TASK 1: WEB APPLICATION SECURITY TESTING

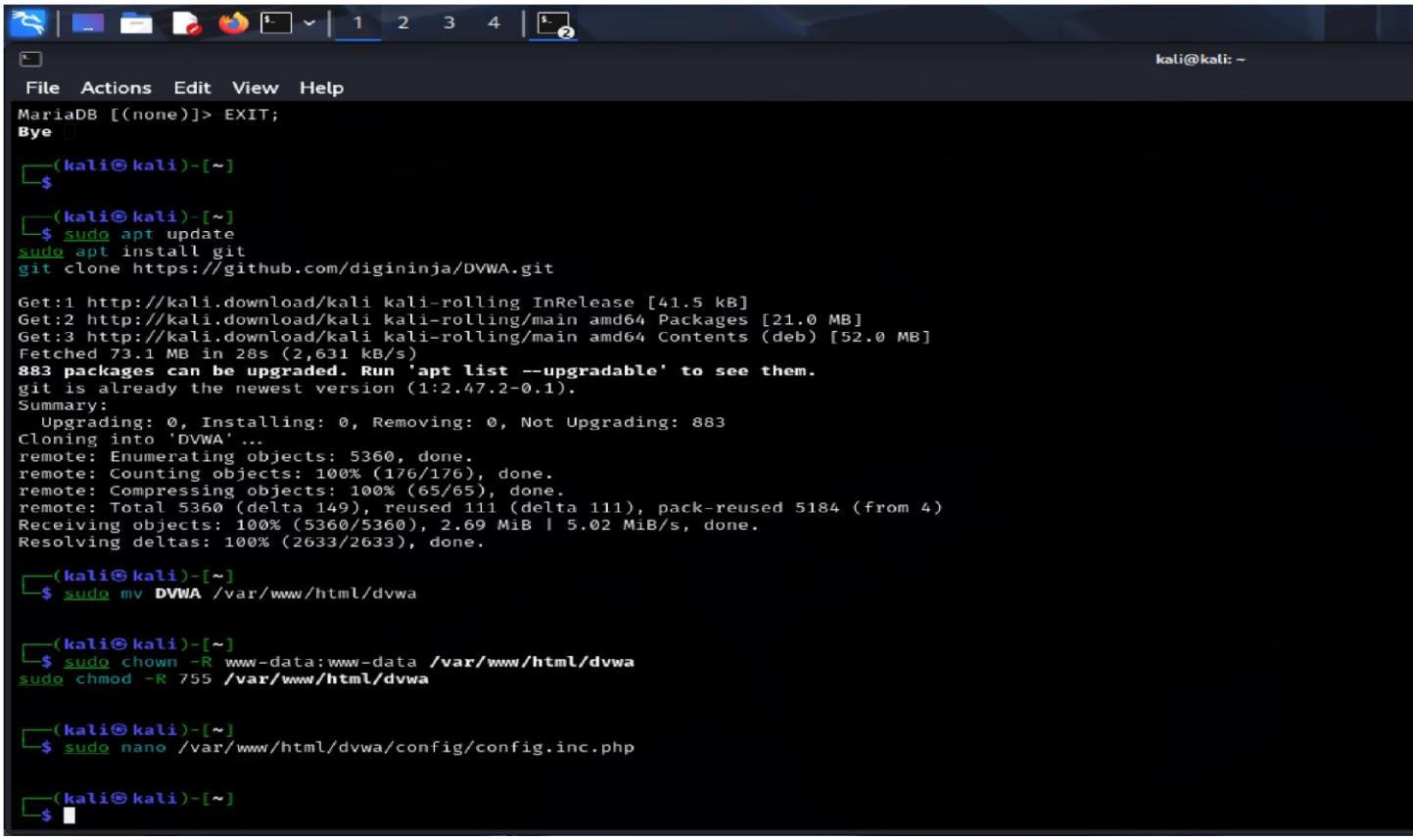
In this task we are going to test the web application for vulnerabilities by using cross site scripting, sql injections, authentication failures.

Open kali linux and first step is to update and download the mariadb server using the below commands.

sudo apt update sudo apt install git git cole

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

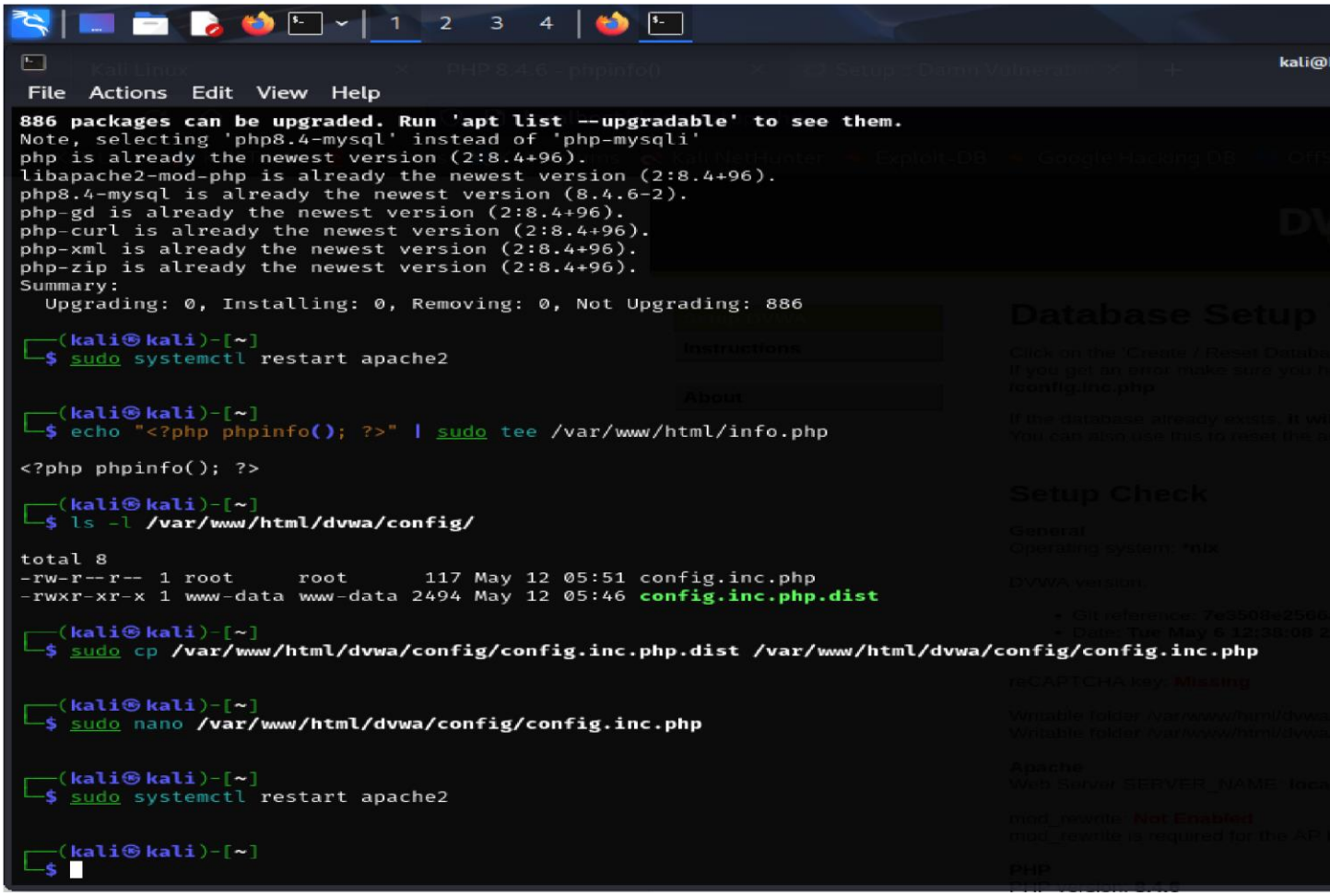
After downloading I have moved to this destination path /var/www/html/dvwa then changing the owner of dvwa and permissions here 7 is for admin he can read,write, execute but group



