Tutorial No. 4

Title: Installation of DVWA

K. J. SOMAIYA COLLEGE OF ENGG.

Roll No.: 16010423076 **Tutorial No.:4**

Aim: Installation of DVWA

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

Theory:

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. The main goal of this pen testing playground is to aid pen testers and security professionals to test their skills and tools. In addition, it can aid web devs better understand how to secure web apps, but also aid students/teachers to learn all about web app security and possible vulnerabilities

DVWA offers multiple levels

- Low
- Medium
- High
- Impossible

Pen Tester or security professional can freely choose the one that they want

It also shows multiple forms of attack that we can launch like Brute Force, Command Injection, CSRF, etc

Now, let's look at the installation process.

Installation Process

```
┌──(kali㉿kali)-[~]
└─$ cd /var/www/html

┌──(kali㉿kali)-[/var/www/html]
└─$ sudo apt-get update
```

//This is just a way to check that we are all up to date

//Though it hadn’t worked properly :P (Explained well, later)

┌──(kali㉿kali)-[/var/www/html]

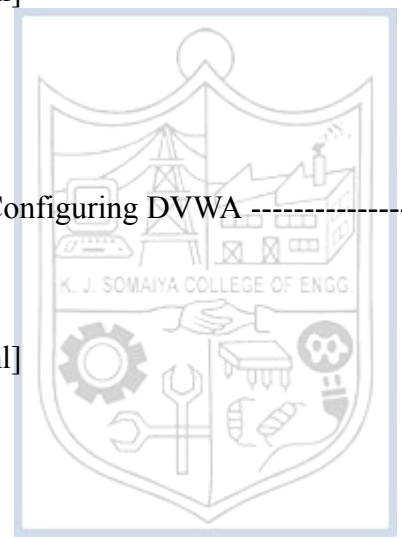
└─$ sudo git clone https://github.com/digininja/DVWA

fatal: destination path 'DVWA' already exists and is not an empty directory.

┌──(kali㉿kali)-[/var/www/html]

└─$ sudo mv DVWA dvwa

----------Configuring DVWA ----------



┌──(kali㉿kali)-[/var/www/html]

└─$ sudo chmod -R 777 dvwa/

┌──(kali㉿kali)-[/var/www/html]

└─$ cd dvwa/DVWA/config

┌──(kali㉿kali)-[/var/…/html/dvwa/DVWA/config]

└─$ sudo cp config.inc.php.dist config.inc.php

//Here, we created a copy of the file as a backup in case we mess up somewhere in the code later on.

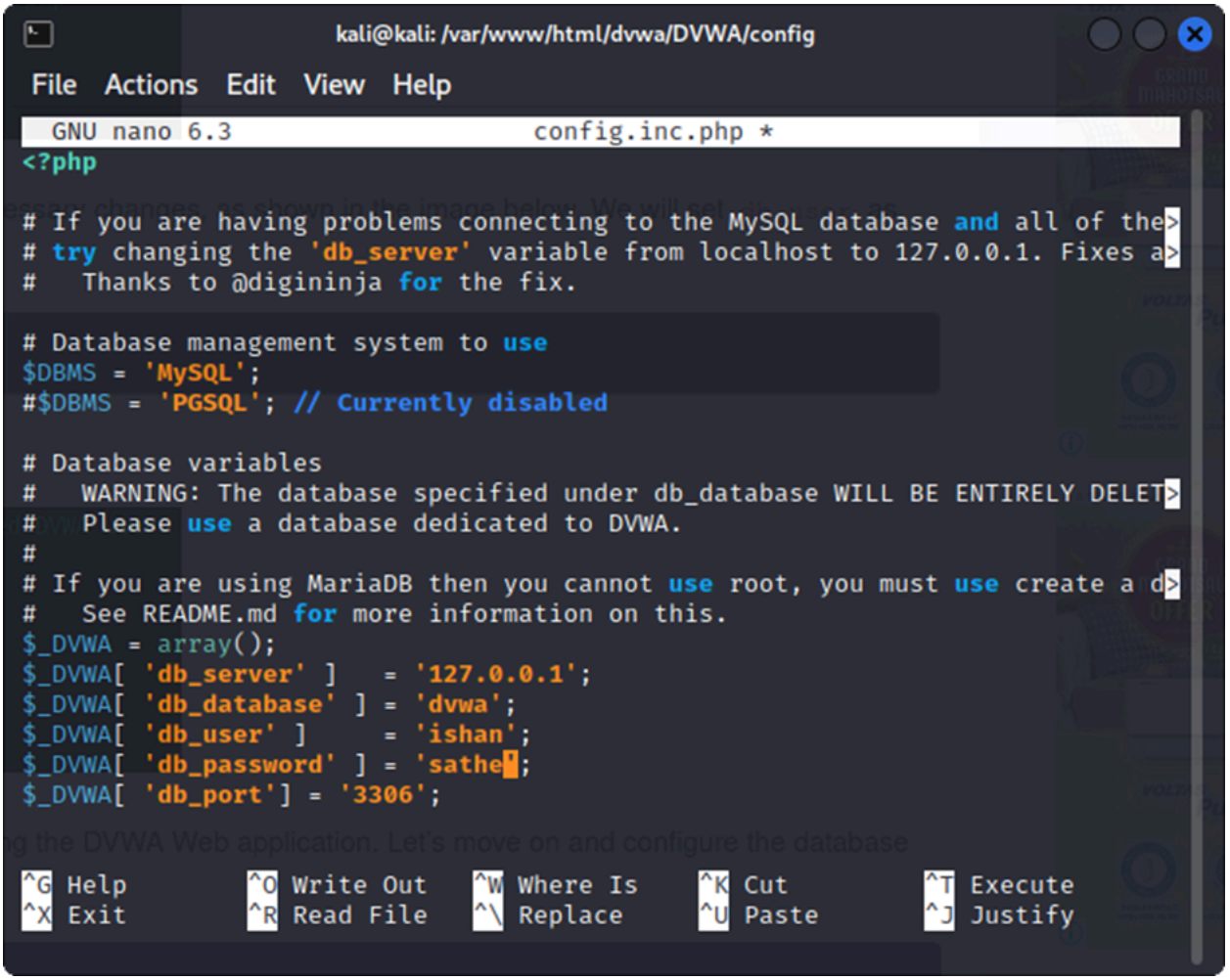
┌──(kali㉿kali)-[/var/…/html/dvwa/DVWA/config]

└─$ sudo nano config.inc.php

//We then changed the db_user and db_password to 'ishan' and 'sathe' respectively.

