Task 3 :- Web App "Mystery Box" - Vulnerability Assessment with OWASP ZAP

Name :- Rushikesh Sanjay Kumavat

INTERN ID:- SN1000726

DOMAIN:- Cyber Security

Aim :-

To perform an automated vulnerability assessment on the Metasploitable web application using OWASP ZAP and identify security flaws

OBJECTIVE :-

- Access Metasploitable2 web interface
- Perform automated scan using OWASP ZAP
- Identify security vulnerabilities
- Analyze security misconfigurations

Tools Used :-

- Kali Linux
- Metasploitable 2
- OWASP ZAP

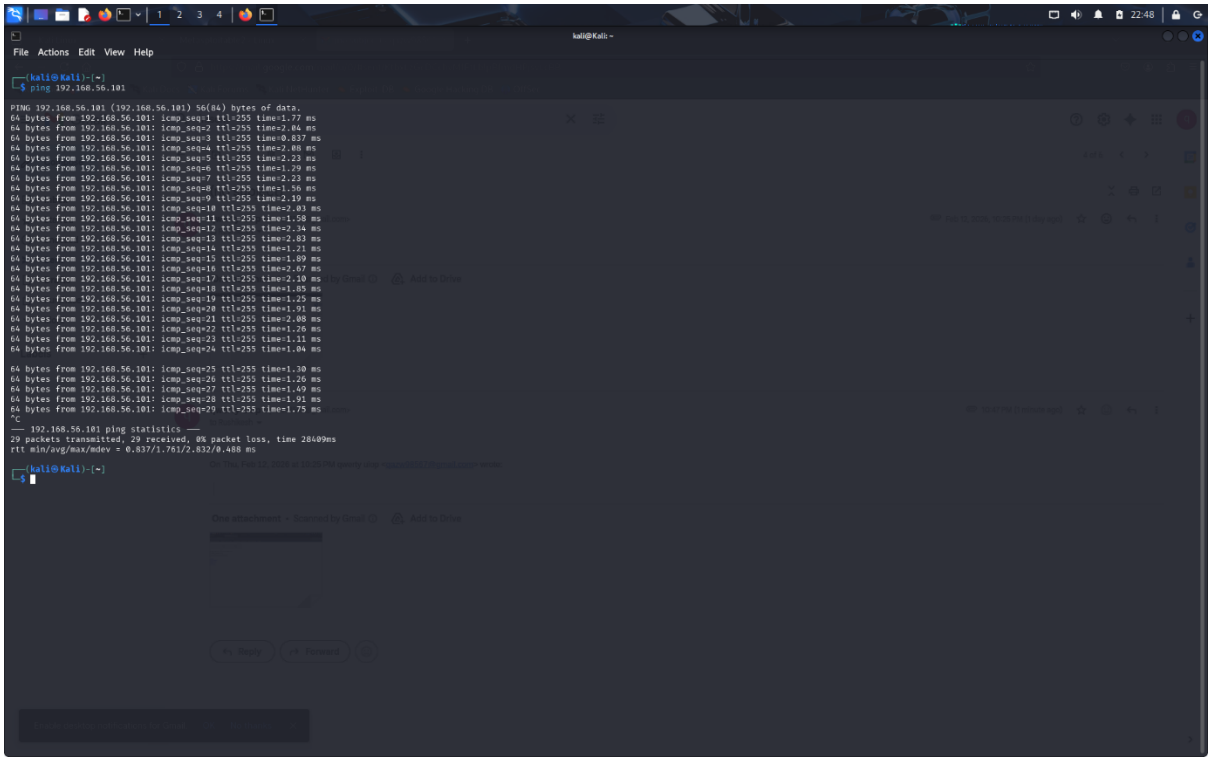
Procedure :-

Step 1: Verify Target Connectivity

Command used:

➔ ping 192.168.56.101

Result: Target is reachable.