and other usres can only read and execute dvwa.

sudo systemctl restart apache2

sudo apt install apache2 mariadb-server php libapache2-mod-php php-mysqli php-gd php-curl php-xml php-zip sudo systemctl restart mariadb start the apache2 services and download mariadb server then create the database .



```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo mysql -u root -p
[sudo] password for kali:
Enter password:
ERROR 2002 (HY000): Can't connect to local server through socket '/run/mysqld/mysqld.sock' (2)

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start mariadb

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status mariadb

● mariadb.service - MariaDB 11.8.1 database server
     Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
     Active: active (running) since Mon 2025-05-12 04:56:06 EDT; 1min 57s ago
 Invocation: b412a5d6a183440486b4d913bf87e1a7
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
    Process: 7453 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)
    Process: 7455 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||  VAR=`/usr/bin/galera_recovery`; [ $? -eq 0 ]  && echo _WSREP_START_POSITION=$VAR > /run/mysqld/wsrep-sta
    Process: 7549 ExecStartPost=/bin/rm -f /run/mysqld/wsrep-start-position (code=exited, status=0/SUCCESS)
    Process: 7551 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
   Main PID: 7508 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 12 (limit: 14518)
     Memory: 331.2M (peak: 421.2M)
        CPU: 2.938s
     CGroup: /system.slice/mariadb.service
             └─7508 /usr/sbin/mariadbd

May 12 04:56:05 kali mariadbd[7508]: 2025-05-12  4:56:05 0 [Note] InnoDB: Buffer pool(s) load completed at 250512  4:56:05
May 12 04:56:06 kali mariadbd[7508]: 2025-05-12  4:56:06 0 [Note] Server socket created on IP: '127.0.0.1'.
May 12 04:56:06 kali mariadbd[7508]: 2025-05-12  4:56:06 0 [Note] mariadbd: Event Scheduler: Loaded 0 events
May 12 04:56:06 kali mariadbd[7508]: 2025-05-12  4:56:06 0 [Note] /usr/sbin/mariadbd: ready for connections.
May 12 04:56:06 kali mariadbd[7508]: Version: '11.8.1-MariaDB-4'  socket: '/run/mysqld/mysqld.sock'  port: 3306  Debian n/a
May 12 04:56:06 kali systemd[1]: Started mariadb.service - MariaDB 11.8.1 database server.
May 12 04:56:07 kali debian-start[7568]: ────────────
May 12 04:56:07 kali debian-start[7568]: SELECT count(*) FROM mysql.user WHERE user='root' and password='' and password_expired='N' and plugin in ('', 'mysql_native_password', 'mysql_old_passwor
May 12 04:56:07 kali debian-start[7568]: ────────────
May 12 04:56:07 kali debian-start[7568]: ERROR 1267 (HY000) at line 1: Illegal mix of collations (utf8mb4_general_ci,COERCIBLE) and (utf8mb4_uca1400_ai_ci,COERCIBLE) for operation '='
```

