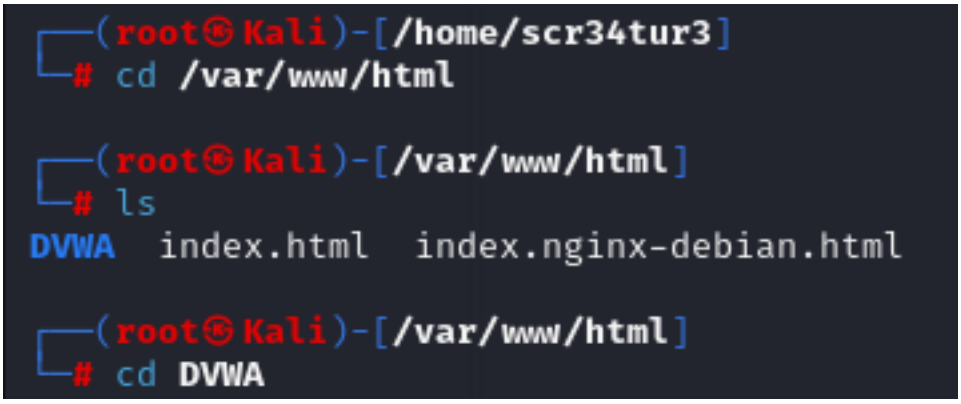
DVWA

INTRODUCTION:
~ Here is a step by step guide on how to set up DVWA for web app sec testing.
~Lets get started;

# switch to root

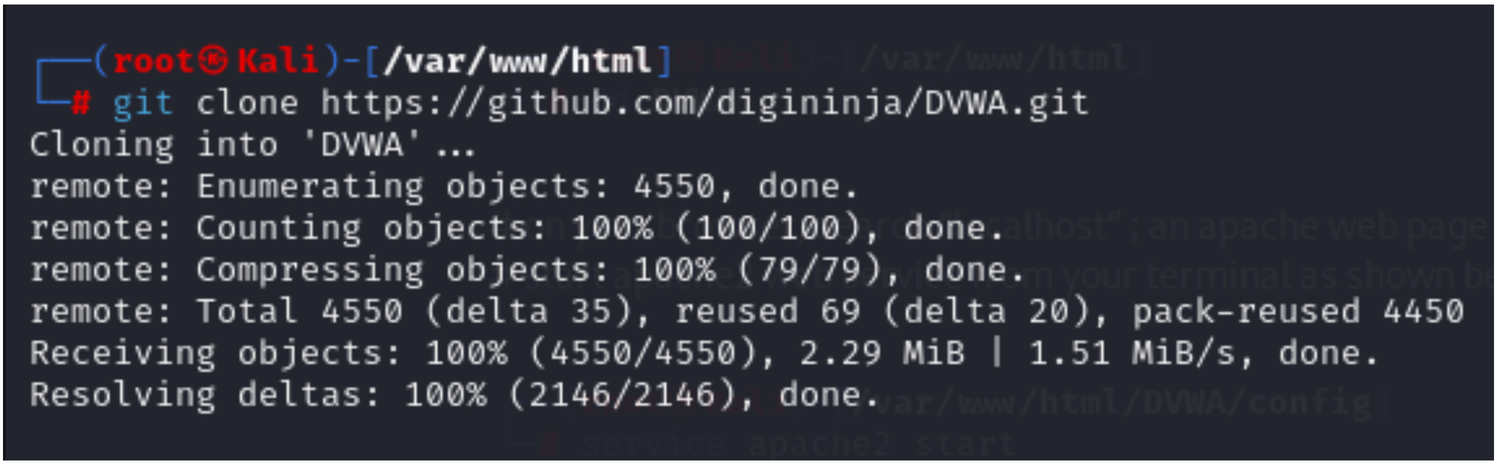
# update your system - apt update

#navigate to /var/www/html: this is where all web applications are hosted



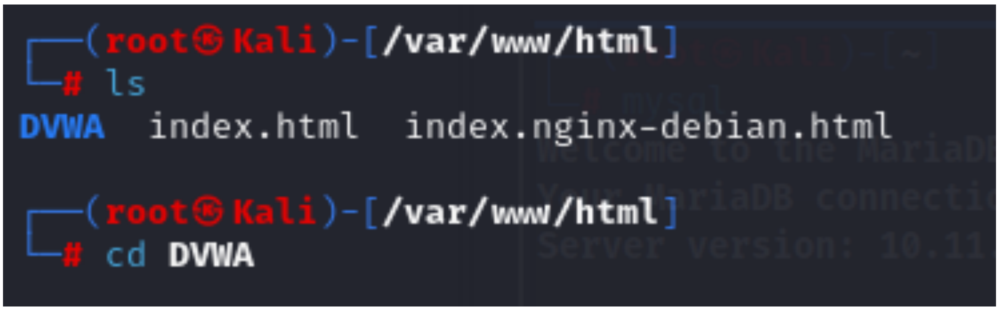
```
┌──(root㉿Kali)-[/home/scr34tur3]
└─# cd /var/www/html

┌──(root㉿Kali)-[/var/www/html]
└─# ls
DVWA  index.html  index.nginx-debian.html

┌──(root㉿Kali)-[/var/www/html]
└─# cd DVWA
```

# clone DVWA by digininja.



```
┌──(root㉿Kali)-[/var/www/html]
└─# git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA'...
remote: Enumerating objects: 4550, done.
remote: Counting objects: 100% (100/100), done.
remote: Compressing objects: 100% (79/79), done.
remote: Total 4550 (delta 35), reused 69 (delta 20), pack-reused 4450
Receiving objects: 100% (4550/4550), 2.29 MiB | 1.51 MiB/s, done.
Resolving deltas: 100% (2146/2146), done.
```

# cd into DVWA

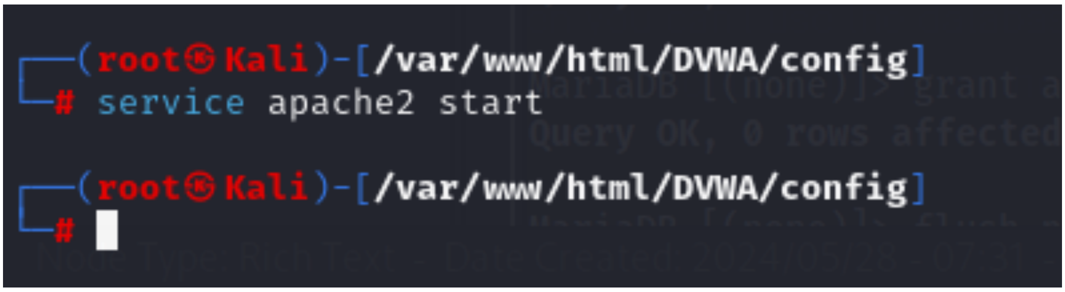


```
┌──(root㉿Kali)-[/var/www/html]
└─# ls
DVWA  index.html  index.nginx-debian.html

┌──(root㉿Kali)-[/var/www/html]
└─# cd DVWA
```

