**Project Name : Cyber Security Project**

**Project Statement : Clone a Facebook page and try to perform Desktop Phishing in your local machine and capture the credentials Project Deadline : 24-September 2021**

**Assignment 06**

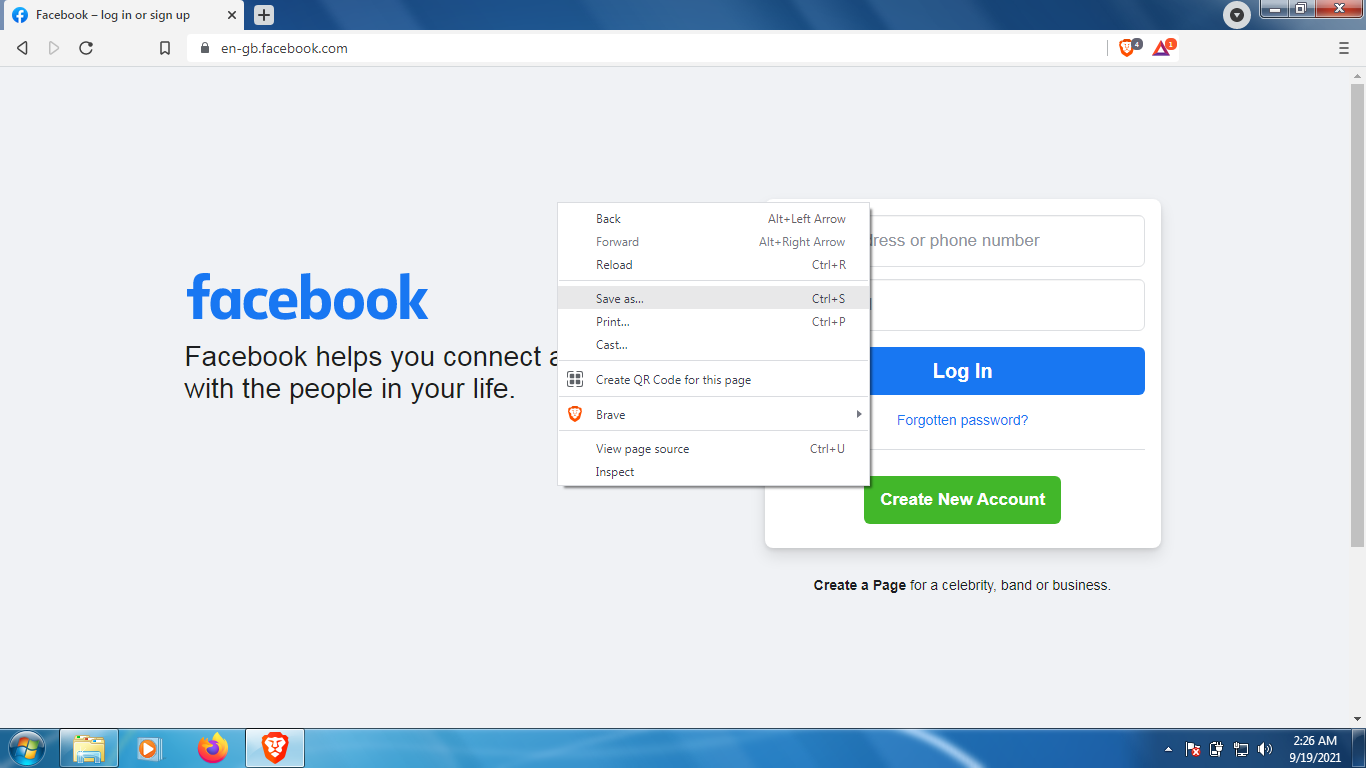
**Lab Objective:** Clone a Facebook page and try to perform Desktop Phishing in your local machine and capture the credentials

**Requirement:**

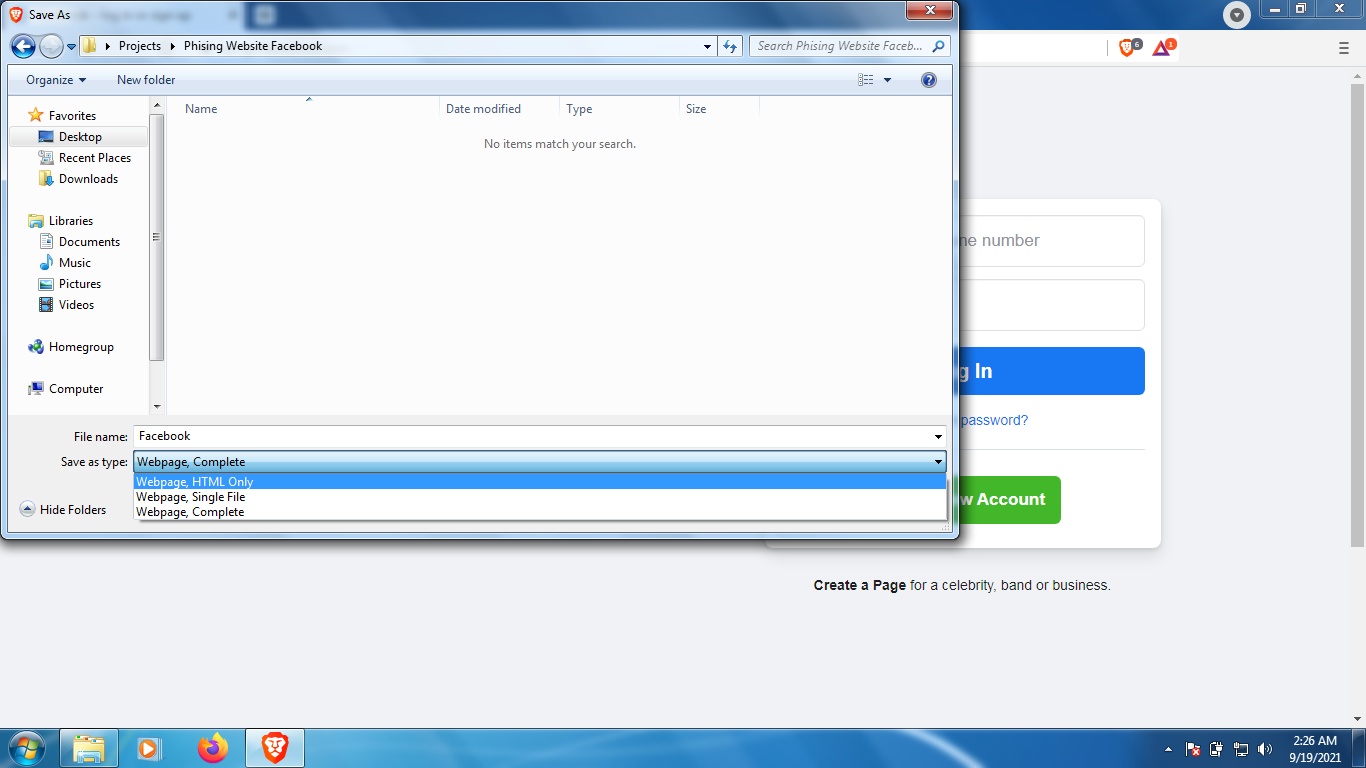
* HTML file ---> Original Facebook page.
* PHP file ---> Malicious code will be there.
* TXT file ---> will be used to save user ID & password

**Steps:**

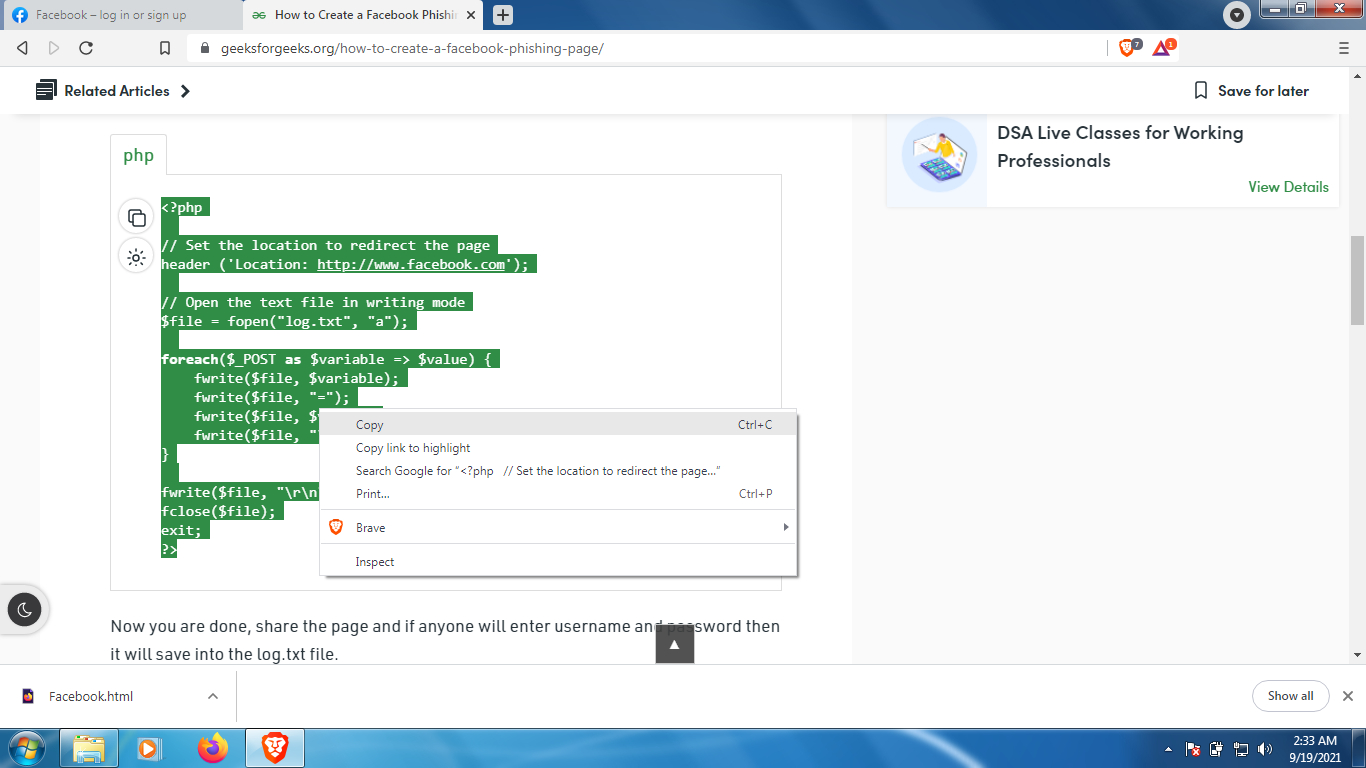
1. Save original html file of Facebook login page,