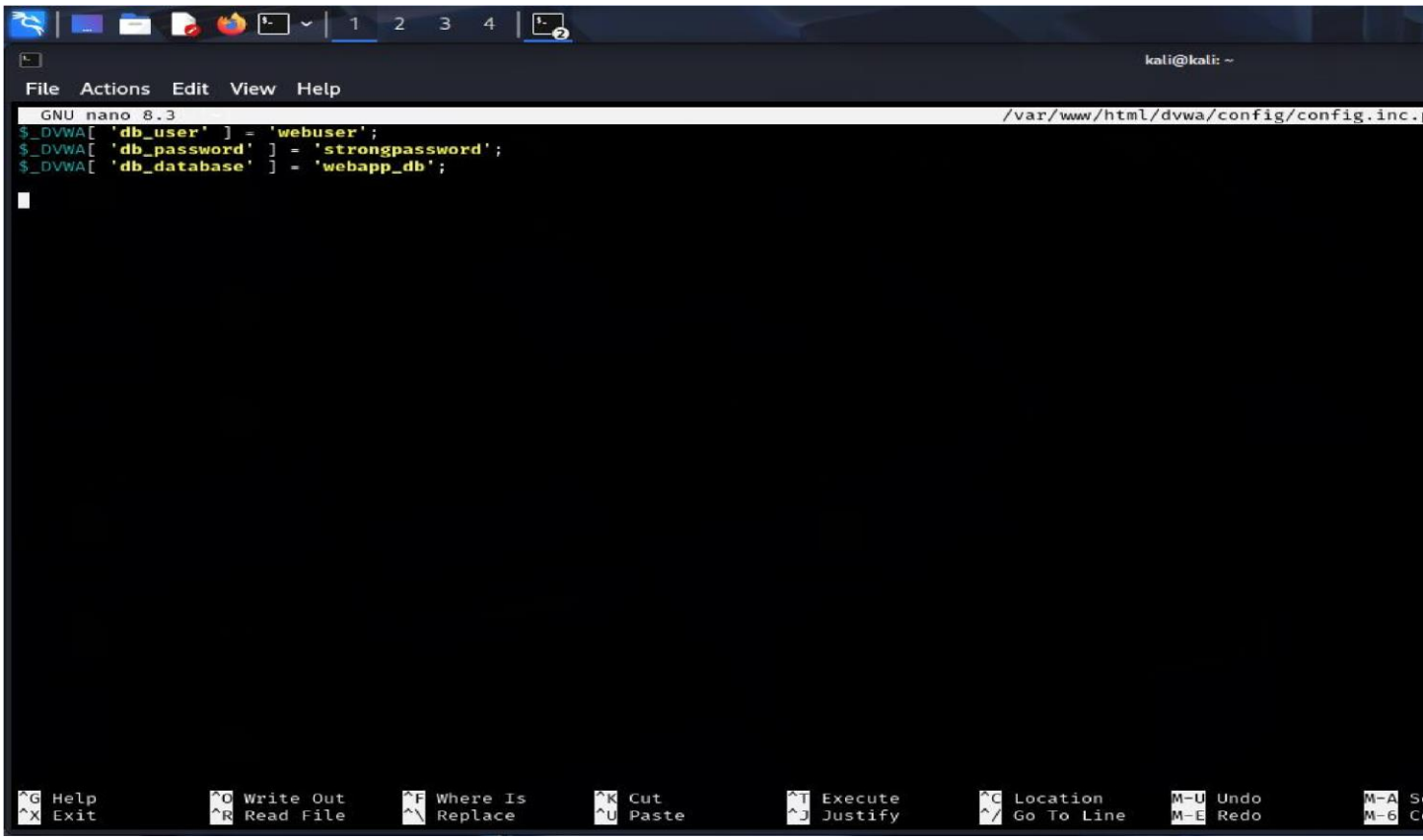
Now open config file which is at /var/www/html/dvwa/config/config.inc.php add the below commands

```
File  Actions  Edit  View  Help
     Status: "Taking your SQL requests now..."
      Tasks: 12 (limit: 14518)
     Memory: 331.2M (peak: 421.2M)
        CPU: 2.938s
     CGroup: /system.slice/mariadb.service
             └─7508 /usr/sbin/mariadbd

May 12 04:56:05 kali mariadbd[7508]: 2025-05-12  4:56:05 0 [Note] InnoDB: Buffer pool(s) load completed at 250512  4:56:05
May 12 04:56:06 kali mariadbd[7508]: 2025-05-12  4:56:06 0 [Note] Server socket created on IP: '127.0.0.1'.
May 12 04:56:06 kali mariadbd[7508]: 2025-05-12  4:56:06 0 [Note] mariadbd: Event Scheduler: Loaded 0 events
May 12 04:56:06 kali mariadbd[7508]: 2025-05-12  4:56:06 0 [Note] /usr/sbin/mariadbd: ready for connections.
May 12 04:56:06 kali mariadbd[7508]: Version: '11.8.1-MariaDB-4'  socket: '/run/mysqld/mysqld.sock'  port: 3306  Debian n/a
May 12 04:56:06 kali systemd[1]: Started mariadb.service - MariaDB 11.8.1 database server.
May 12 04:56:07 kali debian-start[7568]: ────────────
May 12 04:56:07 kali debian-start[7568]: SELECT count(*) FROM mysql.user WHERE user='root' and password='' and password_expired='N' and plugin in ('', 'mysq
May 12 04:56:07 kali debian-start[7568]: ────────────
May 12 04:56:07 kali debian-start[7568]: ERROR 1267 (HY000) at line 1: Illegal mix of collations (utf8mb4_general_ci,COERCIBLE) and (utf8mb4_uca1400_ai_ci,C
lines 1-28/28 (END)
zsh: suspended  sudo systemctl status mariadb

┌──(kali㉿kali)-[~]
└─$ sudo mysql -u root -p

Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 5
Server version: 11.8.1-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 my_database;
Query OK, 1 row affected (0.067 sec)

MariaDB [(none)]> CREATE USER 'my_user'@'localhost' IDENTIFIED BY 'my_password';
Query OK, 0 rows affected (0.069 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON my_database.* TO 'my_user'@'localhost';
Query OK, 0 rows affected (0.001 sec)
```

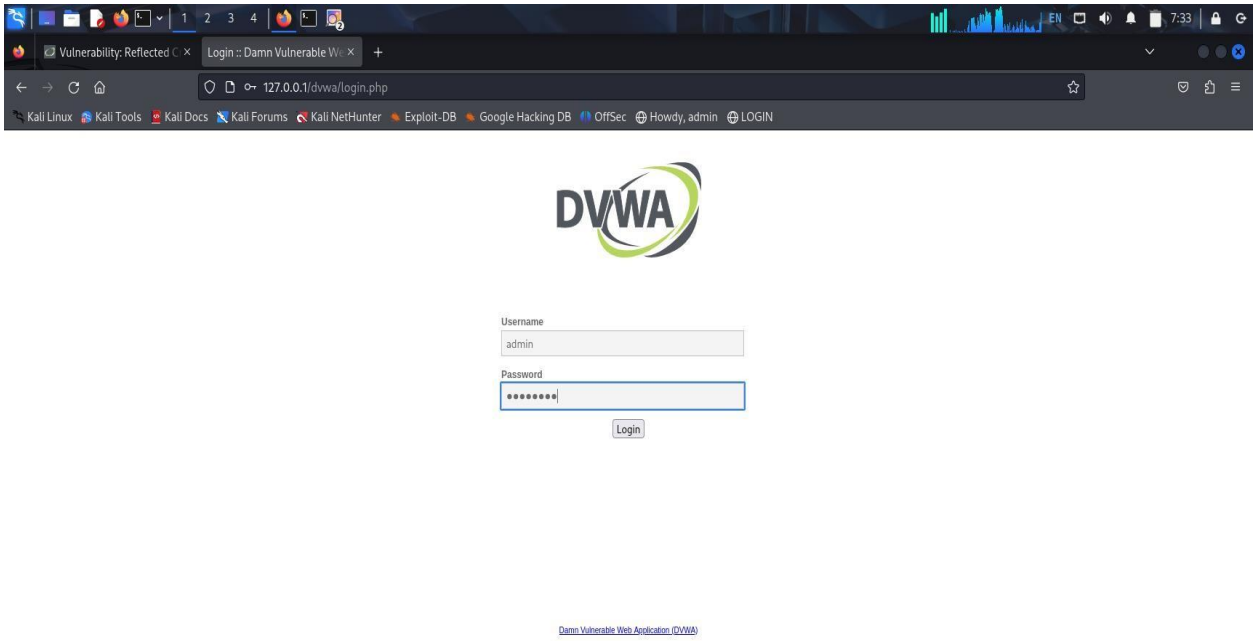
$_DVWA['db_user'] = 'webuser';

$_DVWA['db_password'] = 'strongpassword';