# on your browser, search "localhost" ; an apache web page should be presented. Trying to search something

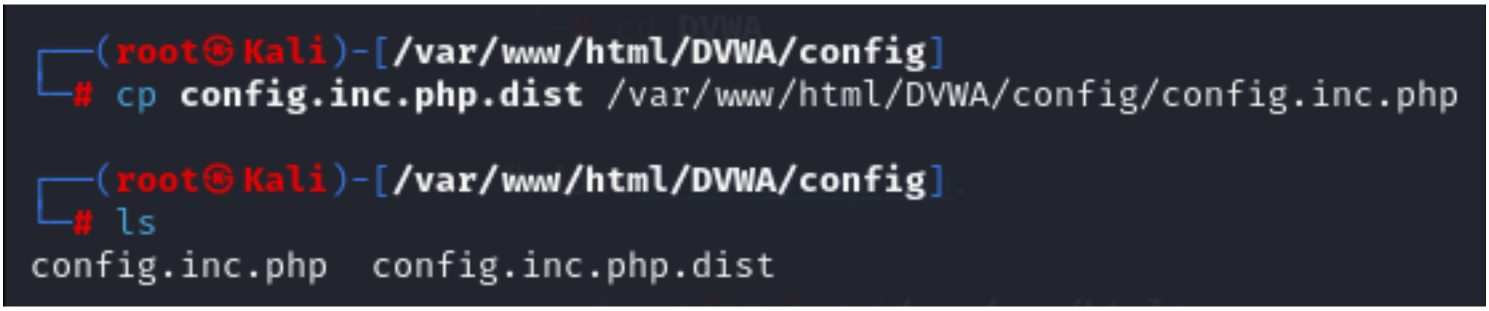
addition, won't yield anything useful. So we start the apache server on our local machine

# start apache2 web service from your terminal as shown below.



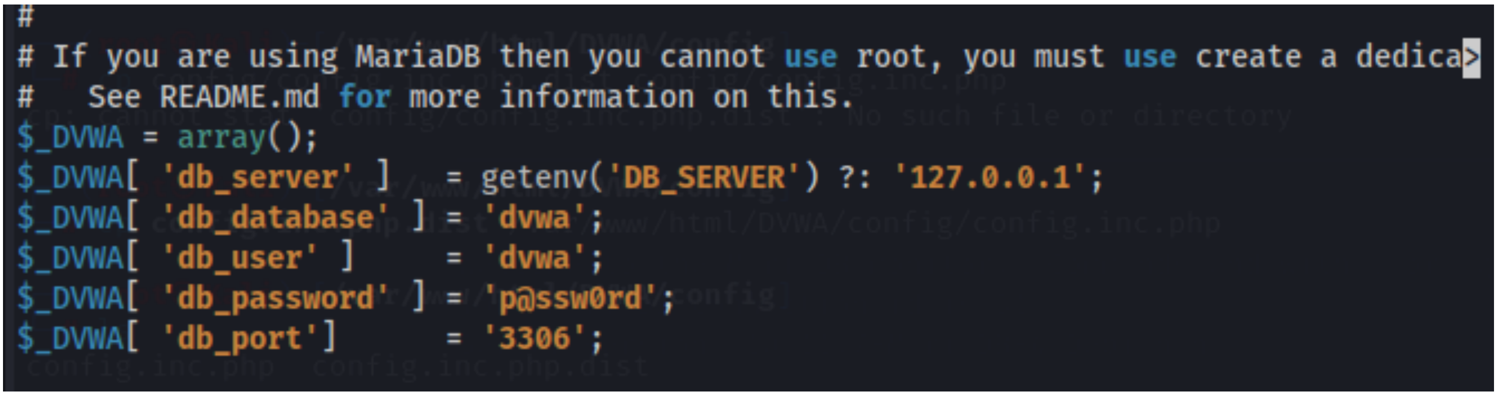
```
┌──(root㉿Kali)-[/var/www/html/DVWA/config]
└─# service apache2 start

┌──(root㉿Kali)-[/var/www/html/DVWA/config]
└─# 
```

# Now go into the DVWA folder into the config folder and copy the config.inc.php.dist and save it using the name config.inc.php.



```
┌──(root㉿Kali)-[/var/www/html/DVWA/config]
└─# cp config.inc.php.dist /var/www/html/DVWA/config/config.inc.php

┌──(root㉿Kali)-[/var/www/html/DVWA/config]
└─# ls
config.inc.php  config.inc.php.dist
```

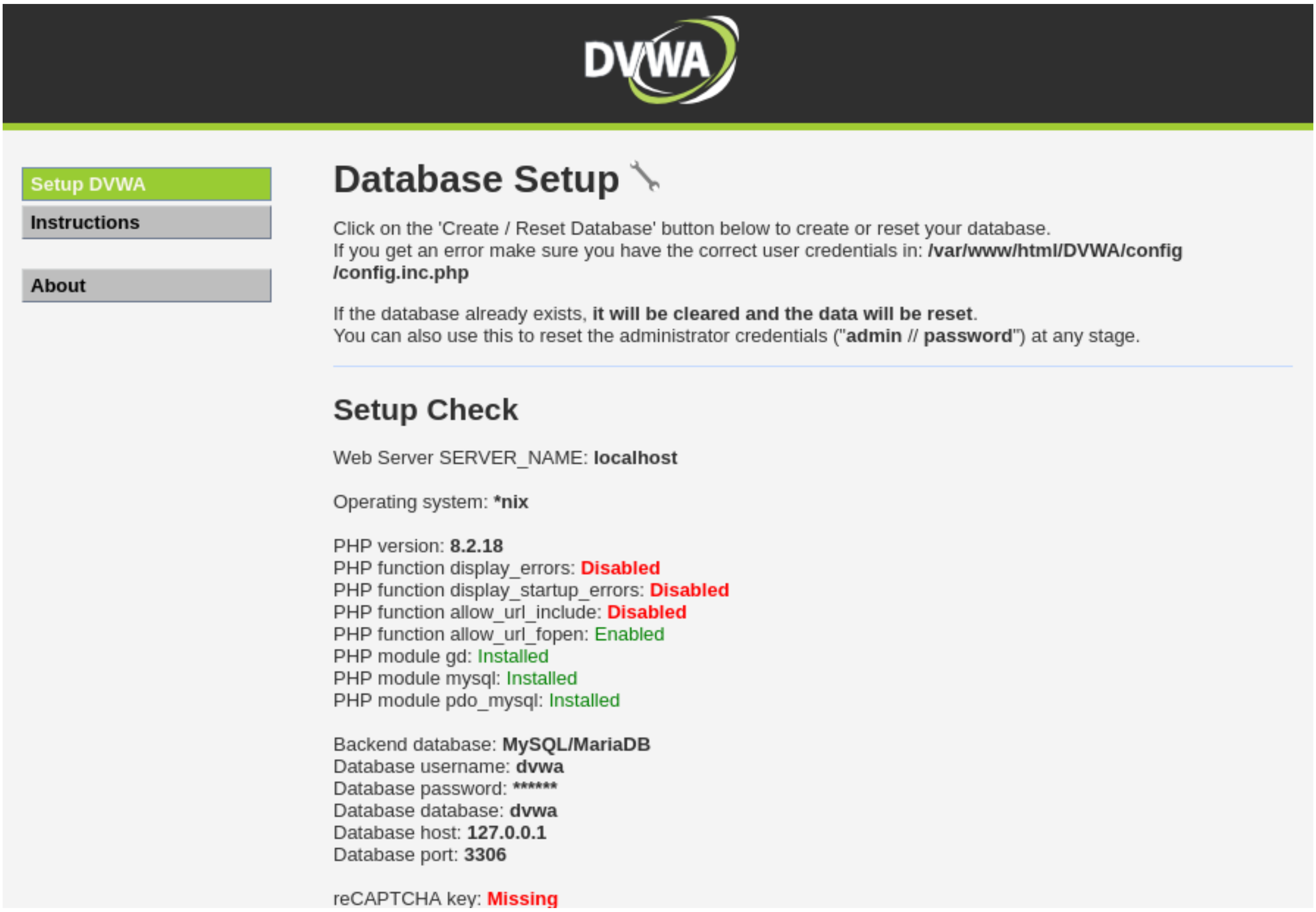
# Open the .inc.php file using vim and configure the login credentials correctly as shown below.



```
#
# If you are using MariaDB then you cannot use root, you must use create a dedica>
#   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';
```

