ZAP by Checkmarx Scanning Report

Site: http://localhost:4200

Generated on Sat, 14 Dec 2024 05:33:19

ZAP Version: 2.15.0

ZAP by Checkmarx

Summary of Alerts

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

Alerts

Name	Risk Level	Number of Instances
Cloud Metadata Potentially Exposed	High	1
Hidden File Found	Medium	4

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:4200/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	**Hidden File Found**
Description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
URL	http://localhost:4200/._darcs
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	http://localhost:4200/.bzr
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	http://localhost:4200/.hg
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	http://localhost:4200/BitKeeper
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
Instances	4
Solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.
Reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
CWE Id	538
WASC Id	13
Plugin Id	40035