

Practical No.9

Aim: SQL Injection Attack

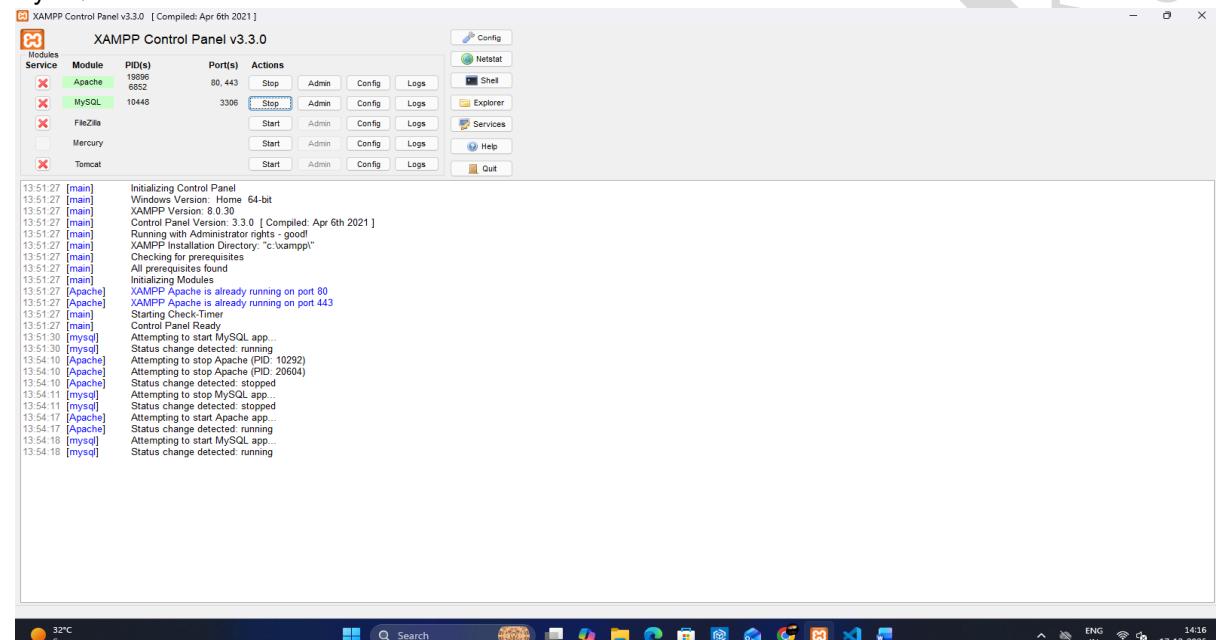
- Identify a web application vulnerable to SQL injection.
- Craft and execute SQL injection queries to exploit the vulnerability.
- Extract sensitive information or manipulate the database through the SQL injection attack.

Step 1: Start XAMPP

Open XAMPP Control Panel.

Click Start for:

Apache
MySQL

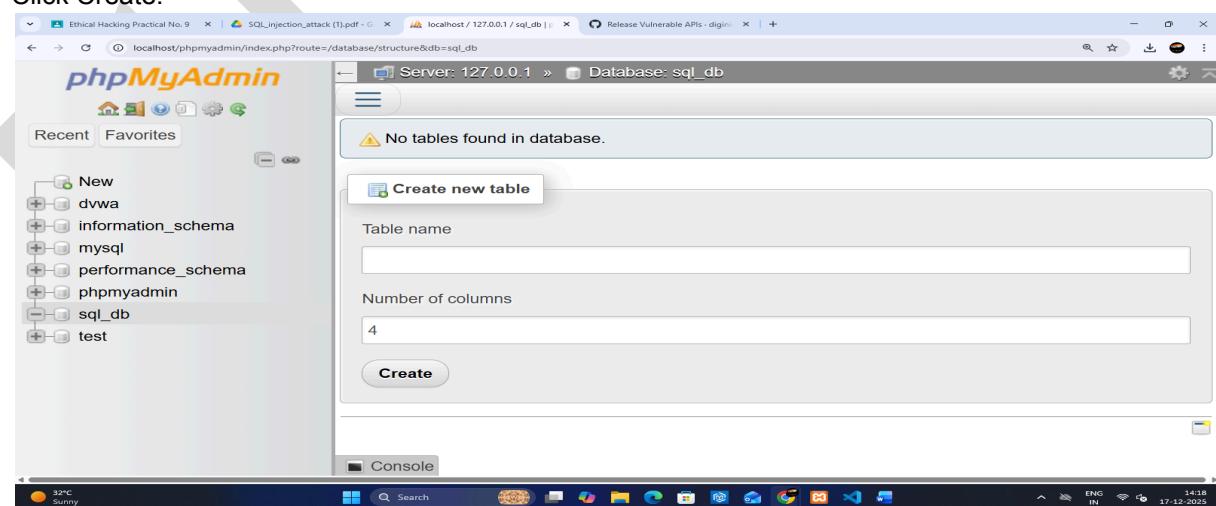


Step 2: Open phpMyAdmin

Create a Database

sql_db

Click Create.



