ZAP by Checkmarx Scanning Report

Sites: https://cdnjs.cloudflare.com https://juice-shop.herokuapp.com

Generated on Wed, 10 Dec 2025 07:36:21

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	6
Low	5
Informational	4

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	61
Cross-Domain Misconfiguration	Medium	98
Hidden File Found	Medium	2
Missing Anti-clickjacking Header	Medium	2
Session ID in URL Rewrite	Medium	8
Vulnerable JS Library	Medium	1
Cross-Domain JavaScript Source File Inclusion	Low	96
Private IP Disclosure	Low	1
Strict-Transport-Security Header Not Set	Low	105
Timestamp Disclosure - Unix	Low	289
X-Content-Type-Options Header Missing	Low	8
Information Disclosure - Suspicious Comments	Informational	3
Modern Web Application	Informational	49
Re-examine Cache-control Directives	Informational	33
Retrieved from Cache	Informational	6

Alert Detail

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	https://juice-shop.herokuapp.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/api/Quantitys/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/main.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/polyfills.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/runtime.js
Method	GET
Attack	

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

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

Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	

Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/layer.js:95:5
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/main.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/polyfills.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/runtime.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/vendor.js
Method	GET
Attack	
Evidence	
Other Info	

URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/main.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/polyfills.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/runtime.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/index.js:145:39

Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/main.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/polyfills.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/runtime.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/
Method	GET

Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/coupons_2013.md.bak
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/eastere.gg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/encrypt.pyc
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/package-lock.json.bak
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/package.json.bak
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/quarantine
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/suspicious_errors.yml
Method	GET
Attack	
Evidence	

Other Info	
URL	https://juice-shop.herokuapp.com/rest/products/search?q=
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EIk0&sid=hX-fC4f6a4dQXCsmAAE3
Method	POST
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ESNn&sid=RbvahvyzOLsNTuEWAAF1
Method	POST
Attack	
Evidence	
Other Info	
Instances	61
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
URL	https://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	https://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	https://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	https://juice-shop.herokuapp.com/
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/build/routes/fileServer.js:59:18
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://juice-shop.herokuapp.com/app/build/routes/main.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser

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

Info	authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
	The CORS misconfiguration on the web server permits cross-domain read requests from

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

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

Info	authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	98
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	**Hidden File Found**
Description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
URL	https://juice-shop.herokuapp.com/._darcs
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	https://juice-shop.herokuapp.com/BitKeeper
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other	

Info	
Instances	2
Solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.
Reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
CWE Id	538
WASC Id	13
Plugin Id	40035

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	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EIk0&sid=hX-fC4f6a4dQXCsmAAE3
Method	POST
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ESNn&sid=RbvahvyzOLsNTuEWAAF1
Method	POST
Attack	
Evidence	
Other Info	
Instances	2
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	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EIkC&sid=hX-fC4f6a4dQXCsmAAE3
Method	GET
Attack	
Evidence	hX-fC4f6a4dQXCsmAAE3

Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EJ7J&sid=hX-fC4f6a4dQXCsmAAE3
Method	GET
Attack	
Evidence	hX-fC4f6a4dQXCsmAAE3
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ESNv&sid=RbvahvyzOLsNTuEWAAF1
Method	GET
Attack	
Evidence	RbvahvyzOLsNTuEWAAF1
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ETPs&sid=RbvahvyzOLsNTuEWAAF1
Method	GET
Attack	
Evidence	RbvahvyzOLsNTuEWAAF1
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=websocket&sid=hX-fC4f6a4dQXCsmAAE3
Method	GET
Attack	
Evidence	hX-fC4f6a4dQXCsmAAE3
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=websocket&sid=RbvahvyzOLsNTuEWAAF1
Method	GET
Attack	
Evidence	RbvahvyzOLsNTuEWAAF1
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EIk0&sid=hX-fC4f6a4dQXCsmAAE3
Method	POST
Attack	
Evidence	hX-fC4f6a4dQXCsmAAE3
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ESNn&sid=RbvahvyzOLsNTuEWAAF1
Method	POST

Attack	
Evidence	RbvahvyzOLsNTuEWAAF1
Other Info	
Instances	8
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	https://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	https://juice-shop.herokuapp.com/
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	
URL	https://juice-shop.herokuapp.com/
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other	

Info	
URL	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	
	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public

URL	/polyfills.js
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	
URL	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/runtime.js
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	
URL	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	
	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/favicon_js.