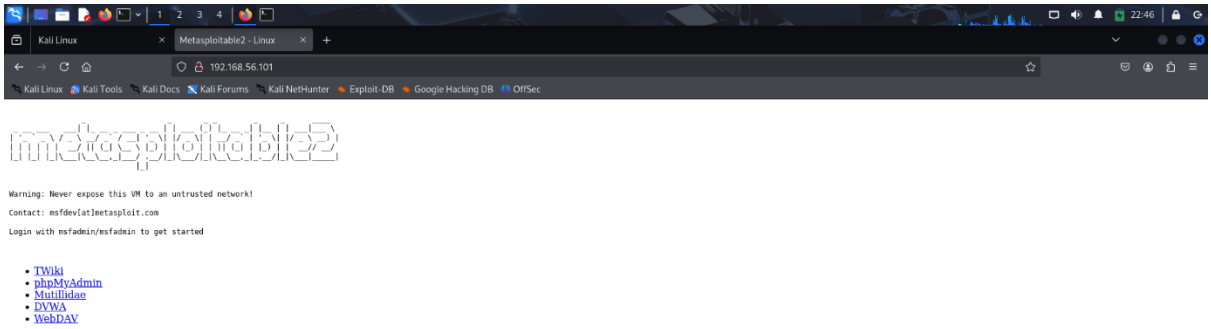
Step 2: Open Target in Browser

Open browser and enter:

➔ http://192.168.56.101

You will see Metasploitable2 homepage with:

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV



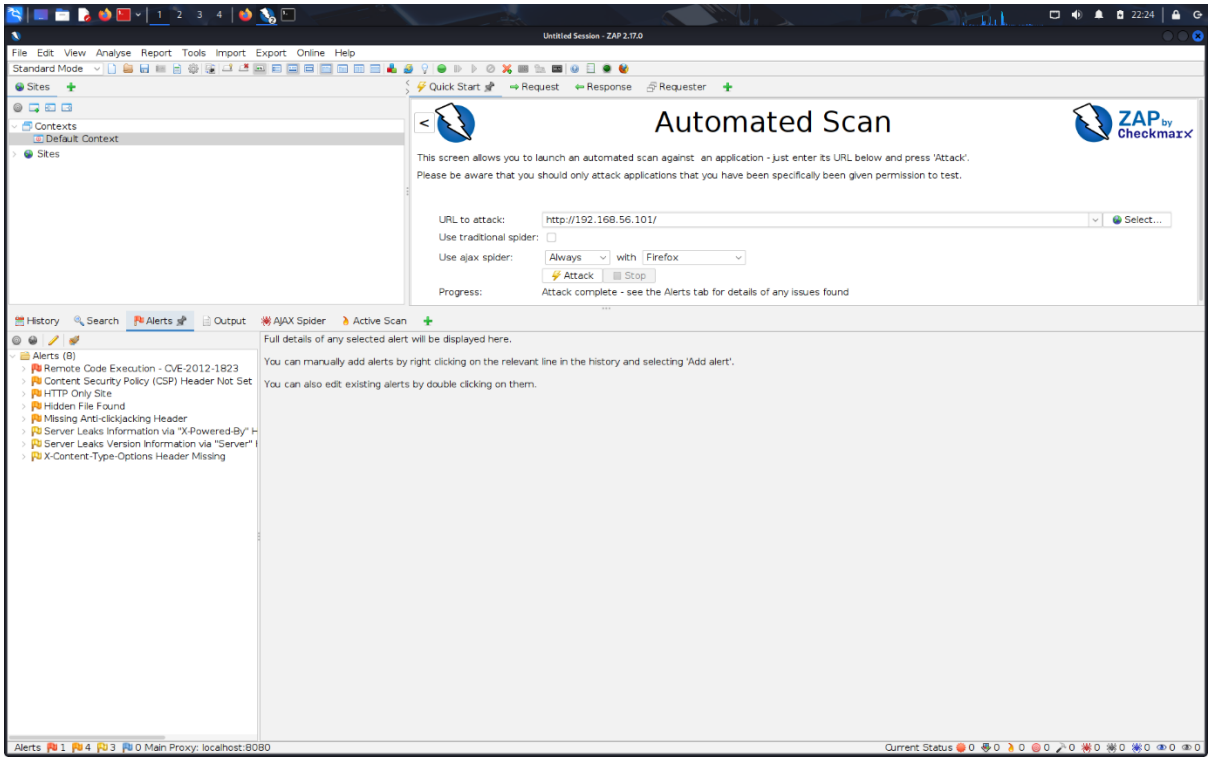
Step 3: Open OWASP ZAP

Open ZAP in Kali Linux.