//then Ctrl+O and enter to save the file

//Ctrl+X to exit.



----------Installing MySQL on Kali Linux----------

//Now, according to the site I was following. It said that it is normal for Kali Linux OS to have mysql-client and mysql-server pre-installed.

//However, if in a case it is not, we use following command

┌──(kali㉿kali)-[/var/…/html/dvwa/DVWA/config]

└─$ sudo apt install default-mysql-server

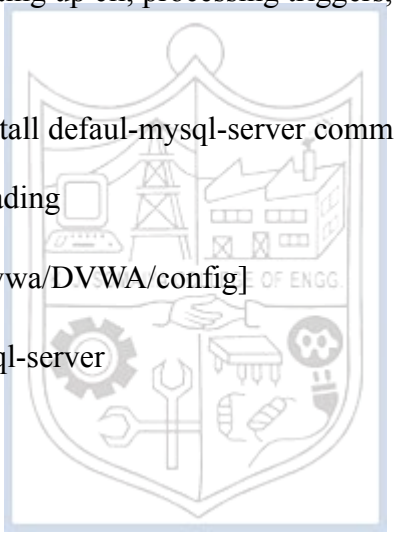
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem.

┌──(kali㉿kali)-[/var/…/html/dvwa/DVWA/config]

└─$ sudo dpkg --configure -a

//Running the above commands seems to have installed php7.3-common and all its related packages. It took some time to complete the process.

//Mostly creating config giles, setting up cli, processing triggers, etc



//I have now again entered the install defaul-mysql-server command

//It seems to have started downloading

┌──(kali㉿kali)-[/var/…/html/dvwa/DVWA/config]

└─$ sudo apt install default-mysql-server

Reading package lists... Done

Building dependency tree... Done

Reading state information... Done

default-mysql-server is already the newest version (1.0.8).

0 upgraded, 0 newly installed, 0 to remove and 1050 not upgraded.

//So far so good

----------Configuring MySQL----------

┌──(kali㉿kali)-[/var/…/html/dvwa/DVWA/config]

└─$ sudo service mysql start

//Below is the status of mysql service, it is very large so I won't be showing all of its output

//But key fact being that it is loaded and running.

```
┌──(kali㉿kali)-[/var/…/html/dvwa/DVWA/config]
└─$ systemctl status mysql
● mariadb.service - MariaDB 10.6.8 database server
     Loaded: loaded (/lib/systemd/system/mariadb.service; disabled; vendor p>
     Active: active (running) since Mon 2022-10-17 06:40:36 EDT; 47s ago
```

//We now login to MySQL database. For this we need certainty form user, that's why they asked for password

```
┌──(kali㉿kali)-[/var/…/html/dvwa/DVWA/config]
└─$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.6.8-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)]> create user 'ishan'@'127.0.0.1' identified by 'sathe';
Query OK, 0 rows affected (0.046 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'ishan'@'127.0.0.1' identified by 'sathe';
Query OK, 0 rows affected (0.635 sec)
```

MariaDB [(none)]> exit

Bye

//TBH I think the commands used here are pretty straightforward so I won't be explaining them

----------Install PHP----------

PHP comes installed in Kali Linux. However, if you want to install a particular version, you can do it manually from the Terminal. In this post, we will install PHP 7.4 which is the latest release as of writing this post. Follow the steps below.

First, update your system and add the SURY PHP PPA repository by executing the commands below.

sudo apt update command is not working

It says that the ppa repository does not have a release file and hence cannot be doing anything

Run the following commands

[Note: Other than 'sudo apt update' all other commands are working properly.

Even so, failure of apt update has not caused any problems so far]

sudo apt update

sudo apt -y install lsb-release apt-transport-https ca-certificates

sudo wget -O /etc/apt/trusted.gpg.d/php.gpg https://packages.sury.org/php/apt.gpg

echo "deb https://packages.sury.org/php/ buster main" | sudo tee /etc/apt/sources.list.d/php.list

sudo apt install php7.4 -y

//Now the above command does not work and says set up has broken packages.

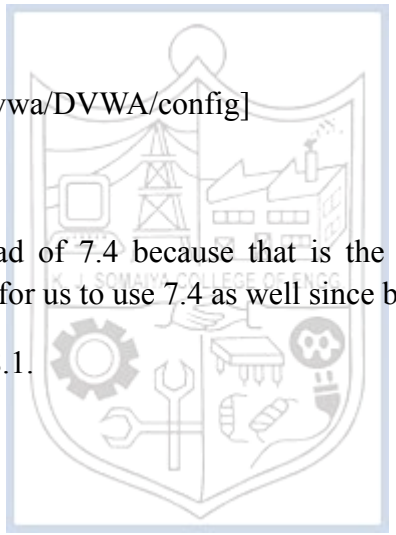
//Now to improvise, download the latest php version and it has been successful

Run this command

sudo apt install php -y

Congratulations! we have now finally become successful in installing PHP

----------Configuring Apache Server----------



┌──(kali㉿kali)-[/var/…/html/dvwa/DVWA/config]