# After this DVWA can be accessed using the url 127.0.0.1/DVWA hosted on local server.

#Now that DVWA is running, it has to be set up in order to use it properly for practicing penetration testing . Before setting up DVWA this is how its setup page will look.



Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **/var/www/html/DVWA/config/config.inc.php**

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Web Server SERVER_NAME: **localhost**

Operating system: ***nix**

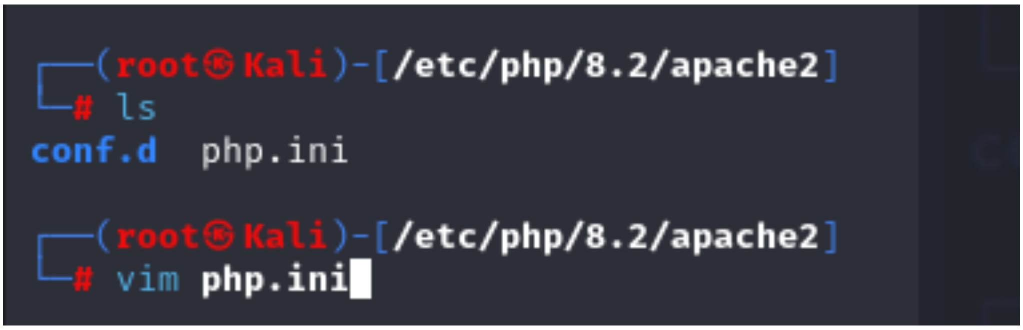
PHP version: **8.2.18**
PHP function display_errors: **Disabled**
PHP function display_startup_errors: **Disabled**
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: **MySQL/MariaDB**
Database username: **dvwa**
Database password: **********
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3306**

reCAPTCHA key: **Missing**

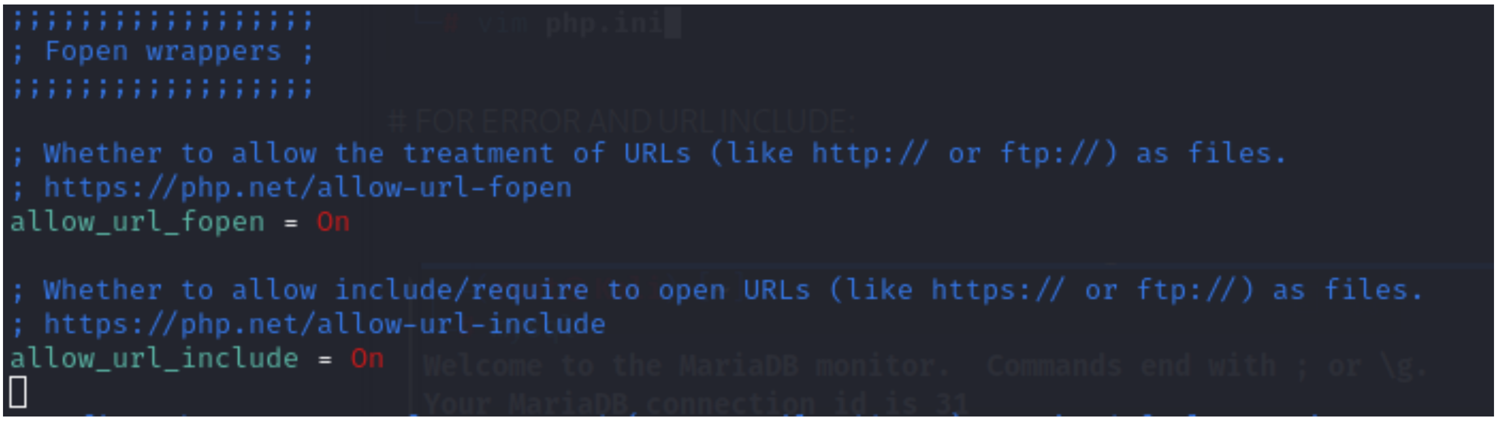
#***Setting up DVWA:***

Now to set up the various parameters of DVWA, navigate to /etc/php/8.1/apache2 folder where the php.ini file can be found. Edit this file to enable error handling and url_include.