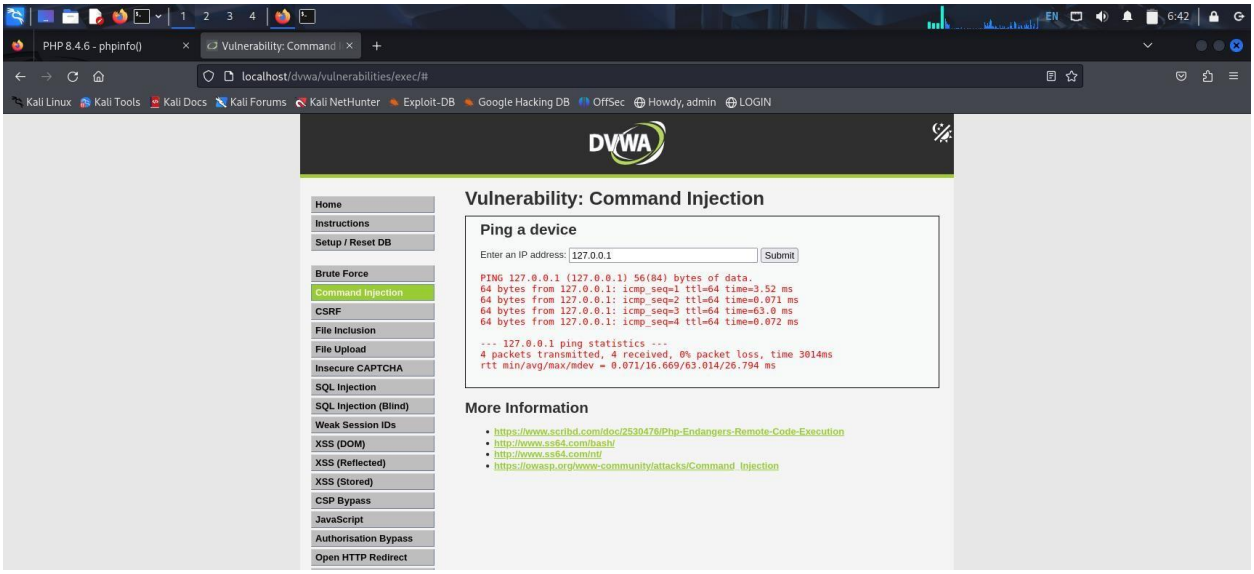
$_DVWA['db_database'] = 'webapp_db';



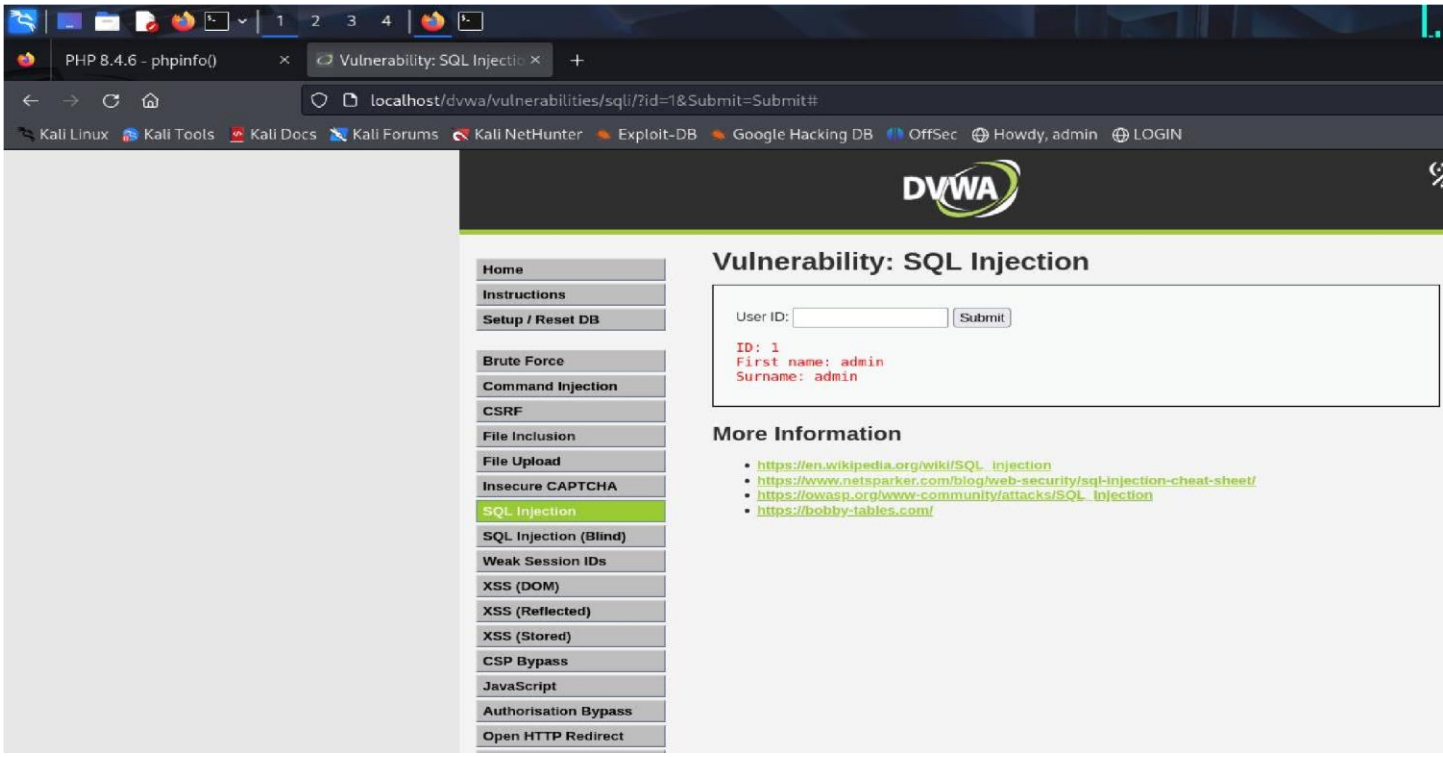
Now open browser type http://localhost/dvwa you can see the below interface.



Login using password and username.

