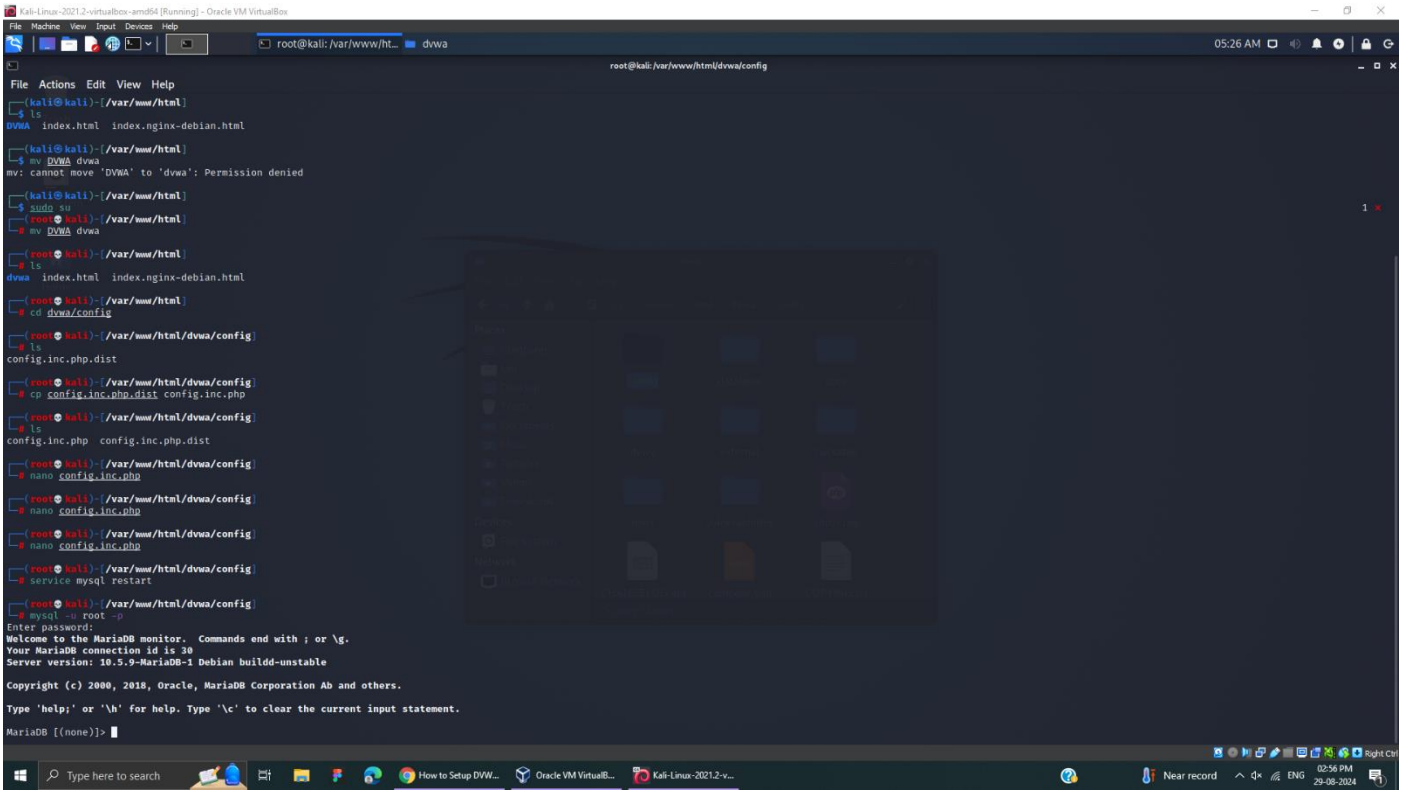
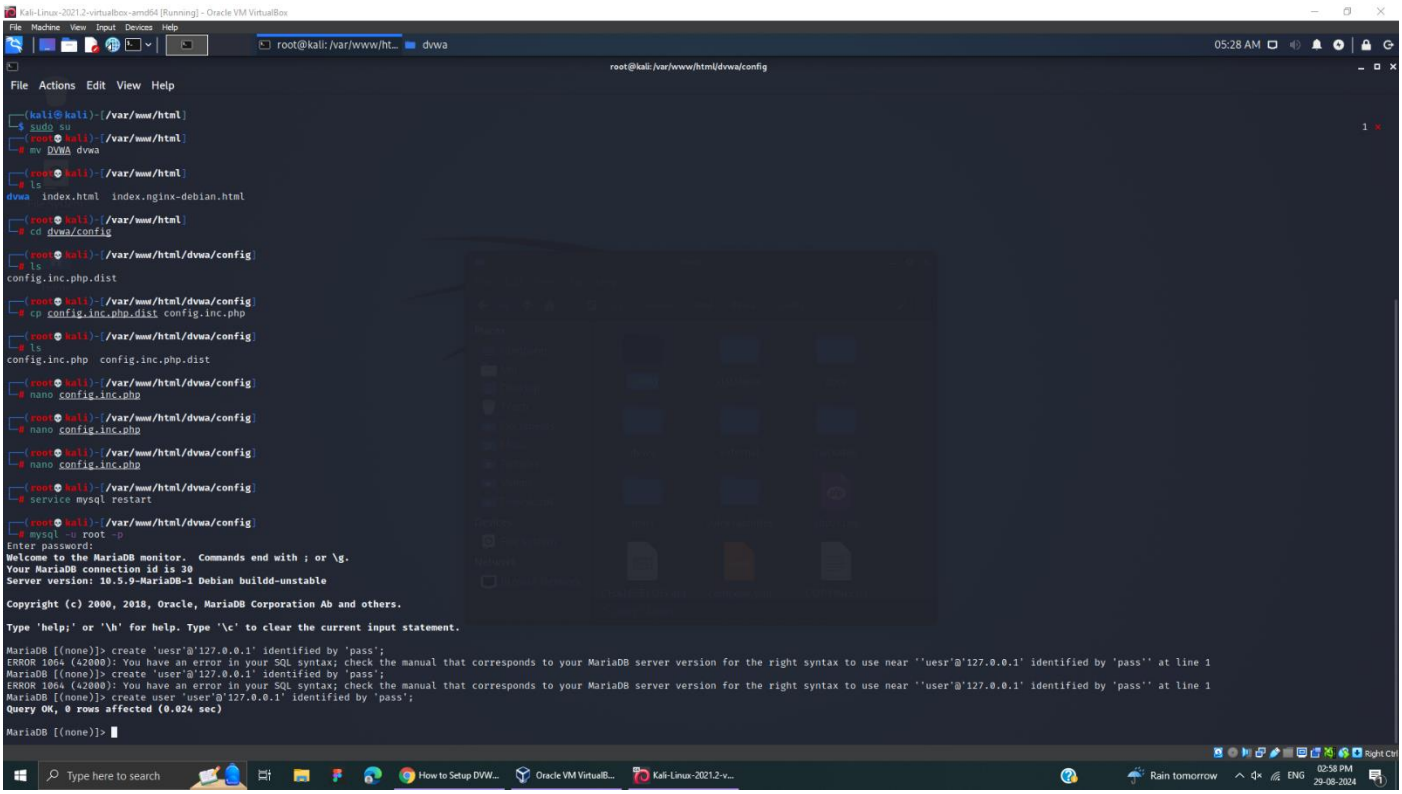
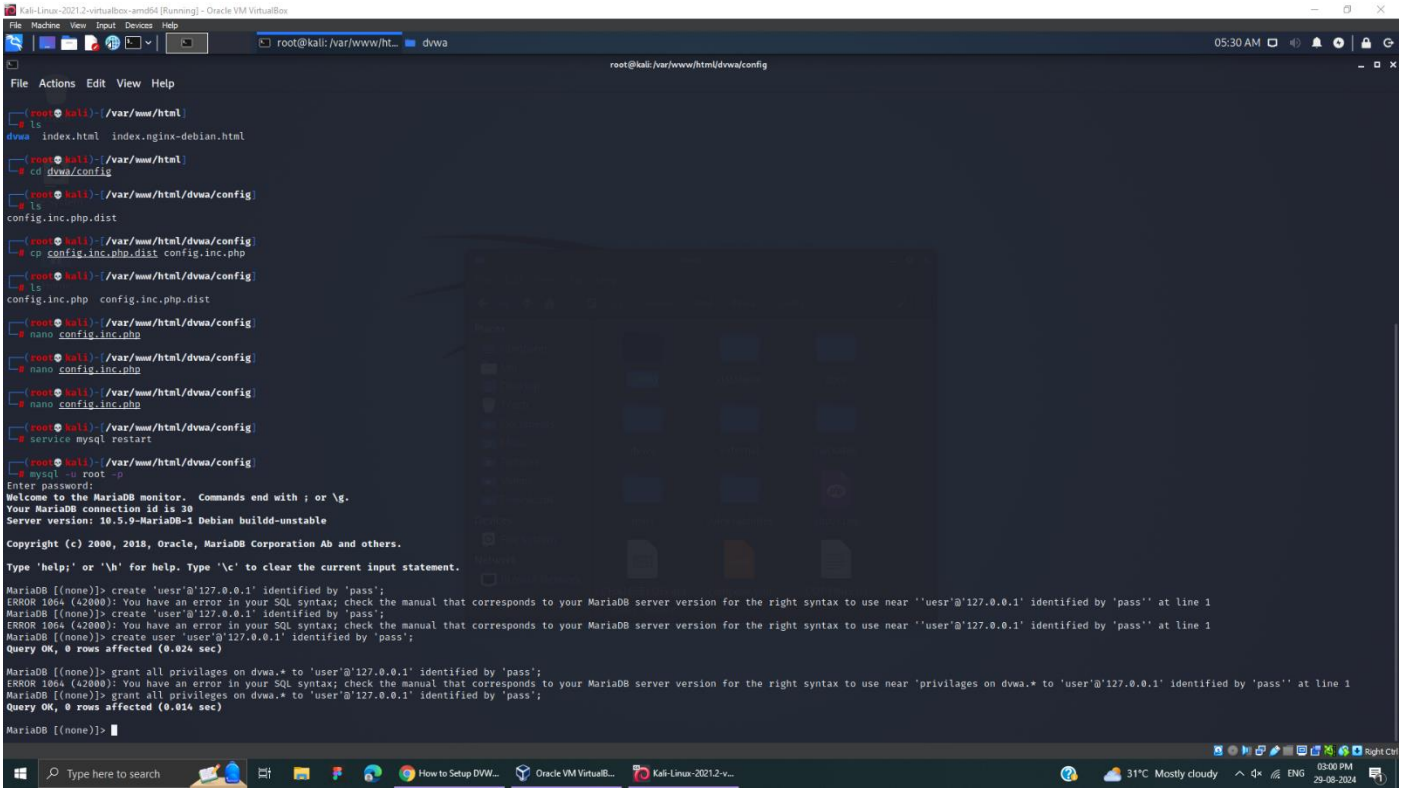
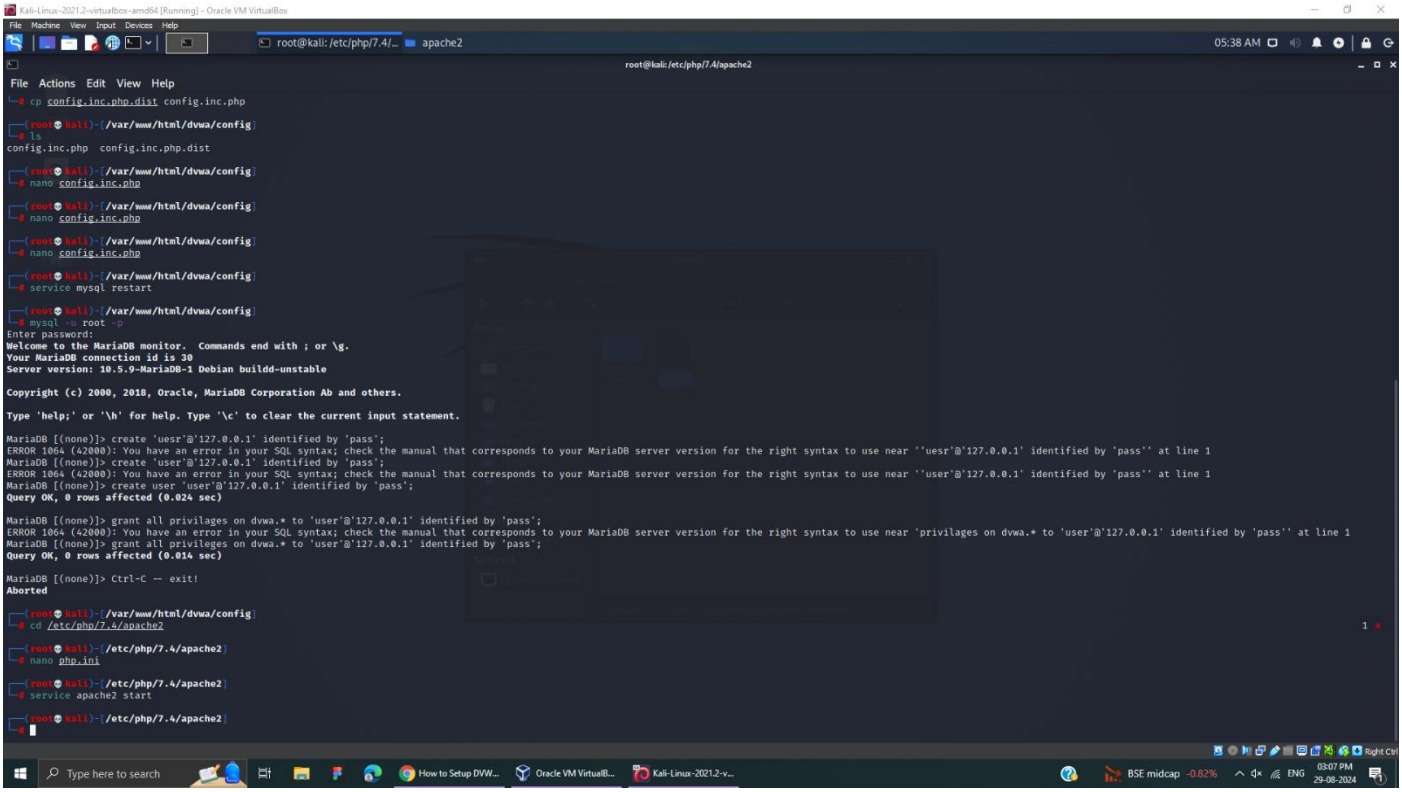
Practical 5

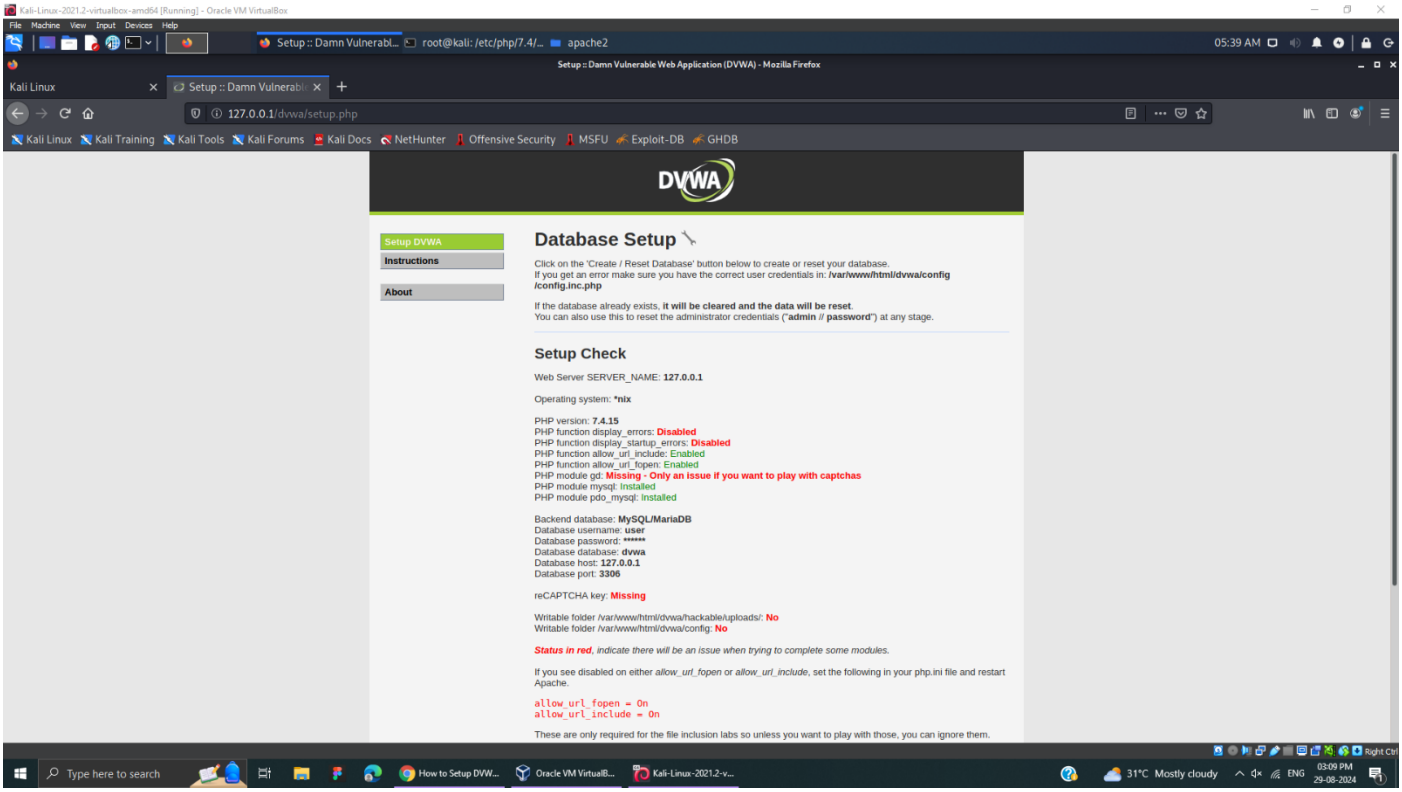
Implement SQL Injection and XSS using DVWA in Kali Linux

