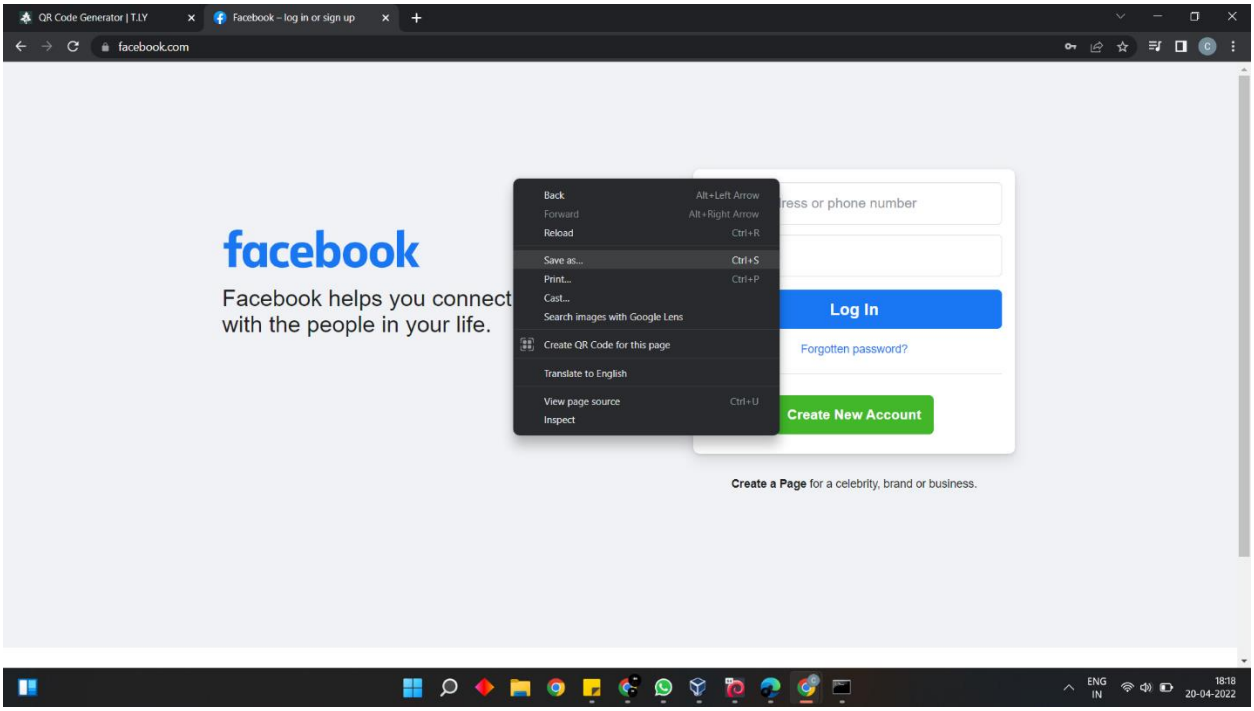
Smartknower Minor Project

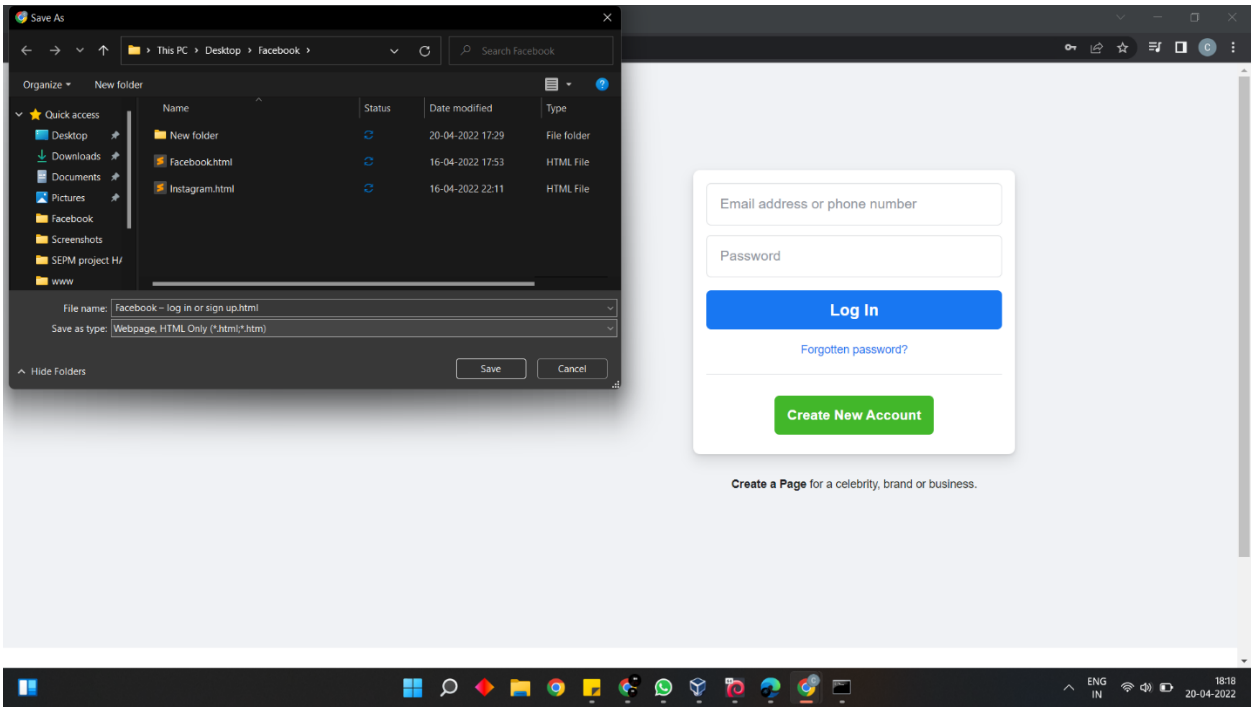
Project Name: Cyber Security March Minor Project