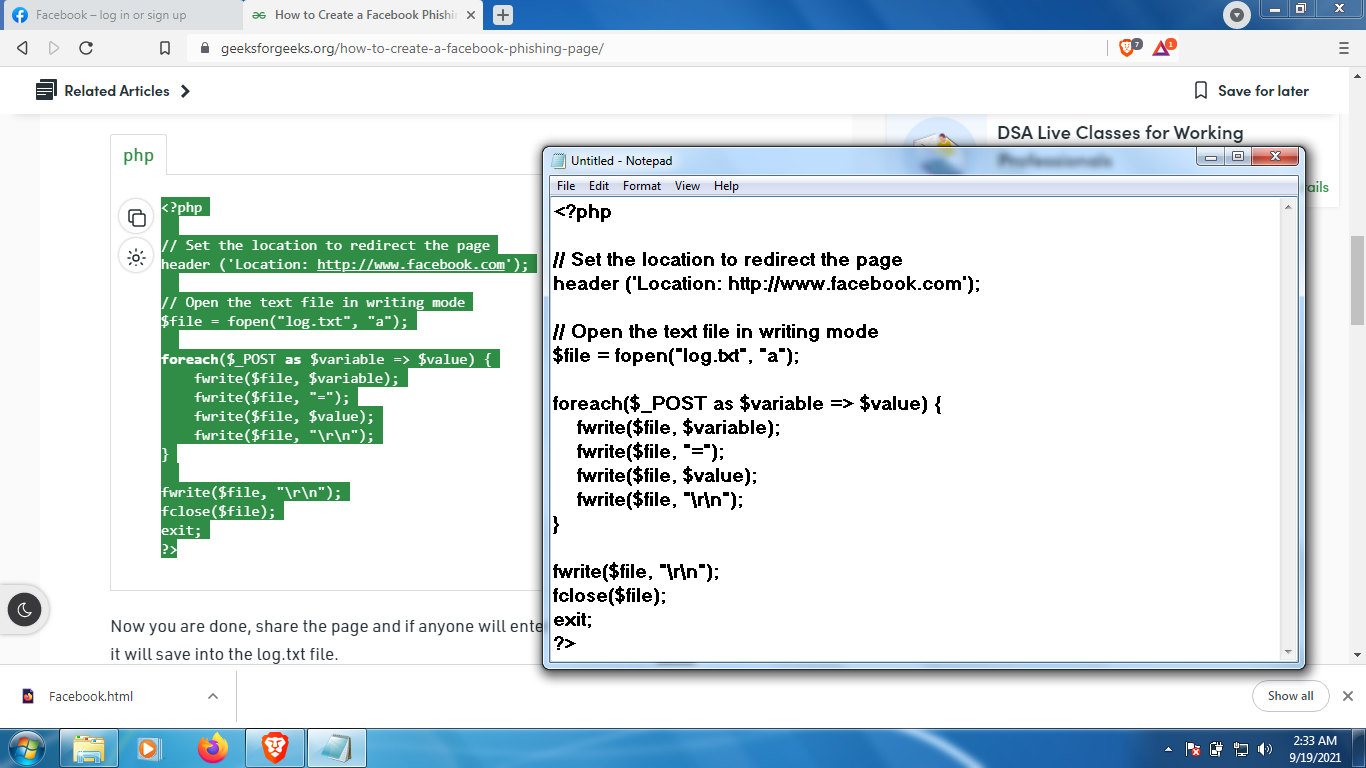
Save the file as “Webpage,HTML Only”.



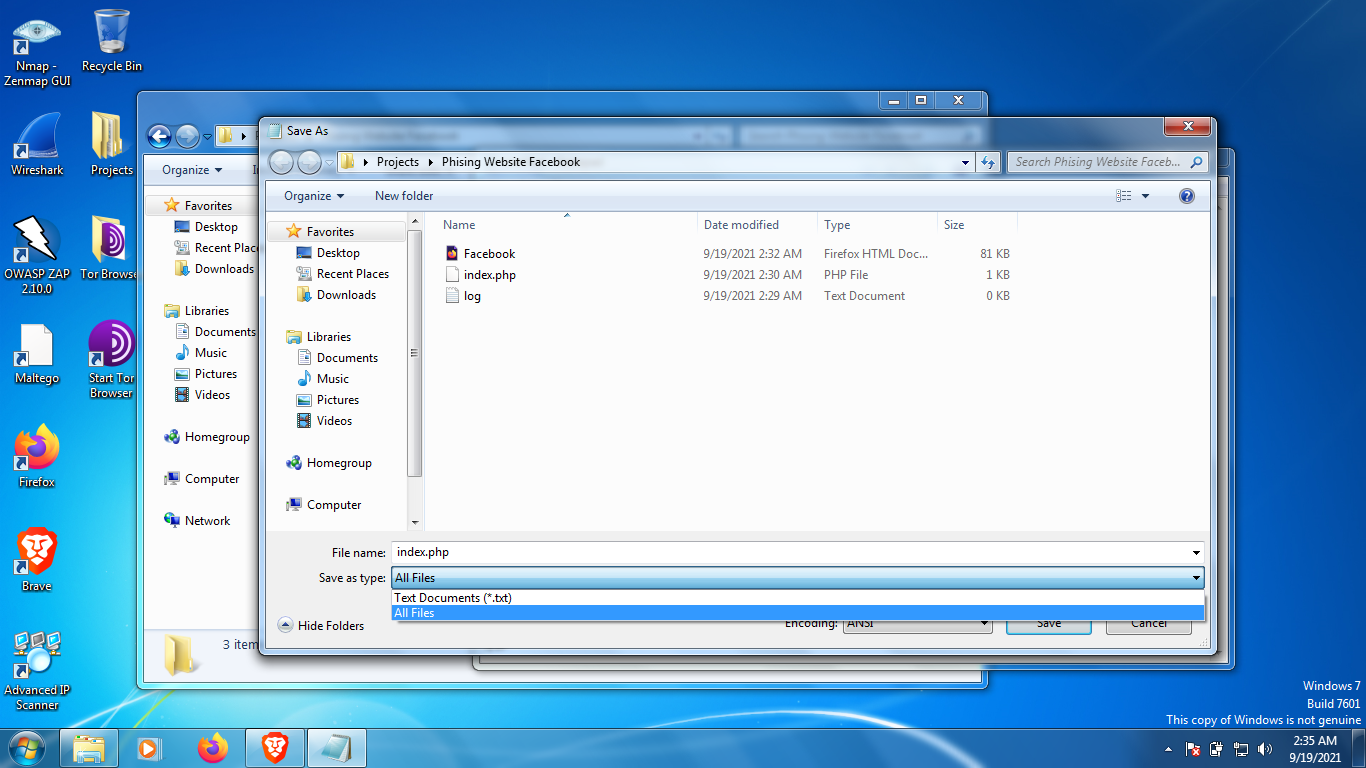
1. Download Facebook Phishing php script from Google or from the given link below (<https://www.geeksforgeeks.org/how-to-create-a-facebook-phishing-page/>) & Copy

