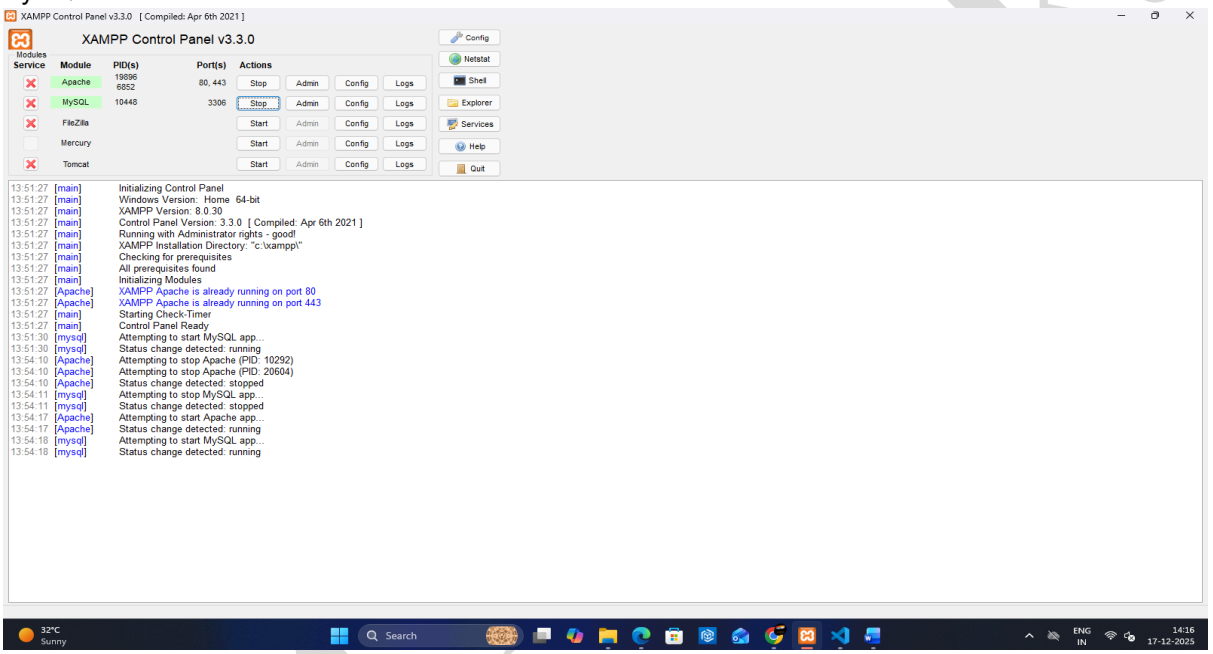
Practical No.9

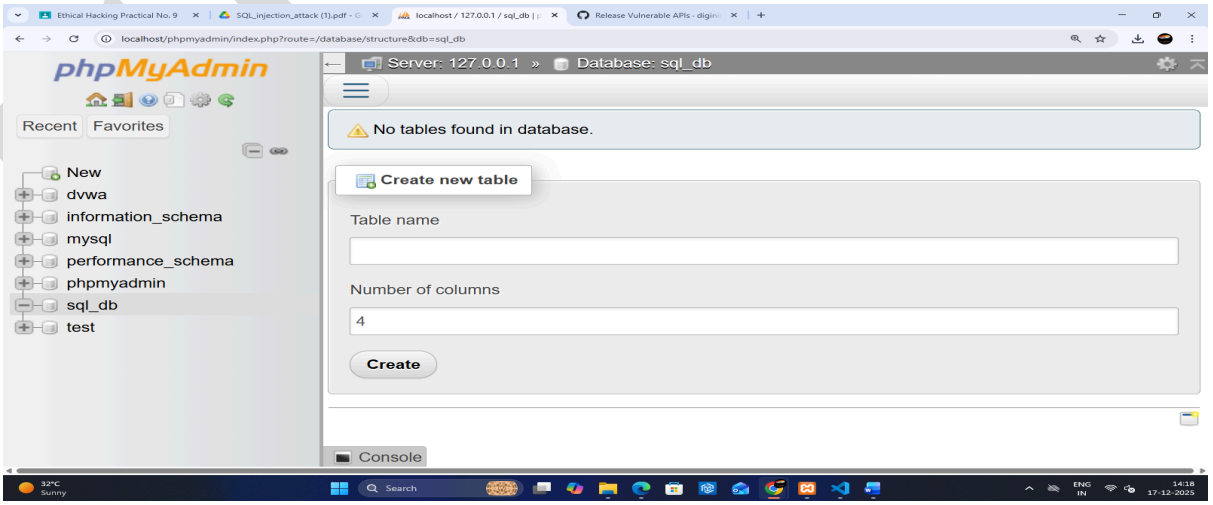
Aim: SQL Injection Attack

- **