Project:2

Mini Penetration Testing Report

Used (DVWA and bWAPP)

The purpose of this assessment was to understand how common web vulnerabilities appear, how they can be exploited, and how security controls differ across applications.

Objective

The objectives of this project were:

- To set up DVWA locally on Kali Linux
- To deploy bWAPP on a separate virtual machine
- To access bWAPP remotely using its IP address
- To perform reconnaissance, scanning, and exploitation
- To compare vulnerabilities found in both applications
- To document findings in a professional penetration testing report

---

Scope of Testing

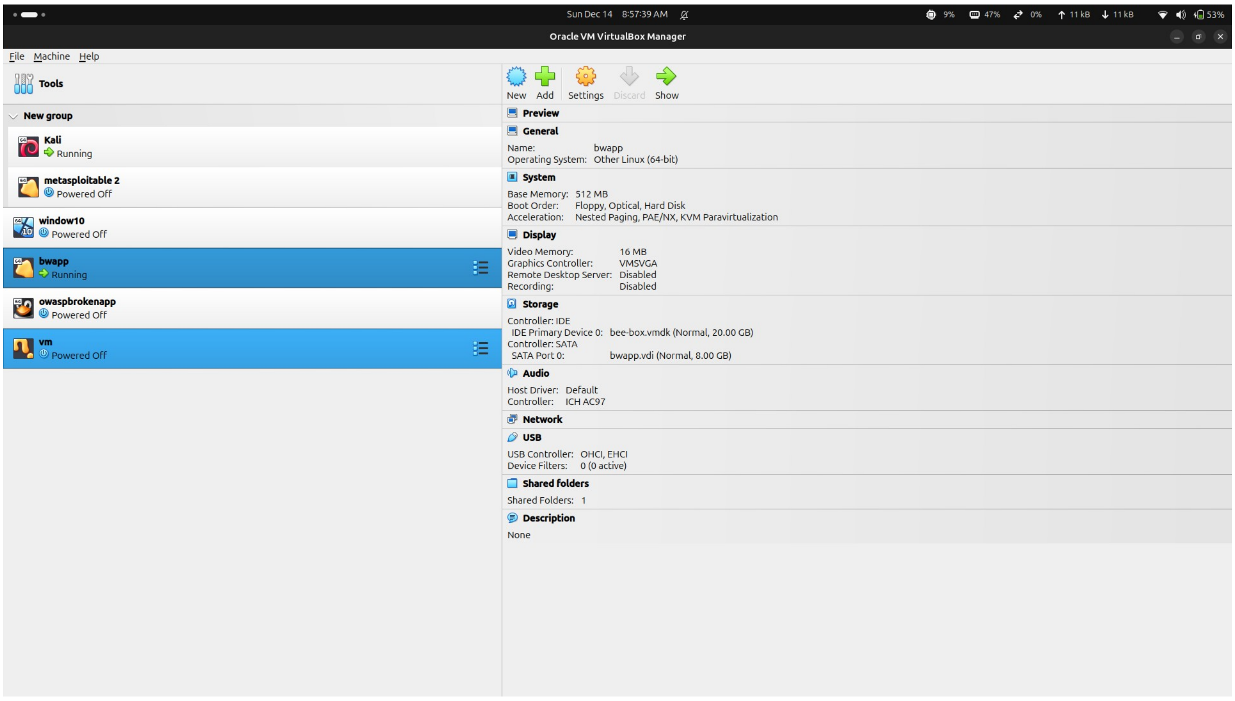
The scope of this penetration test included:

- DVWA running locally on Kali Linux
- bWAPP running on a virtual machine accessible via IP
- Web application level testing only

All testing was conducted in a controlled lab environment.

Lab Environment

- Attacker Machine: Kali Linux
- DVWA: Installed and running locally in Kali browser
- bWAPP: Installed on a separate virtual machine
- Network: Virtual network (Host-only / NAT)
- Access Method: Browser-based testing using IP address



Kali
Running

metasploitable 2
Powered Off

window10
Powered Off

bwapp
Running

owaspbrokenapp
Powered Off

vm
Powered Off

```
Preview
General
Name:               bwapp
Operating System:   Other Linux (64-bit)
System
Base Memory:   512 MB
Boot Order:    Floppy, Optical, Hard Disk
Acceleration:  Nested Paging, PAE/NX, KVM Paravirtualization
Display
Video Memory:            16 MB
Graphics Controller:     VMSVGA
Remote Desktop Server:   Disabled
Recording:               Disabled
Storage
Controller: IDE
 IDE Primary Device 0:  bee-box.vmdk (Normal, 20.00 GB)
Controller: SATA
 SATA Port 0:           bwapp.vdi (Normal, 8.00 GB)
Audio
Host Driver:  Default
Controller:   ICH AC97
Network
USB
USB Controller:  OHCI, EHCI
Device Filters:  0 (0 active)
Shared folders
Shared Folders:  1
Description
None
```

Tools Used

- Kali Linux
- DVWA
- bWAPP Virtual Machine
- Nmap
- DIRB
- Nikto
- Firefox Browser

Methodology

The penetration testing process followed these phases:

- Reconnaissance
- Scanning and enumeration
- Vulnerability identification
- Exploitation
- Analysis and reporting

