

Site: <https://www.example.com>

Generated on Sat, 19 Apr 2025 12:56:04

ZAP Version: 2.16.0

ZAP by [Checkmarx](#)

## Summary of Alerts

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

## Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

## Alerts

Name	Risk Level	Number of Instances
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	3
<a href="#">Missing Anti-clickjacking Header</a>	Medium	1
<a href="#">Strict-Transport-Security Header Not Set</a>	Low	3
<a href="#">X-Content-Type-Options Header Missing</a>	Low	1
<a href="#">Re-examine Cache-control Directives</a>	Informational	1

## Alert Detail

Medium	Content Security Policy (CSP) Header Not Set
--------	--

Description	<p>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.</p>		
URL	<a href="https://www.example.com">https://www.example.com</a>		
Method	GET		
Parameter			
Attack			
Evidence			
Other Info			
URL	<a href="https://www.example.com/robots.txt">https://www.example.com/robots.txt</a>		
Method	GET		
Parameter			
Attack			
Evidence			
Other Info			
URL	<a href="https://www.example.com/sitemap.xml">https://www.example.com/sitemap.xml</a>		
Method	GET		
Parameter			
Attack			
Evidence			
Other Info			
Instances	3		
Solution	<p>Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.</p>		

Reference	<a href="https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy">https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy</a>	
	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html</a>	
	<a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a>	
	<a href="https://w3c.github.io/webappsec-csp/">https://w3c.github.io/webappsec-csp/</a>	
	<a href="https://web.dev/articles/csp">https://web.dev/articles/csp</a>	
	<a href="https://caniuse.com/#feat=contentsecuritypolicy">https://caniuse.com/#feat=contentsecuritypolicy</a>	
	<a href="https://content-security-policy.com/">https://content-security-policy.com/</a>	
CWE Id	<a href="#">693</a>	
WASC Id	15	
Plugin Id	<a href="#">10038</a>	
<b>Medium</b>	<b>Missing Anti-clickjacking Header</b>	
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	<a href="https://www.example.com">https://www.example.com</a>	
Method	GET	
Parameter	x-frame-options	
Attack		
Evidence		
Other Info		
Instances	1	
	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.	
Solution	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	<a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</a>	
CWE Id	<a href="#">1021</a>	
WASC Id	15	
Plugin Id	<a href="#">10020</a>	
<b>Low</b>	<b>Strict-Transport-Security Header Not Set</b>	
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	<a href="https://www.example.com">https://www.example.com</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="https://www.example.com/robots.txt">https://www.example.com/robots.txt</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="https://www.example.com/sitemap.xml">https://www.example.com/sitemap.xml</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	3
Solution	<p>Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.</p> <p><a href="https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html</a></p>
Reference	<p><a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a></p> <p><a href="https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security">https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security</a></p> <p><a href="https://caniuse.com/stricttransportsecurity">https://caniuse.com/stricttransportsecurity</a></p> <p><a href="https://datatracker.ietf.org/doc/html/rfc6797">https://datatracker.ietf.org/doc/html/rfc6797</a></p>
CWE Id	<a href="#">319</a>
WASC Id	15
Plugin Id	<a href="#">10035</a>

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	<a href="https://www.example.com">https://www.example.com</a>	
	Method	GET	
	Parameter	x-content-type-options	
	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	1		
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	<a href="https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/c">https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/c</a>		
	<a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a>		
CWE Id	<a href="#">693</a>		
WASC Id	15		
Plugin Id	<a href="#">10021</a>		
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	<a href="https://www.example.com">https://www.example.com</a>	
	Method	GET	
	Parameter	cache-control	
	Attack		

Evidence	max-age=1252
Other Info	
Instances	1
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	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching">https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching</a> <a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control</a> <a href="https://grayduck.mn/2021/09/13/cache-control-recommendations/">https://grayduck.mn/2021/09/13/cache-control-recommendations/</a>
CWE Id	<a href="#">525</a>
WASC Id	13
Plugin Id	<a href="#">10015</a>

## Sequence Details

With the associated active scan results.