# Cybersecurity Project Report

# Vulnerability Assessment and Penetration Testing (VAPT)

## 1. Introduction

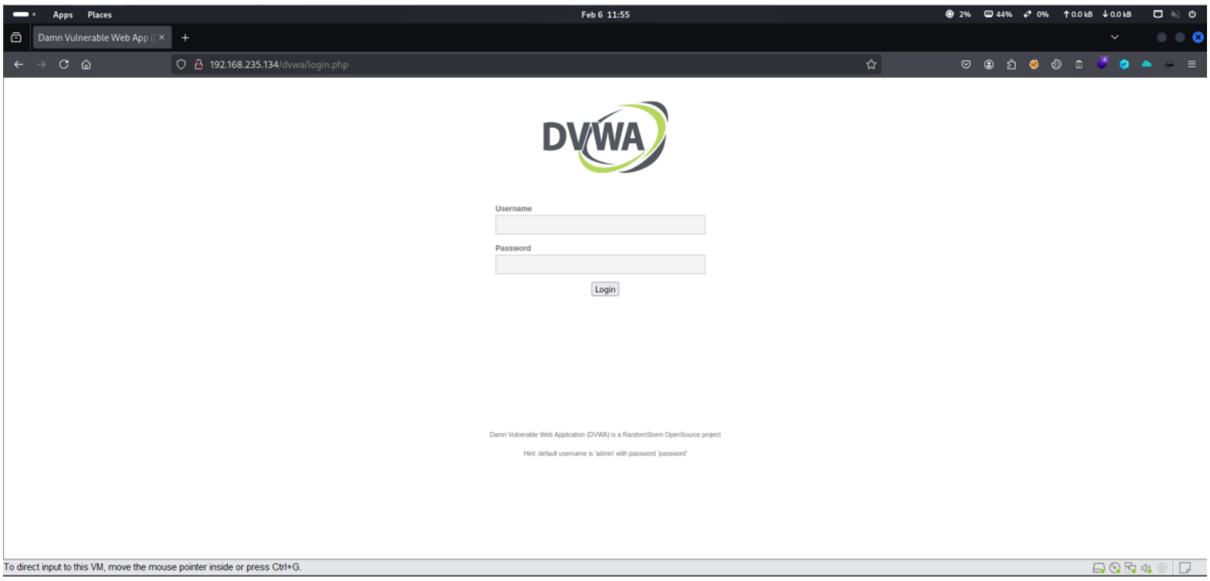
This project focuses on performing **Vulnerability Assessment and Penetration Testing (VAPT)** on a deliberately vulnerable web application in a controlled lab environment.
The objective is to identify security weaknesses, exploit them ethically, assess their impact, and recommend mitigation strategies.

The assessment follows a standard VAPT methodology including:

- Reconnaissance
- Vulnerability Identification
- Exploitation
- Impact Analysis
- Mitigation Recommendations

## 2. Scope of Testing

- **Target Application:** Damn Vulnerable Web Application (DVWA)
- **Environment:** Localhost / Virtual Machine
- **Testing Type:** Black-box testing
- **Out of Scope:** Denial of Service (DoS), real-world systems.



192.168.235.134/dvwa/login.php

Username

Password

Login

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

**Figure 1:** DVWA login page accessed through the browser, showing the target web application used for vulnerability assessment and penetration testing. The URL and DVWA interface confirm the testing scope and target environment.

## 3. Tools Used

- Kali Linux
- Nmap
- Burp Suite (Proxy & Intruder)
- Web Browser (Firefox)
- DVWA

