**PENETRATION TEST REPORT**

Metasploitable 2 — Infrastructure Assessment

⚠ **CONFIDENTIAL — RESTRICTED DISTRIBUTION** ⚠

|  |  |
| --- | --- |
| **REPORT CLASSIFICATION** | CONFIDENTIAL |
| **TARGET SYSTEM** | Metasploitable 2 |
| **TARGET IP ADDRESS** | 192.168.56.104 |
| **ATTACKER MACHINE** | Kali Linux — 192.168.56.101 |
| **TEST DATE** | 23 February 2026 |
| **TESTER** | Azizul Rahman |
| **PROGRAM** | Masters of Cybersecurity |
| **REPORT VERSION** | 1.0 — Final |
| **OVERALL RISK RATING** | * **CRITICAL** |

**OVERALL RISK RATING**

**CRITICAL**

11 Vulnerabilities · 5 Critical · Root Access Achieved via 5 Methods

|  |  |
| --- | --- |
| **Prepared By**  **Azizul Rahaman**  Masters of Cybersecurity Department of Cybersecurity | **Submitted To**  **Satch Hegde**  Assessment: Module 8 — Penetration Testing  23 February 2026 |

# 1. EXECUTIVE SUMMARY

A comprehensive penetration test was conducted against a Metasploitable 2 target system (192.168.56.104) from an attacker machine running Kali Linux (192.168.56.101) on an isolated VirtualBox Host-Only network. The assessment simulated a realistic internal network attack scenario, testing all major attack surfaces including network services, web applications, and post-exploitation capabilities.

The results were severe. The target system was fully compromised using multiple independent attack vectors, with root-level access achieved through 5 distinct exploitation methods within a single testing session. All 11 attack objectives were successfully completed, ranging from unauthenticated remote code execution via known CVEs to web application attacks including SQL injection and Cross-Site Scripting.

The system's overall security posture is rated CRITICAL. No meaningful security controls were observed

no firewall, no intrusion detection, no patch management, and no secure configuration baseline.

**1.1 Key Statistics**

|  |  |
| --- | --- |
| **Metric** | **Value** |
| Total Vulnerabilities Found | 11 |
| Critical Severity | 5 |
| High Severity | 4 |
| Medium Severity | 2 |
| Root Access Achieved | YES — 5 independent methods |
| Password Hashes Obtained | YES — all system accounts |
| Web App Vulnerabilities | 4 (SQLi, CMDi, XSS Reflected, XSS Stored) |
| Time to First Root Shell | < 30 seconds |

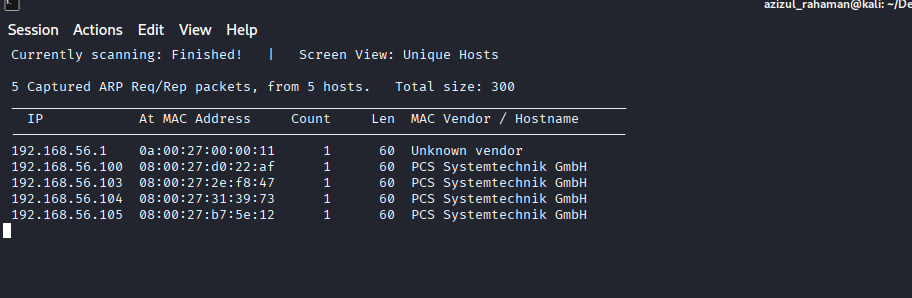
# 2. SCOPE & METHODOLOGY

* 1. **Scope**

|  |  |
| --- | --- |
| **Parameter** | **Details** |
| Target IP | 192.168.56.104 |
| Target OS | Ubuntu 8.04 (Linux 2.6.24-16-server i686) |
| Network | 192.168.56.0/24 (VirtualBox Host-Only — isolated) |
| Attacker IP | 192.168.56.101 |
| Attacker OS | Kali Linux 2024 (Metasploit v6.4.84) |
| Test Type | Black-box internal network penetration test |
| Authorization | Authorized lab environment — Metasploitable 2 |

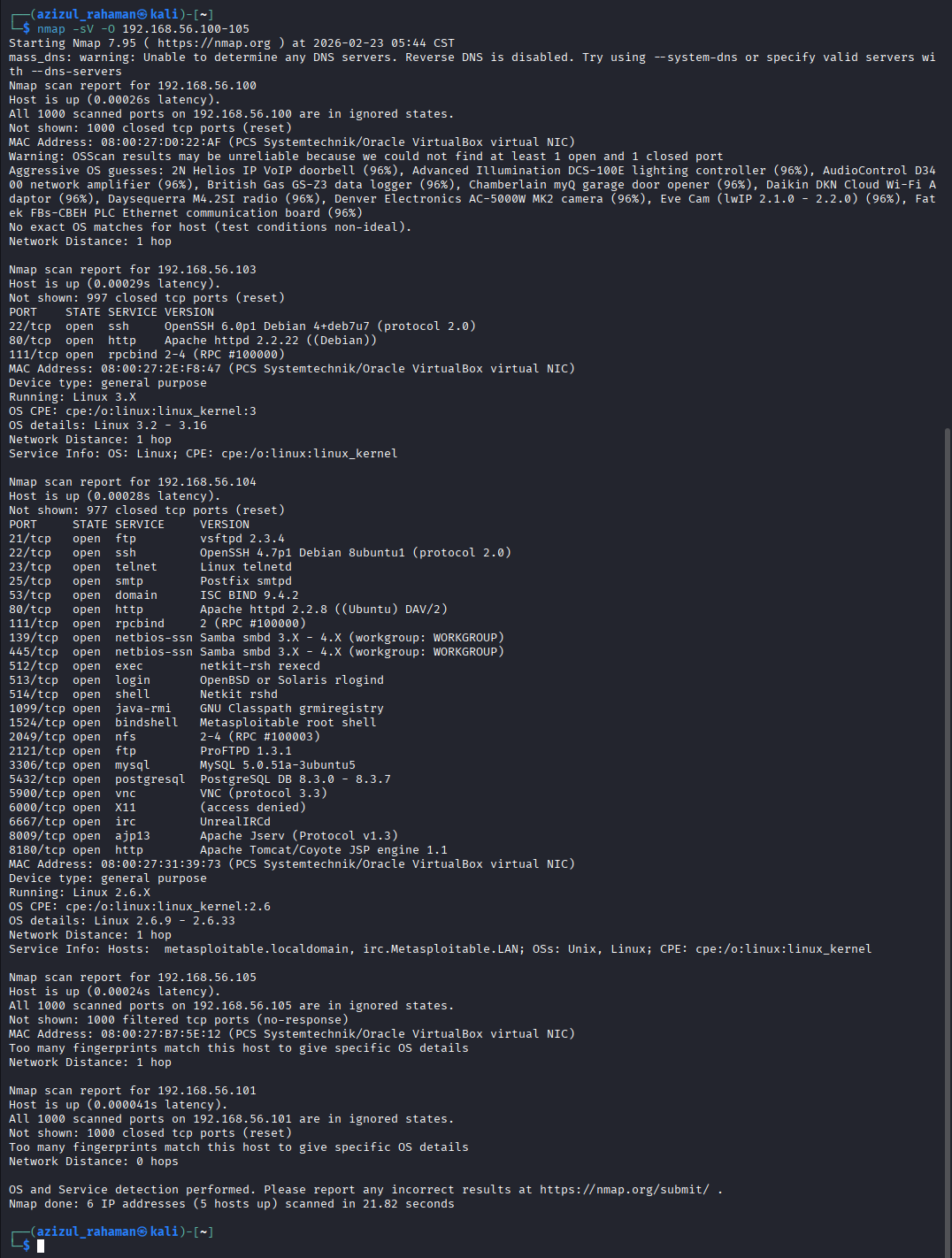
* 1. **Reconnaissance — Network Discovery**

The assessment began with ARP-based network discovery using netdiscover to identify all live hosts on the subnet, followed by a comprehensive Nmap service version scan.



netdiscover ARP scan: 5 hosts discovered on 192.168.56.0/24 including target 192.168.56.104

Nmap -sV service scan: all open ports enumerated on 192.168.56.104 revealing vsftpd 2.3.4, Samba 3.x, port 1524 bindshell, MySQL, PostgreSQL, Apache, OpenSSH



* 1. **Methodology — PTES Framework**

|  |  |  |
| --- | --- | --- |
| **Phase** | **Activities** | **Tools Used** |
| 1. Reconnaissance | ARP scan, host discovery, network mapping | netdiscover, arp-scan |
| 2. Scanning | Port scan, service version detection, OS fingerprint | Nmap 7.x (-sV -sC -O) |
| 3. Exploitation | CVE exploitation, web application attacks | Metasploit, Netcat, Browser |
| 4. Post- Exploitation | Privilege escalation, credential dumping, pivoting | John the Ripper, Meterpreter |
| 5. Reporting | Documentation, risk rating, remediation guidance | This report |

