Vulnerability Assessment Report – Internship Task

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

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

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

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

Alerts

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

Alert Detail

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

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

High	**SQL Injection - SQLite**
Description	SQL injection may be possible.
URL	http://localhost:3000/rest/products/search?q=%27%28
Method	GET
Attack	'(
Evidence	SQLITE_ERROR
Other Info	RDBMS [SQLite] likely, given error message regular expression [SQLITE_ERROR] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
Instances	1
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client.

	Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40018

Medium	Content Security Policy (CSP) Header Not Set
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://localhost:3000
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/assets/public/images/uploads/%E1%93%9A%E1%98%8F%E1%97%A2-
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/favicon.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/ftp
Method	GET

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

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

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

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

Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/layer.js:95:5
Method	GET
Attack	
Evidence	
Other	

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

URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/main.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/polyfills.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/runtime.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/assets/public/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/index.js:145:39
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/main.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/polyfills.js
Method	GET

Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/runtime.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNgoe&sid=2I5bMp82Z9dUQqfVAAAC
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNjrf&sid=-mlVhTFFp9RS7Ff4AAAE
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNrwa&sid=7K5VpH6acNpSwKXeAAAG
Method	POST

Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNsZs&sid=Zi_Slhms1STDM57iAAAH
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNwFT&sid=fX51XeedI4pt4YQJAAAK
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNy3a&sid=Kwa8OeOh2pxuMSaVAAAM
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO-IB&sid=UeL35-cfUjXzywO9AAAw
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO2D2&sid=bdeyXpKNMNcBpQAbAAAO
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO5At&sid=kA4CWjF19xGageFyAAAQ
Method	POST
Attack	
Evidence	
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXlObAs&sid=r0Gyydx5_nXCEI3-AAAi
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOBZA&sid=06f47PLdT2QjJRdRAAAS
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOEhG&sid=-rRTtWVV6yEWZkqNAAAU
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOhlU&sid=YsqTY6ctxcuAcjvwAAAk
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOiVN&sid=0BngYOnC9ZPURbtcAAAl
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOJih&sid=c8KluezYgHSr0yHGAAAW
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOmD9&sid=a9JjFEvJao43zt6CAAAo
Method	POST
Attack	
Evidence	

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOMeM&sid=i6bdX8p1D0EFVnupAAAY
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOP46&sid=ruBBrVn9fE_F1wM-AAAa
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOqDD&sid=JC1ekD_Zh9n659q9AAAq
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOQFF&sid=k6F6sgkqu7-F3mdHAAAc
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOSVu&sid=SdCA5TaV_EE9dy19AAAe
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOVCY&sid=L4knAU540ljVTjTFAAAg
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOw_E&sid=E8bG5H88ZZu6x7DXAAAs
Method	POST

Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOwJC&sid=drxMb855dSnsb3-0AAAt
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP1nf&sid=4tMqpwECVd3QYn6LAAAy
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP7wO&sid=B-VwIotrGvt_zZJgAAA0
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP9px&sid=RSMsBj2nWSvCnbDbAAA2
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPg7v&sid=lOUKVOyvWg9SAcXBAABE
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPh0v&sid=F2Wh9nt7bXo9pSlVAABG
Method	POST
Attack	
Evidence	
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXlPhzC&sid=LHJ6ah5Z_SHnhYOIAABI
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPItZ&sid=NWf5_adIRpq6XRiUAAA5
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPJAr&sid=7DdeBruF0OwBhp67AAA4
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPjw3&sid=rgfE_I7RPl1LHFbFAABK
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPlVT&sid=1Lt6h3A3eZVMp7NrAABM
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPmMd&sid=pQdzAuDtIJRC4tKRAABO
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPnB8&sid=gtGYScX-WJR9eBWLAABQ
Method	POST
Attack	
Evidence	

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPNP8&sid=t3jFQ_asoWrzfGkqAAA8
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPo1v&sid=RHZWQ0DPD1TDDq8oAABS
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPokU&sid=4sp63Er9EkvPF6aPAABU
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPPdM&sid=Me_bKGbJk93GH-fYAAA-
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPWZx&sid=lng5-c-rNyDCFS5CAABA
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPYQE&sid=BVad5NVM2JlZA8g9AABC
Method	POST
Attack	
Evidence	
Other Info	
Instances	102
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser

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

	be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/i18n/en.json
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/carousel/1.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/carousel/2.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/carousel/3.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

URL	http://localhost:3000/assets/public/images/carousel/4.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/carousel/5.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/carousel/6.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/carousel/7.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/hackingInstructor.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/JuiceShop_Logo.png

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

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

Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/products/melon_bike.jpeg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/products/no-results.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/products/permafrost.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/uploads/%E1%93%9A%E1%98%8F%E1%97%A2-
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/uploads/BeeHaven.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *

Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/uploads/building-something-literally-bottom-up-1721152342603.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/uploads/everything-up-and-running!-1721152385146.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/uploads/favorite-hiking-place.png
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/uploads/IMG_4253.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/uploads/magn(et)ificent!-1571814229653.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *

Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/uploads/my-rare-collectors-item!-%5B%CC%B2%CC%85$%CC%B2%CC%85(%CC%B2%CC%85-%CD%A1%C2%B0-%CD%9C%CA%96-%CD%A1%C2%B0%CC%B2%CC%85)%CC%B2%CC%85$%CC%B2%CC%85%5D-1572603645543.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/uploads/putting-in-the-hardware-1721152366854.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/assets/public/images/uploads/sorted-the-pieces,-starting-assembly-process-1721152307290.jpg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/az.svg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/bd.svg
Method	GET

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

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

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

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

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

URL	http://localhost:3000/ftp/quarantine
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/quarantine/juicy_malware_linux_amd_64.url
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/quarantine/juicy_malware_linux_arm_64.url
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/quarantine/juicy_malware_macos_64.url
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/quarantine/juicy_malware_windows_64.exe.url
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ftp/suspicious_errors.yml

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

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

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

Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/runtime.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/styles.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/vendor.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:43:13
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/juice-shop/build/routes/fileServer.js:59:18
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser

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

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

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

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

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

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

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

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

Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/mm.svg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/nl.svg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/no.svg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/pl.svg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/polyfills.js
Method	GET
Attack	

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

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

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

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

URL	http://localhost:3000/tutorial.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/tw.svg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/ua.svg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/us.svg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	http://localhost:3000/vendor.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	167

Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14
Plugin Id	10098

Medium	Missing Anti-clickjacking Header
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNgoe&sid=2I5bMp82Z9dUQqfVAAAC
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNjrf&sid=-mlVhTFFp9RS7Ff4AAAE
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNrwa&sid=7K5VpH6acNpSwKXeAAAG
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNsZs&sid=Zi_Slhms1STDM57iAAAH
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNwFT&sid=fX51XeedI4pt4YQJAAAK
Method	POST
Attack	
Evidence	
Other	

Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNy3a&sid=Kwa8OeOh2pxuMSaVAAAM
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO-IB&sid=UeL35-cfUjXzywO9AAAw
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO2D2&sid=bdeyXpKNMNcBpQAbAAAO
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO5At&sid=kA4CWjF19xGageFyAAAQ
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlObAs&sid=r0Gyydx5_nXCEI3-AAAi
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOBZA&sid=06f47PLdT2QjJRdRAAAS
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOEhG&sid=-rRTtWVV6yEWZkqNAAAU
Method	POST
Attack	

Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOhlU&sid=YsqTY6ctxcuAcjvwAAAk
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOiVN&sid=0BngYOnC9ZPURbtcAAAl
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOJih&sid=c8KIuezYgHSr0yHGAAAW
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOmD9&sid=a9JjFEvJao43zt6CAAAo
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOMeM&sid=i6bdX8p1D0EFVnupAAAY
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOP46&sid=ruBBrVn9fE_F1wM-AAAa
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOqDD&sid=JC1ekD_Zh9n659q9AAAq

Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOQFF&sid=k6F6sgkqu7-F3mdHAAAc
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOSVu&sid=SdCA5TaV_EE9dy19AAAe
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOVCY&sid=L4knAU540ljVTjTFAAAg
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOw_E&sid=E8bG5H88ZZu6x7DXAAAs
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOwJC&sid=drxMb855dSnsb3-0AAAt
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP1nf&sid=4tMqpwECVd3QYn6LAAAy
Method	POST
Attack	
Evidence	
Other	

Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP7wO&sid=B-VwIotrGvt_zZJgAAA0
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP9px&sid=RSMsBj2nWSvCnbDbAAA2
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPg7v&sid=lOUKVOyvWg9SAcXBAABE
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPh0v&sid=F2Wh9nt7bXo9pSlVAABG
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPhzC&sid=LHJ6ah5Z_SHnhYOIAABI
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPItZ&sid=NWf5_adIRpq6XRiUAAA5
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPJAr&sid=7DdeBruF0OwBhp67AAA4
Method	POST
Attack	

Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPjw3&sid=rgfE_I7RPl1LHFbFAABK
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPlVT&sid=1Lt6h3A3eZVMp7NrAABM
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPmMd&sid=pQdzAuDtIJRC4tKRAABO
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPnB8&sid=gtGYScX-WJR9eBWLAABQ
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPNP8&sid=t3jFQ_asoWrzfGkqAAA8
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPo1v&sid=RHZWQ0DPD1TDDq8oAABS
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPokU&sid=4sp63Er9EkvPF6aPAABU

Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPPdM&sid=Me_bKGbJk93GH-fYAAA-
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPWZx&sid=lng5-c-rNyDCFS5CAABA
Method	POST
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPYQE&sid=BVad5NVM2JlZA8g9AABC
Method	POST
Attack	
Evidence	
Other Info	
Instances	42
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=PXlNgog&sid=2I5bMp82Z9dUQqfVAAAC
Method	GET
Attack	
Evidence	2I5bMp82Z9dUQqfVAAAC

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNhTs&sid=2I5bMp82Z9dUQqfVAAAC
Method	GET
Attack	
Evidence	2I5bMp82Z9dUQqfVAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNhYn&sid=2I5bMp82Z9dUQqfVAAAC
Method	GET
Attack	
Evidence	2I5bMp82Z9dUQqfVAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNjtH&sid=-mlVhTFFp9RS7Ff4AAAE
Method	GET
Attack	
Evidence	-mlVhTFFp9RS7Ff4AAAE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNkJJ&sid=-mlVhTFFp9RS7Ff4AAAE
Method	GET
Attack	
Evidence	-mlVhTFFp9RS7Ff4AAAE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNrx1&sid=7K5VpH6acNpSwKXeAAAG
Method	GET
Attack	
Evidence	7K5VpH6acNpSwKXeAAAG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNsac&sid=Zi_Slhms1STDM57iAAAH
Method	GET
Attack	
Evidence	Zi_Slhms1STDM57iAAAH
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNsmJ&sid=7K5VpH6acNpSwKXeAAAG
Method	GET

Attack	
Evidence	7K5VpH6acNpSwKXeAAAG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNteT&sid=Zi_Slhms1STDM57iAAAH
Method	GET
Attack	
Evidence	Zi_Slhms1STDM57iAAAH
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNtMP&sid=7K5VpH6acNpSwKXeAAAG
Method	GET
Attack	
Evidence	7K5VpH6acNpSwKXeAAAG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNtOO&sid=Zi_Slhms1STDM57iAAAH
Method	GET
Attack	
Evidence	Zi_Slhms1STDM57iAAAH
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNw-b&sid=fX51Xeedl4pt4YQJAAAK
Method	GET
Attack	
Evidence	fX51Xeedl4pt4YQJAAAK
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNwep&sid=fX51Xeedl4pt4YQJAAAK
Method	GET
Attack	
Evidence	fX51Xeedl4pt4YQJAAAK
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNwG5&sid=fX51Xeedl4pt4YQJAAAK
Method	GET
Attack	
Evidence	fX51Xeedl4pt4YQJAAAK
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXlNy3z&sid=Kwa8OeOh2pxuMSaVAAAM
Method	GET
Attack	
Evidence	Kwa8OeOh2pxuMSaVAAAM
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNyTN&sid=Kwa8OeOh2pxuMSaVAAAM
Method	GET
Attack	
Evidence	Kwa8OeOh2pxuMSaVAAAM
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO-IP&sid=UeL35-cfUjXzywO9AAAw
Method	GET
Attack	
Evidence	UeL35-cfUjXzywO9AAAw
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO-YT&sid=UeL35-cfUjXzywO9AAAw
Method	GET
Attack	
Evidence	UeL35-cfUjXzywO9AAAw
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO2-k&sid=bdeyXpKNMNcBpQAbAAAO
Method	GET
Attack	
Evidence	bdeyXpKNMNcBpQAbAAAO
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO2Dq&sid=bdeyXpKNMNcBpQAbAAAO
Method	GET
Attack	
Evidence	bdeyXpKNMNcBpQAbAAAO
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO3Hw&sid=bdeyXpKNMNcBpQAbAAAO
Method	GET
Attack	
Evidence	bdeyXpKNMNcBpQAbAAAO

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO5Az&sid=kA4CWjF19xGageFyAAAQ
Method	GET
Attack	
Evidence	kA4CWjF19xGageFyAAAQ
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO5cR&sid=kA4CWjF19xGageFyAAAQ
Method	GET
Attack	
Evidence	kA4CWjF19xGageFyAAAQ
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO5s9&sid=kA4CWjF19xGageFyAAAQ
Method	GET
Attack	
Evidence	kA4CWjF19xGageFyAAAQ
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO_5g&sid=UeL35-cfUjXzywO9AAAw
Method	GET
Attack	
Evidence	UeL35-cfUjXzywO9AAAw
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlObB3&sid=r0Gyydx5_nXCEI3-AAAi
Method	GET
Attack	
Evidence	r0Gyydx5_nXCEI3-AAAi
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlObll&sid=r0Gyydx5_nXCEI3-AAAi
Method	GET
Attack	
Evidence	r0Gyydx5_nXCEI3-AAAi
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlObWa&sid=r0Gyydx5_nXCEI3-AAAi
Method	GET