SHETH L.U.J. COLLEGE OF ARTS & SIR M.V. COLLEGE OF SCIENCE & COMMERCE

Step 3: Download & Setup DVWA

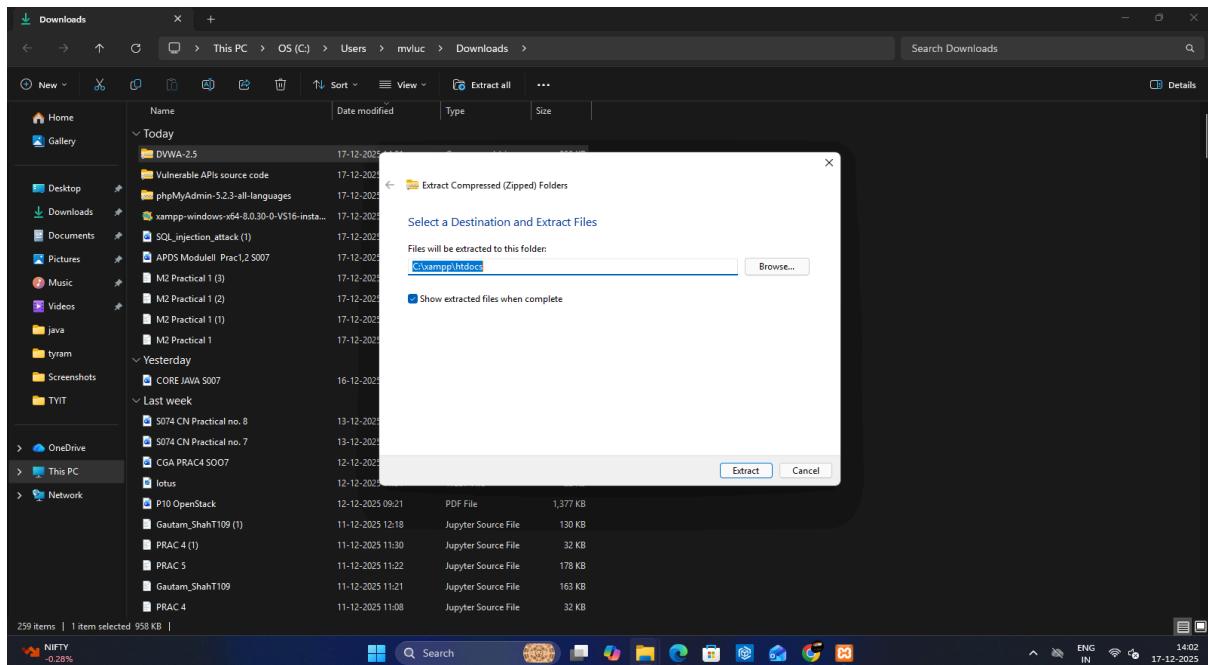
Set Up the SQL Injection Environment

Download DVWA from GitHub:

Go to: <https://github.com/digininja/DVWA>

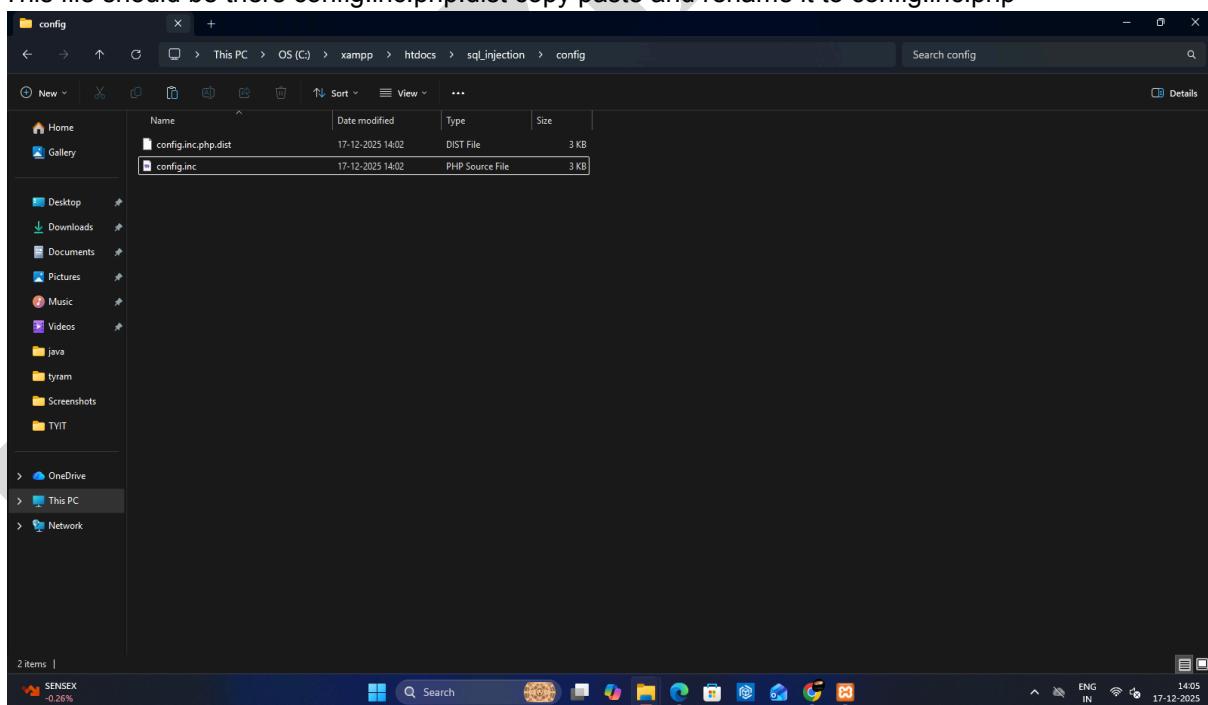
Click Code → Download ZIP.

- Extract the downloaded ZIP file inside C:\xampp\htdocs\.
- Rename the DVWA-master folder to sql_injection.



Now go to the sql_injection\config folder

This file should be there config.inc.php.dist copy paste and rename it to config.inc.php



Modify the Database Credentials

Inside config.inc.php, find this section:

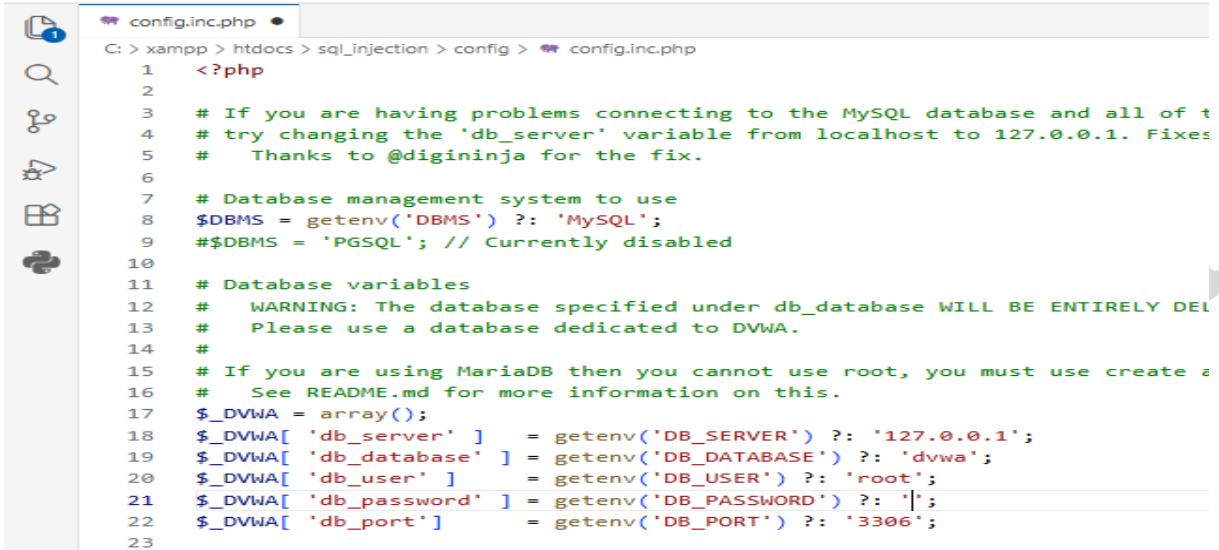
```
$_DVWA[ 'db_user' ] = 'dvwa';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
```

SHETH L.U.J. COLLEGE OF ARTS & SIR M.V. COLLEGE OF SCIENCE & COMMERCE

- ◆ Change it to use MySQL's default root user:

```
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = "";
```

Since XAMPP MySQL doesn't have a password for root by default, leaving it empty will work.