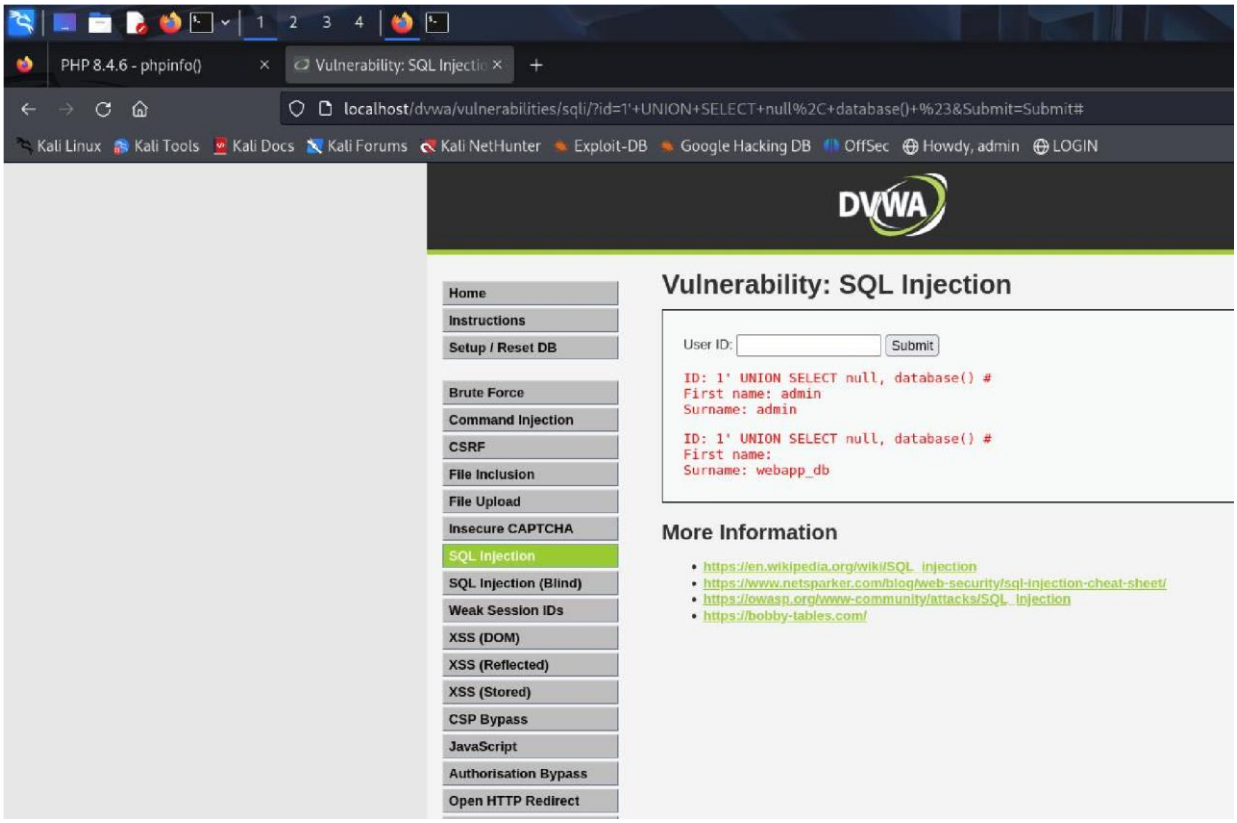


go to command injection and add 127.0.0.1 ip address and submit it then we are ready for sql injection.

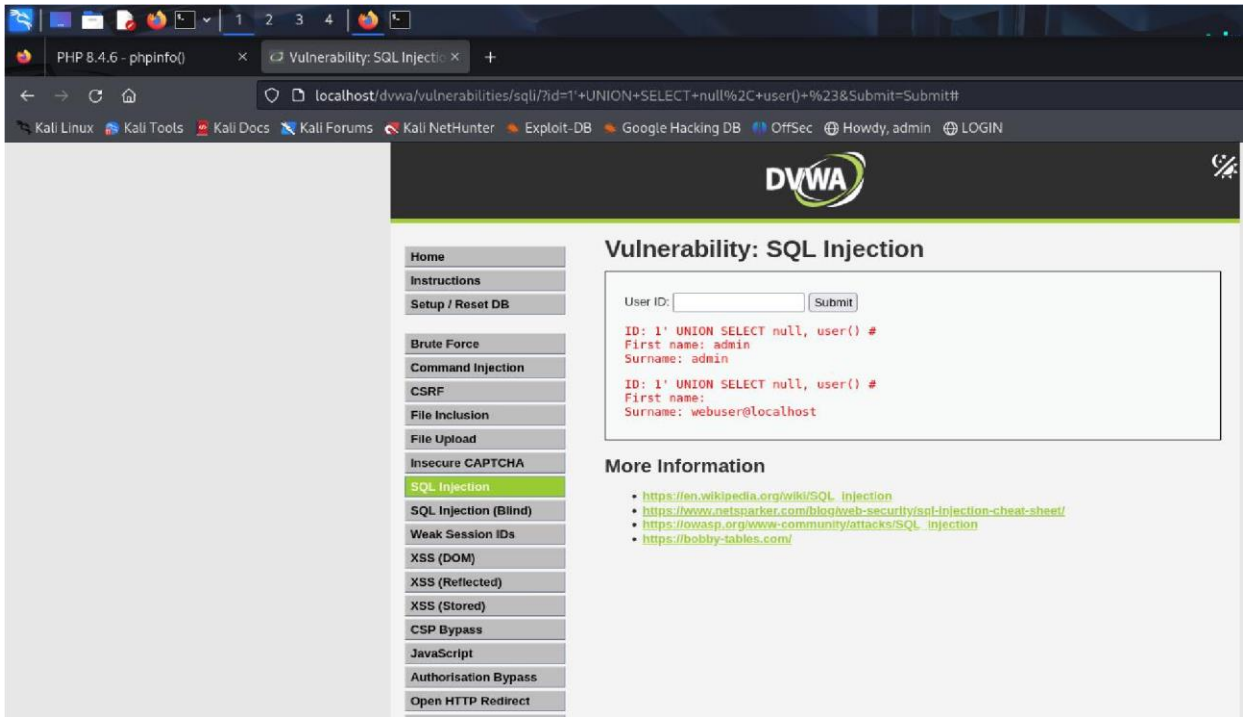


The application is showing data from the database and proves the SQL Injection vulnerability exists.

1' UNION SELECT null, database()