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.**

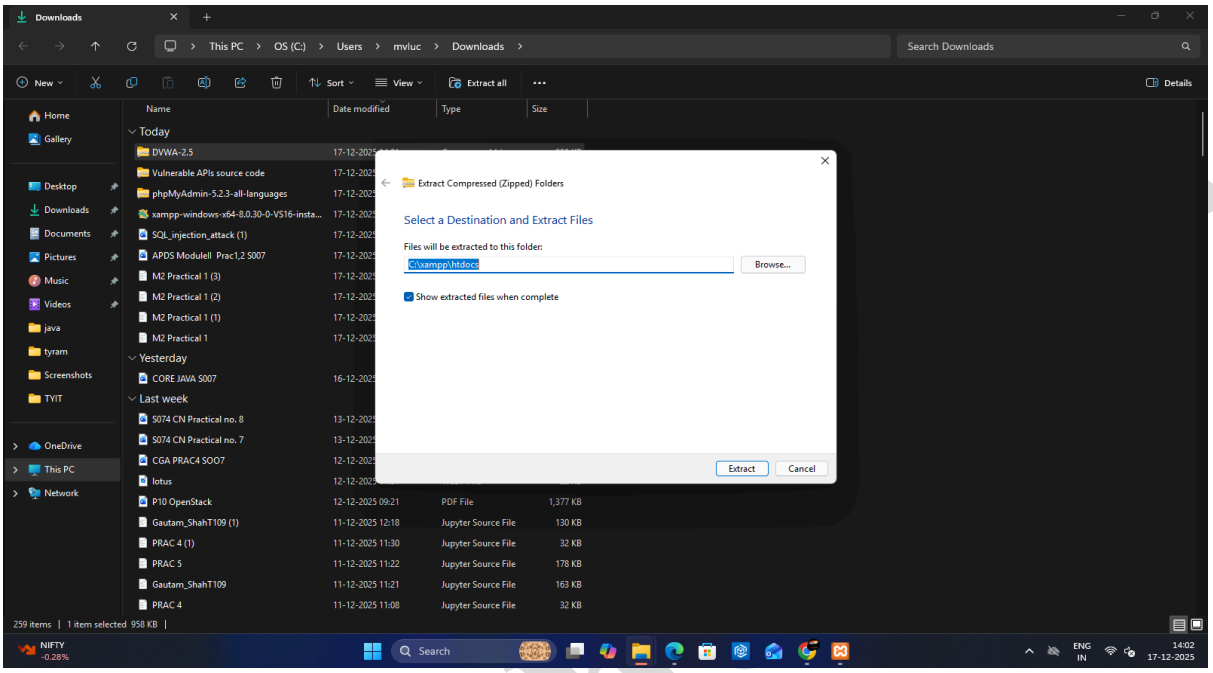
Step 1: Start XAMPP
Open XAMPP Control Panel.
Click Start for:
Apache
MySQL