Problem Statement: 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.

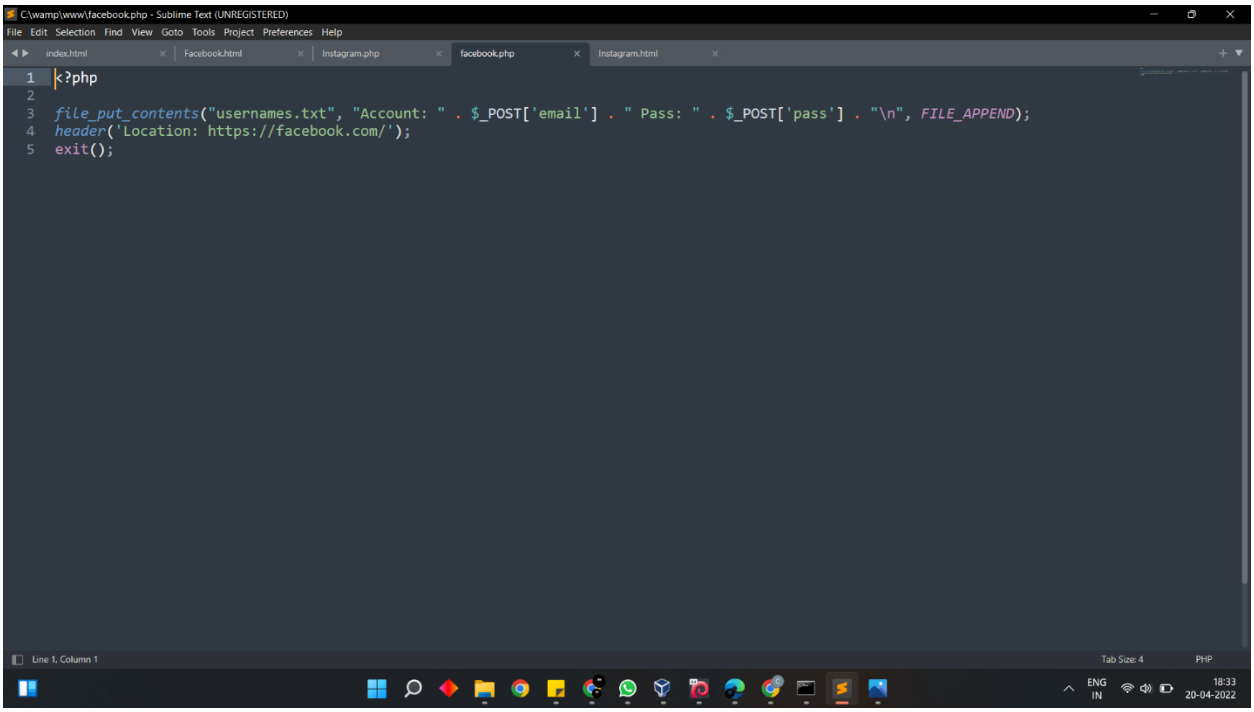
Steps to perform Desktop Phishing are as follows:

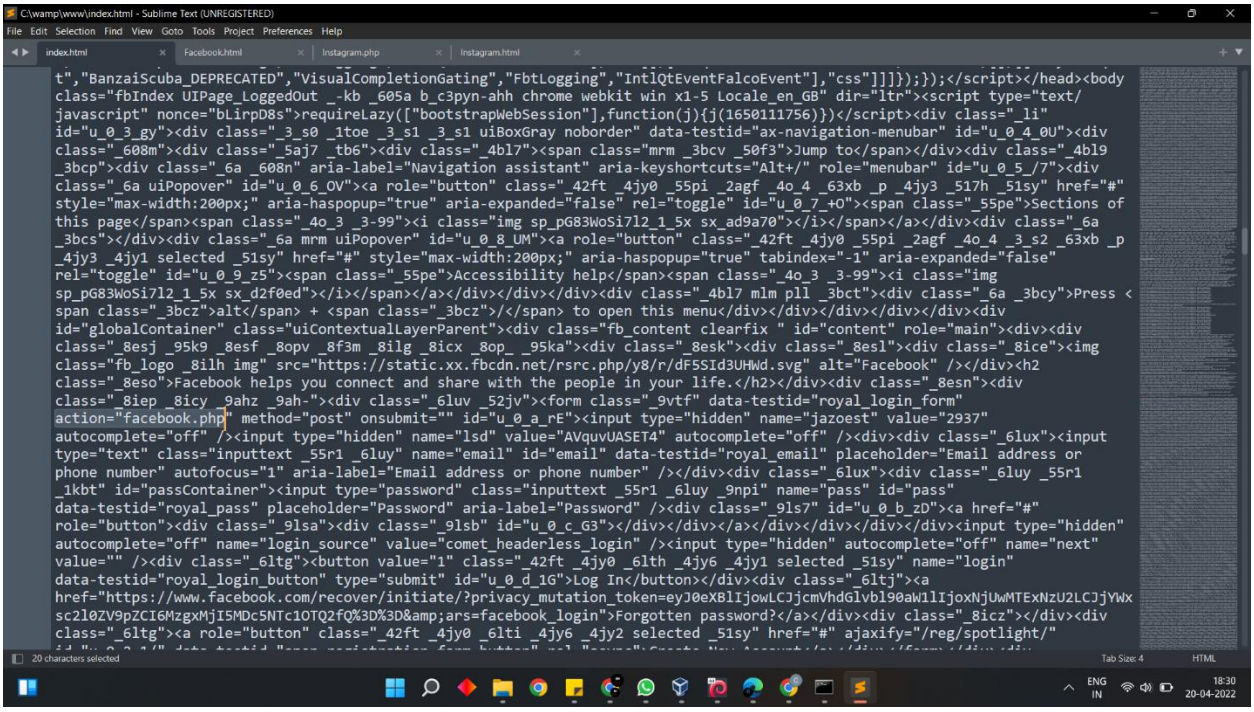
Step1: Choose a target site (here www.facebook.com), clone the site by downloading the HTML only file of the target site.





Step2: Prepare a malicious PHP file which is to be replaced by the original file in the Facebook html file.



