

ZAP Scanning Report

Site: <http://localhost:8089>

Generated on dom, 17 mar 2024 21:42:10

ZAP Version: 2.14.0

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	1

Alertas

Nome	Nível de Risco	Number of Instances
X-Content-Type-Options Header Missing	Baixo	1
User Agent Fuzzer	Informativo	12

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://localhost:8089/webhooks/pagamentos-confirmados/2
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	1
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

Informativo	User Agent Fuzzer
Descrição	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://localhost:8089/webhooks/pagamentos-confirmados/2
Método	POST
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:8089/webhooks/pagamentos-confirmados/2
Método	POST
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:8089/webhooks/pagamentos-confirmados/2
Método	POST
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:8089/webhooks/pagamentos-confirmados/2
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:8089/webhooks/pagamentos-confirmados/2
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://localhost:8089/webhooks/pagamentos-confirmados/2
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	

Other Info	
URL	http://localhost:8089/webhooks/pagamentos-confirmados/2
Método	POST
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:8089/webhooks/pagamentos-confirmados/2
Método	POST
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:8089/webhooks/pagamentos-confirmados/2
Método	POST
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:8089/webhooks/pagamentos-confirmados/2
Método	POST
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://localhost:8089/webhooks/pagamentos-confirmados/2
Método	POST
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://localhost:8089/webhooks/pagamentos-confirmados/2
Método	POST
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	12
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	

Plugin Id

[10104](#)