# 3. FINDINGS SUMMARY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Vulnerability** | **CVE** | **Risk** | **CVSS** |
| 1 | Unauthenticated Root Backdoor — Port 1524 | — | **Critical** | 10.0 |
| 2 | vsftpd 2.3.4 Backdoor — Remote Code Execution | CVE-2011- 2523 | **Critical** | 10.0 |
| 3 | Samba Usermap Script — Remote Code Execution | CVE-2007- 2447 | **Critical** | 9.3 |
| 4 | Default SSH Credentials + Privilege Escalation | — | **Critical** | 9.0 |
| 5 | Meterpreter Post-Exploitation | — | **Critical** | 8.8 |
| 6 | SQL Injection — DVWA (UNION-based) | — | **High** | 8.5 |
| 7 | OS Command Injection — DVWA | — | **High** | 8.0 |
| 8 | Reflected XSS + Session Cookie Theft | — | **High** | 7.2 |
| 9 | Stored XSS — Persistent Cookie Theft | — | **High** | 6.5 |
| 10 | Sensitive Data Exposure (/etc/shadow) | — | **Medium** | 6.0 |
| 11 | Sensitive Data Exposure (/etc/passwd via Web) | — | **Medium** | 5.3 |

|  |  |  |
| --- | --- | --- |
| **Severity** | **Count** | **Percentage** |
| **Critical** | 5 | 45% |
| **High** | 4 | 36% |
| **Medium** | 2 | 18% |
| Low | 0 | 0% |

**4. DETAILED FINDINGS**

**Finding 1 — Unauthenticated Root Backdoor (Port 1524)**

|  |  |
| --- | --- |
| **Severity** | **Critical** |
| **CVSS Score** | 10.0 |
| **Port/Service** | 1524/tcp — Metasploitable bindshell |
| **CVE** | N/A — Intentional backdoor |

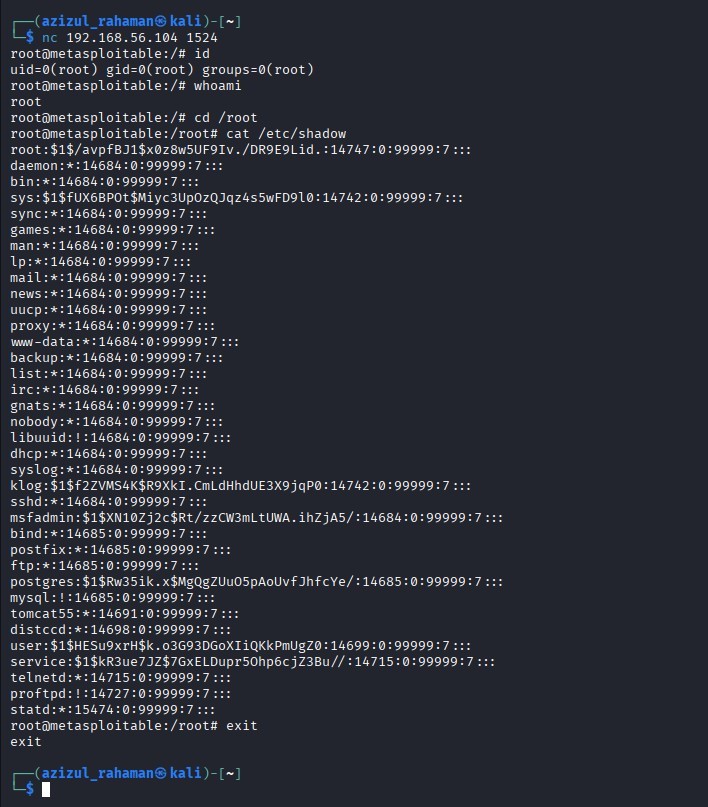
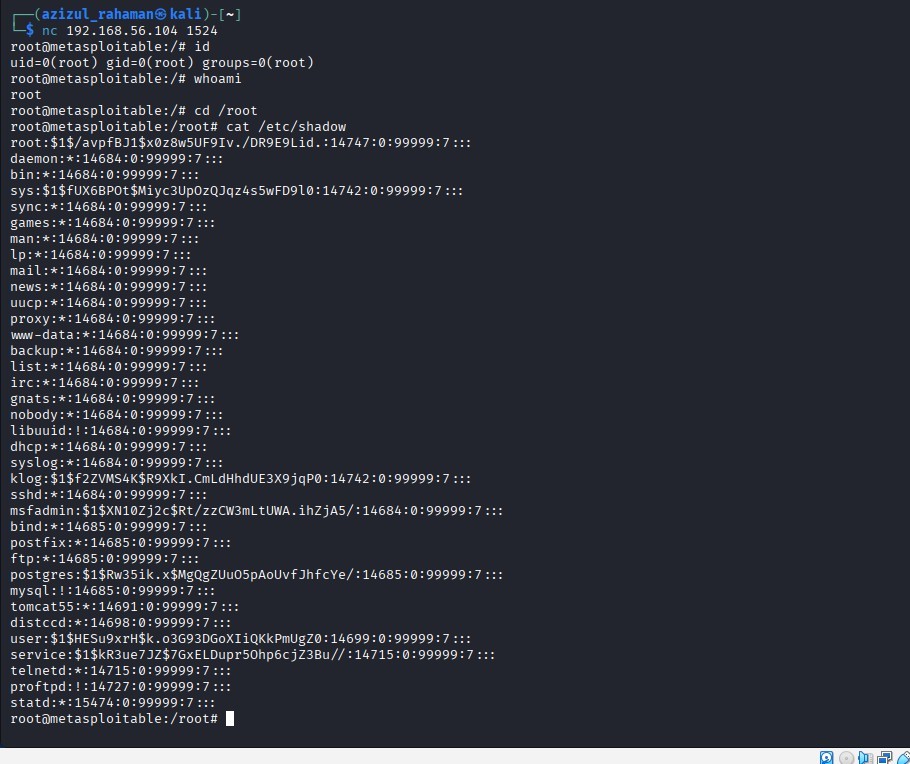
Port 1524 was found open on the target, providing an unauthenticated root shell to any connecting client. No credentials or special knowledge required a single Netcat command yielded instant root access plus full /etc/shadow dump.

Netcat to port 1524: instant root shell, id=uid=0(root), /etc/shadow dumped

$ nc 192.168.56.104 1524

root@metasploitable:/# id

uid=0(root) gid=0(root) groups=0(root)



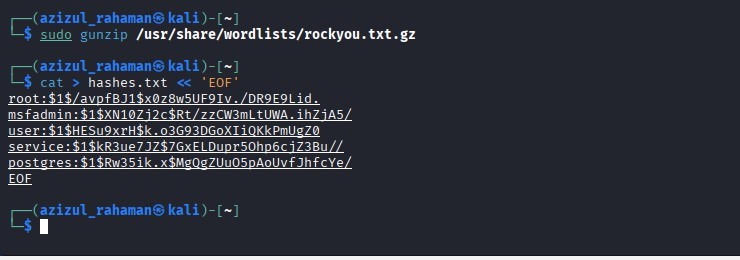
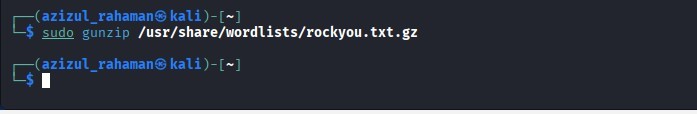
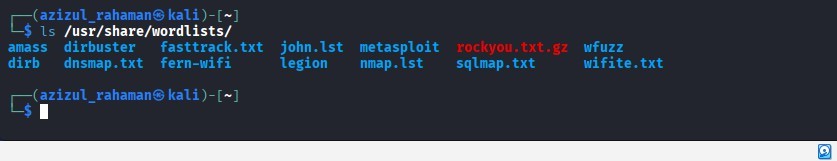
Full /etc/shadow contents obtained via root backdoor showing all system password hashes

Remediation: Close port 1524 via firewall immediately. Audit all listening services. Implement iptables/ufw baseline deny policy.

**Finding 2 — vsftpd 2.3.4 Backdoor (CVE-2011-2523)**

|  |  |
| --- | --- |
| **Severity** | **Critical** |
| **CVSS Score** | 10.0 |
| **Port/Service** | 21/tcp — vsftpd 2.3.4 |
| **CVE** | CVE-2011-2523 |

vsftpd 2.3.4 contains a malicious backdoor inserted into the source distribution in 2011. When a username containing is submitted during FTP authentication, the backdoor opens a root shell on port 6200.



Wordlist directory: rockyou.txt.gz present for password cracking phase

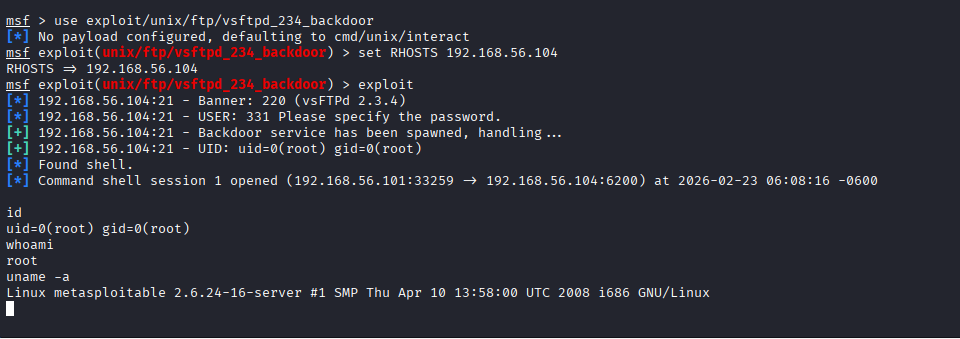
Wordlists at /usr/share/wordlists/ confirmed

hashes.txt prepared from /etc/shadow for John the Ripper

John the Ripper launched with rockyou.txt against MD5-crypt hashes

John the Ripper result: service:service cracked successfully

vsftpd CVE-2011-2523 via Metasploit: Session 1 opened, UID=root confirmed



Remediation: Upgrade vsftpd to 3.x. Replace FTP with SFTP. Verify all software checksums to detect supply chain tampering.