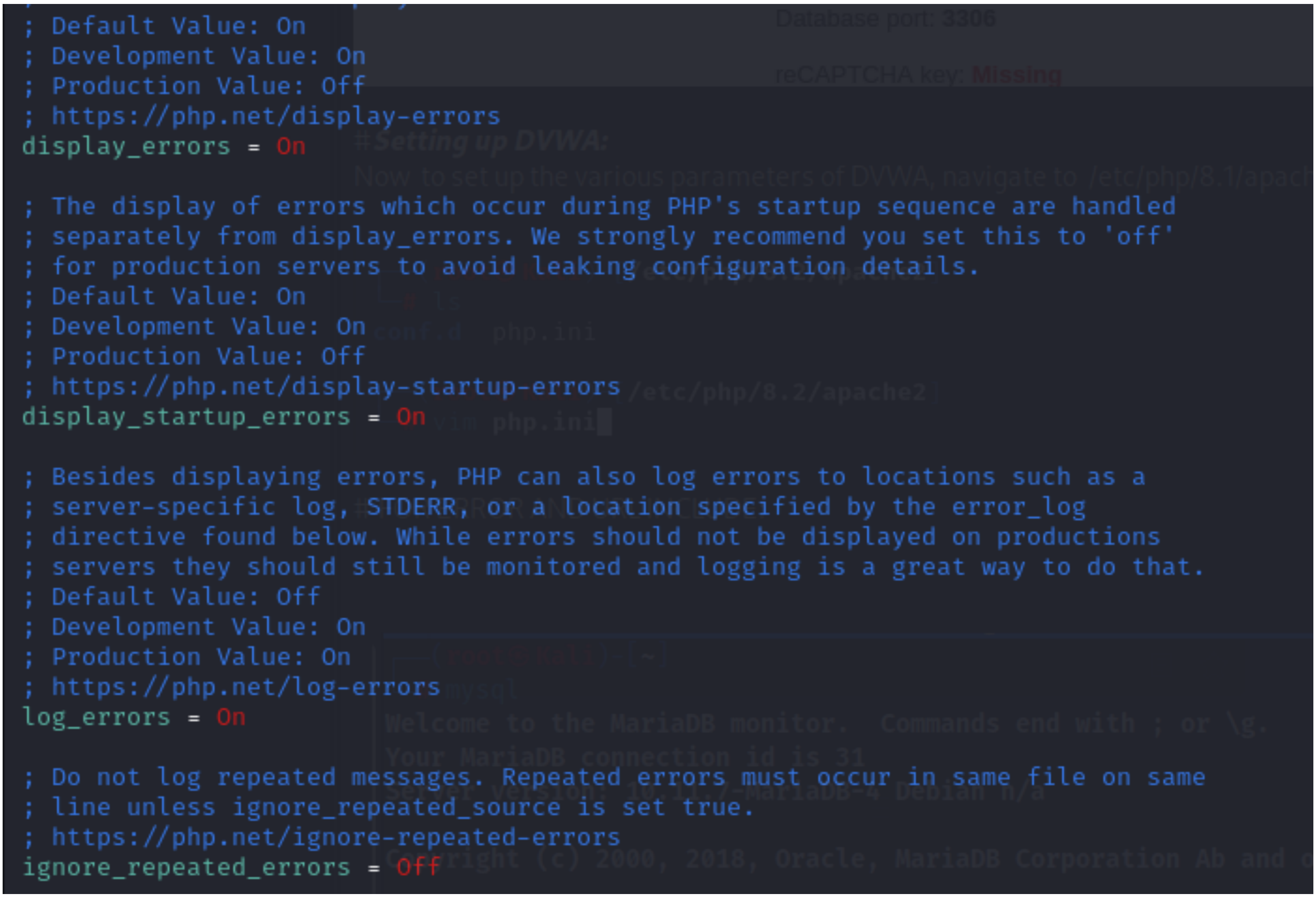


```
┌──(root㉿Kali)-[/etc/php/8.2/apache2]
└─# ls
conf.d   php.ini

┌──(root㉿Kali)-[/etc/php/8.2/apache2]
└─# vim php.ini
```

# FOR ERROR AND URL INCLUDE:

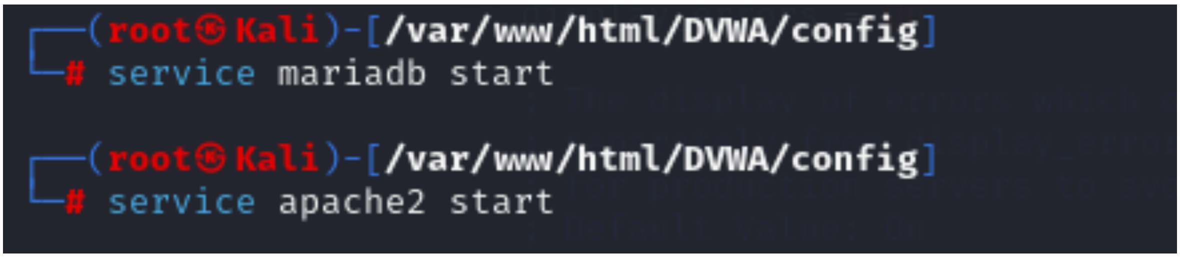


```
;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;

; 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
```



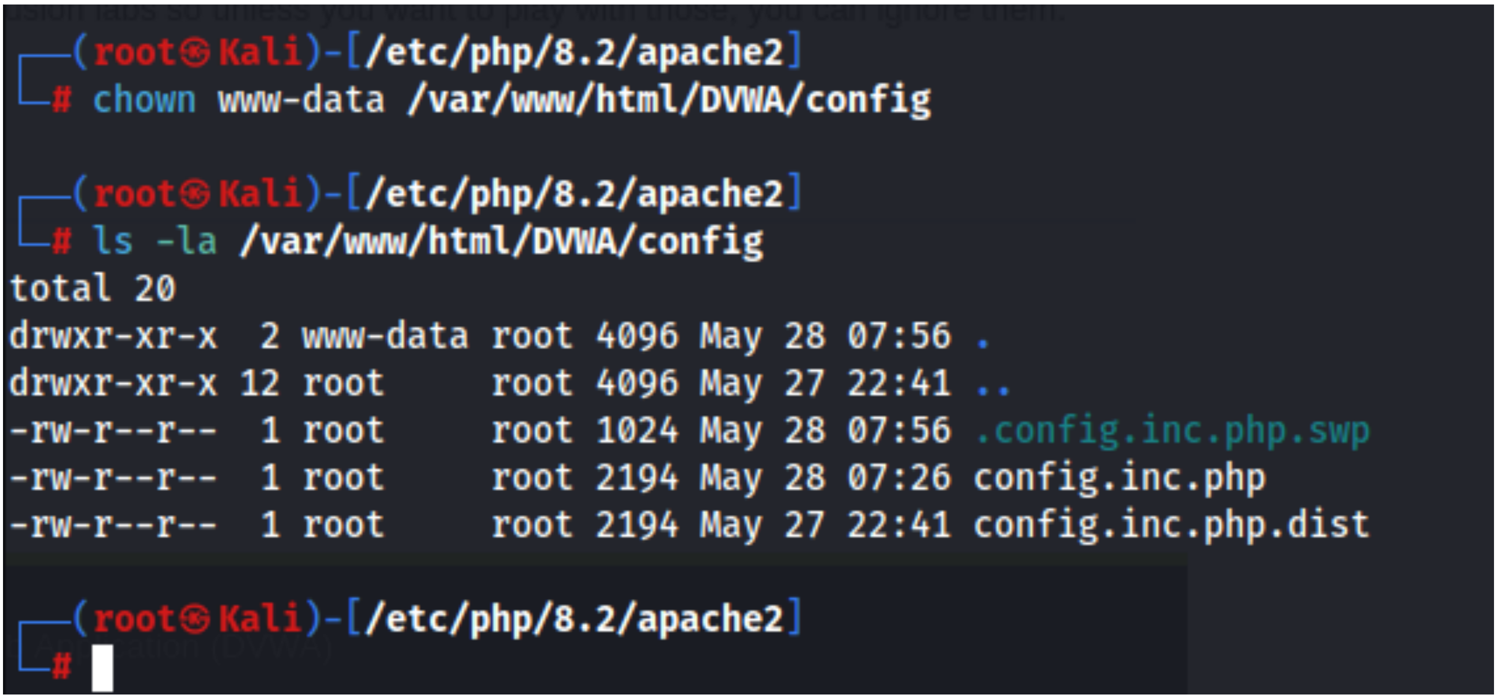
```
; Default Value: On
; Development Value: On
; Production Value: Off
; https://php.net/display-errors
display_errors = On

; The display of errors which occur during PHP's startup sequence are handled
; separately from display_errors. We strongly recommend you set this to 'off'
; for production servers to avoid leaking configuration details.
; Default Value: On
; Development Value: On
; Production Value: Off
; https://php.net/display-startup-errors
display_startup_errors = On

; Besides displaying errors, PHP can also log errors to locations such as a
; server-specific log, STDERR, or a location specified by the error_log
; directive found below. While errors should not be displayed on productions
; servers they should still be monitored and logging is a great way to do that.
; Default Value: Off
; Development Value: On
; Production Value: On
; https://php.net/log-errors
log_errors = On

; Do not log repeated messages. Repeated errors must occur in same file on same
; line unless ignore_repeated_source is set true.
; https://php.net/ignore-repeated-errors
ignore_repeated_errors = Off
```