└─$ cd /etc/php/8.1/apache2

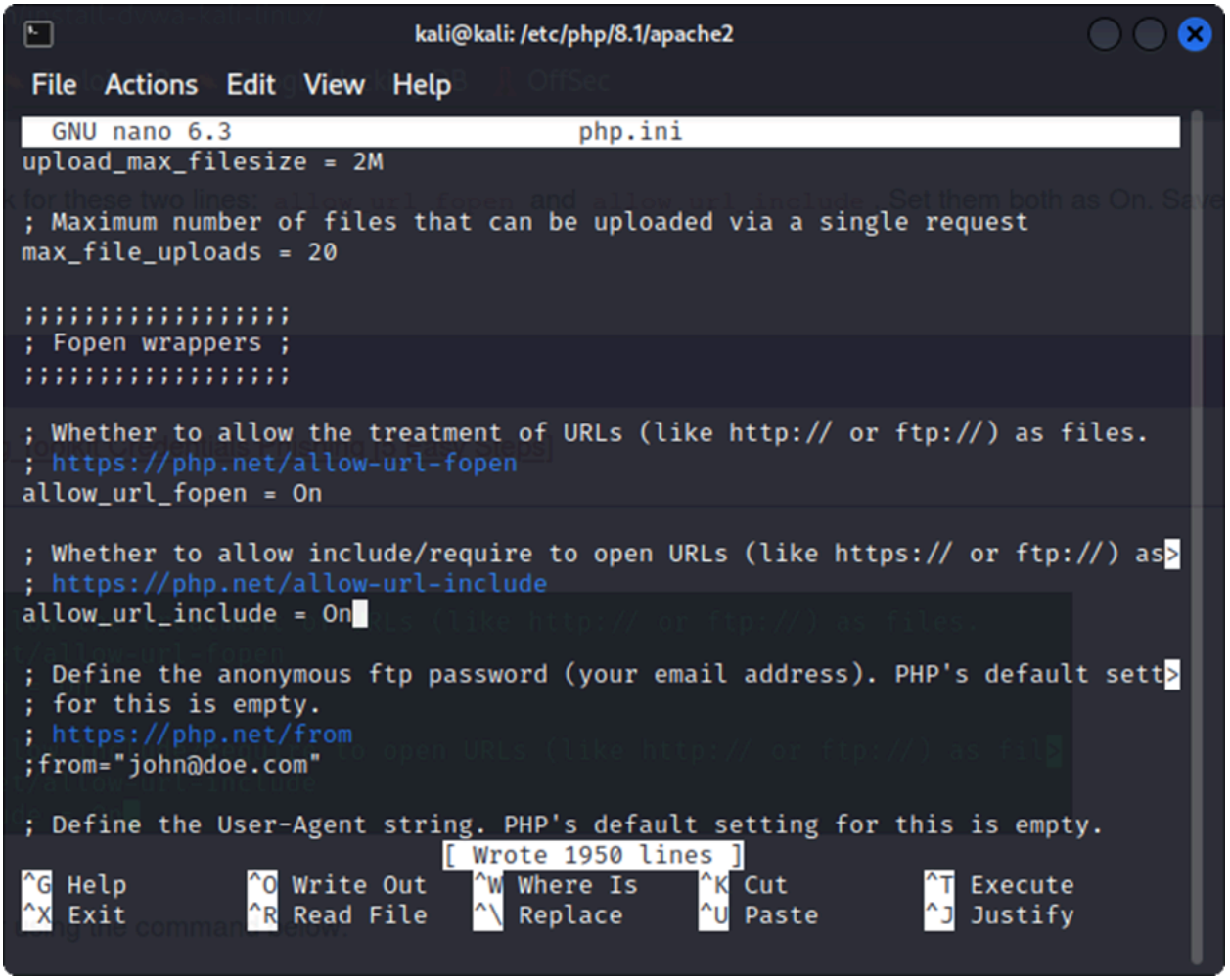
//Here, we have used 8.1 instead of 7.4 because that is the php version (latest) that we installed. Though it was possible for us to use 7.4 as well since both of them got installed

//Still, we will move ahead with 8.1.

//Because we are badasses.

┌──(kali㉿kali)-[/etc/php/8.1/apache2]

└─$ sudo nano php.ini



//The file opened by this is very large

//in order to search for the place where we want to make changes we enter

// Ctrl+W and then enter the text that we want (may have to press enter again?)

//Once at the place, we make the necessary changes

//P.S You have to set both allow_url_fopen and allow_url_include to 'on'

┌──(kali㉿kali)-[/etc/php/8.1/apache2]

└─$ sudo service apache2 start

┌──(kali㉿kali)-[/etc/php/8.1/apache2]

└─$ systemctl status apache2

● apache2.service - The Apache HTTP Server

Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor p>

Active: active (running) since Mon 2022-10-17 07:17:17 EDT; 15s ago

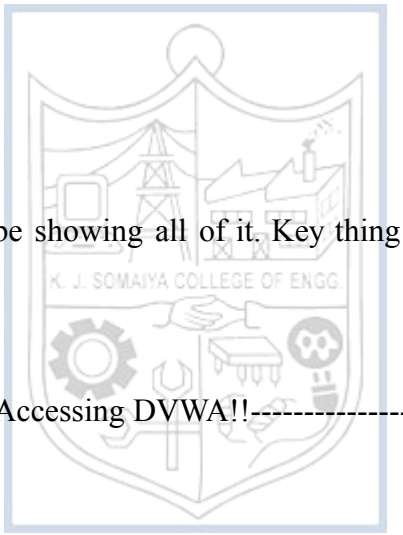
Docs: https://httpd.apache.org/docs/2.4/

Process: 26511 ExecStart=/usr/sbin/apachectl start (code=exited, status=>

Main PID: 26515 (apache2)

Tasks: 6 (limit: 2293)

//Again, large output and won't be showing all of it. Key thing to notice is that apache 2 is loaded and active (running)



----------Accessing DVWA!!----------

That's all! We now have everything configured and can proceed to launch DVWA.

Open your browser and enter the URL

http://127.0.0.1/dvwa/DVWA/setup.php

//That's the URL for existing set up

//For you it can be different

//Just note that even in that, you have to be in 'setup.php' file

//and not 'login.php' file. That's where I was earlier and nothing would load.