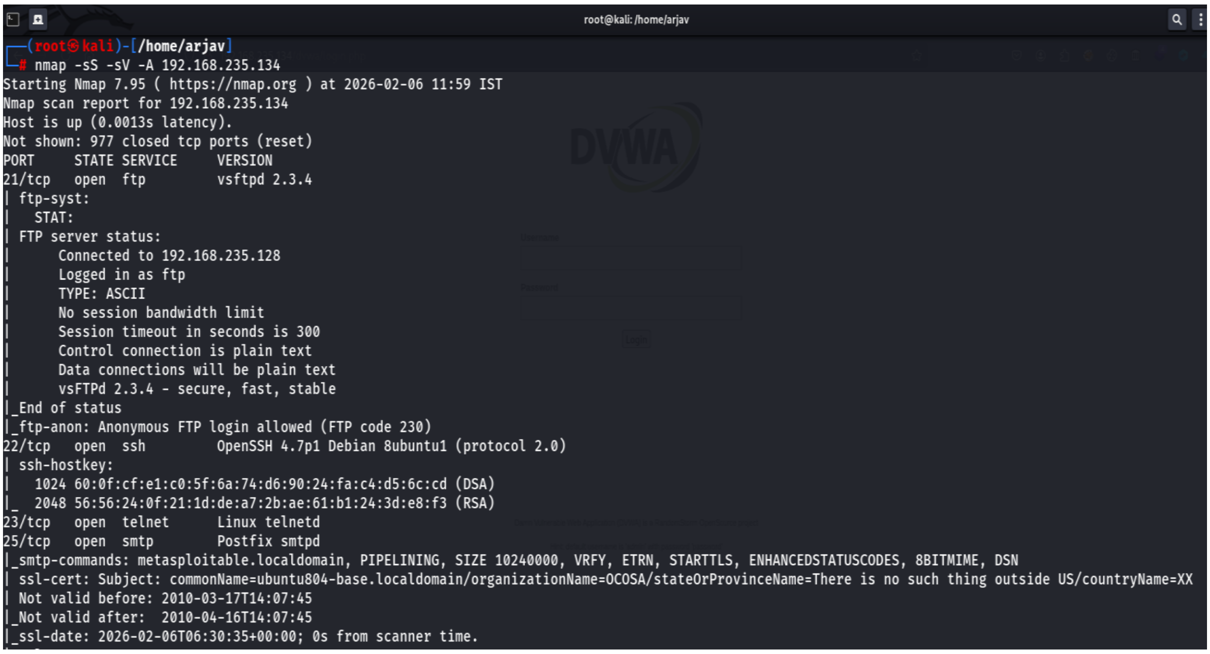
## 4. Reconnaissance & Scanning

### 4.1 Network Scanning using Nmap

Nmap was used to identify open ports, running services, and potential attack vectors on the target system.

**Command Used:**

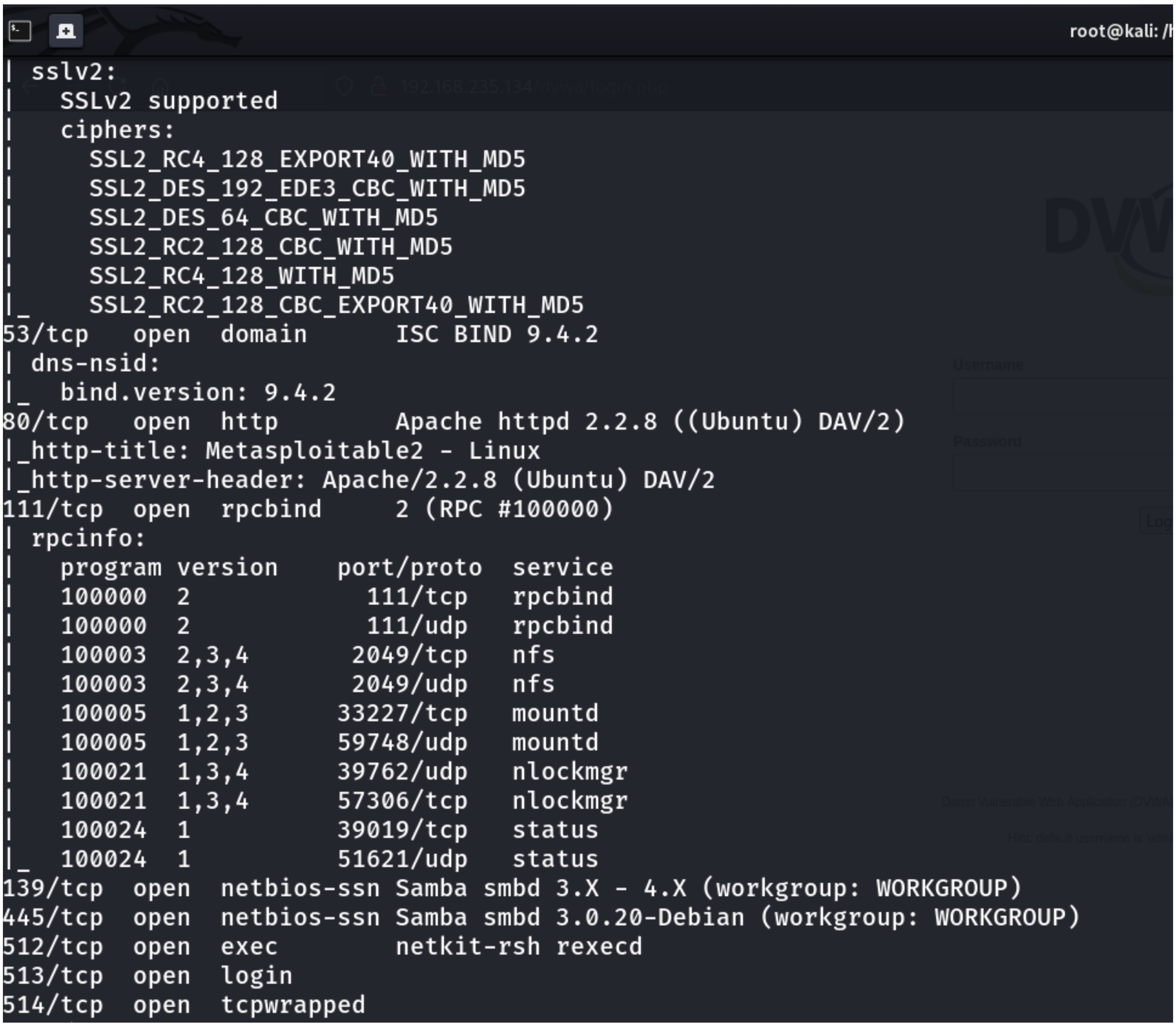
nmap -sS -sV -A 192.168.235.134



```
┌──(root㉿kali)-[/home/arjav]
└─# nmap -sS -sV -A 192.168.235.134
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-06 11:59 IST
Nmap scan report for 192.168.235.134
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.235.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2026-02-06T06:30:35+00:00; 0s from scanner time.
```

