PRACTICAL 7 & 8

Date: 28/02/2025

AIM: Conducting a phishing simulation and analyzing the results to identify potential threats.

Theory:

Zphisher:

A phishing simulation using tools like Zphisher involves creating a fake replica of a legitimate website to deceive users into providing sensitive information, such as login credentials. By cloning an application's login page, setting up a local tunneling service (like LocalXpose), and crafting a convincing message, attackers can lure targets into visiting the fraudulent page, enabling the capture of their credentials. This simulation helps identify vulnerabilities and raises awareness about phishing threats.

Steps:

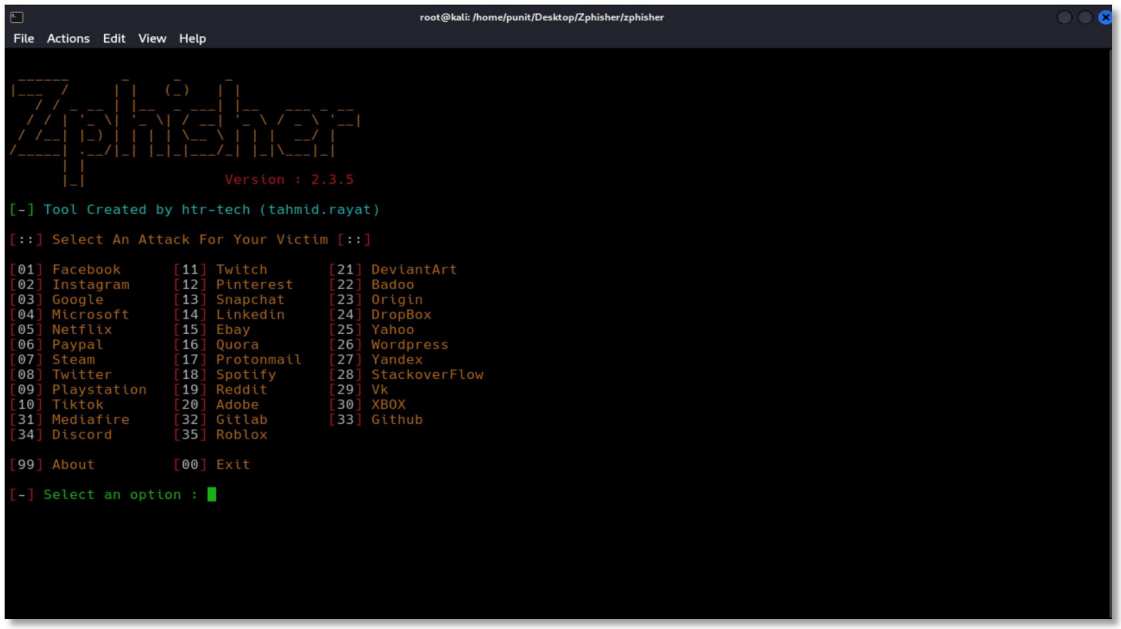
1. Install Zpisher Tool Using Github in Kali Linux.

