ACADEMOR

COURSE : CYBER SECURITY

BY : GUDA LOHITHA REDDY

GMAIL : [lohithareddy182004@gmail.com](mailto:lohithareddy182004@gmail.com)



ACKNOWLEDGMENT

It is great pleasure for me to express my gratitude to Academor, for giving the opportunity and platform with facilities in accomplishing the project report.

I express my sincere gratitude to Rajesh Biswas sir for his administration towards Cyber Security knowledge growth.

Finally , it is pleased to acknowledge the indebtedness to all those who devoted themselves directly or indirectly to make this project report success.

ABSTRACT

Perform Web Application Penetration Testing (WAPT) on http://testphp.vulnweb.com and create a Vulnerability Assessment and Penetration Testing (VAPT) report on it and submit the report (Using OWASP ZAP).

INDEX

**S.NO TITLE**

1. Introduction
2. Aim of the project
3. Procedure
4. Commands
5. Results and screenshots
6. Conclusion

INTRODUCTION

This project deals with web application penetration testing is a process by which Cyber Security Experts simulate a real-life-cyber-attack against e web applications, websites, or web services to identify probable threats.

Vulnerability Assessment and Penetration Testing, commonly known as VAPT. This comprehensive guide aims to provide an in-depth understanding of VAPT, its different types, benefits, frequency, performers, phases, tools, challenges, improvement strategies, and best practices.

And also includes OWSAP include Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities(XXE), Broken Access Control, Security Misconfiguration, Cross-Site Scripting XSS, Insecure Deserialization, Using Components with known Vulnerabilities, Insufficient Logging & Monitoring.

**AIM OF THE PROJECT**

Perform Web Application Penetration Testing (WAPT) on http://testphp.vulnweb.com and create a Vulnerability Assessment and Penetration Testing (VAPT) report on it and submit the report (Using OWASP ZAP).

PROCEDURE

Web Application Penetration Testing (WAPT) :-

A web application penetration testing process provides a detailed testing process provides a detailed report with security insights.

Web application penetration is typically implemented in three phases:

1. Planning
2. Exploitation
3. Post-execution

Important aspects for planning phase:

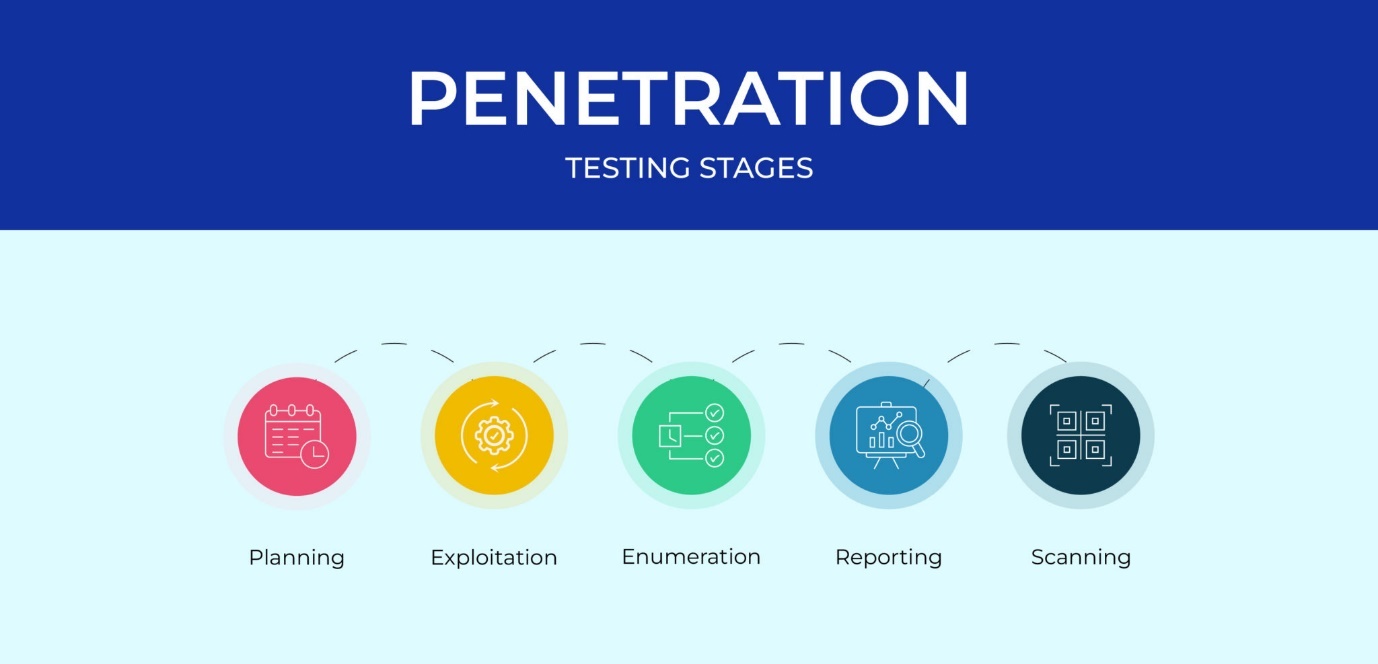
1. Define the scope of the test.
2. Provide the penetration testing with needed information, including relevant documentation.
3. Determine a success criterion for the test.