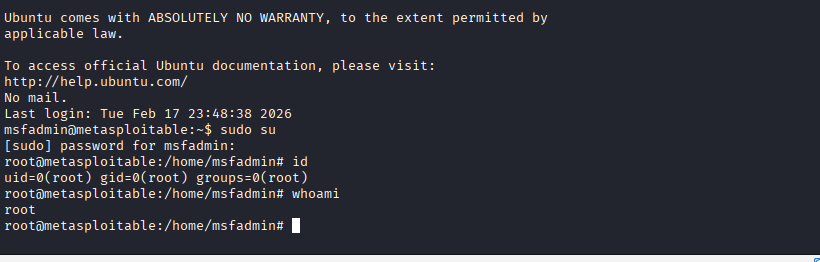
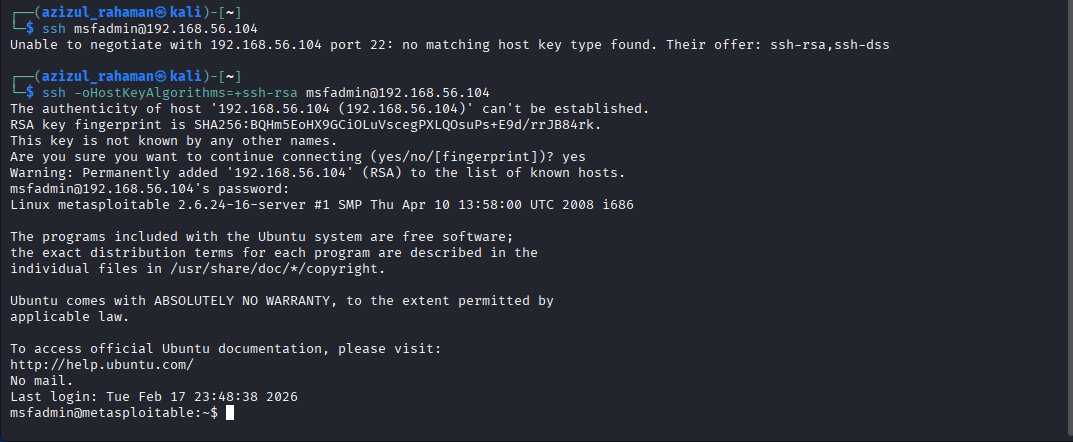
**Finding 3 — Default SSH Credentials & Privilege Escalation**

|  |  |
| --- | --- |
| **Severity** | **Critical** |
| **CVSS Score** | 9.0 |
| **Port/Service** | 22/tcp — OpenSSH 4.7p1 |
| **CVE** | N/A — Configuration weakness |

SSH accepted login with default credentials msfadmin:msfadmin. Once authenticated, unrestricted sudo access allowed immediate escalation to root with no additional barriers.

SSH login: msfadmin:msfadmin accepted, Ubuntu 8.04 banner confirmed

sudo su: privilege escalation to root, id=uid=0(root) gid=0(root)

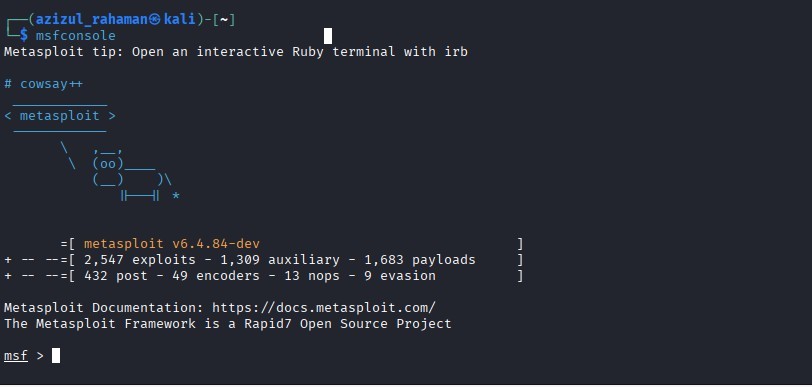


Remediation: Enforce strong passwords. Disable password-based SSH — use key pairs only. Restrict sudo to specific commands per user.

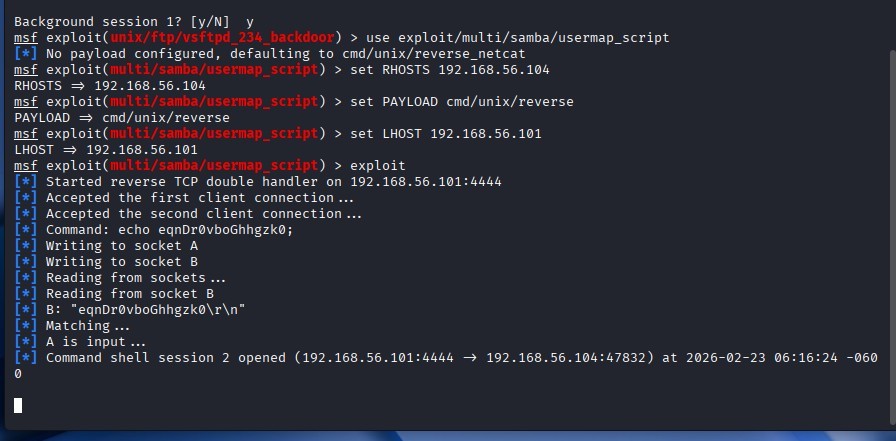
**Finding 4 — Samba Usermap Script RCE (CVE-2007-2447)**

|  |  |
| --- | --- |
| **Severity** | **Critical** |
| **CVSS Score** | 9.3 |
| **Port/Service** | 139/445/tcp — Samba 3.0.20 |
| **CVE** | CVE-2007-2447 |

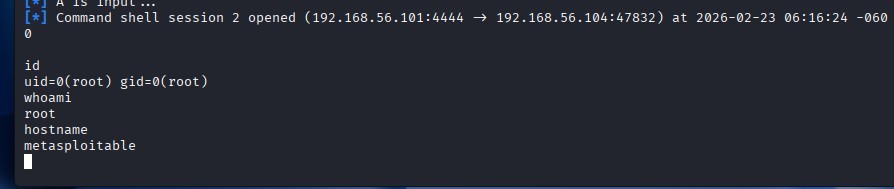
Samba 3.0.0–3.0.25rc3 allows shell metacharacters in the username to execute arbitrary OS commands. Exploited via Metasploit resulting in an unauthenticated root reverse shell (Session 2).



Samba exploit setup: usermap\_script module, RHOSTS=192.168.56.104, PAYLOAD=cmd/unix/reverse



Samba CVE-2007-2447: Session 2 opened 101:4444→104:47832, id=root confirmed



Session 2 shell: uid=0(root), whoami=root, hostname=metasploitable

Remediation: Upgrade Samba to 4.x. Block SMB (139/445) at firewall if not required. Remove 'username map script' from smb.conf.

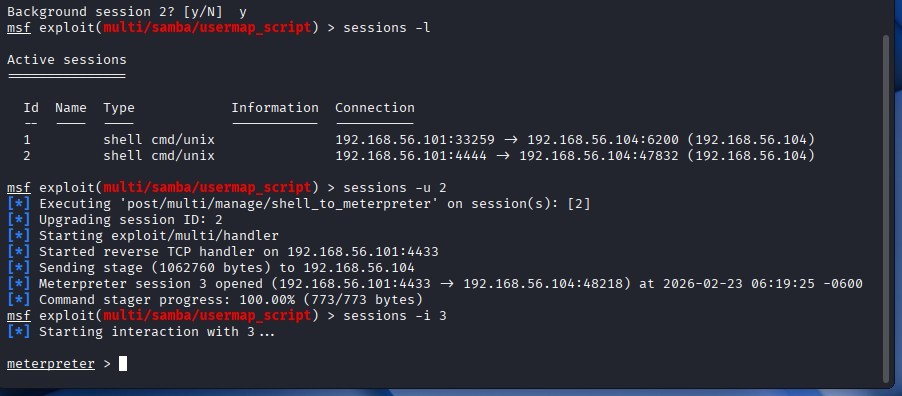
**Finding 5 — Meterpreter Session & Post-Exploitation**