**Figure 2: Nmap Reconnaissance Scan (Service & OS Detection)**

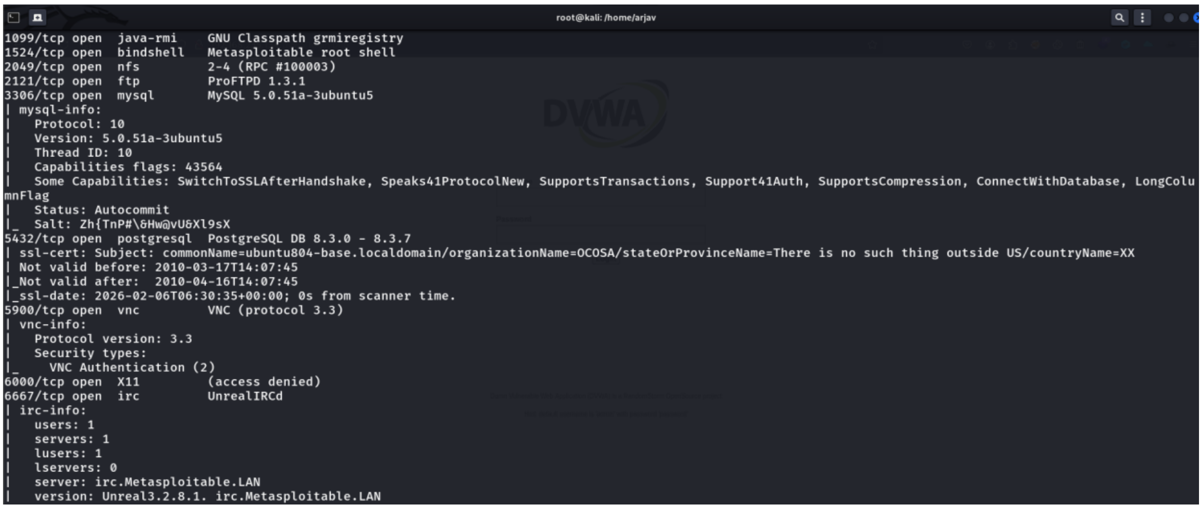
Nmap scan results showing multiple open TCP ports and running services on the target system. The scan reveals exposed services such as FTP, SSH, HTTP, SMTP, DNS, MySQL, and Samba, indicating a large attack surface. Service version detection and OS fingerprinting identify the host as a Linux-based system.



```
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      33227/tcp   mountd
|   100005  1,2,3      59748/udp   mountd
|   100021  1,3,4      39762/udp   nlockmgr
|   100021  1,3,4      57306/tcp   nlockmgr
|   100024  1          39019/tcp   status
|_  100024  1          51621/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
```