# Now we'll start the mariadb server and apache2 server as shown below.



```
┌──(root㉿Kali)-[/var/www/html/DVWA/config]
└─# service mariadb start

┌──(root㉿Kali)-[/var/www/html/DVWA/config]
└─# service apache2 start
```

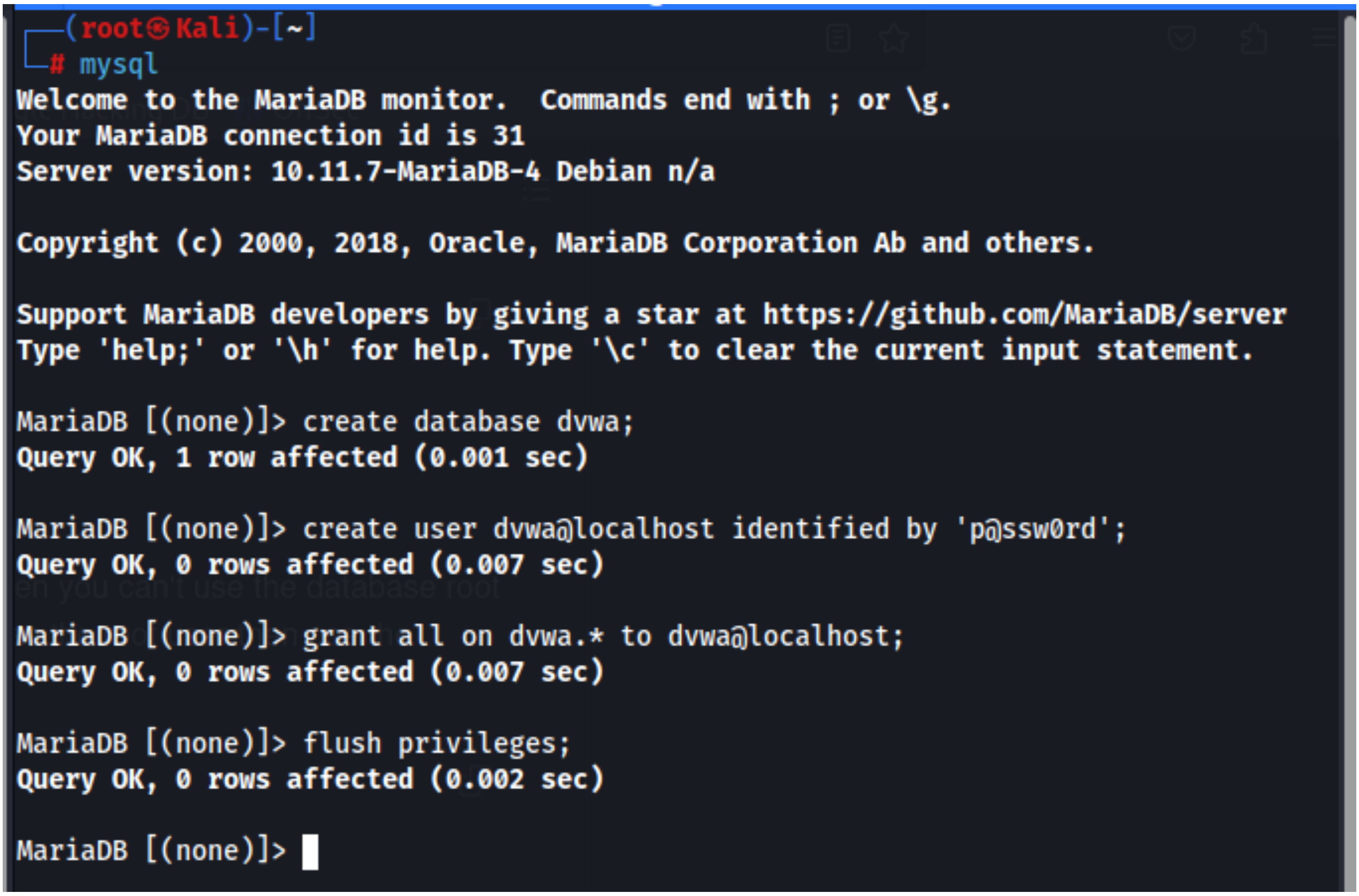
# Now we'll make files and folders writable, by using the commands as shown below.



```
┌──(root㉿Kali)-[/etc/php/8.2/apache2]
└─# chown www-data /var/www/html/DVWA/config

┌──(root㉿Kali)-[/etc/php/8.2/apache2]
└─# ls -la /var/www/html/DVWA/config
total 20
drwxr-xr-x  2 www-data root 4096 May 28 07:56 .
drwxr-xr-x 12 root     root 4096 May 27 22:41 ..
-rw-r--r--  1 root     root 1024 May 28 07:56 .config.inc.php.swp
-rw-r--r--  1 root     root 2194 May 28 07:26 config.inc.php
-rw-r--r--  1 root     root 2194 May 27 22:41 config.inc.php.dist

┌──(root㉿Kali)-[/etc/php/8.2/apache2]
└─# 
```