URL	ico
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">< /script>
Other Info	
URL	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Other Info	
URL	https://juice-shop.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Other Info	
Instances	96
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

Low	**Private IP Disclosure**
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

URL	https://juice-shop.herokuapp.com/rest/admin/application-configuration
Method	GET
Attack	
Evidence	192.168.99.100:3000
Other Info	192.168.99.100:3000 192.168.99.100:4200
Instances	1
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP /PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Reference	https://tools.ietf.org/html/rfc1918
CWE Id	497
WASC Id	13
Plugin Id	2

Low	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://juice-shop.herokuapp.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/api/Challenges/?name=Score%20Board
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/api/Quantitys/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/favicon_js.ico
Method	GET
Attack	

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

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

Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/main.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/polyfills.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/runtime.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	

Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/layer.js:95:5
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/main.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/polyfills.js
Method	GET
Attack	
Evidence	
Other Info	

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

Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/index.js:145:39
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/main.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/polyfills.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/runtime.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/styles.css
Method	GET

Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/assets/i18n/en.json
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/assets/public/images/JuiceShop_Logo.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/assets/public/images/products/apple_juice.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/assets/public/images/products/apple_pressings.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/assets/public/images/products/artwork2.jpg
Method	GET
Attack	
Evidence	

Other Info	
URL	https://juice-shop.herokuapp.com/assets/public/images/products/banana_juice.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/assets/public/images/products/carrot_juice.jpeg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/assets/public/images/products/eggfruit_juice.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/assets/public/images/products/fan_facemask.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/assets/public/images/products/fruit_press.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/assets/public/images/products/green_smoothie.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/assets/public/images/products/lemon_juice.jpg
Method	GET
Attack	
Evidence	
Other Info	

URL	https://juice-shop.herokuapp.com/assets/public/images/products/melon_bike.jpeg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/assets/public/images/products/permafrost.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/font-mfizz.woff
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/acquisitions.md
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/announcement_encrypted.md
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/coupons_2013.md.bak
Method	GET

Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/eastere.gg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/encrypt.pyc
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/incident-support.kdbx
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/legal.md
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/package-lock.json.bak
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/package.json.bak
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/quarantine
Method	GET
Attack	

Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/quarantine/juicy_malware_linux_amd_64.url
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/quarantine/juicy_malware_linux_arm_64.url
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/quarantine/juicy_malware_macos_64.url
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/quarantine/juicy_malware_windows_64.exe.url
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/suspicious_errors.yml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/main.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/MaterialIcons-Regular.woff2
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://juice-shop.herokuapp.com/polyfills.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/rest/admin/application-configuration
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/rest/admin/application-version
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/rest/languages
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/rest/products/search?q=
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/rest/user/whoami
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/runtime.js

Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EIkC&sid=hX-fC4f6a4dQXCsmAAE3
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EIOc
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EJ7J&sid=hX-fC4f6a4dQXCsmAAE3
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ER_d
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ESNv&sid=RbvahvyzOLsNTuEWAAF1
Method	GET
Attack	
Evidence	
Other Info	
	https://juice-shop.herokuapp.com/socket.io/?

URL	EIO=4&transport=polling&t=Pi8ETPs&sid=RbvahvyzOLsNTuEWAAF1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=websocket&sid=hX-fC4f6a4dQXCsmAAE3
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=websocket&sid=RbvahvyzOLsNTuEWAAF1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EIk0&sid=hX-fC4f6a4dQXCsmAAE3
Method	POST
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ESNn&sid=RbvahvyzOLsNTuEWAAF1
Method	POST
Attack	
Evidence	
Other Info	

Instances	105
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://juice-shop.herokuapp.com/
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/
Method	GET
Attack	
Evidence	1765369473
Other Info	1765369473, which evaluates to: 2025-12-10 07:24:33.
URL	https://juice-shop.herokuapp.com/
Method	GET
Attack	
Evidence	1765369474
Other Info	1765369474, which evaluates to: 2025-12-10 07:24:34.
URL	https://juice-shop.herokuapp.com/

Method	GET
Attack	
Evidence	1765369516
Other Info	1765369516, which evaluates to: 2025-12-10 07:25:16.
URL	https://juice-shop.herokuapp.com/
Method	GET
Attack	
Evidence	1765369551
Other Info	1765369551, which evaluates to: 2025-12-10 07:25:51.
URL	https://juice-shop.herokuapp.com/api/Challenges/?name=Score%20Board
Method	GET
Attack	
Evidence	1765369522
Other Info	1765369522, which evaluates to: 2025-12-10 07:25:22.
URL	https://juice-shop.herokuapp.com/api/Quantitys/
Method	GET
Attack	
Evidence	1765369522
Other Info	1765369522, which evaluates to: 2025-12-10 07:25:22.
URL	https://juice-shop.herokuapp.com/api/Quantitys/
Method	GET
Attack	
Evidence	1765369583
Other Info	1765369583, which evaluates to: 2025-12-10 07:26:23.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	

Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1765369491
Other Info	1765369491, which evaluates to: 2025-12-10 07:24:51.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1765369490
Other Info	1765369490, which evaluates to: 2025-12-10 07:24:50.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/main.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/main.js
Method	GET
Attack	
Evidence	1981395349

Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/main.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/main.js
Method	GET
Attack	
Evidence	1765369491
Other Info	1765369491, which evaluates to: 2025-12-10 07:24:51.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/polyfills.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1765369491
Other Info	1765369491, which evaluates to: 2025-12-10 07:24:51.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/runtime.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.

URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/runtime.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/runtime.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/runtime.js
Method	GET
Attack	
Evidence	1765369491
Other Info	1765369491, which evaluates to: 2025-12-10 07:24:51.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/styles.css
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/styles.css
Method	GET
Attack	
Evidence	1765369491
Other Info	1765369491, which evaluates to: 2025-12-10 07:24:51.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/vendor.js
Method	GET

Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/vendor.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/vendor.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/build/routes/assets/public/vendor.js
Method	GET
Attack	
Evidence	1765369491
Other Info	1765369491, which evaluates to: 2025-12-10 07:24:51.
URL	https://juice-shop.herokuapp.com/app/build/routes/fileServer.js:43:13
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/build/routes/fileServer.js:43:13
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/build/routes/fileServer.js:43:13
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/build/routes/fileServer.js:43:13
Method	GET
Attack	

Evidence	1765369487
Other Info	1765369487, which evaluates to: 2025-12-10 07:24:47.
URL	https://juice-shop.herokuapp.com/app/build/routes/fileServer.js:59:18
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/build/routes/fileServer.js:59:18
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/build/routes/fileServer.js:59:18
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/build/routes/fileServer.js:59:18
Method	GET
Attack	
Evidence	1765369487
Other Info	1765369487, which evaluates to: 2025-12-10 07:24:47.
URL	https://juice-shop.herokuapp.com/app/build/routes/main.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/build/routes/main.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/build/routes/main.js
Method	GET
Attack	
Evidence	2038834951
Other	

Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/build/routes/main.js
Method	GET
Attack	
Evidence	1765369490
Other Info	1765369490, which evaluates to: 2025-12-10 07:24:50.
URL	https://juice-shop.herokuapp.com/app/build/routes/polyfills.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/build/routes/polyfills.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/build/routes/polyfills.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/build/routes/polyfills.js
Method	GET
Attack	
Evidence	1765369490
Other Info	1765369490, which evaluates to: 2025-12-10 07:24:50.
URL	https://juice-shop.herokuapp.com/app/build/routes/runtime.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/build/routes/runtime.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/build/routes/runtime.js

Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/build/routes/runtime.js
Method	GET
Attack	
Evidence	1765369490
Other Info	1765369490, which evaluates to: 2025-12-10 07:24:50.
URL	https://juice-shop.herokuapp.com/app/build/routes/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/build/routes/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/build/routes/styles.css
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/build/routes/styles.css
Method	GET
Attack	
Evidence	1765369490
Other Info	1765369490, which evaluates to: 2025-12-10 07:24:50.
URL	https://juice-shop.herokuapp.com/app/build/routes/vendor.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/build/routes/vendor.js
Method	GET

Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/build/routes/vendor.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/build/routes/vendor.js
Method	GET
Attack	
Evidence	1765369490
Other Info	1765369490, which evaluates to: 2025-12-10 07:24:50.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1765369491
Other Info	1765369491, which evaluates to: 2025-12-10 07:24:51.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/favicon_js.ico

Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1765369489
Other Info	1765369489, which evaluates to: 2025-12-10 07:24:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/main.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/main.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/main.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.

URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/main.js
Method	GET
Attack	
Evidence	1765369491
Other Info	1765369491, which evaluates to: 2025-12-10 07:24:51.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/polyfills.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1765369491
Other Info	1765369491, which evaluates to: 2025-12-10 07:24:51.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/runtime.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/runtime.js
Method	GET
Attack	

Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/runtime.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/runtime.js
Method	GET
Attack	
Evidence	1765369491
Other Info	1765369491, which evaluates to: 2025-12-10 07:24:51.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/styles.css
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/styles.css
Method	GET
Attack	
Evidence	1765369491
Other Info	1765369491, which evaluates to: 2025-12-10 07:24:51.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/vendor.js

Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/vendor.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/vendor.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/assets/public/vendor.js
Method	GET
Attack	
Evidence	1765369491
Other Info	1765369491, which evaluates to: 2025-12-10 07:24:51.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:280:10

Method	GET
Attack	
Evidence	1765369488
Other Info	1765369488, which evaluates to: 2025-12-10 07:24:48.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	1765369488
Other Info	1765369488, which evaluates to: 2025-12-10 07:24:48.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	

Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	1765369488
Other Info	1765369488, which evaluates to: 2025-12-10 07:24:48.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	1765369488
Other Info	1765369488, which evaluates to: 2025-12-10 07:24:48.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	1981395349

Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	1765369488
Other Info	1765369488, which evaluates to: 2025-12-10 07:24:48.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	1765369488
Other Info	1765369488, which evaluates to: 2025-12-10 07:24:48.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/layer.js:95:5
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.

URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/layer.js:95:5
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/layer.js:95:5
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/layer.js:95:5
Method	GET
Attack	
Evidence	1765369487
Other Info	1765369487, which evaluates to: 2025-12-10 07:24:47.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/main.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/main.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/main.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/main.js
Method	GET
Attack	
Evidence	1765369490
Other Info	1765369490, which evaluates to: 2025-12-10 07:24:50.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/polyfills.js
Method	GET

Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/polyfills.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/polyfills.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/polyfills.js
Method	GET
Attack	
Evidence	1765369489
Other Info	1765369489, which evaluates to: 2025-12-10 07:24:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/runtime.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/runtime.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/runtime.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/runtime.js
Method	GET
Attack	

Evidence	1765369489
Other Info	1765369489, which evaluates to: 2025-12-10 07:24:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/styles.css
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/styles.css
Method	GET
Attack	
Evidence	1765369489
Other Info	1765369489, which evaluates to: 2025-12-10 07:24:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/vendor.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/vendor.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/vendor.js
Method	GET
Attack	
Evidence	2038834951
Other	

Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/vendor.js
Method	GET
Attack	
Evidence	1765369489
Other Info	1765369489, which evaluates to: 2025-12-10 07:24:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1765369491
Other Info	1765369491, which evaluates to: 2025-12-10 07:24:51.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/favicon_js.ico
Method	GET
Attack	

Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1765369490
Other Info	1765369490, which evaluates to: 2025-12-10 07:24:50.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/main.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/main.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/main.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/main.js
Method	GET
Attack	
Evidence	1765369492
Other Info	1765369492, which evaluates to: 2025-12-10 07:24:52.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1650485437

Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/polyfills.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/polyfills.js
Method	GET
Attack	
Evidence	1765369492
Other Info	1765369492, which evaluates to: 2025-12-10 07:24:52.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/runtime.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/runtime.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/runtime.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/runtime.js
Method	GET
Attack	
Evidence	1765369492
Other Info	1765369492, which evaluates to: 2025-12-10 07:24:52.

URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/styles.css
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/styles.css
Method	GET
Attack	
Evidence	1765369492
Other Info	1765369492, which evaluates to: 2025-12-10 07:24:52.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/vendor.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/vendor.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/vendor.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/assets/public/vendor.js
Method	GET

Attack	
Evidence	1765369492
Other Info	1765369492, which evaluates to: 2025-12-10 07:24:52.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/index.js:145:39
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/index.js:145:39
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/index.js:145:39
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/index.js:145:39
Method	GET
Attack	
Evidence	1765369489
Other Info	1765369489, which evaluates to: 2025-12-10 07:24:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/main.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/main.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/main.js
Method	GET
Attack	

Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/main.js
Method	GET
Attack	
Evidence	1765369491
Other Info	1765369491, which evaluates to: 2025-12-10 07:24:51.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/polyfills.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/polyfills.js
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/polyfills.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/polyfills.js
Method	GET
Attack	
Evidence	1765369490
Other Info	1765369490, which evaluates to: 2025-12-10 07:24:50.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/runtime.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/runtime.js
Method	GET
Attack	
Evidence	1981395349
Other	

Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/runtime.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/runtime.js
Method	GET
Attack	
Evidence	1765369490
Other Info	1765369490, which evaluates to: 2025-12-10 07:24:50.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/styles.css
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/styles.css
Method	GET
Attack	
Evidence	1765369490
Other Info	1765369490, which evaluates to: 2025-12-10 07:24:50.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/vendor.js
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/vendor.js

Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/vendor.js
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/vendor.js
Method	GET
Attack	
Evidence	1765369491
Other Info	1765369491, which evaluates to: 2025-12-10 07:24:51.
URL	https://juice-shop.herokuapp.com/assets/i18n/en.json
Method	GET
Attack	
Evidence	1765369521
Other Info	1765369521, which evaluates to: 2025-12-10 07:25:21.
URL	https://juice-shop.herokuapp.com/assets/i18n/en.json
Method	GET
Attack	
Evidence	1765369561
Other Info	1765369561, which evaluates to: 2025-12-10 07:26:01.
URL	https://juice-shop.herokuapp.com/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1765369475
Other Info	1765369475, which evaluates to: 2025-12-10 07:24:35.
URL	https://juice-shop.herokuapp.com/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1765369521
Other Info	1765369521, which evaluates to: 2025-12-10 07:25:21.
URL	https://juice-shop.herokuapp.com/assets/public/favicon_js.ico
Method	GET