Important aspects for Exploitation phase:

1. Run the test using several different roles.
2. Follow the pre-defined success criteria and reporting procedure when discovering vulnerabilities.
3. Create a clear and detailed report, explaining the measures taken, vulnerabilities detected, and the severity of each vulnerability.

Now, important aspects for post-execution phase:

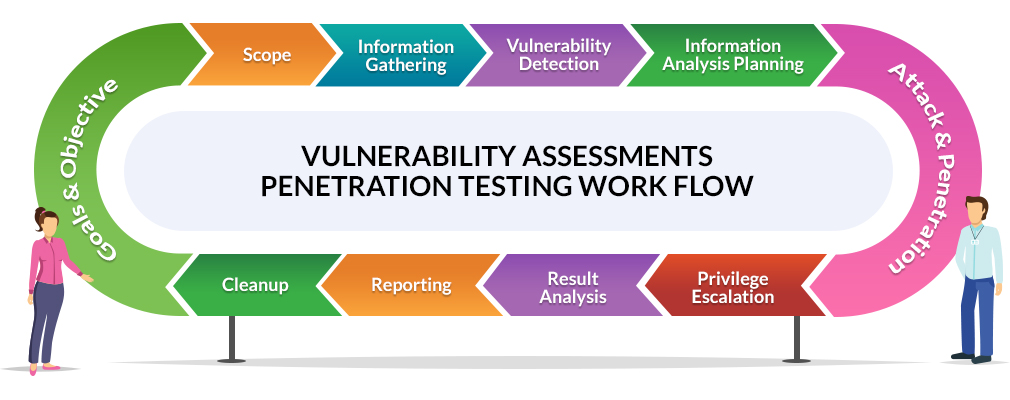
1. Provide recommendations for remediating the detected vulnerabilities.
2. Re-test to check that the discovered vulnerabilities were properly remediated.
3. Once all tests are conducted, revert all changes back to the original configuration, including proxy settings.

No 

**Vulnerability Assessment and Penetration Testing(VAPT) :**

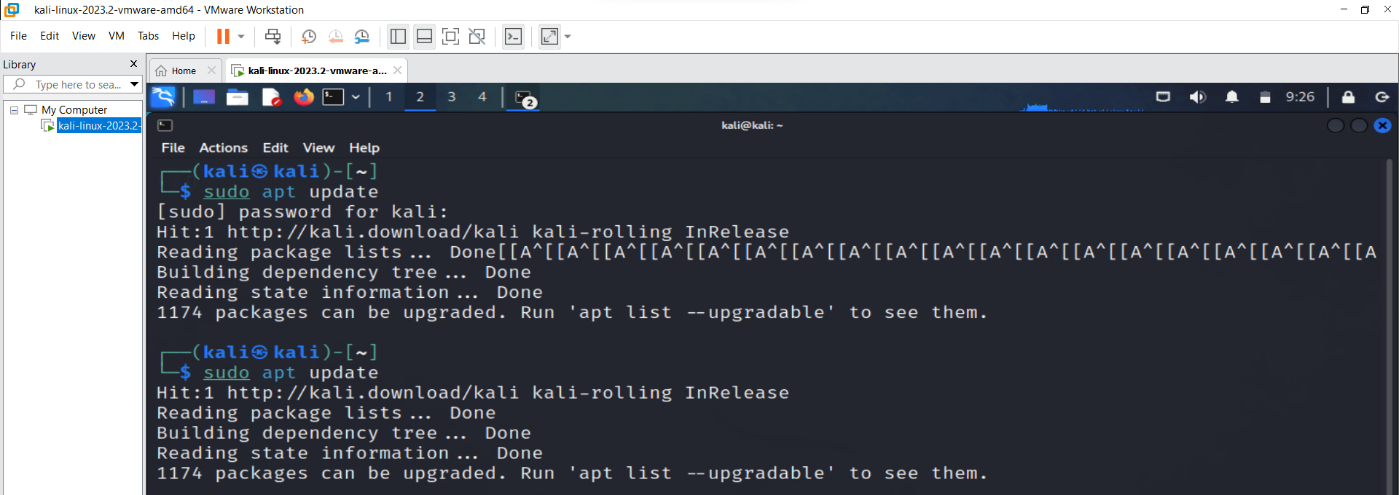
Vulnerability Assessment and penetration testing comprehensive approach to identifying and rectifying vulnerabilities in a network, application, or system. The process involves two main steps:

* **Vulnerability Assessment:** This is the process of identifying potential vulnerabilities in a system, network, or application. It involves scanning the system to find weak points that could be exploited by attackers.
* **Penetration Testing:** This is the process of simulating a cyber-attack on the system to exploit the identified vulnerabilities. The purpose is to understand the potential impact of an attack and to test the effectiveness of the existing security measures.



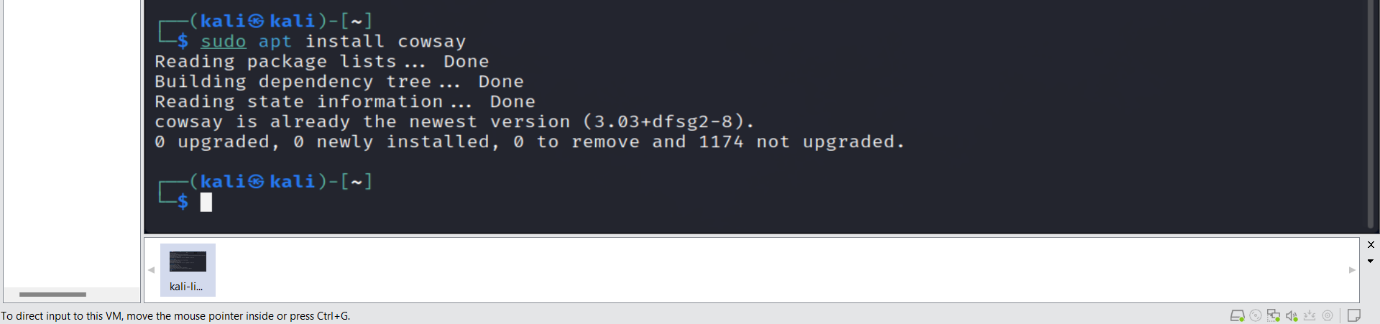
COMMANDS : Using Kali Linux

