ZAP Scanning Report handmatig

Site: https://192.168.0.142

Generated on Mon, 3 Jun 2024 17:23:00

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	13
Missing Anti-clickjacking Header	Medium	13

Alert Detail

Medium	Content Security Policy (CSP) Header Not Set
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://192.168.0.142/E-cars4U/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/car-huren.php?auto_id=24
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/dashboard-anonymous.php
Method	GET

Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/dashboard-anonymous.php?zoeken=linux
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/dashboard-landlords.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/dashboard-landlords.php?delete_id=25
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/index.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/index.php?message=logged_out
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/index.php?success=login_complete
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/index.php?success=registration_complete
Method	GET
Attack	
Evidence	

Other Info	
URL	https://192.168.0.142/E-cars4U/login.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/register.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/top-cheaper-cars.php
Method	GET
Attack	
Evidence	
Other Info	
Instances	13
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Missing Anti-clickjacking Header**
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	https://192.168.0.142/E-cars4U/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/car-huren.php?auto_id=24
Method	GET
Attack	

Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/dashboard-anonymous.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/dashboard-anonymous.php?zoeken=linux
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/dashboard-landlords.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/dashboard-landlords.php?delete_id=25
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/index.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/index.php?message=logged_out
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/index.php?success=login_complete
Method	GET
Attack	
Evidence	

Other Info	
URL	https://192.168.0.142/E-cars4U/index.php?success=registration_complete
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/login.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/register.php
Method	GET
Attack	
Evidence	
Other Info	
URL	https://192.168.0.142/E-cars4U/top-cheaper-cars.php
Method	GET
Attack	
Evidence	
Other Info	
Instances	13
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020