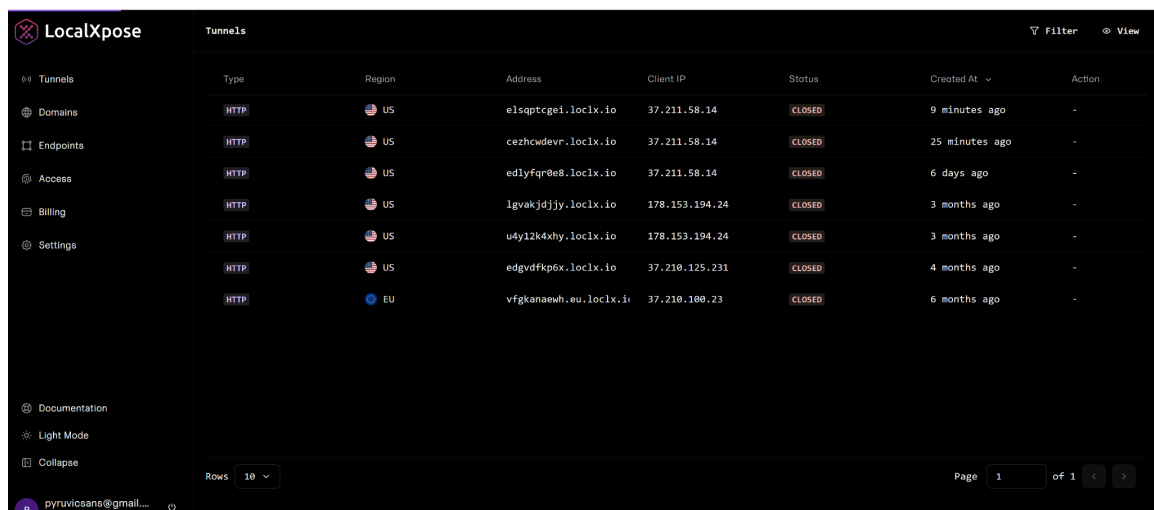


Steps In Generating a WordPress Phishing Link with Zphisher

This document records the exact steps I followed to build and deliver a WordPress-style phishing page for an internal security exercise.

1 · Prerequisites I Confirmed

- I prepared a dedicated Kali Linux VM with outbound Internet access.
- I secured written approval and defined scope for the simulation.
- I set up a Localxpose account for external port forwarding.



The screenshot shows the LocalXpose web interface. On the left is a sidebar with navigation links: Tunnels, Domains, Endpoints, Access, Billing, Settings, Documentation, Light Mode, and Collapse. The main area is titled 'Tunnels' and contains a table with the following columns: Type, Region, Address, Client IP, Status, Created At, and Action. The table lists seven tunnels, all with a status of 'CLOSED'. The bottom of the interface shows 'Rows 10', 'Page 1 of 1', and a user profile for 'pyruvicasana@gmail...'.

Type	Region	Address	Client IP	Status	Created At	Action
HTTP	US	elsqptcgei.loc1x.io	37.211.58.14	CLOSED	9 minutes ago	-
HTTP	US	cezhcwevvr.loc1x.io	37.211.58.14	CLOSED	25 minutes ago	-
HTTP	US	edlyfqr0e8.loc1x.io	37.211.58.14	CLOSED	6 days ago	-
HTTP	US	lgvakjdjyy.loc1x.io	178.153.194.24	CLOSED	3 months ago	-
HTTP	US	u4y12k4xhy.loc1x.io	178.153.194.24	CLOSED	3 months ago	-
HTTP	US	edgvdffkp6x.loc1x.io	37.210.125.231	CLOSED	4 months ago	-
HTTP	EU	vfgkanaewh.eu.loc1x.io	37.210.100.23	CLOSED	6 months ago	-

2 · Installing Zphisher

- I cloned the project to my home directory: `git clone https://github.com/htr-tech/zphisher.git ~/zphisher``.
- I confirmed the script launched without errors: `~/zphisher/zphisher.sh -h``.

```
(kali㉿kali)-[~]  
$ git clone https://github.com/htr-tech/zphisher.git  
Cloning into 'zphisher' ...  
remote: Enumerating objects: 1801, done.  
remote: Total 1801 (delta 0), reused 0 (delta 0), pack-reused  
1801 (from 1)  
Receiving objects: 100% (1801/1801), 28.68 MiB | 3.36 MiB/s, d  
one.  
Resolving deltas: 100% (817/817), done.  
  
(kali㉿kali)-[~]  
$ █
```