Enter target URL:

➔ http://192.168.56.101

Click **Attack**



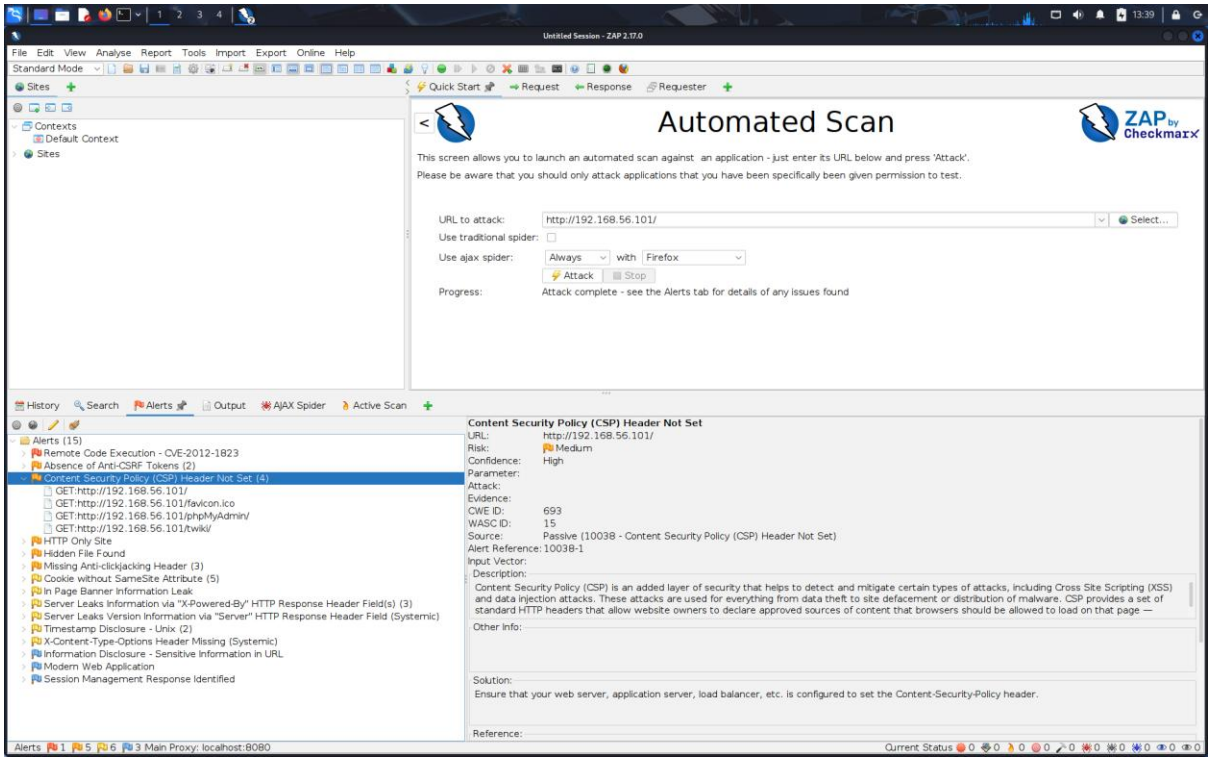
Step 4: Analyze Alerts

After scanning, go to:

➞ Alerts Tab

Vulnerabilities Found:

- Remote Code Execution (CVE-2012-1823)
- Content Security Policy Header Not Set
- Missing Anti-clickjacking Header
- Server Version Information Leak
- X-Content-Type-Options Header Missing



VULNERABILITY ANALYSIS:-

- **Remote Code Execution – CVE-2012-1823**

  Risk: High
  Description: Allows attacker to execute arbitrary commands.

- **Missing Security Headers**

  - CSP Header Not Set
  - X-Content-Type-Options Missing
  - Anti-clickjacking Header Missing

  Risk: Medium

- **Information Disclosure**

  - Server version leaked
  - PHP version visible

  Risk: Low

RESULT :-

Successfully performed web vulnerability assessment using OWASP ZAP and identified multiple security vulnerabilities in Metasploitable2 machine.

CONCLUSION :-

The Metasploitable2 machine contains multiple web application vulnerabilities including Remote Code Execution and missing security headers. OWASP ZAP successfully detected these vulnerabilities.