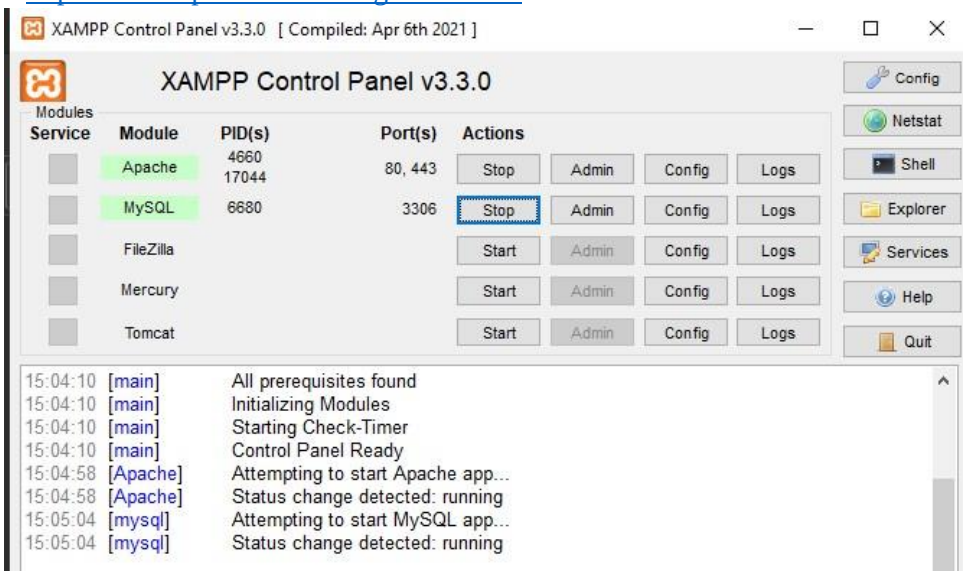
V Module: Penetration Testing using Metasploit and Metasploitable

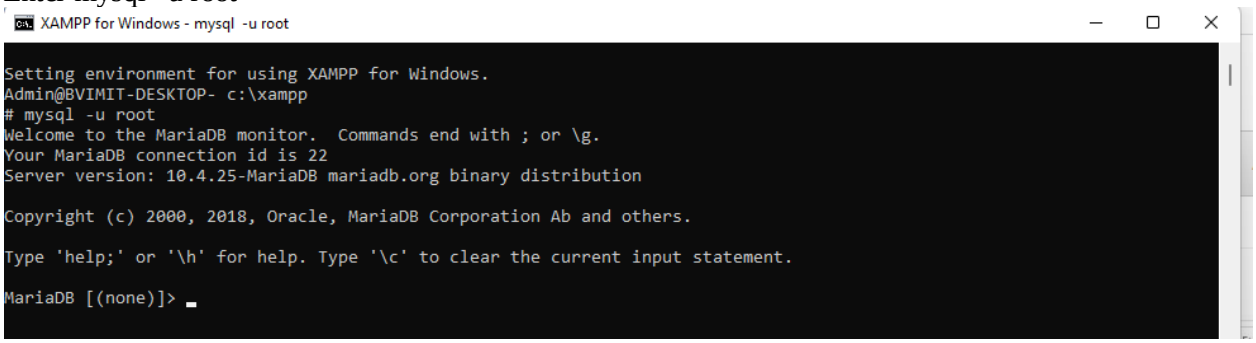
A. Hack a website by Remote File Inclusion

