ZAP Scanning Report JuiceShop

Site: http://localhost:3000

Generated on Wed, 19 Jan 2022 15:53:30

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	2
Informational	1

Alerts

Name	Risk Level	Number of Instances
Cross-Domain Misconfiguration	Medium	26
Cross-Domain JavaScript Source File Inclusion	Low	6
Timestamp Disclosure - Unix	Low	15
Information Disclosure - Suspicious Comments	Informational	3

Alert Detail

Medium	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	http://localhost:3000
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/assets/public/favicon_js.ico
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/ftp
Method	GET
Attack	

Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/ftp/
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/ftp/acquisitions.md
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/ftp/announcement_encrypted.md
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/ftp/coupons_2013.md.bak
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/ftp/eastere.gg
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/ftp/encrypt.pyc
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/ftp/incident-support.kdbx
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/ftp/legal.md
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/ftp/package.json.bak
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/ftp/quarantine
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *

URL	http://localhost:3000/ftp/quarantine/juicy_malware_linux_amd_64.url
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/ftp/quarantine/juicy_malware_linux_arm_64.url
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/ftp/quarantine/juicy_malware_macos_64.url
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/ftp/quarantine/juicy_malware_windows_64.exe.url
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/ftp/suspicious_errors.yml
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/main.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/polyfills.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/robots.txt
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/runtime.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/styles.css

Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost:3000/vendor.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Instances	26
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	http://localhost:3000
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://localhost:3000
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
URL	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://localhost:3000/sitemap.xml

Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Instances	6
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	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server - Unix
URL	http://localhost:3000/main.js
Method	GET
Attack	
Evidence	1734944650
URL	http://localhost:3000/main.js
Method	GET
Attack	
Evidence	384948954
URL	http://localhost:3000/main.js
Method	GET
Attack	
Evidence	435235279
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	00000005
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	00000024
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	00000042
URL	http://localhost:3000/styles.css
Method	GET
Attack	
Evidence	00000061
URL	http://localhost:3000/vendor.js

Method	GET
Attack	
Evidence	0000000004
URL	http://localhost:3000/vendor.js
Method	GET
Attack	
Evidence	0000000005
URL	http://localhost:3000/vendor.js
Method	GET
Attack	
Evidence	0000039834
URL	http://localhost:3000/vendor.js
Method	GET
Attack	
Evidence	0000051215
URL	http://localhost:3000/vendor.js
Method	GET
Attack	
Evidence	179464974
URL	http://localhost:3000/vendor.js
Method	GET
Attack	
Evidence	1801948466
URL	http://localhost:3000/vendor.js
Method	GET
Attack	
Evidence	1801949248
URL	http://localhost:3000/vendor.js
Method	GET
Attack	
Evidence	1803700518
Instances	15
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
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	http://localhost:3000/main.js

Method	GET
Attack	
Evidence	query
URL	http://localhost:3000/polyfills.js
Method	GET
Attack	
Evidence	select
URL	http://localhost:3000/vendor.js
Method	GET
Attack	
Evidence	query
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	200
WASC Id	13
Plugin Id	10027