Phishing Security Awareness Training Simulation Report

Cybersecurity Audit Project – Employee Vigilance Assessment

Organisation: Cyberttech

Date: NOV 26,2025

Prepared By: JARINAT KAREEM (Cybersecurity Analyst)

1 · Overview

A phishing simulation was conducted across Sales (30 employees), Marketing (40 employees), and IT (35 employees) to evaluate the effectiveness of prior phishing awareness training.

The exercise simulated a credential-harvesting phishing campaign using a cloned login portal. Results demonstrated a positive trend in employee vigilance:

- Click rates were relatively low (14–20%),
- Credential submissions were minimal (0–1 total),
- Reporting rates increased significantly, especially in Marketing and IT.

These findings show measurable improvement in security culture, with fewer risky behaviors and stronger reporting habits.

2 · Objectives

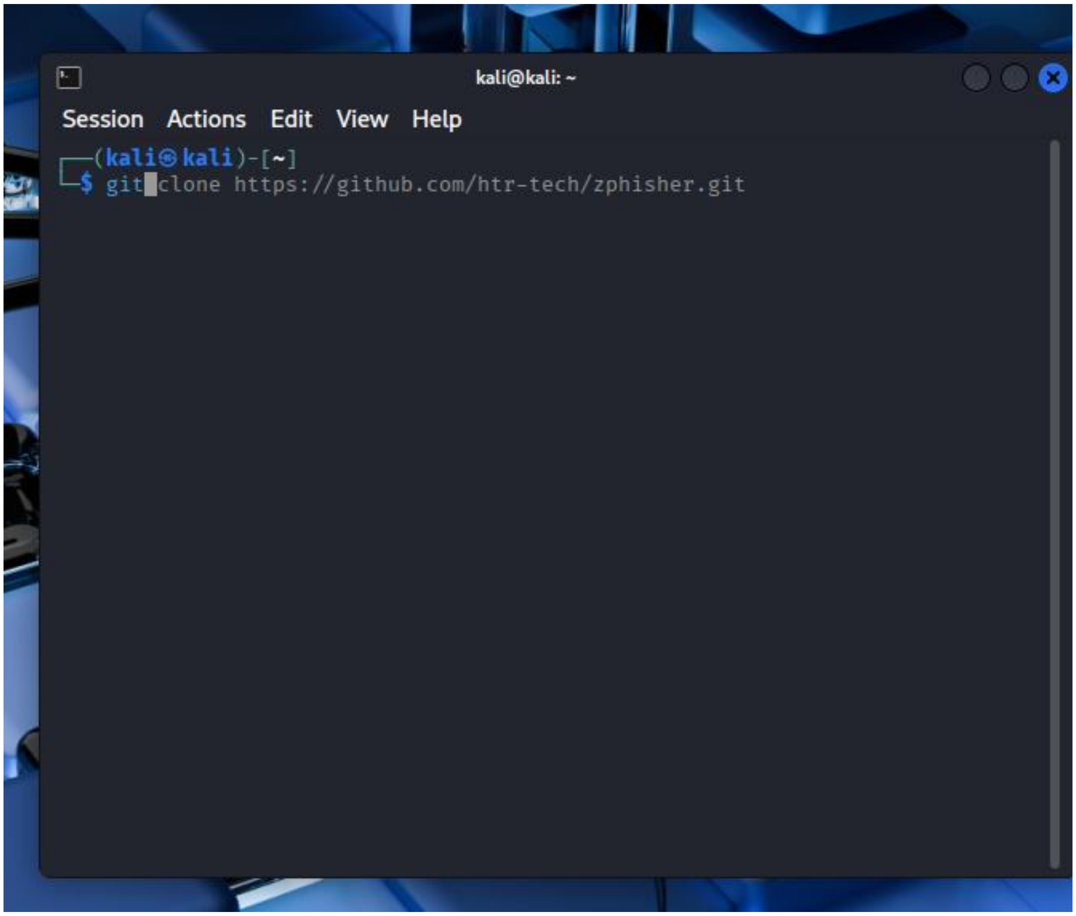
- Lower link-click rate among targeted employees.
- Increase phishing incident reports submitted to the security team.
- Reduce credential submission attempts on the phishing landing page.