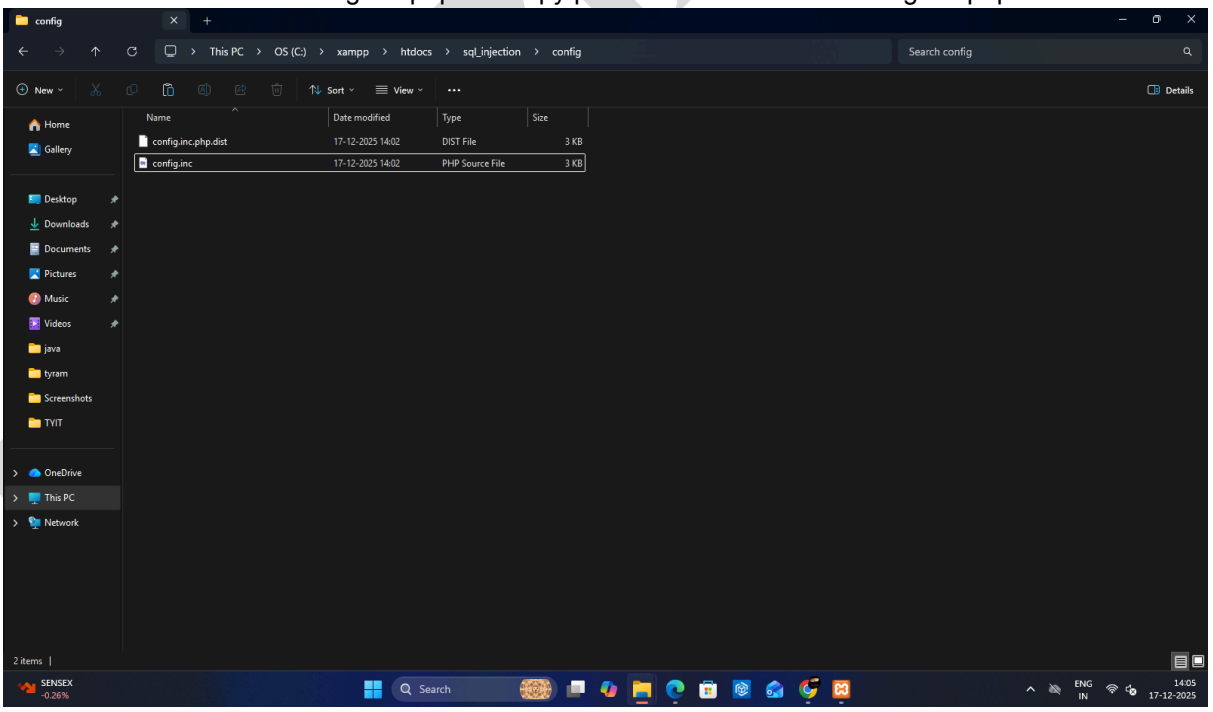
Step 2: Open phpMyAdmin
Create a Database
sql_db
Click Create.



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.



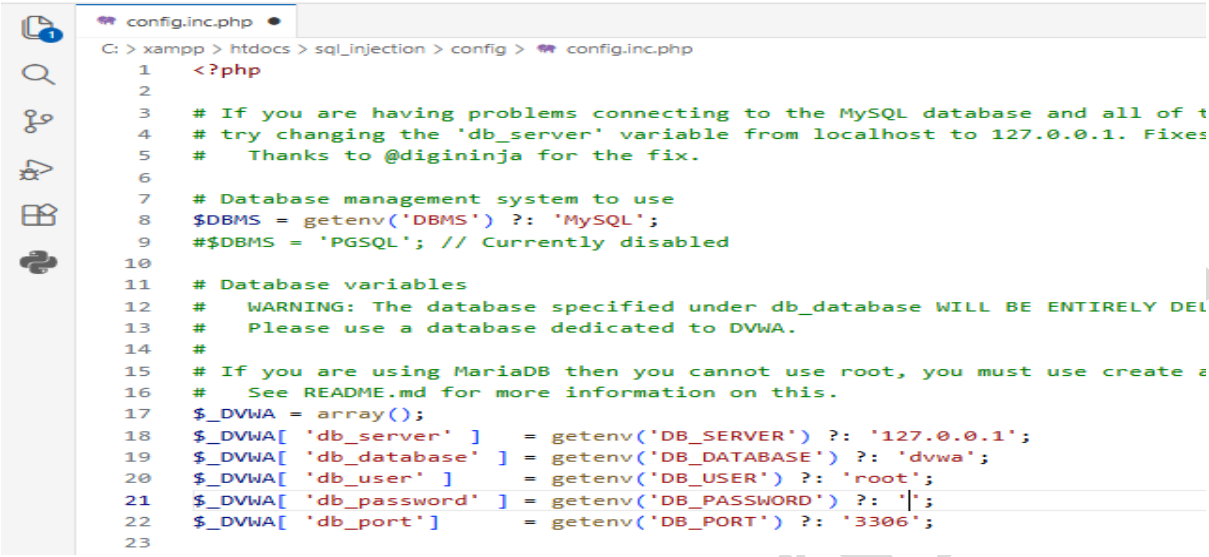
Now go to the sql_injection\config folder
This file should be there config.inc.php.dist copy paste and rename it to config.inc.php