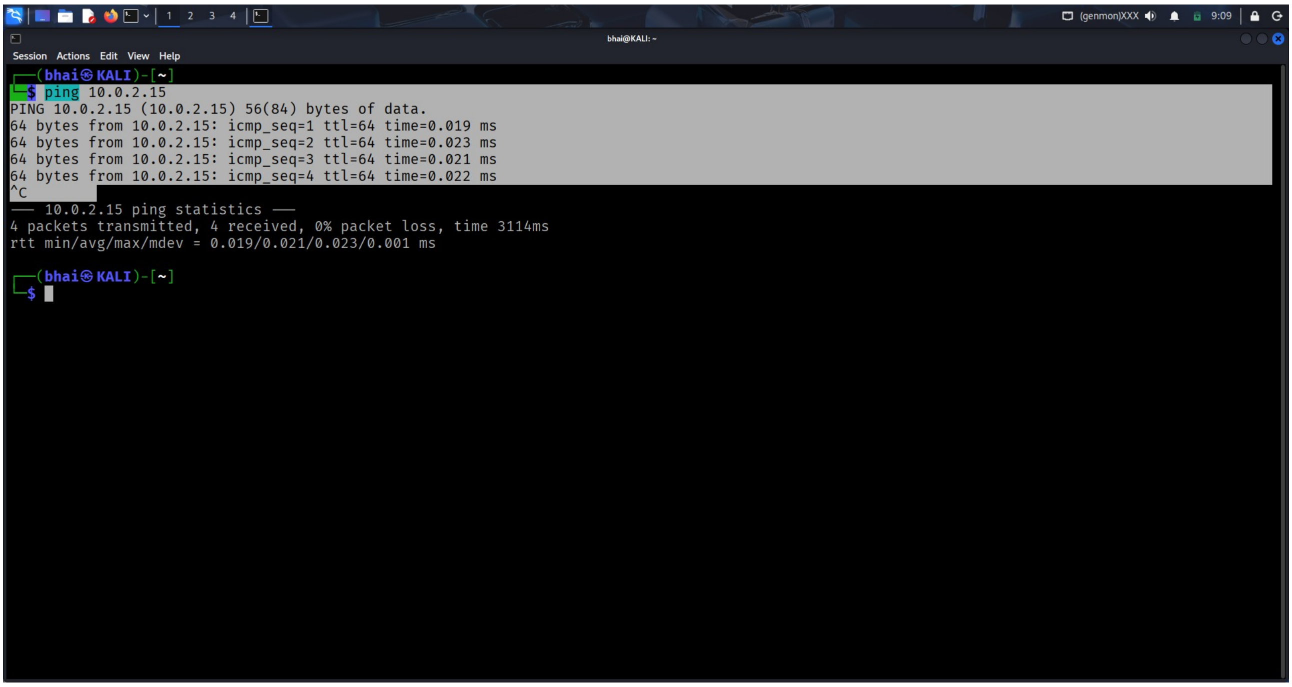
Reconnaissance and Scanning

Nmap Scanning for bWAPP VM (IP :- 10.0.2.15)

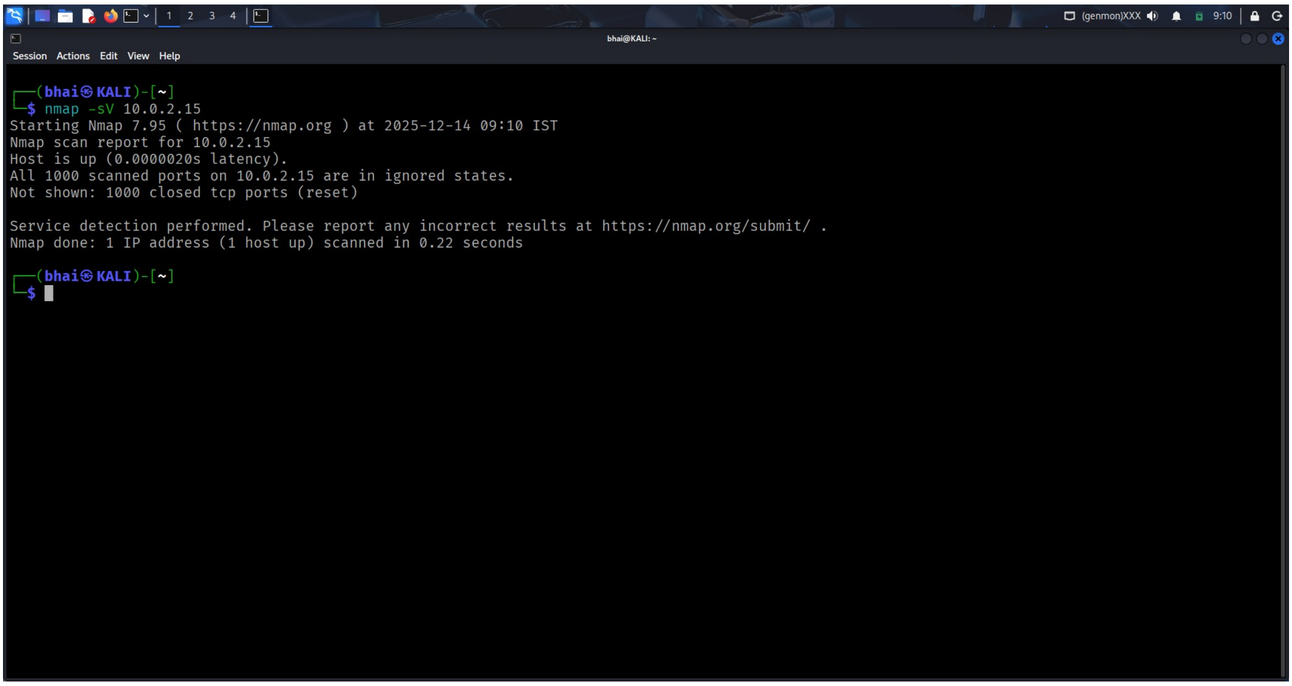
Nmap was used to identify open ports and running services on the bWAPP virtual machine.