**Figure 3: Identification of Vulnerable FTP and SSH Services**

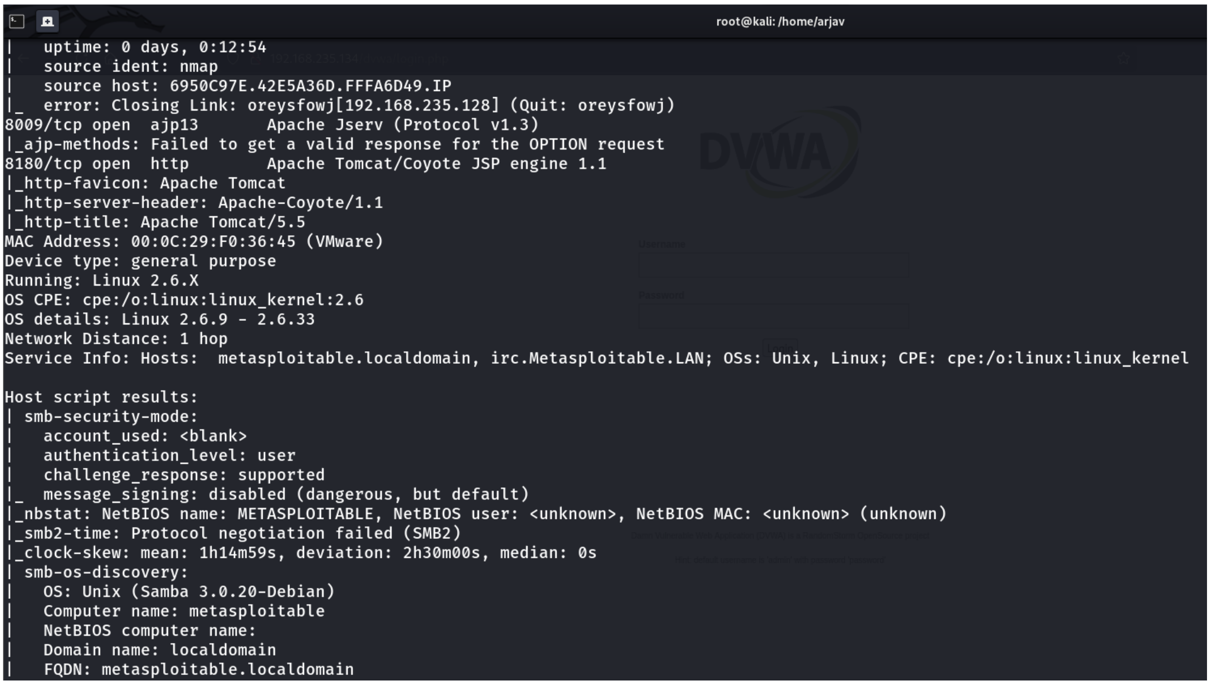
Nmap output highlighting critical services including **vsftpd 2.3.4 (FTP)** with anonymous login enabled and **OpenSSH 4.7p1**, both known to have historical security weaknesses. These services represent potential entry points for exploitation.



```
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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 10
|   Capabilities flags: 43564
|   Some Capabilities: SwitchToSSLAfterHandshake, Speaks41ProtocolNew, SupportsTransactions, Support41Auth, SupportsCompression, ConnectWithDatabase, LongColu
mnFlag
|   Status: Autocommit
|_  Salt: Zh{TnP#\&Hw@vU&Xl9sX
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2026-02-06T06:30:35+00:00; 0s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
```

**Figure 4: Detection of Web, RPC, and File-Sharing Services**

Scan results showing open HTTP (Apache), RPC, NFS, and Samba services. The presence of file-sharing and remote procedure call services increases the risk of unauthorized access and remote exploitation.

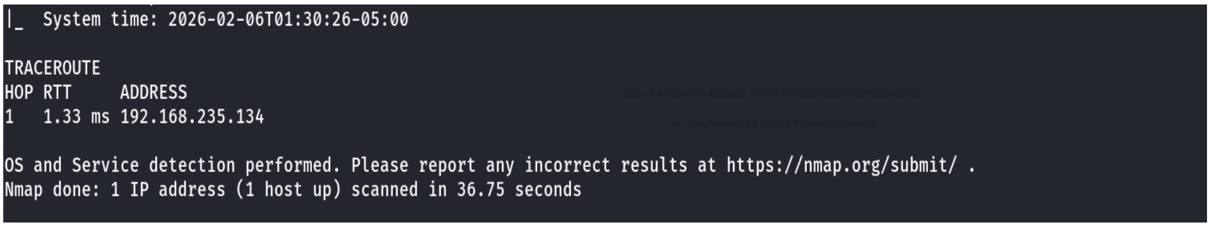


```
|   uptime: 0 days, 0:12:54
|   source ident: nmap
|   source host: 6950C97E.42E5A36D.FFFA6D49.IP
|_  error: Closing Link: oreysfowj[192.168.235.128] (Quit: oreysfowj)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:F0:36:45 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h14m59s, deviation: 2h30m00s, median: 0s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
```

**Figure 5: Enumeration of Database and Remote Access Services**

Nmap scan identifying database services such as **MySQL** and **PostgreSQL**, along with VNC and remote shell services. Exposed database ports may lead to data compromise if weak authentication or misconfigurations exist.



```
|_  System time: 2026-02-06T01:30:26-05:00

TRACEROUTE
HOP RTT     ADDRESS
1   1.33 ms 192.168.235.134

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.75 seconds
```

**Figure 6: Comprehensive Attack Surface Enumeration**

Final Nmap scan output summarizing the complete attack surface of the target system, including IRC, Java RMI, bind shell, and multiple legacy services. This enumeration phase confirms that the system is intentionally vulnerable and suitable for penetration testing exercises.