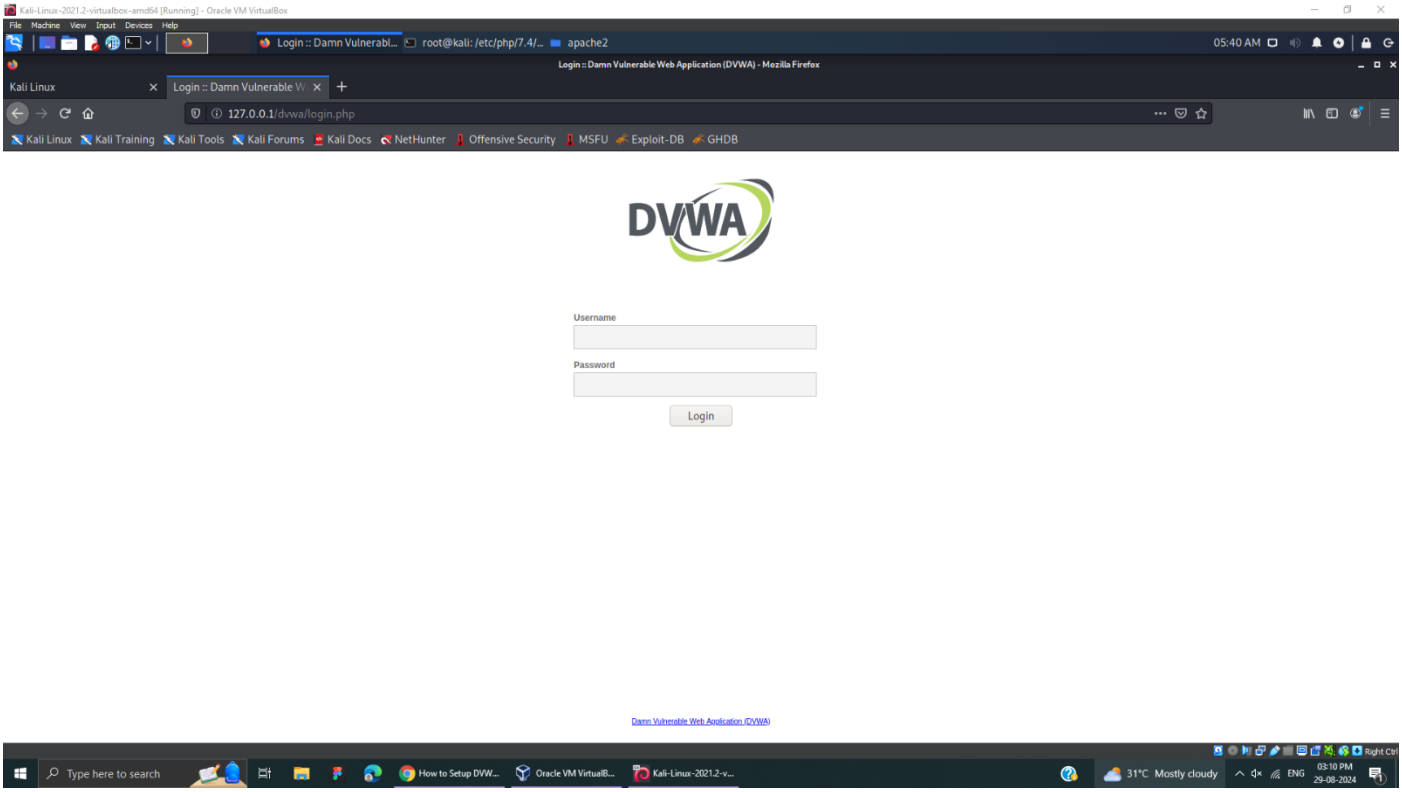


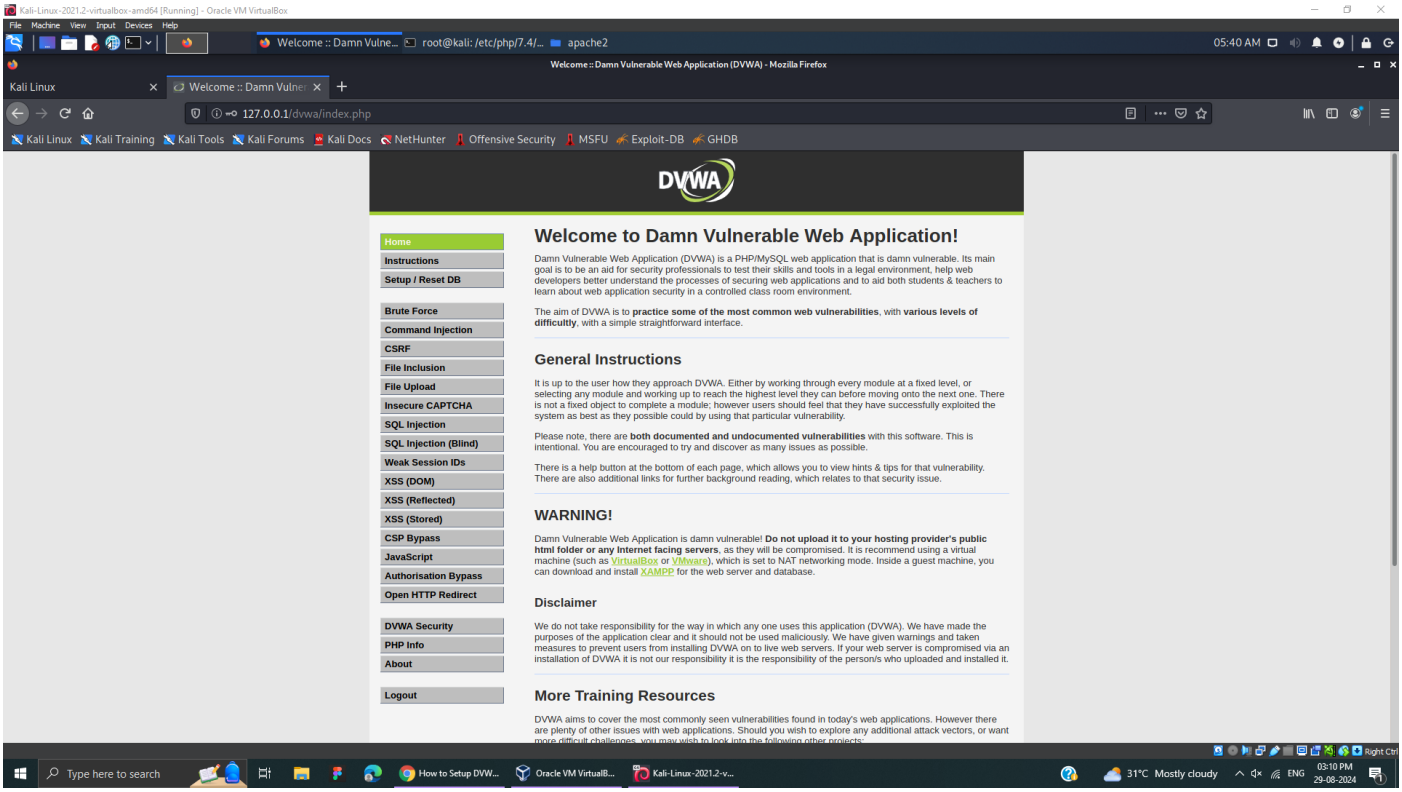



Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
root@kali: /var/www/ht... dvwa
05:30 AM
root@kali: /var/www/html/dvwa/config
File Actions Edit View Help
┌──(root㉿kali)-[/var/www/html]