Command used:

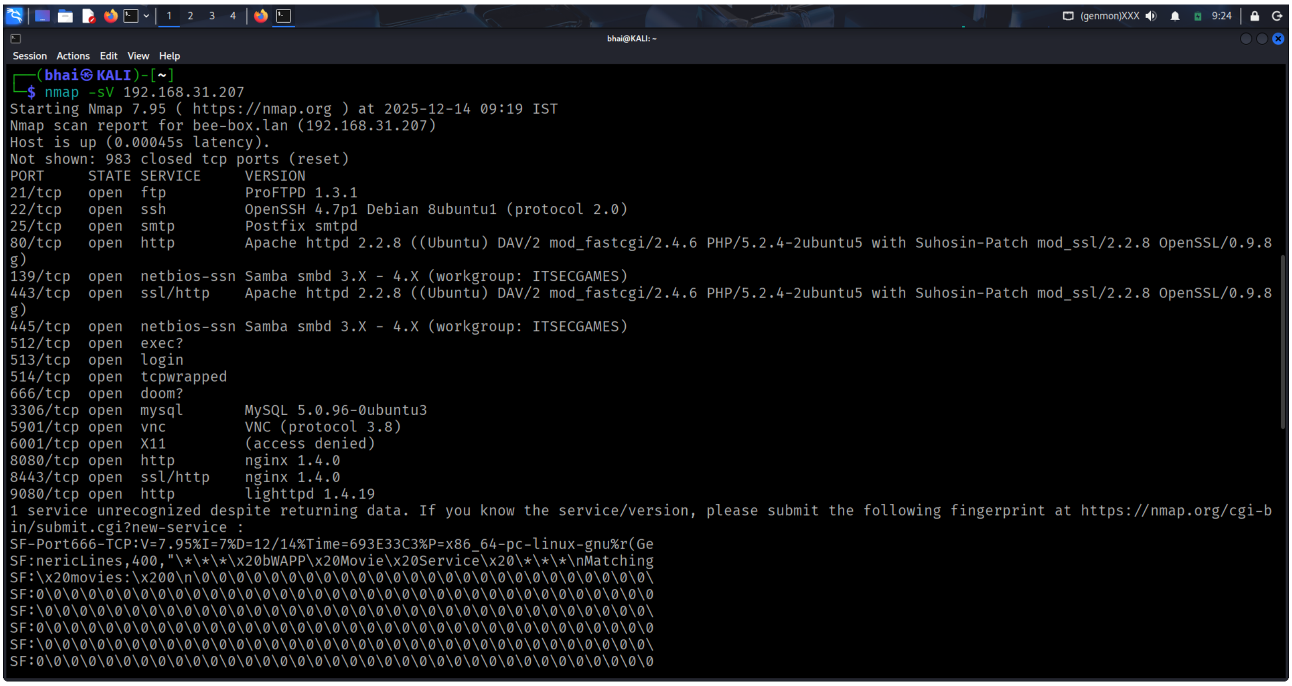
```
nmap -sV 10.0.2.15
```



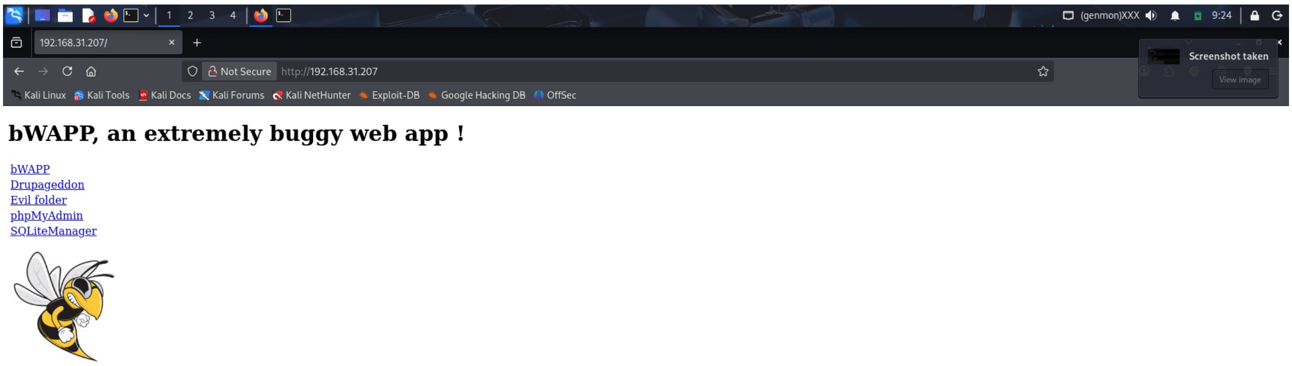
```
┌──(bhai㉿KALI)-[~]
└─$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.019 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.023 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.021 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.022 ms
^C
—— 10.0.2.15 ping statistics ——
4 packets transmitted, 4 received, 0% packet loss, time 3114ms
rtt min/avg/max/mdev = 0.019/0.021/0.023/0.001 ms

┌──(bhai㉿KALI)-[~]
└─$ 
```



```
┌──(bhai㉿KALI)-[~]
└─$ nmap -sV 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-14 09:10 IST
Nmap scan report for 10.0.2.15
Host is up (0.0000020s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds

┌──(bhai㉿KALI)-[~]
└─$ 
```



```
┌──(bhai㉿KALI)-[~]
└─$ nmap -sV 192.168.31.207
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-14 09:19 IST
Nmap scan report for bee-box.lan (192.168.31.207)
Host is up (0.00045s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp   open  smtp        Postfix smtpd
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8
g)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
443/tcp  open  ssl/http    Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8
g)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
512/tcp  open  exec?
513/tcp  open  login
514/tcp  open  tcpwrapped
666/tcp  open  doom?
3306/tcp open  mysql       MySQL 5.0.96-0ubuntu3
5901/tcp open  vnc         VNC (protocol 3.8)
6001/tcp open  X11         (access denied)
8080/tcp open  http        nginx 1.4.0
8443/tcp open  ssl/http    nginx 1.4.0
9080/tcp open  http        lighttpd 1.4.19
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-b
in/submit.cgi?new-service :
SF-Port666-TCP:V=7.95%I=7%D=12/14%Time=693E33C3%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,400,"\*\*\*\x20bWAPP\x20Movie\x20Service\x20\*\*\*\nMatching
SF:\x20movies:\x200\n\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
```