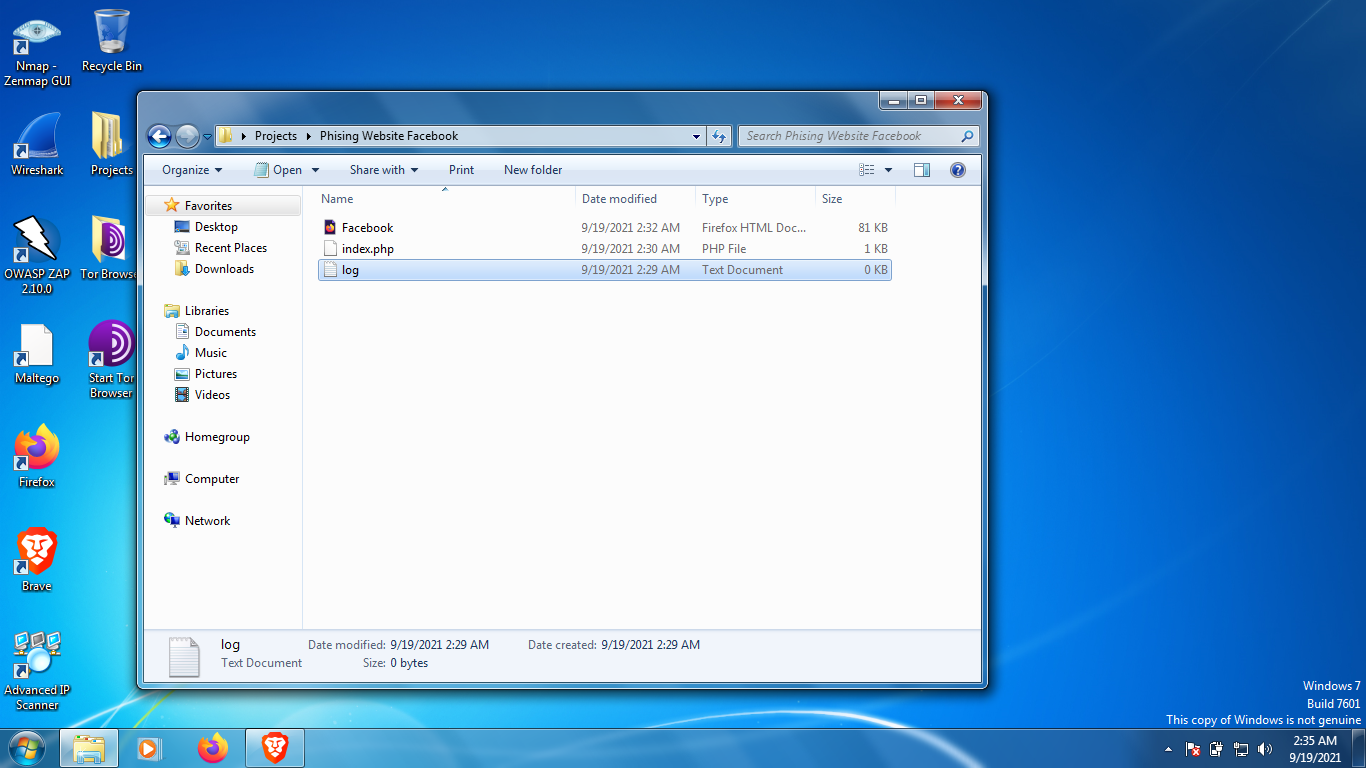


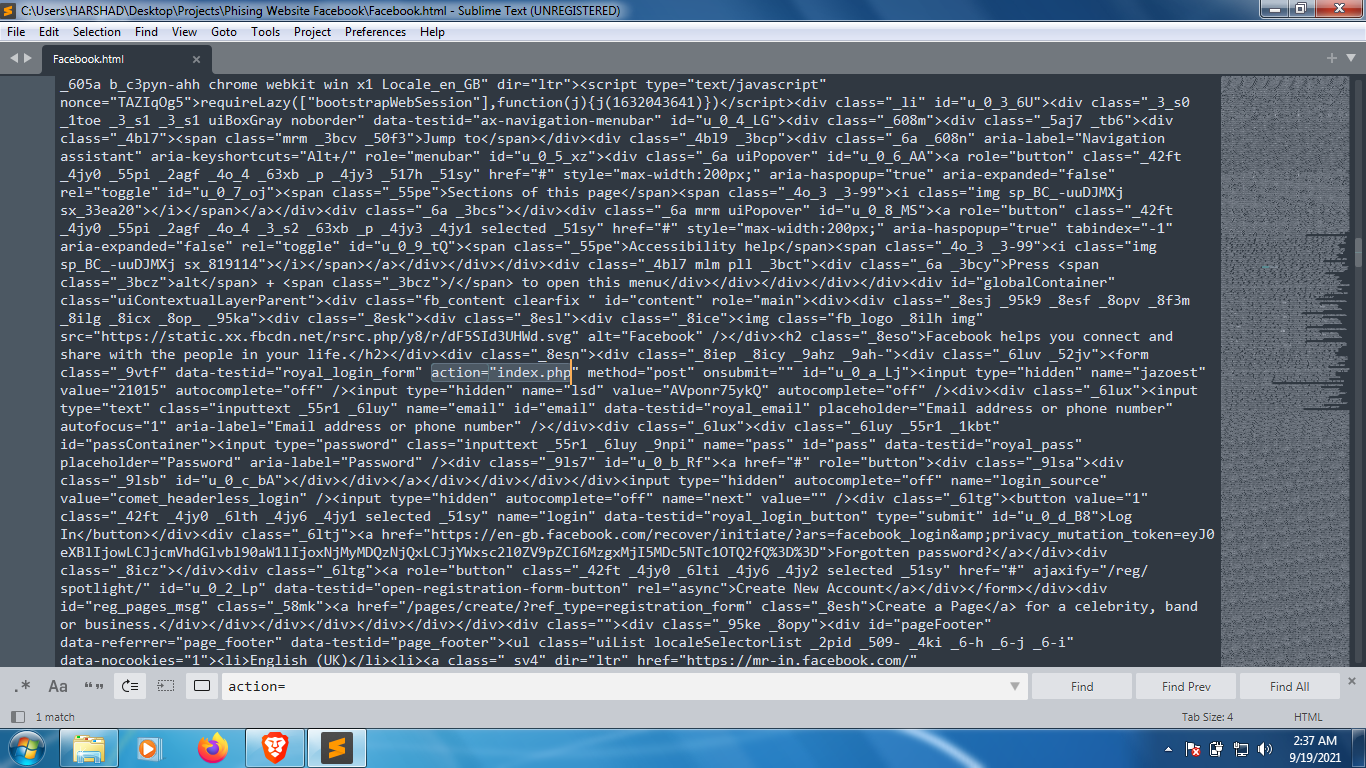
the php script to Notepad.



