Setup a Vulnerable Web Server DVWA in Kali Linux localhost

Why we need a vulnerable web server?

Attacking on a website or server in internet without legal permission will considered as crime. Practice makes perfect, but where to practice our hacking skills ?

A simple answer is on our localhost. Localhost is a locally hosted web server it can be hosted on our PC and not connected to the internet.

There is a famous quote "There is no place like 127.0.0.1". This 127.0.0.1 is our home server or local server. This is an awesome place to learn and practice our skills. That's why it is the best place. No place can better then localhost.

How to set up ?

DVWA stands for Damn Vulnerable Web Application. Oh yes, it is too vulnerable. In this web application security researchers, penetration testers or ethical hackers test their skills and run tools in a legal environment.

DVWA is designed for practice some most common web vulnerability. It is made with PHP and mySQL. Let's start without wasting time.

In Linux environment localhost files are stored in /var/www/html directory, so we open a terminal and change our directory to that directory using following command:

```
cd /var/www/html
```

Here we clone DVWA from it's Github repository. To clone it we run following command:

```
git clone https://github.com/ethicalhack3r/DVWA
```

```
root@kali:~# cd /var/www/html
root@kali:/var/www/html# git clone https://github.com/ethicalhack3r/DVWA
Cloning into 'DVWA'...
remote: Enumerating objects: 11, done.
remote: Counting objects: 100% (11/11), done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 3022 (delta 3), reused 2 (delta 0), pack-reused 3011
Receiving objects: 100% (3022/3022), 1.53 MiB | 123.00 KiB/s, done.
Resolving deltas: 100% (1327/1327), done.
root@kali:/var/www/html#
```

After the cloning complete, we rename the DVWA to dvwa (it is not necessary but it will save our effort).

```
mv DVWA dvwa
```

Then we change the permission on dvwa directory by using following command:-

```
chmod -R 777 dvwa/
```

```
root@kali:/var/www/html# chmod -R 777 dvwa
root@kali:/var/www/html#
```

Now we have to setup this web application to run properly for that we have to go into /dvwa/config directory.

```
cd dvwa/config
```

Using ls command we can the list of files.

```
ls
```

```
root@kali:/var/www/html# chmod -R 777 dvwa
root@kali:/var/www/html# cd dvwa/config
root@kali:/var/www/html/dvwa/config# ls
config.inc.php.dist
root@kali:/var/www/html/dvwa/config#
```

In the above screenshot we can see the config.inc.php.dist file. This file contains default configuration. We need to make a copy of this file with .php extension name, we are coping this file because in future if anything goes wrong then we have the default values. So we copy this file with .php extension name using following command:-

```
cp config.inc.php.dist config.inc.php
```

Then we check the copied file using ls command:

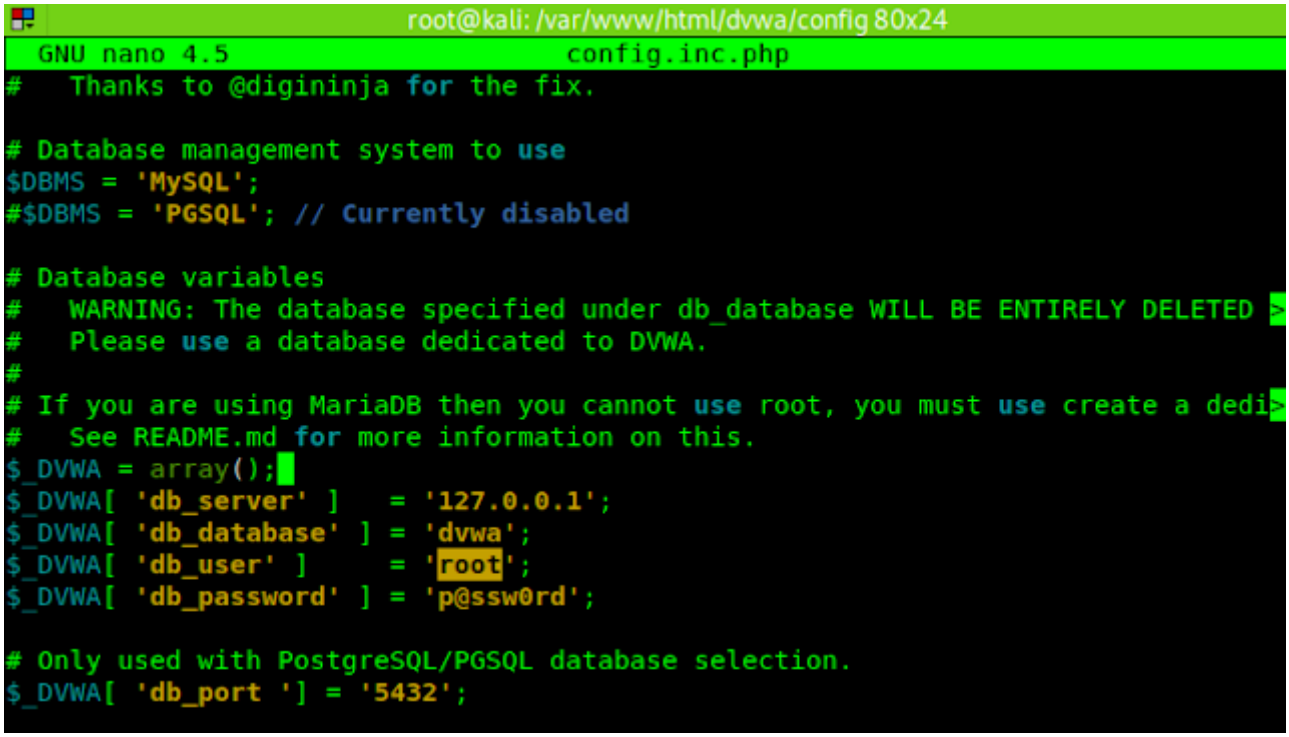
```
ls
```

```
root@kali:/var/www/html# chmod -R 777 dvwa
root@kali:/var/www/html# cd dvwa/config
root@kali:/var/www/html/dvwa/config# ls
config.inc.php.dist
root@kali:/var/www/html/dvwa/config# cp config.inc.php.dist config.inc.php
root@kali:/var/www/html/dvwa/config# ls
config.inc.php  config.inc.php.dist
root@kali:/var/www/html/dvwa/config#
```

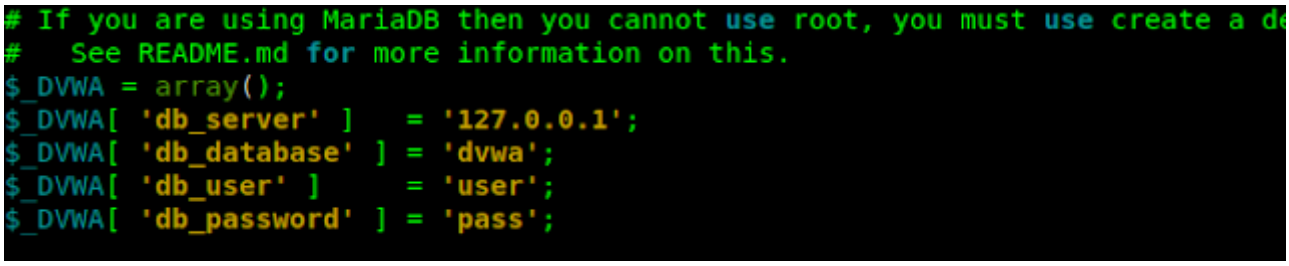
Then we use nano editor to make changes on our newly created PHP file.

```
nano config.inc.php
```

The screenshot is following:-



We will make changes in this part the p@ssw0rd to pass and the user from root. Watch the following screenshot:-



Then we save it using CTRL+X and press Y to save changes and Enter button to save and exit.

The next is configuring the database.

Here we have opened a new terminal window closing the previous one. We start the mysql at first using following command:-

```
service mysql start
```

If there are no errors that means the service is started.