- **git clone --depth=1 https://github.com/htr-tech/zphisher.git**

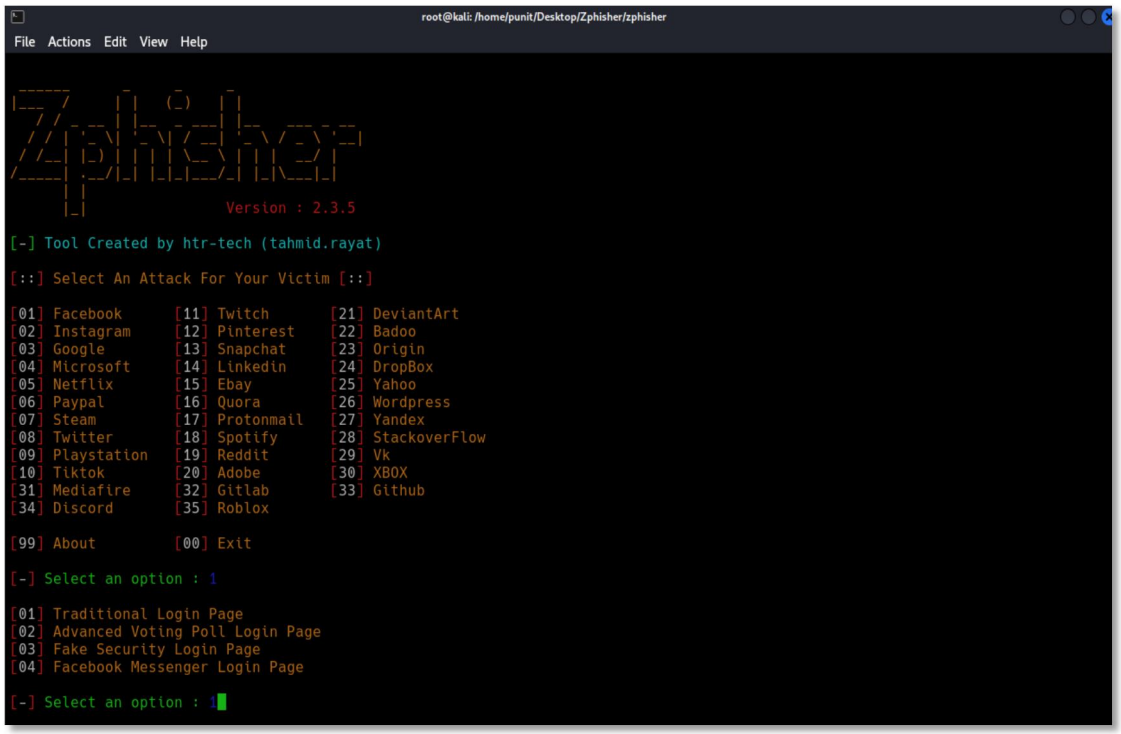
2. Go into Zphisher Directory and run bash File.

- bash zphisher.sh

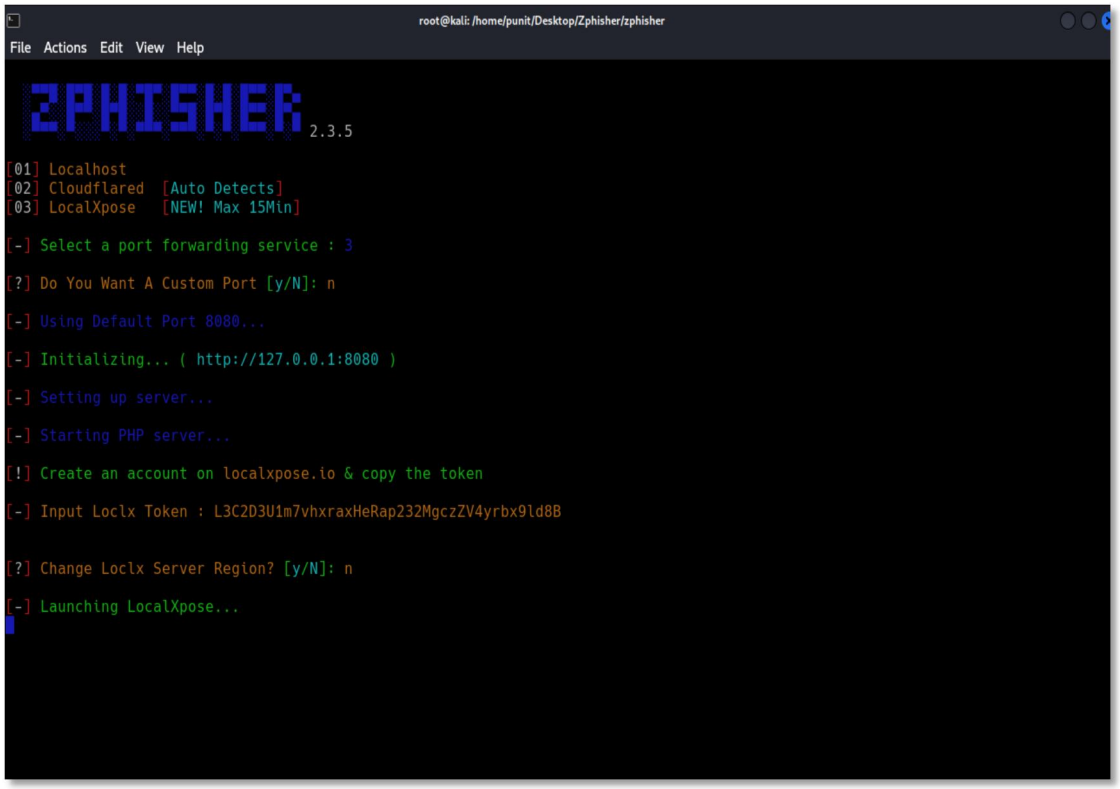
3. Select which application you want to clone.