1. Save php file(index.php) as “All files” & add txt file with name (log.txt)

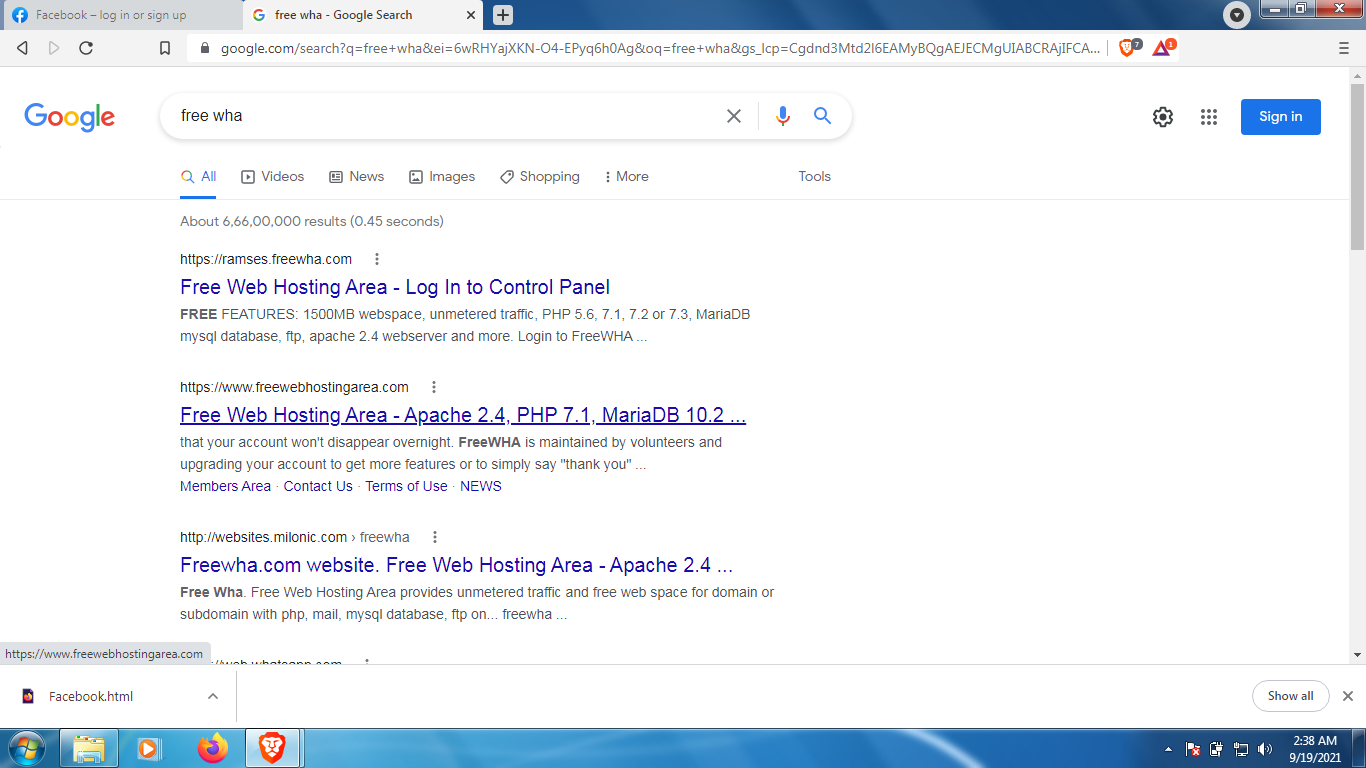




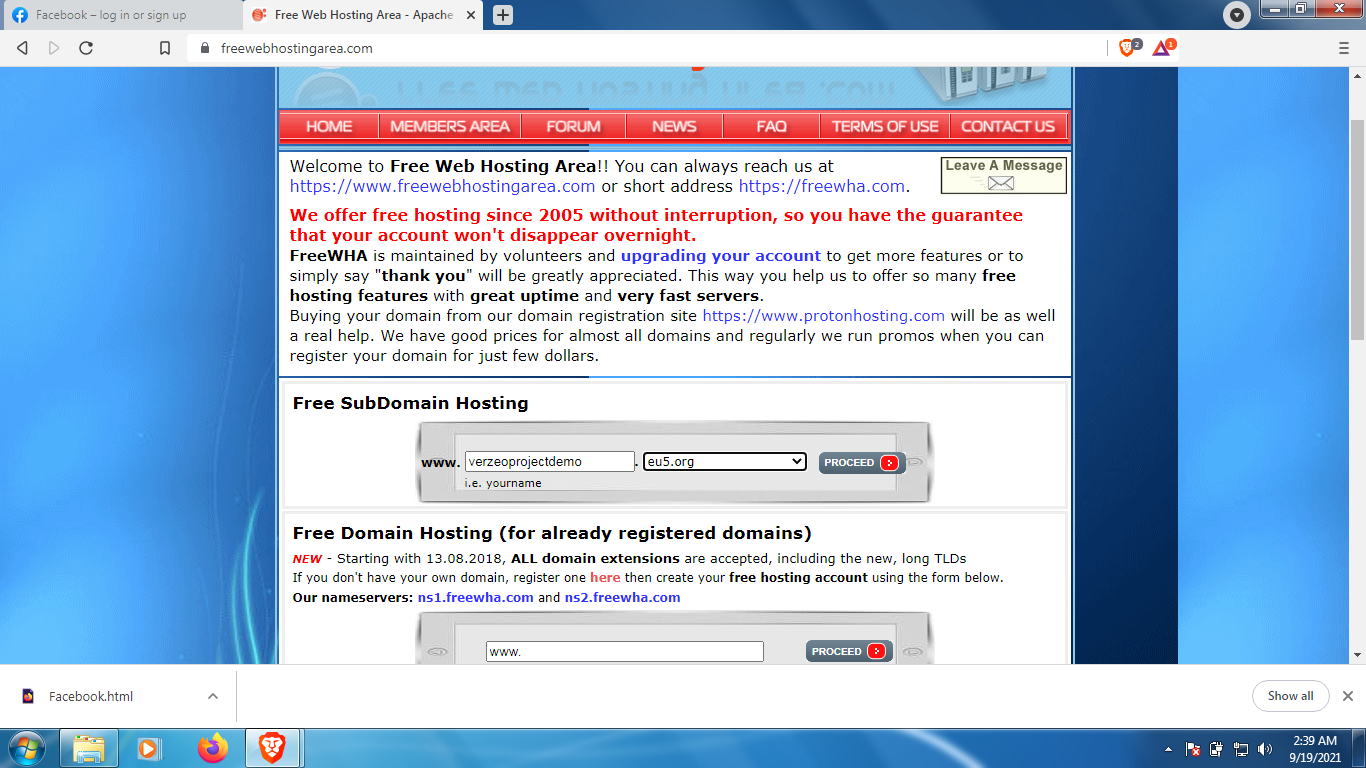
1. Edit the HTML file, as I am using Sublime Text but you can use Notepad, Notepad++ etc. Find keyword “action=” in the HTML document.

Replace the original link with php script file name(index.php).

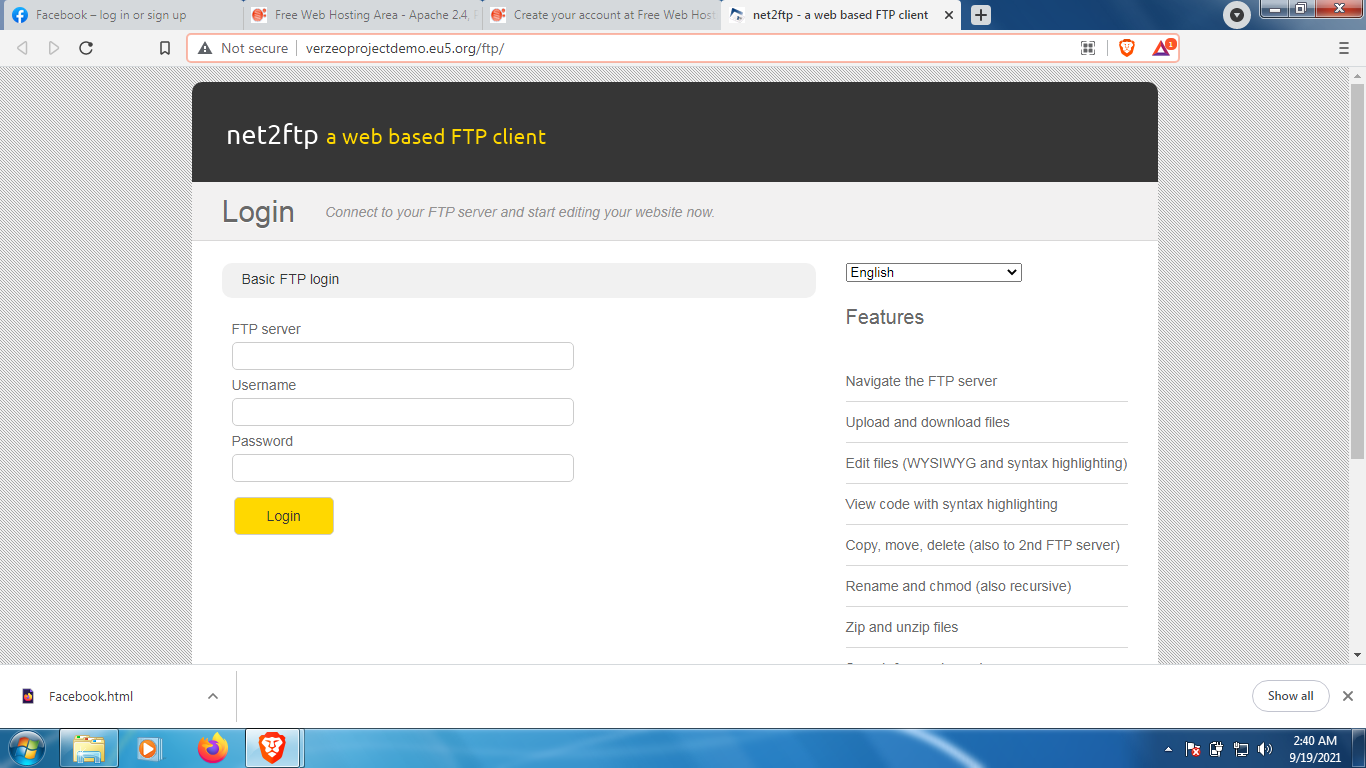
1. Now create a free website using any free hosting sites.