Attack	
Evidence	r0Gyydx5_nXCEI3-AAAi
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOBZd&sid=06f47PLdT2QjJRdRAAAS
Method	GET
Attack	
Evidence	06f47PLdT2QjJRdRAAAS
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOCGk&sid=06f47PLdT2QjJRdRAAAS
Method	GET
Attack	
Evidence	06f47PLdT2QjJRdRAAAS
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOEiH&sid=-rRTtWVV6yEWZkqNAAAU
Method	GET
Attack	
Evidence	-rRTtWVV6yEWZkqNAAAU
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOFYU&sid=-rRTtWVV6yEWZkqNAAAU
Method	GET
Attack	
Evidence	-rRTtWVV6yEWZkqNAAAU
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOhla&sid=YsqTY6ctxcuAcjvwAAAk
Method	GET
Attack	
Evidence	YsqTY6ctxcuAcjvwAAAk
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOiEA&sid=YsqTY6ctxcuAcjvwAAAk
Method	GET
Attack	
Evidence	YsqTY6ctxcuAcjvwAAAk
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXlOiQ2&sid=YsqTY6ctxcuAcjvwAAAk
Method	GET
Attack	
Evidence	YsqTY6ctxcuAcjvwAAAk
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOiq_&sid=0BngYOnC9ZPURbtcAAAl
Method	GET
Attack	
Evidence	0BngYOnC9ZPURbtcAAAl
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOiVo&sid=0BngYOnC9ZPURbtcAAAl
Method	GET
Attack	
Evidence	0BngYOnC9ZPURbtcAAAl
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOJjH&sid=c8KIuezYgHSr0yHGAAAW
Method	GET
Attack	
Evidence	c8KIuezYgHSr0yHGAAAW
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOK4P&sid=c8KIuezYgHSr0yHGAAAW
Method	GET
Attack	
Evidence	c8KIuezYgHSr0yHGAAAW
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOKHI&sid=c8KIuezYgHSr0yHGAAAW
Method	GET
Attack	
Evidence	c8KIuezYgHSr0yHGAAAW
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOmDk&sid=a9JjFEvJao43zt6CAAAo
Method	GET
Attack	
Evidence	a9JjFEvJao43zt6CAAAo

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOMeb&sid=i6bdX8p1D0EFVnupAAAY
Method	GET
Attack	
Evidence	i6bdX8p1D0EFVnupAAAY
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOmlv&sid=a9JjFEvJao43zt6CAAAo
Method	GET
Attack	
Evidence	a9JjFEvJao43zt6CAAAo
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOMvp&sid=i6bdX8p1D0EFVnupAAAY
Method	GET
Attack	
Evidence	i6bdX8p1D0EFVnupAAAY
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlONAQ&sid=i6bdX8p1D0EFVnupAAAY
Method	GET
Attack	
Evidence	i6bdX8p1D0EFVnupAAAY
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOP4X&sid=ruBBrVn9fE_F1wM-AAAa
Method	GET
Attack	
Evidence	ruBBrVn9fE_F1wM-AAAa
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOPXD&sid=ruBBrVn9fE_F1wM-AAAa
Method	GET
Attack	
Evidence	ruBBrVn9fE_F1wM-AAAa
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOqE2&sid=JC1ekD_Zh9n659q9AAAq
Method	GET

Attack	
Evidence	JC1ekD_Zh9n659q9AAAq
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOQFx&sid=k6F6sgkqu7-F3mdHAAAc
Method	GET
Attack	
Evidence	k6F6sgkqu7-F3mdHAAAc
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOQpI&sid=k6F6sgkqu7-F3mdHAAAc
Method	GET
Attack	
Evidence	k6F6sgkqu7-F3mdHAAAc
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOqVu&sid=JC1ekD_Zh9n659q9AAAq
Method	GET
Attack	
Evidence	JC1ekD_Zh9n659q9AAAq
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOSVw&sid=SdCA5TaV_EE9dy19AAAe
Method	GET
Attack	
Evidence	SdCA5TaV_EE9dy19AAAe
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOT8H&sid=SdCA5TaV_EE9dy19AAAe
Method	GET
Attack	
Evidence	SdCA5TaV_EE9dy19AAAe
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOVDz&sid=L4knAU540ljVTjTFAAAg
Method	GET
Attack	
Evidence	L4knAU540ljVTjTFAAAg
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXlOw_M&sid=E8bG5H88ZZu6x7DXAAAs
Method	GET
Attack	
Evidence	E8bG5H88ZZu6x7DXAAAs
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOWjT&sid=L4knAU540ljVTjTFAAAg
Method	GET
Attack	
Evidence	L4knAU540ljVTjTFAAAg
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOwKB&sid=drxMb855dSnsb3-0AAAt
Method	GET
Attack	
Evidence	drxMb855dSnsb3-0AAAt
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOwun&sid=drxMb855dSnsb3-0AAAt
Method	GET
Attack	
Evidence	drxMb855dSnsb3-0AAAt
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOxBv&sid=E8bG5H88ZZu6x7DXAAAs
Method	GET
Attack	
Evidence	E8bG5H88ZZu6x7DXAAAs
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOxJF&sid=E8bG5H88ZZu6x7DXAAAs
Method	GET
Attack	
Evidence	E8bG5H88ZZu6x7DXAAAs
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP1np&sid=4tMqpwECVd3QYn6LAAAy
Method	GET
Attack	
Evidence	4tMqpwECVd3QYn6LAAAy

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP2Eg&sid=4tMqpwECVd3QYn6LAAAy
Method	GET
Attack	
Evidence	4tMqpwECVd3QYn6LAAAy
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP7we&sid=B-VwIotrGvt_zZJgAAA0
Method	GET
Attack	
Evidence	B-VwIotrGvt_zZJgAAA0
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP8mH&sid=B-VwIotrGvt_zZJgAAA0
Method	GET
Attack	
Evidence	B-VwIotrGvt_zZJgAAA0
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP8R5&sid=B-VwIotrGvt_zZJgAAA0
Method	GET
Attack	
Evidence	B-VwIotrGvt_zZJgAAA0
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP8vQ&sid=B-VwIotrGvt_zZJgAAA0
Method	GET
Attack	
Evidence	B-VwIotrGvt_zZJgAAA0
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP9q0&sid=RSMsBj2nWSvCnbDbAAA2
Method	GET
Attack	
Evidence	RSMsBj2nWSvCnbDbAAA2
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPAM8&sid=RSMsBj2nWSvCnbDbAAA2
Method	GET

