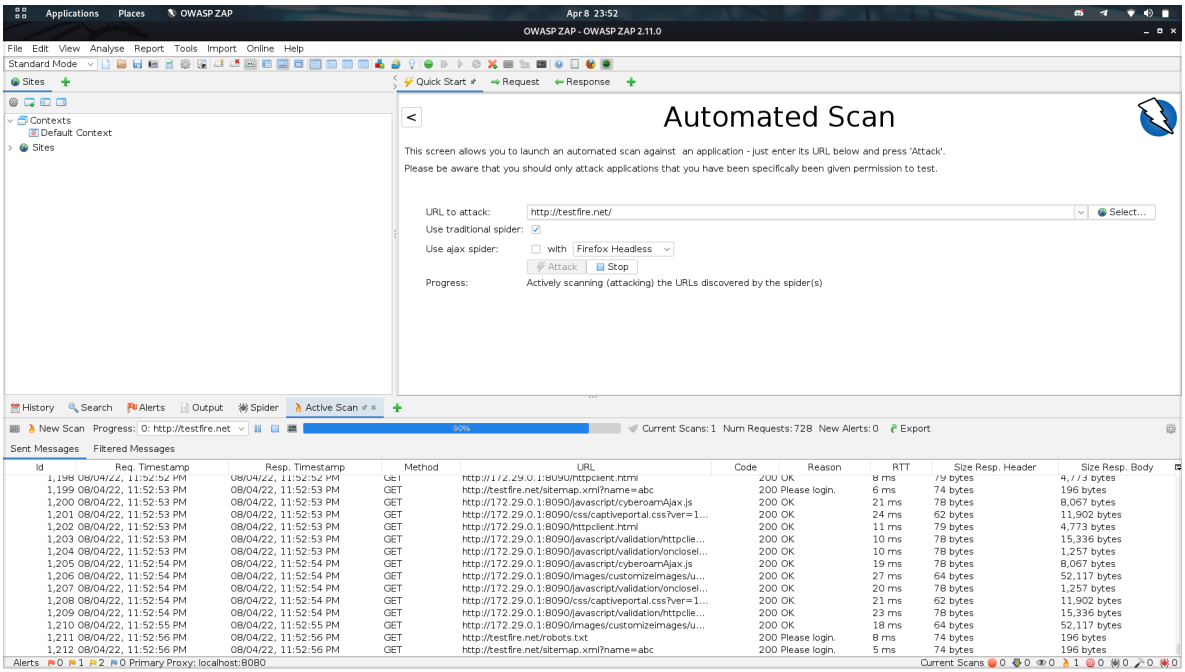
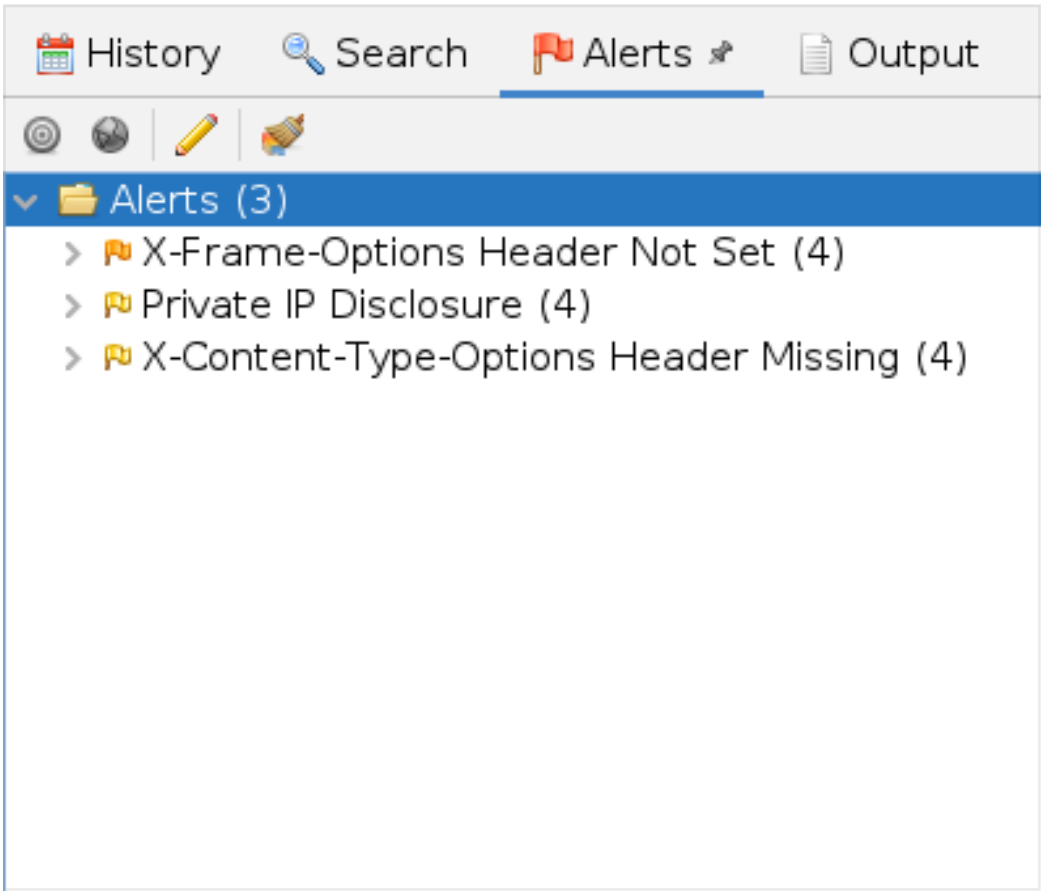
Project 2:

