack	
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">< 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">< //recompanies/apax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><//r/> /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/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/jquery/2.2.4/jquery.min.js"></script> Script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><	Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Method GET Attack Evidence		
Evidence	URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js
Evidence	Method	GET
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 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"><</scriptsrc="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</scriptsrc="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</scriptsrc="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</scriptsrc="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</scriptsrc="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</scriptsrc="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</scriptsrc="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</scriptsrc="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</scriptsrc="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</scriptsrc="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</scriptsrc="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</scriptsrc="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><</scriptsrc="//cdnjs.cl</td><td>Attack</td><td></td></tr><tr><td>Info URL http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js Method GET Attack Evidence <pre></td><td>Evidence</td><td></td></tr><tr><td>Method GET Attack Evidence</td><td></td><td></td></tr><tr><td>Attack Evidence</td><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/express/lib/router/polyfills.js</td></tr><tr><td>Evidence</td><td>Method</td><td>GET</td></tr><tr><td>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"> 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 src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"> /script></td><td>Attack</td><td></td></tr><tr><td>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/runtime.js Method GET Attack Evidence script Other Info URL http://localhost:3000/juice-shop/node_modules/express/lib/router/styles.css Method GET Attack Evidence <a href="script-src="//cdnjs.cloudflar</td><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>		
Method GET Attack Evidence		
Attack Evidence	URL	http://localhost:3000/juice-shop/node modules/express/lib/router/runtime.js
Evidence	Method	GET
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>	Attack	
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></td><td>Evidence</td><td></td></tr><tr><td>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></td><td></td><td></td></tr><tr><td>Attack Evidence</td><td>URL</td><td>http://localhost:3000/juice-shop/node modules/express/lib/router/runtime.js</td></tr><tr><td>Evidence <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script> Other Info URL http://localhost:3000/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></td><td>Method</td><td>GET</td></tr><tr><td>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></td><td>Attack</td><td></td></tr><tr><td>URL http://localhost:3000/juice-shop/node_modules/express/lib/router/styles.css Method GET Attack Evidence < /a> /script></td><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>		
Method GET Attack Evidence <a 3.1.0="" ajax="" cdnjs.cloudflare.com="" cookieconsent.min.js"="" cookieconsent2="" href="mailto:script-src=" libs="">< /a> /script>		
Method GET Attack Evidence <a 3.1.0="" ajax="" cdnjs.cloudflare.com="" cookieconsent.min.js"="" cookieconsent2="" href="mailto:script-src=" libs="">< /a> /script>	URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/styles.css
Evidence <pre> <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></pre> <pre>/script></pre></td><td>Method</td><td>GET</td></tr><tr><td>Evidence <pre> <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></pre> <pre>/script></pre></td><td>Attack</td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td>Other</td><td></td></tr></tbody></table></script></pre>		

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

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

Evidence	/script>
Other	75CHPL>
Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/styles.css
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/vendor.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/vendor.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/index.js:145:39
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/index.js:145:39</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/main.js
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/main.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td></td><td></td></tr></tbody></table></script></pre>

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

Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
URL	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td>Other Info</td><td></td></tr><tr><td>URL</td><td>http://localhost:3000/sitemap.xml</td></tr><tr><td>Method</td><td>GET</td></tr><tr><td>Attack</td><td></td></tr><tr><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script></pre>
Other Info	
Instances	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

Dlugio Id	0
riugiri ia	<u> </u>

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

Evidence	1981395349
Other	1981395349, which evaluates to: 2032-10-14 15:35:49.
Info URL	http://localhost:3000/juice-shop/build/routes/fileServer.is:43:13
Method	GET
Attack	GET
Evidence	2038834951
Other	2030034931
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