|  |  |
| --- | --- |
| **Severity** | **Critical** |

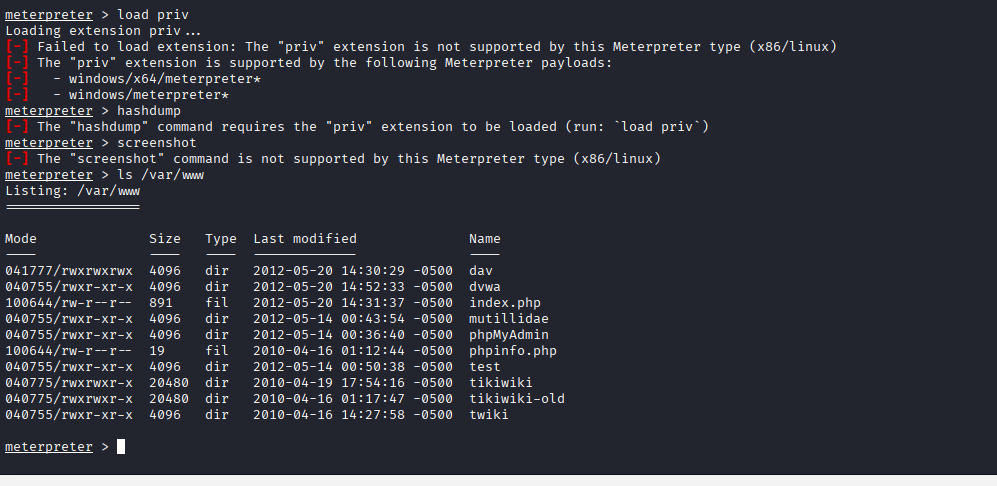
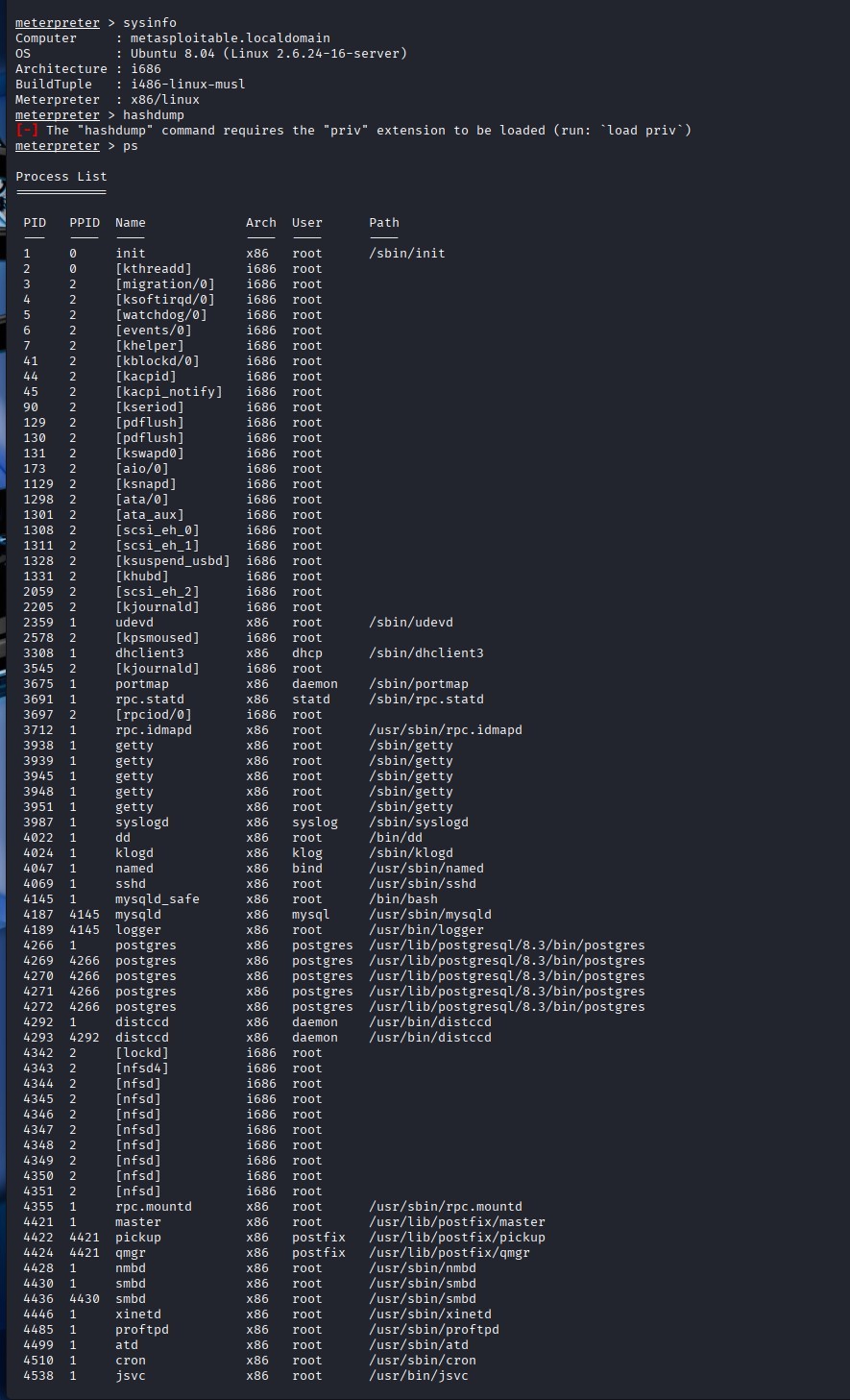
|  |  |
| --- | --- |
| **CVSS Score** | 8.8 |
| **Port/Service** | Session upgrade from Samba shell |
| **CVE** | N/A — Post-exploitation capability |

Samba Session 2 was upgraded to a full Meterpreter session (Session 3), enabling advanced post- exploitation: file system access, process listing, network pivoting, and /etc/shadow extraction.

sessions -u 2: Session 2 upgraded to Meterpreter Session 3, meterpreter> prompt



Meterpreter sysinfo: full OS profile, architecture, hostname confirmed



Meterpreter shell: cat /etc/shadow — root-level file access achieved

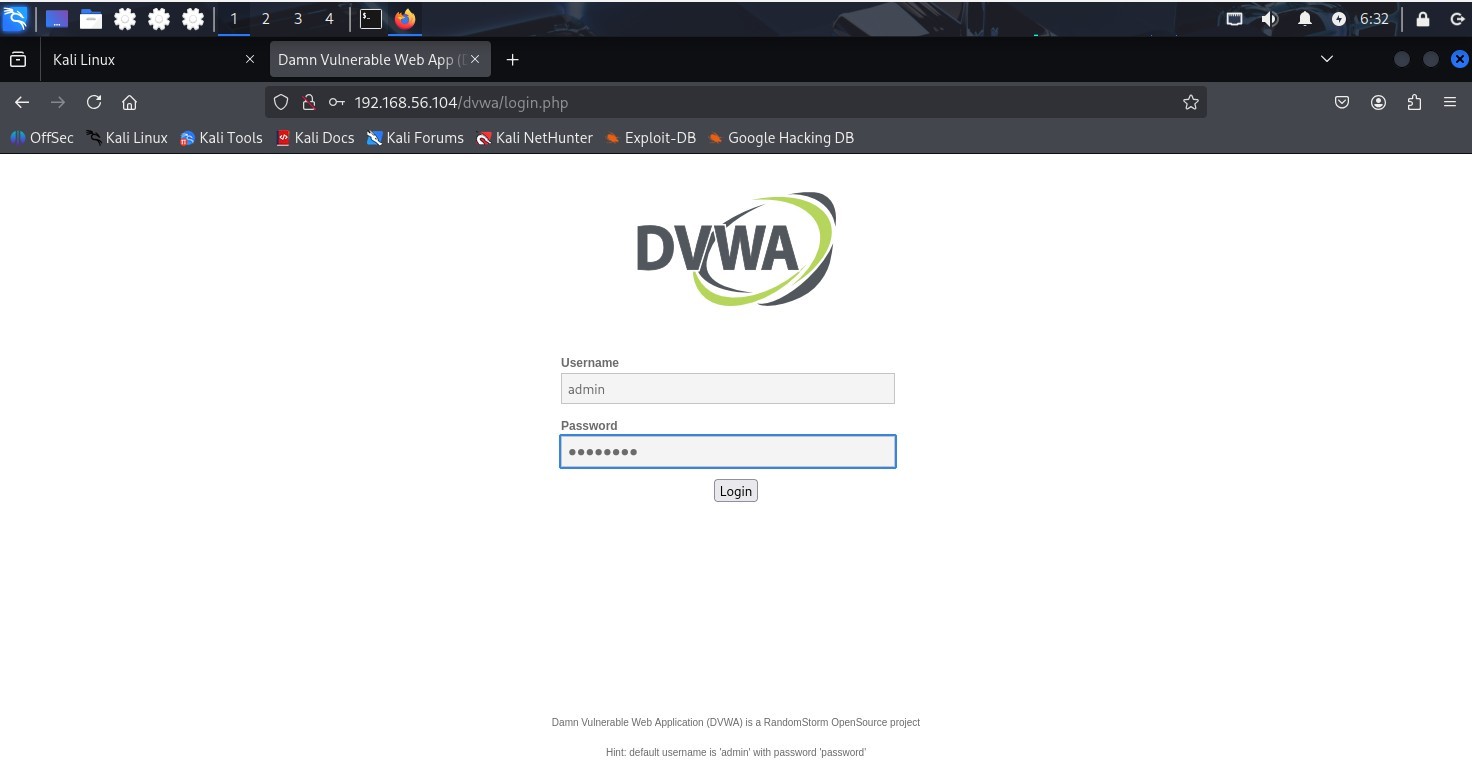
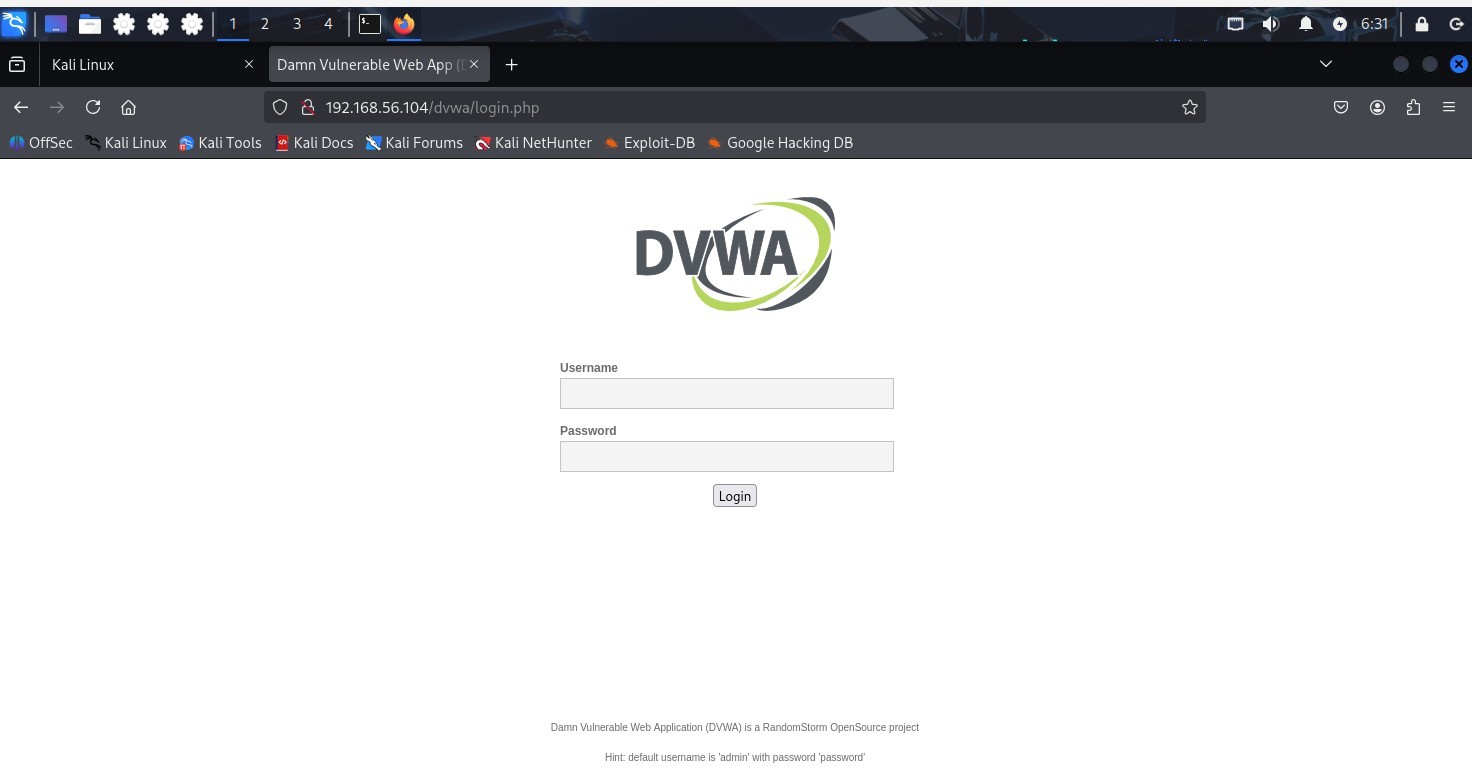
Remediation: Remediate all three underlying exploits (Samba, vsftpd, backdoor). Implement egress filtering and network segmentation.

