ZAP Scanning Report

Site: http://localhost:3000

Generated on sex, 8 mar 2024 20:57:39

ZAP Version: 2.14.0

Summary of Alerts

Nível de Risco	Number of Alerts
Alto	0
Médio	0
Baixo	3
Informativo	0

Alertas

Nome	Nível de Risco	Number of Instances
Divulgação de Data e Hora - Unix	Baixo	1
O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By"	Baixo	3
X-Content-Type-Options Header Missing	Baixo	1

Alert Detail

Baixo	**Divulgação de Data e Hora - Unix**
Descrição	Um carimbo de data/hora foi divulgado pela aplicação/servidor web - Unix
URL	http://localhost:3000/produtos
Método	GET
Ataque	
Evidence	1561041695
Other Info	1561041695, que avalia: 2019-06-20 11:41:35
Instances	1
Solution	Confirme manualmente se os dados do carimbo de data/hora não são confidenciais e se os dados não podem ser agregados para divulgar padrões exploráveis.
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Plugin Id	10096

Baixo	**O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By"**

Descrição	O servidor da web/aplicativo está vazando informações por meio de um ou mais cabeçalhos de resposta HTTP "X-Powered-By". O acesso a essas informações pode facilitar que os invasores identifiquem outras estruturas/componentes dos quais seu aplicativo da web depende e as vulnerabilidades às quais esses componentes podem estar sujeitos.
URL	http://localhost:3000/produtos
Método	GET
Ataque	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost:3000/robots.txt
Método	GET
Ataque	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost:3000/sitemap.xml
Método	GET
Ataque	
Evidence	X-Powered-By: Express
Other Info	
Instances	3
Solution	Certifique-se de que seu servidor web, servidor de aplicativos, balanceador de carga, etc. esteja configurado para suprimir cabeçalhos "X-Powered-By".
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

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:3000/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.
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