URL http://focalhost/3000/juice-shop/node_modules/express/lib/router/assets/public/styles.css Method GET Attack Evidence 2038834951 Other Info Info 2038834951, which evaluates to: 2034-08-10 11:02:31. URL http://focalhost/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://focalhost/3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js Method GET Attack Evidence 1981395349, which evaluates to: 2032-10-14 15:35:49. URL http://focalhost/3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js Method GET Attack Evidence 2038834951 Other Info 2038834951 Other 1nfo Attack Evidence Evidence 1650485437 Other 1650485437, which evaluates to: 2022-04-20 16:10:37. URL	Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
Attack	URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/styles.css
Evidence 2038834951 Cher 170 2038834951, which evaluates to: 2034-08-10 11:02:31. Info	Method	GET
Other Info	Attack	
URL http://localhost:3000/juice-shop/node modules/express/lib/router/assets/public/vendor.js Method GET Attack Evidence 1650485437 Other Info 1850485437, 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 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, 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 1981395349, 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, 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 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 2038834951 Other 2038834951	Evidence	2038834951
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 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 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 Linto 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 Other 1981395349, which evaluates to: 2032-10-1		2038834951, which evaluates to: 2034-08-10 11:02:31.
Attack Evidence 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 1981395349, which evaluates to: 2032-10-14 15:35:49. Http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js Method GET Attack Evidence 2038834951 Other 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 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 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 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
Evidence	Method	GET
Other Info Info	Attack	
Info Info	Evidence	1650485437
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 Cother 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 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 Other 2038834951 Other <td></td> <td>1650485437, which evaluates to: 2022-04-20 16:10:37.</td>		1650485437, which evaluates to: 2022-04-20 16:10:37.
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 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 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 1981395349 Other 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 URL http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10 URL http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10 URL http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10 URL http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10 URL http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10 Other 203834951 Other 203834951	URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js
Evidence 1981395349	Method	GET
Other Info URL http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js Method GET Attack Evidence 2038834951 Other Info URL http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10 Wethod 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 Wethod GET Attack Evidence 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 Attack Evidence 2038834951 Other Other 2038834951 which evaluates to: 2034-08-10 11:02:31	Attack	
Info URL http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js Method GET Attack Evidence 2038834951 Other Info URL http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js URL http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10 Method GET Attack Evidence 1650485437 Other Info URL http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10 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 URL http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10 Method GET Attack Evidence 2038834951 Other	Evidence	1981395349
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 Other 2038834951 Other 2038834951		1981395349, which evaluates to: 2032-10-14 15:35:49.
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 2038834951 which evaluates to: 2034-08-10.11/103-31	URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js
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 0ther Info 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 URL http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10 Method GET Attack Evidence 2038834951 Other 2038834951 which evaluates to: 2034-08-10 11:02:31	Method	GET
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 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 URL http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10 Method GET Attack Evidence 2038834951 Other 2038834951 which evaluates to: 2034-08-10 11:02:31	Attack	
URL	Evidence	2038834951
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 2038834951 which evaluates to: 2034-08-10 11:02:31		2038834951, which evaluates to: 2034-08-10 11:02:31.
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 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
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 URL http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10 Method GET Attack Evidence 2038834951 Other 2038834951 Which evaluates to: 2034-08-10 11:02:31	Method	GET
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 2038834951 which evaluates to: 2034-08-10 11:02:31	Attack	
Info Info	Evidence	1650485437
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 2038834951, which evaluates to: 2034-08-10 11:03:31		1650485437, which evaluates to: 2022-04-20 16:10:37.
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 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
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 2038834951, which evaluates to: 2034-08-10 11:02:31	Method	GET
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 2038834951, which evaluates to: 2034-08-10 11:02:31	Attack	
Info Info	Evidence	1981395349
Method GET Attack Evidence 2038834951 Other 2038834951 which evaluates to: 2034-08-10 11:02:31		1981395349, which evaluates to: 2032-10-14 15:35:49.
Attack Evidence 2038834951 Other 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
Evidence 2038834951 Other 2038834951 which evaluates to: 2034-08-10 11:02:31	Method	GET
Other 2038834051 which evaluates to: 2034-08-10 11:02:31	Attack	
711388 3/10P.1 Minicu 0/(31113106 to, 3/13/1-118-111 11:113, 3.1	Evidence	2038834951
		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

