ZAP Scanning Report

Site: http://a8eb728894f8d401e905ecb6ed2bbb5d-1568986704.us-east-1.elb.amazonaws.com

Generated on sáb, 27 jul 2024 13:53:37

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Nível de Risco	Number of Alerts
Alto	0
Médio	0
Baixo	1
Informativo	0

Alertas

Nome	Nível de Risco	Number of Instances
X-Content-Type-Options Header Missing	Baixo	2

Alert Detail

Baixo	X-Content-Type-Options Header Missing
Descrição	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://a8eb728894f8d401e905ecb6ed2bbb5d-1568986704.us-east-1.elb.amazonaws.com/pedido/api/produtos
Método	GET
Ataque	
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://a8eb728894f8d401e905ecb6ed2bbb5d-1568986704.us-east-1.elb.amazonaws.com/pedido/api/pedidos/checkout
Método	POST
Ataque	
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	2
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