ZAP Scanning Report

Sites: http://localhost:8080 http://localhost:3000

Generated on Fri, 3 Nov 2023 17:38:10

ZAP Version: 2.14.0

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	2
Low	1
Informational	2

Alerts

Name	Risk Level	Number of Instances
Cloud Metadata Potentially Exposed	High	1
Content Security Policy (CSP) Header Not Set	Medium	9
Missing Anti-clickjacking Header	Medium	9
X-Content-Type-Options Header Missing	Low	15
Information Disclosure - Suspicious Comments	Informational	1
Modern Web Application	Informational	9

Alert Detail

High	Cloud Metadata Potentially Exposed
Description	The Cloud Metadata Attack attempts to abuse a misconfigured NGINX server in order to access the instance metadata maintained by cloud service providers such as AWS, GCP and Azure. All of these providers provide metadata via an internal unroutable IP address '169.254.169.254' - this can be exposed by incorrectly configured NGINX servers and accessed by using this IP address in the Host header field.
URL	http://localhost:3000/latest/meta-data/
Method	GET
Attack	169.254.169.254
Evidence	
Other Info	Based on the successful response status code cloud metadata may have been returned in the response. Check the response data to see if any cloud metadata has been returned. The meta data returned can include information that would allow an attacker to completely compromise the system.
Instances	1

Solution	Do not trust any user data in NGINX configs. In this case it is probably the use of the $host variable which is set from the 'Host' header and can be controlled by an attacker.
Reference	https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/
CWE Id	
WASC Id	
Plugin Id	90034

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://localhost:3000
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/latest
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/latest/meta-data
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/latest/meta-data/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/sitemap.xml
Method	GET

Attack	
Evidence	
Other Info	
URL	http://localhost:3000/static
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/static/css
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/static/js
Method	GET
Attack	
Evidence	
Other Info	
Instances	9
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	**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://localhost:3000
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/

Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/latest
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/latest/meta-data
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/latest/meta-data/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/static
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/static/css
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:3000/static/js
Method	GET

Attack	
Evidence	
Other Info	
Instances	9
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://localhost:3000
Method	GET
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://localhost:3000/
Method	GET
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://localhost:3000/favicon.ico
Method	GET
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://localhost:3000/latest
Method	GET
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://localhost:3000/latest/meta-data
Method	GET
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://localhost:3000/latest/meta-data/
Method	GET
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://localhost:3000/logo192.png
Method	GET
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://localhost:3000/manifest.json
Method	GET
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://localhost:3000/robots.txt
Method	GET
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://localhost:3000/sitemap.xml
Method	GET
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://localhost:3000/static
Method	GET
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://localhost:3000/static/css
Method	GET
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://localhost:3000/static/css/main.6b3b8193.css
Method	GET
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://localhost:3000/static/js
Method	GET
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://localhost:3000/static/js/main.ad937bd7.js
Method	GET
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	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	**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://localhost:3000/static/js/main.ad937bd7.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "!function(){var e={426:function(e,t,n){(e=n.nmd(e)).exports=function(){"use strict";var t,n;function r(){return t.apply(null,arg", see evidence field for the suspicious comment/snippet.
Instances	1
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://localhost:3000
Method	GET
Attack	
Evidence	<script defer="defer" src="/static/js/main.ad937bd7.js"></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://localhost:3000/
Method	GET
Attack	
Evidence	<script defer="defer" src="/static/js/main.ad937bd7.js"></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://localhost:3000/latest
Method	GET
Attack	
Evidence	<script defer="defer" src="/static/js/main.ad937bd7.js"></script>
Other	No links have been found while there are scripts, which is an indication that this is a modern

Info	web application.
URL	http://localhost:3000/latest/meta-data
Method	GET
Attack	
Evidence	<script defer="defer" src="/static/js/main.ad937bd7.js"></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://localhost:3000/latest/meta-data/
Method	GET
Attack	
Evidence	<script defer="defer" src="/static/js/main.ad937bd7.js"></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://localhost:3000/sitemap.xml
Method	GET
Attack	
Evidence	<script defer="defer" src="/static/js/main.ad937bd7.js"></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://localhost:3000/static
Method	GET
Attack	
Evidence	<script defer="defer" src="/static/js/main.ad937bd7.js"></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://localhost:3000/static/css
Method	GET
Attack	
Evidence	<script defer="defer" src="/static/js/main.ad937bd7.js"></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://localhost:3000/static/js
Method	GET
Attack	
Evidence	<script defer="defer" src="/static/js/main.ad937bd7.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	9
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109