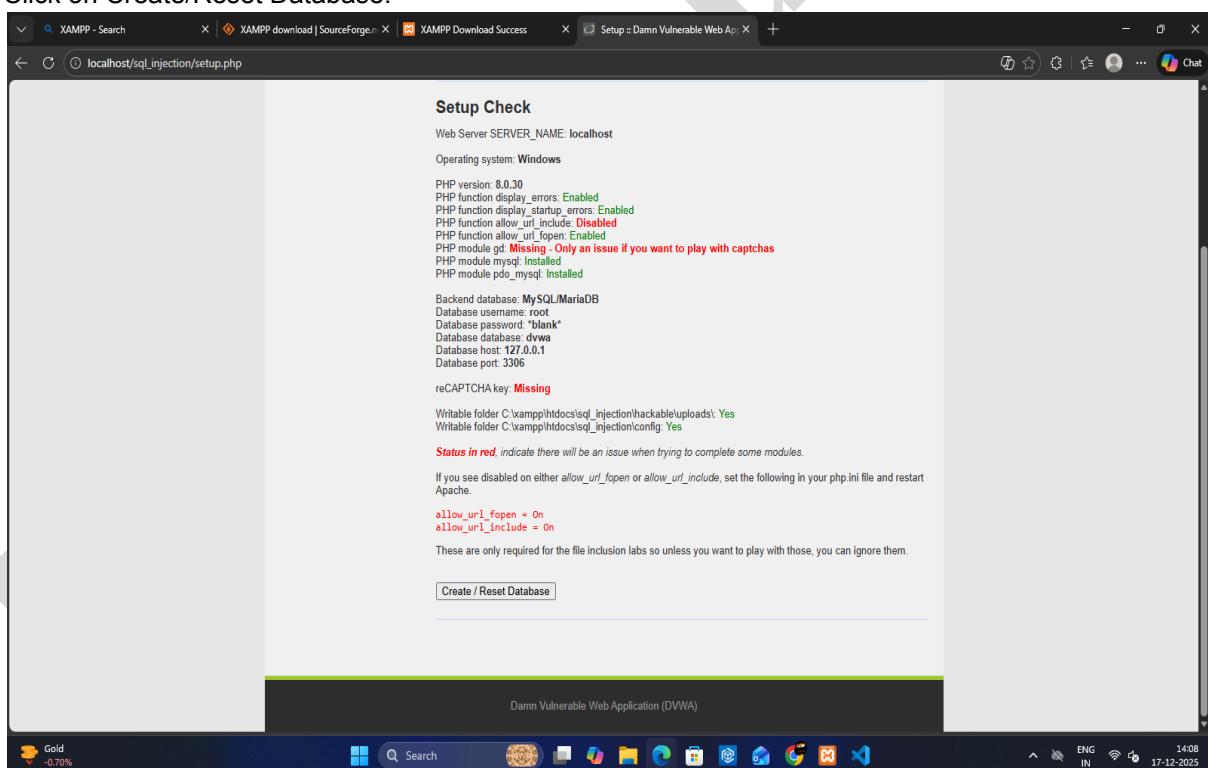
```
C: > xampp > htdocs > sql_injection > config > config.inc.php
1  <?php
2
3  # If you are having problems connecting to the MySQL database and all of t
4  # try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes
5  # Thanks to @digininja for the fix.
6
7  # Database management system to use
8 $DBMS = getenv('DBMS') ?: 'MySQL';
9 ##$DBMS = 'PGSQL'; // Currently disabled
10
11 # Database variables
12 # WARNING: The database specified under db_database WILL BE ENTIRELY DEL
13 # Please use a database dedicated to DVWA.
14 #
15 # If you are using MariaDB then you cannot use root, you must use create a
16 # See README.md for more information on this.
17 $_DVWA = array();
18 $_DVWA[ 'db_server' ] = getenv('DB_SERVER') ?: '127.0.0.1';
19 $_DVWA[ 'db_database' ] = getenv('DB_DATABASE') ?: 'dvwa';
20 $_DVWA[ 'db_user' ] = getenv('DB_USER') ?: 'root';
21 $_DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ?: '';
22 $_DVWA[ 'db_port' ] = getenv('DB_PORT') ?: '3306';
23
```

Step 4: Open a web browser.