Attack	
Evidence	1765369560
Other Info	1765369560, which evaluates to: 2025-12-10 07:26:00.
URL	https://juice-shop.herokuapp.com/assets/public/images/JuiceShop_Logo.png
Method	GET
Attack	
Evidence	1765369522
Other Info	1765369522, which evaluates to: 2025-12-10 07:25:22.
URL	https://juice-shop.herokuapp.com/assets/public/images/JuiceShop_Logo.png
Method	GET
Attack	
Evidence	1765369566
Other Info	1765369566, which evaluates to: 2025-12-10 07:26:06.
URL	https://juice-shop.herokuapp.com/assets/public/images/products/apple_juice.jpg
Method	GET
Attack	
Evidence	1765369524
Other Info	1765369524, which evaluates to: 2025-12-10 07:25:24.
URL	https://juice-shop.herokuapp.com/assets/public/images/products/apple_pressings.jpg
Method	GET
Attack	
Evidence	1765369524
Other Info	1765369524, which evaluates to: 2025-12-10 07:25:24.
URL	https://juice-shop.herokuapp.com/assets/public/images/products/artwork2.jpg
Method	GET
Attack	
Evidence	1765369524
Other Info	1765369524, which evaluates to: 2025-12-10 07:25:24.
URL	https://juice-shop.herokuapp.com/assets/public/images/products/banana_juice.jpg
Method	GET
Attack	
Evidence	1765369524
Other Info	1765369524, which evaluates to: 2025-12-10 07:25:24.
URL	https://juice-shop.herokuapp.com/assets/public/images/products/carrot_juice.jpeg
Method	GET
Attack	
Evidence	1765369524

Other Info	1765369524, which evaluates to: 2025-12-10 07:25:24.
URL	https://juice-shop.herokuapp.com/assets/public/images/products/eggfruit_juice.jpg
Method	GET
Attack	
Evidence	1765369524
Other Info	1765369524, which evaluates to: 2025-12-10 07:25:24.
URL	https://juice-shop.herokuapp.com/assets/public/images/products/fan_facemask.jpg
Method	GET
Attack	
Evidence	1765369524
Other Info	1765369524, which evaluates to: 2025-12-10 07:25:24.
URL	https://juice-shop.herokuapp.com/assets/public/images/products/fruit_press.jpg
Method	GET
Attack	
Evidence	1765369524
Other Info	1765369524, which evaluates to: 2025-12-10 07:25:24.
URL	https://juice-shop.herokuapp.com/assets/public/images/products/green_smoothie.jpg
Method	GET
Attack	
Evidence	1765369524
Other Info	1765369524, which evaluates to: 2025-12-10 07:25:24.
URL	https://juice-shop.herokuapp.com/assets/public/images/products/lemon_juice.jpg
Method	GET
Attack	
Evidence	1765369524
Other Info	1765369524, which evaluates to: 2025-12-10 07:25:24.
URL	https://juice-shop.herokuapp.com/assets/public/images/products/melon_bike.jpeg
Method	GET
Attack	
Evidence	1765369524
Other Info	1765369524, which evaluates to: 2025-12-10 07:25:24.
URL	https://juice-shop.herokuapp.com/assets/public/images/products/permafrost.jpg
Method	GET
Attack	
Evidence	1765369524
Other Info	1765369524, which evaluates to: 2025-12-10 07:25:24.

URL	https://juice-shop.herokuapp.com/ftp
Method	GET
Attack	
Evidence	1765369475
Other Info	1765369475, which evaluates to: 2025-12-10 07:24:35.
URL	https://juice-shop.herokuapp.com/ftp/
Method	GET
Attack	
Evidence	1765369492
Other Info	1765369492, which evaluates to: 2025-12-10 07:24:52.
URL	https://juice-shop.herokuapp.com/ftp/acquisitions.md
Method	GET
Attack	
Evidence	1765369486
Other Info	1765369486, which evaluates to: 2025-12-10 07:24:46.
URL	https://juice-shop.herokuapp.com/ftp/announcement_encrypted.md
Method	GET
Attack	
Evidence	1765369486
Other Info	1765369486, which evaluates to: 2025-12-10 07:24:46.
URL	https://juice-shop.herokuapp.com/ftp/coupons_2013.md.bak
Method	GET
Attack	
Evidence	1765369486
Other Info	1765369486, which evaluates to: 2025-12-10 07:24:46.
URL	https://juice-shop.herokuapp.com/ftp/eastere.gg
Method	GET
Attack	
Evidence	1765369486
Other Info	1765369486, which evaluates to: 2025-12-10 07:24:46.
URL	https://juice-shop.herokuapp.com/ftp/encrypt.pyc
Method	GET
Attack	
Evidence	1765369486
Other Info	1765369486, which evaluates to: 2025-12-10 07:24:46.
URL	https://juice-shop.herokuapp.com/ftp/incident-support.kdbx
Method	GET

Attack	
Evidence	1765369487
Other Info	1765369487, which evaluates to: 2025-12-10 07:24:47.
URL	https://juice-shop.herokuapp.com/ftp/legal.md
Method	GET
Attack	
Evidence	1765369487
Other Info	1765369487, which evaluates to: 2025-12-10 07:24:47.
URL	https://juice-shop.herokuapp.com/ftp/package-lock.json.bak
Method	GET
Attack	
Evidence	1765369487
Other Info	1765369487, which evaluates to: 2025-12-10 07:24:47.
URL	https://juice-shop.herokuapp.com/ftp/package.json.bak
Method	GET
Attack	
Evidence	1765369487
Other Info	1765369487, which evaluates to: 2025-12-10 07:24:47.
URL	https://juice-shop.herokuapp.com/ftp/quarantine
Method	GET
Attack	
Evidence	1765369486
Other Info	1765369486, which evaluates to: 2025-12-10 07:24:46.
URL	https://juice-shop.herokuapp.com/ftp/quarantine/juicy_malware_linux_amd_64.url
Method	GET
Attack	
Evidence	1765369492
Other Info	1765369492, which evaluates to: 2025-12-10 07:24:52.
URL	https://juice-shop.herokuapp.com/ftp/quarantine/juicy_malware_linux_arm_64.url
Method	GET
Attack	
Evidence	1765369492
Other Info	1765369492, which evaluates to: 2025-12-10 07:24:52.
URL	https://juice-shop.herokuapp.com/ftp/quarantine/juicy_malware_macos_64.url
Method	GET
Attack	