bWAPP, an extremely buggy web app !

bWAPP
Drupageddon
Evil folder
phpMyAdmin
SQLiteManager

Observation:

- The target host was reachable and responded to network probes
- Multiple open ports were discovered on the system
- FTP, SSH, and SMTP services were exposed, increasing remote access risk
- HTTP and HTTPS services were running on ports 80 and 443
- Additional web services were detected on ports 8080, 8443, and 9080
- SMB services were enabled on ports 139 and 445

- MySQL database service was exposed on port 3306
- VNC remote access service was found running on port 5901
- Several services were running outdated software versions
- The large number of exposed services indicated poor system hardening and an expanded attack surface

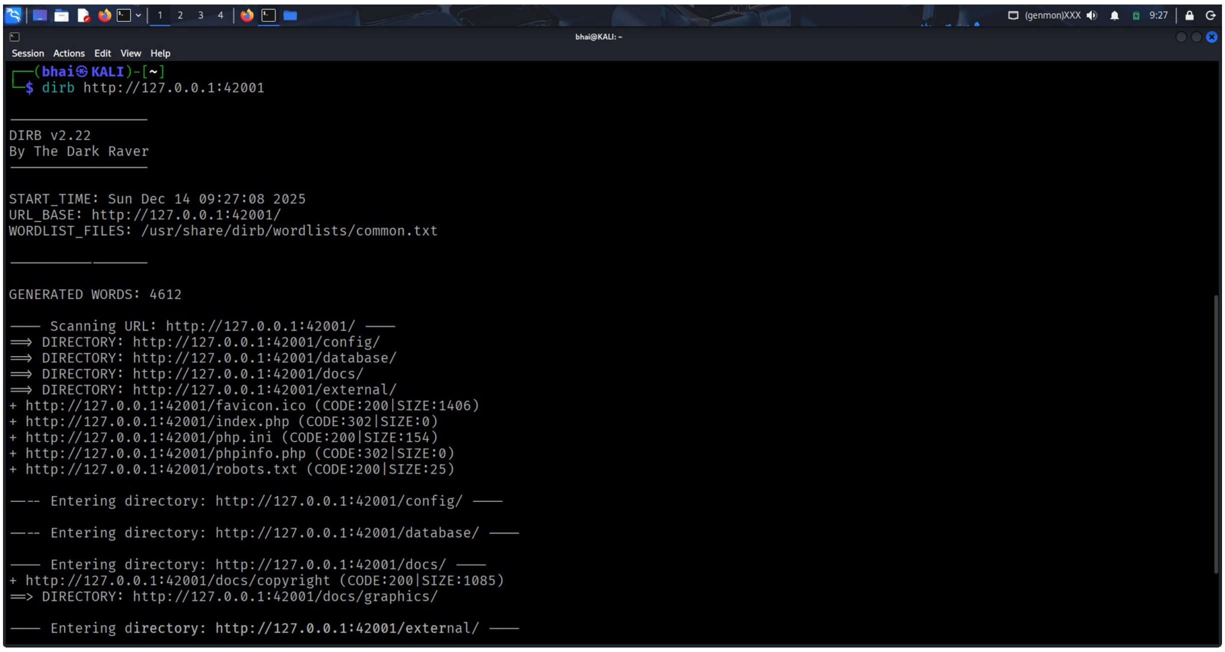
---

Directory Enumeration using DIRB

DIRB was used to discover hidden directories and endpoints.

