VulTURE Scan Report

Site: https://juice-shop.herokuapp.com

Generated on Sun, 7 Apr 2024

By Team DankBytes

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	3
Informational	3

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	2
Cross-Domain Misconfiguration	Medium	9
Cross-Domain JavaScript Source File Inclusion	Low	4
Strict-Transport-Security Header Not Set	Low	9
Timestamp Disclosure - Unix	Low	10
Information Disclosure - Suspicious Comments	Informational	2
Modern Web Application	Informational	2
Re-examine Cache-control Directives	Informational	3

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/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	2
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://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/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/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/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/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	9
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

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/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	4
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	**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/assets/public/favicon_js.ico
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/polyfills.js
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/styles.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://juice-shop.herokuapp.com/vendor.js
Method	GET
Attack	
Evidence	
Other Info	
Instances	9
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	1712444893
Other Info	1712444893, which evaluates to: 2024-04-07 04:38:13

URL	https://juice-shop.herokuapp.com/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	1712444894
Other Info	1712444894, which evaluates to: 2024-04-07 04:38:14
URL	https://juice-shop.herokuapp.com/main.js
Method	GET
Attack	
Evidence	1734944650
Other Info	1734944650, which evaluates to: 2024-12-23 14:34:10
URL	https://juice-shop.herokuapp.com/main.js
Method	GET
Attack	
Evidence	1712444894
Other Info	1712444894, which evaluates to: 2024-04-07 04:38:14
URL	https://juice-shop.herokuapp.com/polyfills.js
Method	GET
Attack	
Evidence	1712444894
Other Info	1712444894, which evaluates to: 2024-04-07 04:38:14
URL	https://juice-shop.herokuapp.com/robots.txt
Method	GET
Attack	
Evidence	1712444894
Other Info	1712444894, which evaluates to: 2024-04-07 04:38:14
URL	https://juice-shop.herokuapp.com/runtime.js
Method	GET
Attack	
Evidence	1712444894
Other Info	1712444894, which evaluates to: 2024-04-07 04:38:14
URL	https://juice-shop.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	1712444894
Other Info	1712444894, which evaluates to: 2024-04-07 04:38:14
URL	https://juice-shop.herokuapp.com/styles.css
Method	GET

Attack	
Evidence	1712444894
Other Info	1712444894, which evaluates to: 2024-04-07 04:38:14
URL	https://juice-shop.herokuapp.com/vendor.js
Method	GET
Attack	
Evidence	1712444894
Other Info	1712444894, which evaluates to: 2024-04-07 04:38:14
Instances	10
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	200
WASC Id	13
Plugin Id	10096

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
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 the element starting with: ""use strict";(self.webpackChunkfrontend=self.webpackChunkfrontend||[]).push([[179],{4550:(tt,K,c)=>{c.d(K,{e:()=>s});var k=c(234", 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 the element starting with: "(self.webpackChunkfrontend=self.webpackChunkfrontend||[]).push([[736],{9187:(At,ae,d)=>{"use strict";d.d(ae,{Xy:()=>X,ne:()=>Be,", see evidence field for the suspicious comment /snippet.
Instances	2
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	200
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/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	2
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/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	
Instances	3

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