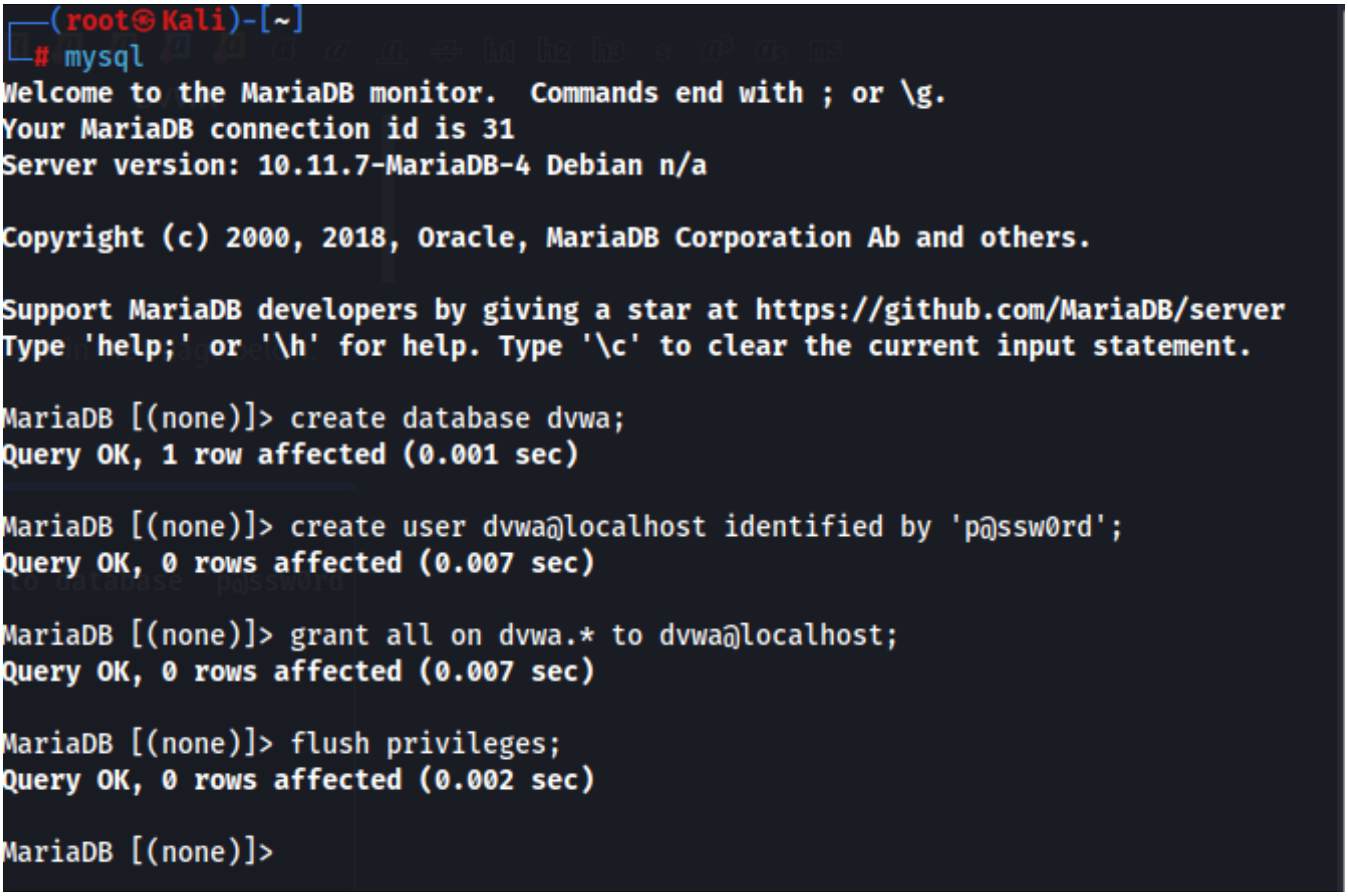
# From the image below, you can see there is no table created on the mysql db.

#



```
┌──(root㉿Kali)-[~]
└─# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.7-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 (0.001 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> 
```

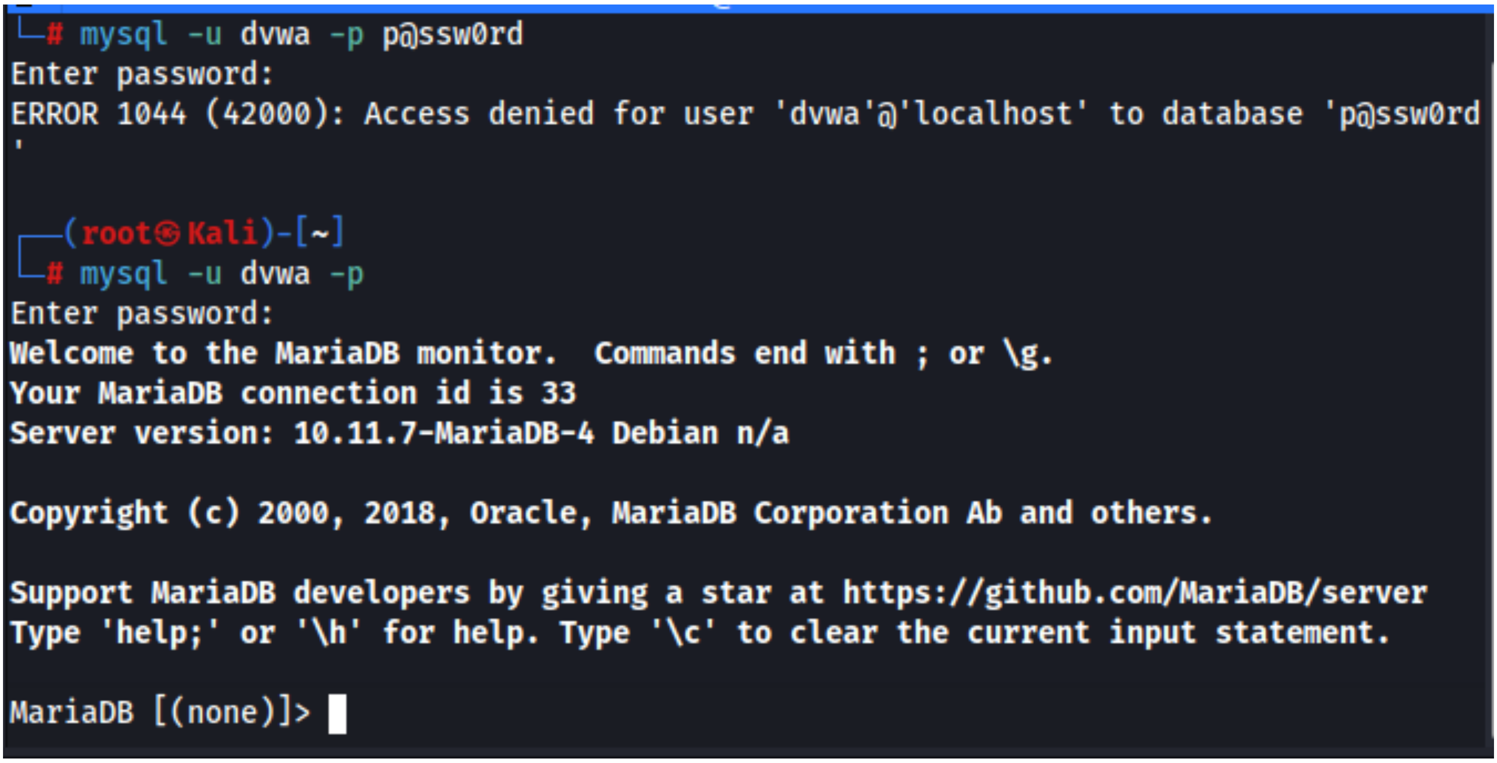
# Now on our terminal we will create and configure a new database just as shown in the image below.



```
┌──(root㉿Kali)-[~]
└─# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.7-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 (0.001 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]>
```