A	
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
URL Method	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3 GET
Method	
Method Attack	GET
Method Attack Evidence Other	GET 1650485437
Method Attack Evidence Other Info	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37.
Method Attack Evidence Other Info URL	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3
Method Attack Evidence Other Info URL Method	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3
Method Attack Evidence Other Info URL Method Attack	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3 GET
Method Attack Evidence Other Info URL Method Attack Evidence Other	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3 GET 1981395349
Method Attack Evidence Other Info URL Method Attack Evidence Other Info	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3 GET 1981395349 1981395349, which evaluates to: 2032-10-14 15:35:49.
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3 GET 1981395349 1981395349, which evaluates to: 2032-10-14 15:35:49. http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3

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

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 <u>I</u>	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 Ł	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/vendor.js
Method (GET
Attack	
Evidence 2	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL Ł	http://localhost:3000/juice-shop/node modules/serve-index/index.js:145:39
Method	GET
Attack	
Evidence	1650485437
Other ,	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL Ł	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 Ł	http://localhost:3000/juice-shop/node_modules/serve-index/index.js:145:39
Method (GET
Attack	
Evidence 2	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 ,	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	2020024054
Other	2038834951
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
URL Method	http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js GET
Method	
Method Attack	GET
Method Attack Evidence Other	GET 1650485437
Method Attack Evidence Other Info	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37.
Method Attack Evidence Other Info URL	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js
Method Attack Evidence Other Info URL Method	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js
Method Attack Evidence Other Info URL Method Attack	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js GET
Method Attack Evidence Other Info URL Method Attack Evidence Other	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js GET 1981395349
Method Attack Evidence Other Info URL Method Attack Evidence Other Info	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js GET 1981395349 1981395349, which evaluates to: 2032-10-14 15:35:49.
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL URL URL URL URL URL URL	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js GET 1981395349 1981395349, which evaluates to: 2032-10-14 15:35:49. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js GET 1981395349 1981395349, which evaluates to: 2032-10-14 15:35:49. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js GET 1981395349 1981395349, which evaluates to: 2032-10-14 15:35:49. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js GET
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js GET 1981395349 1981395349, which evaluates to: 2032-10-14 15:35:49. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js GET 2038834951
Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Contract Method Attack Evidence Other Info URL Method Attack Evidence Other Info	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js GET 1981395349 1981395349, which evaluates to: 2032-10-14 15:35:49. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js GET 2038834951 2038834951, which evaluates to: 2034-08-10 11:02:31.
Method Attack Evidence Other Info URL URL Method Attack URL URL URL URL URL URL URL	GET 1650485437 1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js GET 1981395349 1981395349, which evaluates to: 2032-10-14 15:35:49. http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js GET 2038834951 2038834951, which evaluates to: 2034-08-10 11:02:31. http://localhost:3000/main.js

Evidence	1734944650
Other	1734944650, which evaluates to: 2024-12-23 04:04:10.
Info	
URL	http://localhost:3000/rest/admin/application-configuration
Method	GET
Attack Evidence	1969196030
Other	1969 196030
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
Evidence Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
Other	
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
Other Info URL	1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/sitemap.xml
Other Info URL Method	1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/sitemap.xml
Other Info URL Method Attack	1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/sitemap.xml GET
Other Info URL Method Attack Evidence Other	1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/sitemap.xml GET 1981395349
Other Info URL Method Attack Evidence Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/sitemap.xml GET 1981395349 1981395349, which evaluates to: 2032-10-14 15:35:49.
Other Info URL Method Attack Evidence Other Info URL	1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/sitemap.xml GET 1981395349 1981395349, which evaluates to: 2032-10-14 15:35:49. http://localhost:3000/sitemap.xml
Other Info URL Method Attack Evidence Other Info URL Method	1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/sitemap.xml GET 1981395349 1981395349, which evaluates to: 2032-10-14 15:35:49. http://localhost:3000/sitemap.xml
Other Info URL Method Attack Evidence Other Info URL Method Attack	1650485437, which evaluates to: 2022-04-20 16:10:37. http://localhost:3000/sitemap.xml GET 1981395349 1981395349, which evaluates to: 2032-10-14 15:35:49. http://localhost:3000/sitemap.xml GET

Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1680327869
Other Info	1680327869, which evaluates to: 2023-04-01 01:44:29.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1701244813
Other Info	1701244813, which evaluates to: 2023-11-29 03:00:13.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	18181818
Other Info	18181818, which evaluates to: 2027-08-13 14:30:18.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1839622642
Other Info	1839622642, which evaluates to: 2028-04-17 18:17:22.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1863874346
Other Info	1863874346, which evaluates to: 2029-01-23 09:52:26.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1917098446
Other Info	1917098446, which evaluates to: 2030-10-01 11:20:46.
URL	http://localhost:3000/styles.css

Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	2033195021
Other Info	2033195021, which evaluates to: 2034-06-06 04:23:41.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
Instances	162
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
	17
Plugin Id	<u>10096</u>
Plugin Id	10096
Plugin Id Low	X-Content-Type-Options Header Missing 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-
Plugin Id Low Description	X-Content-Type-Options Header Missing 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.
Plugin Id Low Description URL	X-Content-Type-Options Header Missing 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. http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbaE
Plugin Id Low Description URL Method	X-Content-Type-Options Header Missing 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. http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbaE
Plugin Id Low Description URL Method Attack	X-Content-Type-Options Header Missing 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. http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbaE
Plugin Id Low Description URL Method Attack Evidence Other	X-Content-Type-Options Header Missing 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. http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbaE GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client
Plugin Id Low Description URL Method Attack Evidence Other Info	X-Content-Type-Options Header Missing 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. http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbaE GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbl3&sid=k8EZRNNfT3-
Plugin Id Low Description URL Method Attack Evidence Other Info URL	X-Content-Type-Options Header Missing 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. http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbaE GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbl3&sid=k8EZRNNfT3-tQELHAAAW
Plugin Id Low Description URL Method Attack Evidence Other Info URL Method	X-Content-Type-Options Header Missing 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. http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbaE GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbl3&sid=k8EZRNNfT3-tQELHAAAW
Plugin Id Low Description URL Method Attack Evidence Other Info URL Method Attack	X-Content-Type-Options Header Missing 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. http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbaE GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbl3&sid=k8EZRNNfT3-tQELHAAAW