Attack	
Evidence	RSMsBj2nWSvCnbDbAAA2
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPAS4&sid=RSMsBj2nWSvCnbDbAAA2
Method	GET
Attack	
Evidence	RSMsBj2nWSvCnbDbAAA2
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPg89&sid=lOUKVOyvWg9SAcXBAABE
Method	GET
Attack	
Evidence	lOUKVOyvWg9SAcXBAABE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPghg&sid=lOUKVOyvWg9SAcXBAABE
Method	GET
Attack	
Evidence	lOUKVOyvWg9SAcXBAABE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPh0-&sid=F2Wh9nt7bXo9pSlVAABG
Method	GET
Attack	
Evidence	F2Wh9nt7bXo9pSlVAABG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPhE0&sid=F2Wh9nt7bXo9pSlVAABG
Method	GET
Attack	
Evidence	F2Wh9nt7bXo9pSlVAABG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPhzH&sid=LHJ6ah5Z_SHnhYOIAABI
Method	GET
Attack	
Evidence	LHJ6ah5Z_SHnhYOIAABI
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXlPilj&sid=LHJ6ah5Z_SHnhYOIAABI
Method	GET
Attack	
Evidence	LHJ6ah5Z_SHnhYOIAABI
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPIta&sid=NWf5_adIRpq6XRiUAAA5
Method	GET
Attack	
Evidence	NWf5_adIRpq6XRiUAAA5
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPJAU&sid=NWf5_adIRpq6XRiUAAA5
Method	GET
Attack	
Evidence	NWf5_adIRpq6XRiUAAA5
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPJBH&sid=7DdeBruF0OwBhp67AAA4
Method	GET
Attack	
Evidence	7DdeBruF0OwBhp67AAA4
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPJIx&sid=NWf5_adIRpq6XRiUAAA5
Method	GET
Attack	
Evidence	NWf5_adIRpq6XRiUAAA5
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPJSH&sid=7DdeBruF0OwBhp67AAA4
Method	GET
Attack	
Evidence	7DdeBruF0OwBhp67AAA4
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPjwO&sid=rgfE_I7RPl1LHFbFAABK
Method	GET
Attack	
Evidence	rgfE_I7RPl1LHFbFAABK

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPk5V&sid=rgfE_I7RPl1LHFbFAABK
Method	GET
Attack	
Evidence	rgfE_I7RPl1LHFbFAABK
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPlmI&sid=1Lt6h3A3eZVMp7NrAABM
Method	GET
Attack	
Evidence	1Lt6h3A3eZVMp7NrAABM
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPlVs&sid=1Lt6h3A3eZVMp7NrAABM
Method	GET
Attack	
Evidence	1Lt6h3A3eZVMp7NrAABM
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPmOQ&sid=pQdzAuDtIJRC4tKRAABO
Method	GET
Attack	
Evidence	pQdzAuDtIJRC4tKRAABO
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPmSo&sid=pQdzAuDtIJRC4tKRAABO
Method	GET
Attack	
Evidence	pQdzAuDtIJRC4tKRAABO
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPN_X&sid=t3jFQ_asoWrzfGkqAAA8
Method	GET
Attack	
Evidence	t3jFQ_asoWrzfGkqAAA8
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPnBR&sid=gtGYScX-WJR9eBWLAABQ
Method	GET

Attack	
Evidence	gtGYScX-WJR9eBWLAABQ
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPndt&sid=gtGYScX-WJR9eBWLAABQ
Method	GET
Attack	
Evidence	gtGYScX-WJR9eBWLAABQ
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPnLw&sid=gtGYScX-WJR9eBWLAABQ
Method	GET
Attack	
Evidence	gtGYScX-WJR9eBWLAABQ
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPNQI&sid=t3jFQ_asoWrzfGkqAAA8
Method	GET
Attack	
Evidence	t3jFQ_asoWrzfGkqAAA8
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPo25&sid=RHZWQ0DPD1TDDq8oAABS
Method	GET
Attack	
Evidence	RHZWQ0DPD1TDDq8oAABS
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPoCP&sid=RHZWQ0DPD1TDDq8oAABS
Method	GET
Attack	
Evidence	RHZWQ0DPD1TDDq8oAABS
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPolS&sid=4sp63Er9EkvPF6aPAABU
Method	GET
Attack	
Evidence	4sp63Er9EkvPF6aPAABU
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXlPOXI&sid=t3jFQ_asoWrzfGkqAAA8
Method	GET
Attack	
Evidence	t3jFQ_asoWrzfGkqAAA8
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPoxn&sid=4sp63Er9EkvPF6aPAABU
Method	GET
Attack	
Evidence	4sp63Er9EkvPF6aPAABU
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPPdb&sid=Me_bKGbJk93GH-fYAAA-
Method	GET
Attack	
Evidence	Me_bKGbJk93GH-fYAAA-
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPPrc&sid=Me_bKGbJk93GH-fYAAA-
Method	GET
Attack	
Evidence	Me_bKGbJk93GH-fYAAA-
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPWa5&sid=lng5-c-rNyDCFS5CAABA
Method	GET
Attack	
Evidence	lng5-c-rNyDCFS5CAABA
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPY3-&sid=lng5-c-rNyDCFS5CAABA
Method	GET
Attack	
Evidence	lng5-c-rNyDCFS5CAABA
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPY_f&sid=BVad5NVM2JlZA8g9AABC
Method	GET
Attack	
Evidence	BVad5NVM2JlZA8g9AABC

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPYA4&sid=lng5-c-rNyDCFS5CAABA
Method	GET
Attack	
Evidence	lng5-c-rNyDCFS5CAABA
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPYmv&sid=BVad5NVM2JlZA8g9AABC
Method	GET
Attack	
Evidence	BVad5NVM2JlZA8g9AABC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPYQH&sid=BVad5NVM2JlZA8g9AABC
Method	GET
Attack	
Evidence	BVad5NVM2JlZA8g9AABC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=-mlVhTFFp9RS7Ff4AAAE
Method	GET
Attack	
Evidence	-mlVhTFFp9RS7Ff4AAAE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=-rRTtWVV6yEWZkqNAAAU
Method	GET
Attack	
Evidence	-rRTtWVV6yEWZkqNAAAU
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=06f47PLdT2QjJRdRAAAS
Method	GET
Attack	
Evidence	06f47PLdT2QjJRdRAAAS
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=0BngYOnC9ZPURbtcAAAl
Method	GET
Attack	

Evidence	0BngYOnC9ZPURbtcAAAl
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=1Lt6h3A3eZVMp7NrAABM
Method	GET
Attack	
Evidence	1Lt6h3A3eZVMp7NrAABM
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=2I5bMp82Z9dUQqfVAAAC
Method	GET
Attack	
Evidence	2I5bMp82Z9dUQqfVAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=4sp63Er9EkvPF6aPAABU
Method	GET
Attack	
Evidence	4sp63Er9EkvPF6aPAABU
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=4tMqpwECVd3QYn6LAAAy
Method	GET
Attack	
Evidence	4tMqpwECVd3QYn6LAAAy
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=7DdeBruF0OwBhp67AAA4
Method	GET
Attack	
Evidence	7DdeBruF0OwBhp67AAA4
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=7K5VpH6acNpSwKXeAAAG
Method	GET
Attack	
Evidence	7K5VpH6acNpSwKXeAAAG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=a9JjFEvJao43zt6CAAAo
Method	GET