A. Building a Web Hacking Lab (w/ XAMPP and DVWA) :
1. Install XAMPP : XAMPP

- https://www.apachefriends.org/index.html o Create database

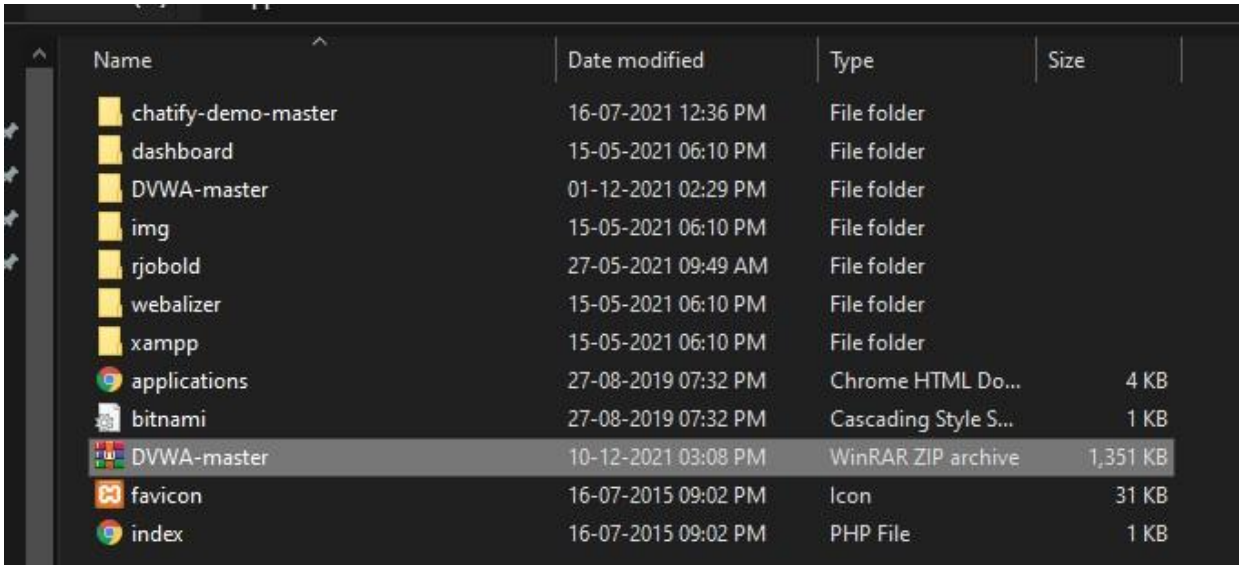


Enter mysql –u root

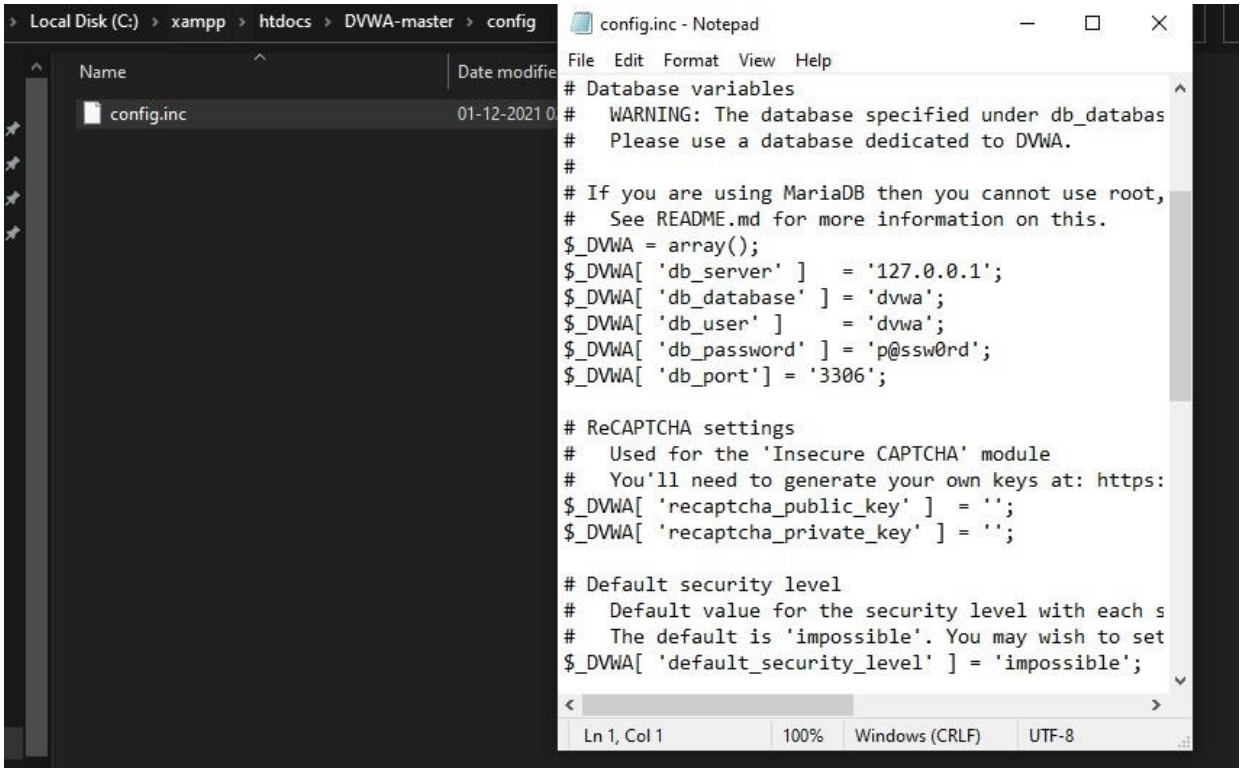


```
XAMPP for Windows - mysql -u root
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| phpmyadmin         |
| test               |
+--------------------+
5 rows in set (0.001 sec)

MariaDB [(none)]> create database mcab24_eh
    -> ;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mcab24_eh          |
| mysql              |
| performance_schema |
| phpmyadmin         |
| test               |
+--------------------+
6 rows in set (0.001 sec)

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> show databases;
ERROR 2006 (HY000): MySQL server has gone away
No connection. Trying to reconnect...
Connection id:    29
Current database: *** NONE ***

+--------------------+
| Database           |
+--------------------+
| dvwa               |
| information_schema |
| mcab24_eh          |
| mysql              |
| performance_schema |
| phpmyadmin         |
| test               |
+--------------------+
7 rows in set (0.004 sec)

MariaDB [(none)]>
```