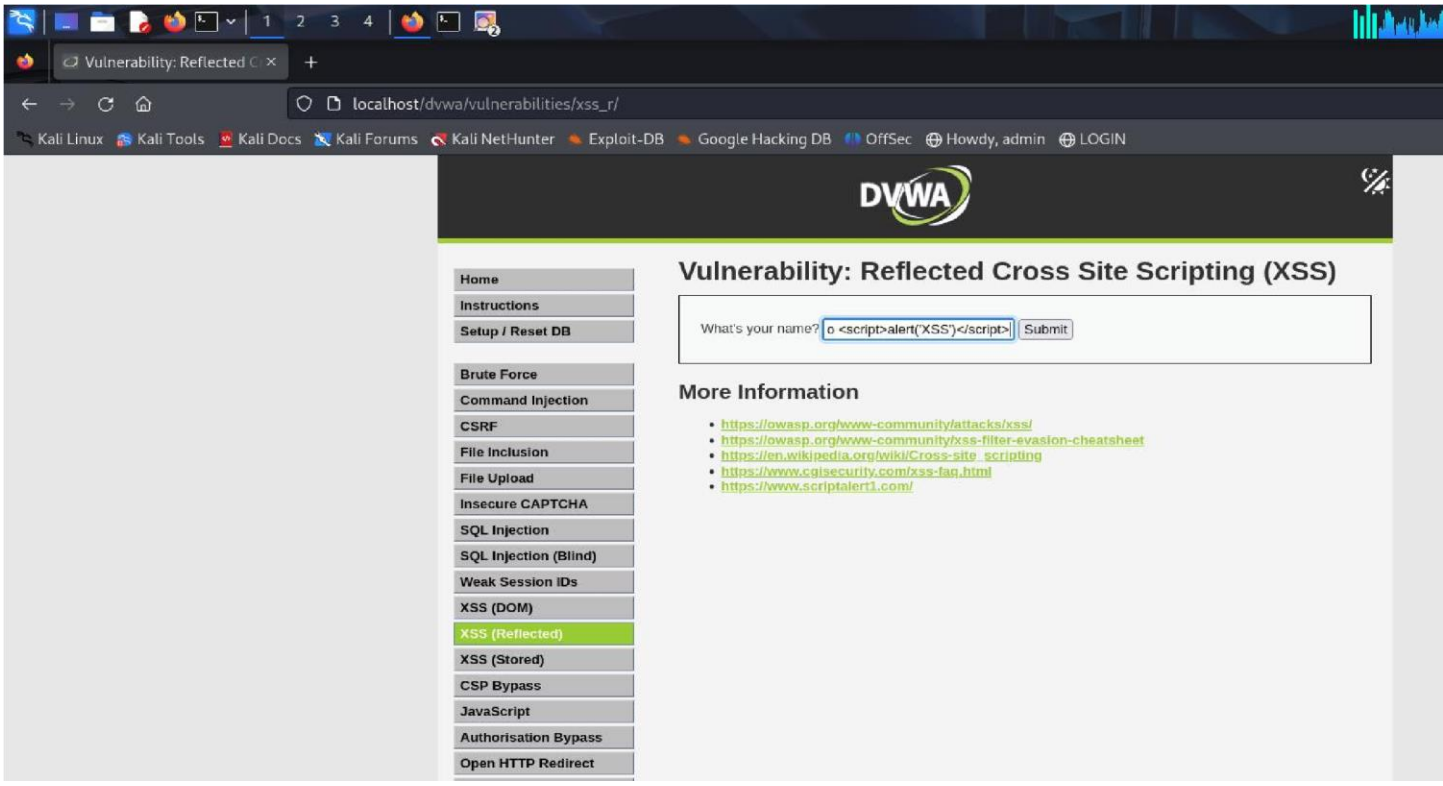


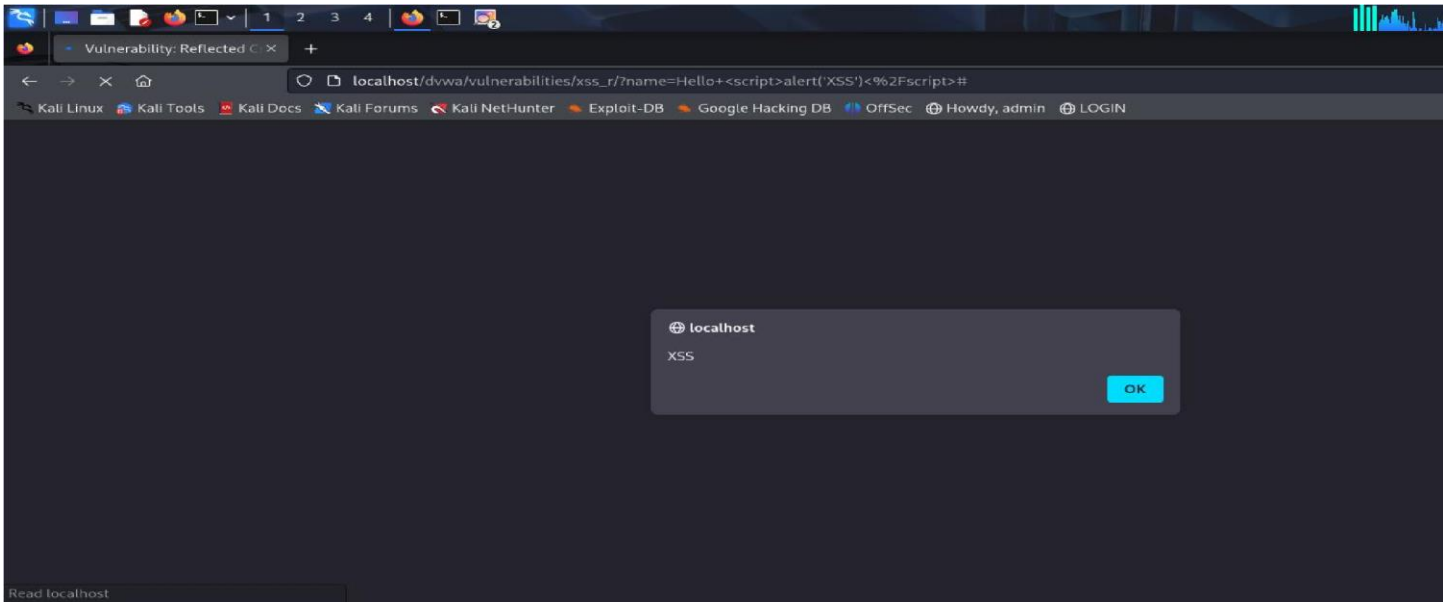
1' UNION SELECT null, version()