Attack	
Evidence	a9JjFEvJao43zt6CAAAo
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=B-VwIotrGvt_zZJgAAA0
Method	GET
Attack	
Evidence	B-VwIotrGvt_zZJgAAA0
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=bdeyXpKNMNcBpQAbAAAO
Method	GET
Attack	
Evidence	bdeyXpKNMNcBpQAbAAAO
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=BVad5NVM2JlZA8g9AABC
Method	GET
Attack	
Evidence	BVad5NVM2JlZA8g9AABC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=c8KIuezYgHSr0yHGAAAW
Method	GET
Attack	
Evidence	c8KIuezYgHSr0yHGAAAW
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=drxMb855dSnsb3-0AAAt
Method	GET
Attack	
Evidence	drxMb855dSnsb3-0AAAt
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=E8bG5H88ZZu6x7DXAAAs
Method	GET
Attack	
Evidence	E8bG5H88ZZu6x7DXAAAs
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=F2Wh9nt7bXo9pSlVAABG

Method	GET
Attack	
Evidence	F2Wh9nt7bXo9pSlVAABG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=fX51XeedI4pt4YQJAAAK
Method	GET
Attack	
Evidence	fX51XeedI4pt4YQJAAAK
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=gtGYScX-WJR9eBWLAABQ
Method	GET
Attack	
Evidence	gtGYScX-WJR9eBWLAABQ
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=i6bdX8p1D0EFVnupAAAY
Method	GET
Attack	
Evidence	i6bdX8p1D0EFVnupAAAY
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=JC1ekD_Zh9n659q9AAAq
Method	GET
Attack	
Evidence	JC1ekD_Zh9n659q9AAAq
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=k6F6sgkqu7-F3mdHAAAc
Method	GET
Attack	
Evidence	k6F6sgkqu7-F3mdHAAAc
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=kA4CWjF19xGageFyAAAQ
Method	GET
Attack	
Evidence	kA4CWjF19xGageFyAAAQ
Other Info	

URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=Kwa8OeOh2pxuMSaVAAAM
Method	GET
Attack	
Evidence	Kwa8OeOh2pxuMSaVAAAM
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=L4knAU540ljVTjTFAAAg
Method	GET
Attack	
Evidence	L4knAU540ljVTjTFAAAg
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=LHJ6ah5Z_SHnhYOIAABI
Method	GET
Attack	
Evidence	LHJ6ah5Z_SHnhYOIAABI
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=lng5-c-rNyDCFS5CAABA
Method	GET
Attack	
Evidence	lng5-c-rNyDCFS5CAABA
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=lOUKVOyvWg9SAcXBAABE
Method	GET
Attack	
Evidence	lOUKVOyvWg9SAcXBAABE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=Me_bKGbJk93GH-fYAAA-
Method	GET
Attack	
Evidence	Me_bKGbJk93GH-fYAAA-
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=NWf5_adIRpq6XRiUAAA5
Method	GET
Attack	
Evidence	NWf5_adIRpq6XRiUAAA5
Other	

Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=pQdzAuDtIJRC4tKRAABO
Method	GET
Attack	
Evidence	pQdzAuDtIJRC4tKRAABO
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=r0Gyydx5_nXCEI3-AAAi
Method	GET
Attack	
Evidence	r0Gyydx5_nXCEI3-AAAi
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=rgfE_I7RPl1LHFbFAABK
Method	GET
Attack	
Evidence	rgfE_I7RPl1LHFbFAABK
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=RHZWQ0DPD1TDDq8oAABS
Method	GET
Attack	
Evidence	RHZWQ0DPD1TDDq8oAABS
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=RSMsBj2nWSvCnbDbAAA2
Method	GET
Attack	
Evidence	RSMsBj2nWSvCnbDbAAA2
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=ruBBrVn9fE_F1wM-AAAa
Method	GET
Attack	
Evidence	ruBBrVn9fE_F1wM-AAAa
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=SdCA5TaV_EE9dy19AAAe
Method	GET
Attack	
Evidence	SdCA5TaV_EE9dy19AAAe

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=t3jFQ_asoWrzfGkqAAA8
Method	GET
Attack	
Evidence	t3jFQ_asoWrzfGkqAAA8
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=UeL35-cfUjXzywO9AAAw
Method	GET
Attack	
Evidence	UeL35-cfUjXzywO9AAAw
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=YsqTY6ctxcuAcjvwAAAk
Method	GET
Attack	
Evidence	YsqTY6ctxcuAcjvwAAAk
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=Zi_Slhms1STDM57iAAAH
Method	GET
Attack	
Evidence	Zi_Slhms1STDM57iAAAH
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNgoe&sid=2I5bMp82Z9dUQqfVAAAC
Method	POST
Attack	
Evidence	2I5bMp82Z9dUQqfVAAAC
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNjrf&sid=-mlVhTFFp9RS7Ff4AAAE
Method	POST
Attack	
Evidence	-mlVhTFFp9RS7Ff4AAAE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNrwa&sid=7K5VpH6acNpSwKXeAAAG
Method	POST
Attack	
Evidence	7K5VpH6acNpSwKXeAAAG

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNsZs&sid=Zi_Slhms1STDM57iAAAH
Method	POST
Attack	
Evidence	Zi_Slhms1STDM57iAAAH
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNwFT&sid=fX51XeedI4pt4YQJAAAK
Method	POST
Attack	
Evidence	fX51XeedI4pt4YQJAAAK
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNy3a&sid=Kwa8OeOh2pxuMSaVAAAM
Method	POST
Attack	
Evidence	Kwa8OeOh2pxuMSaVAAAM
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO-IB&sid=UeL35-cfUjXzywO9AAAw
Method	POST
Attack	
Evidence	UeL35-cfUjXzywO9AAAw
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO2D2&sid=bdeyXpKNMNcBpQAbAAAO
Method	POST
Attack	
Evidence	bdeyXpKNMNcBpQAbAAAO
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO5At&sid=kA4CWjF19xGageFyAAAQ
Method	POST
Attack	
Evidence	kA4CWjF19xGageFyAAAQ
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlObAs&sid=r0Gyydx5_nXCEI3-AAAi
Method	POST

Attack	
Evidence	r0Gyydx5_nXCEI3-AAAi
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOBZA&sid=06f47PLdT2QjJRdRAAAS
Method	POST
Attack	
Evidence	06f47PLdT2QjJRdRAAAS
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOEhG&sid=-rRTtWVV6yEWZkqNAAAU
Method	POST
Attack	
Evidence	-rRTtWVV6yEWZkqNAAAU
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOhlU&sid=YsqTY6ctxcuAcjvwAAAk
Method	POST
Attack	
Evidence	YsqTY6ctxcuAcjvwAAAk
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOiVN&sid=0BngYOnC9ZPURbtcAAAl
Method	POST
Attack	
Evidence	0BngYOnC9ZPURbtcAAAl
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOJih&sid=c8KIuezYgHSr0yHGAAAW
Method	POST
Attack	
Evidence	c8KIuezYgHSr0yHGAAAW
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOmD9&sid=a9JjFEvJao43zt6CAAAo
Method	POST
Attack	
Evidence	a9JjFEvJao43zt6CAAAo
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXlOMeM&sid=i6bdX8p1D0EFVnupAAAY
Method	POST
Attack	
Evidence	i6bdX8p1D0EFVnupAAAY
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOP46&sid=ruBBrVn9fE_F1wM-AAAa
Method	POST
Attack	
Evidence	ruBBrVn9fE_F1wM-AAAa
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOqDD&sid=JC1ekD_Zh9n659q9AAAq
Method	POST
Attack	
Evidence	JC1ekD_Zh9n659q9AAAq
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOQFF&sid=k6F6sgkqu7-F3mdHAAAc
Method	POST
Attack	
Evidence	k6F6sgkqu7-F3mdHAAAc
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOSVu&sid=SdCA5TaV_EE9dy19AAAe
Method	POST
Attack	
Evidence	SdCA5TaV_EE9dy19AAAe
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOVCY&sid=L4knAU540ljVTjTFAAAg
Method	POST
Attack	
Evidence	L4knAU540ljVTjTFAAAg
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOw_E&sid=E8bG5H88ZZu6x7DXAAAs
Method	POST
Attack	
Evidence	E8bG5H88ZZu6x7DXAAAs

Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOwJC&sid=drxMb855dSnsb3-0AAAt
Method	POST
Attack	
Evidence	drxMb855dSnsb3-0AAAt
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP1nf&sid=4tMqpwECVd3QYn6LAAAy
Method	POST
Attack	
Evidence	4tMqpwECVd3QYn6LAAAy
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP7wO&sid=B-VwIotrGvt_zZJgAAA0
Method	POST
Attack	
Evidence	B-VwIotrGvt_zZJgAAA0
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP9px&sid=RSMsBj2nWSvCnbDbAAA2
Method	POST
Attack	
Evidence	RSMsBj2nWSvCnbDbAAA2
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPg7v&sid=lOUKVOyvWg9SAcXBAABE
Method	POST
Attack	
Evidence	lOUKVOyvWg9SAcXBAABE
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPh0v&sid=F2Wh9nt7bXo9pSlVAABG
Method	POST
Attack	
Evidence	F2Wh9nt7bXo9pSlVAABG
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPhzC&sid=LHJ6ah5Z_SHnhYOIAABI
Method	POST

Attack	
Evidence	LHJ6ah5Z_SHnhYOIAABI
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPItZ&sid=NWf5_adIRpq6XRiUAAA5
Method	POST
Attack	
Evidence	NWf5_adIRpq6XRiUAAA5
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPJAr&sid=7DdeBruF0OwBhp67AAA4
Method	POST
Attack	
Evidence	7DdeBruF0OwBhp67AAA4
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPjw3&sid=rgfE_I7RPl1LHFbFAABK
Method	POST
Attack	
Evidence	rgfE_I7RPl1LHFbFAABK
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPlVT&sid=1Lt6h3A3eZVMp7NrAABM
Method	POST
Attack	
Evidence	1Lt6h3A3eZVMp7NrAABM
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPmMd&sid=pQdzAuDtIJRC4tKRAABO
Method	POST
Attack	
Evidence	pQdzAuDtIJRC4tKRAABO
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPnB8&sid=gtGYScX-WJR9eBWLAABQ
Method	POST
Attack	
Evidence	gtGYScX-WJR9eBWLAABQ
Other Info	
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXlPNP8&sid=t3jFQ_asoWrzfGkqAAA8
Method	POST
Attack	
Evidence	t3jFQ_asoWrzfGkqAAA8
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPo1v&sid=RHZWQ0DPD1TDDq8oAABS
Method	POST
Attack	
Evidence	RHZWQ0DPD1TDDq8oAABS
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPokU&sid=4sp63Er9EkvPF6aPAABU
Method	POST
Attack	
Evidence	4sp63Er9EkvPF6aPAABU
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPPdM&sid=Me_bKGbJk93GH-fYAAA-
Method	POST
Attack	
Evidence	Me_bKGbJk93GH-fYAAA-
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPWZx&sid=lng5-c-rNyDCFS5CAABA
Method	POST
Attack	
Evidence	lng5-c-rNyDCFS5CAABA
Other Info	
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPYQE&sid=BVad5NVM2JlZA8g9AABC
Method	POST
Attack	
Evidence	BVad5NVM2JlZA8g9AABC
Other Info	
Instances	188
Solution	For secure content, put session ID in a cookie. To be even more secure consider using a combination of cookie and URL rewrite.
Reference	https://seclists.org/webappsec/2002/q4/111
CWE Id	598

WASC Id	13
Plugin Id	3

Medium	Vulnerable JS Library
Description	The identified library appears to be vulnerable.
URL	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	/2.2.4/jquery.min.js
Other Info	The identified library jquery, version 2.2.4 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/advisories/GHSA-rmxg-73gg-4p98 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://github.com/jquery/jquery.com/issues/162 https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
Instances	1
Solution	Upgrade to the latest version of the affected library.
Reference	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
CWE Id	1395
WASC Id	
Plugin Id	10003

Low	Cross-Domain JavaScript Source File Inclusion
Description	The page includes one or more script files from a third-party domain.
URL	http://localhost:3000
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	
URL	http://localhost:3000
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	
URL	http://localhost:3000/

Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/assets/public/images/uploads/%E1%93%9A%E1%98%8F%E1%97%A2-
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/assets/public/images/uploads/%E1%93%9A%E1%98%8F%E1%97%A2-
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/favicon.ico
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	
URL	http://localhost:3000/favicon.ico
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	
URL	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	

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

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

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

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

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

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

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

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

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

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

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

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

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

Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	
URL	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
Instances	102
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	[829](829)
WASC Id	15
Plugin Id	[10017](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](497)
WASC Id	13
Plugin Id	[2](2)

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

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

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

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

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

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

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

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

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

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

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

Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 14:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 10:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 15:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 14:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 10:02:31.
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 15:10:37.
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 14:35:49.
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 10:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 15:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 14:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 10:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 15:10:37.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 14:35:49.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 10:02:31.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 15:10:37.

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

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

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

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

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

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

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

URL	http://localhost:3000/juice-shop/node_modules/serve-index/styles.css
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 10:02:31.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 15:10:37.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 14:35:49.
URL	http://localhost:3000/juice-shop/node_modules/serve-index/vendor.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 10:02:31.
URL	http://localhost:3000/main.js
Method	GET
Attack	
Evidence	1734944650
Other Info	1734944650, which evaluates to: 2024-12-23 03:04:10.
URL	http://localhost:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1969196030
Other Info	1969196030, which evaluates to: 2032-05-26 09:53:50.
URL	http://localhost:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1970691216
Other Info	1970691216, which evaluates to: 2032-06-12 17:13:36.
URL	http://localhost:3000/rest/products/search?q=
Method	GET

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

Evidence	1701244813
Other Info	1701244813, which evaluates to: 2023-11-29 02:00:13.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1818181818
Other Info	1818181818, which evaluates to: 2027-08-13 13:30:18.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1839622642
Other Info	1839622642, which evaluates to: 2028-04-17 17:17:22.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1863874346
Other Info	1863874346, which evaluates to: 2029-01-23 08:52:26.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1917098446
Other Info	1917098446, which evaluates to: 2030-10-01 10:20:46.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 14:35:49.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	2033195021
Other Info	2033195021, which evaluates to: 2034-06-06 03:23:41.
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	2038834951
Other	