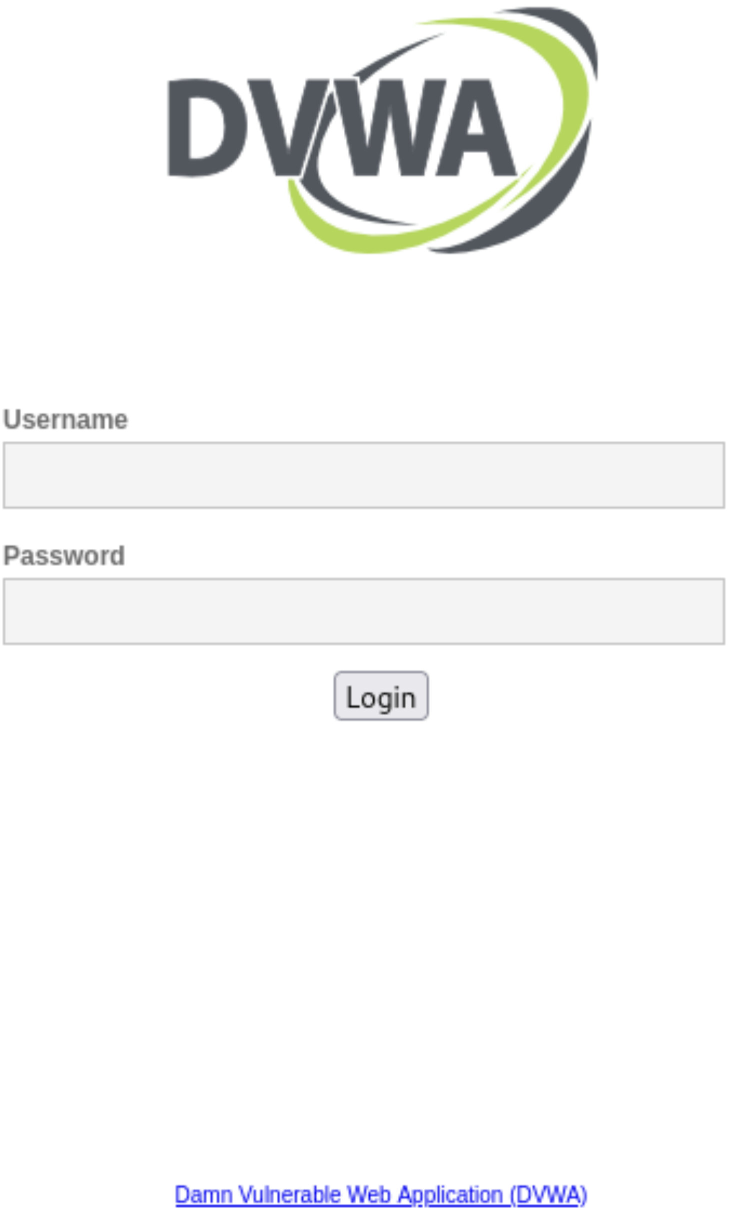
NOTE: We have created a table named "dvwa"
we have created a user "dvwa@localhost"
we have grant all permission to this user as well.

# Now we will login to the mysql to access the dvwa table using the login cred above.

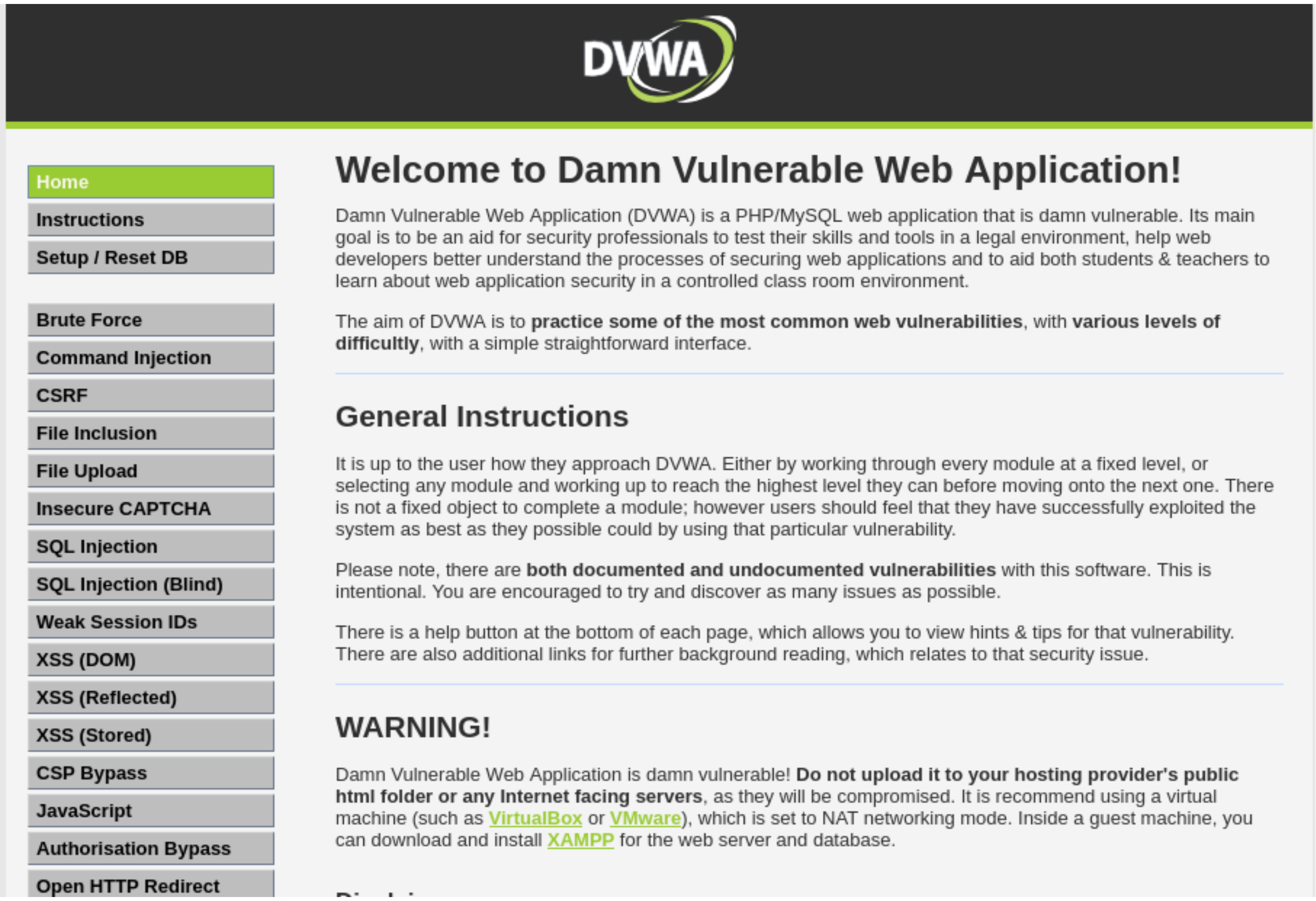


```
└─# mysql -u dvwa -p p@ssw0rd
Enter password:
ERROR 1044 (42000): Access denied for user 'dvwa'@'localhost' to database 'p@ssw0rd
'

┌──(root㉿Kali)-[~]
└─# mysql -u dvwa -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 33
Server version: 10.11.7-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)]> █
```