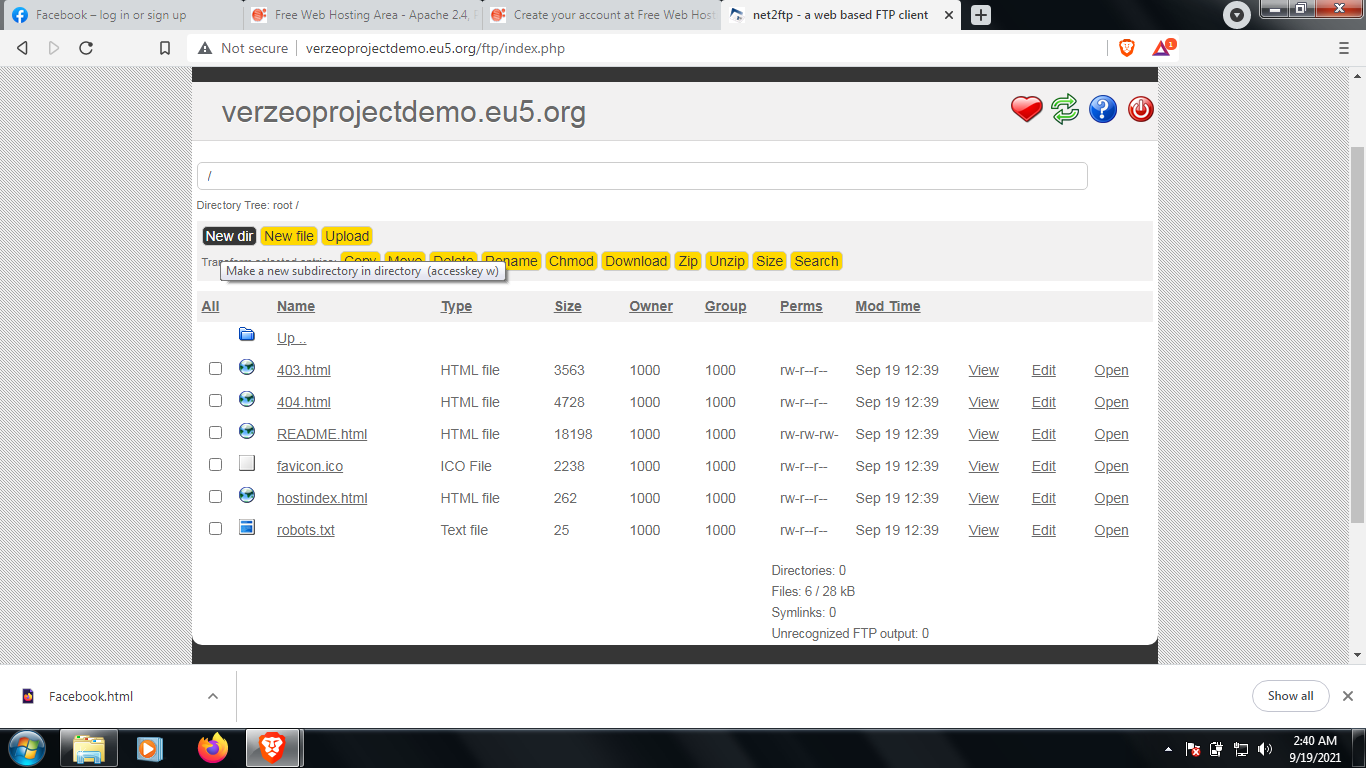


Here I am using https://www.freewebhostingarea.com/

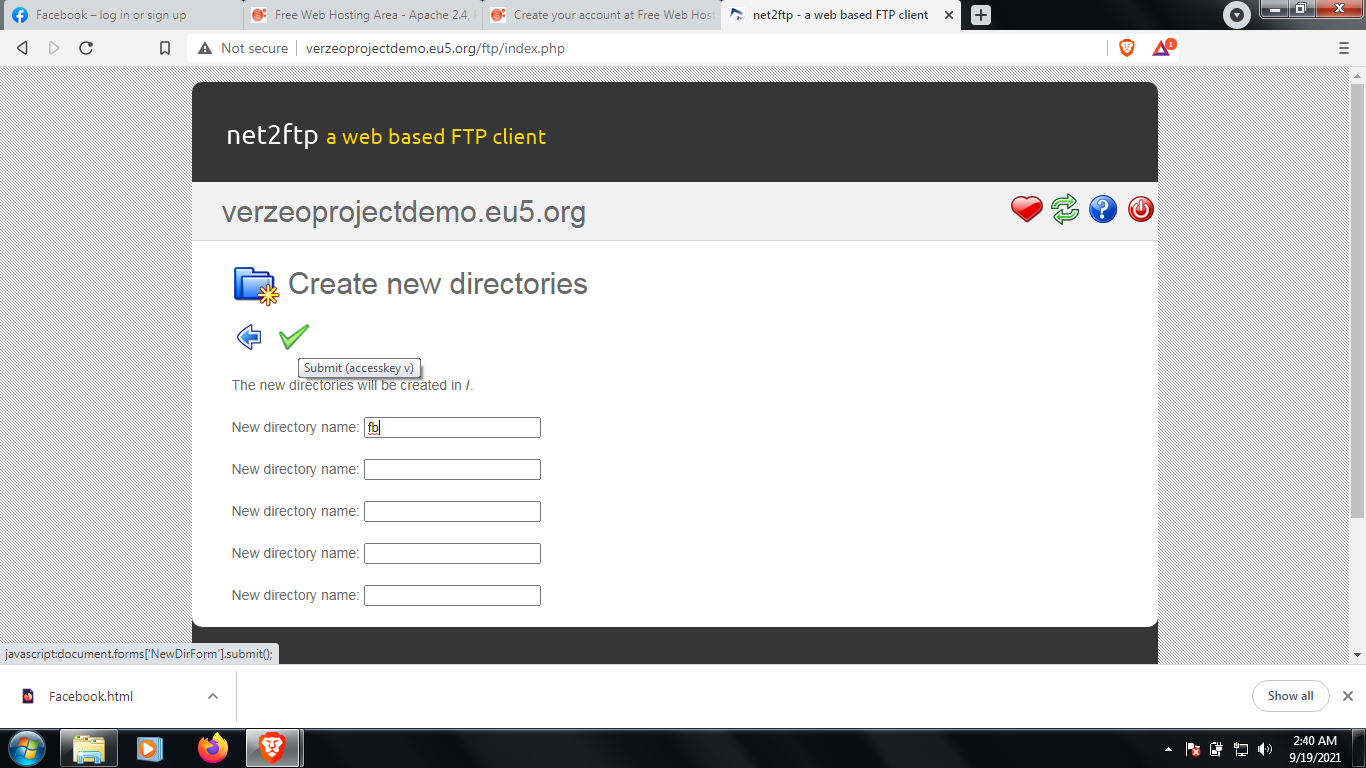


Create your own domain.

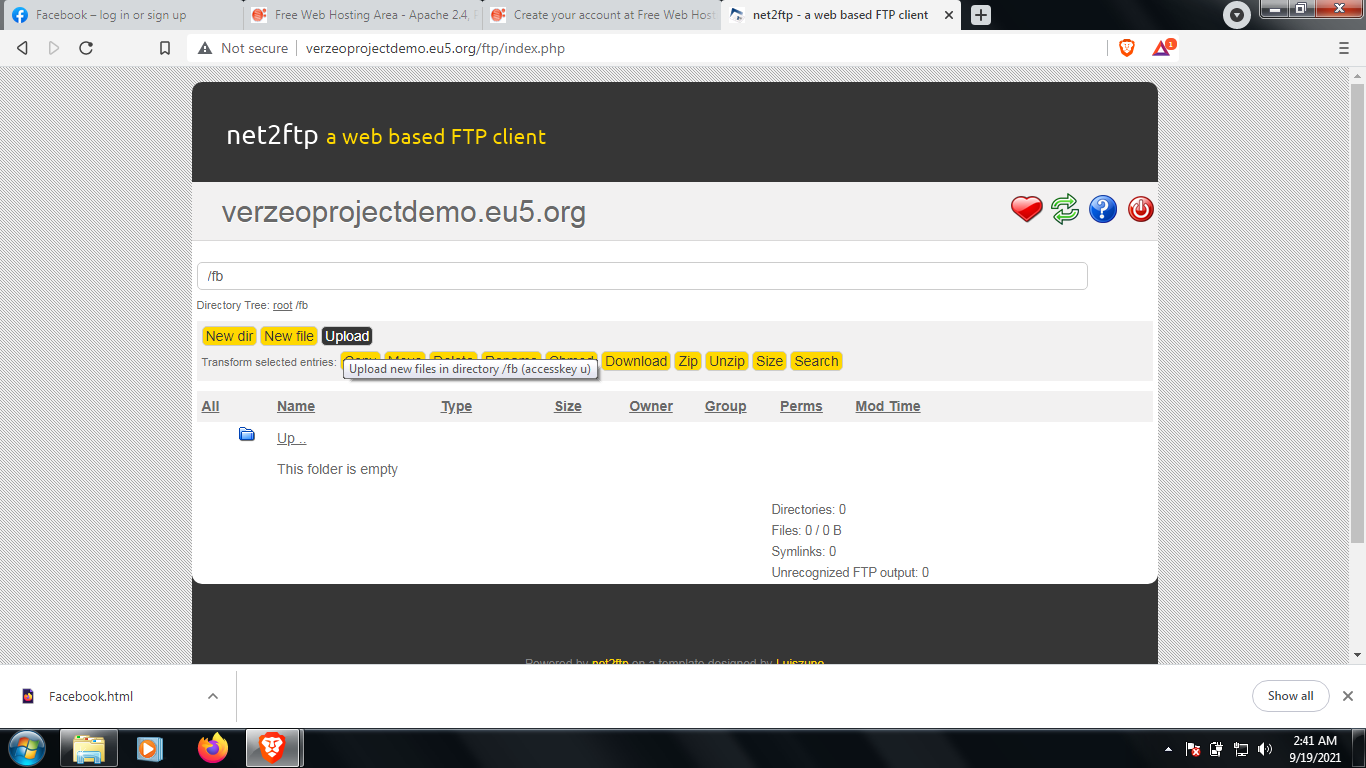
1. After successfully creating your domain go to ftp server to upload the files we created.