└─# ls
dvwa index.html index.nginx-debian.html
┌──(root㉿kali)-[/var/www/html]
└─# cd dvwa/config
┌──(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]
└─# nano config.inc.php
┌──(root㉿kali)-[/var/www/html/dvwa/config]
└─# nano config.inc.php
┌──(root㉿kali)-[/var/www/html/dvwa/config]
└─# nano config.inc.php
┌──(root㉿kali)-[/var/www/html/dvwa/config]
└─# service mysql restart
┌──(root㉿kali)-[/var/www/html/dvwa/config]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 30
Server version: 10.5.9-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 'uesr'@'127.0.0.1' identified by 'pass';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''uesr'@'127.0.0.1' identified by 'pass'' at line 1
MariaDB [(none)]> create 'user'@'127.0.0.1' identified by 'pass';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''user'@'127.0.0.1' identified by 'pass'' at line 1
MariaDB [(none)]> create user 'user'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.024 sec)
MariaDB [(none)]> grant all privilages on dvwa.* to 'user'@'127.0.0.1' identified by 'pass';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'privilages on dvwa.* to 'user'@'127.0.0.1' identified by 'pass'' at line 1
MariaDB [(none)]> grant all privileges on dvwa.* to 'user'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.014 sec)
MariaDB [(none)]>
Type here to search
How to Setup DVW...
