ZAP by Checkmarx Scanning Report

: http://automationexercise.com

, 28 . 2025 03:36:34

ZAP Version: 2.16.1

ZAP by Checkmarx

🟥	0
🟧	1
🟨	3
🟦	2

Content Security Policy (CSP)	🟧	1
Cookie No HttpOnly Flag	🟨	1
JavaScript	🟨	1
HTTP- "X-Powered-By"	🟨	3
Session Management Response Identified	🟦	1
-	🟦	1

	Content Security Policy (CSP)
	(CSP) — , , (XSS) . : . CSP HTTP-, - , . JavaScript, CSS, HTML-, , , Java. ActiveX, .
URL-	http://automationexercise.com/
	GET
	1
	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

	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	693
WASC ID	15
	10038

	Cookie No HttpOnly Flag
	cookie HttpOnly, , JavaScript. , cookie . cookie , .
URL-	http://automationexercise.com/
	GET
	Set-Cookie: csrftoken
	1
	, cookie HttpOnly.
	https://owasp.org/www-community/HttpOnly
CWE	1004
WASC ID	13
	10010

	JavaScript
	.
URL-	http://automationexercise.com/
	GET
	<script async src="https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js?client=ca-pub-1677597403311019" crossorigin="anonymous"></script>
	1
	, JavaScript , .
CWE	829
WASC ID	15
	10017

	HTTP- "X-Powered-By"
	- / HTTP- «X-Powered-By». / ,

	-, , .
URL-	http://automationexercise.com/
	GET
	X-Powered-By: Phusion Passenger(R) 6.0.23
URL-	http://automationexercise.com/robots.txt
	GET
	X-Powered-By: Phusion Passenger(R) 6.0.23
URL-	http://automationexercise.com/sitemap.xml
	GET
	X-Powered-By: Phusion Passenger(R) 6.0.23
	3
	, -, , . . «X-Powered-By».
	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE	497
WASC ID	13
	10037

	Session Management Response Identified
	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL-	http://automationexercise.com/
	GET
	hHURAFbYA2CKfavDXhFub8Isa4N9RuXww2ca0k8dErqP2ogLt3nV8bXaJEU8jTp5
	cookie:csrftoken
	1
	This is an informational alert rather than a vulnerability and so there is nothing to fix.
	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE	
WASC ID	
	10112

	-
	-. , Ajax Spider , .
URL-	http://automationexercise.com/
	GET
	<a data-product-id="1" class="btn btn-default add-to-cart"><i class="fa fa-shopping-cart"></i>Add to cart</a>
	, href, , -.
	1
	, .
CWE	
WASC ID	
	10109