

Site: <https://saucedemo.com>

Generated on Sat, 19 Apr 2025 13:11:15

ZAP Version: 2.16.0

ZAP by [Checkmarx](#)

## Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	2
Informational	4
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	1
<a href="#">Cross-Domain Misconfiguration</a>	Medium	1
<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="#">Modern Web Application</a>	Informational	1
<a href="#">Re-examine Cache-control Directives</a>	Informational	1
<a href="#">Retrieved from Cache</a>	Informational	3
<a href="#">User Agent Fuzzer</a>	Informational	24

## 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	<a href="https://saucedemo.com">https://saucedemo.com</a>		
Method	GET		
Parameter			
Attack			
Evidence			
Other Info			
Instances	1		
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.		
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>		
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	<a href="https://saucedemo.com">https://saucedemo.com</a>		
Method	GET		
Parameter			
Attack			
Evidence	Access-Control-Allow-Origin: *		

Other Info	<p>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.</p>		
Instances	<p>1</p> <p>Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).</p>		
Solution	<p>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.</p>		
Reference	<p><a href="https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy">https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy</a></p>		
CWE Id	<p><a href="#">264</a></p>		
WASC Id	<p>14</p>		
Plugin Id	<p><a href="#">10098</a></p>		
<b>Medium</b>	<b>Missing Anti-clickjacking Header</b>		
Description	<p>The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.</p>		
URL	<p><a href="https://saucedemo.com">https://saucedemo.com</a></p>		
Method	<p>GET</p>		
Parameter	<p>x-frame-options</p>		
Attack			
Evidence			
Other Info			
Instances	<p>1</p> <p>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.</p>		
Solution	<p>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.</p>		
Reference	<p><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></p>		
CWE Id	<p><a href="#">1021</a></p>		

WASC Id	15
Plugin Id	<a href="#">10020</a>
<b>Low</b>	<b>Strict-Transport-Security Header Not Set</b>
Description	<p>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.</p>
URL	<a href="https://saucedemo.com">https://saucedemo.com</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="https://saucedemo.com/robots.txt">https://saucedemo.com/robots.txt</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="https://saucedemo.com/sitemap.xml">https://saucedemo.com/sitemap.xml</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Reference <https://owasp.org/www-community/Security-Headers>  
[https://en.wikipedia.org/wiki/HTTP\\_Strict\\_Transport\\_Security](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 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://saucedemo.com>

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

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.

Solution 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 <https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/>  
<https://owasp.org/www-community/Security-Headers>

CWE Id [693](#)

WASC Id 15

Plugin Id [10021](#)

**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	<a href="https://saucedemo.com">https://saucedemo.com</a>		
Method	GET		
Parameter			
Attack			
Evidence	<script type="text/javascript">!function(n){if("/")===n.search[1]){var a=n.search.slice(1).split("&").map((function(n){return n.replace(/~and~/g,"%&"))).join("?");window.history.replaceState(null,null,n.pathname.slice(0,-1)+a+n.hash		
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.		
Instances	1		
Solution	This is an informational alert and so no changes are required.		
Reference			
CWE Id			
WASC Id			
Plugin Id	<a href="#">10109</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://saucedemo.com">https://saucedemo.com</a>		
Method	GET		
Parameter	cache-control		
Attack			
Evidence	max-age=600		
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".		

[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)

Reference

<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](#)

Informational

Retrieved from Cache

Description

The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

URL

<https://saucedemo.com>

Method

GET

Parameter

Attack

Evidence

HIT

Other  
Info

URL

<https://saucedemo.com/robots.txt>

Method

GET

Parameter

Attack

Evidence

Age: 0

Other  
Info

The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL

<https://saucedemo.com/sitemap.xml>

Method

GET

Parameter

Attack

Evidence

Age: 0

	Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	3	<p>Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:</p> <p>Cache-Control: no-cache, no-store, must-revalidate, private</p>
Solution	<p>Pragma: no-cache</p> <p>Expires: 0</p> <p>This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.</p>	
Reference	<p><a href="https://tools.ietf.org/html/rfc7234">https://tools.ietf.org/html/rfc7234</a></p> <p><a href="https://tools.ietf.org/html/rfc7231">https://tools.ietf.org/html/rfc7231</a></p> <p><a href="https://www.rfc-editor.org/rfc/rfc9110.html">https://www.rfc-editor.org/rfc/rfc9110.html</a></p>	
CWE Id		
WASC Id		
Plugin Id	<a href="#">10050</a>	
<b>Informational      User Agent Fuzzer</b>		
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.	
URL	<a href="https://saucedemo.com/robots.txt">https://saucedemo.com/robots.txt</a>	
Method	GET	
Parameter	Header User-Agent	
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)	
Evidence		
Other Info		
URL	<a href="https://saucedemo.com/robots.txt">https://saucedemo.com/robots.txt</a>	
Method	GET	
Parameter	Header User-Agent	



Attack Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)

Evidence

Other  
Info

URL <https://saucedemo.com/robots.txt>

Method GET

Parameter Header User-Agent

Attack Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

Evidence

Other  
Info

URL <https://saucedemo.com/robots.txt>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko

Evidence

Other  
Info

URL <https://saucedemo.com/robots.txt>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0

Evidence

Other  
Info

URL <https://saucedemo.com/robots.txt>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/91.0.4472.124 Safari/537.36

Evidence

Other  
Info

URL <https://saucedemo.com/robots.txt>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0

Evidence

Other  
Info

URL <https://saucedemo.com/robots.txt>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Evidence

Other  
Info

URL <https://saucedemo.com/robots.txt>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)

Evidence

Other  
Info

URL <https://saucedemo.com/robots.txt>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8\_0\_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4

Evidence

Other  
Info

URL <https://saucedemo.com/robots.txt>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3\_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16

Evidence

Other  
Info

URL <https://saucedemo.com/robots.txt>

Method GET

Parameter Header User-Agent

Attack msnbot/1.1 (+http://search.msn.com/msnbot.htm)

Evidence

Other  
Info

URL <https://saucedemo.com/sitemap.xml>

Method GET

Parameter Header User-Agent

Attack Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Evidence

Other  
Info

URL <https://saucedemo.com/sitemap.xml>

Method GET

Parameter Header User-Agent

Attack Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)

Evidence

Other  
Info

URL <https://saucedemo.com/sitemap.xml>

Method GET

Parameter Header User-Agent

Attack Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

Evidence

Other  
Info

URL <https://saucedemo.com/sitemap.xml>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko

Evidence

Other  
Info

URL <https://saucedemo.com/sitemap.xml>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0

Evidence

Other  
Info

URL <https://saucedemo.com/sitemap.xml>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/91.0.4472.124 Safari/537.36

Evidence

Other  
Info

URL <https://saucedemo.com/sitemap.xml>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0

Evidence

Other  
Info

URL <https://saucedemo.com/sitemap.xml>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Evidence

Other  
Info

URL <https://saucedemo.com/sitemap.xml>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)

Evidence

Other  
Info

URL <https://saucedemo.com/sitemap.xml>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (iPhone; CPU iPhone OS 8\_0\_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4

Evidence

Other  
Info

URL <https://saucedemo.com/sitemap.xml>

Method GET

Parameter Header User-Agent

Attack Mozilla/5.0 (iPhone; U; CPU iPhone OS 3\_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16

Evidence

Other  
Info

URL	<a href="https://saucedemo.com/sitemap.xml">https://saucedemo.com/sitemap.xml</a>
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	24
Solution	
Reference	<a href="https://owasp.org/wstg">https://owasp.org/wstg</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10104</a>

Sequence Details

With the associated active scan results.