Oracle VM VirtualB...
Kali-Linux-2021.2-v...
31°C Mostly cloudy
ENG
03:00 PM
29-08-2024


Kali-Linux-2021.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
root@kali: /etc/php/7.4/... apache2
05:38 AM
root@kali: /etc/php/7.4/apache2
File Actions Edit View Help
└─# 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]
└─# nano config.inc.php
┌──(root㉿kali)-[/var/www/html/dvwa/config]
└─# nano config.inc.php
┌──(root㉿kali)-[/var/www/html/dvwa/config]
└─# nano config.inc.php
┌──(root㉿kali)-[/var/www/html/dvwa/config]
└─# service mysql restart
┌──(root㉿kali)-[/var/www/html/dvwa/config]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 30
Server version: 10.5.9-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 'uesr'@'127.0.0.1' identified by 'pass';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''uesr'@'127.0.0.1' identified by 'pass'' at line 1
MariaDB [(none)]> create 'user'@'127.0.0.1' identified by 'pass';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''user'@'127.0.0.1' identified by 'pass'' at line 1
MariaDB [(none)]> create user 'user'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.024 sec)
MariaDB [(none)]> grant all privilages on dvwa.* to 'user'@'127.0.0.1' identified by 'pass';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'privilages on dvwa.* to 'user'@'127.0.0.1' identified by 'pass'' at line 1
MariaDB [(none)]> grant all privileges on dvwa.* to 'user'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.014 sec)
MariaDB [(none)]> Ctrl-C -- exit!
Aborted
┌──(root㉿kali)-[/var/www/html/dvwa/config]
└─# cd /etc/php/7.4/apache2
┌──(root㉿kali)-[/etc/php/7.4/apache2]
└─# nano php.ini
┌──(root㉿kali)-[/etc/php/7.4/apache2]
└─# service apache2 start
┌──(root㉿kali)-[/etc/php/7.4/apache2]
└─#
Type here to search
How to Setup DVW...
Oracle VM VirtualB...
Kali-Linux-2021.2-v...
BSE midcap -0.82%
ENG
03:07 PM
29-08-2024


Setup :: Damn Vulnerable Web Application (DVWA) - Mozilla Firefox
127.0.0.1/dvwa/setup.php
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
Web Server SERVER_NAME: 127.0.0.1
Operating system: *nix
PHP version: 7.4.15
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: Missing - Only an issue if you want to play with captchas
PHP module mysql: Installed
PHP module pdo_mysql: Installed
Backend database: MySQL/MariaDB
Database username: user
Database password: ******
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306
reCAPTCHA key: Missing
Writable folder /var/www/html/dvwa/hackable/uploads/: No
Writable folder /var/www/html/dvwa/config: No
Status in red, indicate there will be an issue when trying to complete some modules.
If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.
allow_url_fopen = On
allow_url_include = On
These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.


Login :: Damn Vulnerable Web Application (DVWA) - Mozilla Firefox
127.0.0.1/dvwa/login.php
DVWA
Username
Password
Login
Damn Vulnerable Web Application (DVWA)


Welcome :: Damn Vulnerable Web Application (DVWA) - Mozilla Firefox
127.0.0.1/dvwa/index.php
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
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
DVWA Security
PHP Info
About
Logout
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 are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want