Info	2038834951, which evaluates to: 2034-08-10 10:02:31.
Instances	168
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNg0y
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=PXlNgog&sid=2I5bMp82Z9dUQqfVAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNhTs&sid=2I5bMp82Z9dUQqfVAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNhYn&sid=2I5bMp82Z9dUQqfVAAAC
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNjG-
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=PXlNjtH&sid=-mlVhTFFp9RS7Ff4AAAE
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=PXlNkJJ&sid=-mlVhTFFp9RS7Ff4AAAE
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=PXlNrAU
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=PXlNrfx
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=PXlNrx1&sid=7K5VpH6acNpSwKXeAAAG
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client

	or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNsac&sid=Zi_Slhms1STDM57iAAAH
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNsmJ&sid=7K5VpH6acNpSwKXeAAAG
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNteT&sid=Zi_Slhms1STDM57iAAAH
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNtMP&sid=7K5VpH6acNpSwKXeAAAG
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNtOO&sid=Zi_Slhms1STDM57iAAAH
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNvy4
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=PXlNw-b&sid=fX51XeedI4pt4YQJAAAK
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNwep&sid=fX51XeedI4pt4YQJAAAK
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNwG5&sid=fX51XeedI4pt4YQJAAAK
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNxRe
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=PXlNy3z&sid=Kwa8OeOh2pxuMSaVAAAM
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNyTN&sid=Kwa8OeOh2pxuMSaVAAAM
Method	GET

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO-IP&sid=UeL35-cfUjXzywO9AAAw
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO-YT&sid=UeL35-cfUjXzywO9AAAw
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO0b-
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=PXlO2-k&sid=bdeyXpKNMNcBpQAbAAAO
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO2Dq&sid=bdeyXpKNMNcBpQAbAAAO
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO3Hw&sid=bdeyXpKNMNcBpQAbAAAO
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO4R8
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=PXlO5Az&sid=kA4CWjF19xGageFyAAAQ
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO5cR&sid=kA4CWjF19xGageFyAAAQ
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO5s9&sid=kA4CWjF19xGageFyAAAQ
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlO_5g&sid=UeL35-cfUjXzywO9AAAw
Method	GET
Attack	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOAjk
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=PXlObB3&sid=r0Gyydx5_nXCEI3-AAAi
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlObll&sid=r0Gyydx5_nXCEI3-AAAi
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlObWa&sid=r0Gyydx5_nXCEI3-AAAi
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOBZd&sid=06f47PLdT2QjJRdRAAAS
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOCGk&sid=06f47PLdT2QjJRdRAAAS
Method	GET

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlODjg
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=PXlOEiH&sid=-rRTtWVV6yEWZkqNAAAU
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOFYU&sid=-rRTtWVV6yEWZkqNAAAU
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOhd1
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=PXlOhla&sid=YsqTY6ctxcuAcjvwAAAk
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOhPj

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=PXlOiEA&sid=YsqTY6ctxcuAcjvwAAAk
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOiQ2&sid=YsqTY6ctxcuAcjvwAAAk
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOiq_&sid=0BngYOnC9ZPURbtcAAAl
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=PXlOiVo&sid=0BngYOnC9ZPURbtcAAAl
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=PXlOIwX
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=PXlOJjH&sid=c8KIuezYgHSr0yHGAAAW
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=PXlOK4P&sid=c8KIuezYgHSr0yHGAAAW
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=PXlOKHI&sid=c8KIuezYgHSr0yHGAAAW
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=PXlOlL5
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=PXlOmDk&sid=a9JjFEvJao43zt6CAAAo
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOMeb&sid=i6bdX8p1D0EFVnupAAAY
Method	GET
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOMEq
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=PXlOmlv&sid=a9JjFEvJao43zt6CAAAo
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOMvp&sid=i6bdX8p1D0EFVnupAAAY
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlONAQ&sid=i6bdX8p1D0EFVnupAAAY
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOOJa
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=PXlOP4X&sid=ruBBrVn9fE_F1wM-AAAa
Method	GET

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOpal
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=PXlOPgI
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=PXlOPXD&sid=ruBBrVn9fE_F1wM-AAAa
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOqE2&sid=JC1ekD_Zh9n659q9AAAq
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOQFx&sid=k6F6sgkqu7-F3mdHAAAc
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOQpI&sid=k6F6sgkqu7-

URL	F3mdHAAAc
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOqVu&sid=JC1ekD_Zh9n659q9AAAq
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlORuQ
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=PXlOSVw&sid=SdCA5TaV_EE9dy19AAAe
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOT8H&sid=SdCA5TaV_EE9dy19AAAe
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOUoX
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=PXlOVDz&sid=L4knAU540ljVTjTFAAAg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOvOC
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=PXlOvU0
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=PXlOw_M&sid=E8bG5H88ZZu6x7DXAAAs
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOWjT&sid=L4knAU540ljVTjTFAAAg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOwKB&sid=drxMb855dSnsb3-0AAAt
Method	GET
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOwun&sid=drxMb855dSnsb3-0AAAt
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOxBv&sid=E8bG5H88ZZu6x7DXAAAs
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOxJF&sid=E8bG5H88ZZu6x7DXAAAs
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOzbf
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=PXlOZUF
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=PXlP1A2
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=PXlP1np&sid=4tMqpwECVd3QYn6LAAAy
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP2Eg&sid=4tMqpwECVd3QYn6LAAAy
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP7UK
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=PXlP7we&sid=B-VwIotrGvt_zZJgAAA0
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP8mH&sid=B-VwIotrGvt_zZJgAAA0
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP8R5&sid=B-VwIotrGvt_zZJgAAA0

Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIP8vQ&sid=B-VwIotrGvt_zZJgAAA0
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIP9A0
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIP9q0&sid=RSMsBj2nWSvCnbDbAAA2
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPAM8&sid=RSMsBj2nWSvCnbDbAAA2
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXIPAS4&sid=RSMsBj2nWSvCnbDbAAA2
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client

	or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPfY3
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=PXlPg89&sid=lOUKVOyvWg9SAcXBAABE
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=PXlPghg&sid=lOUKVOyvWg9SAcXBAABE
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=PXlPgia
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=PXlPh0-&sid=F2Wh9nt7bXo9pSlVAABG
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=PXlPhE0&sid=F2Wh9nt7bXo9pSlVAABG
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=PXlPhhu
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=PXlPhzH&sid=LHJ6ah5Z_SHnhYOIAABI
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPilj&sid=LHJ6ah5Z_SHnhYOIAABI
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPIKC
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=PXlPIMS
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=PXlPIta&sid=NWf5_adIRpq6XRiUAAA5
Method	GET
Attack	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPJAU&sid=NWf5_adIRpq6XRiUAAA5
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPJBH&sid=7DdeBruF0OwBhp67AAA4
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPjFy
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=PXlPJIx&sid=NWf5_adIRpq6XRiUAAA5
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPJSH&sid=7DdeBruF0OwBhp67AAA4
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPjwO&sid=rgfE_I7RPl1LHFbFAABK