Command used for DVWA:

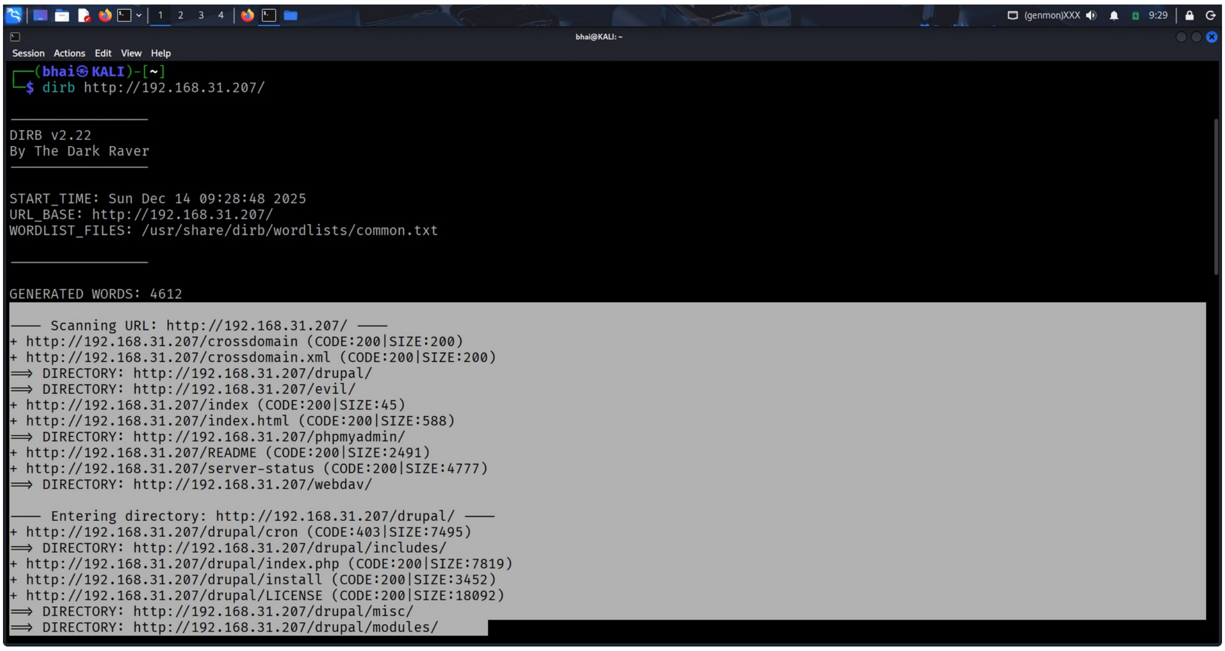
`dirb http://127.0.0.1:42001`



```
┌──(bhai㉿KALI)-[~]
└─$ dirb http://127.0.0.1:42001

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Dec 14 09:27:08 2025
URL_BASE: http://127.0.0.1:42001/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://127.0.0.1:42001/ ----
==> DIRECTORY: http://127.0.0.1:42001/config/
==> DIRECTORY: http://127.0.0.1:42001/database/
==> DIRECTORY: http://127.0.0.1:42001/docs/
==> DIRECTORY: http://127.0.0.1:42001/external/
+ http://127.0.0.1:42001/favicon.ico (CODE:200|SIZE:1406)
+ http://127.0.0.1:42001/index.php (CODE:302|SIZE:0)
+ http://127.0.0.1:42001/php.ini (CODE:200|SIZE:154)
+ http://127.0.0.1:42001/phpinfo.php (CODE:302|SIZE:0)
+ http://127.0.0.1:42001/robots.txt (CODE:200|SIZE:25)

---- Entering directory: http://127.0.0.1:42001/config/ ----

---- Entering directory: http://127.0.0.1:42001/database/ ----

---- Entering directory: http://127.0.0.1:42001/docs/ ----
+ http://127.0.0.1:42001/docs/copyright (CODE:200|SIZE:1085)
==> DIRECTORY: http://127.0.0.1:42001/docs/graphics/

---- Entering directory: http://127.0.0.1:42001/external/ ----
```

Command used for bWAPP:

`dirb http://192.168.31.207/`



```
┌──(bhai㉿KALI)-[~]
└─$ dirb http://192.168.31.207/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Dec 14 09:28:48 2025
URL_BASE: http://192.168.31.207/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.31.207/ ----
+ http://192.168.31.207/crossdomain (CODE:200|SIZE:200)
+ http://192.168.31.207/crossdomain.xml (CODE:200|SIZE:200)
==> DIRECTORY: http://192.168.31.207/drupal/
==> DIRECTORY: http://192.168.31.207/evil/
+ http://192.168.31.207/index (CODE:200|SIZE:45)
+ http://192.168.31.207/index.html (CODE:200|SIZE:588)
==> DIRECTORY: http://192.168.31.207/phpmyadmin/
+ http://192.168.31.207/README (CODE:200|SIZE:2491)
+ http://192.168.31.207/server-status (CODE:200|SIZE:4777)
==> DIRECTORY: http://192.168.31.207/webdav/

---- Entering directory: http://192.168.31.207/drupal/ ----
+ http://192.168.31.207/drupal/cron (CODE:403|SIZE:7495)
==> DIRECTORY: http://192.168.31.207/drupal/includes/
+ http://192.168.31.207/drupal/index.php (CODE:200|SIZE:7819)
+ http://192.168.31.207/drupal/install (CODE:200|SIZE:3452)
+ http://192.168.31.207/drupal/LICENSE (CODE:200|SIZE:18092)
==> DIRECTORY: http://192.168.31.207/drupal/misc/
==> DIRECTORY: http://192.168.31.207/drupal/modules/
```

Observation:

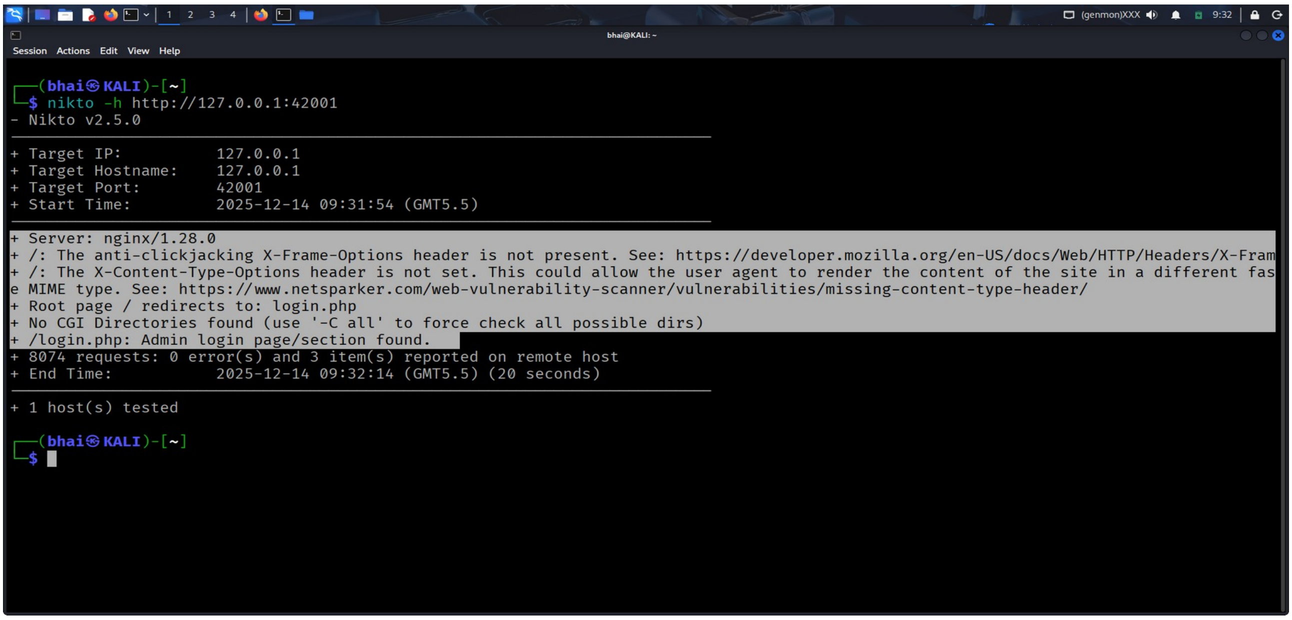
- DVWA exposed multiple vulnerable endpoints
- bWAPP revealed several testable paths

Web Server Scanning using Nikto

Nikto was used to identify server-level security issues.

Command used for DVWA:

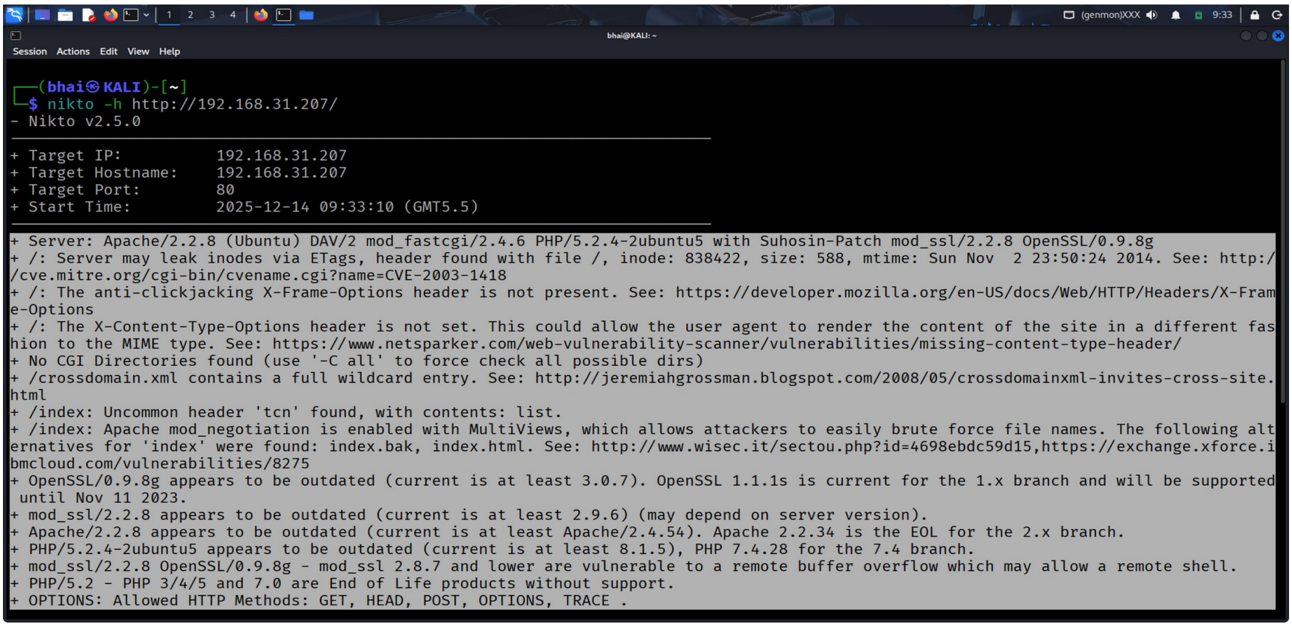
```
nikto -h http://127.0.0.1:42001
```



```
┌──(bhai㉿KALI)-[~]
└─$ nikto -h http://127.0.0.1:42001
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    127.0.0.1
+ Target Port:        42001
+ Start Time:         2025-12-14 09:31:54 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx/1.28.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Fram
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fas
e MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /login.php: Admin login page/section found.
+ 8074 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2025-12-14 09:32:14 (GMT5.5) (20 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(bhai㉿KALI)-[~]
└─$ 
```