**Finding 6 — SQL Injection (UNION-Based) — DVWA**

|  |  |
| --- | --- |
| **Severity** | **High** |
| **CVSS Score** | 8.5 |
| **Port/Service** | 80/tcp — Apache 2.2.8 / DVWA |
| **CVE** | N/A — Application vulnerability |

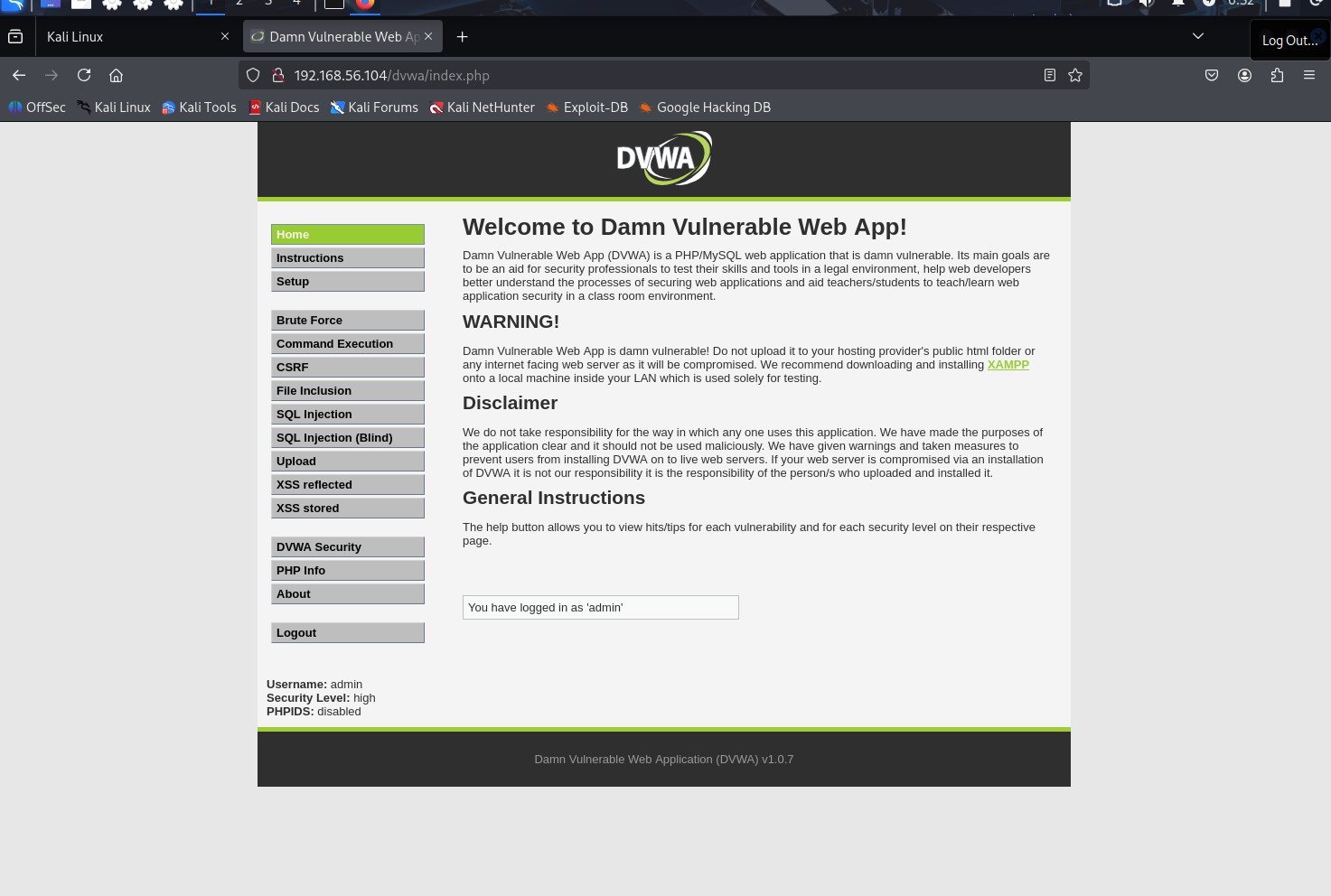
DVWA's SQL Injection module passes unsanitised user input directly into SQL queries. A UNION-based injection extracted all usernames and MD5 password hashes from the database.