Now let's login to mysql using following command:-

```
mysql -u root -p
```

Here in our Kali Linux root is our superuser name, if we have something else then we need to change that user.

In the password field we press Enter without typing password; because we didn't set any password for it, now mysql will open like following screenshot:-

```
root@kali:~# service mysql start
root@kali:~# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 38
Server version: 10.3.20-MariaDB-1 Debian buildd-unstable

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

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Now to setup a database, we start with creating a new user by applying following command:-

```
create user 'user'@'127.0.0.1' identified by 'pass';
```

Here using this command we are creating a user called 'user' running server on 127.0.0.1(localhost) and the password is 'pass'. Remember that this username and password should exactly same as the password and username we have entered in the configuration file of dvwa web application.

```
MariaDB [(none)]> create user 'user'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.002 sec)
```

In the screenshot we can see the query is OK. That means the user is created.

Then we grant this user all the privileges over the database. For that we type following command:-

```
grant all privileges on dvwa.* to 'user'@'127.0.0.1' identified by 'pass';
```

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'user'@'127.0.0.1' identified by 'pass'
Query OK, 0 rows affected (0.021 sec)

MariaDB [(none)]>
```

Yes, we have finished the work of database, now we configure the server. For this we need to configure our apache2 server. Let's change our directory to /etc/php/7.3/apache2

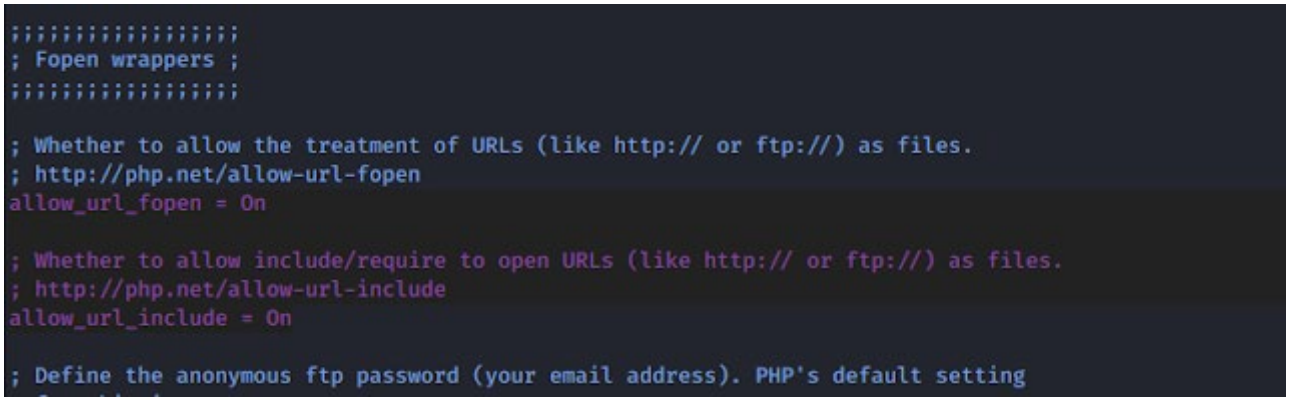
Here we are using version 7.3, if we use another version then the path might be change.

```
cd /etc/php/7.3/apache2
```

Here we configure the php.ini file using leafpad of any good text editor. We have used mousepad editor.

```
mousepad php.ini
```

We need to change the *allow_url_fopen* and *allow_url_include* values. We set both of them 'On'. In some cases when we are first time configuring it, we might find that one of this or both of this configuration is set to 'Off'. We have turned both of these configuration to 'On', as the following screenshot:-