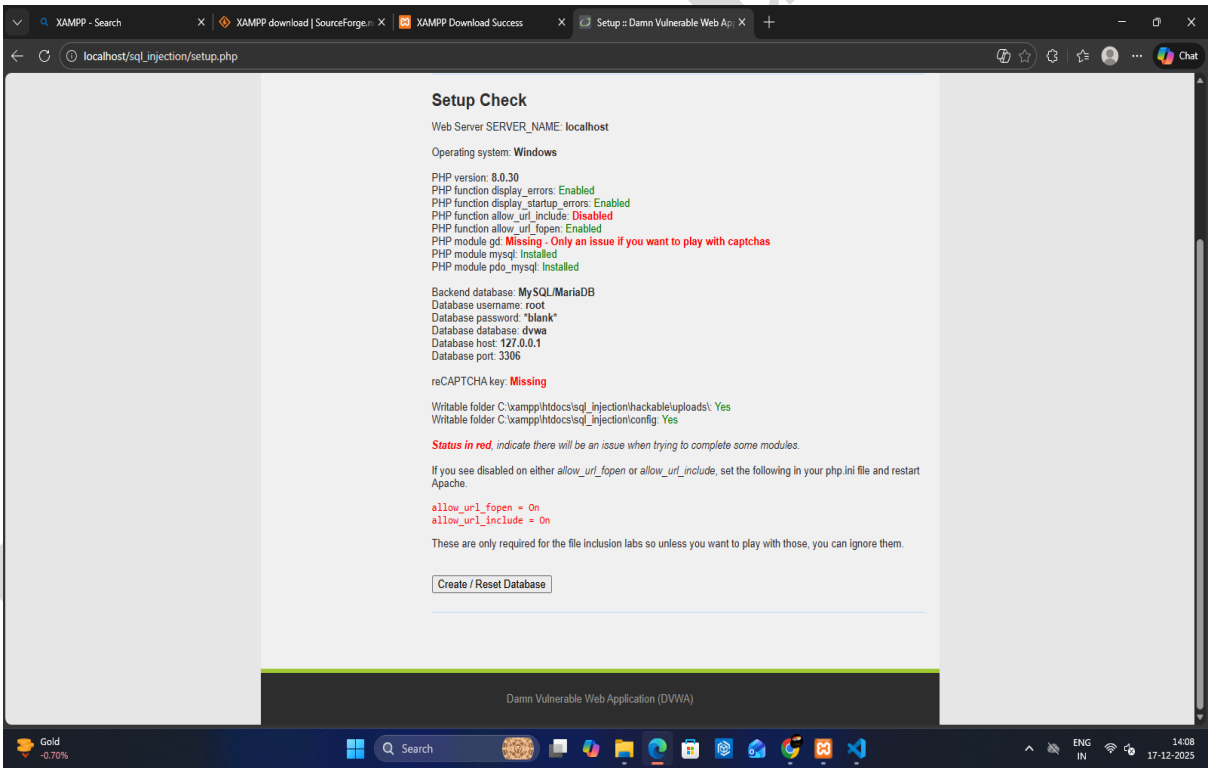
Modify the Database Credentials
Inside config.inc.php, find this section:
$_DVWA['db_user'] = 'dvwa';
$_DVWA['db_password'] = 'p@ssw0rd';

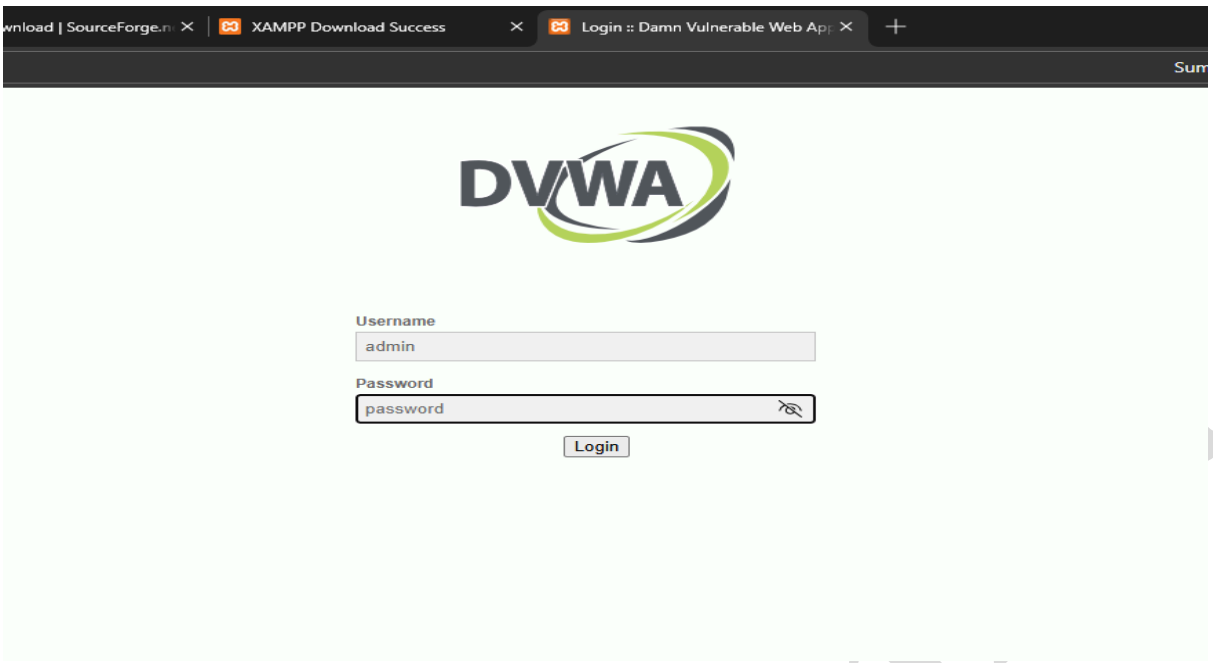
- Change it to use MySQL's default root user:

$_DVWA['db_user'] = 'root';
$_DVWA['db_password'] = '';
Since XAMPP MySQL doesn't have a password for root by default, leaving it empty will work.



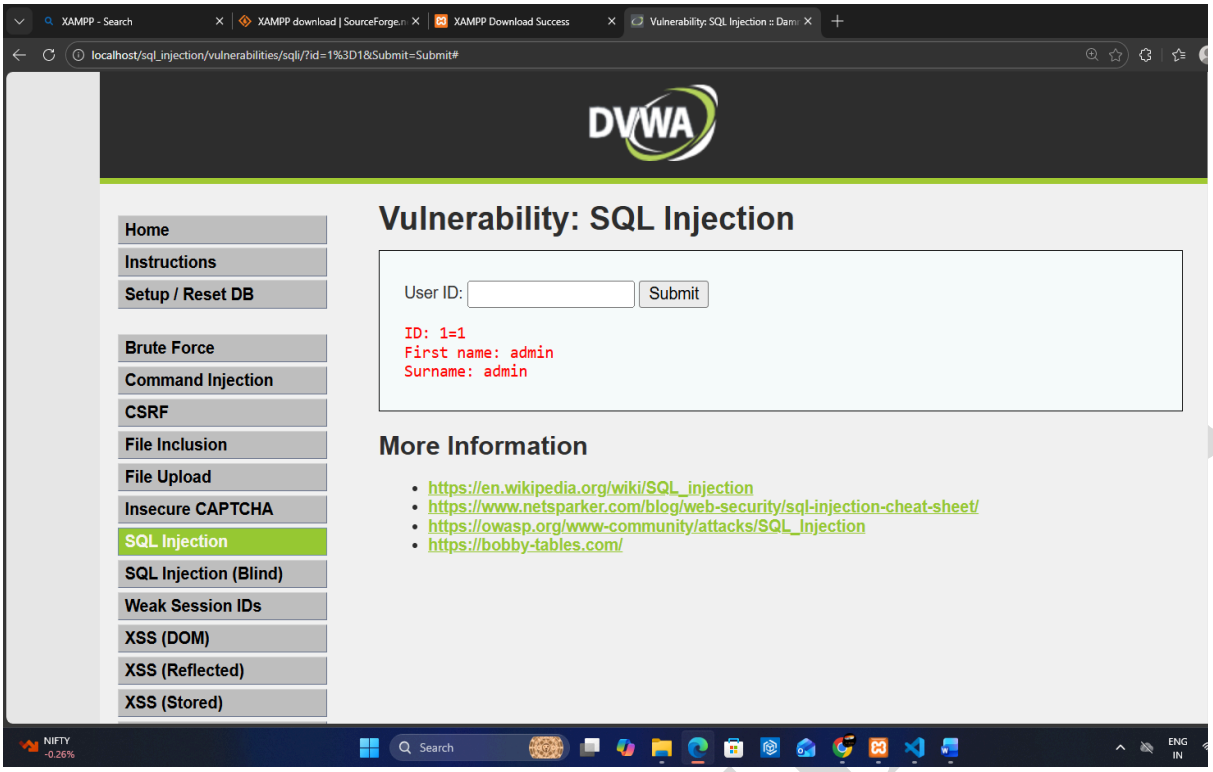
Step 4: Open a web browser.
Type in the URL:
http://localhost/sql_injection/setup.php
Click on Create/Reset Database.