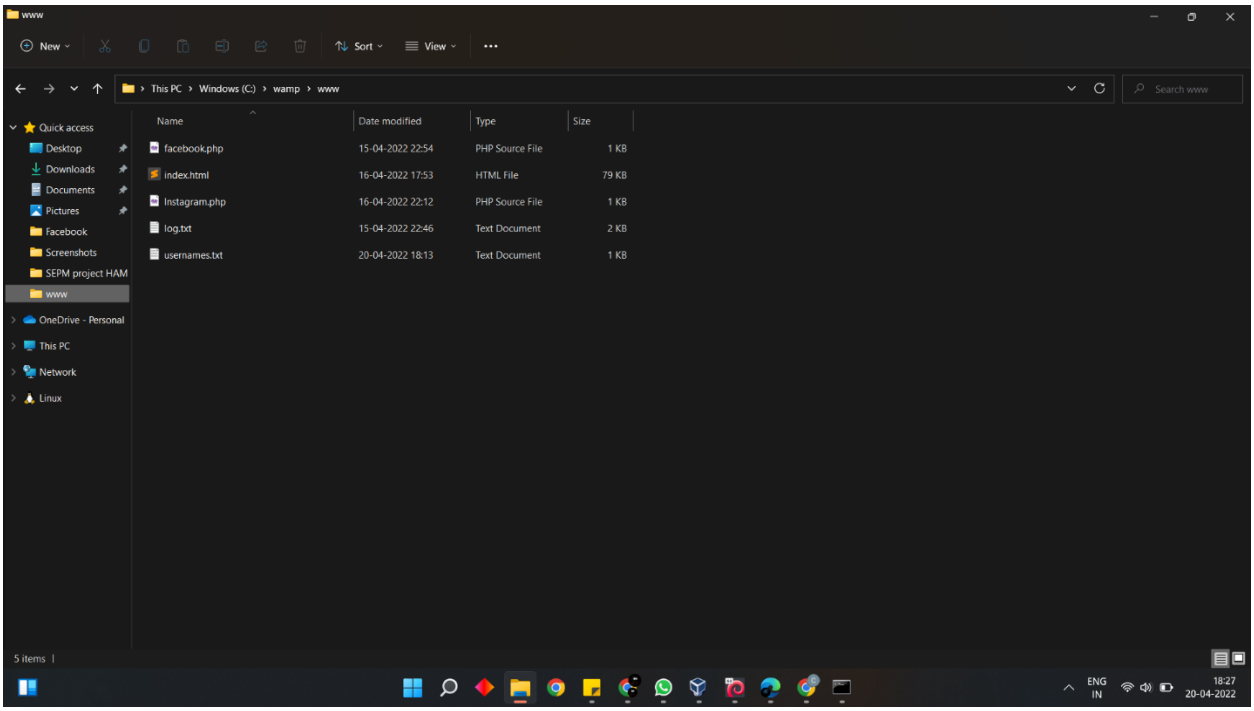


Step3: Prepare an empty log text file to save the entered credentials of the victim.

Step4: Download wamp server to make your own PC a server to host the malicious Facebook file.

Step5: Go to www folder of wamp server and change the previous files to the newly created files:

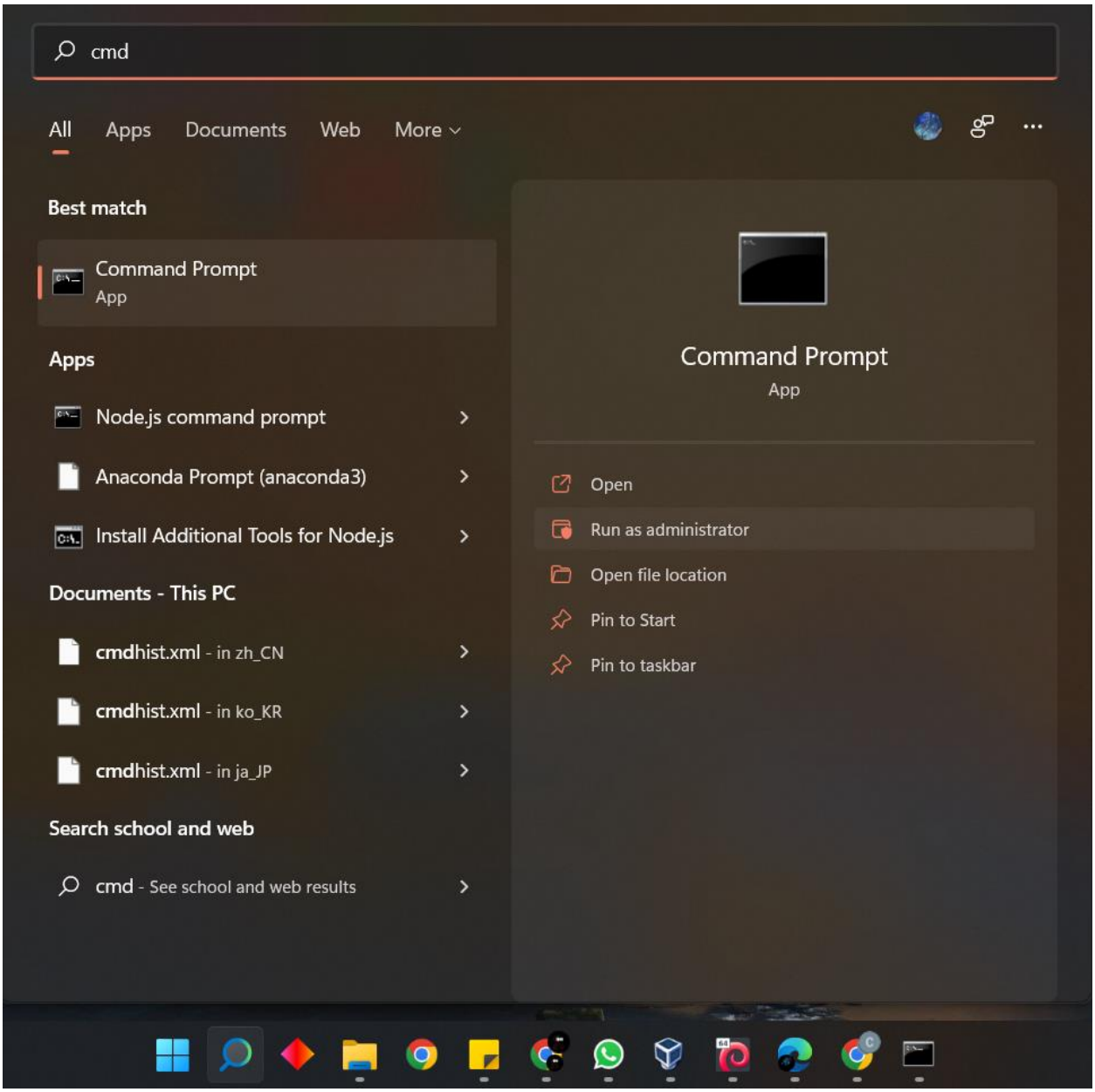
- Facebook HTML file
- PHP file
- Log file