Command used for bWAPP:

```
nikto -h http://192.168.31.207/
```



```
┌──(bhai㉿KALI)-[~]
└─$ nikto -h http://192.168.31.207/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.31.207
+ Target Hostname:    192.168.31.207
+ Target Port:        80
+ Start Time:         2025-12-14 09:33:10 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
+ /: Server may leak inodes via ETags, header found with file /, inode: 838422, size: 588, mtime: Sun Nov  2 23:50:24 2014. See: http:/
/cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Fram
e-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fas
hion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.
html
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alt
ernatives for 'index' were found: index.bak, index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.i
bmcloud.com/vulnerabilities/8275
+ OpenSSL/0.9.8g appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported
 until Nov 11 2023.
+ mod_ssl/2.2.8 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ PHP/5.2.4-2ubuntu5 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the 7.4 branch.
+ mod_ssl/2.2.8 OpenSSL/0.9.8g - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell.
+ PHP/5.2 - PHP 3/4/5 and 7.0 are End of Life products without support.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
```

Observation:

- Missing security headers
- Outdated server configurations
- Information disclosure issues

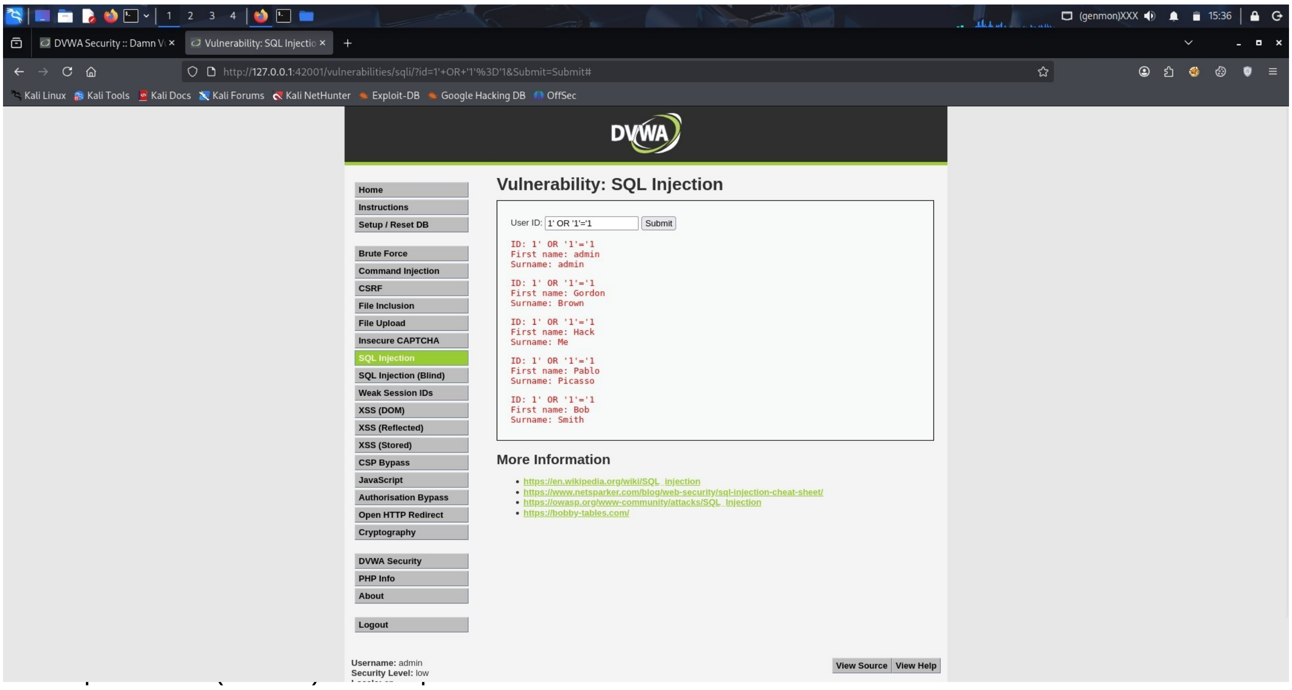
Vulnerability Findings in DVWA

SQL Injection

SQL Injection was tested on DVWA input fields.