***Updating kali***: $ sudo apt update

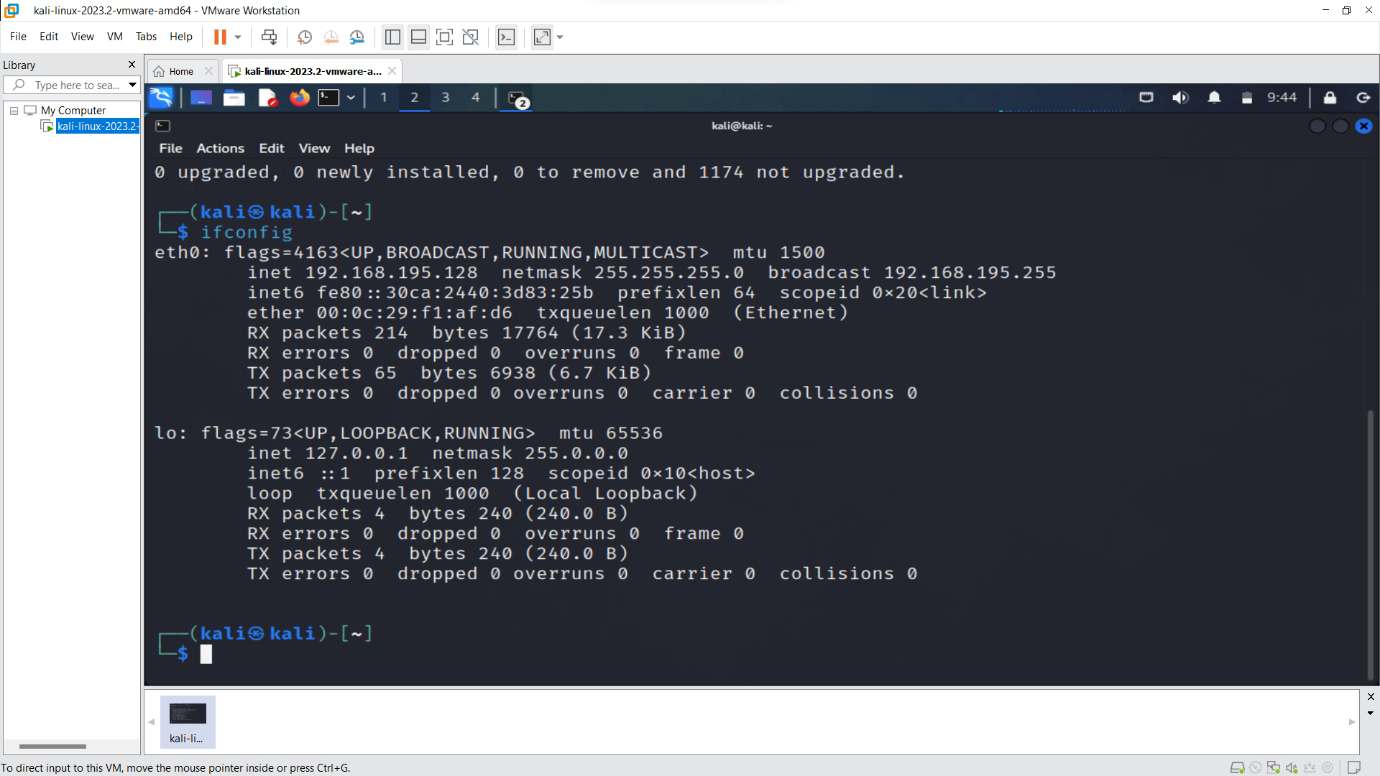




***Installing in kali*** : $ sudo apt install #softwarefile

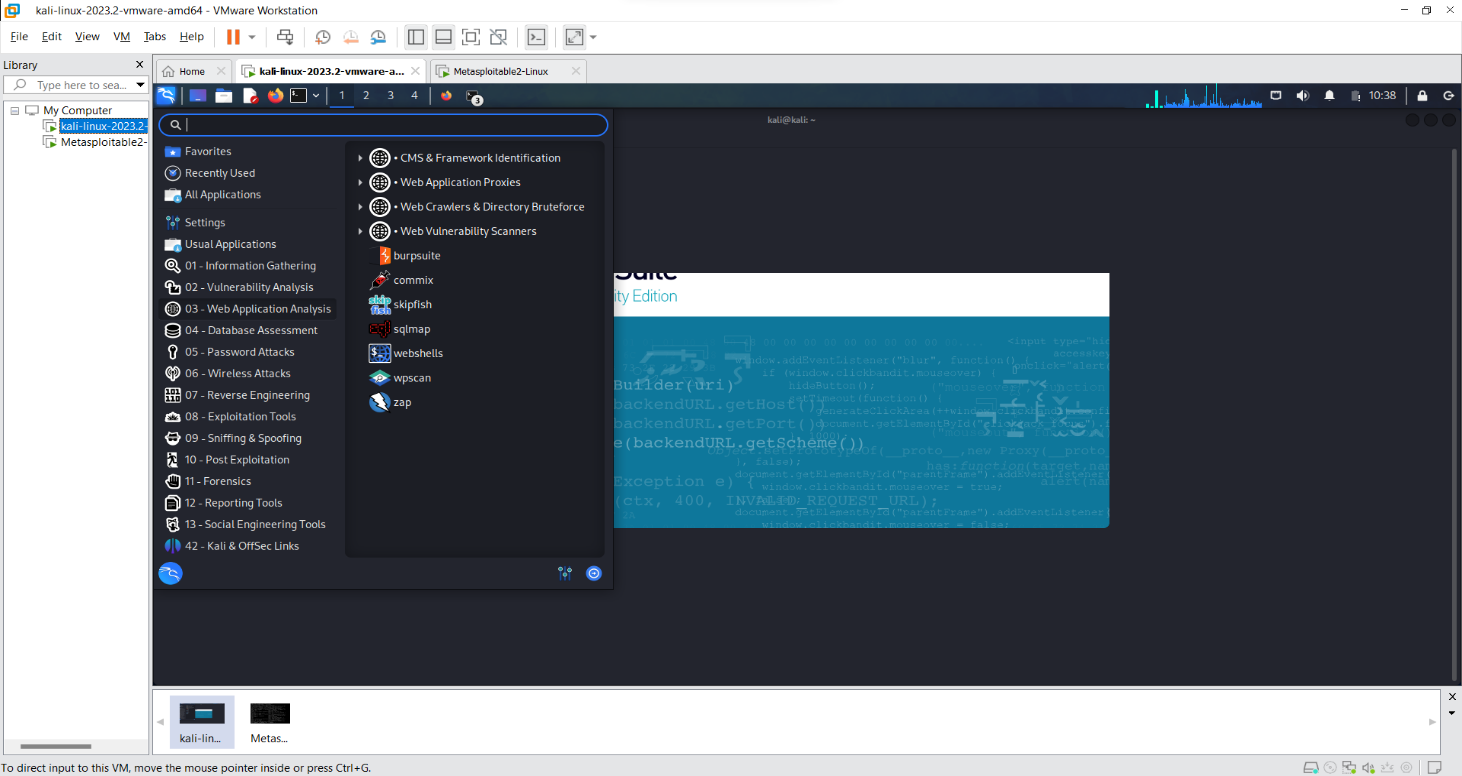


***To check networking***: $ if configu

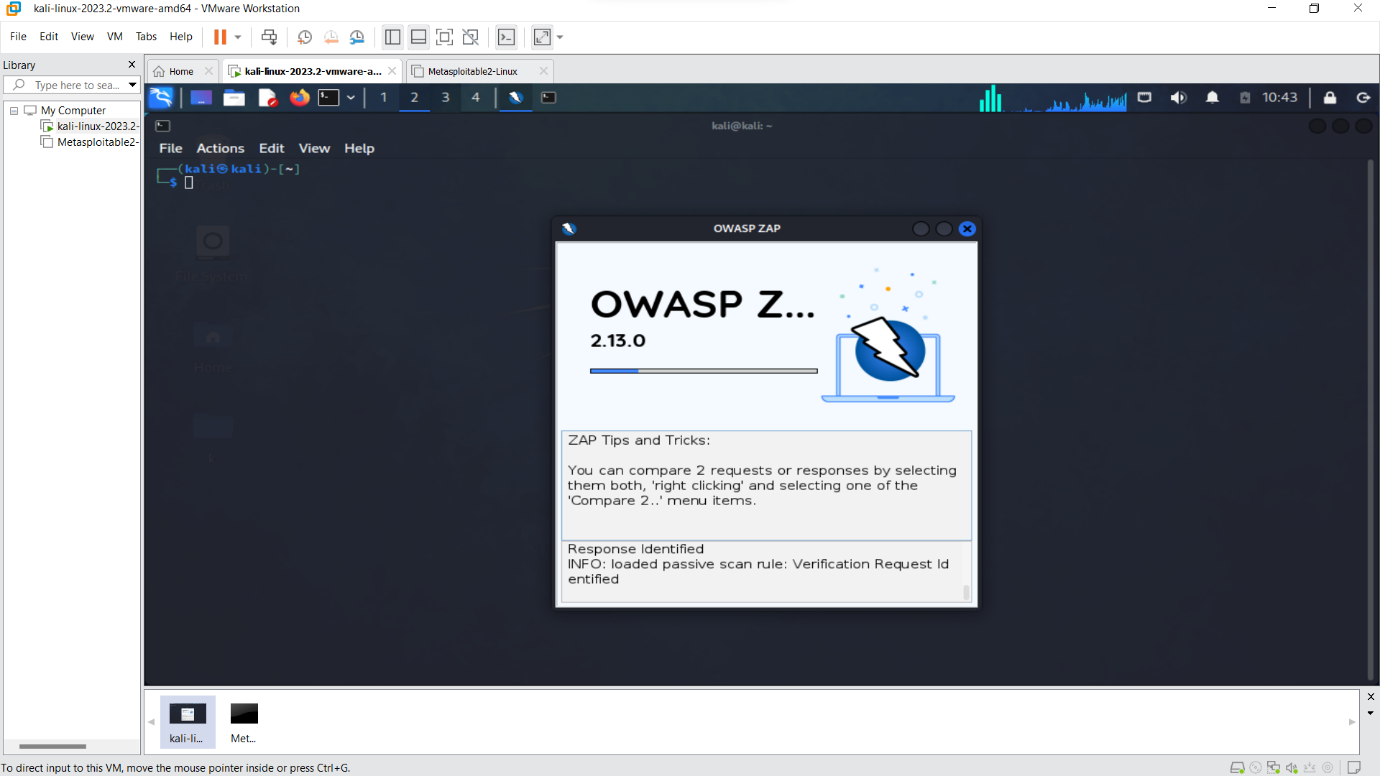


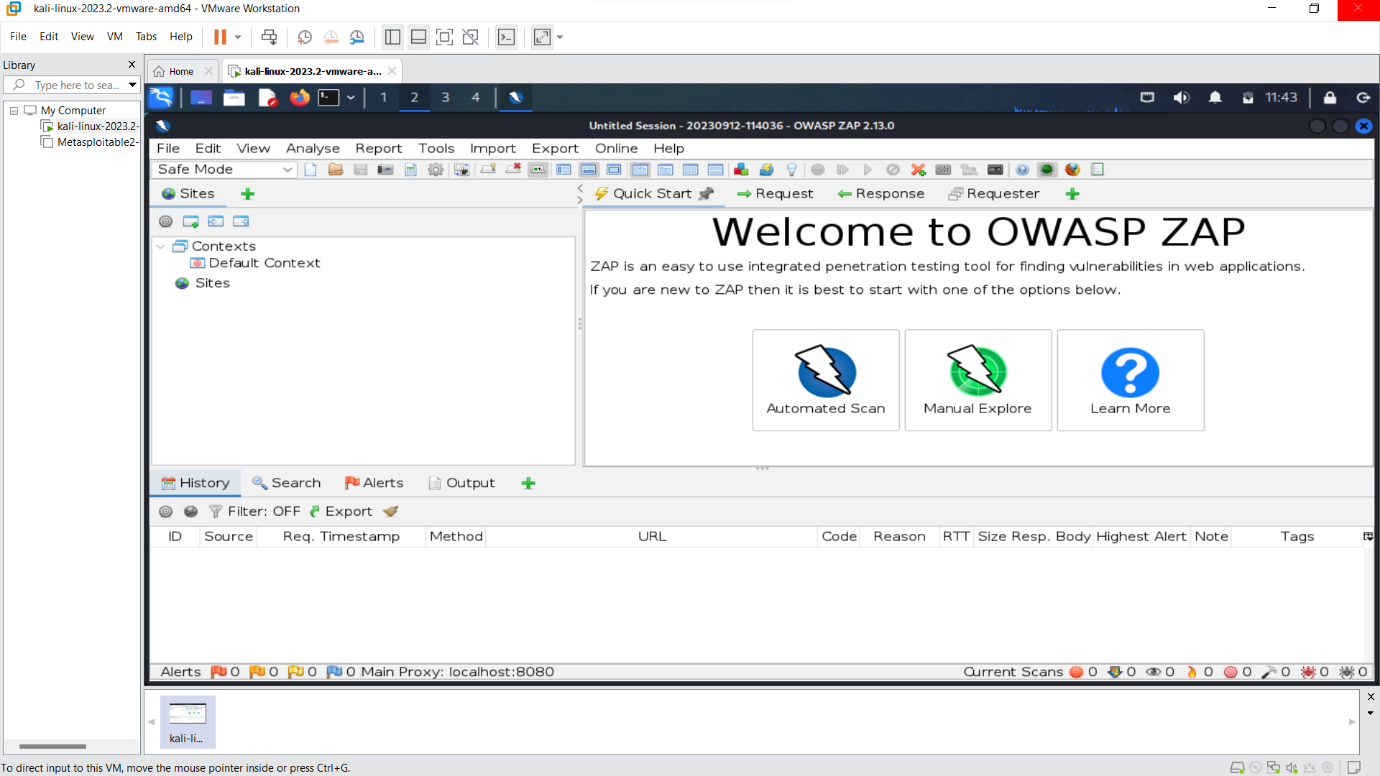
Results :