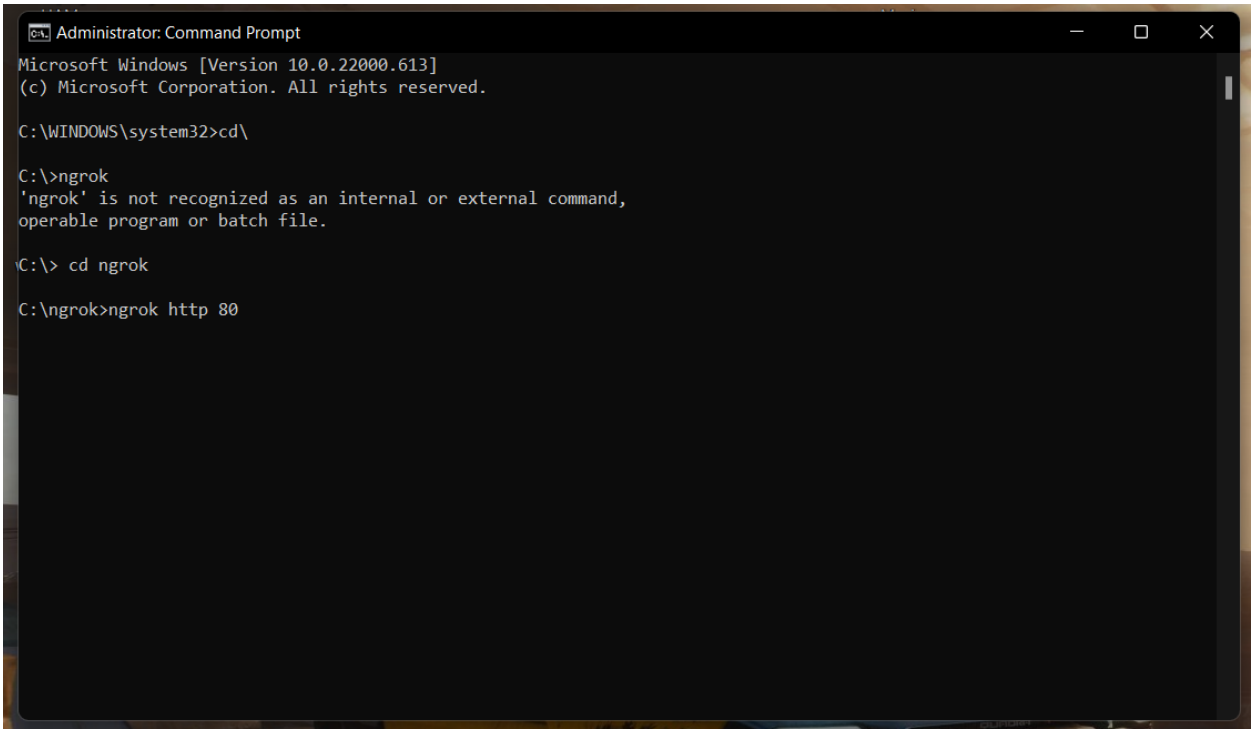


Step6: Start the wamp server and wait for it to turn green.