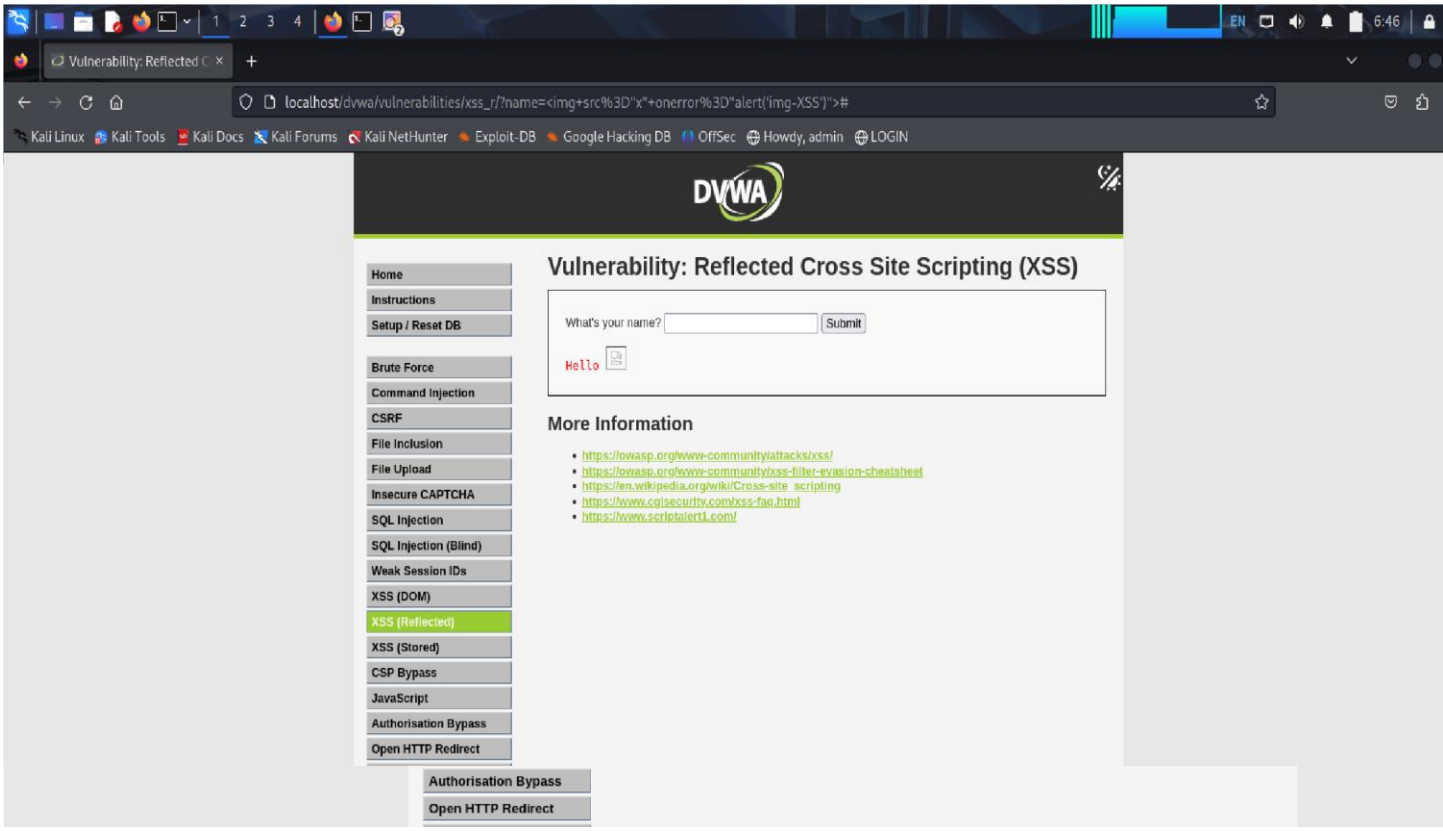


Cross site scripting(xxs)

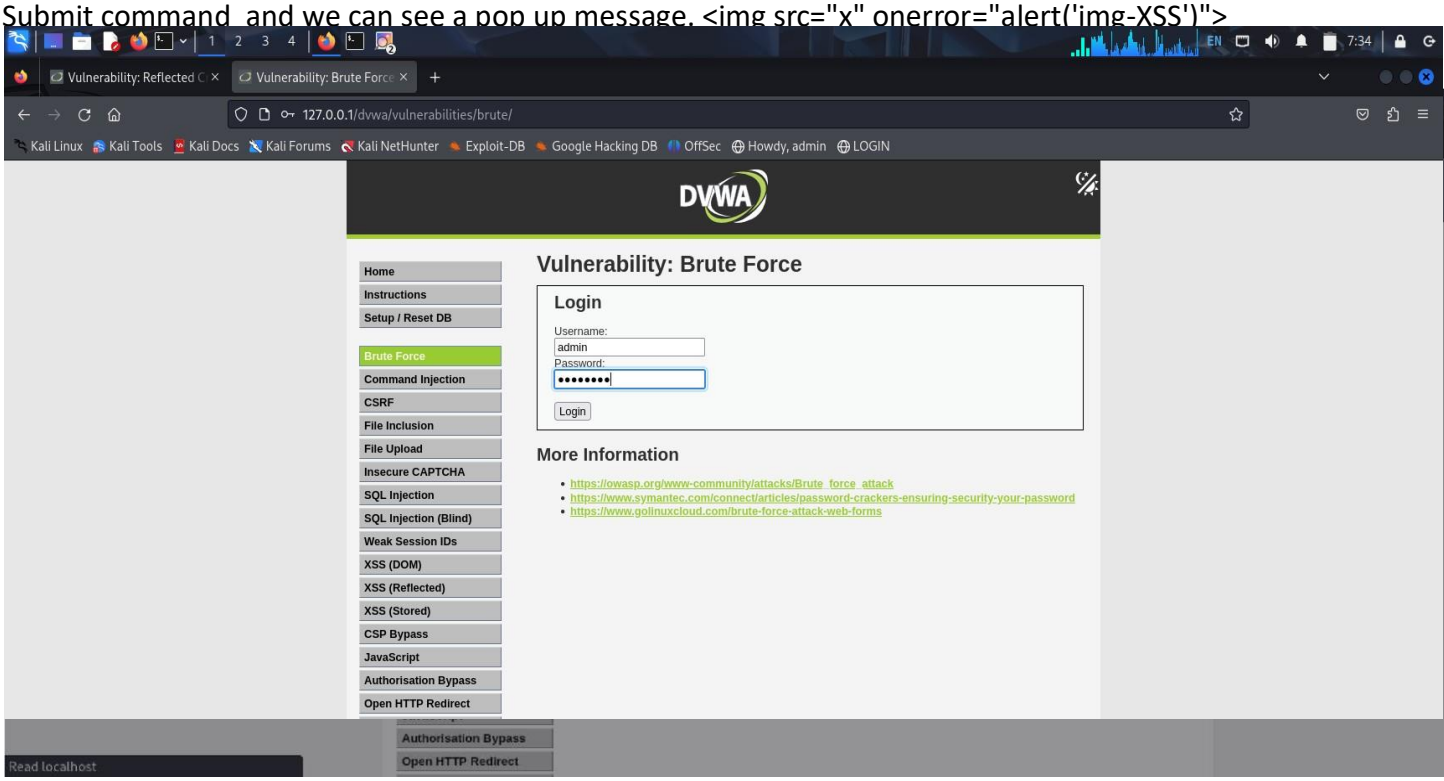
Go to xxs(Reflected) and execute scripting commands