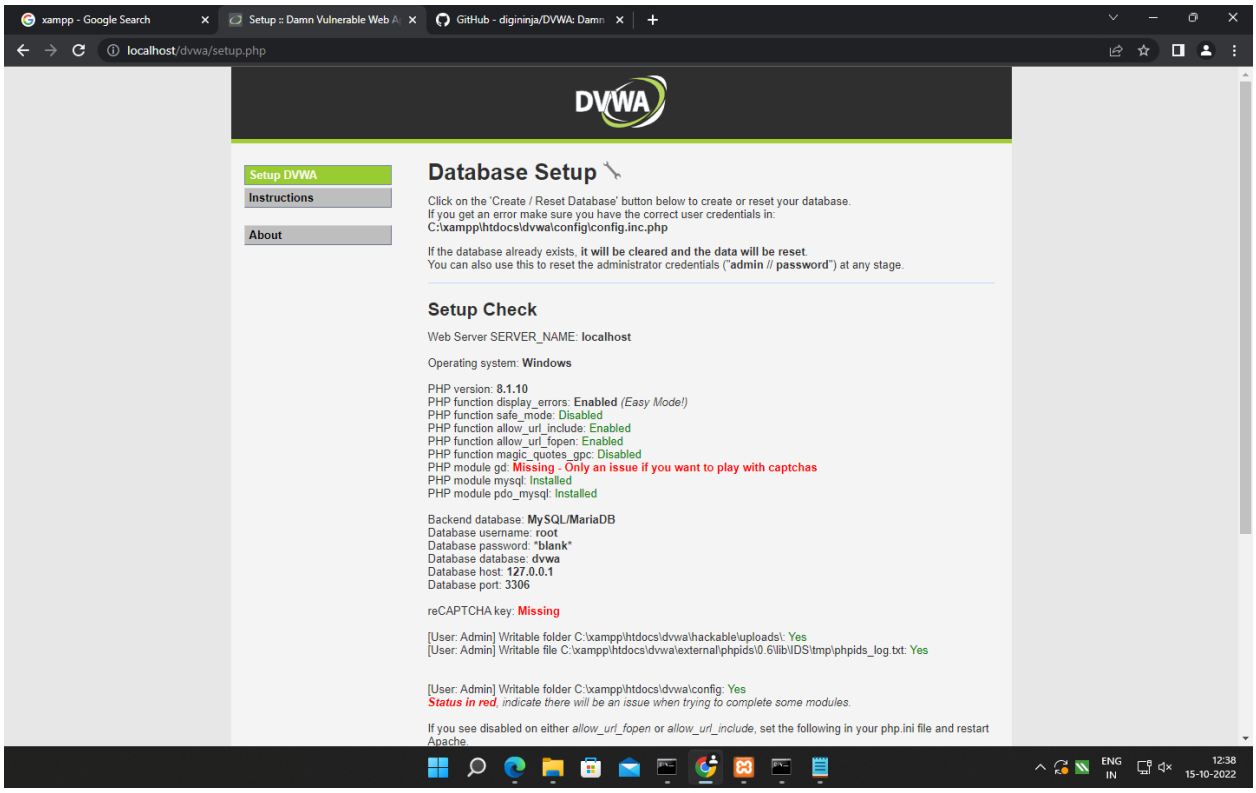
- Download DVWA-master.zip
- Install DVWA in C:\xampp\htdocs