Don't panic over the error/etc in red

Scroll down and click 'Create/Reset Database' button

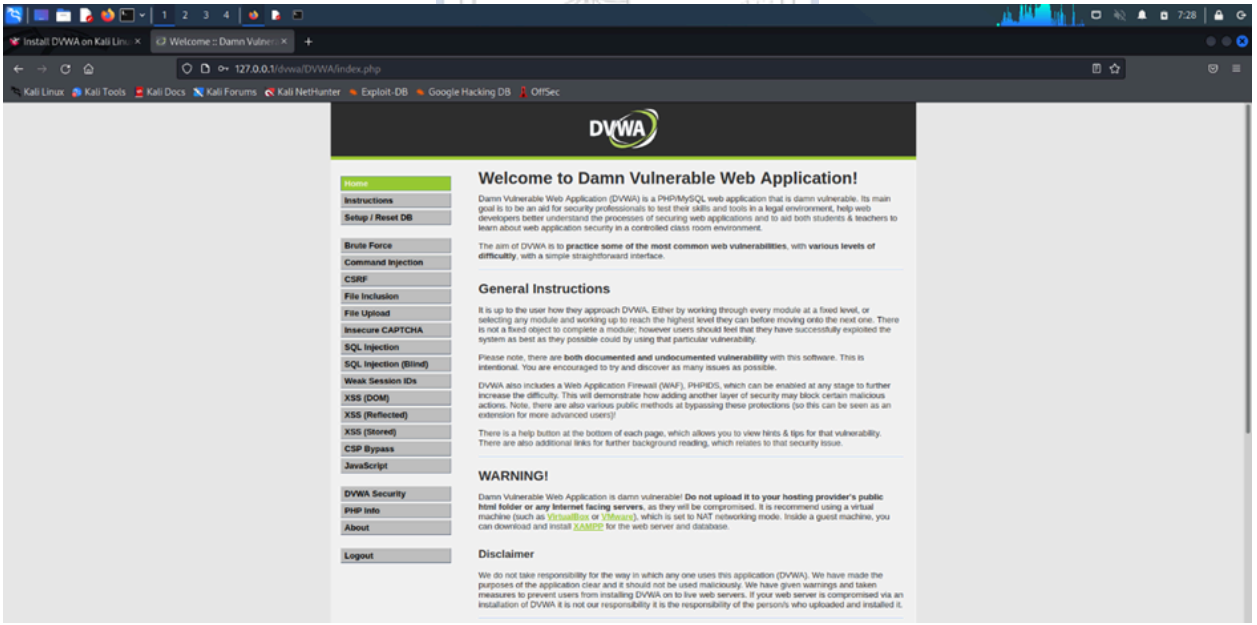
This will create and configure the database. After some time you will be redirected to the DVWA login page

There, enter the following credentials

Username - admin

Password - password

Once logged in. you will see the DVWA main page. On the left panel, we have different types of attacks you can exploit and the DVWA security button that allows you to choose the desired security level!

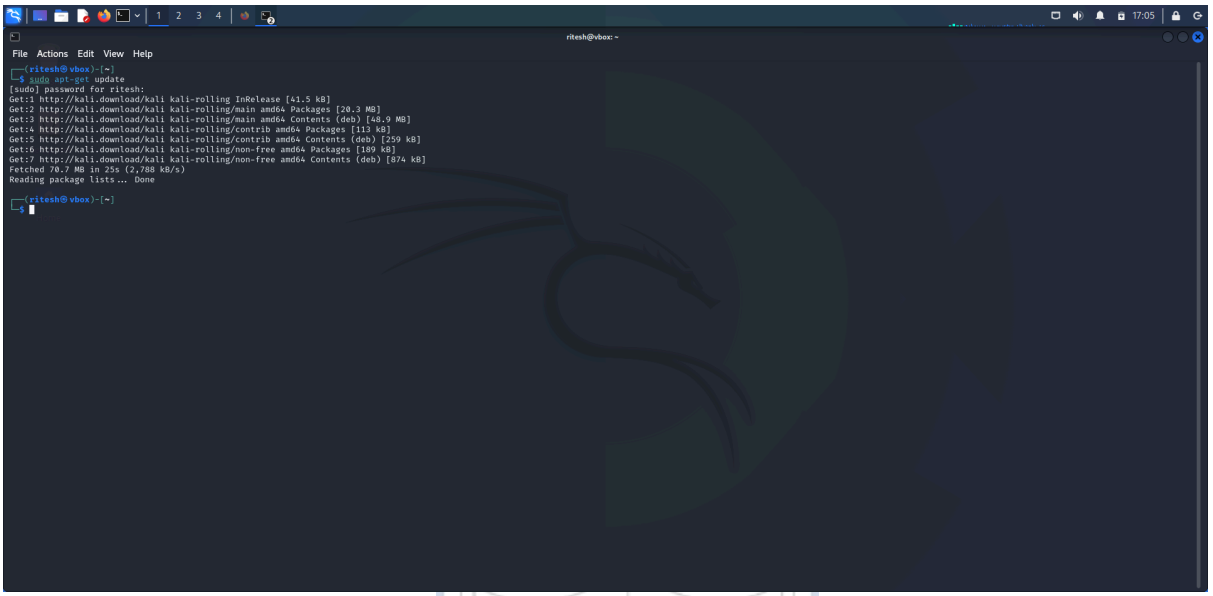


That's it!

