ZAP Report

Site: http://192.168.1.120:5173

Generated on Wed, 23 Apr 2025 21:18:10

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	1
Informational	3
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
Content Security Policy (CSP) Header Not Set	Medium	2
Missing Anti-clickjacking Header	Medium	2
X-Content-Type-Options Header Missing	Low	5
Information Disclosure - Suspicious Comments	Informational	2
Modern Web Application	Informational	4
User Agent Fuzzer	Informational	18

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://192.168.1.120:5173
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://192.168.1.120:5173/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	2
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 https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Missing Anti-clickjacking Header**
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	http://192.168.1.120:5173
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://192.168.1.120:5173/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	

Instances	2
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	**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://192.168.1.120:5173
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.
URL	http://192.168.1.120:5173/
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.
URL	http://192.168.1.120:5173/app/entry.client.tsx
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.
URL	http://192.168.1.120:5173/app/root.tsx

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.
URL	http://192.168.1.120:5173/app/routes/_index.tsx
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	5
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	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) 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.
URL	http://192.168.1.120:5173
Method	GET
Parameter	
Attack	
Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected in likely comment: "//tailwindcss.com\n*//*\n1. Prevent padding and border from affecting element width. (https://github.com/mozdevs/cssremedy/issue", see evidence field for the suspicious comment/snippet.
URL	http://192.168.1.120:5173/
Method	GET
Parameter	
Attack	

Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected in likely comment: "//tailwindcss.com\n*//*\n1. Prevent padding and border from affecting element width. (https://github.com/mozdevs/cssremedy/issue", see evidence field for the suspicious comment/snippet.
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	[615](615)
WASC Id	13
Plugin Id	[10027](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://192.168.1.120:5173
Method	GET
Parameter	
Attack	
Evidence	<script>((STORAGE_KEY, restoreKey) => { if (!window.history.state || !window.history.state.key) { let key = Math.random().toString(32).slice(2); window.history.replaceState({ key }, ""); } try { let positions = JSON.parse(sessionStorage.getItem(STORAGE_KEY) || "{}"); let storedY = positions[restoreKey || window.history.state.key]; if (typeof storedY === "number") { window.scrollTo(0, storedY); } } catch (error) { console.error(error); sessionStorage.removeItem(STORAGE_KEY); } })("positions", null)</script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://192.168.1.120:5173/
Method	GET
Parameter	
Attack	
Evidence	<script>((STORAGE_KEY, restoreKey) => { if (!window.history.state || !window.history.state.key) { let key = Math.random().toString(32).slice(2); window.history.replaceState({ key }, ""); } try { let positions = JSON.parse(sessionStorage.getItem(STORAGE_KEY) || "{}"); let storedY = positions[restoreKey || window.history.state.key]; if (typeof storedY === "number") { window.scrollTo(0, storedY); } } catch (error) { console.error(error); sessionStorage.removeItem(STORAGE_KEY); } })("positions", null)</script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://192.168.1.120:5173/robots.txt
Method	GET
Parameter	
Attack	
Evidence	<script> console.log("💿 Hey developer 👋. You can provide a way better UX than this when your app throws errors. Check out https://remix.run/guides/errors for more information."); </script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.

URL	http://192.168.1.120:5173/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	<script> console.log("💿 Hey developer 👋. You can provide a way better UX than this when your app throws errors. Check out https://remix.run/guides/errors for more information."); </script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	4
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**User Agent Fuzzer**
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	http://192.168.1.120:5173
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://192.168.1.120:5173
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	http://192.168.1.120:5173
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://192.168.1.120:5173/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Evidence	
Other Info	
URL	http://192.168.1.120:5173/
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	http://192.168.1.120:5173/
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://192.168.1.120:5173/app
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://192.168.1.120:5173/app
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	http://192.168.1.120:5173/app
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://192.168.1.120:5173/app/routes
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://192.168.1.120:5173/app/routes

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	http://192.168.1.120:5173/app/routes
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://192.168.1.120:5173/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	http://192.168.1.120:5173/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	http://192.168.1.120:5173/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://192.168.1.120:5173/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	http://192.168.1.120:5173/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	http://192.168.1.120:5173/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	18
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

Sequence Details

With the associated active scan results.