Payload: 1' UNION SELECT user, password FROM users#

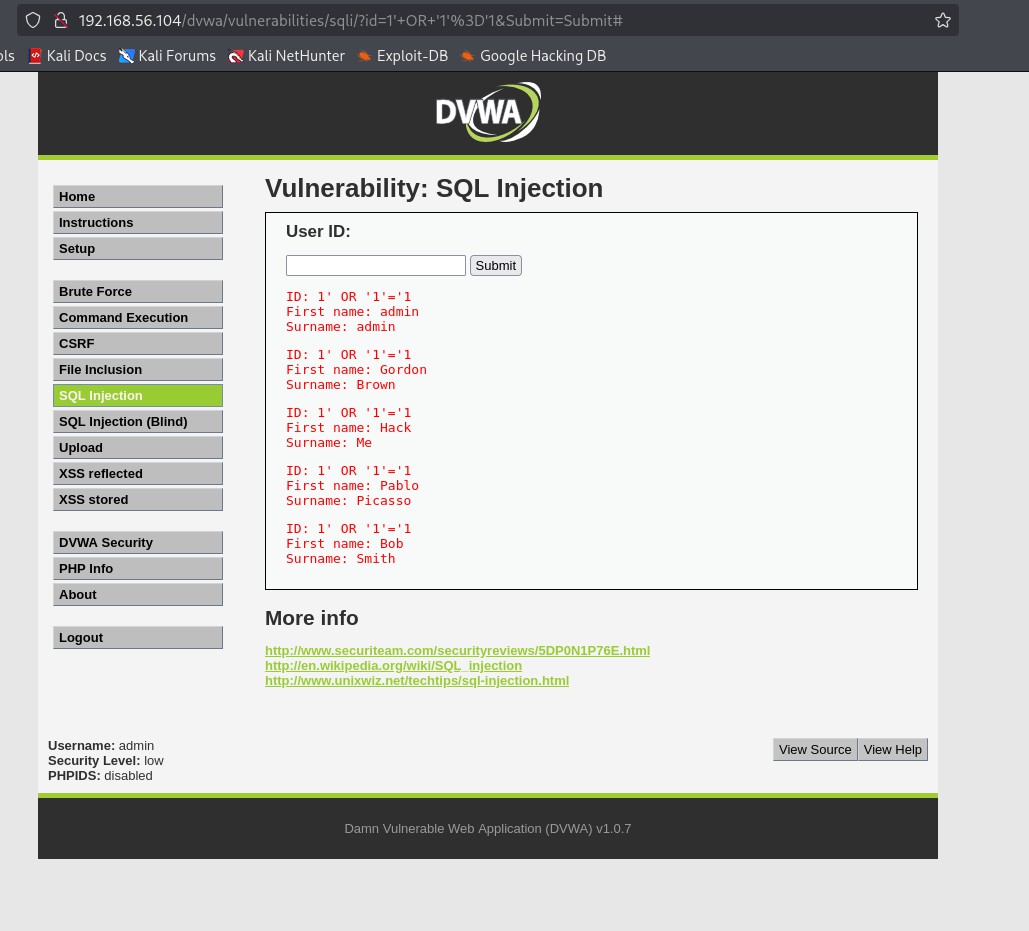


DVWA login: admin:password authenticated successfully

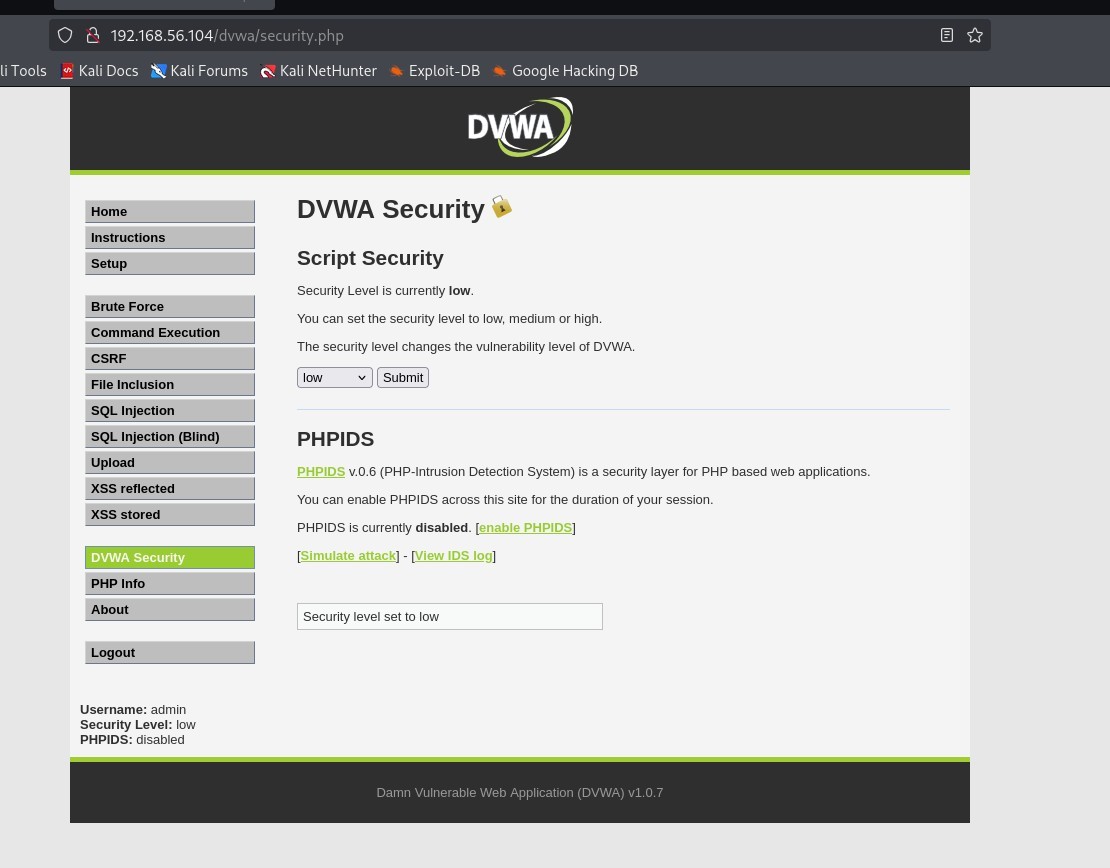
DVWA security level set to LOW — all protections disabled



DVWA SQL Injection module — User ID field identified as vulnerable



OR bypass: 1' OR '1'='1 returns all users from database



UNION SELECT: all usernames and MD5 hashes extracted

admin : 5f4dcc3b5aa765d61d8327deb882cf99 → password gordonb : e99a18c428cb38d5f260853678922e03 → abc123 pablo : 0d107d09f5bbe40cade3de5c71e9e9b7 → letmein smithy : 5f4dcc3b5aa765d61d8327deb882cf99 → password

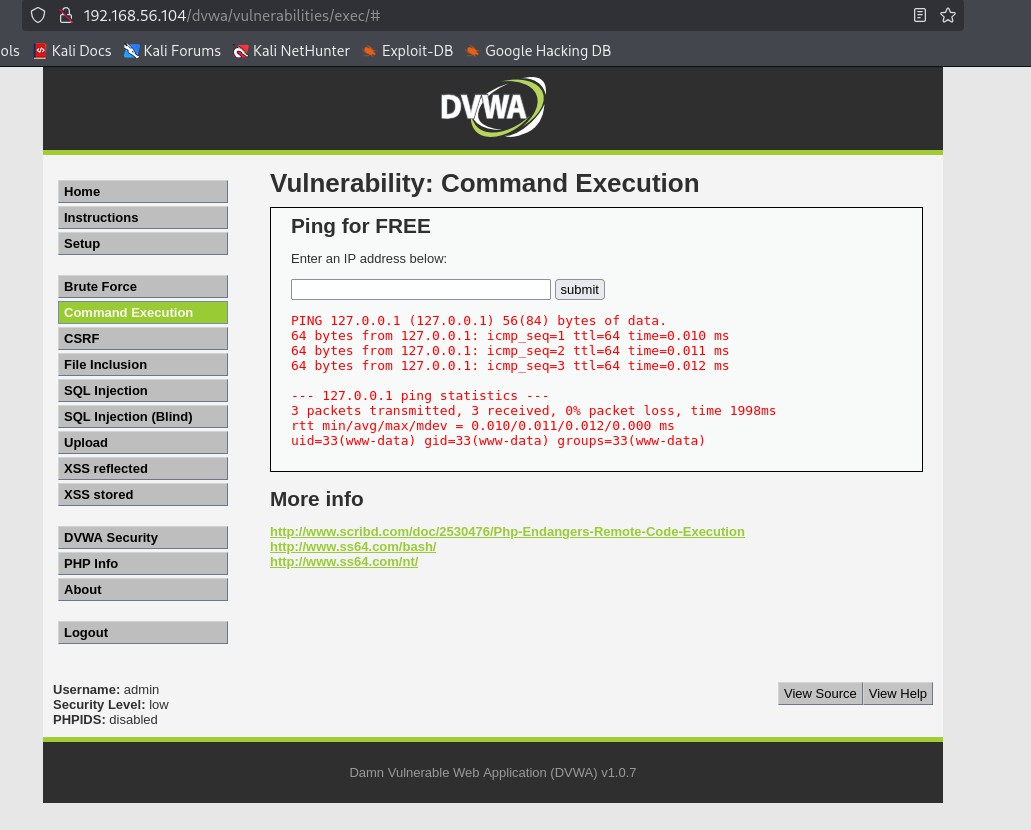
Remediation: Use parameterised queries. Never concatenate user input into SQL. Replace MD5 with bcrypt/Argon2.