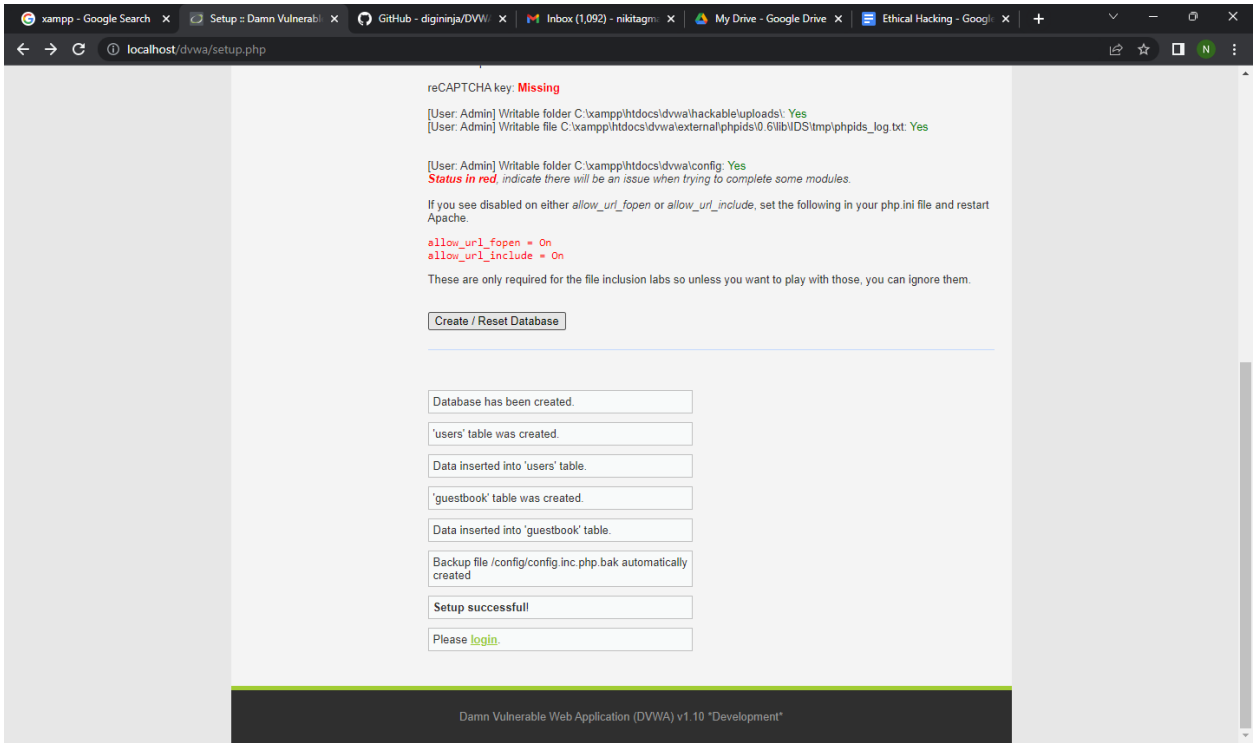


Goto C:\xampp\htdocs\DVWA-master\config. Change the file name config.inc.php.dist to config.inc.php

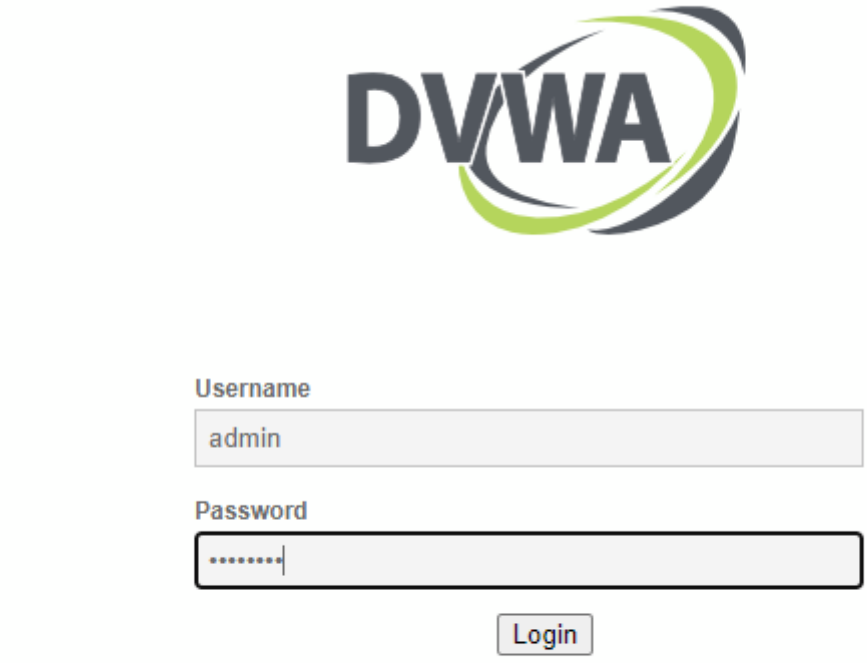


In the browser, enter http://localhost/dvwa-master/setup.php . Scroll below to find:

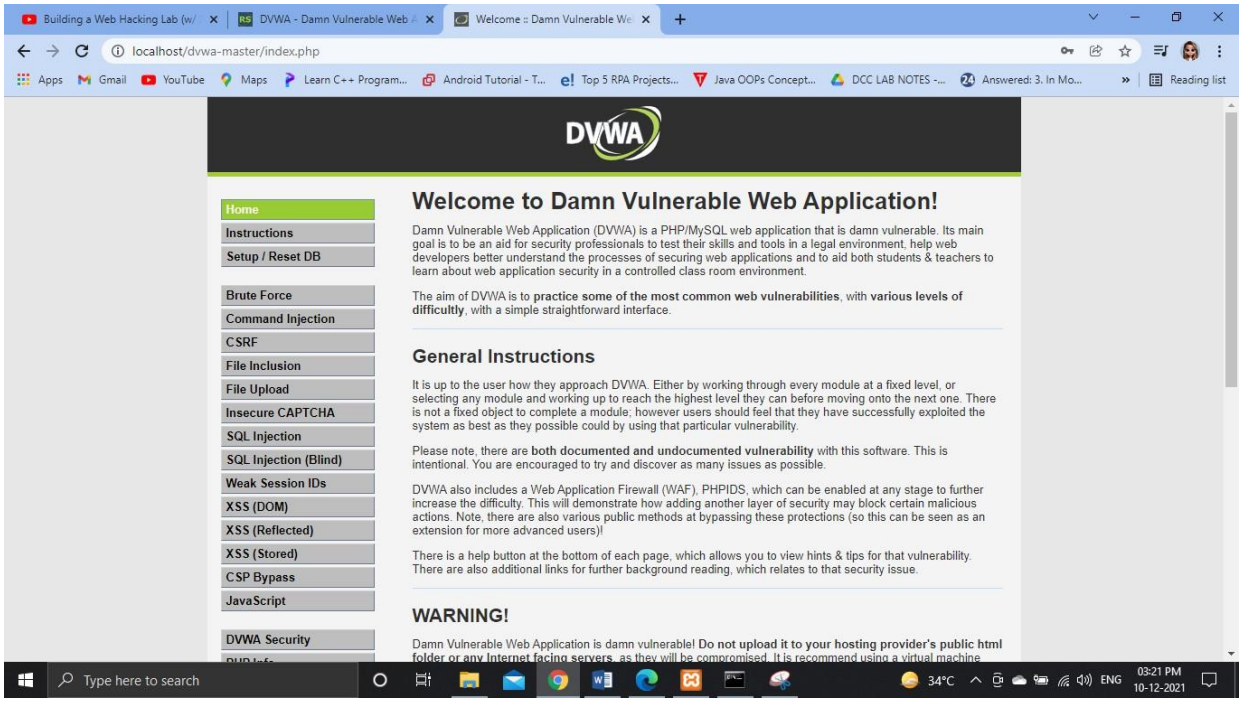




Next, it opens the window below: http://localhost/DVWA-master/login.php



Enter default credentials username =admin and password=password
We are now logged into DVWA



Local file inclusion and Remote file inclusion What is DVWA?

- PHP/MySQL web application that is vulnerable.
- Main goals:

- 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.
- Aid teachers/students to teach/learn web application security in a class room environment.