Evidence	1765369492
Other Info	1765369492, which evaluates to: 2025-12-10 07:24:52.
URL	https://juice-shop.herokuapp.com/ftp/quarantine/juicy_malware_windows_64.exe.url
Method	GET
Attack	
Evidence	1765369492
Other Info	1765369492, which evaluates to: 2025-12-10 07:24:52.
URL	https://juice-shop.herokuapp.com/ftp/suspicious_errors.yml
Method	GET
Attack	
Evidence	1765369487
Other Info	1765369487, which evaluates to: 2025-12-10 07:24:47.
URL	https://juice-shop.herokuapp.com/main.js
Method	GET
Attack	
Evidence	1734944650
Other Info	1734944650, which evaluates to: 2024-12-23 04:04:10.
URL	https://juice-shop.herokuapp.com/main.js
Method	GET
Attack	
Evidence	1765369480
Other Info	1765369480, which evaluates to: 2025-12-10 07:24:40.
URL	https://juice-shop.herokuapp.com/main.js
Method	GET
Attack	
Evidence	1765369517
Other Info	1765369517, which evaluates to: 2025-12-10 07:25:17.
URL	https://juice-shop.herokuapp.com/main.js
Method	GET
Attack	
Evidence	1765369555
Other Info	1765369555, which evaluates to: 2025-12-10 07:25:55.
URL	https://juice-shop.herokuapp.com/polyfills.js
Method	GET
Attack	
Evidence	1765369480
Other	

Info	1765369480, which evaluates to: 2025-12-10 07:24:40.
URL	https://juice-shop.herokuapp.com/polyfills.js
Method	GET
Attack	
Evidence	1765369517
Other Info	1765369517, which evaluates to: 2025-12-10 07:25:17.
URL	https://juice-shop.herokuapp.com/polyfills.js
Method	GET
Attack	
Evidence	1765369555
Other Info	1765369555, which evaluates to: 2025-12-10 07:25:55.
URL	https://juice-shop.herokuapp.com/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1969196030
Other Info	1969196030, which evaluates to: 2032-05-26 10:53:50.
URL	https://juice-shop.herokuapp.com/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1970691216
Other Info	1970691216, which evaluates to: 2032-06-12 18:13:36.
URL	https://juice-shop.herokuapp.com/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1765369522
Other Info	1765369522, which evaluates to: 2025-12-10 07:25:22.
URL	https://juice-shop.herokuapp.com/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1765369523
Other Info	1765369523, which evaluates to: 2025-12-10 07:25:23.
URL	https://juice-shop.herokuapp.com/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1765369561
Other Info	1765369561, which evaluates to: 2025-12-10 07:26:01.
URL	https://juice-shop.herokuapp.com/rest/admin/application-configuration

Method	GET
Attack	
Evidence	1765369562
Other Info	1765369562, which evaluates to: 2025-12-10 07:26:02.
URL	https://juice-shop.herokuapp.com/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1765369563
Other Info	1765369563, which evaluates to: 2025-12-10 07:26:03.
URL	https://juice-shop.herokuapp.com/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1765369565
Other Info	1765369565, which evaluates to: 2025-12-10 07:26:05.
URL	https://juice-shop.herokuapp.com/rest/admin/application-version
Method	GET
Attack	
Evidence	1765369522
Other Info	1765369522, which evaluates to: 2025-12-10 07:25:22.
URL	https://juice-shop.herokuapp.com/rest/admin/application-version
Method	GET
Attack	
Evidence	1765369561
Other Info	1765369561, which evaluates to: 2025-12-10 07:26:01.
URL	https://juice-shop.herokuapp.com/rest/admin/application-version
Method	GET
Attack	
Evidence	1765369562
Other Info	1765369562, which evaluates to: 2025-12-10 07:26:02.
URL	https://juice-shop.herokuapp.com/rest/languages
Method	GET
Attack	
Evidence	1765369522
Other Info	1765369522, which evaluates to: 2025-12-10 07:25:22.
URL	https://juice-shop.herokuapp.com/rest/languages
Method	GET