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=PXlPk5V&sid=rgfE_I7RPl1LHFbFAABK
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=PXlPl8R
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=PXlPlmI&sid=1Lt6h3A3eZVMp7NrAABM
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPluw
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=PXlPlVs&sid=1Lt6h3A3eZVMp7NrAABM
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPmOQ&sid=pQdzAuDtIJRC4tKRAABO
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=PXlPmSo&sid=pQdzAuDtIJRC4tKRAABO
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=PXlPMtQ
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=PXlPn1u
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=PXlPN_X&sid=t3jFQ_asoWrzfGkqAAA8
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPnBR&sid=gtGYScX-WJR9eBWLAABQ
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=PXlPndt&sid=gtGYScX-WJR9eBWLAABQ
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPnLw&sid=gtGYScX-WJR9eBWLAABQ
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPNQI&sid=t3jFQ_asoWrzfGkqAAA8
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPnrh
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=PXlPo25&sid=RHZWQ0DPD1TDDq8oAABS
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPob2
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=PXlPoCP&sid=RHZWQ0DPD1TDDq8oAABS
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPolS&sid=4sp63Er9EkvPF6aPAABU
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=PXlPOXI&sid=t3jFQ_asoWrzfGkqAAA8
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPoxn&sid=4sp63Er9EkvPF6aPAABU
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=PXlPOxq
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=PXlPPdb&sid=Me_bKGbJk93GH-fYAAA-
Method	GET

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPPrc&sid=Me_bKGbJk93GH-fYAAA-
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPWa5&sid=lng5-c-rNyDCFS5CAABA
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPWJD
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=PXlPY3-&sid=lng5-c-rNyDCFS5CAABA
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPY5y
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=PXlPY_f&sid=BVad5NVM2JlZA8g9AABC
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=PXlPYA4&sid=lng5-c-rNyDCFS5CAABA
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPYmv&sid=BVad5NVM2JlZA8g9AABC
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=PXlPYQH&sid=BVad5NVM2JlZA8g9AABC
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=PXlNgoe&sid=2I5bMp82Z9dUQqfVAAAC
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNjrf&sid=-mlVhTFFp9RS7Ff4AAAE
Method	POST
Attack	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlNrwa&sid=7K5VpH6acNpSwKXeAAAG
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=PXlNsZs&sid=Zi_Slhms1STDM57iAAAH
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=PXlNwFT&sid=fX51XeedI4pt4YQJAAAK
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=PXlNy3a&sid=Kwa8OeOh2pxuMSaVAAAM
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=PXlO-IB&sid=UeL35-cfUjXzywO9AAAw
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=PXlO2D2&sid=bdeyXpKNMNcBpQAbAAAO
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=PXlO5At&sid=kA4CWjF19xGageFyAAAQ
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlObAs&sid=r0Gyydx5_nXCEI3-AAAi
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOBZA&sid=06f47PLdT2QjJRdRAAAS
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOEhG&sid=-rRTtWVV6yEWZkqNAAAU
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOhlU&sid=YsqTY6ctxcuAcjvwAAAk
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOiVN&sid=0BngYOnC9ZPURbtcAAAl
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=PXlOJih&sid=c8KIuezYgHSr0yHGAAAW
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=PXlOmD9&sid=a9JjFEvJao43zt6CAAAo
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOMeM&sid=i6bdX8p1D0EFVnupAAAY
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOP46&sid=ruBBrVn9fE_F1wM-AAAa
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOqDD&sid=JC1ekD_Zh9n659q9AAAq
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=PXlOQFF&sid=k6F6sgkqu7-F3mdHAAAc
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOSVu&sid=SdCA5TaV_EE9dy19AAAe
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOVCY&sid=L4knAU540ljVTjTFAAAg
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOw_E&sid=E8bG5H88ZZu6x7DXAAAs
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlOwJC&sid=drxMb855dSnsb3-0AAAt
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP1nf&sid=4tMqpwECVd3QYn6LAAAy

Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP7wO&sid=B-VwIotrGvt_zZJgAAA0
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlP9px&sid=RSMsBj2nWSvCnbDbAAA2
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPg7v&sid=lOUKVOyvWg9SAcXBAABE
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=PXlPh0v&sid=F2Wh9nt7bXo9pSlVAABG
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=PXlPhzC&sid=LHJ6ah5Z_SHnhYOIAABI
Method	POST
Attack	
Evidence	
Other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPItZ&sid=NWf5_adIRpq6XRiUAAA5
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPJAr&sid=7DdeBruF0OwBhp67AAA4
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPjw3&sid=rgfE_I7RPl1LHFbFAABK
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=PXlPlVT&sid=1Lt6h3A3eZVMp7NrAABM
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPmMd&sid=pQdzAuDtIJRC4tKRAABO
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPnB8&sid=gtGYScX-WJR9eBWLAABQ
Method	POST
Attack	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPNP8&sid=t3jFQ_asoWrzfGkqAAA8
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPo1v&sid=RHZWQ0DPD1TDDq8oAABS
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPokU&sid=4sp63Er9EkvPF6aPAABU
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPPdM&sid=Me_bKGbJk93GH-fYAAA-
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PXlPWZx&sid=lng5-c-rNyDCFS5CAABA
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
	http://localhost:3000/socket.io/?

URL	EIO=4&transport=polling&t=PXlPYQE&sid=BVad5NVM2JlZA8g9AABC
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	188
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	Db
Other Info	The following pattern was used: \bDB\b and was detected in likely comment: "//,sb={},tb={}, ub="*/".concat("*"),vb=d.createElement("a");vb.href=jb.href;function wb(a){return function(b, c){"string"!=typeof ", see evidence field for the suspicious comment/snippet.
URL	http://localhost:3000/main.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//owasp. org' target='_blank'>Open Worldwide Application Security Project (OWASP)</a> and is developed and maintained by voluntee", see evidence field for the suspicious comment /snippet.
URL	http://localhost:3000/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&amp; color=%23ff5500&amp;auto&lowbar;play=true&amp;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 d="M0 256C0 397.4 114.6 512 256 512s256-114.6 256-256S397.4 0 256 0S0 114.6 0", see evidence field for the suspicious comment/snippet.
Instances	4
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	[615](615)
WASC Id	13
Plugin Id	[10027](10027)

Informational	Modern Web Application
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	http://localhost:3000
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/assets/public/images/uploads/%E1%93%9A%E1%98%8F%E1%97%A2-
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/favicon.ico
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/ftp/
Method	GET

Attack	
Evidence	<a href="">ftp</a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/main.js
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/polyfills.js
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/runtime.js
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/styles.css
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/build/routes/assets/public/vendor.js

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

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

Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/assets/public/vendor.js
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://localhost:3000/juice-shop/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.

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

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

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

URL	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	52
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Retrieved from Cache**
Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Method	GET
Attack	
Evidence	Age: 869750
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Method	GET
Attack	
Evidence	Age: 869796
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Method	GET
Attack	
Evidence	Age: 269082
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	http://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Method	GET
Attack	
Evidence	Age: 269129
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js

Method	GET
Attack	
Evidence	Age: 2321820
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	http://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	Age: 2321866
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	6
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	
WASC Id	
Plugin Id	10050