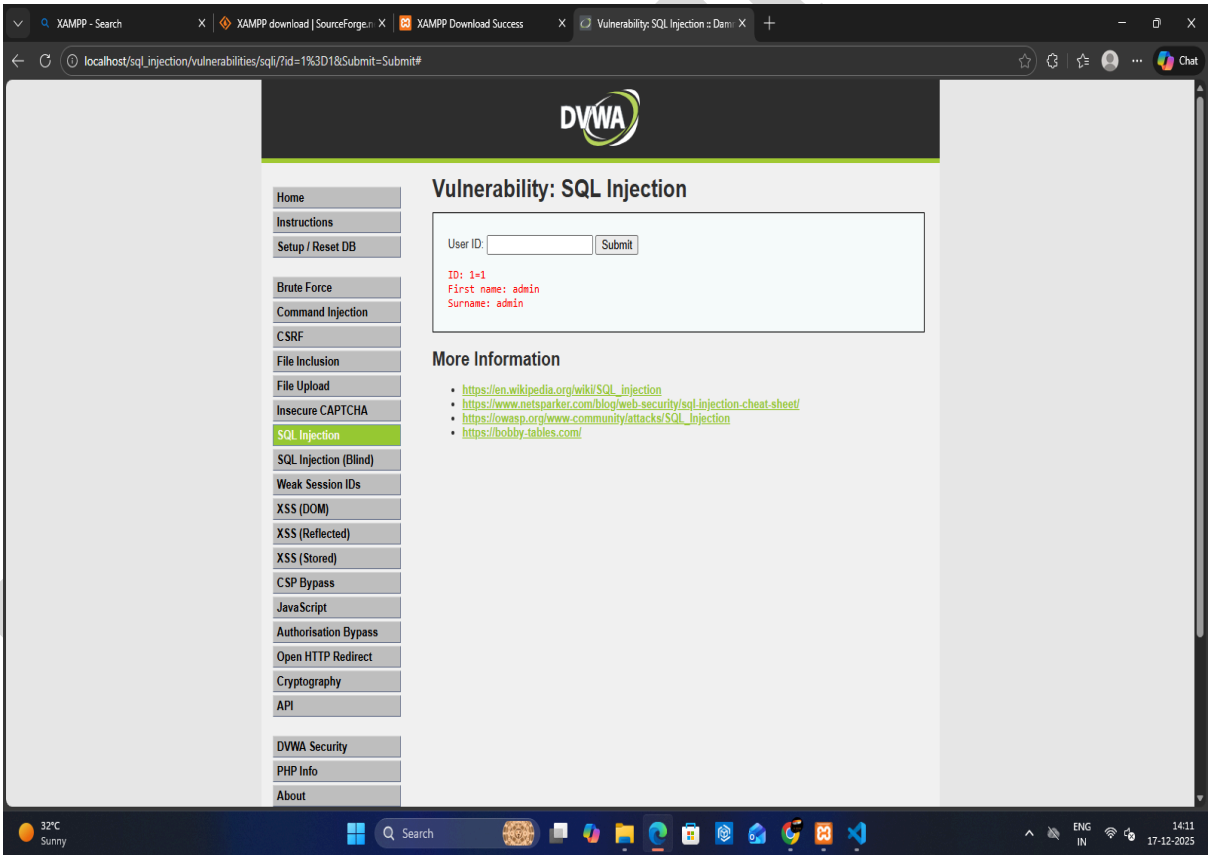




Step 6: Lower Security Level
Look at the left-side menu.
Click on DVWA Security.
Set the Security Level to Low.

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*


XAMPP - Search
XAMPP download | SourceForge.n
XAMPP Download Success
Vulnerability: SQL Injection :: Dami
localhost/sql_injection/vulnerabilities/sqli/?id=1%3D1&Submit=Submit#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
Vulnerability: SQL Injection
User ID:
Submit
ID: 1=1
First name: admin
Surname: admin
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/
NIFTY
-0.26%
Search
ENG
IN


XAMPP - Search
XAMPP download | SourceForge.n
XAMPP Download Success
Vulnerability: SQL Injection :: Dami
localhost/sql_injection/vulnerabilities/sqli/?id=1%3D1&Submit=Submit#
Chat
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
Vulnerability: SQL Injection
User ID:
Submit
ID: 1=1
First name: admin
Surname: admin
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/
32°C
Sunny
Search
ENG
IN
14:11
17-12-2025