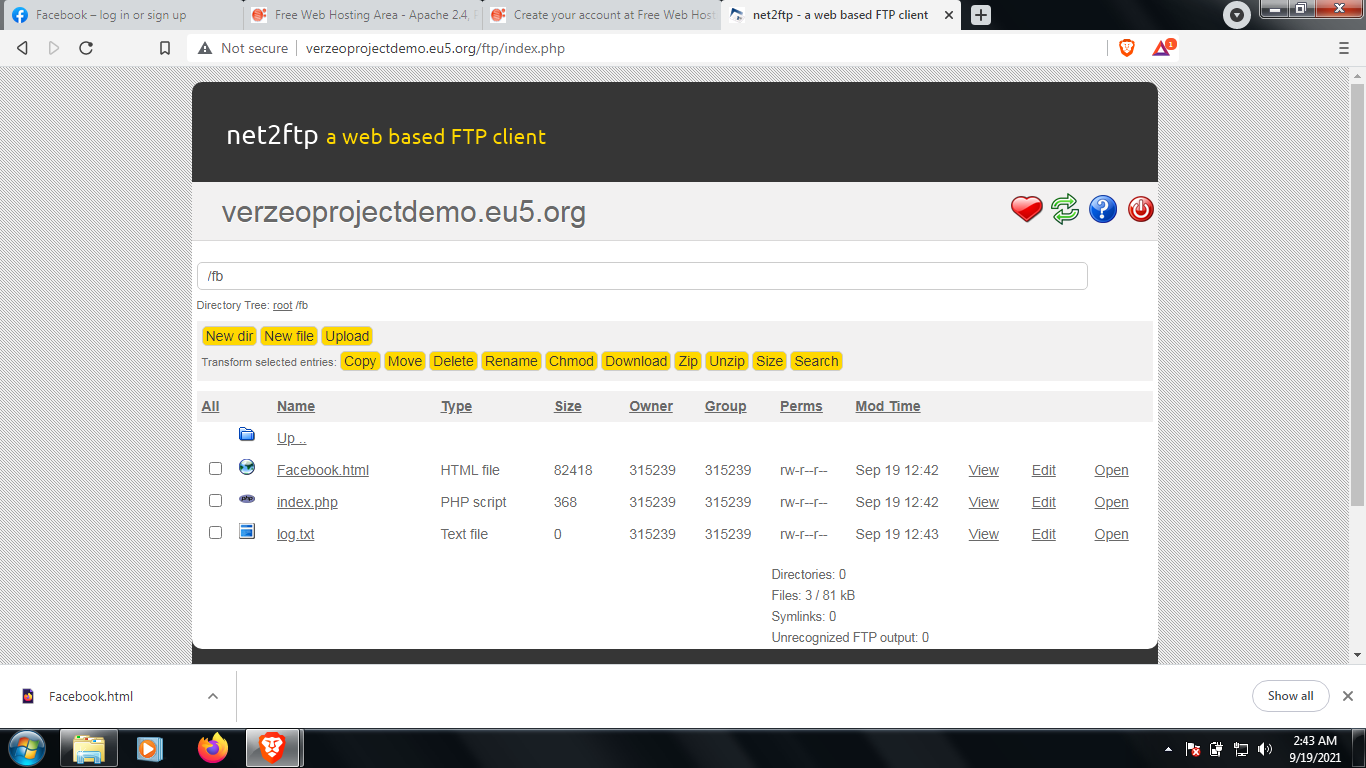


1. Now create a directories(fb)

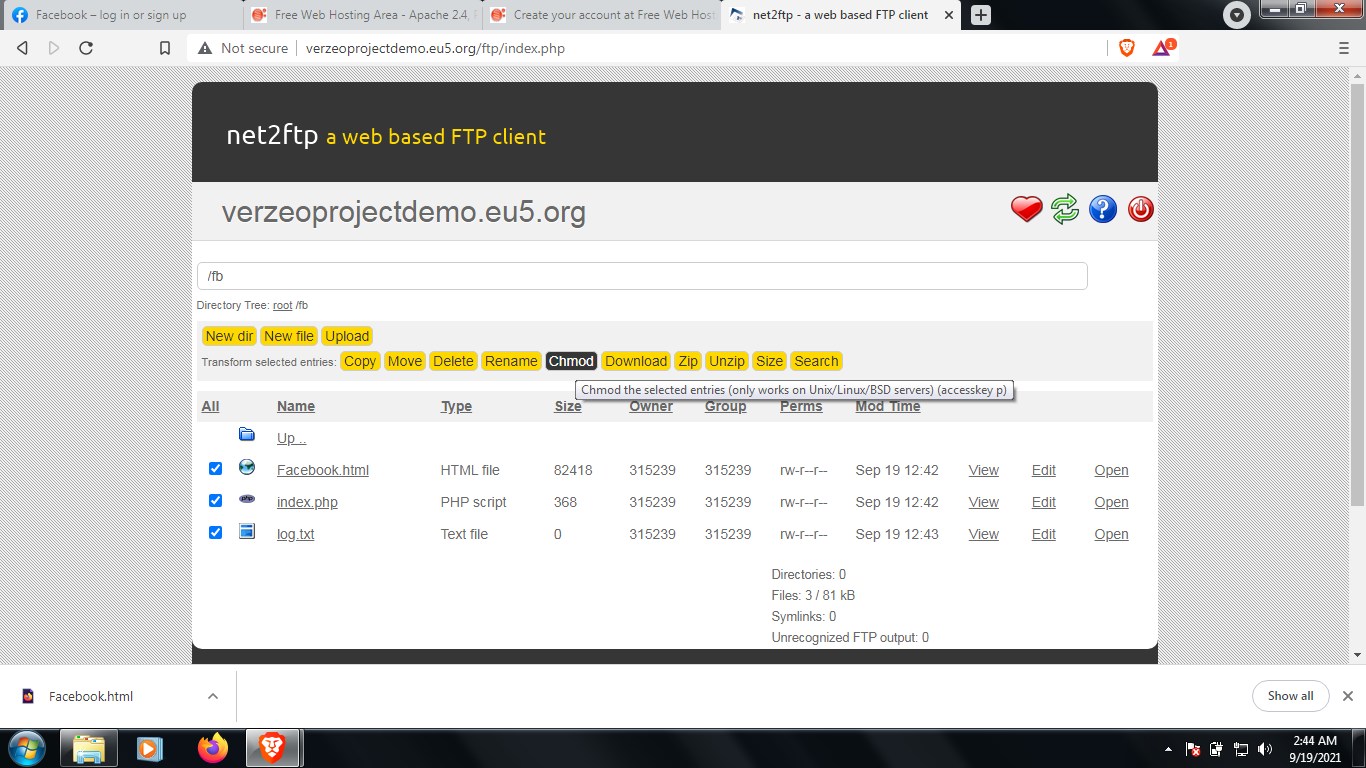


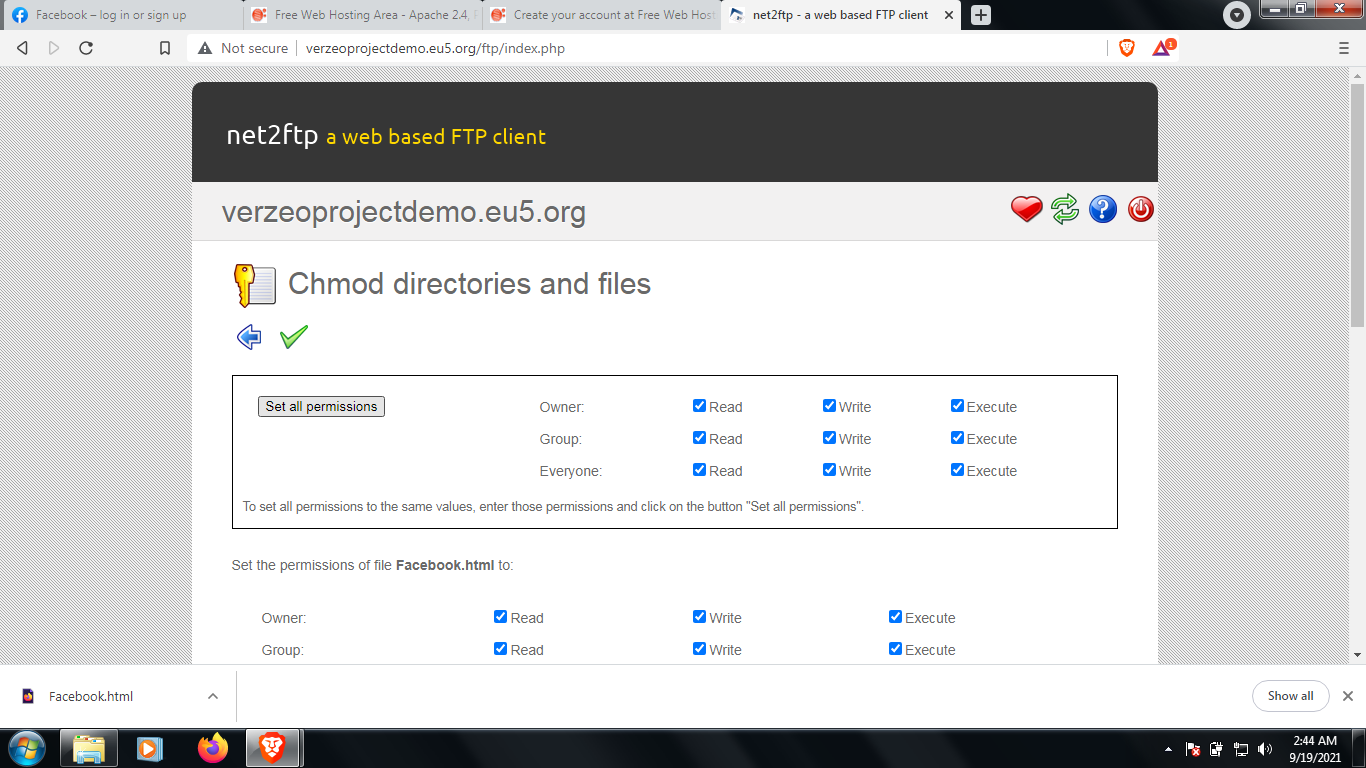
After successfully creating directories upload the files you created in it(Facebook.htm, index.php, log.txt).



