ZAP Scanning Report

Site: https://u9w3fmdh1h.execute-api.us-east-1.amazonaws.com

Generated on Mon, 5 Aug 2024 23:25:07

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

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

Alerts

Name	Risk Level	Number of Instances
Strict-Transport-Security Header Not Set	Low	1

Alert Detail

Low	Strict-Transport-Security Header Not Set
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	https://u9w3fmdh1h.execute-api.us-east-1.amazonaws.com/prd/orders-mgmt/api/v1/orders/df26e5ca-6bb9-49c3-82d4-a75d36b0afd9/payment
Method	POST
Attack	
Evidence	
Other Info	
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers 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