Payload used:

```
' OR '1'='1
```



Vulnerability: SQL Injection

User ID: 1' OR '1'='1 Submit

```
ID: 1' OR '1'='1
First name: admin
Surname: admin

ID: 1' OR '1'='1
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1
First name: Hack
Surname: Me

ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1
First name: Bob
Surname: Smith
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

Username: admin
Security Level: low

Result:

- Browser alert appeared

Cause:

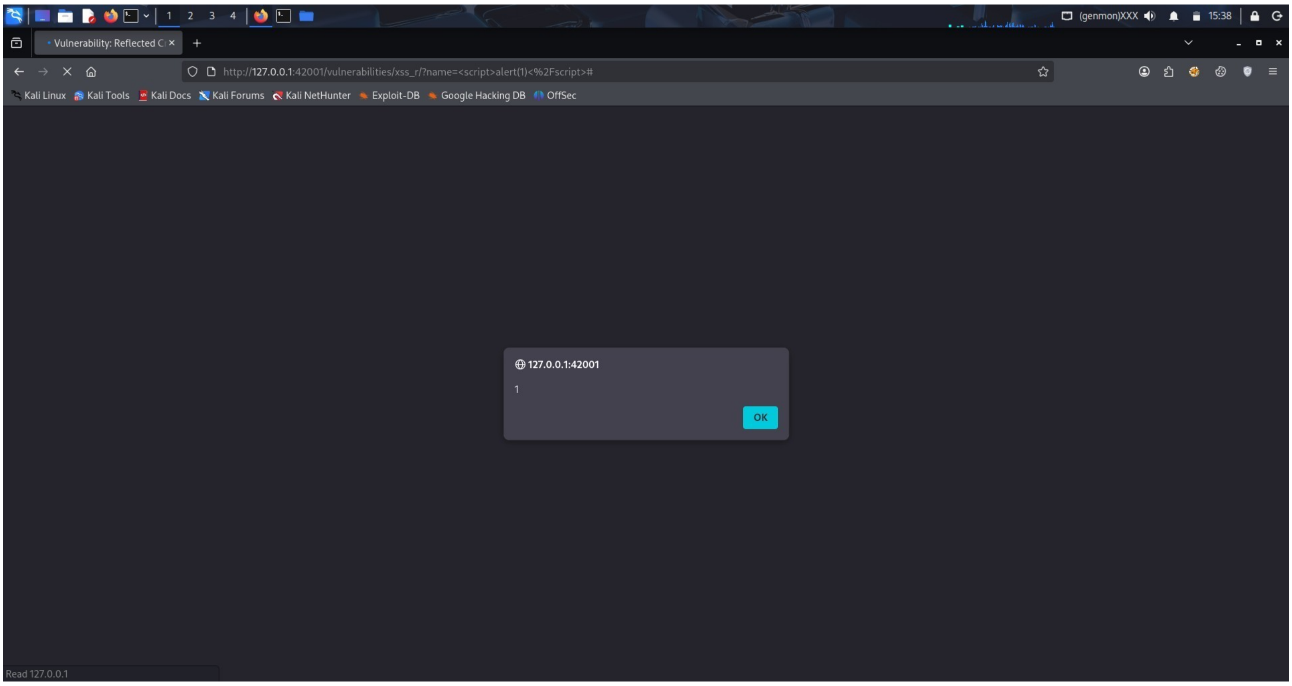
- Output rendered without encoding

Cross-Site Scripting

XSS was tested using input fields in dvwa.

Payload used:

```
<img src=x onerror=alert('XSS')>
```



http://127.0.0.1:42001/vulnerabilities/xss_r/?name=<script>alert(1)<%2Fscript>#

127.0.0.1:42001

1

Result:

- Script executed in browser

Cause:

- Missing input filtering and output encoding

Comparison of DVWA and bWAPP

DVWA is designed to demonstrate common web vulnerabilities at different security levels, making it easier to understand how insecure coding leads to exploitation and how defenses gradually improve. It provides a structured learning environment where vulnerabilities such as SQL Injection and Cross-Site Scripting can be clearly observed and tested.

bWAPP, on the other hand, offers a broader collection of vulnerabilities in a more realistic deployment environment. Running bWAPP on a separate virtual machine helped simulate real-world penetration testing scenarios where the attacker and target reside on different systems. While DVWA supported direct manual exploitation, bWAPP was primarily assessed through reconnaissance, service enumeration, and configuration analysis.

Executive Summary

This mini penetration testing project assessed two intentionally vulnerable web applications, DVWA and bWAPP, in a controlled lab environment. Critical web vulnerabilities such as SQL Injection and

Cross-Site Scripting were successfully validated in DVWA, highlighting the risks of insecure input handling.

In the case of bWAPP, multiple high-risk security issues were identified through scanning and reconnaissance, including excessive service exposure and outdated software components. The assessment emphasizes the importance of secure coding practices, system hardening, and regular security testing to reduce attack surfaces.

Technical Findings

- SQL Injection vulnerabilities successfully identified and exploited in DVWA
- Cross-Site Scripting vulnerabilities validated in DVWA
- Multiple unnecessary network services exposed on the bWAPP system
- Outdated versions of web server and supporting services detected
- Missing HTTP security headers
- Weak system hardening and insufficient service minimization

---

Remediation Recommendations

- Use prepared statements and parameterized queries for database access
- Validate and sanitize all user-supplied input
- Apply proper output encoding to prevent XSS
- Implement secure authentication and session management
- Disable unnecessary services and close unused ports
- Regularly update and patch software components
- Follow OWASP Top 10 security best practices

Conclusion

This project provided practical exposure to penetration testing techniques in a realistic lab environment. By assessing applications deployed on different systems, the project strengthened understanding of both web application vulnerabilities and network-based attack surfaces.

The combination of manual testing and automated scanning improved technical skills, analytical thinking, and professional security reporting capabilities.

Learning Outcomes

- Understanding of real-world penetration testing environments

- Hands-on experience with DVWA and bWAPP assessment
- Improved vulnerability identification and analysis skills
- Strong understanding of security testing tools and methodologies
- Experience in writing professional penetration testing reports