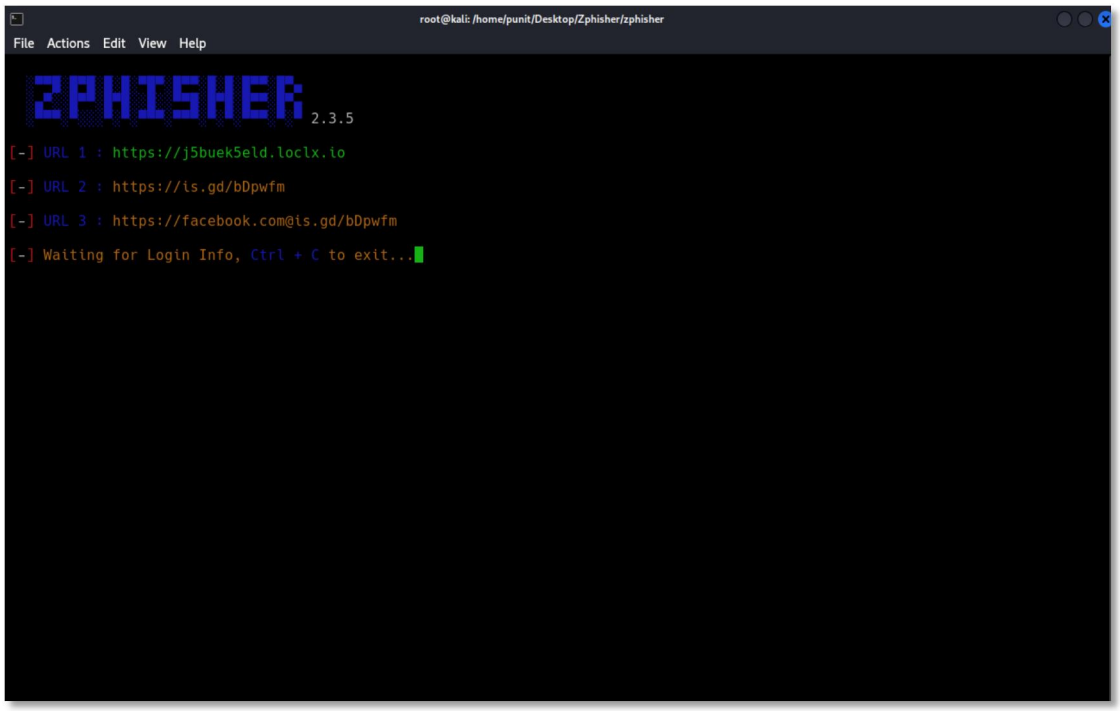
4. Select page of that application.