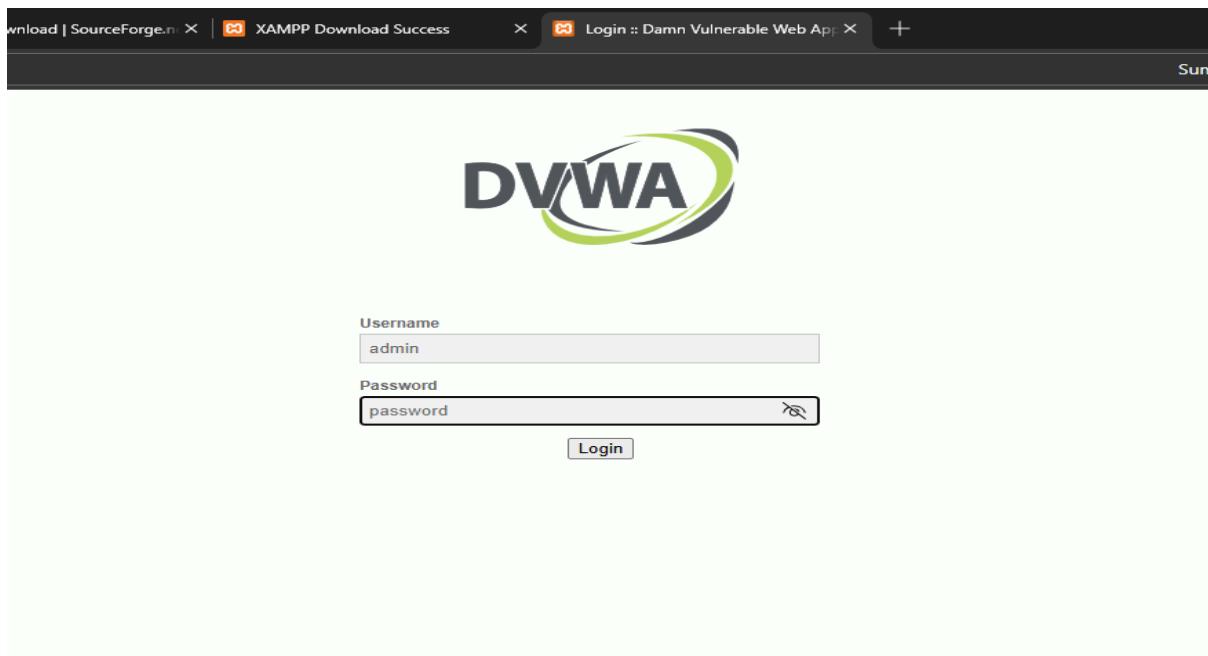
Type in the URL:

http://localhost/sql_injection/setup.php

Click on Create/Reset Database.



**SHETH L.U.J. COLLEGE OF ARTS &
SIR M.V. COLLEGE OF SCIENCE & COMMERCE**



Step 6: Lower Security Level

Look at the left-side menu.

Click on DVWA Security.

Set the Security Level to Low.



Click on SQL Injection from the left-side menu.

Step 7: Performing SQL Injection

Basic Injection

In the text box, type:

1

Bypassing Authentication

In the text box, type:

a' or '='

Extracting Data

In the text box, type:

1=1

Wildcard Injection

In the text box, type:

1*

**SHETH L.U.J. COLLEGE OF ARTS &
SIR M.V. COLLEGE OF SCIENCE & COMMERCE**

The screenshot shows a Microsoft Edge browser window with the URL `localhost/sql_injection/vulnerabilities/sql/?id=1%3D1&Submit=Submit#`. The page title is "Vulnerability: SQL Injection". On the left, a sidebar menu lists various attack types, with "SQL Injection" highlighted in green. The main content area contains a form with a "User ID:" input field and a "Submit" button. Below the form, the output shows the results of the exploit: "ID: 1=1", "First name: admin", and "Surname: admin". A "More Information" section at the bottom provides links to external resources about SQL injection.

This screenshot is nearly identical to the one above, showing the same browser window and DVWA interface. However, the exploit attempt has failed. The output below the "User ID:" field only shows "ID: 1=1", while "First name: admin" and "Surname: admin" are missing. This indicates that the exploit did not successfully retrieve the user's first and last names.