	or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSbpR&sid=k8EZRNNfT3-tQELHAAAW
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=PdfSckS
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=PdfScwq&sid=TYafPcUf8ifUG5cyAAAY
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=PdfSd7x&sid=TYafPcUf8ifUG5cyAAAY
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=PdfSh2p
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=PdfShKA&sid=GY9M8mCaCjAbyyWZAAAa
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=PdfShP- &sid=GY9M8mCaCjAbyyWZAAAa
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=PdfSi9S
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=PdfSiaN&sid=O- RgKKEE5zgL2X87AAAc
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=PdfSiL2&sid=O- RgKKEE5zgL2X87AAAc
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=PdfSiyy
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=PdfSj61&sid=RikHJG_PnMgkz8hEAAAe
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=PdfSjDV&sid=RikHJG_PnMgkz8hEAAAe
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=PdfSnJ1
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=PdfSnxn&sid=yfgGVPJteWWbJDRpAAAg
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=PdfSnXo&sid=yfgGVPJteWWbJDRpAAAg
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=PdfSodg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PdfSonE&sid=DxErFLCztc9zPOn8AAAi
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=PdfSos0&sid=DxErFLCztc9zPOn8AAAi
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=PdfSoxd&sid=oAr-kxL10IHMT7zHAAAj
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=PdfSoY0
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=PdfSp7X&sid=oAr-kxL10IHMT7zHAAAj
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=PdfSpBu&sid=DxErFLCztc9zPOn8AAAi
Method	GET
Attack	
Evidence	
Other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSsfZ&sid=7SQ4y8wodprjukxkAAAm
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=PdfSsH8
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=PdfSsmr&sid=7SQ4y8wodprjukxkAAAm
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=PdfSt78
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=PdfSteA
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=PdfStIG&sid=c5v6lx_4YAzmKpbIAAAo
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=PdfStWm&sid=c5v6lx_4YAzmKpblAAAo
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=PdfSu6S&sid=LioAEUTo_jxaC4i4AAAq
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=PdfSuOM&sid=LioAEUTo_jxaC4i4AAAq
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=PdfSuqg
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=PdfSuTH
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=PdfSuVF&sid=LioAEUTo_jxaC4i4AAAq
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=PdfSuxK&sid=OPAOmz5AmC732BPmAAAs
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=PdfSv6T&sid=MnANeJyZYe5FsmS0AAAt
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=PdfSvae&sid=OPAOmz5AmC732BPmAAAs
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=PdfSvch
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=PdfSvOv&sid=OPAOmz5AmC732BPmAAAs
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=PdfSvYi&sid=MnANeJyZYe5FsmS0AAAt
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=PdfSvyU&sid=p-NWnqV_UNwNVvDfAAAw
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=PdfSw6 &sid=p-NWnqV UNwNVvDfAAAw
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=PdfSwb3&sid=Bw9anqxtgpXYGUTzAAAy
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=PdfSwFJ
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=PdfSwsQ&sid=Bw9anqxtgpXYGUTzAAAy
Method	GET
Attack	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSwTS&sid=p-NWnqV_UNwNVvDfAAAw
GET
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSwxL
GET
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSxbl&sid=Bw9anqxtgpXYGUTzAAAy
GET
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSxct&sid=Bw9anqxtgpXYGUTzAAAy
GET
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSxwW&sid=MJRB9uC6lgB6g_JaAAA0
GET
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
http://localhost:3000/socket.io/? EIO=4&transport=polling&t=PdfSxXk&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxY5&sid=Bw9anqxtgpXYGUTzAAAy
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=PdfSbl2&sid=k8EZRNNfT3-tQELHAAAW
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=PdfScwn&sid=TYafPcUf8ifUG5cyAAAY
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=PdfShK9&sid=GY9M8mCaCjAbyyWZAAAa
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=PdfSiL1&sid=O-RgKKEE5zgL2X87AAAc
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=PdfSj5x&sid=RikHJG_PnMgkz8hEAAAe
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=PdfSnXl&sid=yfgGVPJteWWbJDRpAAAg
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=PdfSon5&sid=DxErFLCztc9zPOn8AAAi
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=PdfSoxT&sid=oAr-kxL10IHMT7zHAAAj
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=PdfSsfM&sid=7SQ4y8wodprjukxkAAAm
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=PdfStI9&sid=c5v6lx_4YAzmKpbIAAAo
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=PdfSu6C&sid=LioAEUTo_jxaC4i4AAAq
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=PdfSuxI&sid=OPAOmz5AmC732BPmAAAs
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=PdfSv6S&sid=MnANeJyZYe5FsmS0AAAt
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=PdfSvyS&sid=p-NWnqV_UNwNVvDfAAAw
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=PdfSwap&sid=Bw9anqxtgpXYGUTzAAAy
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=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0

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	71
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) and is developed and maintained by voluntee", see evidence field for the suspicious comment /snippet.
URL	http://localhost:3000/tutorial.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//w. soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076& color=%23ff5500&auto_play=true&h", see evidence field for the suspicious comment/snippet.
URL	http://localhost:3000/vendor.js
Method	GET
Attack	

