

Project 2:

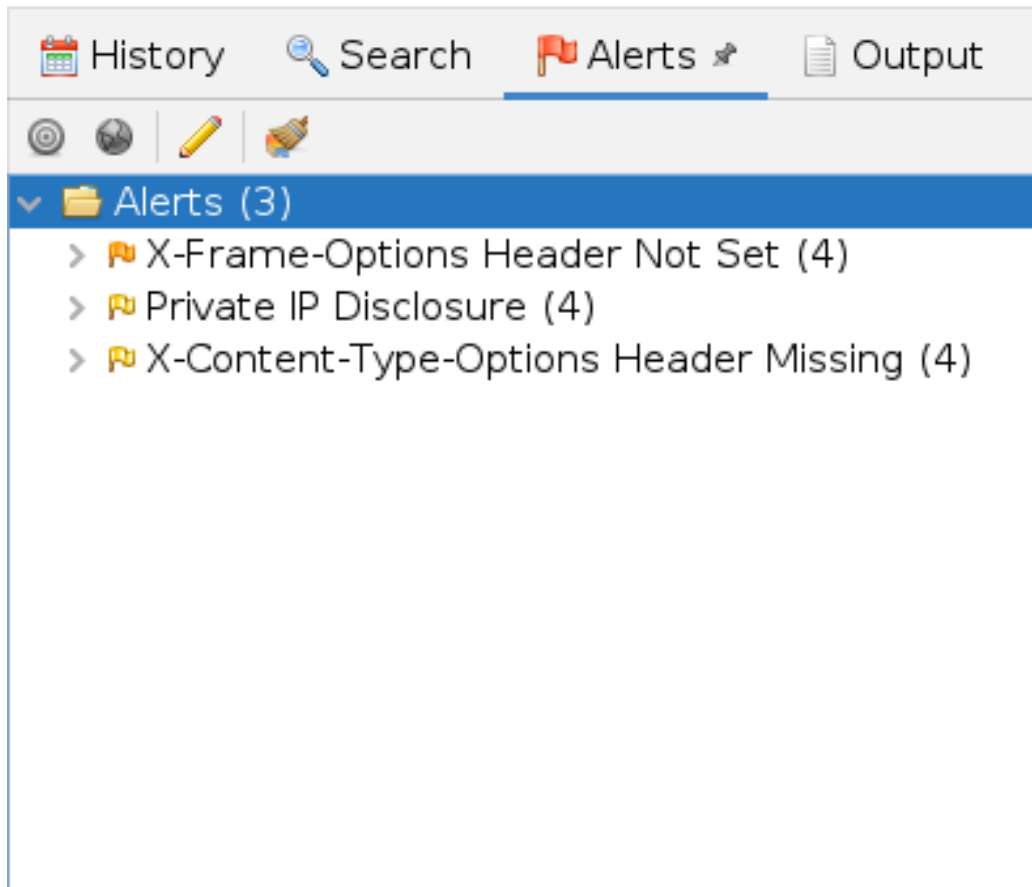
Task 1: Take some website (vulnerable website) , can using OWASP ZAP Tool (quick/automated) .Set of vulnerabilities - [?] make a report with mitigation's

I take testfier.net and initially i am going to set the url in the URL to attack box and ready for scanning as follow:-

The screenshot shows the OWASP ZAP interface with the 'Automated Scan' dialog box open. The URL to attack is set to 'http://testfier.net/'. The scan progress bar is at 100%. Below the dialog box, the 'Sent Messages' tab is active, displaying a list of HTTP requests.

