

**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

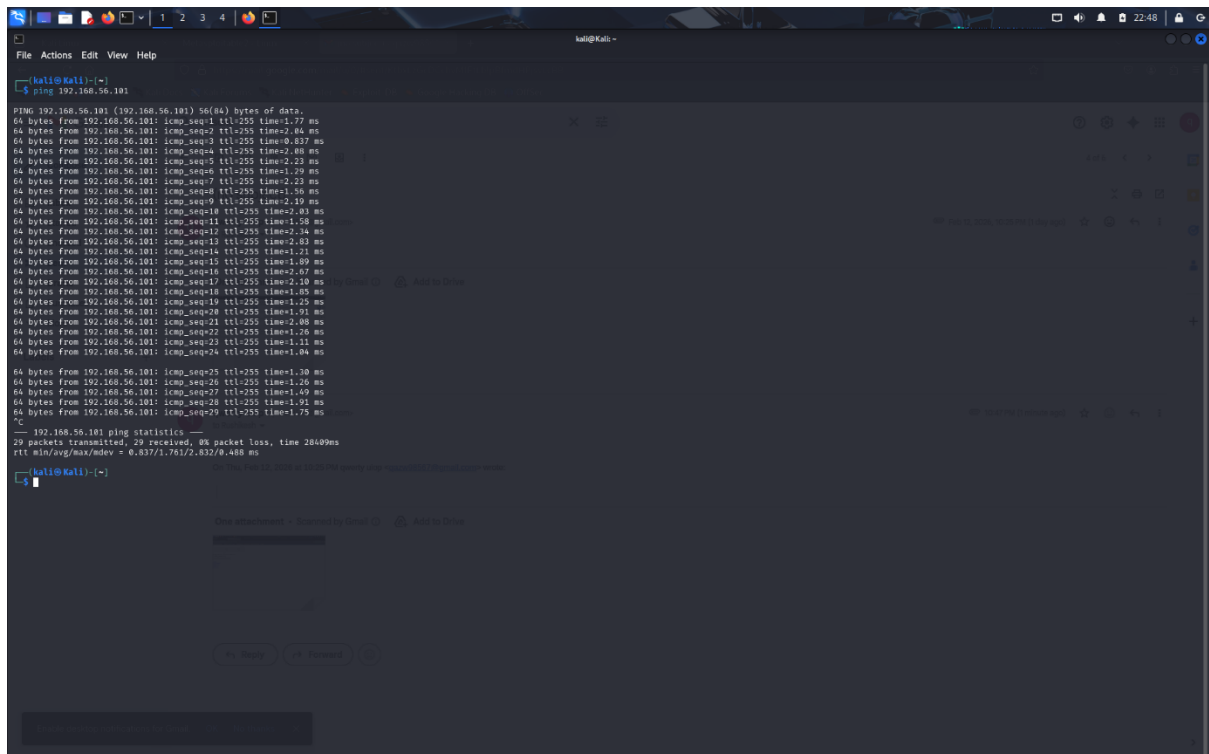
Procedure :-

Step 1: Verify Target Connectivity

Command used:

➔ ping 192.168.56.101

Result: Target is reachable.



```
kali@kali:~$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:
64 bytes from 192.168.56.101: icmp_seq=1 ttl=255 time=1.77 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=255 time=2.04 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=255 time=0.837 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=255 time=1.08 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=255 time=2.23 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=255 time=1.29 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=255 time=2.23 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=255 time=1.56 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=255 time=2.19 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=255 time=2.83 ms
64 bytes from 192.168.56.101: icmp_seq=11 ttl=255 time=1.58 ms
64 bytes from 192.168.56.101: icmp_seq=12 ttl=255 time=2.34 ms
64 bytes from 192.168.56.101: icmp_seq=13 ttl=255 time=2.83 ms
64 bytes from 192.168.56.101: icmp_seq=14 ttl=255 time=1.21 ms
64 bytes from 192.168.56.101: icmp_seq=15 ttl=255 time=1.89 ms
64 bytes from 192.168.56.101: icmp_seq=16 ttl=255 time=2.67 ms
64 bytes from 192.168.56.101: icmp_seq=17 ttl=255 time=2.10 ms
64 bytes from 192.168.56.101: icmp_seq=18 ttl=255 time=1.95 ms
64 bytes from 192.168.56.101: icmp_seq=19 ttl=255 time=1.25 ms
64 bytes from 192.168.56.101: icmp_seq=20 ttl=255 time=1.91 ms
64 bytes from 192.168.56.101: icmp_seq=21 ttl=255 time=2.08 ms
64 bytes from 192.168.56.101: icmp_seq=22 ttl=255 time=1.28 ms
64 bytes from 192.168.56.101: icmp_seq=23 ttl=255 time=1.11 ms
64 bytes from 192.168.56.101: icmp_seq=24 ttl=255 time=1.04 ms
64 bytes from 192.168.56.101: icmp_seq=25 ttl=255 time=1.30 ms
64 bytes from 192.168.56.101: icmp_seq=26 ttl=255 time=1.20 ms
64 bytes from 192.168.56.101: icmp_seq=27 ttl=255 time=1.40 ms
64 bytes from 192.168.56.101: icmp_seq=28 ttl=255 time=1.91 ms
64 bytes from 192.168.56.101: icmp_seq=29 ttl=255 time=1.75 ms
64 bytes from 192.168.56.101: icmp_seq=30 ttl=255 time=1.30 ms
--- 192.168.56.101 ping statistics ---
30 packets transmitted, 30 received, 0% packet loss, time 28409ms
rtt min/avg/max/mdev = 0.837/1.761/2.832/0.488 ms
kali@kali:~$
```