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

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

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

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

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

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

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

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

	Evidence	<pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td></td><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>UR</td><td>L</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js</td></tr><tr><td></td><td>Method</td><td>GET</td></tr><tr><td></td><td>Attack</td><td></td></tr><tr><td></td><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td></td><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>UR</td><td>L</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js</td></tr><tr><td></td><td>Method</td><td>GET</td></tr><tr><td></td><td>Attack</td><td></td></tr><tr><td></td><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td></td><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>UR</td><td>L</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/styles.css</td></tr><tr><td></td><td>Method</td><td>GET</td></tr><tr><td></td><td>Attack</td><td></td></tr><tr><td></td><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td></td><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>UR</td><td>L</td><td>http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js</td></tr><tr><td></td><td>Method</td><td>GET</td></tr><tr><td></td><td>Attack</td><td></td></tr><tr><td></td><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td></td><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>UR</td><td>L</td><td>http://localhost:3000/sitemap.xml</td></tr><tr><td></td><td>Method</td><td>GET</td></tr><tr><td></td><td>Attack</td><td></td></tr><tr><td></td><td>Evidence</td><td><pre><script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script></pre></td></tr><tr><td></td><td>Other Info</td><td>No links have been found while there are scripts, which is an indication that this is a modern web application.</td></tr><tr><td>Instan</td><td>ices</td><td>50</td></tr><tr><td>Soluti</td><td>on</td><td>This is an informational alert and so no changes are required.</td></tr><tr><td>Refere</td><td>ence</td><td></td></tr><tr><td>CWE</td><td>ld</td><td></td></tr><tr><td>WASC</td><td>C ld</td><td></td></tr><tr><td>Plugir</td><td>ı ld</td><td>10109</td></tr><tr><td></td><td></td><td>Patriavad from Cooks</td></tr></tbody></table></script></pre>

Informational

Retrieved from Cache

Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Method	GET
Attack	
Evidence	Age: 26
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Method	GET
Attack	
Evidence	Age: 49
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Method	GET
Attack	
Evidence	Age: 77
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: 26
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: 49
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: 77
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: 26
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: 49
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: 78
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	9
	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
Solution	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
	Check for differences in response based on fuzzed Llaer Agent (og mehile sites, seeses as

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)	Informational	User Agent Fuzzer
Method GET Attack Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Evidence Other Info URL http://localhost:3000/assets Method GET	Description	a Search Engine Crawler). Compares the response statuscode and the hashcode of the
Attack Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Evidence Other Info URL http://localhost:3000/assets Method GET	URL	http://localhost:3000/assets
Evidence Other Info URL http://localhost:3000/assets Method GET	Method	GET
Other Info URL http://localhost:3000/assets Method GET	Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
URL http://localhost:3000/assets Method GET	Evidence	
Method GET		
	URL	http://localhost:3000/assets
Attack Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)	Method	GET
	Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	Evidence	

C :1	
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	

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/rest/languages
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/rest/languages
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/rest/languages
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:3000/rest/languages
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=PdfSwxL
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=PdfSwxL
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=PdfSwxL
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=PdfSwxL
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=PdfSwxL
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=PdfSwxL
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=PdfSwxL
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=PdfSwxL
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=PdfSwxL
URL Method	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSwxL GET

Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PdfSwxL
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=PdfSwxL
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=PdfSwxL
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=PdfSxwW&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxwW&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxwW&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxwW&sid=MJRB9uC6lgB6g_JaAAA0
	The factoring of pointing of the contract of t

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=PdfSxwW&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxwW&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxwW&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxwW&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxwW&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxwW&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxwW&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxwW&sid=MJRB9uC6lgB6g_JaAAA0
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=MJRB9uC6lgB6g_JaAAA0
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=MJRB9uC6lgB6g_JaAAA0
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=MJRB9uC6lgB6g_JaAAA0
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=MJRB9uC6lgB6g_JaAAA0
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=MJRB9uC6lgB6g_JaAAA0

NA d	OFT
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=MJRB9uC6lgB6g_JaAAA0
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=MJRB9uC6lgB6g_JaAAA0
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=MJRB9uC6lgB6g_JaAAA0
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=MJRB9uC6lgB6g_JaAAA0
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=MJRB9uC6lgB6g_JaAAA0
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=MJRB9uC6lgB6g_JaAAA0
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=MJRB9uC6lgB6g_JaAAA0
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=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0
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	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0
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=PdfSxXh&sid=MJRB9uC6lgB6g_JaAAA0
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)

Evidence	
Other Info	
Instances	112
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	<u>10104</u>