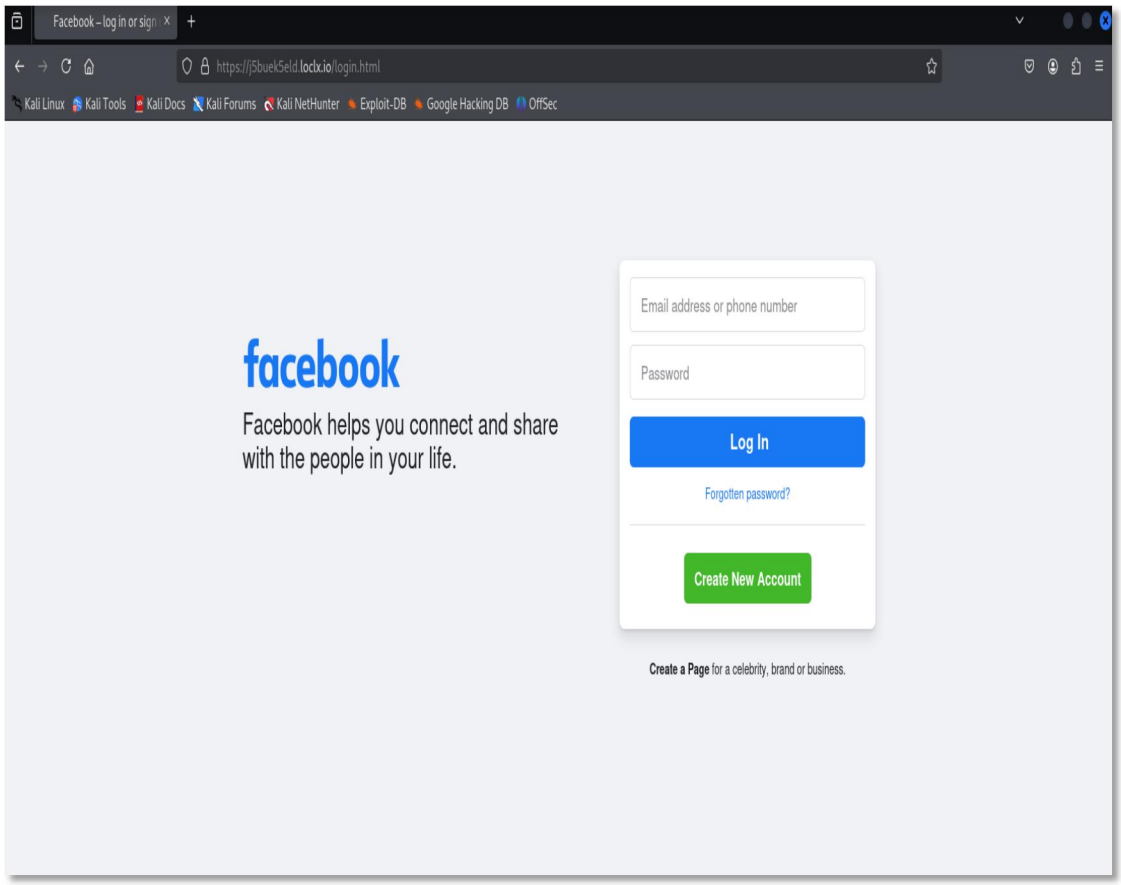


5. Select localxpose and Create account on localxpose using Tempmail and Start the tunnel and Copy the token and Paste it into the terminal.