3 · Compliance Drivers

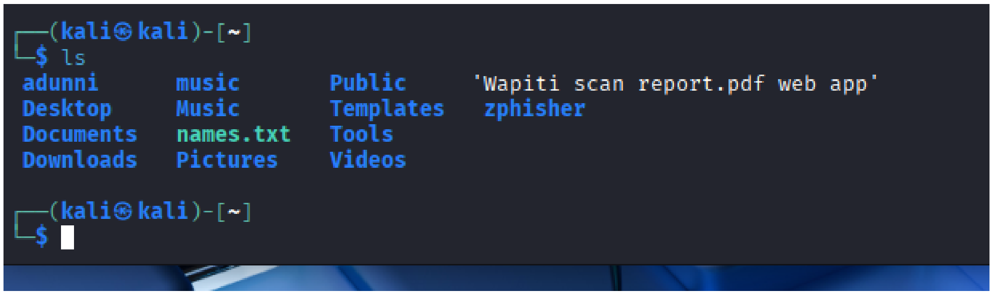
- ISO 27001 A.7.2.2 (Awareness, Education & Training): This simulation evidences employee awareness testing and supports continuous improvement.
- Internal Risk Register: Addresses phishing risks identified as a top threat vector.

4 · Tooling

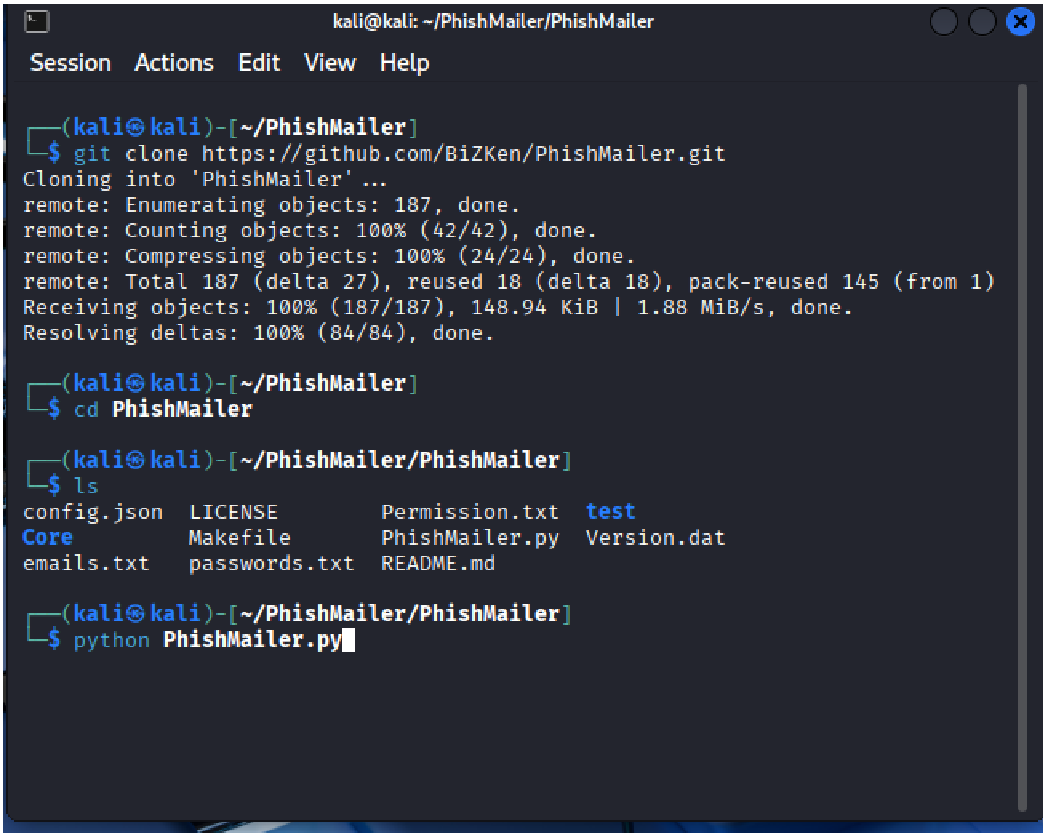
- Zphisher – generated the phishing site and captured interaction data.
- Localxpose – optional port-forwarding for internal access during testing.
- Google Sheets – stored key performance indicators.