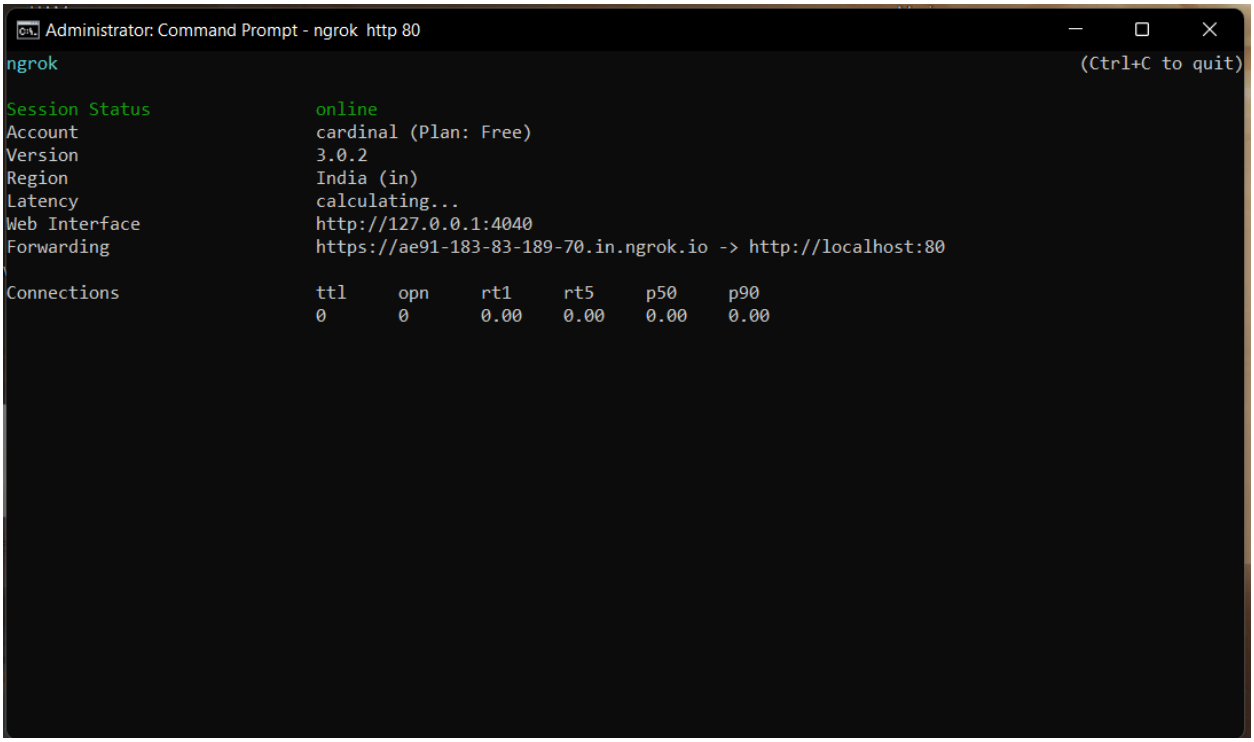
Step7: Download the ngrok application to convert the local ip to public ip.

Step8: Run Command Prompt as administrator and locate the ngrok file. Run the ngrok file (ngrok.exe).