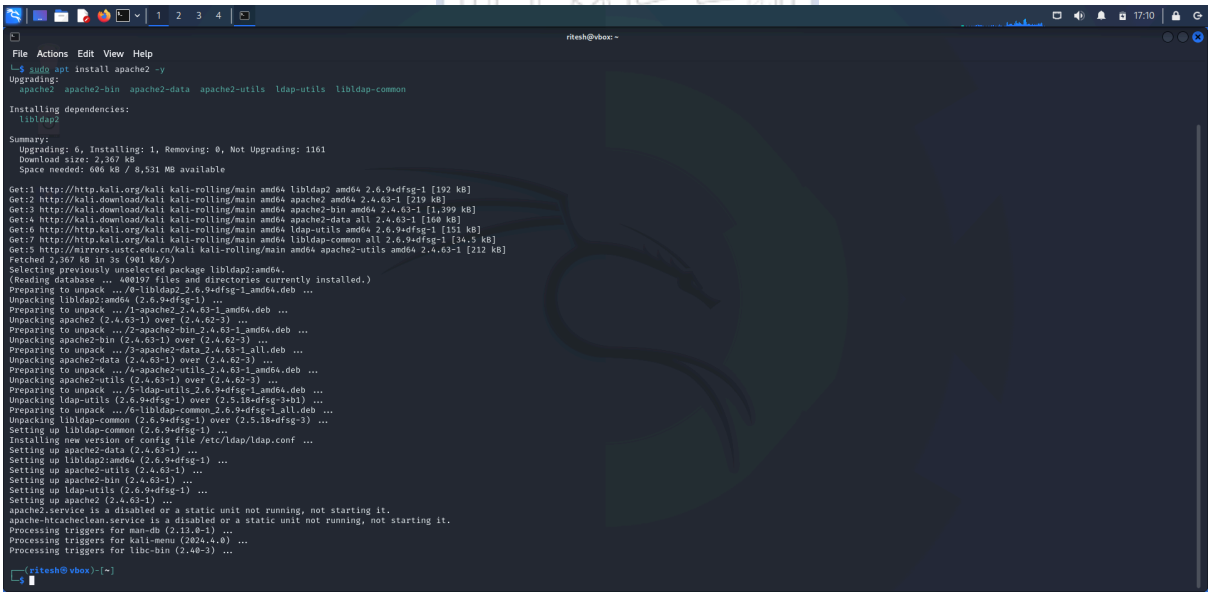
We are done installing DVWA

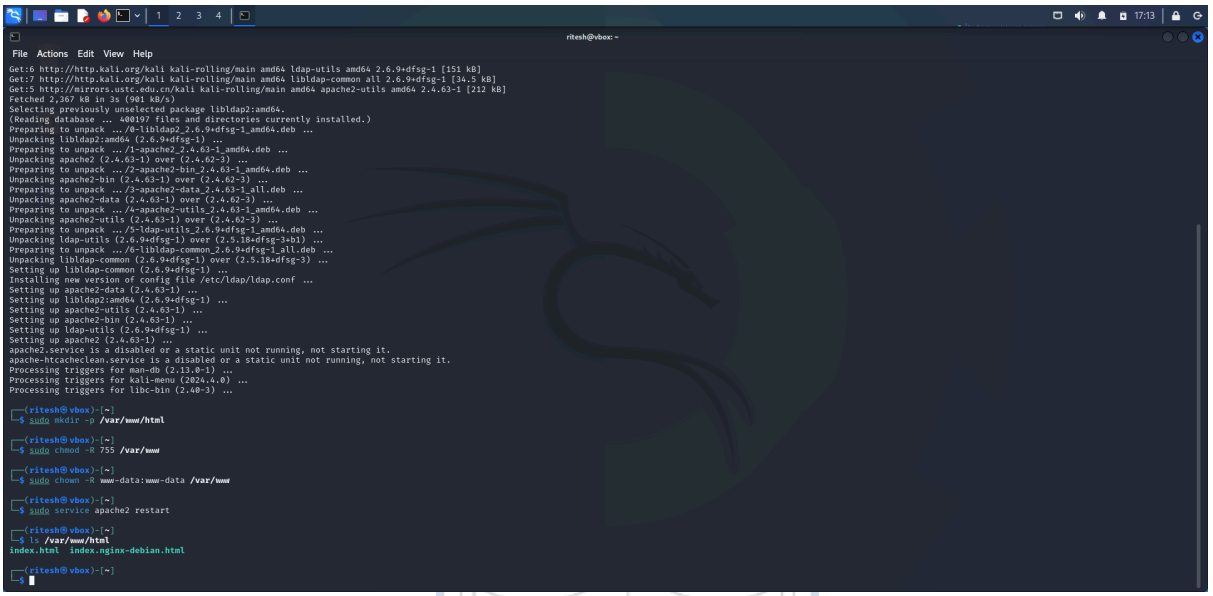
Implementation :