**Findings:**

- Port 80 (HTTP) – Web Application
- Port 21 (FTP) – File Transfer Service
- Port 22 (SSH) – Secure Shell

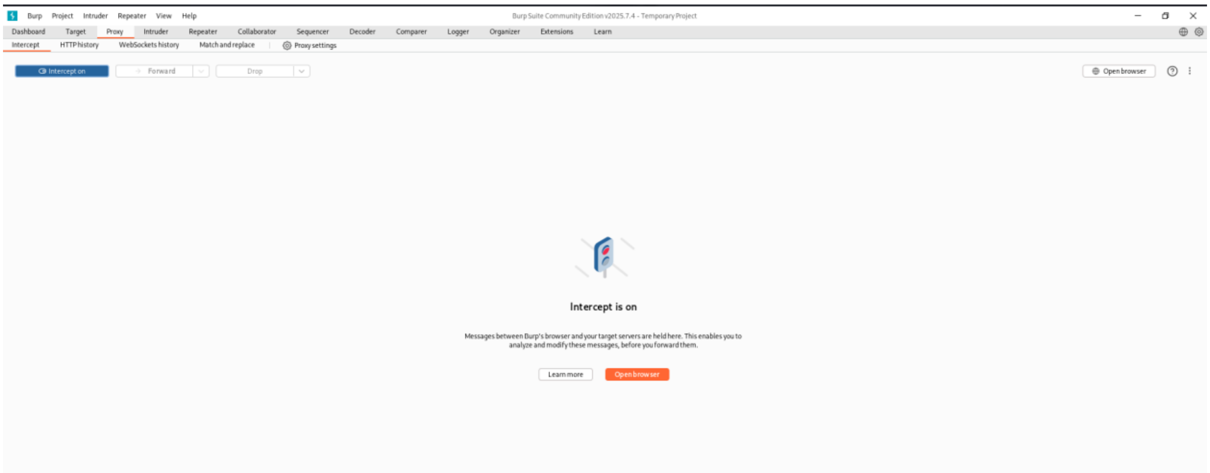
These open services increased the attack surface and were further analyzed for vulnerabilities.

---

### 5. Web Application Analysis using Burp Suite

### 5.1 Intercepting HTTP Requests

Burp Suite was configured as a proxy to intercept browser traffic between the client and DVWA server.
Both GET and POST requests were captured and analyzed.



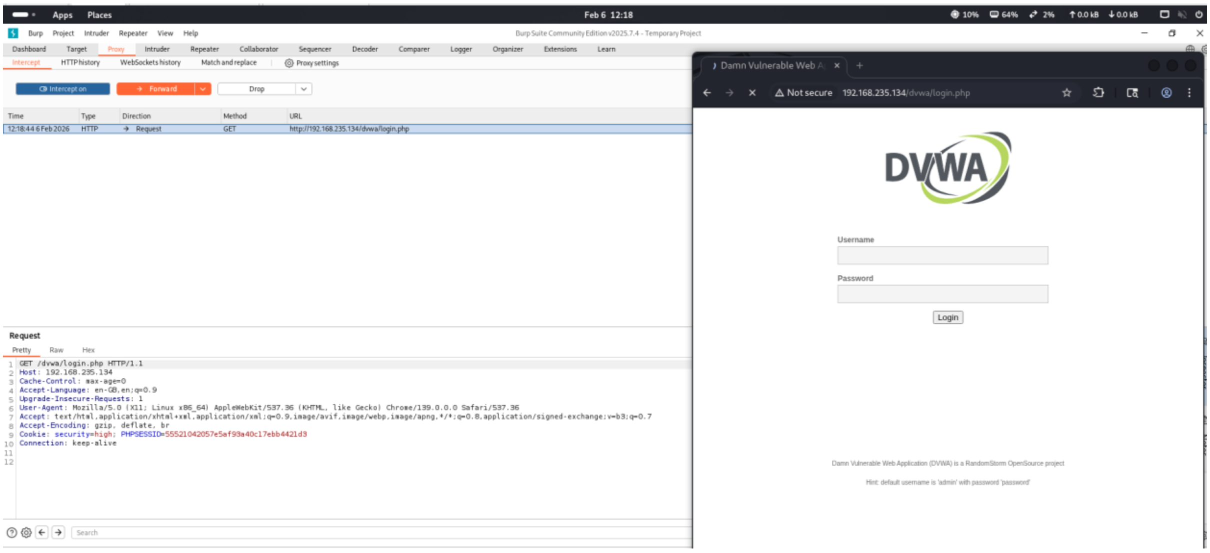
Intercept is on

Messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

**Figure 7:** Burp Suite Proxy module with interception enabled. The "Intercept is on" status confirms that HTTP requests between the browser and the target web application are being captured for analysis and modification during security testing.

