



# Fast N Foodious - Pedido

Site: <http://localhost:3001>

Generated on Sun, 3 Mar 2024 07:54:36

ZAP Version: 2.14.0

## Summary of Alerts

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

## Alerts

Name	Risk Level	Number of Instances
<a href="#">Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)</a>	Low	1
<a href="#">X-Content-Type-Options Header Missing</a>	Low	1

## 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	<a href="http://localhost:3001/v1/pedido/checkout/6">http://localhost:3001/v1/pedido/checkout/6</a>
Method	POST
Attack	
Evidence	X-Powered-By: Express
Other Info	
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	<a href="https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework">https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework</a> <a href="https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html">https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html</a>
CWE Id	<a href="#">200</a>
WASC Id	13
Plugin Id	<a href="#">10037</a>

Low	<b>X-Content-Type-Options Header Missing</b>
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	<a href="http://localhost:3001/v1/pedido/checkout/6">http://localhost:3001/v1/pedido/checkout/6</a>
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	1
Solution	<p>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.</p> <p>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.</p>
Reference	<a href="https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)">https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)</a> <a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10021</a>