

# DVWA SETUP

Setting up DVWA (Damn Vulnerable Web Application) on Kali Linux involves a few steps. DVWA is a PHP/MySQL web application that is intentionally vulnerable to help security professionals test their skills and tools in a legal environment. Here is a step-by-step guide to setting up DVWA on Kali Linux:

## 1. Update Kali Linux:

Open a terminal and run the following commands to update your system:

```
sudo apt update
```

```
sudo apt upgrade
```

## 2. Navigate to the web directory

```
(kali㉿kali)-[~]  
$ cd /var/www/html  
  
(kali㉿kali)-[/var/www/html]  
$ pwd  
/var/www/html
```

## 3. Download DVWA.

```
(kali㉿kali)-[/var/www/html]  
$ sudo git clone https://github.com/digininja/DVWA.git  
Cloning into 'DVWA' ...  
remote: Enumerating objects: 4514, done.  
remote: Counting objects: 100% (64/64), done.  
remote: Compressing objects: 100% (53/53), done.  
remote: Total 4514 (delta 23), reused 42 (delta 10), pack-reused 4450  
Receiving objects: 100% (4514/4514), 2.30 MiB | 3.38 MiB/s, done.  
Resolving deltas: 100% (2118/2118), done.
```

## 4. Set Permissions: Change the ownership of the DVWA directory.

```
(kali㉿kali)-[/var/www/html]  
$ sudo chmod -R 777 DVWA
```

## 5. Configure DVWA: Navigate to the DVWA directory and copy the sample configuration file.

```
(kali㉿kali)-[/var/www/html/DVWA/config]  
$ ls  
config.inc.php.dist  
  
(kali㉿kali)-[/var/www/html/DVWA/config]  
$ sudo cp config.inc.php.dist config.inc.php  
  
(kali㉿kali)-[/var/www/html/DVWA/config]  
$ ls  
config.inc.php config.inc.php.dist
```

6. Edit the config.inc.php file by nano editor:

```
(kali㉿kali)-[/var/www/html/DVWA/config]
$ sudo nano config.inc.php
```

7. Update the database settings as follows:

```
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'dvwa';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
$_DVWA[ 'db_port' ] = '3306';

# ReCAPTCHA settings
$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'admin';
$_DVWA[ 'db_password' ] = 'password';
$_DVWA[ 'db_port' ] = '3306';
```

8. **Configure MySQL:**

Start the MySQL service and log in to MySQL and create the database and user for DVWA.

```
(kali㉿kali)-[/var/www/html/DVWA/config]
$ sudo service mysql start

(kali㉿kali)-[/var/www/html/DVWA/config]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 33
Server version: 10.11.6-MariaDB-2 Debian n/a

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)]> create database dvwa;
```

Inside the MySQL prompt, run:

```
CREATE DATABASE dvwa;
```

```
CREATE USER 'dvwa'@'localhost' IDENTIFIED BY 'password';
```

```
GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa'@'localhost';
```

```
FLUSH PRIVILEGES.
```

```
EXIT.
```

```
MariaDB [(none)]> create database dvwa;  
Query OK, 1 row affected (1.586 sec)  
  
MariaDB [(none)]> create user 'admin'@'127.0.0.1' identified by 'password';  
Query OK, 0 rows affected (0.011 sec)  
  
MariaDB [(none)]> grant all privileges on dvwa.* to 'admin'@'127.0.0.1';  
Query OK, 0 rows affected (0.001 sec)
```

#### 9. Start Apache:

Start the Apache service.

```
(kali㉿kali)-[/var/www/html/DVWA/config]  
$ sudo service apache2 start  
  
(kali㉿kali)-[/var/www/html/DVWA/config]  
$ sudo nano /etc/php/8.1/apache2/php.ini
```

#### 10. Edit php file by nano editor

sudo nano /etc/php/8.2/apache2/php.ini

```
(kali㉿kali)-[~]  
$ sudo nano /etc/php/8.2/apache2/php.ini
```

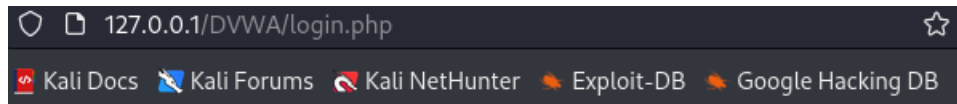
On both the url

```
;;;;;;;;;;;;;;;;;;;;;;;;;  
; Fopen wrappers ;  
;;;;;;;;;;;;;;;;;;;;;;;;;  
  
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.  
; https://php.net/allow-url-fopen  
allow_url_fopen = On  
  
; Whether to allow include/require to open URLs (like https:// or ftp://) as files.  
; https://php.net/allow-url-include  
allow_url_include = on
```

```
(kali@kali)-[~]  
$ sudo service apache2 reload
```

#### 11. Login to DVWA:

After the database setup, navigate to <http://localhost/DVWA/login.php> and use the default credentials:



Username

Password

Login