

PHISHING SIMULATION - QR CODE BASED

Objective:

To simulate a phishing attack by creating a QR code that redirects users to a fake Instagram login page hosted locally. This project aims to understand phishing tactics and improve awareness of cybersecurity risks.

Disclaimer:

This project was conducted in a controlled environment strictly for educational and ethical purposes. It complies with ethical hacking practices, and no unauthorized access or malicious intent was involved.

Tools and Technologies:

- **Kali Linux**
- **Zphisher**
- **Qrcode** (QR Code Generator)
- **Localhost Environment**

Steps:

1.Setup Zphisher tool in kali linux terminal:

```
/_____|_./|/_| |__|___/_| |_|\___||  
File Edit View Go Dev Version 2.0  
[+] Tool Created by htr-tech (tahmid.rayat) ZPhisher  
...Select Any Attack for your Victim..  
  
[01] Facebook [11] Twitch [21] DeviantArt  
[02] Instagram [12] Pinterest [22] Badoo  
[03] Google [13] Snapchat [23] Origin  
[04] Microsoft [14] LinkedIn [24] CryptoCoin  
[05] Netflix [15] Ebay [25] Yahooo  
[06] Paypal [16] Dropbox [26] Wordpress  
[07] Steam [17] Protonmail [27] Yandex  
[08] Twitter [18] Spotify [28] StackoverFlow  
[09] Playstation [19] Reddit [29] Vk  
[10] Github [20] Adobe [x] Exit  
[~] Select an option: 02 all Linux 23_10_2020 01_03_00.png  
[01] Traditional Login Page  
[02] Auto Followers Login Page  
[03] Blue Badge Verify Login Page  
[~] Select an option: 01
```

PHISHING SIMULATION - QR CODE BASED

Step2:

- After launching the Z phisher tool there will be multiple Attacks appears in the list.
- I have selected option **02 – Instagram .**
- Then another list appears, asks to select the login page then I selected the option **01 - Traditional Login Page.**
- After Selecting the login page it asked the port forwarding option to launch the attack then I selected to launch it in my **local Machine(Local Host)**, because I have done it ethically in my own machine and I have no intention to steal others credentials.

```
network
[01] LocalHost
[02] Ngrok.io
[03] Serveo.net
[04] Localhost.run

PHISHING.PPT.webp
phishing.zip
phishing-7487504_192.png
README.md

[~] Select a Port Forwarding option: 01

[~] Select a Port (Default: 5555 ):

[~] Initializing...(localhost:5555)

[~] Successfully Hosted at : http://localhost:5555

[~] Waiting for Login Info, Ctrl + C to exit.
```

- After selecting local host it was hosted in local host and the web address is <http://localhost:5555>.

Step3:

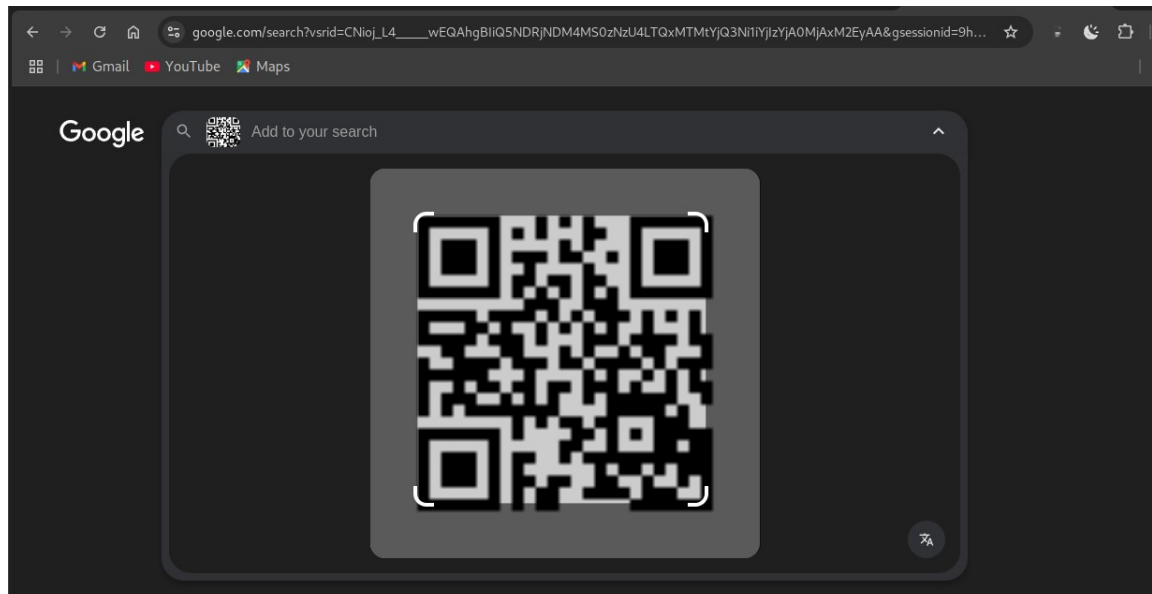
- The next step is to generate a qr code containing the local host link <http://localhost:5555> using qrcode command.

```
(deviprasad@Devi)-[~]
$ qrcode -o qrcode1.png http://localhost:5555

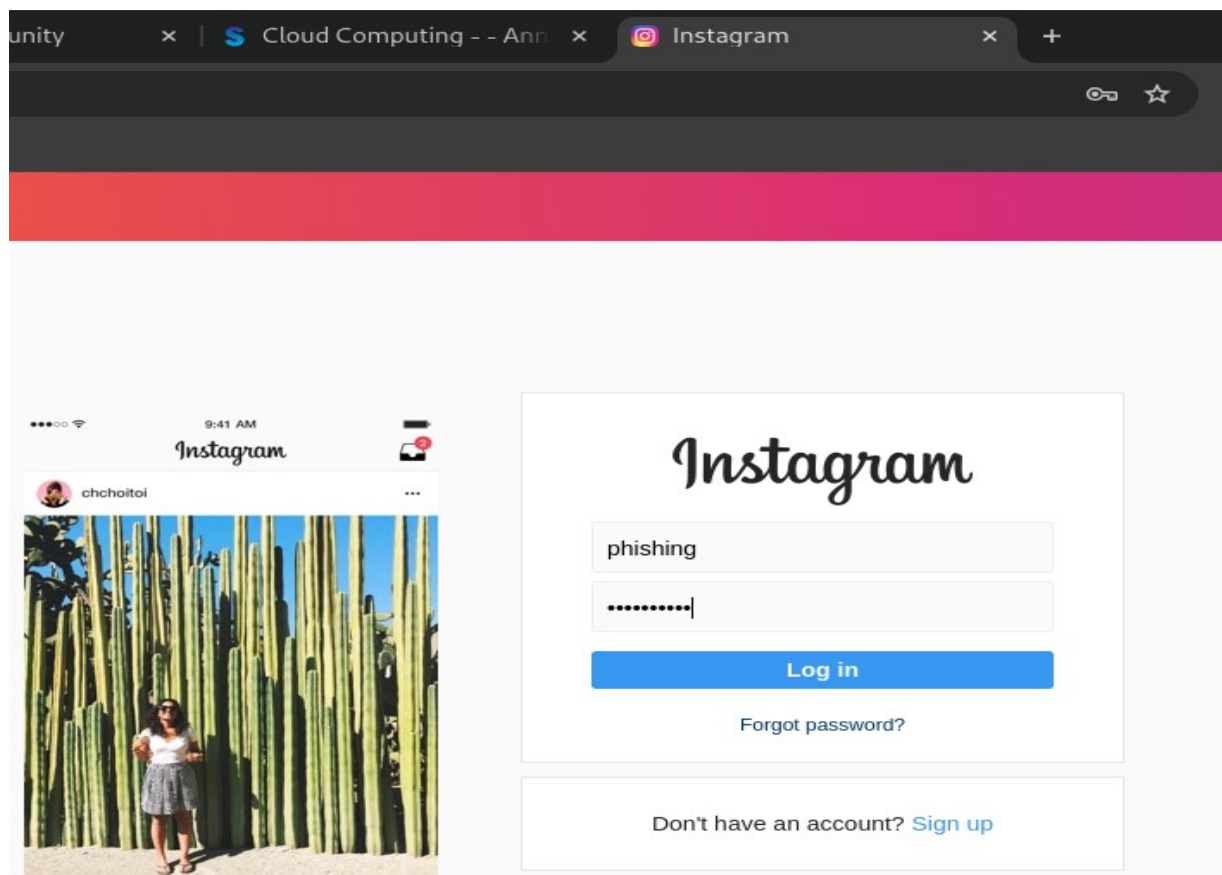
(deviprasad@Devi)-[~]
$
```