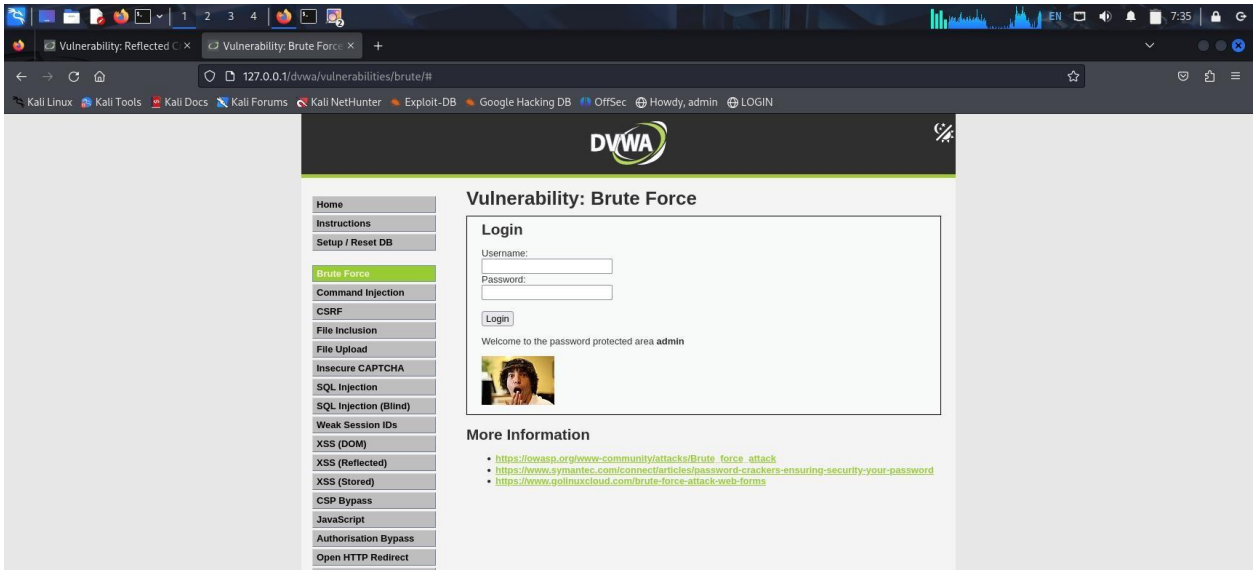




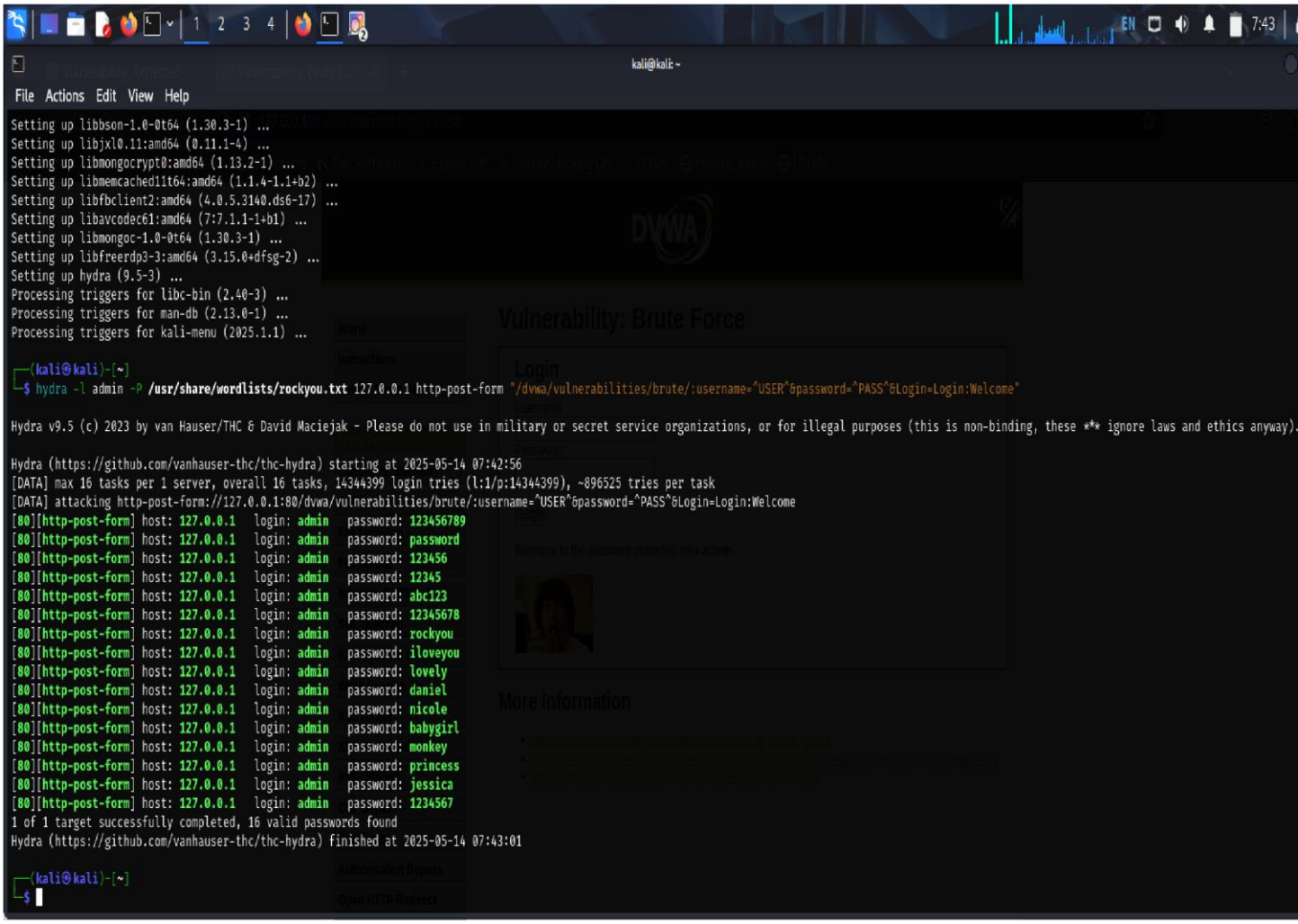
Submit command, and we can see a pop up message. <img src="x" onerror="alert('img-XSS')">



Authentication flaws



to know passwords we can use hydra by using hydra we found 16 passwords and successfully tested vulnerabilities .



Mitigation stratergies

For sql :

Use Prepared Statements / Parameterized Queries,Employ ORM frameworks (like SQLAlchemy, Hibernate) that abstract raw queries, validate and sanitize user input (e.g., no direct injection into SQL strings).

Use stored procedures with input binding (if applicable), limit database permissions (e.g., no DROP access for web users), use Web Application Firewalls (WAFs) to block suspicious SQL patterns.

For xxs:

Escape all user input when displaying it in HTML (htmlspecialchars() in PHP), use Content Security Policy (CSP) headers to restrict script sources, validate and sanitize inputs (e.g., disallow <script> and event handlers).

Use secure frameworks that auto-escape (e.g., React, Django templates), encode output based on context (HTML, JS, URL, etc.).

Apply input length limits to reduce payload risk.

For authentication flaws:

Enforce strong password policies (minimum length, complexity), implement rate-limiting / account lockout after multiple failed attempts.

Use Multi-Factor Authentication (MFA), monitor login attempts and notify users of suspicious activity.

Use CAPTCHAs to block bots during login,salt and hash passwords using secure algorithms (bcrypt, Argon2).