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:-

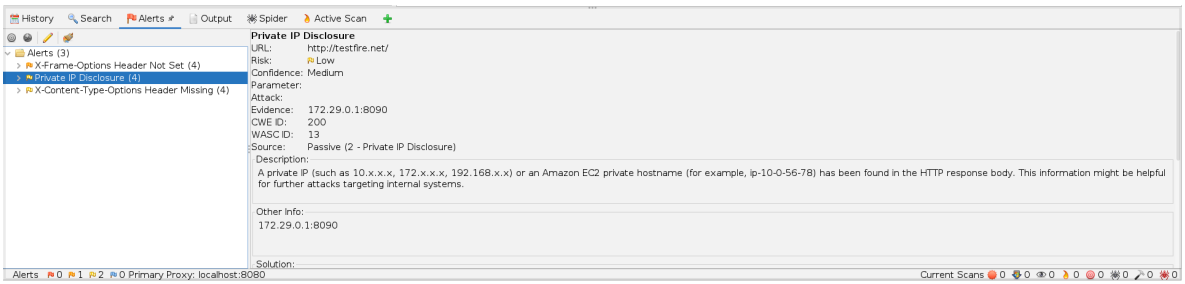


After the completion of scanning . i got that there are 3 “Alerts” are as follow:-

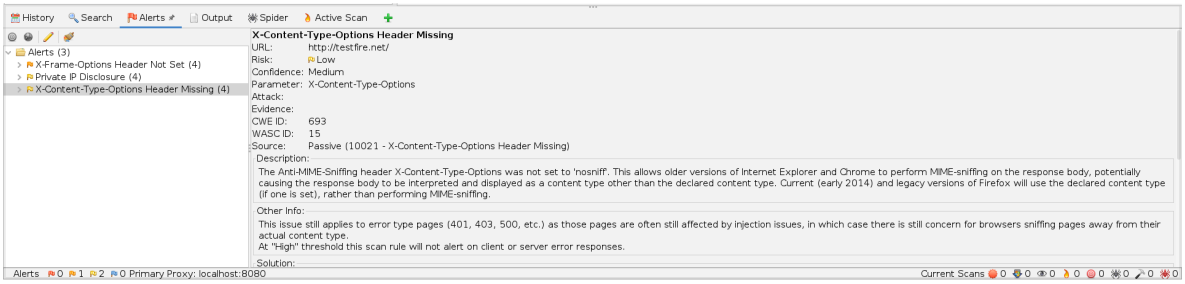


The first is X-Frame-Option Header Not Set(4) and the risk for this vulnerability is medium level