Attack	
Evidence	1765369562
Other Info	1765369562, which evaluates to: 2025-12-10 07:26:02.
URL	https://juice-shop.herokuapp.com/rest/products/search?q=
Method	GET
Attack	
Evidence	1969196030
Other Info	1969196030, which evaluates to: 2032-05-26 10:53:50.
URL	https://juice-shop.herokuapp.com/rest/products/search?q=
Method	GET
Attack	
Evidence	1970691216
Other Info	1970691216, which evaluates to: 2032-06-12 18:13:36.
URL	https://juice-shop.herokuapp.com/rest/products/search?q=
Method	GET
Attack	
Evidence	1765369522
Other Info	1765369522, which evaluates to: 2025-12-10 07:25:22.
URL	https://juice-shop.herokuapp.com/rest/products/search?q=
Method	GET
Attack	
Evidence	1765369583
Other Info	1765369583, which evaluates to: 2025-12-10 07:26:23.
URL	https://juice-shop.herokuapp.com/rest/user/whoami
Method	GET
Attack	
Evidence	1765369574
Other Info	1765369574, which evaluates to: 2025-12-10 07:26:14.
URL	https://juice-shop.herokuapp.com/robots.txt
Method	GET
Attack	
Evidence	1765369474
Other Info	1765369474, which evaluates to: 2025-12-10 07:24:34.
URL	https://juice-shop.herokuapp.com/runtime.js
Method	GET
Attack	
Evidence	1765369480

Other Info	1765369480, which evaluates to: 2025-12-10 07:24:40.
URL	https://juice-shop.herokuapp.com/runtime.js
Method	GET
Attack	
Evidence	1765369517
Other Info	1765369517, which evaluates to: 2025-12-10 07:25:17.
URL	https://juice-shop.herokuapp.com/runtime.js
Method	GET
Attack	
Evidence	1765369554
Other Info	1765369554, which evaluates to: 2025-12-10 07:25:54.
URL	https://juice-shop.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	1765369474
Other Info	1765369474, which evaluates to: 2025-12-10 07:24:34.
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EIkC&sid=hX-fC4f6a4dQXCsmAAE3
Method	GET
Attack	
Evidence	1765369523
Other	

Info	1765369523, which evaluates to: 2025-12-10 07:25:23.
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EIOc
Method	GET
Attack	
Evidence	1765369521
Other Info	1765369521, which evaluates to: 2025-12-10 07:25:21.
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EJ7J&sid=hX-fC4f6a4dQXCsmAAE3
Method	GET
Attack	
Evidence	1765369524
Other Info	1765369524, which evaluates to: 2025-12-10 07:25:24.
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ER_d
Method	GET
Attack	
Evidence	1765369561
Other Info	1765369561, which evaluates to: 2025-12-10 07:26:01.
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ESNv&sid=RbvahvyzOLsNTuEWAAF1
Method	GET
Attack	
Evidence	1765369566
Other Info	1765369566, which evaluates to: 2025-12-10 07:26:06.
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ETPs&sid=RbvahvyzOLsNTuEWAAF1
Method	GET
Attack	
Evidence	1765369567
Other Info	1765369567, which evaluates to: 2025-12-10 07:26:07.
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=websocket&sid=hX-fC4f6a4dQXCsmAAE3
Method	GET
Attack	
Evidence	1765369523
Other Info	1765369523, which evaluates to: 2025-12-10 07:25:23.
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=websocket&sid=RbvahvyzOLsNTuEWAAF1
Method	GET
Attack	
Evidence	1765369564

Other Info	1765369564, which evaluates to: 2025-12-10 07:26:04.
URL	https://juice-shop.herokuapp.com/styles.css
Method	GET
Attack	
Evidence	1650485437
Other Info	1650485437, which evaluates to: 2022-04-20 16:10:37.
URL	https://juice-shop.herokuapp.com/styles.css
Method	GET
Attack	
Evidence	1680327869
Other Info	1680327869, which evaluates to: 2023-04-01 01:44:29.
URL	https://juice-shop.herokuapp.com/styles.css
Method	GET
Attack	
Evidence	1701244813
Other Info	1701244813, which evaluates to: 2023-11-29 03:00:13.
URL	https://juice-shop.herokuapp.com/styles.css
Method	GET
Attack	
Evidence	1818181818
Other Info	1818181818, which evaluates to: 2027-08-13 14:30:18.
URL	https://juice-shop.herokuapp.com/styles.css
Method	GET
Attack	
Evidence	1839622642
Other Info	1839622642, which evaluates to: 2028-04-17 18:17:22.
URL	https://juice-shop.herokuapp.com/styles.css
Method	GET
Attack	
Evidence	1863874346
Other Info	1863874346, which evaluates to: 2029-01-23 09:52:26.
URL	https://juice-shop.herokuapp.com/styles.css
Method	GET
Attack	
Evidence	1917098446
Other Info	1917098446, which evaluates to: 2030-10-01 11:20:46.