1. Update System and Install Dependencies

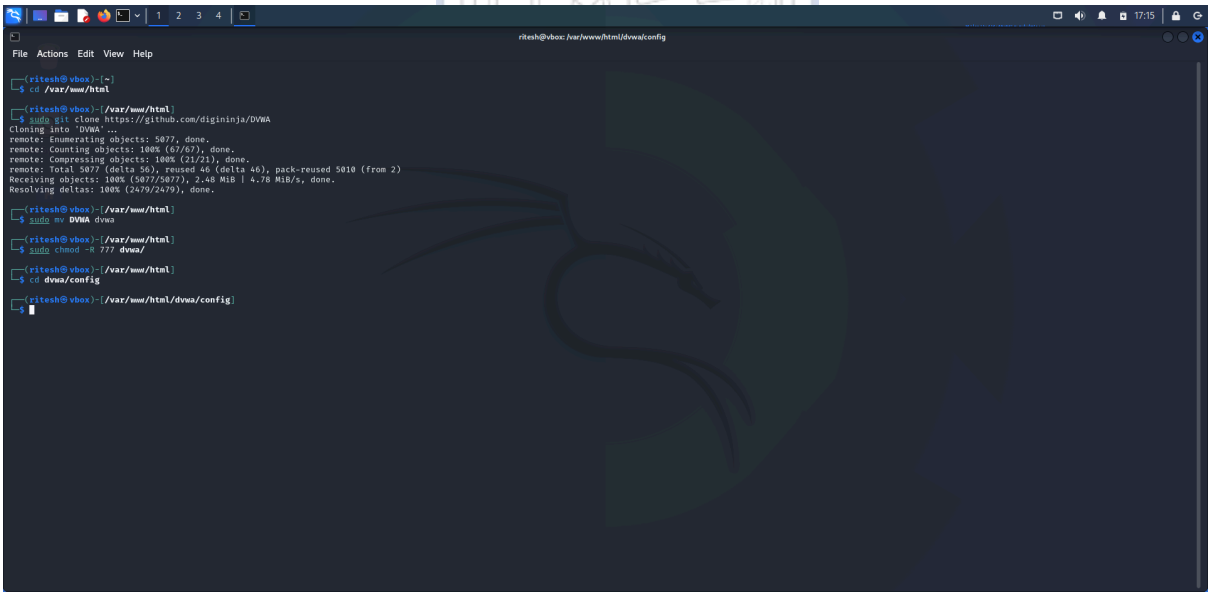


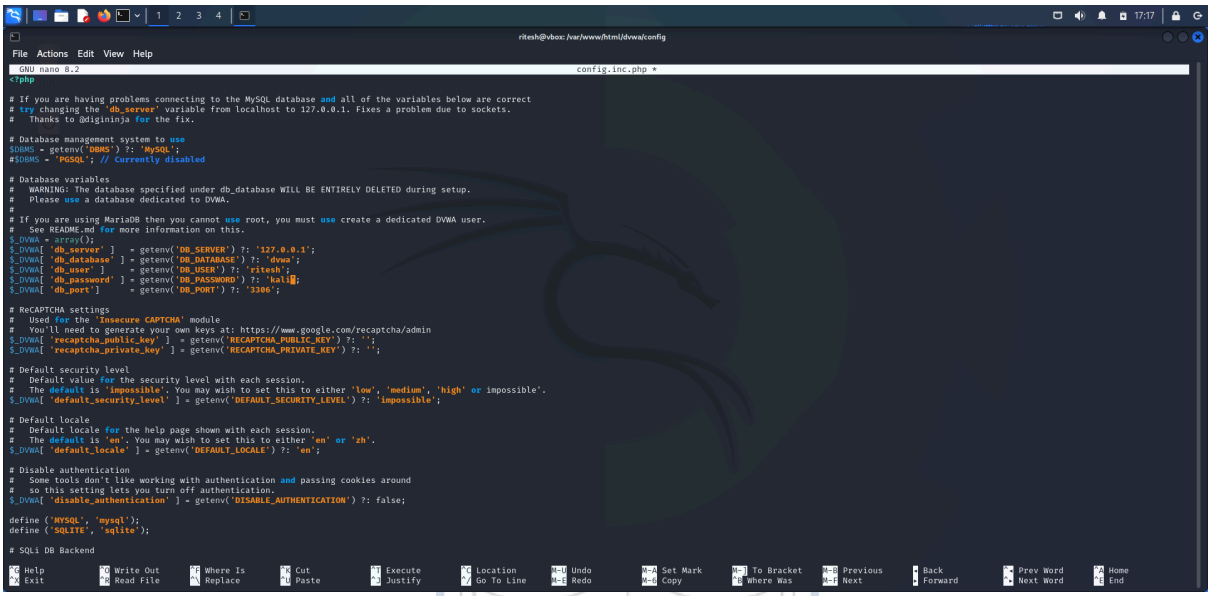
2. Download DVWA

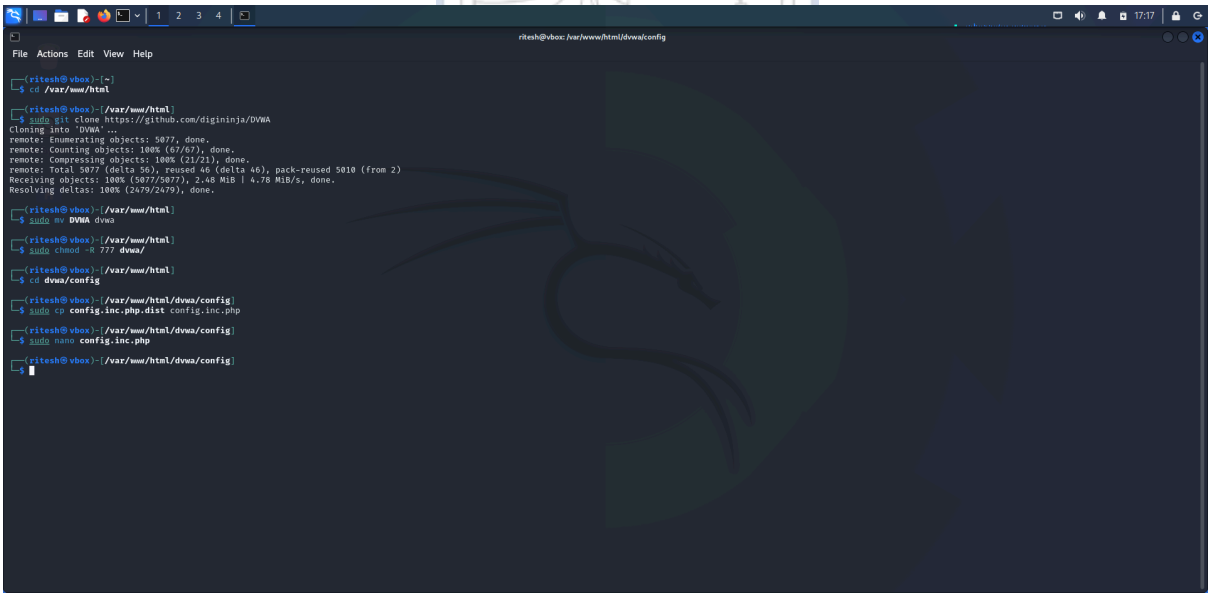




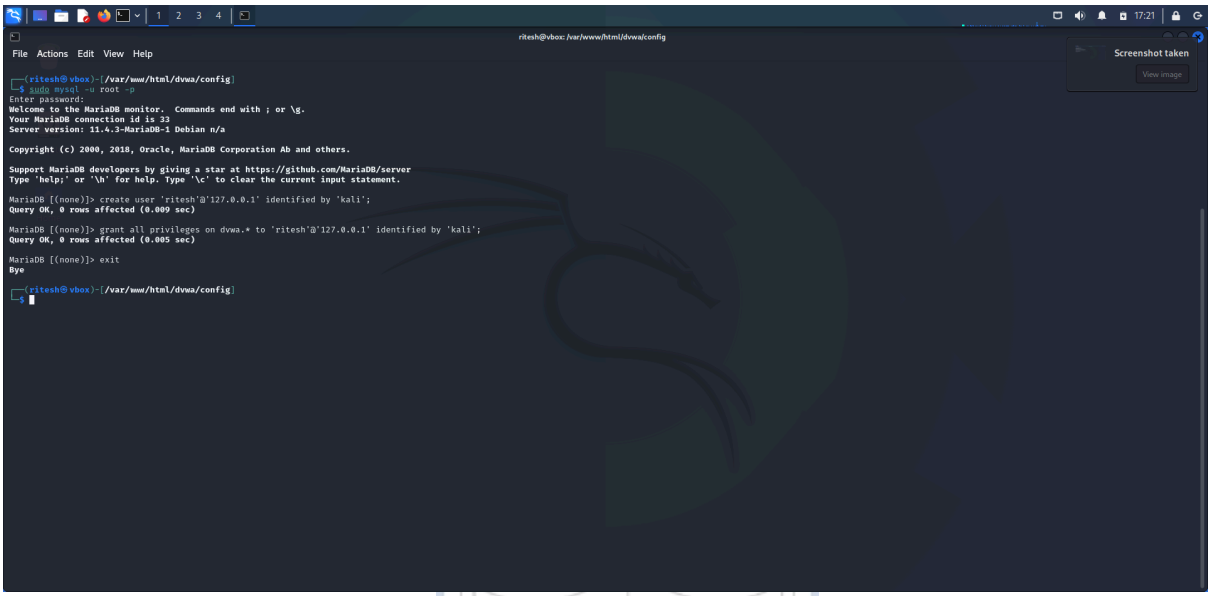
3. Configure DVWA

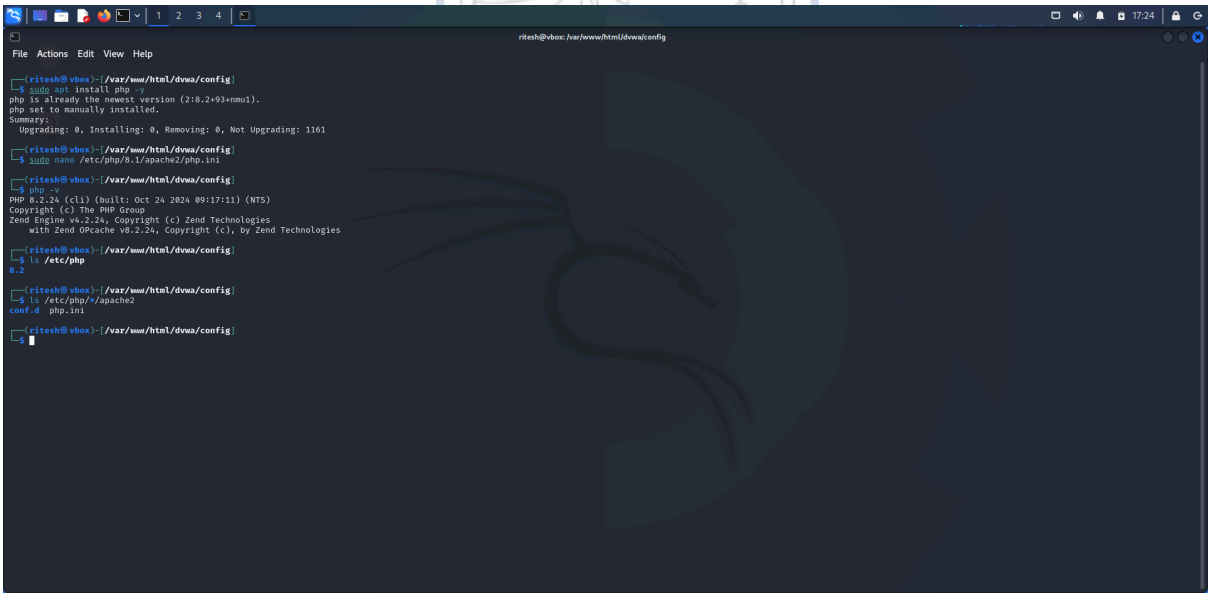




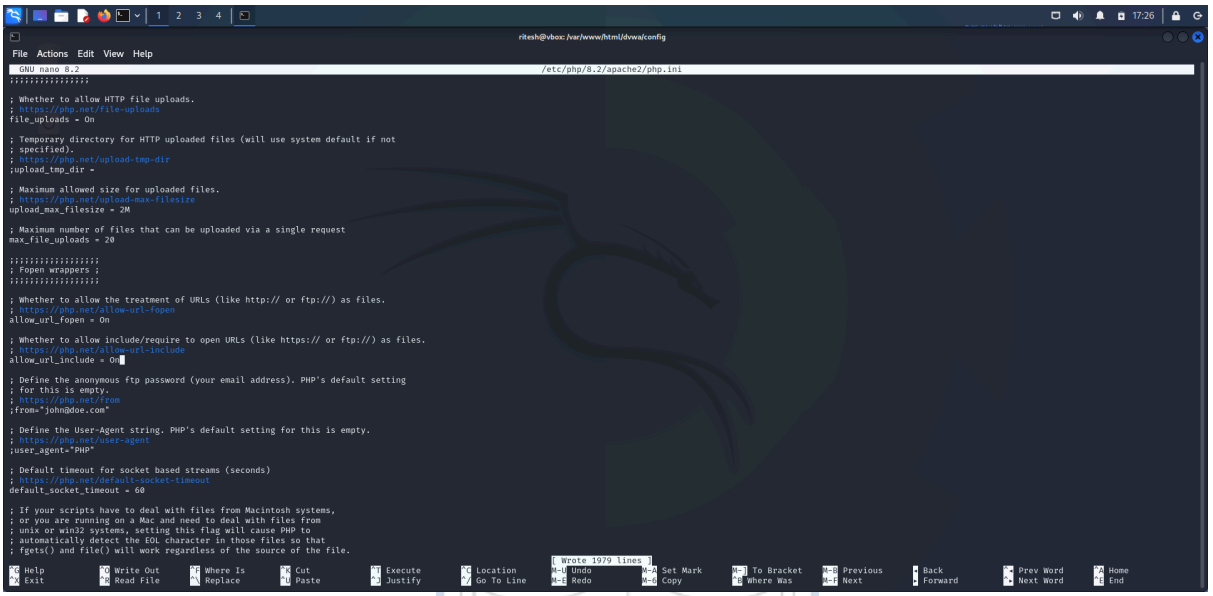


4. Install and Configure MySQL



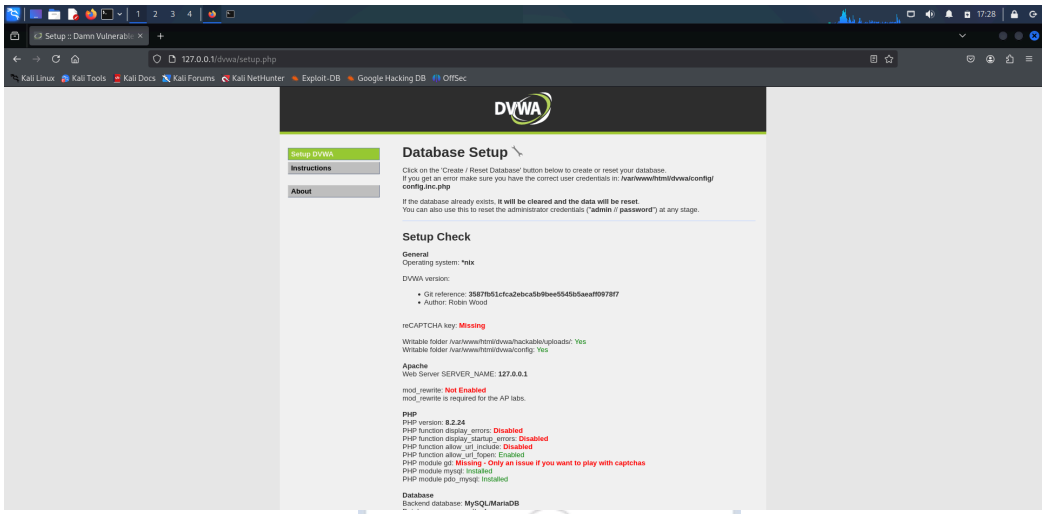


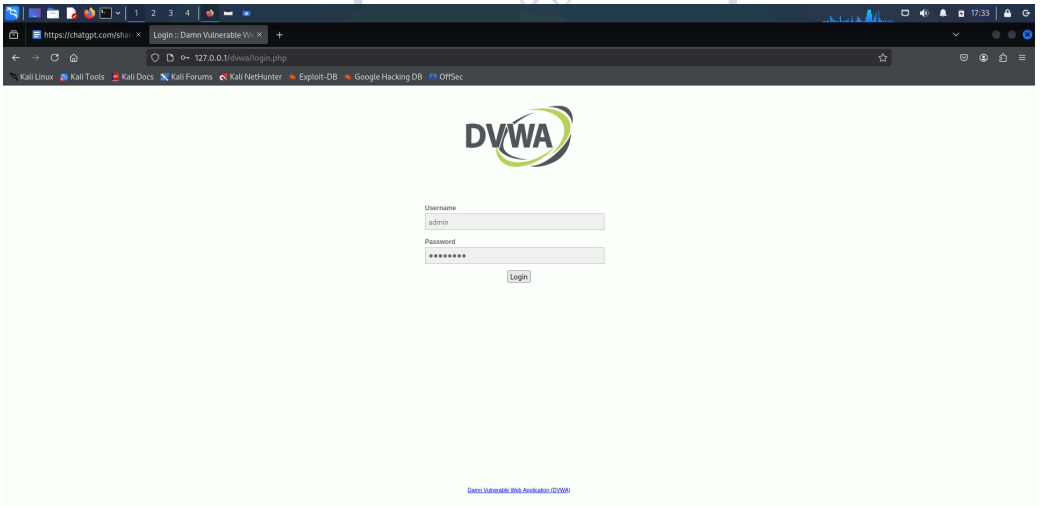
5. Install PHP

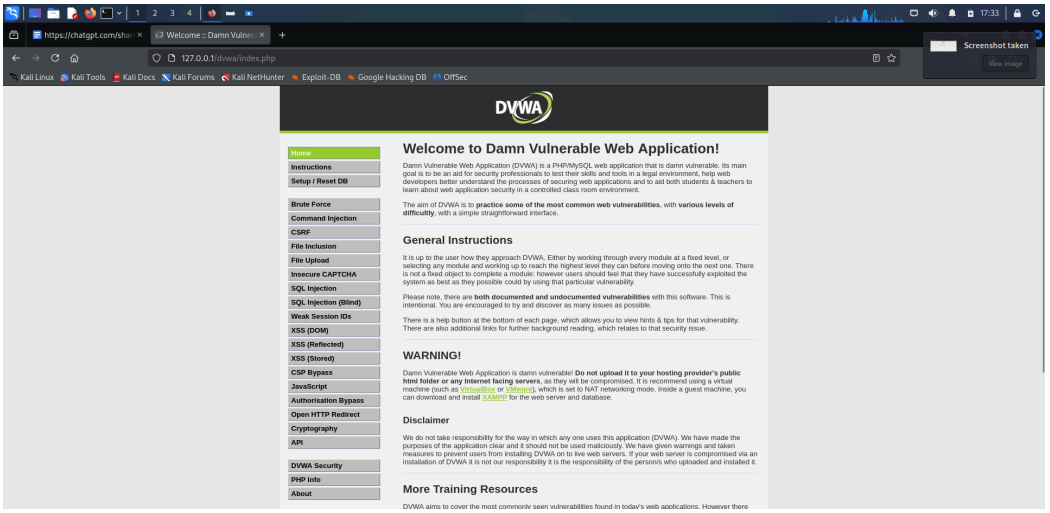


6. Configure Apache Server

7. Access DVWA in Browser


Setup :: Damn Vulnerable
127.0.0.1/dvwa/setup.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Setup DVWA
Instructions
About
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
General
Operating system: *nix
DVWA version:
Git reference: 3587fb51cfca2ebca5b9bee5545b5aeaff0978f7
Author: Robin Wood
reCAPTCHA key: Missing