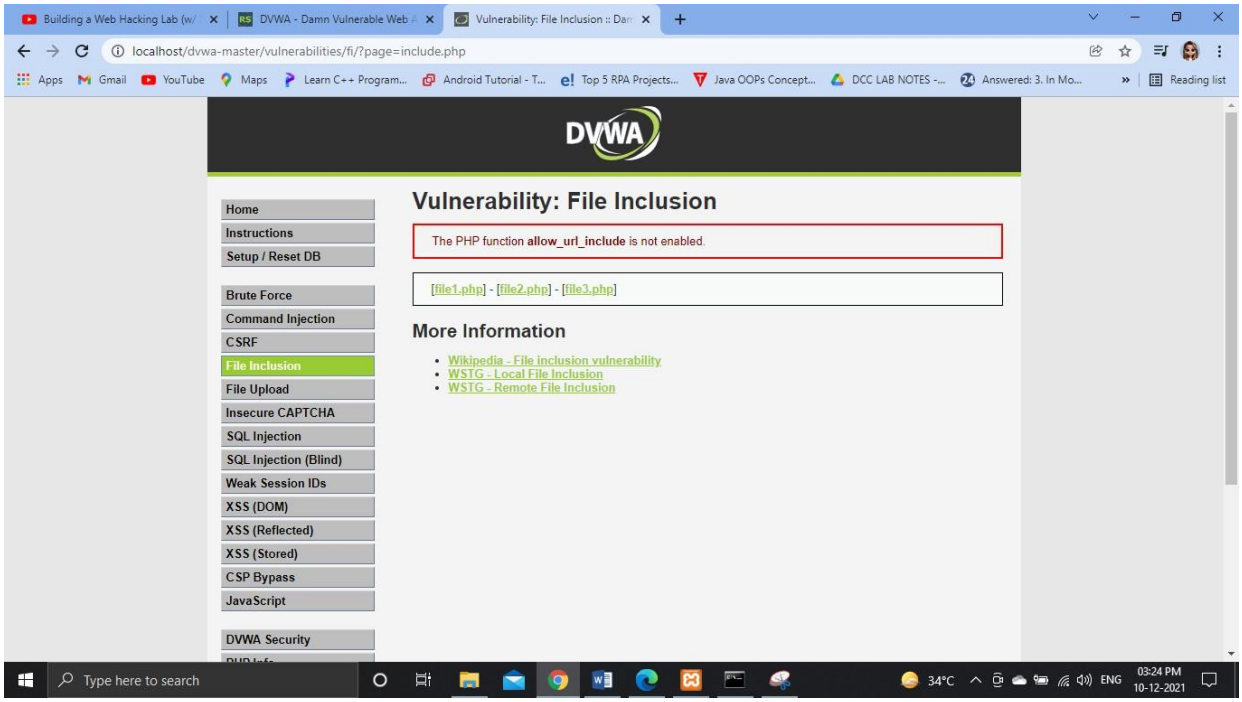
a. A website attack named Remote file inclusion is basically a one of the most common vulnerability found in web application. This type of vulnerability allows the Hacker or attacker to add a remote file on the web server. If the attacker gets successful in performing the attack he/she will gain access to the web server and hence can execute any command on it.

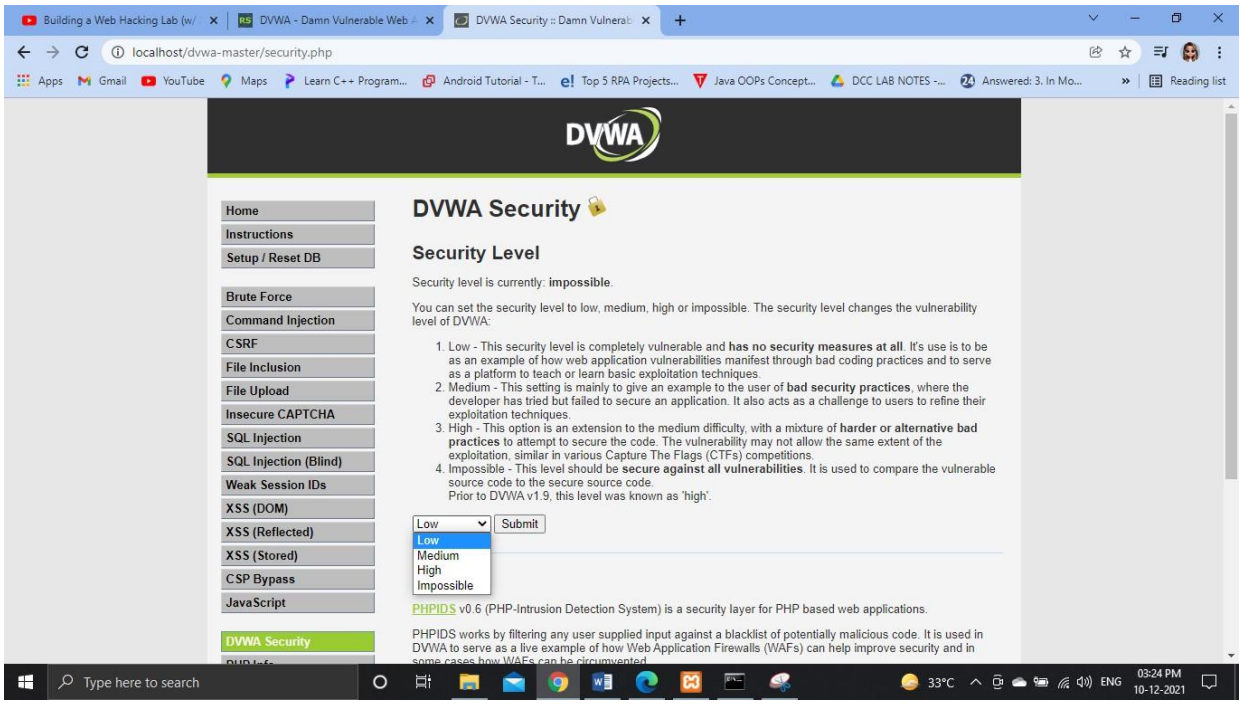
Questions:

1. Create a login.php/registration.php for your website. Perform local file inclusion using

DVWA.

Go to http://localhost/DVWA-master/vulnerabilities/fi/?page=include.php





On the address bar, set page attribute to http://localhost/sqlinjection/login.php

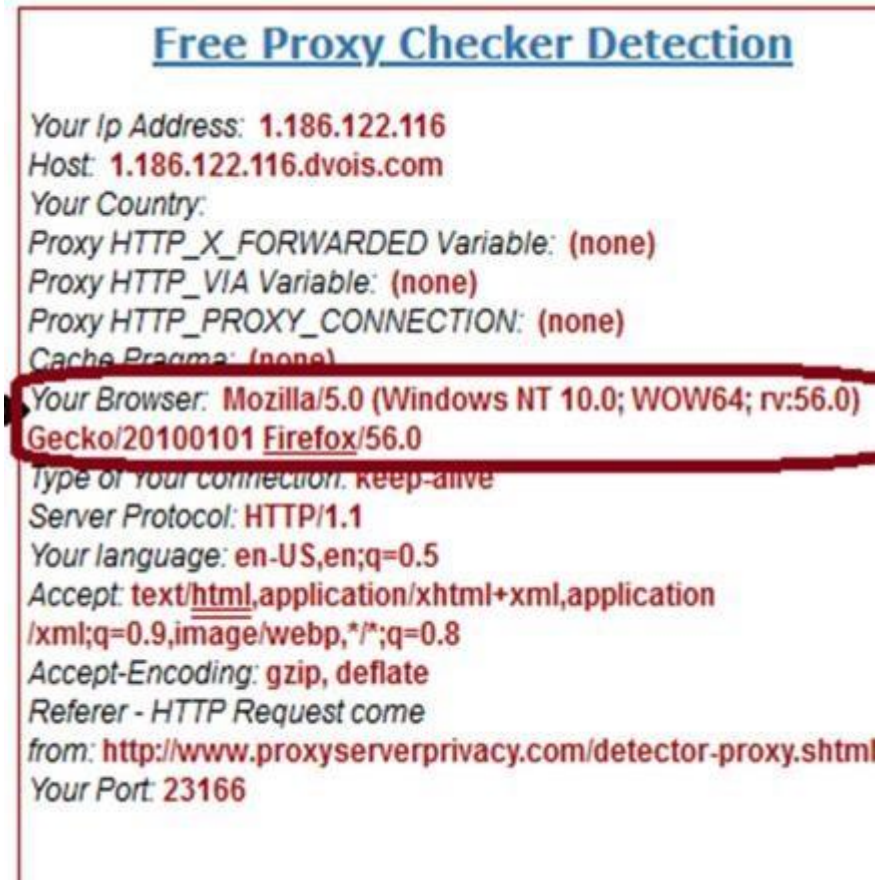
2. Perform remote file inclusion using DVWA. Display the home page of www.google.com On the address bar, set page attribute to http://www.google.com

B. Disguise as Google Bot to view Hidden Content of a Website

Step 1: To determine the user agent of firefox:

a. Go to Mozilla –http://www.proxyserverprivacy.com/

b. Select detector proxy
c. Select advanced proxy detector. Output:

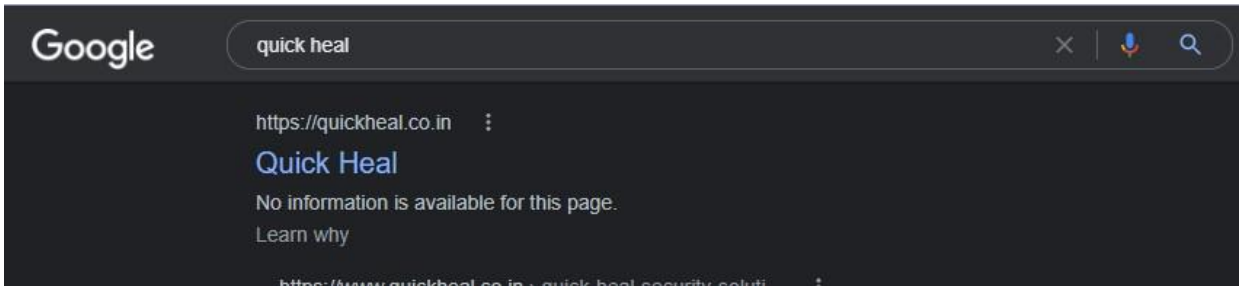


Step 2: To find out the string for google bot. To change the above useragent to googlebot a. Goto http://useragentstring.com/
b. Locate the string for google bot Googlebot/2.1 (+http://www.googlebot.com/bot.html)

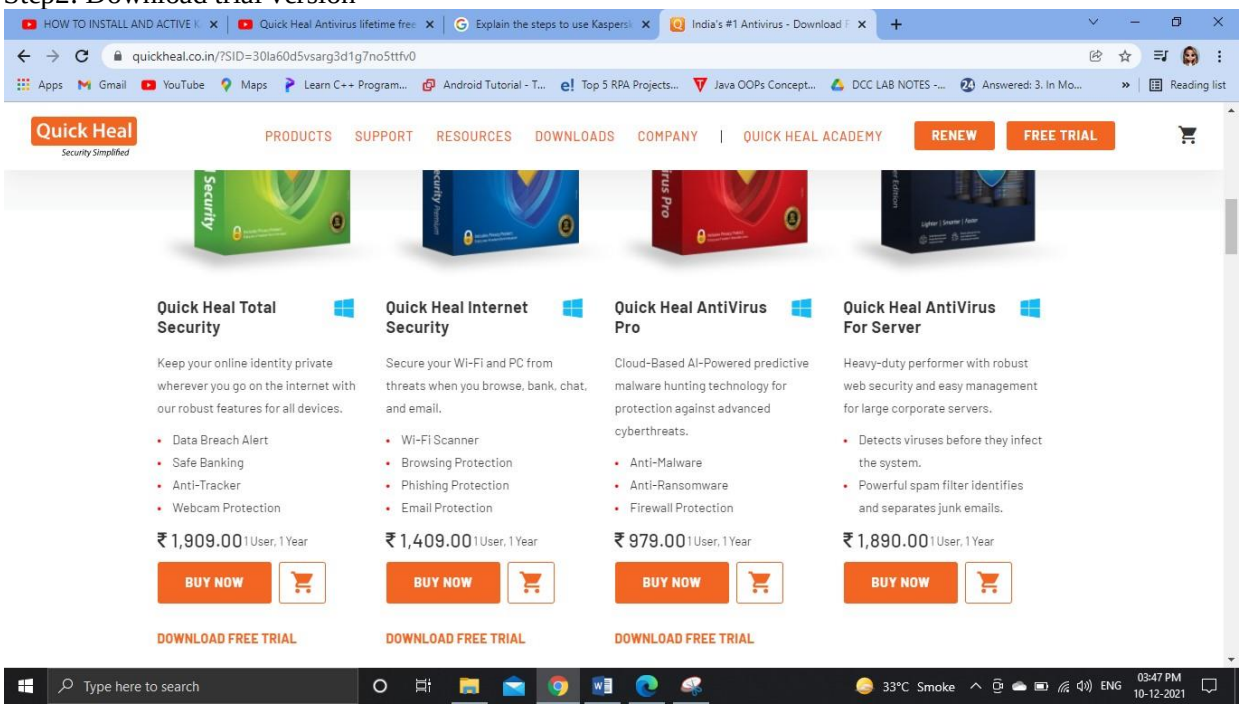
Step 3: Configure a. Go to firefox
b. Type about: config
c. Type general.useragent.override and assign Googlebot/2.1 (+http://www.googlebot.com/bot.html)
d. Goto http://www.proxyserverprivacy.com/ to check that the useragent is googlebot

C. Use Kaspersky/Quick Heal for Lifetime without Patch

Step 1: search for quick heal website on google



Step2: Download trial version



Step3: After 30 days of trial, uninstall the application
Step4: Again download the trial version of it, likewise you can use quick heal for lifetime by downloading its trial version every month.

C. How to use Kaspersky for Lifetime without Patch

a. Explain the steps to use Kaspersky /Quick for lifetime.

Reference
https://www.youtube.com/watch?v=wn_JbYnKax0