We will login as admin:password



#BOOM!!! we are in.



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficultly**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

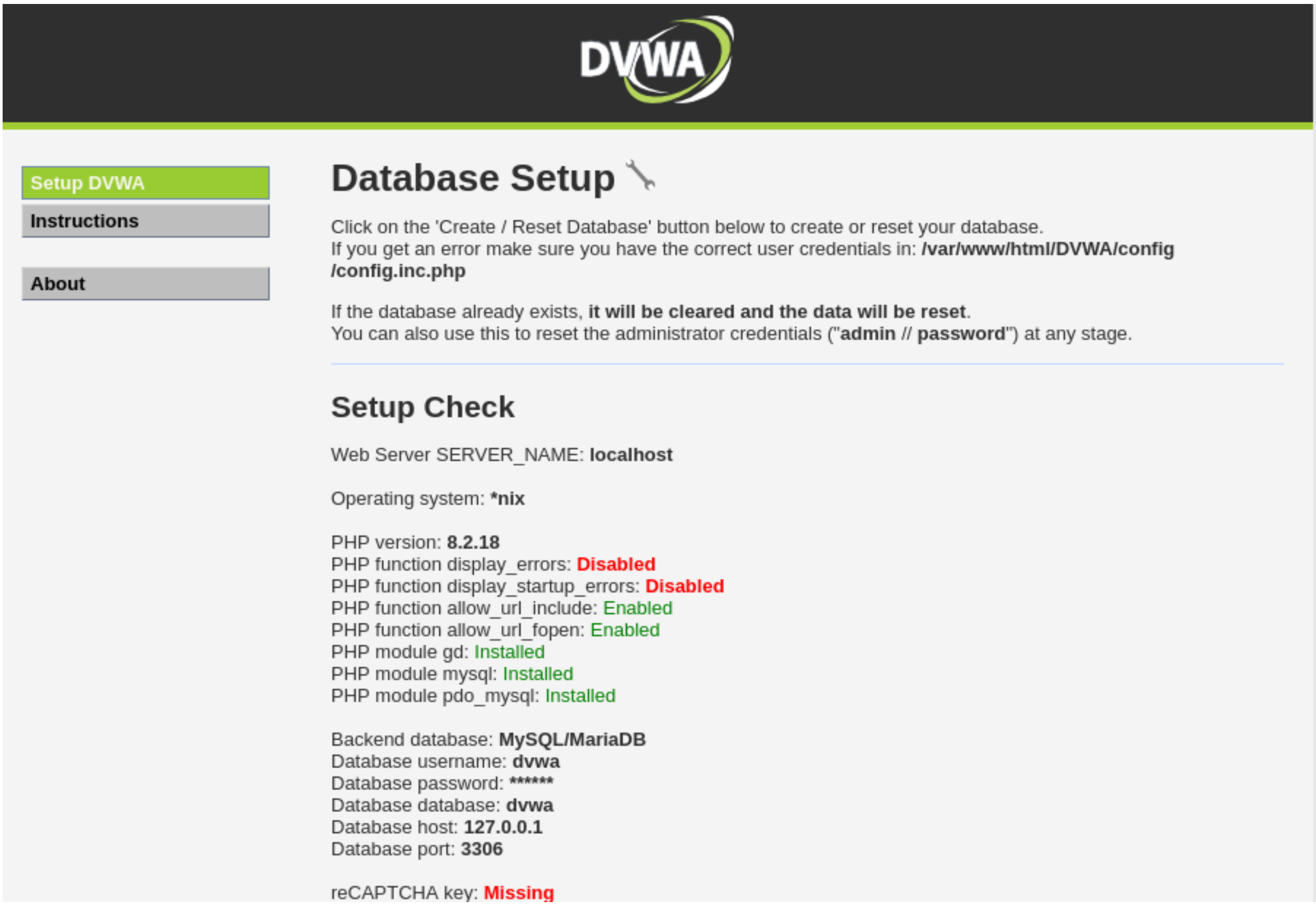
Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

# After setting up DVWA this is how the setup page will look like.



Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **/var/www/html/DVWA/config/config.inc.php**

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Web Server SERVER_NAME: **localhost**

Operating system: ***nix**

PHP version: **8.2.18**
PHP function display_errors: **Disabled**
PHP function display_startup_errors: **Disabled**
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: **MySQL/MariaDB**
Database username: **dvwa**
Database password: **********
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3306**

reCAPTCHA key: **Missing**

# Set DVWA security to low so pen tests can be performed at a difficulty of easy or they can be changed to medium and high after according to user prefrence.

Set up is finished!! Below the homepage of DVWA can be seen where various labs are provided for the practice of exploitation of different types of web vulnerabilities which can be accessed through the menu bar on the left.

WISH YOU ALL THE BEST AS YOU BEGIN THIS JOURNEY!!!