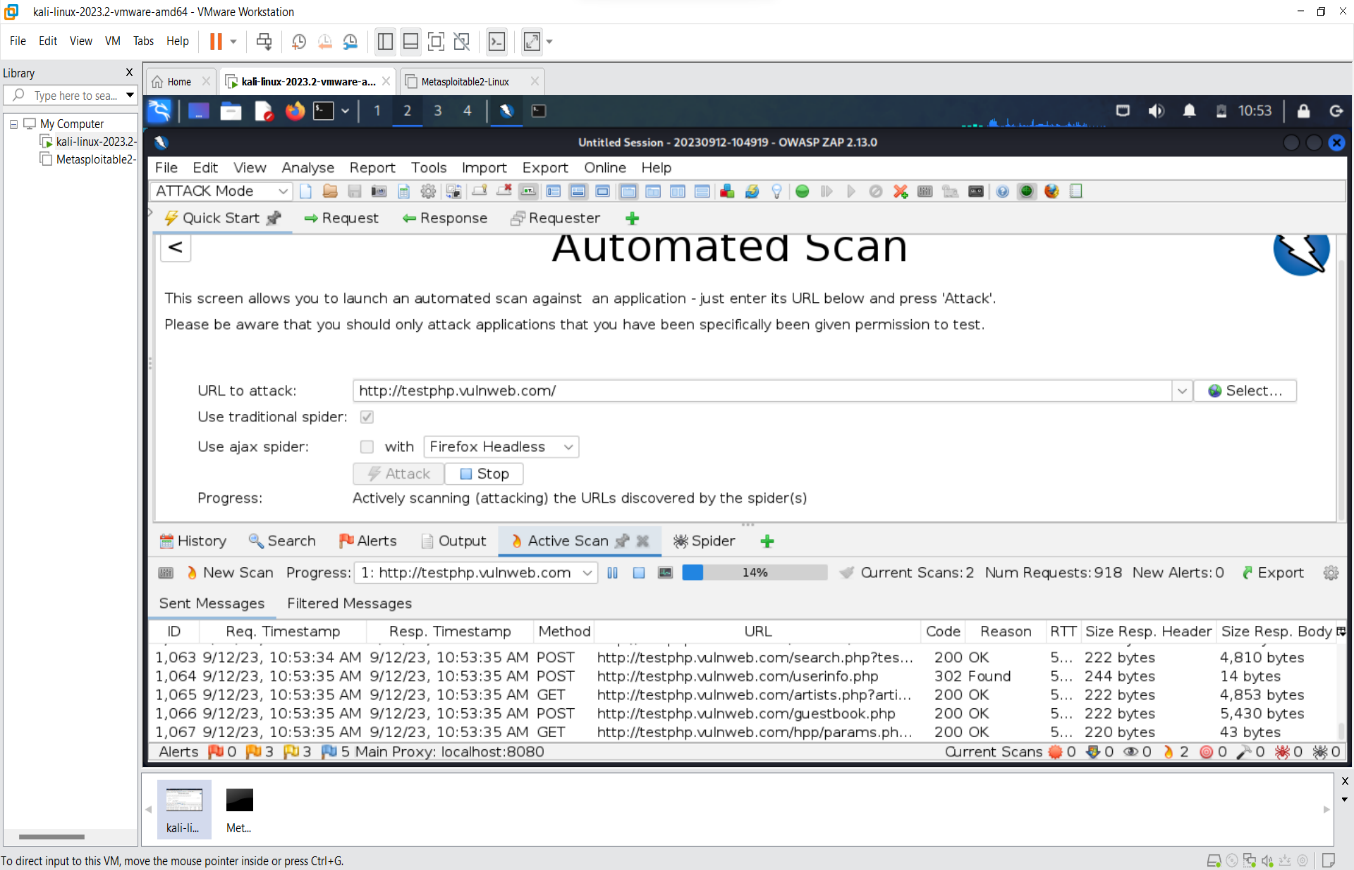
* Open kali linux Go 🡪 Home🡪 select web application analysis🡪web application proxies🡪 owasp zap