### GET Request Observation

- Sensitive parameters were visible in the URL.
- This can expose credentials through browser history or logs.



| Time | Type | Direction | Method | URL |
|---|---|---|---|---|
| 12:18:44 6 Feb 2026 | HTTP | → Request | GET | http://192.168.235.134/dvwa/login.php |

Request

```
GET /dvwa/login.php HTTP/1.1
Host: 192.168.235.134
Cache-Control: max-age=0
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: security=high; PHPSESSID=55521042057e5af93a40c17ebb4421d3
Connection: keep-alive


```

Username

Password

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

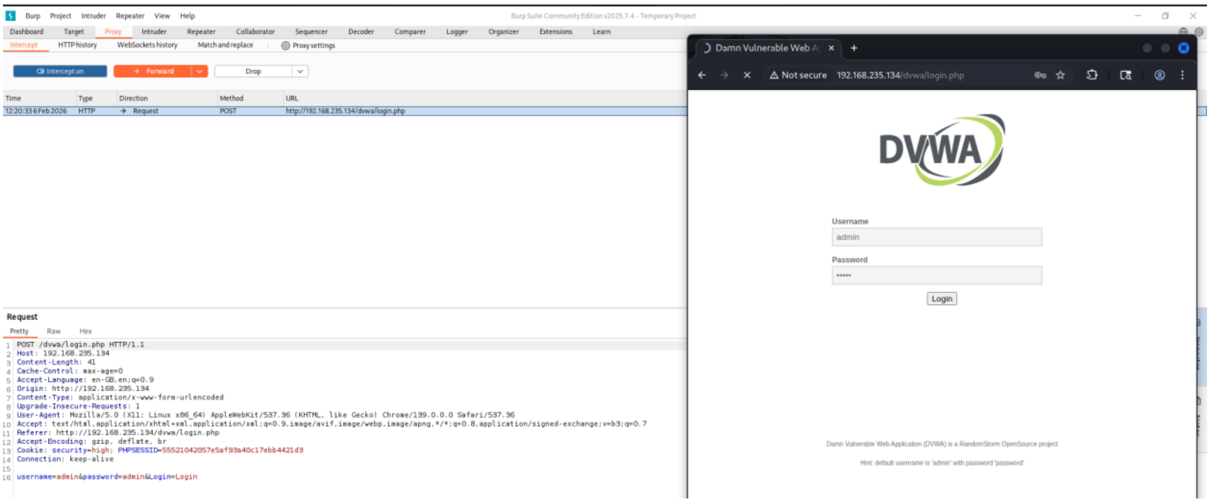
Hint: default username is 'admin' with password 'password'

**Figure 8: Intercepted HTTP GET Request using Burp Suite**

Burp Suite intercepting an HTTP **GET** request sent to the DVWA login page. The captured request shows the target URL and HTTP headers, demonstrating how client requests can be intercepted and analyzed before being forwarded to the server. This highlights the risk of insecure data transmission when using unencrypted HTTP connections.

### POST Request Observation

- Credentials were sent in the request body.
- However, without HTTPS encryption, data can still be intercepted.



| Time | Type | Direction | Method | URL |
|---|---|---|---|---|
| 12:20:33 6 Feb 2026 | HTTP | → Request | POST | http://192.168.235.134/dvwa/login.php |

Username: admin

Password: *****

```
POST /dvwa/login.php HTTP/1.1
Host: 192.168.235.134
Content-Length: 41
Cache-Control: max-age=0
Accept-Language: en-GB,en;q=0.9
Origin: http://192.168.235.134
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.235.134/dvwa/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=high; PHPSESSID=55521042057e5af93a40c17ebb4421d3
Connection: keep-alive

username=admin&password=admin&Login=Login
```

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

**Figure 9: Intercepted HTTP POST Request Containing Login Credentials**

Burp Suite intercepting an HTTP **POST** request sent to the DVWA login endpoint. The request body clearly reveals user-supplied credentials (username=admin and password=admin) transmitted in plaintext over an unencrypted HTTP connection. This demonstrates how sensitive authentication data can be intercepted by an attacker when secure communication mechanisms are not implemented.