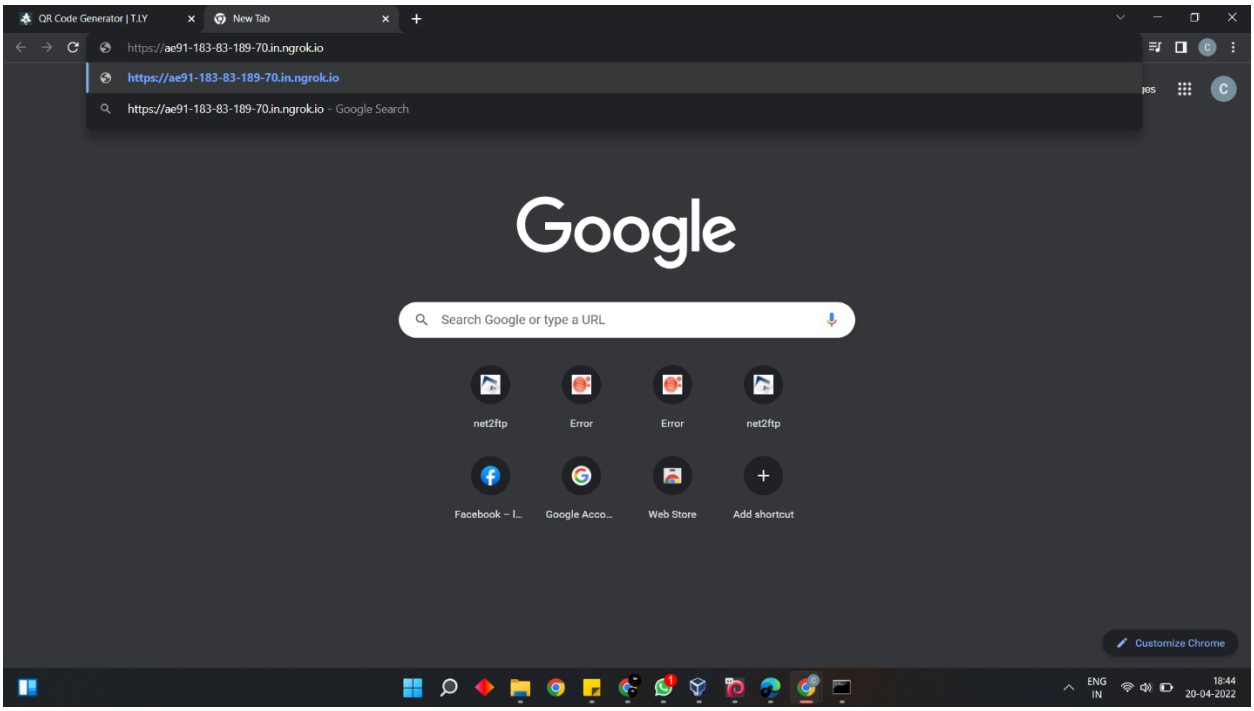

cmd
All
Apps
Documents
Web
More
Best match
Command Prompt
App
Apps
Node.js command prompt
Anaconda Prompt (anaconda3)
Install Additional Tools for Node.js
Documents - This PC
cmdhist.xml - in zh_CN
cmdhist.xml - in ko_KR
cmdhist.xml - in ja_JP
Search school and web
cmd - See school and web results
Command Prompt
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar



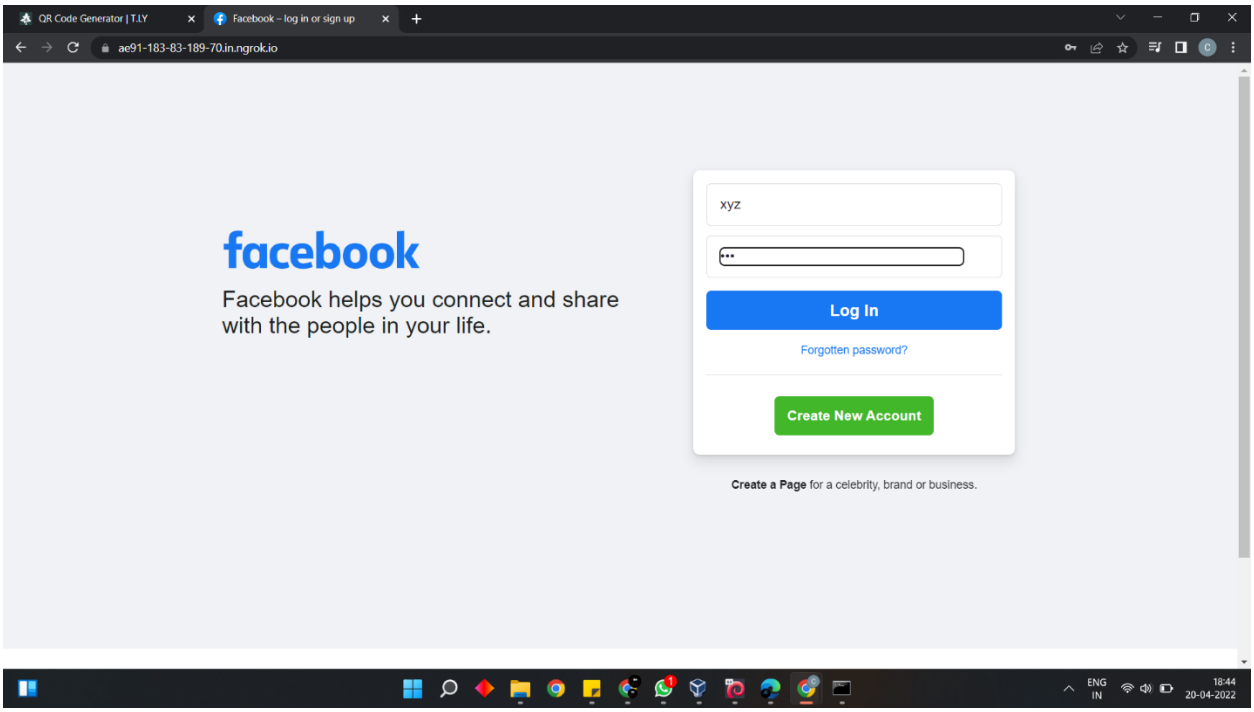
Step9: On execution, enter the command 'ngrok http 80' to convert the local port 80 to public.

