JuiceShop

Site: http://juice_shop:3000

Generated on Mon, 19 Dec 2022 15:46:19

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	4
Informational	2
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	4
Cross-Domain Misconfiguration	Medium	18
Missing Anti-clickjacking Header	Medium	3
Session ID in URL Rewrite	Medium	12
Cross-Domain JavaScript Source File Inclusion	Low	2
Private IP Disclosure	Low	1
Timestamp Disclosure - Unix	Low	5
X-Content-Type-Options Header Missing	Low	12
Information Disclosure - Suspicious Comments	Informational	2
Modern Web Application	Informational	1

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	http://juice_shop:3000/
Method	GET
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh43ti&sid=jqYq_w-yWlwvY7wrAAAA

Method	POST
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh44dj&sid=dyQwWzAILtm-4YTPAAAC
Method	POST
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh457t&sid=YNcYj9Li73LgkyDcAAAE
Method	POST
Attack	
Evidence	
Instances	4
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
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 http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	http://juice_shop:3000/
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/api/Challenges/?name=Score%20Board
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/api/Quantitys/
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/api/SecurityQuestions/
Method	GET

Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/assets/i18n/en.json
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/main.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/MaterialIcons-Regular.woff2
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/polyfills.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/rest/admin/application-version
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/rest/languages
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/rest/products/search?q=
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/rest/user/whoami
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/runtime.js
Method	GET
Attack	

Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/styles.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/vendor.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/api/Users/
Method	POST
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://juice_shop:3000/rest/user/login
Method	POST
Attack	
Evidence	Access-Control-Allow-Origin: *
Instances	18
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14
Plugin Id	10098

Medium	**Missing Anti-clickjacking Header**
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh43ti&sid=jqYq_w-yWlwvY7wrAAAA
Method	POST
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh44dj&sid=dyQwWzAILtm-4YTPAAAC
Method	POST
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh457t&sid=YNcYj9Li73LgkyDcAAAE
Method	POST

Attack	
Evidence	
Instances	3
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Medium	**Session ID in URL Rewrite**
Description	URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site referer header. In addition, the session ID might be stored in browser history or server logs.
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh43tp&sid=jqYq_w-yWlwvY7wrAAAA
Method	GET
Attack	
Evidence	jqYq_w-yWlwvY7wrAAAA
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh43wg&sid=jqYq_w-yWlwvY7wrAAAA
Method	GET
Attack	
Evidence	jqYq_w-yWlwvY7wrAAAA
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh44dm&sid=dyQwWzAILtm-4YTPAAAC
Method	GET
Attack	
Evidence	dyQwWzAILtm-4YTPAAAC
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh44fp&sid=dyQwWzAILtm-4YTPAAAC
Method	GET
Attack	
Evidence	dyQwWzAILtm-4YTPAAAC
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh457x&sid=YNcYj9Li73LgkyDcAAAE
Method	GET
Attack	
Evidence	YNcYj9Li73LgkyDcAAAE
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh45At&sid=YNcYj9Li73LgkyDcAAAE
Method	GET
Attack	

Evidence	YNcYj9Li73LgkyDcAAAE
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=websocket&sid=dyQwWzAILtm-4YTPAAAC
Method	GET
Attack	
Evidence	dyQwWzAILtm-4YTPAAAC
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=websocket&sid=jqYq_w-yWlwvY7wrAAAA
Method	GET
Attack	
Evidence	jqYq_w-yWlwvY7wrAAAA
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=websocket&sid=YNcYj9Li73LgkyDcAAAE
Method	GET
Attack	
Evidence	YNcYj9Li73LgkyDcAAAE
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh43ti&sid=jqYq_w-yWlwvY7wrAAAA
Method	POST
Attack	
Evidence	jqYq_w-yWlwvY7wrAAAA
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh44dj&sid=dyQwWzAILtm-4YTPAAAC
Method	POST
Attack	
Evidence	dyQwWzAILtm-4YTPAAAC
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh457t&sid=YNcYj9Li73LgkyDcAAAE
Method	POST
Attack	
Evidence	YNcYj9Li73LgkyDcAAAE
Instances	12
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	http://seclists.org/lists/webappsec/2002/Oct-Dec/0111.html
CWE Id	200
WASC Id	13
Plugin Id	3

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

URL	http://juice_shop:3000/
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Instances	2
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

Low	**Private IP Disclosure**
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	http://juice_shop:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	192.168.99.100:3000
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	200
WASC Id	13
Plugin Id	2

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server - Unix
URL	http://juice_shop:3000/main.js
Method	GET
Attack	
Evidence	1734944650
URL	http://juice_shop:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1969196030
URL	http://juice_shop:3000/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1970691216
URL	http://juice_shop:3000/rest/products/search?q=
Method	GET

Attack	
Evidence	1969196030
URL	http://juice_shop:3000/rest/products/search?q=
Method	GET
Attack	
Evidence	1970691216
Instances	5
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

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh43kO
Method	GET
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh43tp&sid=jqYq_w-yWlwvY7wrAAAA
Method	GET
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh43wg&sid=jqYq_w-yWlwvY7wrAAAA
Method	GET
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh44dm&sid=dyQwWzAILtm-4YTPAAAC
Method	GET
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh44fp&sid=dyQwWzAILtm-4YTPAAAC
Method	GET
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh44V6

Method	GET
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh452L
Method	GET
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh457x&sid=YNcYj9Li73LgkyDcAAAE
Method	GET
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh45At&sid=YNcYj9Li73LgkyDcAAAE
Method	GET
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh43ti&sid=jqYq_w-yWlwvY7wrAAAA
Method	POST
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh44dj&sid=dyQwWzAILtm-4YTPAAAC
Method	POST
Attack	
Evidence	
URL	http://juice_shop:3000/socket.io/?EIO=4&transport=polling&t=OKh457t&sid=YNcYj9Li73LgkyDcAAAE
Method	POST
Attack	
Evidence	
Instances	12
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	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx 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. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	http://juice_shop:3000/main.js
Method	GET
Attack	
Evidence	query
URL	http://juice_shop:3000/vendor.js
Method	GET
Attack	
Evidence	query
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	http://juice_shop:3000/
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Instances	1
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109