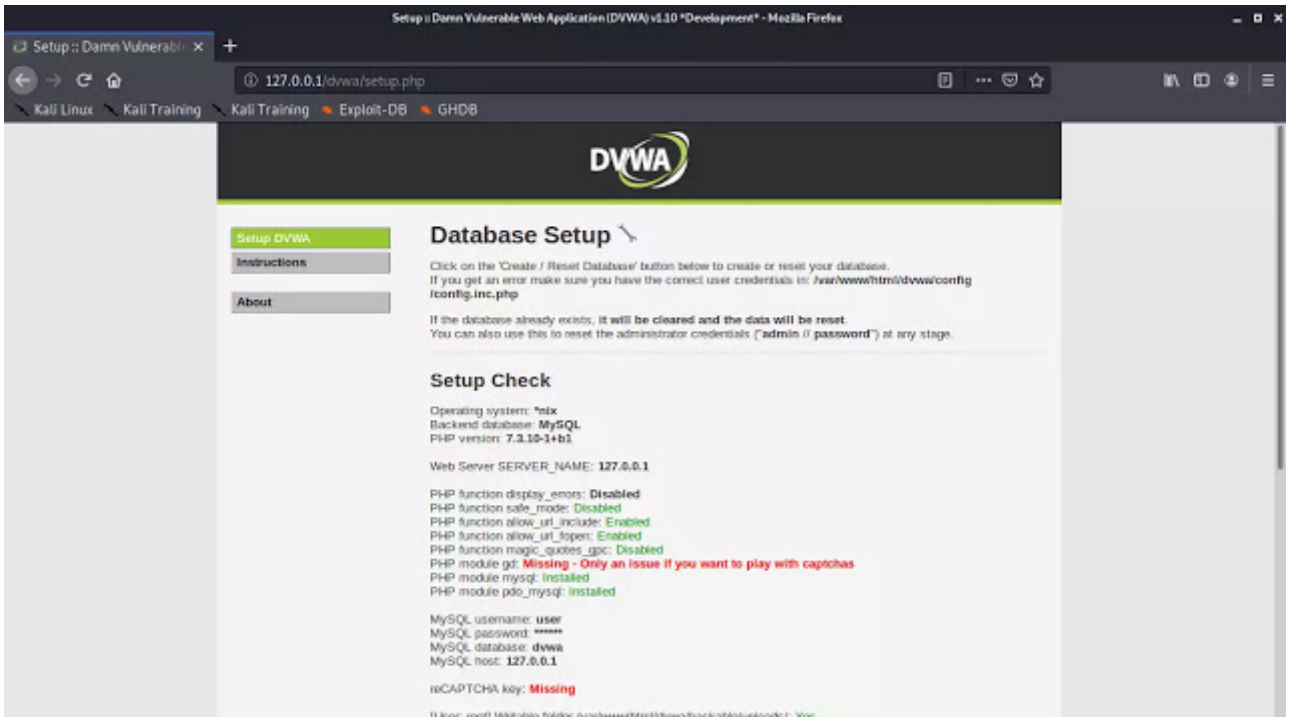


Then we save and close the file.