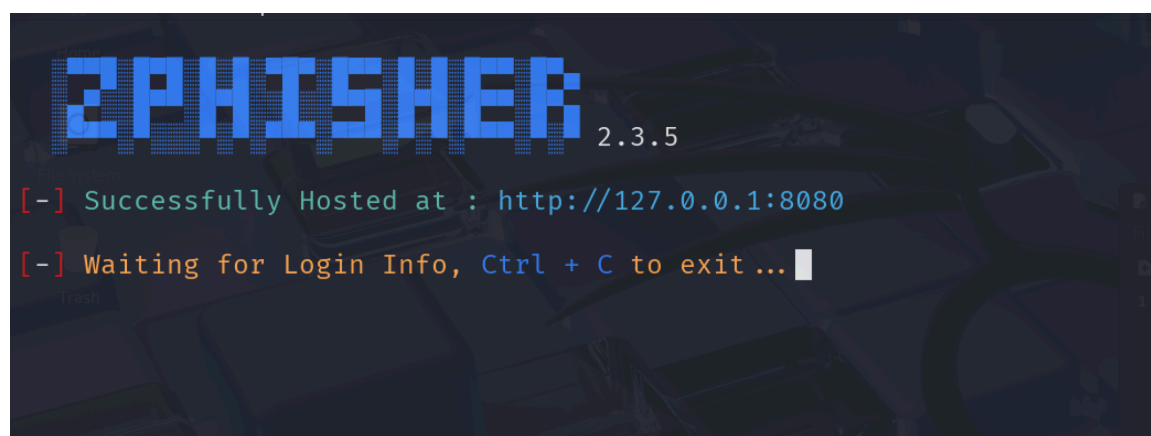
3 · Launching Zphisher

- I changed into the tool directory: ``cd ~/zphisher``.
- I started the script with sudo: ``sudo ./zphisher.sh``.



4 · Selecting or Importing the WordPress Template

- I chose the WordPress login template (option number displayed as 26 in my session).
- Zphisher presented a local URL, `http://127.0.0.1:8080` which I noted for the email.



5 · Sending the Phishing Email

- I drafted the payment-reminder email in the corporate mail client.
- I embedded the link behind a “link” button.
- I scheduled mail delivery during business hours for authenticity.

Hi Alex,

I hope this message finds you well. I am writing to remind you that the payment for the WordPress services provided on your domain cyberttech.com is now due. As per our agreement, the total amount of \$4000 was to be settled by 29TH June, 2025.

We value our relationship and are committed to providing you with the best service possible. If you have already made the payment, please disregard this message. Otherwise, I kindly ask you to arrange for the payment at your earliest convenience.

Please click on this [link](#) if you have any questions or need further details regarding the invoice.

Thank you for your attention to this matter, and I look forward to continuing our successful collaboration.

Warm regards,

Wordpress team.

6· Monitoring Interaction

- I monitored the credential log
- I captured logs for each link click submission.

```
[ - ] Waiting for Login Info, Ctrl + C to exit ...
[ - ] Victim IP Found!
[ - ] Victim's IP : 127.0.0.1
[ - ] Saved in : auth/ip.txt
[ - ] Login info Found !!
[ - ] Account : alex@gmail.com
[ - ] Password : cybertech1234@
[ - ] Saved in : auth/usernames.dat
[ - ] Waiting for Next Login Info, Ctrl + C to exit. █
```

7· Terminating and Cleaning Up

- I stopped Zphisher with `CTRL+C`.
- I closed the localhost with `CTRL+C` if it was running.

```
[ - ] Saved in : auth/usernames.dat
[ - ] Waiting for Next Login Info, Ctrl + C to exit. ^C
[!] Program Interrupted.

(kali@kali)-[~/zphisher]
$ █
```

8· Next Steps

- I analysed the KPI data (clicks, credential submissions, reports) in Google Sheets.
- I included the findings in the final simulation report and updated the risk register.

Measured outcomes			
KPI	Baseline (before-campaign)		Post-Campaign
Link clicks	80%		30%
credential submission	60%		20%
reports	10%		80%

Prepared By: Olalekan Ibikunle (Cybersecurity Analyst)