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
1,198	08/04/22, 11:52:52 PM	08/04/22, 11:52:52 PM	GET	http://172.29.0.1:8090/robots.txt	200	OK	8 ms	74 bytes	196 bytes
1,199	08/04/22, 11:52:53 PM	08/04/22, 11:52:53 PM	GET	http://testfier.net/itemap.xml?name=abc	200	Please login.	6 ms	74 bytes	196 bytes
1,200	08/04/22, 11:52:53 PM	08/04/22, 11:52:53 PM	GET	http://172.29.0.1:8090/javascript/cyberoamAjax.js	200	OK	21 ms	78 bytes	8,067 bytes
1,201	08/04/22, 11:52:53 PM	08/04/22, 11:52:53 PM	GET	http://172.29.0.1:8090/css/captiveportal.css?ver=1...	200	OK	24 ms	62 bytes	11,902 bytes
1,202	08/04/22, 11:52:53 PM	08/04/22, 11:52:53 PM	GET	http://172.29.0.1:8090/httpclient.html	200	OK	11 ms	79 bytes	4,773 bytes
1,203	08/04/22, 11:52:53 PM	08/04/22, 11:52:53 PM	GET	http://172.29.0.1:8090/javascript/validation/httpclie...	200	OK	10 ms	78 bytes	15,336 bytes
1,204	08/04/22, 11:52:53 PM	08/04/22, 11:52:53 PM	GET	http://172.29.0.1:8090/javascript/validation/onclick...	200	OK	10 ms	78 bytes	1,257 bytes
1,205	08/04/22, 11:52:54 PM	08/04/22, 11:52:54 PM	GET	http://172.29.0.1:8090/javascript/cyberoamAjax.js	200	OK	19 ms	78 bytes	8,067 bytes
1,206	08/04/22, 11:52:54 PM	08/04/22, 11:52:54 PM	GET	http://172.29.0.1:8090/images/customizeimages/u...	200	OK	27 ms	64 bytes	52,117 bytes
1,207	08/04/22, 11:52:54 PM	08/04/22, 11:52:54 PM	GET	http://172.29.0.1:8090/javascript/validation/onclick...	200	OK	20 ms	78 bytes	1,257 bytes
1,208	08/04/22, 11:52:54 PM	08/04/22, 11:52:54 PM	GET	http://172.29.0.1:8090/css/captiveportal.css?ver=1...	200	OK	21 ms	62 bytes	11,902 bytes
1,209	08/04/22, 11:52:54 PM	08/04/22, 11:52:54 PM	GET	http://172.29.0.1:8090/javascript/validation/httpclie...	200	OK	23 ms	78 bytes	15,336 bytes
1,210	08/04/22, 11:52:55 PM	08/04/22, 11:52:55 PM	GET	http://172.29.0.1:8090/images/customizeimages/u...	200	OK	18 ms	64 bytes	52,117 bytes
1,211	08/04/22, 11:52:56 PM	08/04/22, 11:52:56 PM	GET	http://testfier.net/robots.txt	200	Please login.	8 ms	74 bytes	196 bytes
1,212	08/04/22, 11:52:56 PM	08/04/22, 11:52:56 PM	GET	http://testfier.net/itemap.xml?name=abc	200	Please login.	5 ms	74 bytes	196 bytes

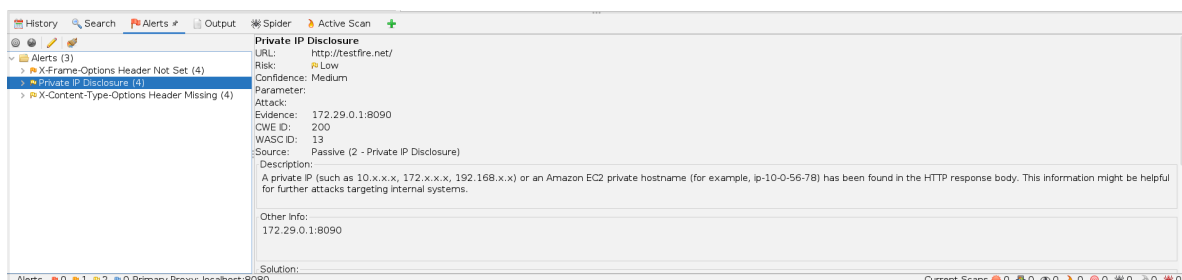
After the completion of scanning . i got that there are 3 "Alerts" are as follow:-