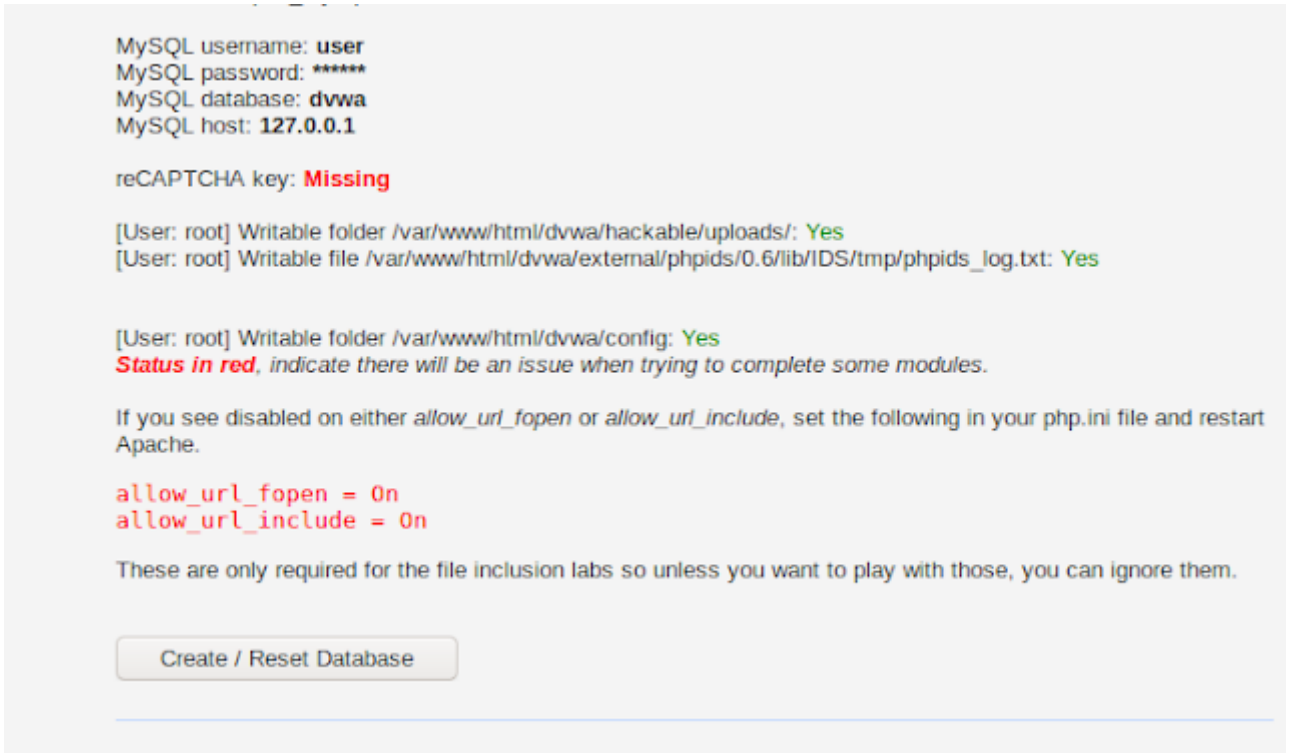
Then we start the apache2 server using following command:-

```
service apache2 start
```

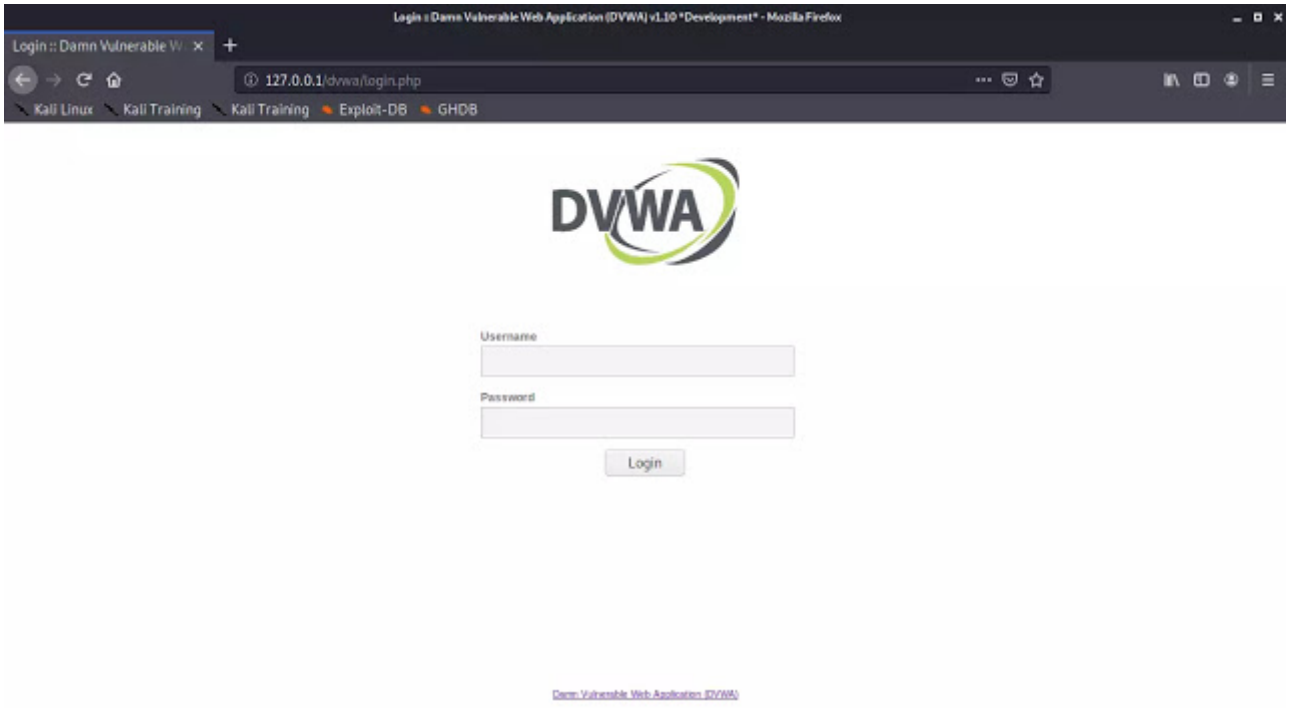
Let's open the browser and navigate to 127.0.0.1/dvwa/ first open will open the setup.php as shown in the screenshot.



