OWASP ZAP Scan Report

Target: https://ticketing.celloscope.net/

All scanned sites: https://ticketing.celloscope.net

Javascript included from: https://ticketing.celloscope.net

Generated on Wed, 12 Jul 2023 04:29:44

ZAP Version: 2.12.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	3
Informational	1

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	4
Cross-Domain Misconfiguration	Medium	15
Missing Anti-clickjacking Header	Medium	4
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	16
Strict-Transport-Security Header Not Set	Low	16
X-Content-Type-Options Header Missing	Low	15
Re-examine Cache-control Directives	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://ticketing.celloscope.net/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/login

Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Instances	4
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 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	https://ticketing.celloscope.net/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://ticketing.celloscope.net/290.398e31b60046383b.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://ticketing.celloscope.net/300.1cc56f33f30909ec.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://ticketing.celloscope.net/672.9d920352c1fd2ddc.js

Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://ticketing.celloscope.net/769.f796cf1726f6779f.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://ticketing.celloscope.net/assets/i18n/en.json
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://ticketing.celloscope.net/login
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://ticketing.celloscope.net/main.c26cba6412f28117.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://ticketing.celloscope.net/manifest.webmanifest
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://ticketing.celloscope.net/polyfills.ab3e68abbbd6ed2e.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://ticketing.celloscope.net/Roboto-Bold.2a63183e6dff7d00.woff2
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://ticketing.celloscope.net/Roboto-Regular.4e7449338f3a9fee.woff2
Method	GET
Parameter	

Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://ticketing.celloscope.net/robots.txt
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://ticketing.celloscope.net/runtime.a7beccc95671831d.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://ticketing.celloscope.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Instances	15
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	https://ticketing.celloscope.net/
Method	GET
Parameter	X-Frame-Options
Attack	
Evidence	
URL	https://ticketing.celloscope.net/login
Method	GET
Parameter	X-Frame-Options
Attack	
Evidence	
URL	https://ticketing.celloscope.net/robots.txt
Method	GET
Parameter	X-Frame-Options
Attack	
Evidence	

URL	https://ticketing.celloscope.net/sitemap.xml
Method	GET
Parameter	X-Frame-Options
Attack	
Evidence	
Instances	4
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

Low	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	https://ticketing.celloscope.net/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://ticketing.celloscope.net/290.398e31b60046383b.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://ticketing.celloscope.net/300.1cc56f33f30909ec.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://ticketing.celloscope.net/672.9d920352c1fd2ddc.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://ticketing.celloscope.net/769.f796cf1726f6779f.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://ticketing.celloscope.net/api

Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://ticketing.celloscope.net/assets/i18n/en.json
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://ticketing.celloscope.net/login
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://ticketing.celloscope.net/main.c26cba6412f28117.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://ticketing.celloscope.net/manifest.webmanifest
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://ticketing.celloscope.net/polyfills.ab3e68abbbd6ed2e.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://ticketing.celloscope.net/Roboto-Bold.2a63183e6dff7d00.woff2
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://ticketing.celloscope.net/Roboto-Regular.4e7449338f3a9fee.woff2
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://ticketing.celloscope.net/robots.txt
Method	GET
Parameter	

Attack	
Evidence	nginx/1.24.0
URL	https://ticketing.celloscope.net/runtime.a7beccc95671831d.js
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
URL	https://ticketing.celloscope.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	nginx/1.24.0
Instances	16
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10036

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://ticketing.celloscope.net/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/290.398e31b60046383b.js
Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/300.1cc56f33f30909ec.js
Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/672.9d920352c1fd2ddc.js
Method	GET
Parameter	
Attack	

Evidence	
URL	https://ticketing.celloscope.net/769.f796cf1726f6779f.js
Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/api
Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/assets/i18n/en.json
Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/login
Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/main.c26cba6412f28117.js
Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/manifest.webmanifest
Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/polyfills.ab3e68abbbd6ed2e.js
Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/Roboto-Bold.2a63183e6dff7d00.woff2
Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/Roboto-Regular.4e7449338f3a9fee.woff2

Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/runtime.a7beccc95671831d.js
Method	GET
Parameter	
Attack	
Evidence	
URL	https://ticketing.celloscope.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Instances	16
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 http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

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://ticketing.celloscope.net/
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://ticketing.celloscope.net/290.398e31b60046383b.js
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://ticketing.celloscope.net/300.1cc56f33f30909ec.js

Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://ticketing.celloscope.net/672.9d920352c1fd2ddc.js
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://ticketing.celloscope.net/769.f796cf1726f6779f.js
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://ticketing.celloscope.net/assets/i18n/en.json
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://ticketing.celloscope.net/login
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://ticketing.celloscope.net/main.c26cba6412f28117.js
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://ticketing.celloscope.net/manifest.webmanifest
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://ticketing.celloscope.net/polyfills.ab3e68abbbd6ed2e.js
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://ticketing.celloscope.net/Roboto-Bold.2a63183e6dff7d00.woff2
Method	GET
Parameter	X-Content-Type-Options

Attack	
Evidence	
URL	https://ticketing.celloscope.net/Roboto-Regular.4e7449338f3a9fee.woff2
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://ticketing.celloscope.net/robots.txt
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://ticketing.celloscope.net/runtime.a7beccc95671831d.js
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	https://ticketing.celloscope.net/sitemap.xml
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
Instances	15
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	**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://ticketing.celloscope.net/
Method	GET
Parameter	Cache-Control
Attack	
Evidence	
URL	https://ticketing.celloscope.net/assets/i18n/en.json
Method	GET
Parameter	Cache-Control

Attack	
Evidence	
URL	https://ticketing.celloscope.net/login
Method	GET
Parameter	Cache-Control
Attack	
Evidence	
URL	https://ticketing.celloscope.net/manifest.webmanifest
Method	GET
Parameter	Cache-Control
Attack	
Evidence	
URL	https://ticketing.celloscope.net/robots.txt
Method	GET
Parameter	Cache-Control
Attack	
Evidence	
URL	https://ticketing.celloscope.net/sitemap.xml
Method	GET
Parameter	Cache-Control
Attack	
Evidence	
Instances	6
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