---

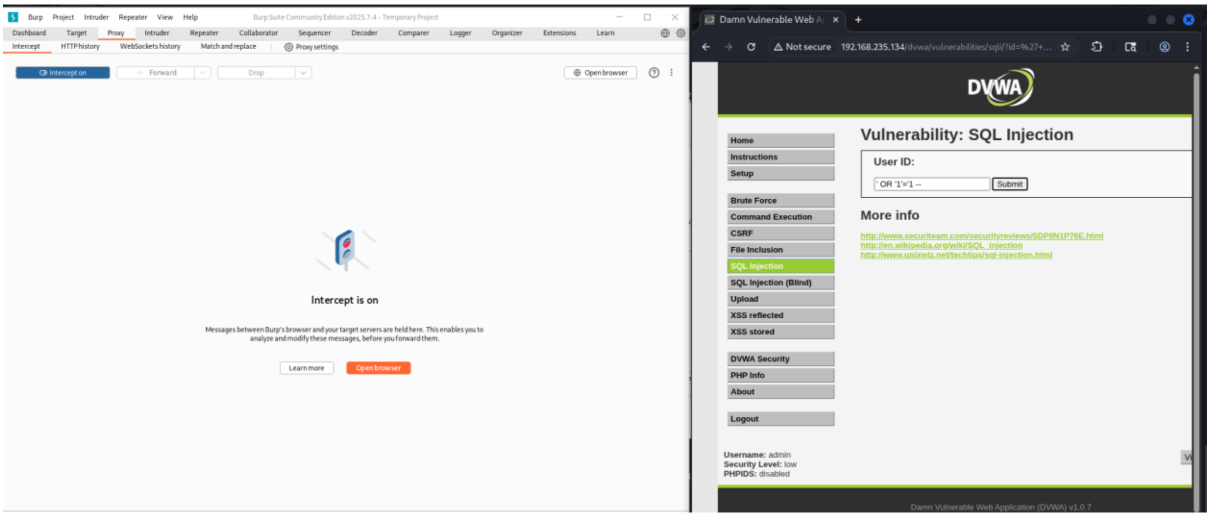
### 5.2 Parameter Manipulation & SQL Injection Testing

User input fields were modified using Burp Suite to test for SQL Injection vulnerabilities.

**Payload Used:**

' OR '1'='1 --

The application returned database errors, indicating improper input validation and a possible SQL Injection vulnerability.



Intercept is on

Messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

Vulnerability: SQL Injection

User ID: ' OR '1'='1 --

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

**Figure 10: Successful SQL Injection Exploitation using Crafted Input Payload**

A SQL Injection attack performed on the DVWA SQL Injection module using the payload ' OR '1'='1 --. The payload bypasses input validation and alters the backend SQL query logic, confirming the presence of a SQL Injection vulnerability that allows unauthorized access to database records.

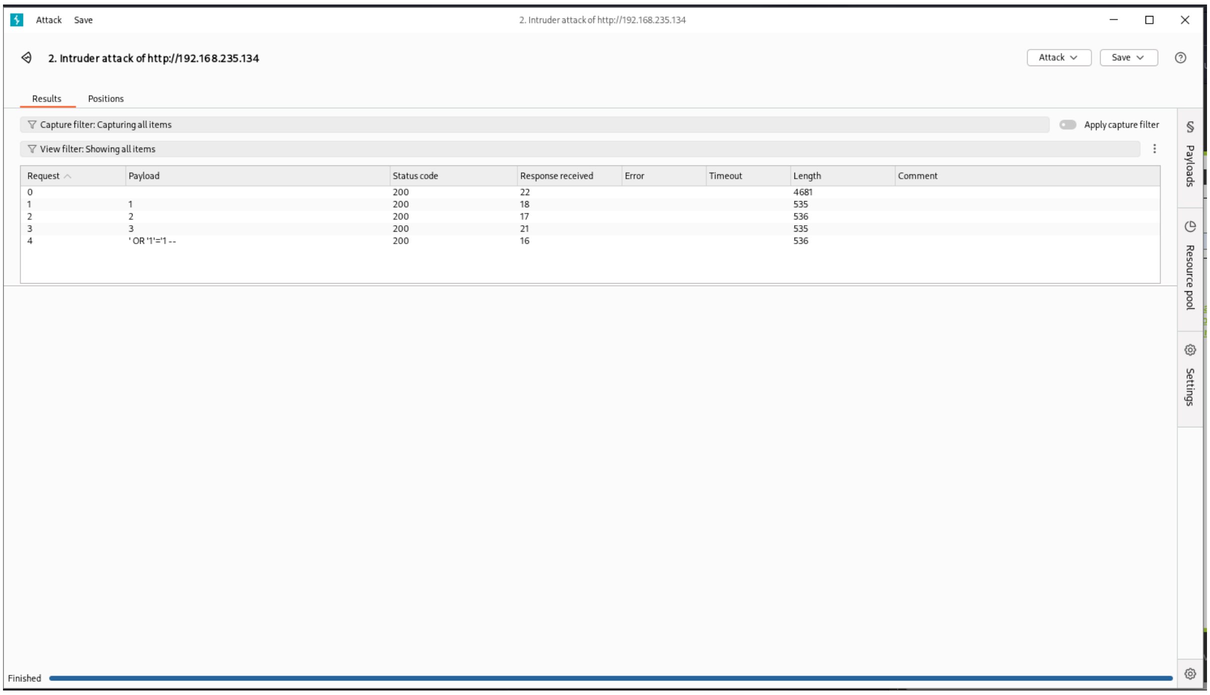
### 5.3 Fuzzing with Burp Intruder

Burp Intruder was used to automate testing of login credentials.