Writable folder /var/www/html/dvwa/hackable/uploads/: Yes
Writable folder /var/www/html/dvwa/config: Yes
Apache
Web Server SERVER_NAME: 127.0.0.1
mod_rewrite: Not Enabled
mod_rewrite is required for the AP labs.
PHP
PHP version: 8.2.24
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: Missing - Only an issue if you want to play with captchas
PHP module mysql: Installed
PHP module pdo_mysql: Installed
Database
Backend database: MySQL/MariaDB


https://chatgpt.com/sha
Login :: Damn Vulnerable
127.0.0.1/dvwa/login.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Username
admin
Password
Login
Damn Vulnerable Web Application (DVWA)


https://chatgpt.com/sha
Welcome :: Damn Vulner
127.0.0.1/dvwa/index.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Screenshot taken
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
API
DVWA Security
PHP Info
About
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.
Disclaimer
We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.
More Training Resources
DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there

---

Outcome :

CO1: Realize the premise of vulnerability analysis and penetration testing (VAPT).

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

From this tutorial, I learned how to install and configure DVWA on Kali Linux by setting up MySQL, PHP, and Apache, adjusting necessary configurations, and ensuring the web application runs properly. The process involved cloning the DVWA repository, modifying configuration files, installing dependencies, and troubleshooting errors like package issues and service failures.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

https://owasp.org/www-community/

https://github.com/digininja/DVWA

https://dvwa.co.uk

https://www.apachefriends.org/download.html