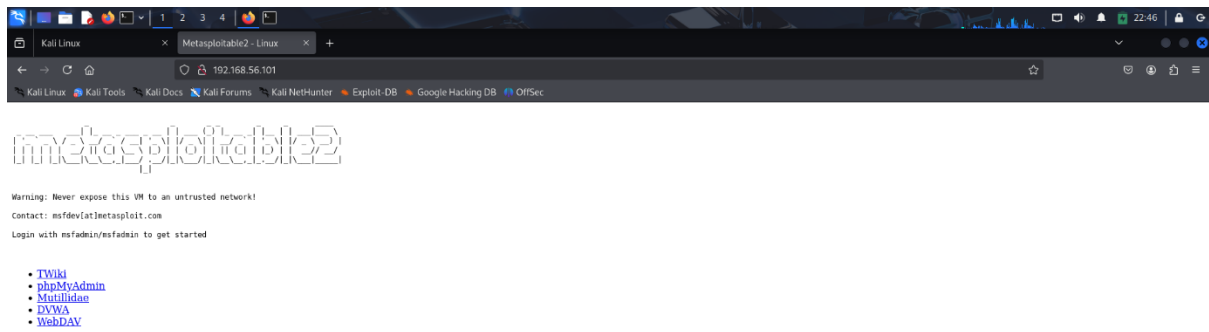
Step 2: Open Target in Browser

Open browser and enter:

➔ <http://192.168.56.101>

You will see Metasploitable2 homepage with:

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV



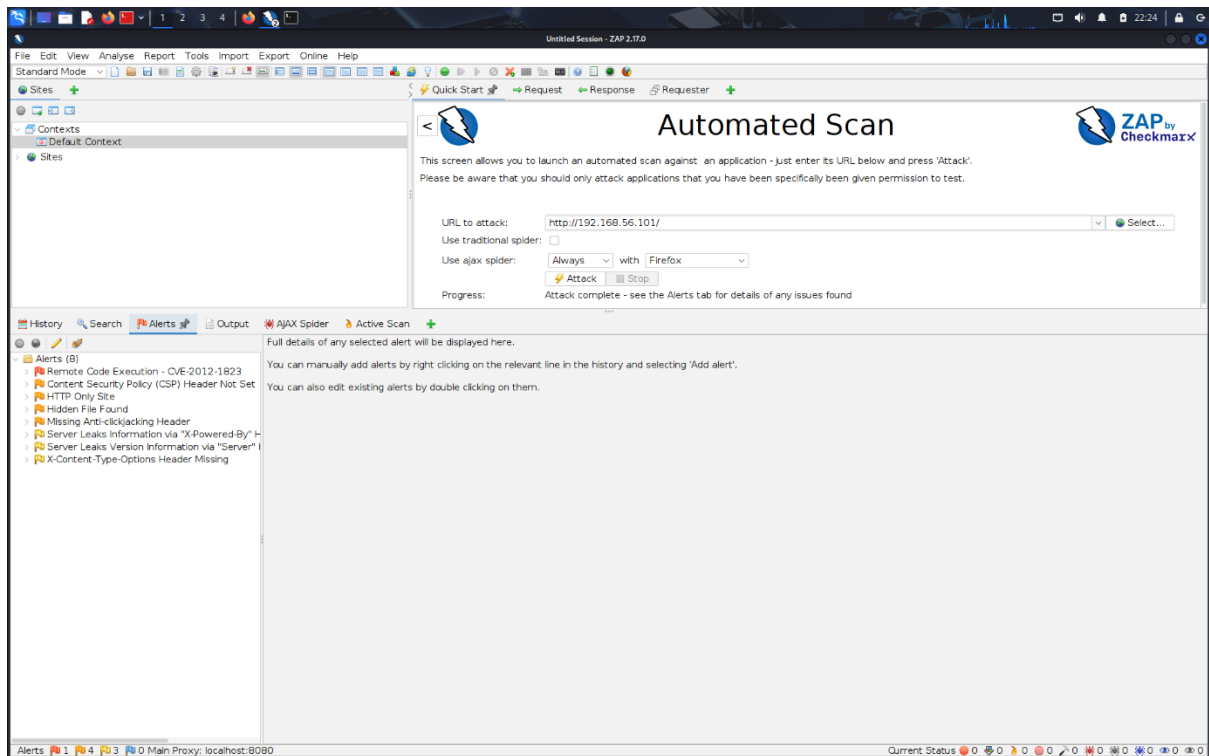
Step 3: Open OWASP ZAP

Open ZAP in Kali Linux.

Enter target URL:

➔ <http://192.168.56.101>

Click **Attack**



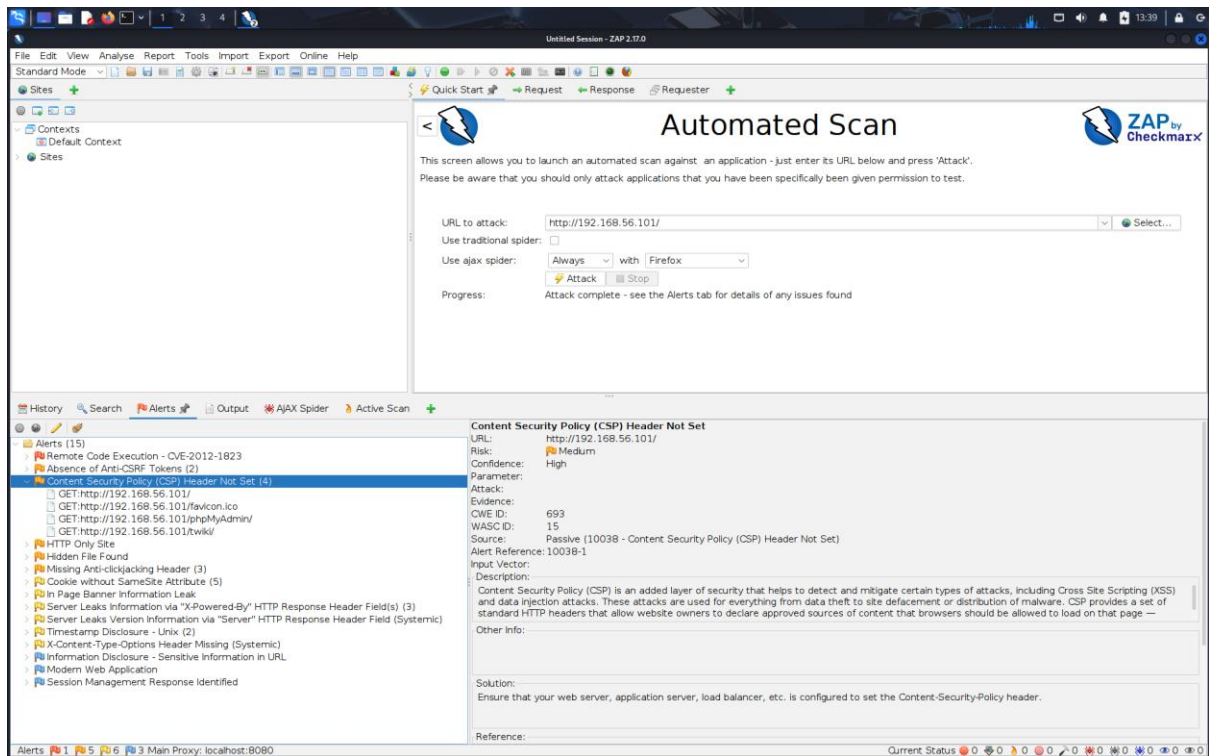
Step 4: Analyze Alerts

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.