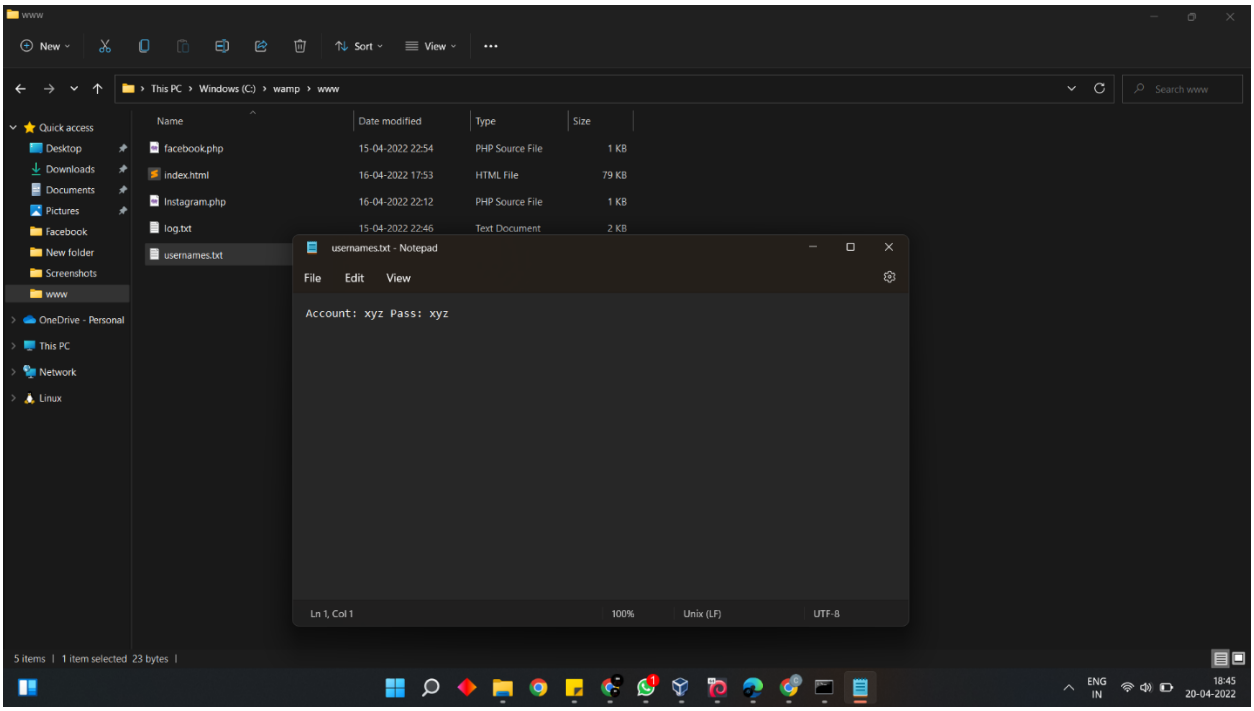


Step10: The malicious Facebook is successfully hosted. Get the link from the ngrok exe file, share it to the victim.



Step11: Once the victim enters the credentials, the login credentials are captured in the empty log file and the user will be redirected to the original Facebook site.





Ways to avoid Desktop Phishing:

- Know what a phishing scam looks like
- Don’t click on that link
- Get free anti-phishing add-ons
- Don’t give your information to an unsecured site
- Rotate passwords regularly
- Don’t ignore the updates
- Install firewalls
- Don’t be tempted by the pop-ups
- Have a data security platform to spot signs of an attack
- Don’t give out important information unless you must
- Verify a site’s security

BY : HARSH JAIN SRM IST