**Finding 7 — OS Command Injection — DVWA**

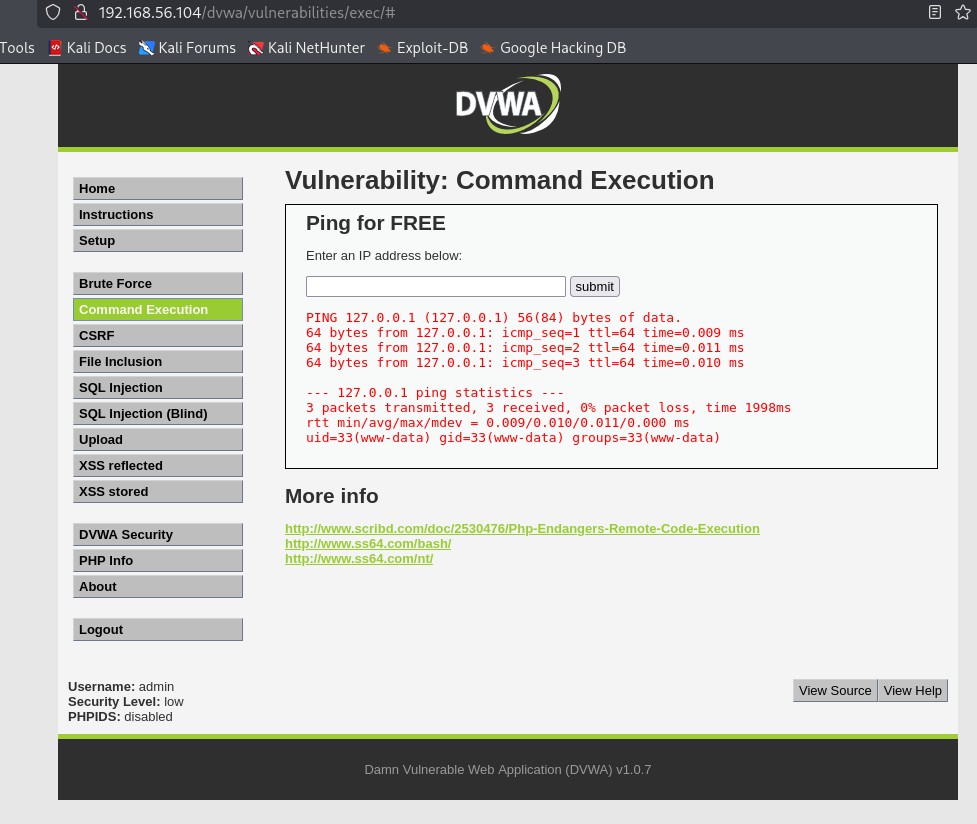
|  |  |
| --- | --- |
| **Severity** | **High** |
| **CVSS Score** | 8.0 |
| **Port/Service** | 80/tcp — Apache 2.2.8 / DVWA |
| **CVE** | N/A — Application vulnerability |

DVWA's Command Execution module passes user input directly to a system shell. Semicolon injection allowed arbitrary OS command execution as www-data, including full /etc/passwd disclosure.

Payload: 127.0.0.1; id → uid=33(www-data) gid=33(www-data) Payload: 127.0.0.1; cat /etc/passwd → Full file disclosed



DVWA Command Execution baseline: ping test successful, uid=www-data returned



cat /etc/passwd: full /etc/passwd dumped via web browser

Remediation: Never pass user data to shell functions. Use native APIs. Whitelist only valid IP address patterns.

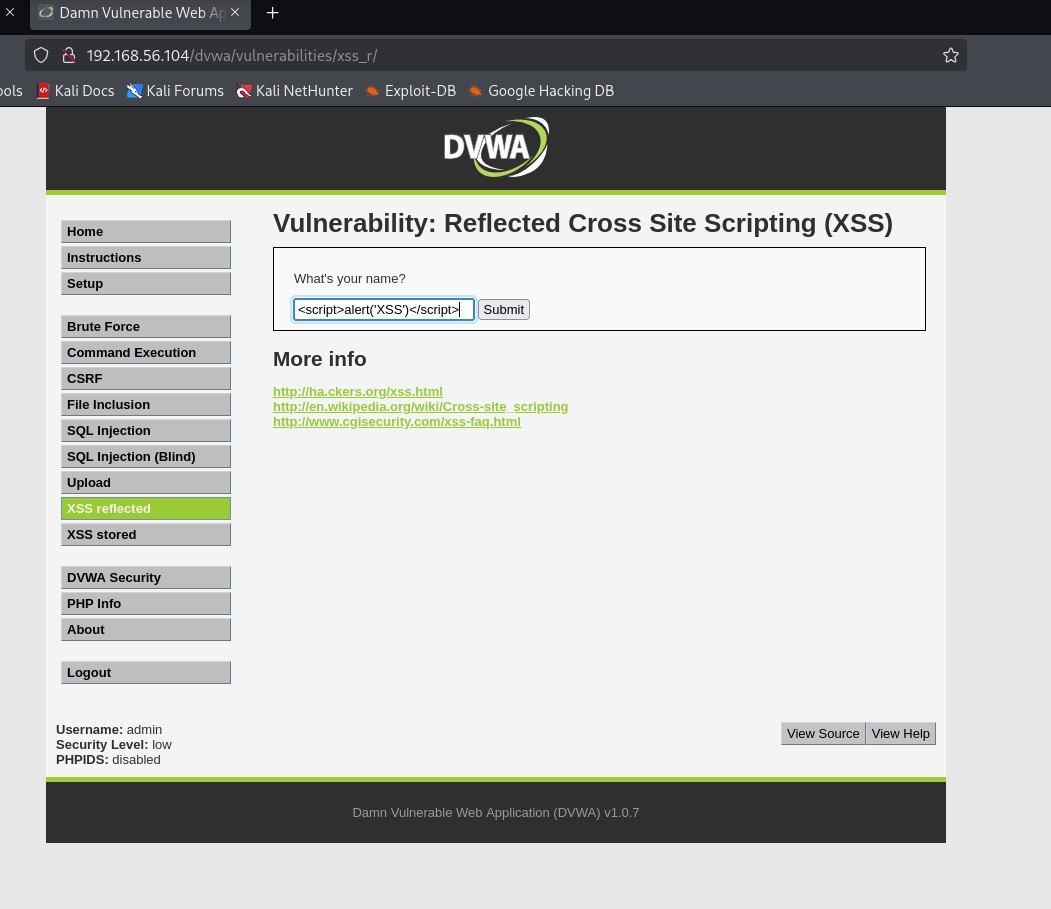
**Finding 8 — Reflected & Stored XSS — DVWA**

|  |  |
| --- | --- |
| **Severity** | **High** |
| **CVSS Score** | 7.2 (Reflected) / 6.5 (Stored) |
| **Port/Service** | 80/tcp — Apache 2.2.8 / DVWA |
| **CVE** | N/A — Application vulnerability |

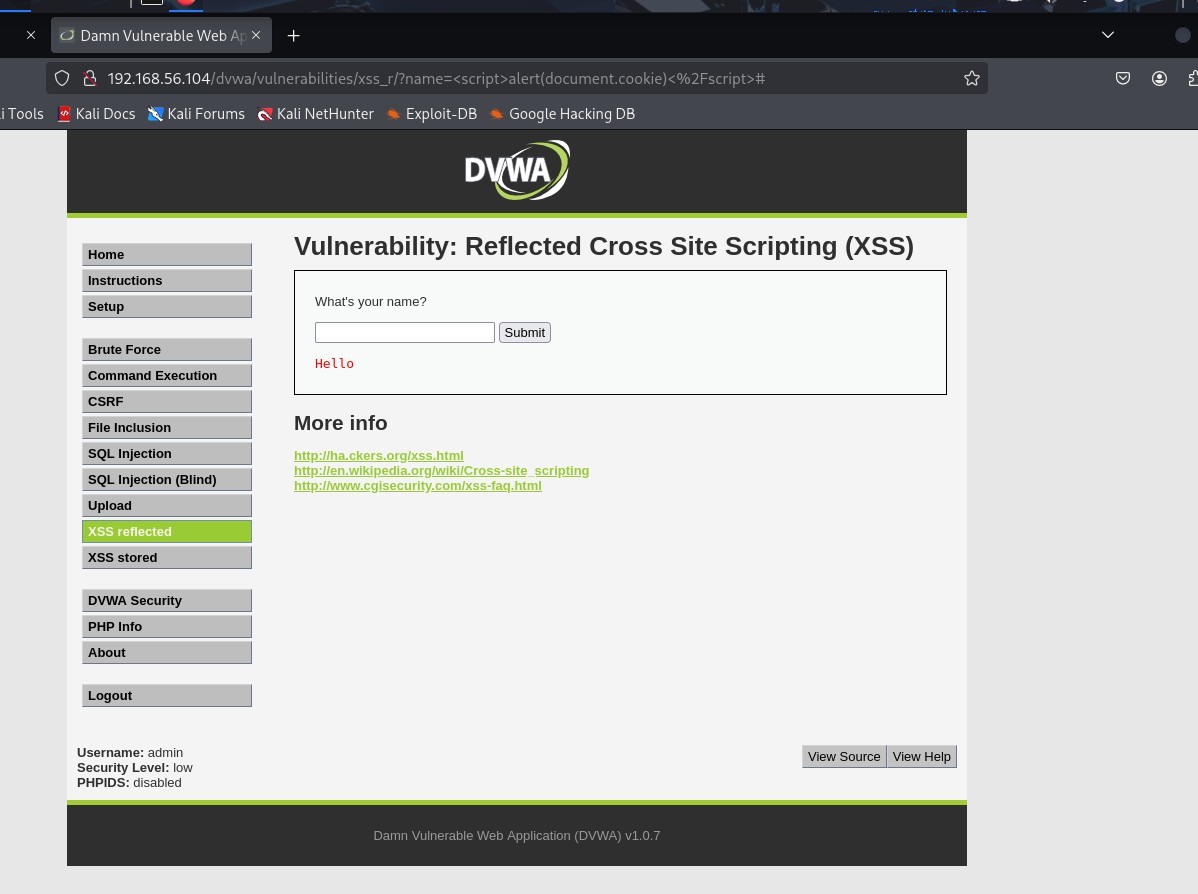
Both reflected and stored XSS vulnerabilities were identified in DVWA. The admin session cookie (PHPSESSID) was successfully stolen via both attack types, enabling account hijacking without credentials.