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

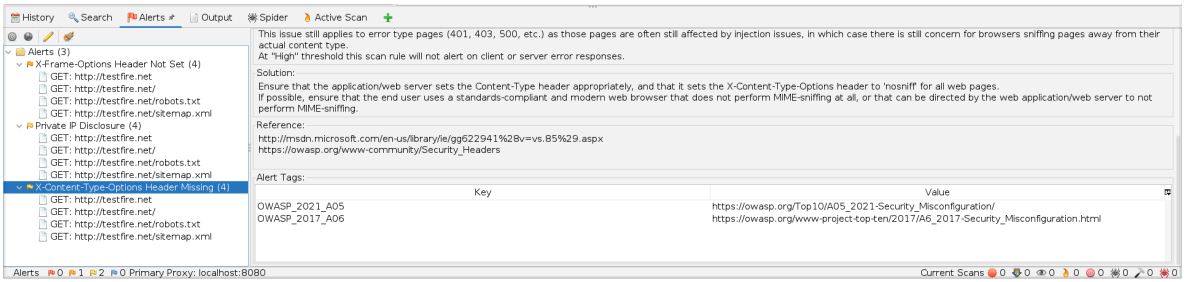


The Third Alert Is X-Content Type-Options Header Missing and the risk is low here.

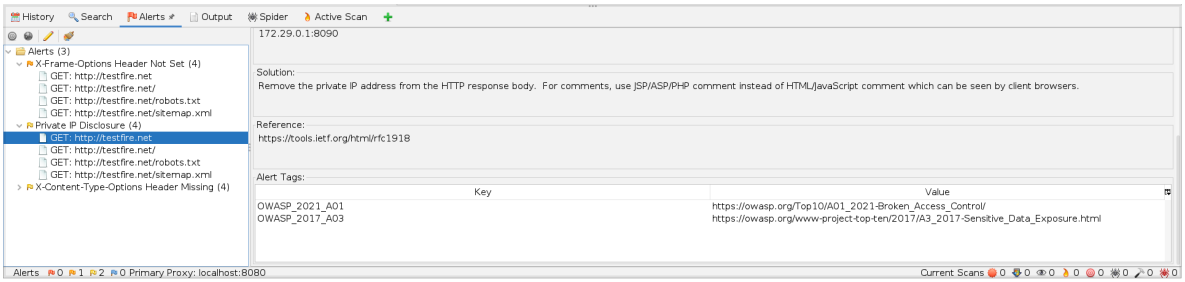


report with solution :

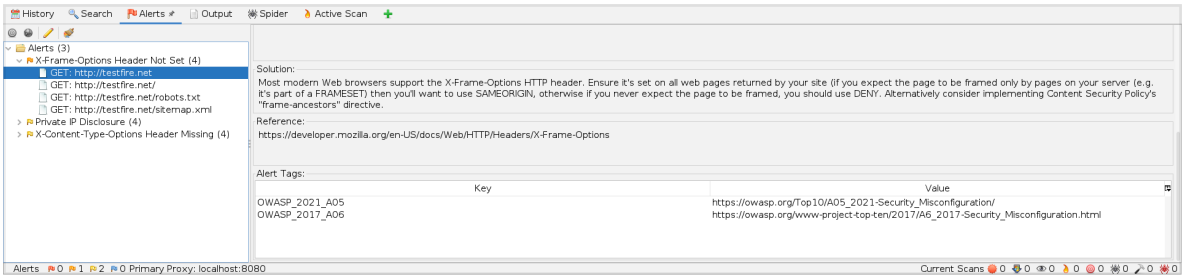
Here Is The Solutions for the Vulnerability “X-Content Type-Options Header Missing”
the solution with some reference captured by OWASP ZAP as follow



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


History
Search
Alerts
Output
Spider
Active 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
Primary Proxy: localhost:8080
Current Scans