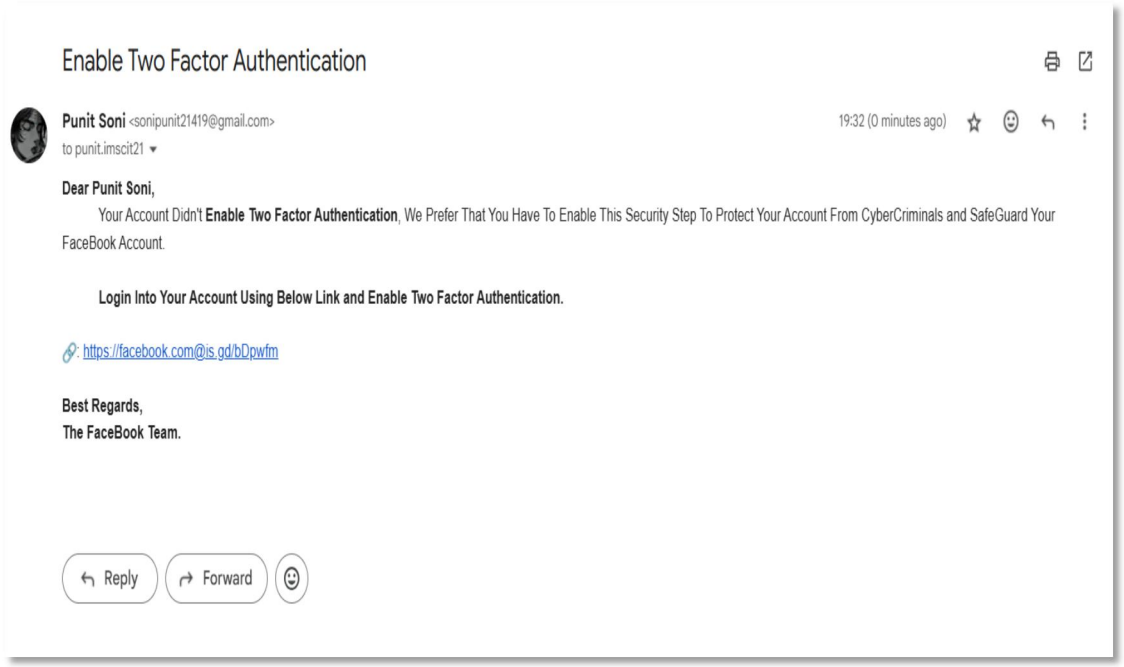


6. Mask URL according to application and you need and open the link.



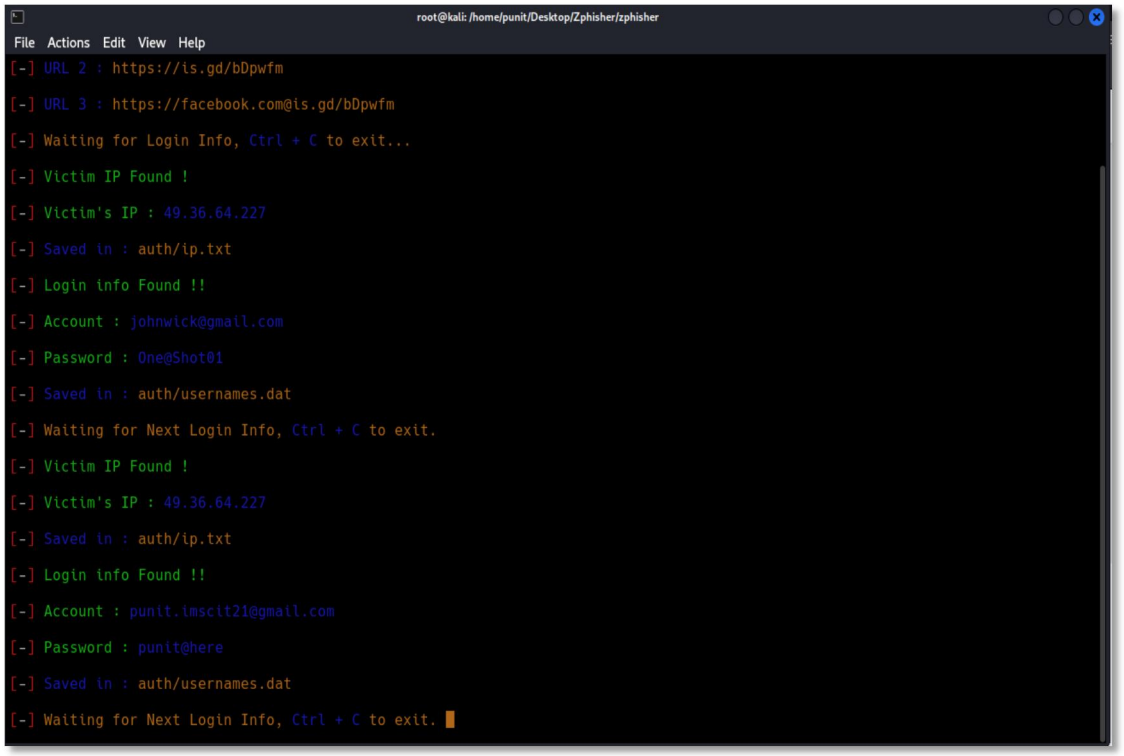


7. Frame a message to trap someone in it to get there credential.

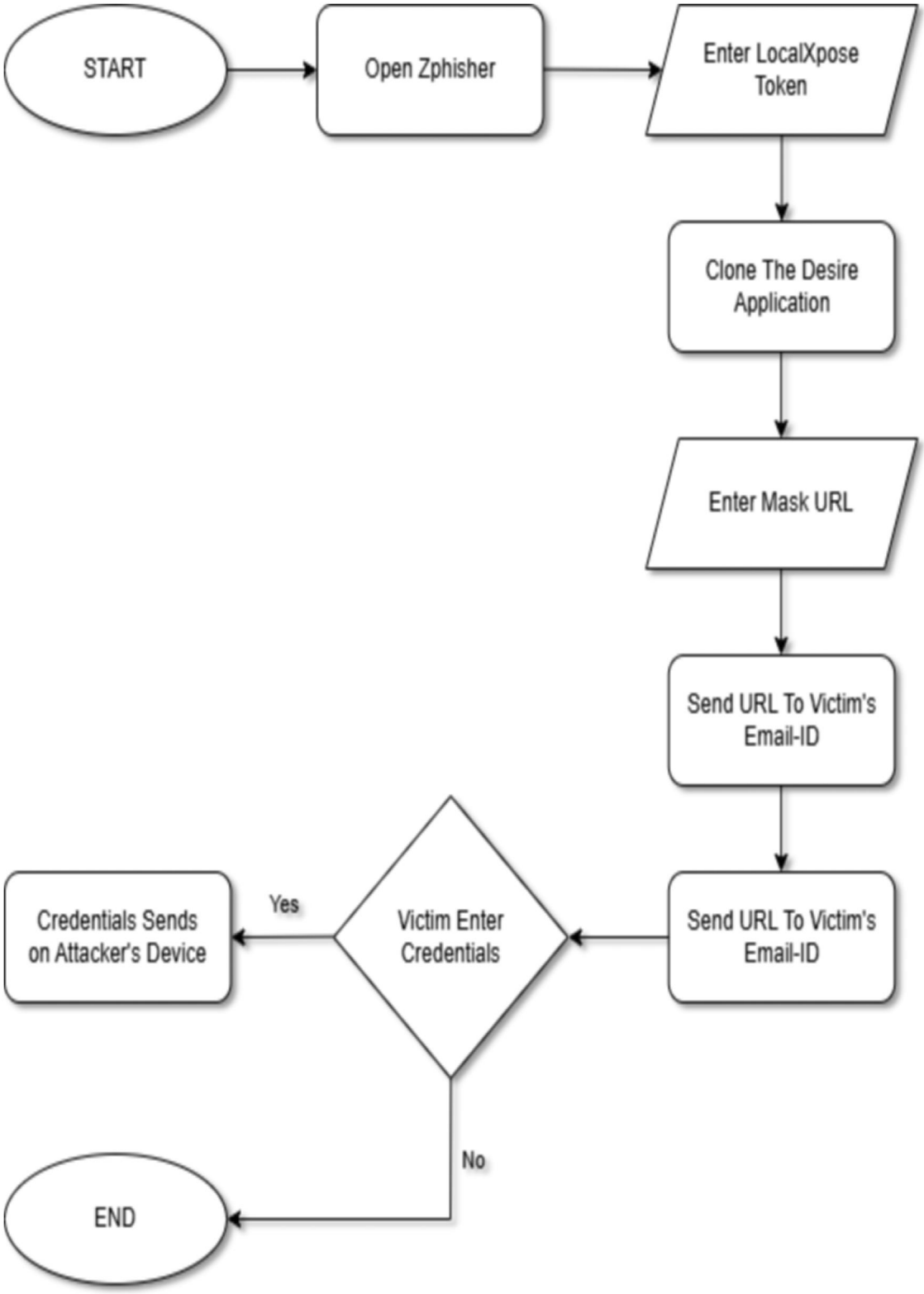


OutPut:

The Victim Entered Their Login Crendential's and that display's on attacker's device.



Phising Email FlowChart Using Zphisher:



Conclusion:

Zphisher is a phishing tool that automates the creation of phishing pages to steal sensitive information, such as login credentials, from unsuspecting individuals. The tool can simulate login pages of popular websites and services, tricking users into entering their personal data, which could then be exploited for malicious purposes. Using a tool like Zphisher to conduct phishing attacks is illegal and unethical.

While Zphisher and similar tools are often used in ethical hacking contexts for educational purposes or penetration testing with explicit consent, their misuse for fraudulent activities constitutes a crime. Engaging in phishing attacks can lead to severe legal consequences, including criminal charges, fines, and imprisonment.