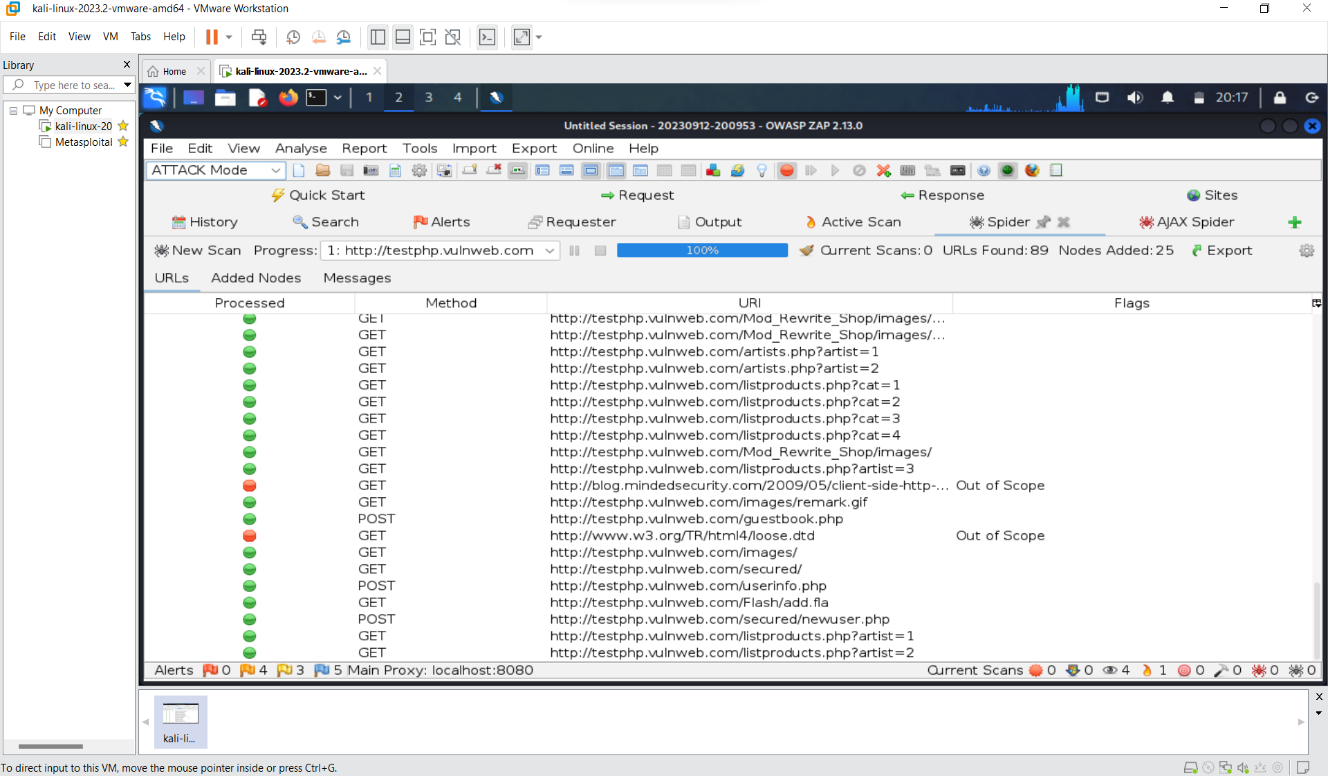


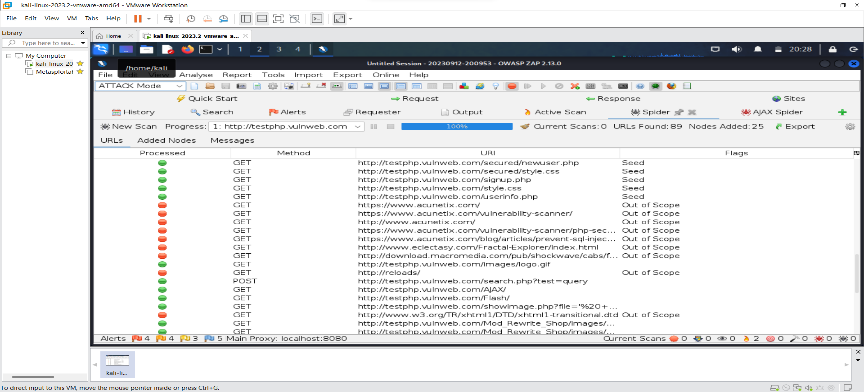
* Select owasp zap

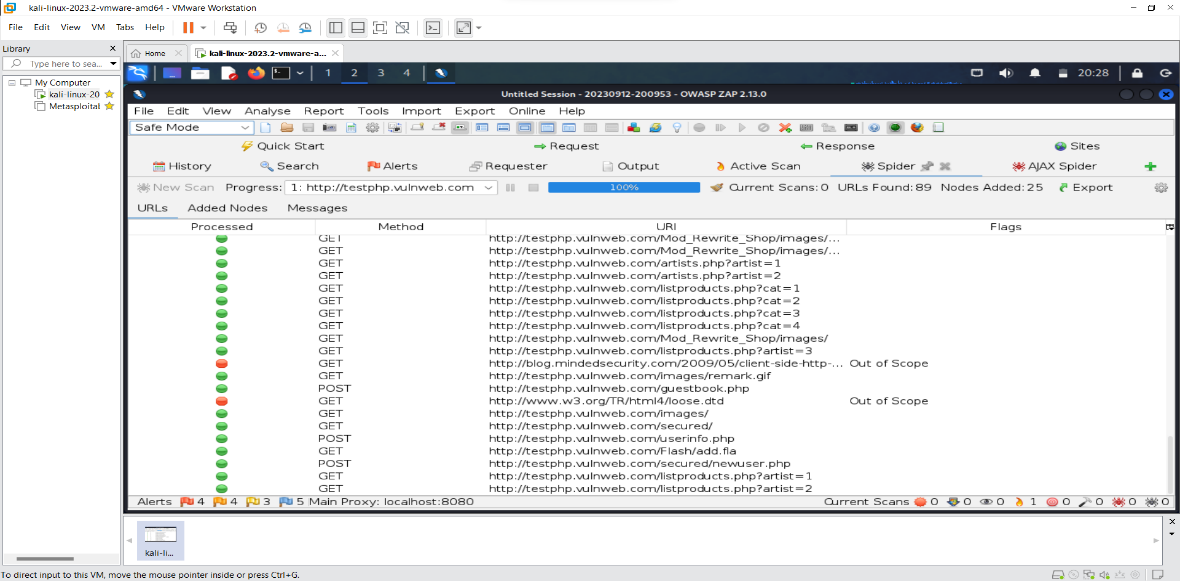


* Select automated scan
* Enter URL to attack<http://testphp.vulweb.com/> and select attack



* URLs found for <http://testphp.vulweb.com/> are 89 and Nodes Added : 25 
* There are URLs Out Of Scope.





CONCLUSION

Here we get 16 alerts for the URL <http://testphp.vulnweb.com/> for each alert having specific description and specific solution by using owasp zap.



