⚡ ZAP Scanning Report

Site: http://localhost:3000

Generated on Sun, 17 Mar 2024 20:49:08

ZAP Version: 2.14.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	2
Informational	1

Alerts

Name	Risk Level	Number of Instances
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	4
X-Content-Type-Options Header Missing	Low	4
User Agent Fuzzer	Informational	12

Alert Detail

Low	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	http://localhost:3000/pedidos
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost:3000/produtos
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost:3000/pedidos

Method	POST	
Attack		
Evidence	X-Powered-By: Express	
Other Info		
URL	http://localhost:3000/pedidos/3/solicitar-pagamento	
Method	POST	
Attack		
Evidence	X-Powered-By: Express	
Other Info		
Instances	4	
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.	
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html	
CWE Id	200	
WASC Id	13	
Plugin Id	10037	

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/pedidos	
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/produtos	
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/pedidos	
Method	POST	
Attack		
Evidence		
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still	

Other Info	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/pedidos/3/solicitar-pagamento
Method	POST
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	4
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	User Agent Fuzzer
Description	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:3000/pedidos
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://localhost:3000/pedidos
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://localhost:3000/pedidos
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://localhost:3000/pedidos
Method	POST

	Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
	Evidence	
	Other Info	
URL		http://localhost:3000/pedidos
	Method	POST
	Attack	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:3000/pedidos
	Method	POST
	Attack	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:3000/pedidos
	Method	POST
	Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
	Evidence	
	Other Info	
URL		http://localhost:3000/pedidos
	Method	POST
	Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
	Evidence	
	Other Info	
URL		http://localhost:3000/pedidos
	Method	POST
	Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
	Evidence	
	Other Info	
URL		http://localhost:3000/pedidos
	Method	POST
	Attack	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:3000/pedidos
	Method	POST

	Attack	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:3000/pedidos
	Method	POST
	Attack	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