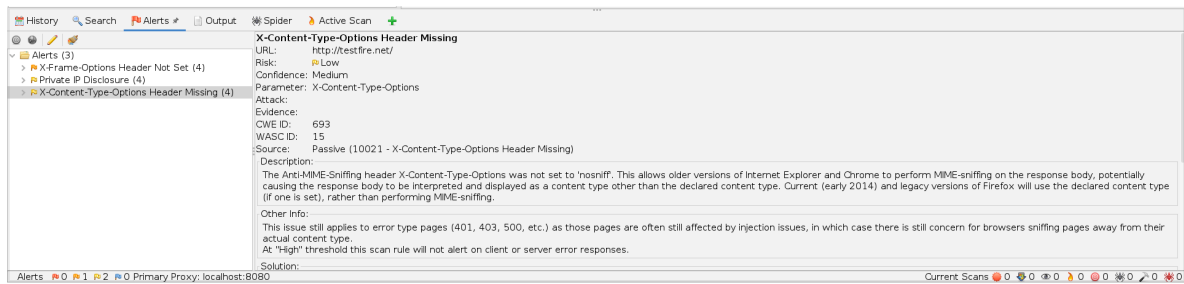
The first is X-Frame-Option Header Not Set(4) and the risk for this vulnerability is medium level



The Second Alert is Private IP Disclosure and the risk of the vulnerability is also Medium.

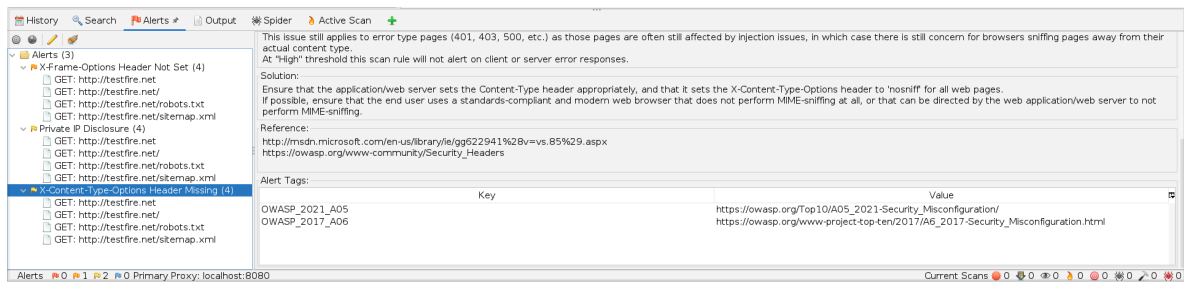


The Third Alert Is X-Content Type-Options Header Missing and the risk is low here.

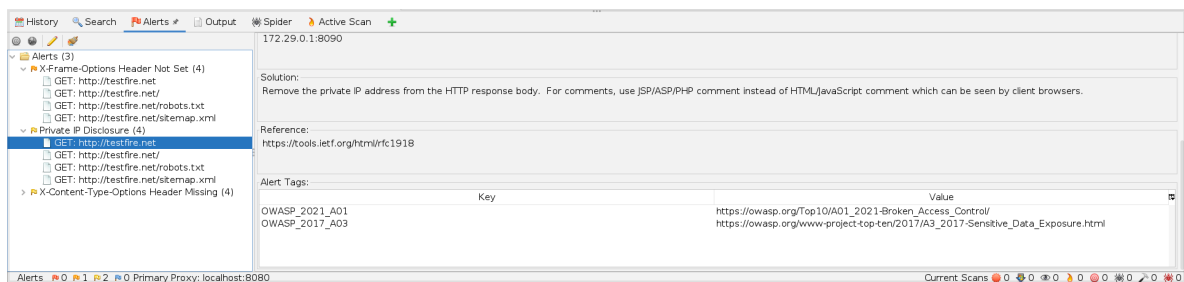


report with solution :

Here Is The Solutions for the Vulnerability "X-Content Type-Options Header Missing"
the solution with some reference captured by OWASP ZAP as follow



Here Is The Solutions for the Vulnerability "**Private IP Disclosure**"
the solution with some reference captured by OWASP ZAP as follow



Here Is The Solutions for the Vulnerability "X-Frame-Option Header Not Set"
the solution with some reference captured by OWASP ZAP as follow

HistorySearchAlertsOutputSpiderActive Scan

Alerts (3)

- X-Frame-Options Header Not Set (4)
 - GET: http://testfire.net
 - GET: http://testfire.net/
 - GET: http://testfire.net/robots.txt
 - GET: http://testfire.net/sitemap.xml
- Private IP Disclosure (4)
- X-Content-Type-Options Header Missing (4)

Solution:

Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (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>

Alert Tags:	
Key	Value
OWASP_2021_A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html

Alerts 0 1 2 Primary Proxy: localhost:8080Current Scans 0 0 0 0 0 0 0 0 0 0