PHISHING SIMULATION - QR CODE BASED

4. Simulate the Phishing Attack:

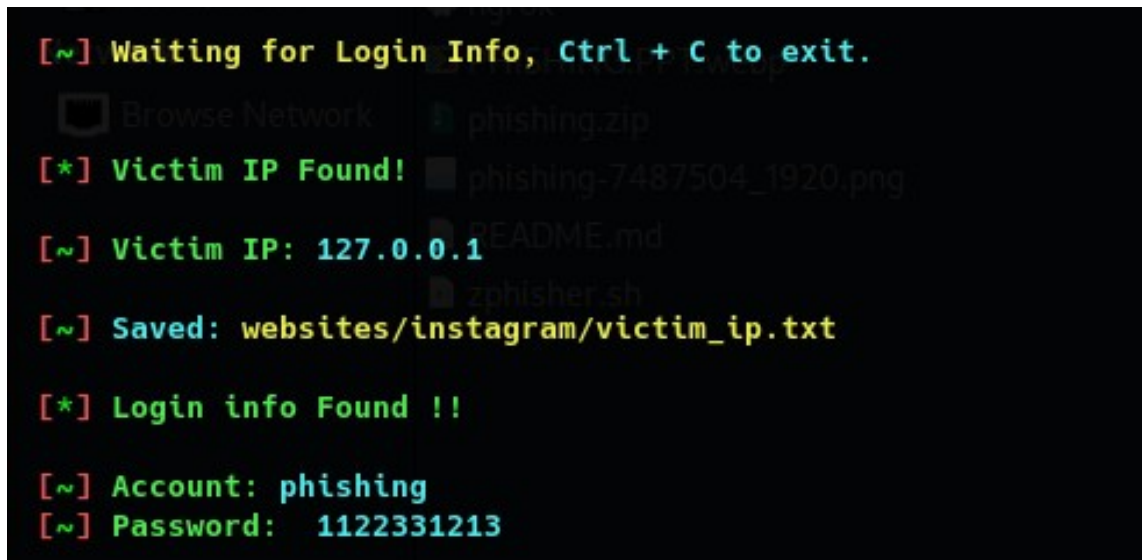


- Scanned the QR code .
- When the QR code was scanned, it redirected to the phishing page hosted on the localhost machine.



PHISHING SIMULATION - QR CODE BASED

- Observed and logged credentials entered into the phishing page using Zphishers built-in logging system.

A screenshot of a terminal window with a black background and multi-colored text. The text shows the Zphisher application's internal logs. It starts with a prompt '[~] Waiting for Login Info, Ctrl + C to exit.' followed by a file browser icon and 'phishing.zip'. Then, it shows '[*] Victim IP Found!' followed by a file icon and 'phishing-7487504_1920.png'. Next is '[~] Victim IP: 127.0.0.1' followed by a file icon and 'README.md'. This is followed by '[~] Saved: websites/instagram/victim_ip.txt' and '[*] Login info Found !!'. The final two lines are '[~] Account: phishing' and '[~] Password: 1122331213'.

```
[~] Waiting for Login Info, Ctrl + C to exit.
Browse Network phishing.zip
[*] Victim IP Found! phishing-7487504_1920.png
[~] Victim IP: 127.0.0.1 README.md
[~] Saved: websites/instagram/victim_ip.txt
[*] Login info Found !!
[~] Account: phishing
[~] Password: 1122331213
```

- I have got the login credentials that I entered are shown in the above screenshot.

Observations:

- **Effectiveness:** The QR code successfully redirected to the fake Instagram login page when scanned.
- **Captured Data:** All credentials entered on the phishing page were logged in Zphisher logs.
- **Environment Scope:** The attack was limited to my device due to the localhost setup.

Learnings:

1. Phishing with QR Codes:

- QR codes can act as an effective medium for phishing attacks, especially in trusted environments.
- Users are less likely to scrutinize URLs when scanning QR codes.

PHISHING SIMULATION - QR CODE BASED

2.Defense Mechanisms:

- Verify URLs after scanning a QR code.
- Avoid scanning QR codes from untrusted sources.
- Implement browser alerts for unsafe pages and two-factor authentication (2FA).

3.Limitations:

- Hosting the phishing site on localhost restricted the scope to the local machine/network.
- Wider attacks would require port forwarding or external hosting tools.

Conclusion:

This project demonstrates the potential of phishing attacks via QR codes within a controlled local environment. It emphasizes the importance of raising awareness about such threats and promoting cybersecurity best practices.

Safety Note:

This project is intended purely for educational purposes. Phishing attacks are illegal and unethical when conducted without proper authorization. Always use such knowledge responsibly and for defending against cyber threats. Cybersecurity professionals have a responsibility to protect, not exploit.

- Deviprasad.