URL	https://juice-shop.herokuapp.com/styles.css
Method	GET
Attack	
Evidence	1981395349
Other Info	1981395349, which evaluates to: 2032-10-14 15:35:49.
URL	https://juice-shop.herokuapp.com/styles.css
Method	GET
Attack	
Evidence	2033195021
Other Info	2033195021, which evaluates to: 2034-06-06 04:23:41.
URL	https://juice-shop.herokuapp.com/styles.css
Method	GET
Attack	
Evidence	2038834951
Other Info	2038834951, which evaluates to: 2034-08-10 11:02:31.
URL	https://juice-shop.herokuapp.com/styles.css
Method	GET
Attack	
Evidence	1765369475
Other Info	1765369475, which evaluates to: 2025-12-10 07:24:35.
URL	https://juice-shop.herokuapp.com/styles.css
Method	GET
Attack	
Evidence	1765369518
Other Info	1765369518, which evaluates to: 2025-12-10 07:25:18.
URL	https://juice-shop.herokuapp.com/styles.css
Method	GET
Attack	
Evidence	1765369556
Other Info	1765369556, which evaluates to: 2025-12-10 07:25:56.
URL	https://juice-shop.herokuapp.com/vendor.js
Method	GET
Attack	
Evidence	1765369480
Other Info	1765369480, which evaluates to: 2025-12-10 07:24:40.
URL	https://juice-shop.herokuapp.com/vendor.js
Method	GET

Attack	
Evidence	1765369517
Other Info	1765369517, which evaluates to: 2025-12-10 07:25:17.
URL	https://juice-shop.herokuapp.com/vendor.js
Method	GET
Attack	
Evidence	1765369555
Other Info	1765369555, which evaluates to: 2025-12-10 07:25:55.
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EIk0&sid=hX-fC4f6a4dQXCsmAAE3
Method	POST
Attack	
Evidence	1765369523
Other Info	1765369523, which evaluates to: 2025-12-10 07:25:23.
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ESNn&sid=RbvahvyzOLsNTuEWAAF1
Method	POST
Attack	
Evidence	1765369564
Other Info	1765369564, which evaluates to: 2025-12-10 07:26:04.
Instances	289
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](497)
WASC Id	13
Plugin Id	[10096](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	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EIkC&sid=hX-fC4f6a4dQXCsmAAE3
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EIOc
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EJ7J&sid=hX-fC4f6a4dQXCsmAAE3
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ER_d
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ESNv&sid=RbvahvyzOLsNTuEWAAF1
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ETPs&sid=RbvahvyzOLsNTuEWAAF1
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EIk0&sid=hX-fC4f6a4dQXCsmAAE3
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	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ESNn&sid=RbvahvyzOLsNTuEWAAF1
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	8
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	https://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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/vendor.js
Method	GET
Attack	
Evidence	Query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//www.w3.org/2000/svg" viewBox="0 0 512 512"><path d="M0 256C0 397.4 114.6 512 256 512s256-114.6 256-256S397.4 0 256 0S0 114.6 0", see evidence field for the suspicious comment/snippet.

Instances	3
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

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

Info	web application.
URL	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"><

Evidence	/script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/app/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	https://juice-shop.herokuapp.com/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	https://juice-shop.herokuapp.com/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	49
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://juice-shop.herokuapp.com/
Method	GET
Attack	
Evidence	public, max-age=0

Other Info	
URL	https://juice-shop.herokuapp.com/api/Challenges/?name=Score%20Board
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/api/Quantitys/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/app/build/routes/fileServer.js:43:13
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://juice-shop.herokuapp.com/app/build/routes/fileServer.js:59:18
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:280:10
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:286:9
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:328:13
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	

URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:365:14
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:376:14
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/index.js:421:3
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/express/lib/router/layer.js:95:5
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://juice-shop.herokuapp.com/app/node_modules/serve-index/index.js:145:39
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://juice-shop.herokuapp.com/assets/i18n/en.json
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://juice-shop.herokuapp.com/ftp
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/
Method	GET

Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/acquisitions.md
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/announcement_encrypted.md
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/legal.md
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://juice-shop.herokuapp.com/ftp/quarantine
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/rest/admin/application-configuration
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/rest/admin/application-version
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/rest/languages
Method	GET
Attack	

Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/rest/products/search?q=
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/rest/user/whoami
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EIkC&sid=hX-fC4f6a4dQXCsmAAE3
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EIOc
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8EJ7J&sid=hX-fC4f6a4dQXCsmAAE3
Method	GET
Attack	
Evidence	

Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ER_d
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ESNv&sid=RbvahvyzOLsNTuEWAAF1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/socket.io/?EIO=4&transport=polling&t=Pi8ETPs&sid=RbvahvyzOLsNTuEWAAF1
Method	GET
Attack	
Evidence	
Other Info	
Instances	33
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

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	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Method	GET
Attack	
Evidence	Age: 1968918
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css

Method	GET
Attack	
Evidence	Age: 1968955
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Method	GET
Attack	
Evidence	Age: 1556180
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Method	GET
Attack	
Evidence	Age: 1556218
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	Age: 1831273
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	Age: 1831310
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