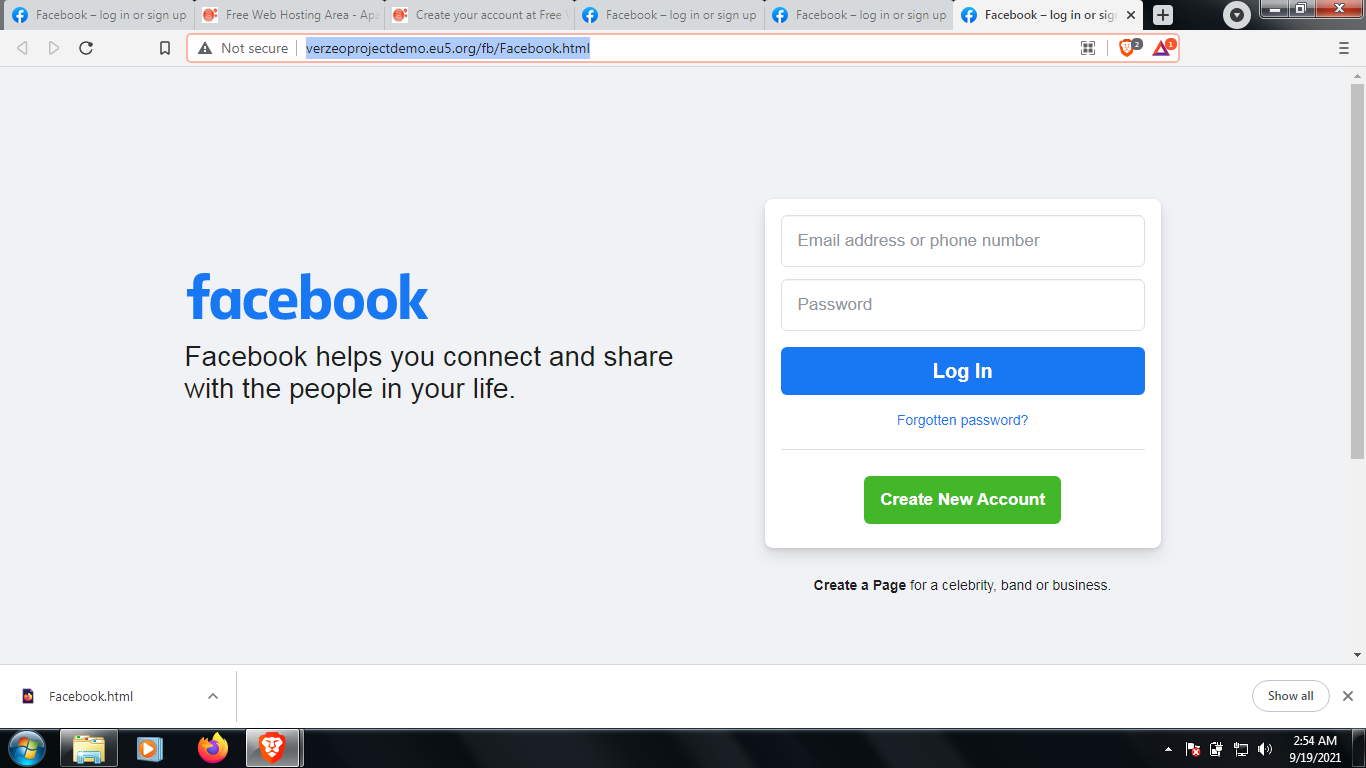


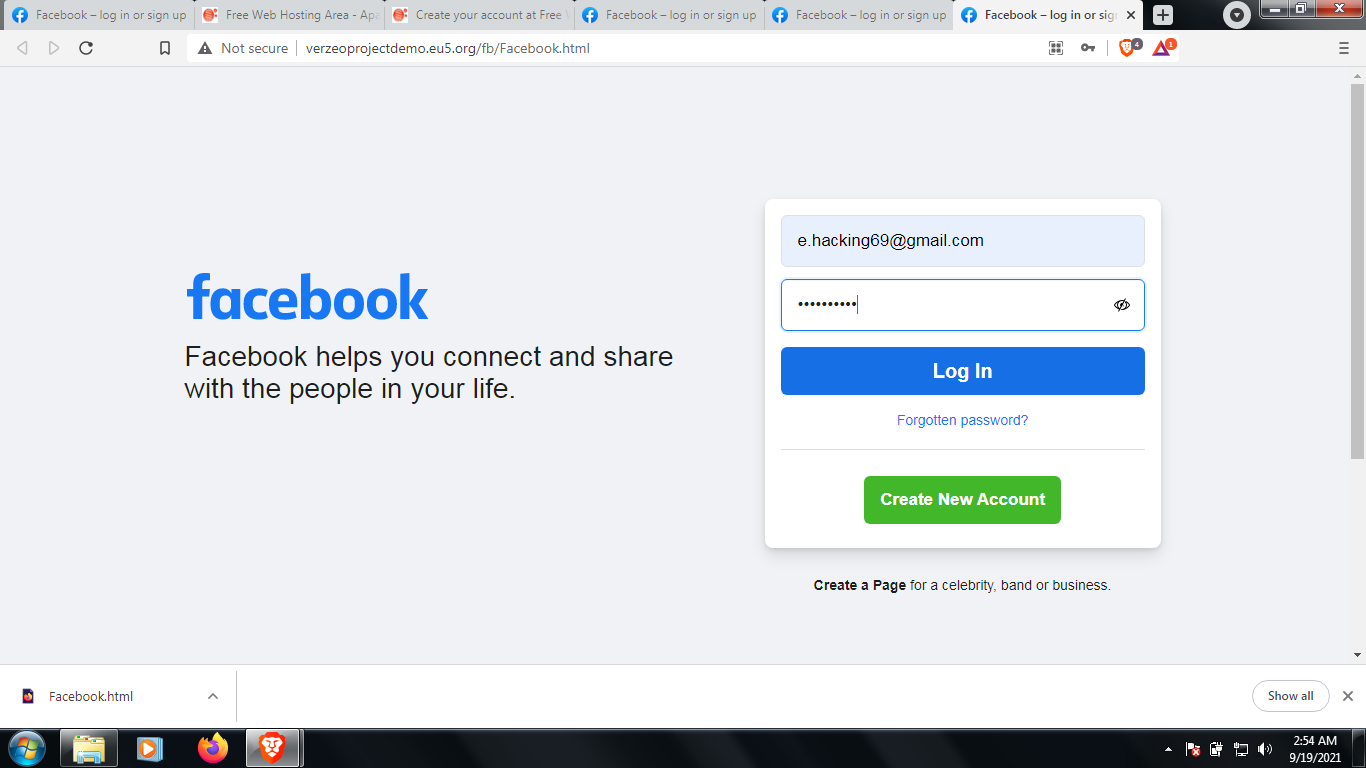
1. After successfully uploading the files we need to give full permission to these 3 files.