Here we scroll down and click on "Create/Reset Database".



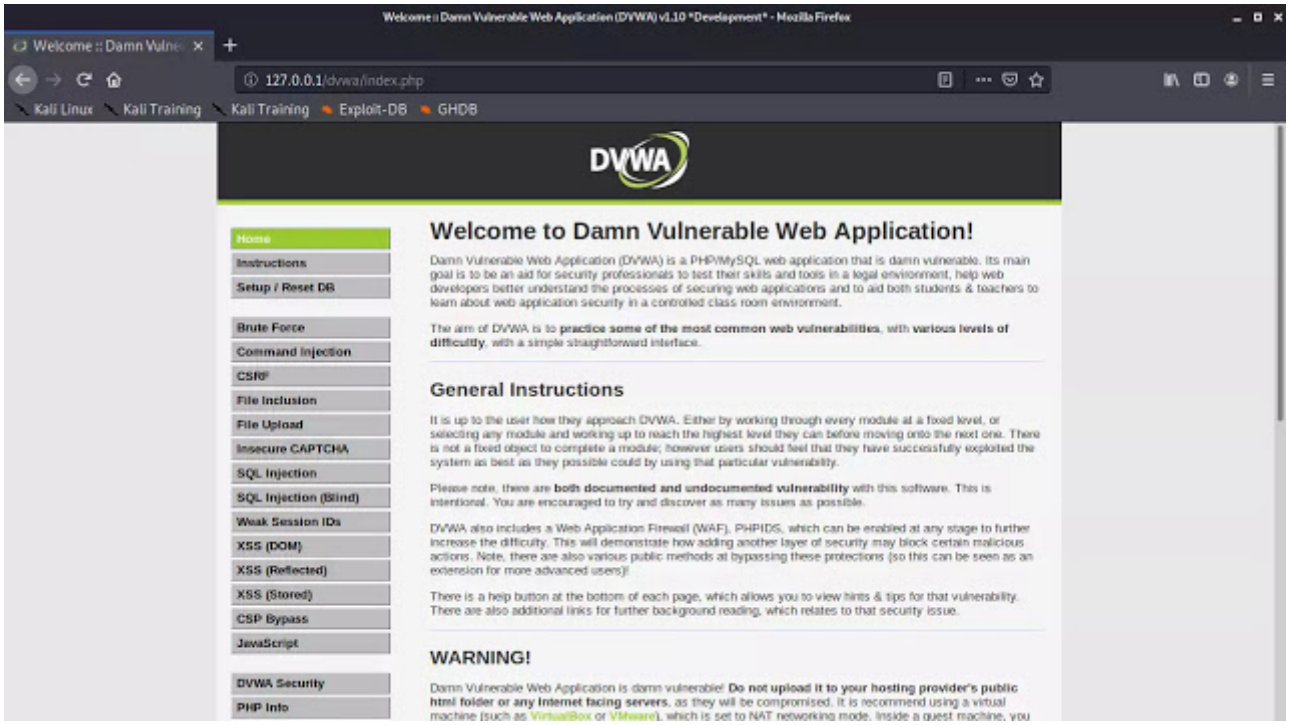
Then it will create and configure the database and we redirected to DVWA login page.



