TASK-2

Arpit Mathur

Scanning Report Summary

Automatic vulnerability scanner- OWASP ZAP Test web application URL - http://zero.webappsecurity.com/

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	1 (14.3%)	3 (42.9%)	1 (14.3%)	5 (71.4%)
	Low	0 (0.0%)	0 (0.0%)	1 (14.3%)	0 (0.0%)	1 (14.3%)
	Informational	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (14.3%)	1 (14.3%)
	Total	0 (0.0%)	1 (14.3%)	4 (57.1%)	2 (28.6%)	7 (100%)

Vulnerability name- Content Security Policy (CSP) Header not set

Alert tags	▪ OWASP_2021_A05 ▪ OWASP_2017_A06
Alert 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.

Request	▾ Request line and header section (214 bytes)
	
	`GET http://zero.webappsecurity.com/ HTTP/1.1`
	`Host: zero.webappsecurity.com`
	`User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0`
	`Pragma: no-cache`
	`Cache-Control: no-cache`
	
	▾ Request body (0 bytes)

Response	▾ Status line and header section (242 bytes)
	
	`HTTP/1.1 200 OK`
	`Date: Thu, 19 May 2022 09:42:24 GMT`
	`Server: Apache-Coyote/1.1`
	`Access-Control-Allow-Origin: *`
	`Cache-Control: no-cache, max-age=0, must-revalidate, no-store`
	`Content-Type: text/html;charset=UTF-8`
	`Content-Language: en-US`
	
	▸ Response body (12471 bytes)

Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.

My Report

- **Test web application name** - http://zero.webappsecurity.com/
- **Vulnerability name**- Content Security Policy (CSP) Header not set
- **About Vulnerability**- A Content Protection Policy (CSP) is a security standard that provides an additional layer of protection from cross site scripting, clickjacking and other code injection attacks. It is a defensive measure against any attacks that rely on executing malicious content in a trusted web context. CSP provides a set of HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page.
- **Impact**- Due to this vulnerability, web application is vulnerable to cross site scripting(**XSS**) , **clickjacking** , **SQL injection** and other data injection attacks. These attacks can be oriented for everything from data theft to site defacement or distribution of malware.
- **Solution-** This vulnerability can be removed by ensuring that the web server, application server etc. are configured to set the content security policy header, so that the web application along with its content and server is not compromised. This also assures the safety of the web application users.