Payload: <script>alert(document.cookie)</script>

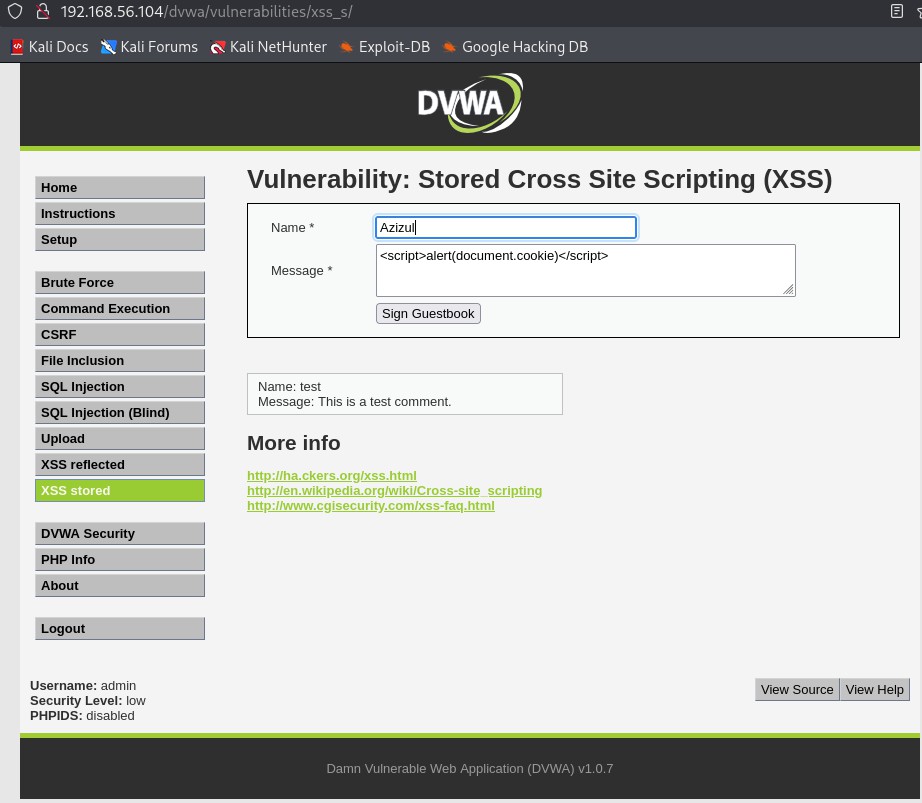
Cookie stolen: security=low; PHPSESSID=2f47d5b2729132d9cefe88b9f4d7aed4



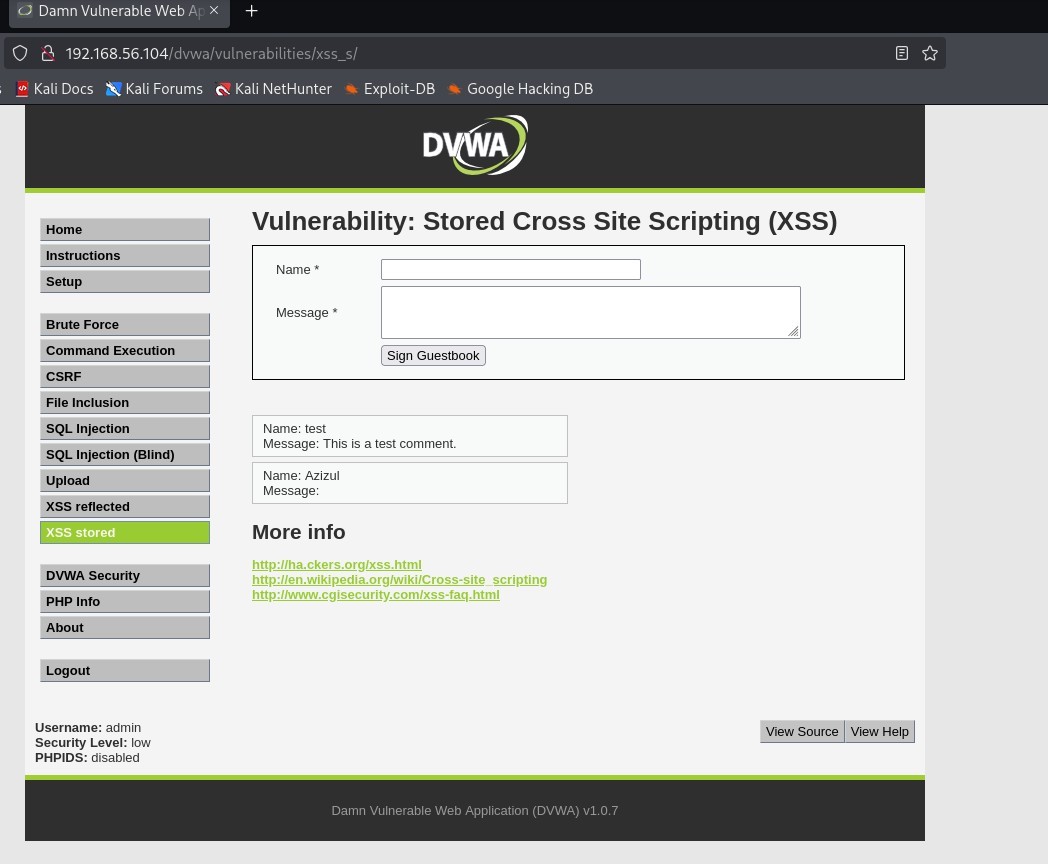
Reflected XSS: payload fires, popup shows PHPSESSID cookie stolen



Stored XSS: payload submitted to guestbook, persisted to database



Stored XSS fires on page load: cookie popup executes for every visitor



Stored XSS confirmed persistent: executes on every subsequent visit

Remediation: Encode all output with htmlspecialchars(). Implement Content Security Policy headers. Set HttpOnly and Secure flags on all session cookies.

# 5. POST-EXPLOITATION FINDINGS

* 1. **Password Hashes Obtained**

|  |  |  |  |
| --- | --- | --- | --- |
| **Username** | **Hash (MD5-crypt)** | **Cracked Password** | **Method** |
| root | $1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid. | — | Not cracked in session |
| msfadmin | $1$XN10Zj2c$Rt/ zzCW3mLtUWA.ihZjA5/ | msfadmin | John the Ripper |
| service | $1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3B u// | service | John the Ripper |
| user | $1$HESu9xrH$k.o3G93DGoXIiQKkPm UgZ0 | user | Known default |
| postgres | $1$Rw35ik.x$MgQgZUuO5pAoUvfJhfc Ye/ | postgres | Known default |

* 1. **Active Sessions Maintained**

|  |  |  |  |
| --- | --- | --- | --- |
| **Se ssi on** | **Type** | **Exploit Method** | **Connection** |
| 1 | cmd/unix shell | vsftpd CVE-2011-2523 | 101:33259 → 104:6200 |
| 2 | cmd/unix shell | Samba CVE-2007-2447 | 101:4444 → 104:47832 |
| 3 | Meterpreter | Upgraded from Session 2 | 101:4433 → 104:48218 |

* 1. **Target System Profile**

|  |  |
| --- | --- |
| **Property** | **Value** |
| Hostname | metasploitable.localdomain |
| OS | Ubuntu 8.04 LTS (Linux 2.6.24-16-server i686) |
| Architecture | i686 32-bit |
| Open Ports | 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049,  3306, 5432, 5900, 6667, 8180 |
| Web Apps | DVWA, Mutillidae, phpMyAdmin, TikiWiki, TWiki |
| Databases | MySQL 5.0.51a, PostgreSQL 8.3.0 |

# 6. REMEDIATION PLAN

|  |  |  |  |
| --- | --- | --- | --- |
| **Priority** | **Action** | **Addresses** | **Effort** |
| 1 — Immediate | Close all unnecessary open ports (firewall) | F1, F2, F3 | Low |
| 2 — Immediate | Change all default credentials | F3 | Low |
| 3 — Immediate | Upgrade vsftpd, Samba, OpenSSH to current | F2, F3, F4 | **Medium** |
| 4 — Urgent | Replace FTP with SFTP; disable Telnet | F2 | Low |
| 5 — Urgent | Parameterised queries for all database calls | F6 | **High** |
| 6 — Urgent | Fix command injection — validate all user inputs | F7 | **Medium** |
| 7 — High | XSS output encoding + CSP HTTP headers | F8 | **Medium** |
| 8 — High | Replace MD5 hashing with bcrypt/Argon2 | F6, F10 | **Medium** |
| 9 — Medium | HttpOnly + Secure flags on all session cookies | F8 | Low |
| 10 — Medium | Upgrade OS from Ubuntu 8.04 (EOL April 2013) | All | **High** |

**7. CONCLUSION**

This penetration test demonstrated complete and total compromise of the target system through multiple independent attack vectors. Root-level access was achieved in under 30 seconds using a trivial unauthenticated backdoor, and maintained persistently through 3 concurrent Metasploit sessions throughout the assessment.

The breadth and severity of findings indicate that the target system has received no meaningful security hardening. Every major vulnerability class was present: unpatched CVEs, default credentials, insecure web applications, weak cryptography, and no network access controls. In a real production environment, a single one of these findings would constitute a critical incident requiring immediate response.

**— END OF REPORT —**

Azizul Rahaman | Masters of Cybersecurity | 23 February 2026