The default login is

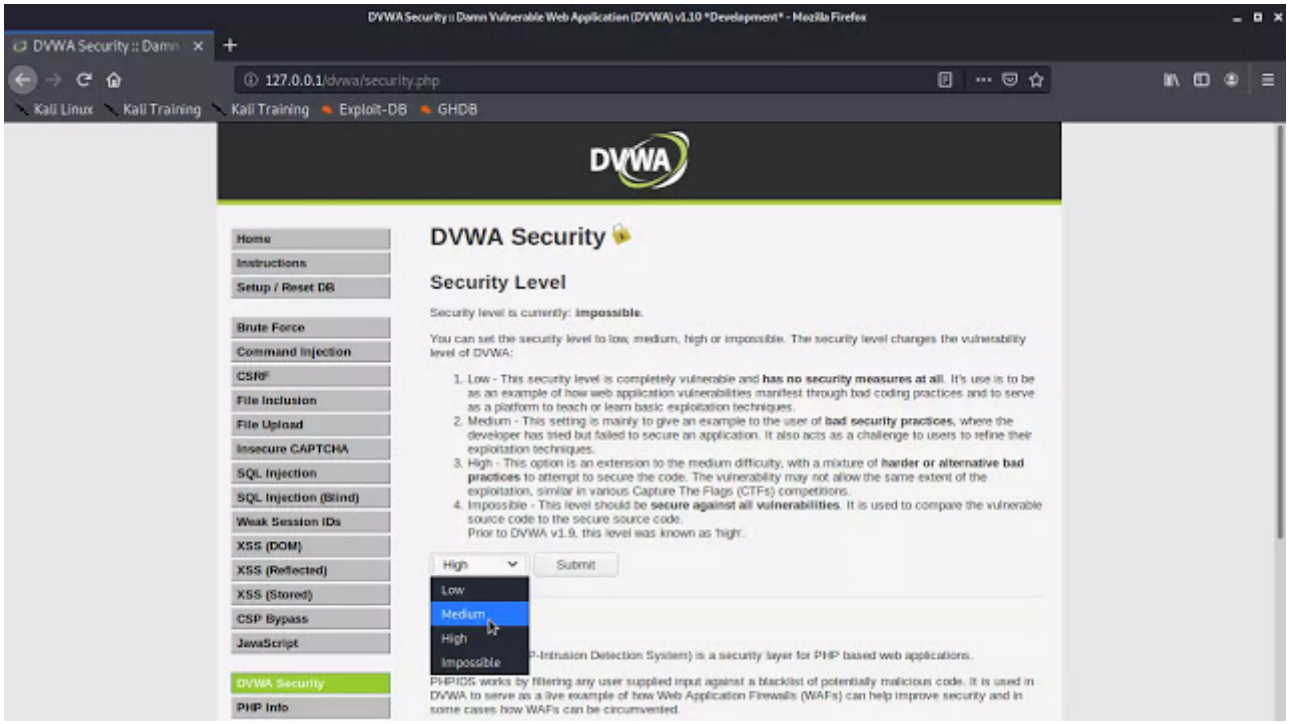
- Username:- admin
- Password:- password

After login we are in Damn Vulnerable Web Applications main page. Here is some general information and warnings.



On the left side we can see lots of vulnerable pages are available we can practice here.

DVWA have different security levels to change those we navigate to DVWA security. There are some security levels low, medium, high, impossible. We can choose difficulty as we need.



Now we can run penetration testing tools and techniques in our localhost.

This is how we can setup **DVWA**, Damn Vulnerable Web Application in our **Kali Linux** system. This is very helpful for beginners to advanced users, because of it multilayered security levels.