**Payloads Used:**

- Usernames: admin, test, user
- Passwords: password, 123456, admin

**Result:**
Weak credentials such as **admin:password** were accepted, indicating poor authentication security.


Attack
Save
2. Intruder attack of http://192.168.235.134
2. Intruder attack of http://192.168.235.134
Attack
Save
Results
Positions
Capture filter: Capturing all items
Apply capture filter
View filter: Showing all items
Payloads
Resource pool
Settings
Finished

| Request | Payload | Status code | Response received | Error | Timeout | Length | Comment |
|---|---|---|---|---|---|---|---|
| 0 | | 200 | 22 | | | 4681 | |
| 1 | 1 | 200 | 18 | | | 535 | |
| 2 | 2 | 200 | 17 | | | 536 | |
| 3 | 3 | 200 | 21 | | | 535 | |
| 4 | ' OR '1'='1 -- | 200 | 16 | | | 536 | |

**Figure 11: Automated SQL Injection Testing using Burp Suite Intruder**

Burp Suite Intruder executing an automated attack against the id parameter using multiple payloads. Variations in response length for different payloads indicate abnormal server behavior, confirming improper input validation and the presence of a SQL Injection vulnerability.

## 6. Exploitation Phase

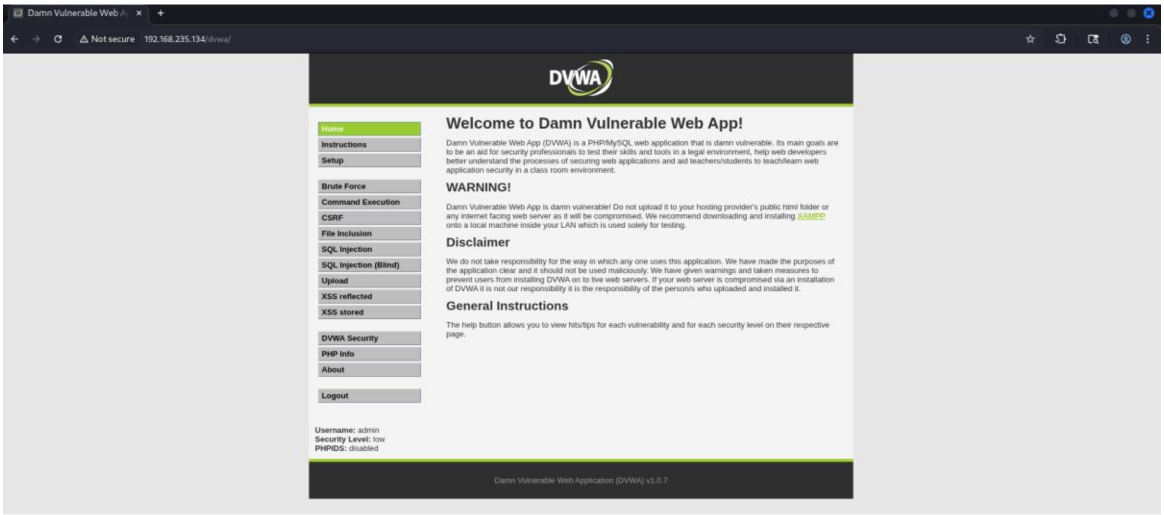
### 6.1 Authentication Bypass Exploitation

Due to weak authentication controls, unauthorized access to the application was achieved using default credentials.

**Impact:**

- Unauthorized access to application features
- Exposure of sensitive data

**Severity:** Medium



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

**Figure 12: Successful Authentication and Access to DVWA Dashboard**

The DVWA dashboard displayed after successful login using default credentials. This confirms weak authentication controls, allowing unauthorized users to gain full access to the application once valid credentials are discovered.

## 7. Vulnerability Summary & Impact Analysis

| Vulnerability | Severity | Impact |
|---|---|---|
| SQL Injection | High | Database manipulation & data leakage |
| Weak Authentication | Medium | Unauthorized access |
| Sensitive Data Exposure | Medium | Credential leakage |

## 8. Mitigation Recommendations

⍰ Implement strong input validation and prepared statements
⍰ Enforce strong password policies
⍰ Disable default credentials
⍰ Use HTTPS to encrypt data in transit
⍰ Apply security patches regularly

## 9. Conclusion

This VAPT exercise demonstrated how common web vulnerabilities can be identified and exploited using standard security tools.
The project highlights the importance of secure coding practices, proper authentication mechanisms, and proactive vulnerability assessment to protect web applications.

## 10. References

- OWASP Testing Guide
- Burp Suite Documentation
- DVWA Official Documentation