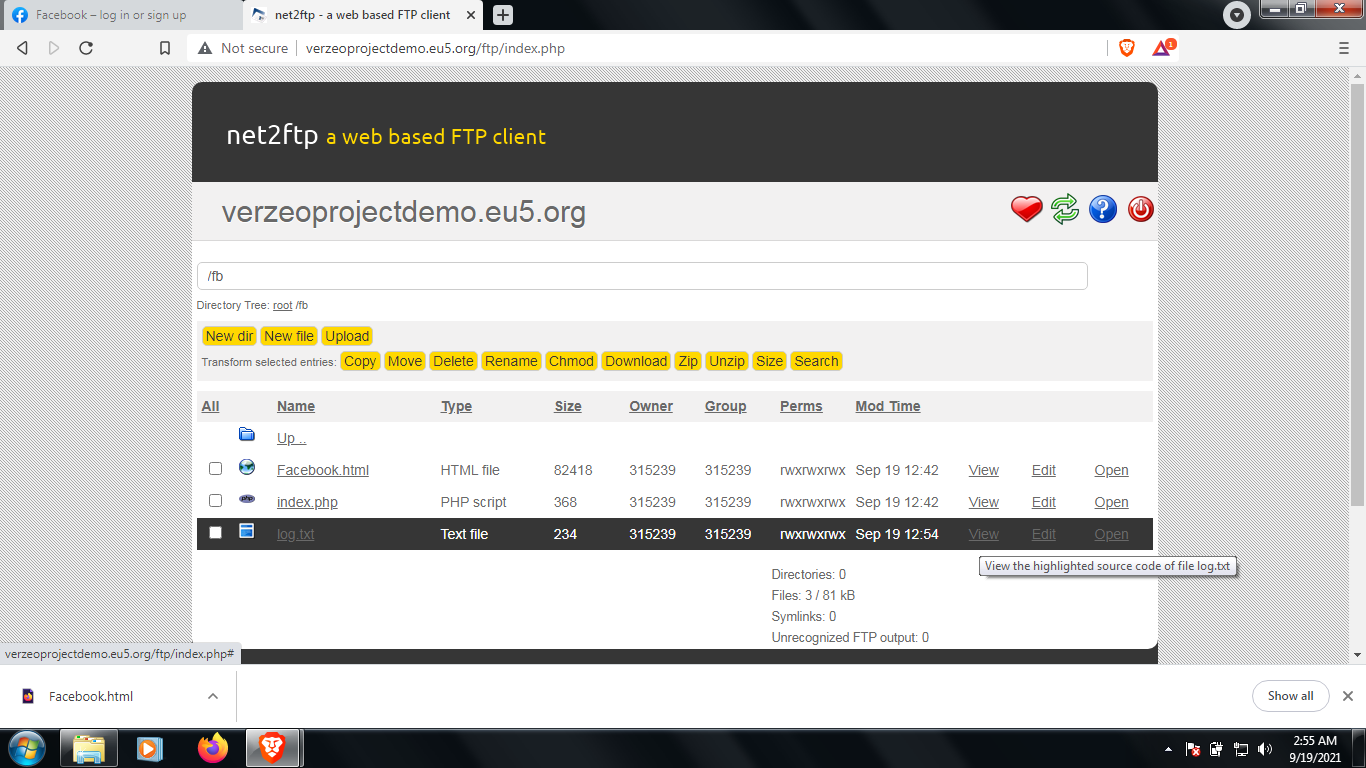


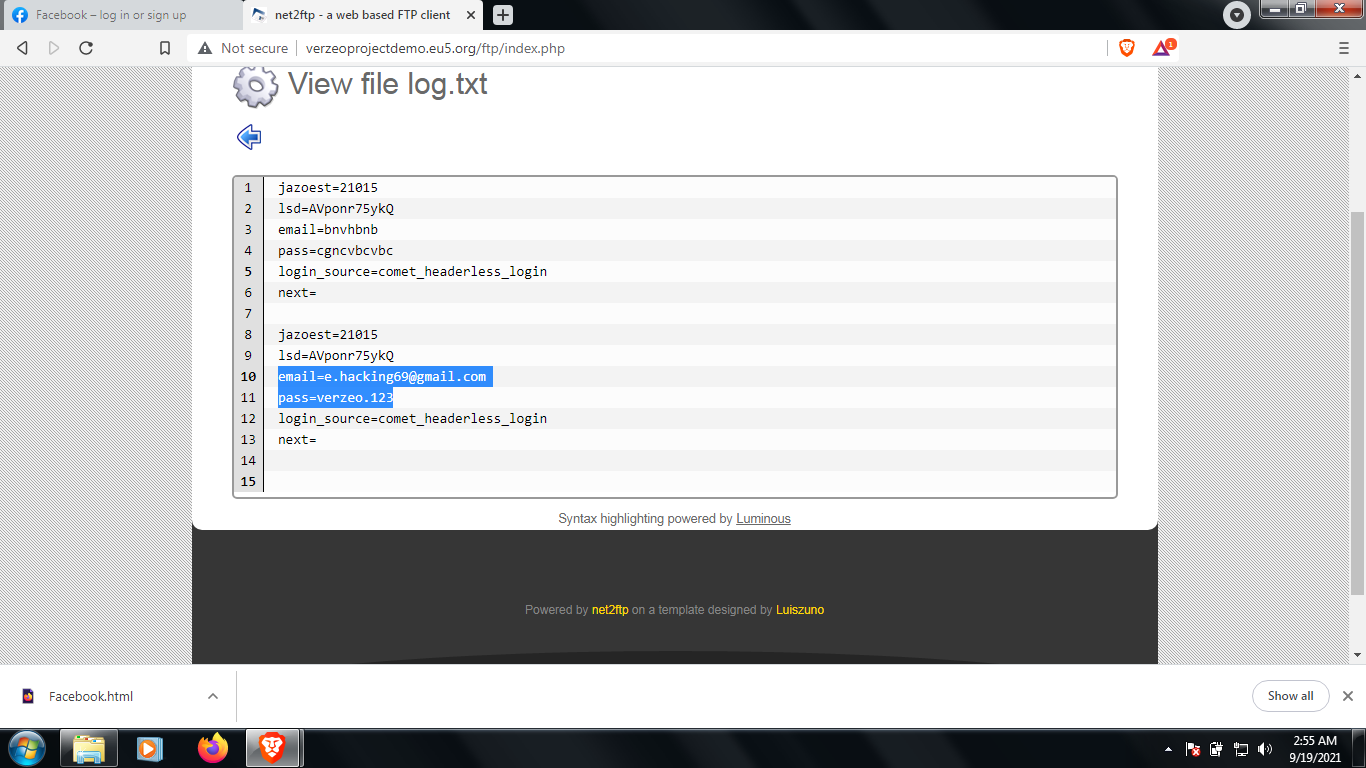


1. After giving full permission we are ready to use our phishing page. Send the link to the victim and convince them to login their credentials there, as soon as they login using their User ID and Password their data will be collected to our log.txt file.









We can see their User ID and Password by logging into our ftp server in the directory we created.

**Phishing scams are one of the most common methods of attack you’re likely to come across. They are a hugely profitable attack method for cybercriminals, as thousands fall victim to them every year. Fortunately, due to their commonplace nature, phishing scams are avoidable if you know how to correctly identify and prevent them.**

**SOLOUTIONS TO PREVENT THEM:**

### 1. Know what a phishing scam looks like

New phishing attack methods are being developed all the time, but they share commonalities that can be identified if you know what to look for. There are many sites online that will keep you informed of the latest phishing attacks and their key identifiers. The earlier you find out about the latest attack methods and share them with your users through regular security awareness training, the more likely you are to avoid a potential attack.

### 2. Don’t click on that link

It’s generally not advisable to click on a link in an email or instant message, even if you know the sender. The bare minimum you should be doing is hovering over the link to see if the destination is the correct one. Some phishing attacks are fairly sophisticated, and the destination URL can look like a carbon copy of the genuine site, set up to record keystrokes or steal login/credit card information. If it’s possible for you to go straight to the site through your search engine, rather than click on the link, then you should do so.

### 3. Get free anti-phishing add-ons

Most browsers nowadays will enable you to download add-ons that spot the signs of a malicious website or alert you about known phishing sites. They are usually completely free so there’s no reason not to have this installed on every device in your organization.

### 4. Don’t give your information to an unsecured site

If the URL of the website doesn’t start with “https”, or you cannot see a closed padlock icon next to the URL, do not enter any sensitive information or download files from that site. Site’s without security certificates may not be intended for phishing scams, but it’s better to be safe than sorry.

### 5. Rotate passwords regularly

If you’ve got online accounts, you should get into the habit of regularly rotating your passwords so that you prevent an attacker from gaining unlimited access. Your accounts may have been compromised without you knowing, so adding that extra layer of protection through password rotation can prevent ongoing attacks and lock out potential attackers.

### 6. Don’t ignore those updates

Receiving numerous update messages can be frustrating, and it can be tempting to put them off or ignore them altogether. Don’t do this. Security patches and updates are released for a reason, most commonly to keep up to date with modern cyber-attack methods by patching holes in security. If you don’t update your browser, you could be at risk of phishing attacks through known vulnerabilities that could have been easily avoided.

### 7. Install firewalls

Firewalls are an effective way to prevent external attacks, acting as a shield between your computer and an attacker. Both desktop firewalls and network firewalls, when used together, can bolster your security and reduce the chances of a hacker infiltrating your environment.

### 8. Don’t be tempted by those pop-ups

Pop-ups aren’t just irritating; they are often linked to malware as part of attempted phishing attacks. Most browsers now allow you to download and install free ad-blocker software that will automatically block most of the malicious pop-ups. If one does manage to evade the ad-blocker though, don’t be tempted to click! Occasionally pop-ups will try and deceive you with where the “Close” button is, so always try and look for an “x” in one of the corners.

### 9. Don’t give out important information unless you must

As a general rule of thumb, unless you 100% trust the site you are on, you should not willingly give out your card information. Make sure, if you have to provide your information, that you verify the website is genuine, that the company is real and that the site itself is secure.

### 10. Have a Data Security Platform to spot signs of an attack

If you are unfortunate enough to be the victim of a successful phishing attack, then it’s important you are able to detect and react in a timely manner. Having a [data security platform](https://www.lepide.com/data-security-platform/) in place helps take some of the pressure off the IT/Security team by automatically alerting on anomalous user behavior and unwanted changes to files. If an attacker has access to your sensitive information, data security platforms can help to identify the affected account so that you can take actions to prevent further damage.

**LINKS USED:**

[**https://www.facebook.com/**](https://www.facebook.com/)

<https://www.geeksforgeeks.org/how-to-create-a-facebook-phishing-page/>

<https://www.freewebhostingarea.com/>

[**http://verzeoprojectdemo.eu5.org/fb/Facebook.html**](http://verzeoprojectdemo.eu5.org/fb/Facebook.html)

**Conclusion: So using these steps we can clone facebook and make a phising website.**