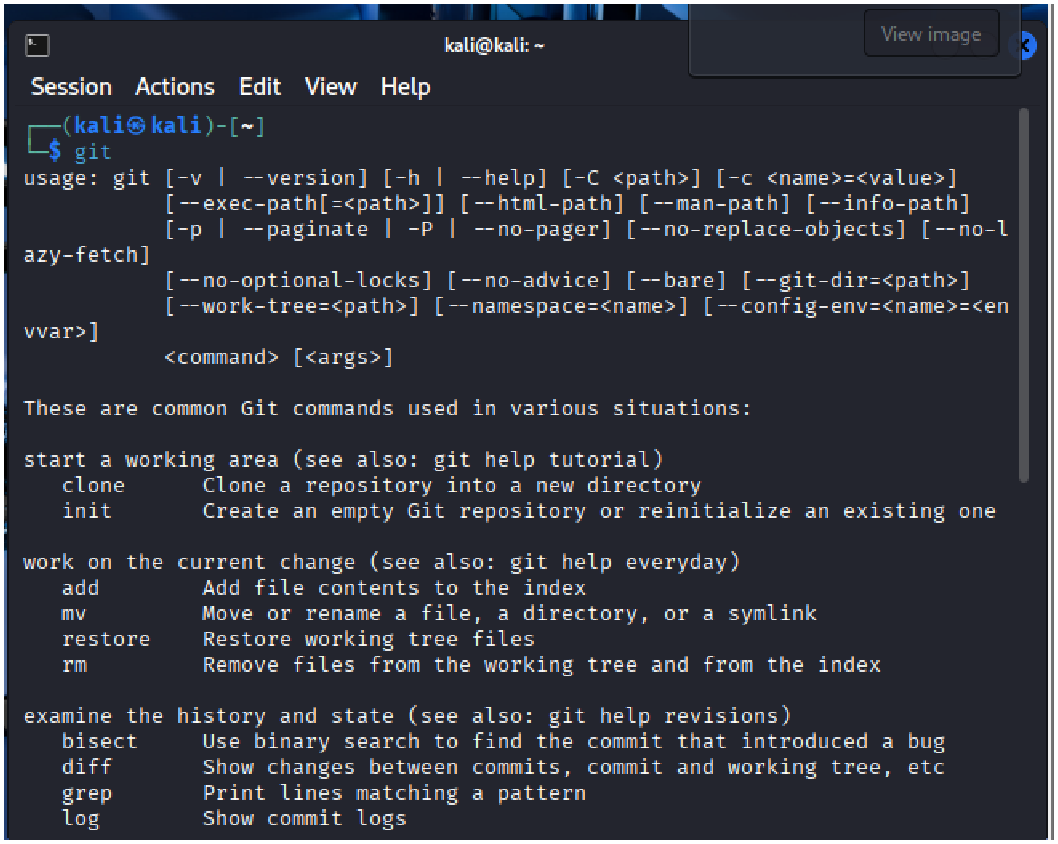
```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/htr-tech/zphisher.git
```



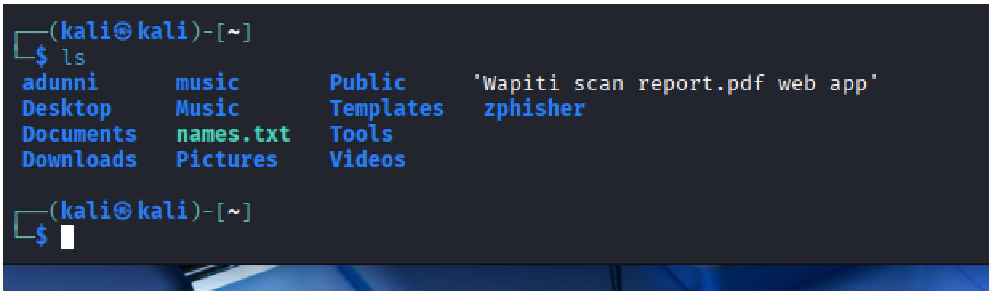
```
┌──(kali㉿kali)-[~]
└─$ ls
adunni      music      Public     'Wapiti scan report.pdf web app'
Desktop     Music      Templates   zphisher
Documents   names.txt  Tools
Downloads   Pictures   Videos

┌──(kali㉿kali)-[~]
└─$ 
```



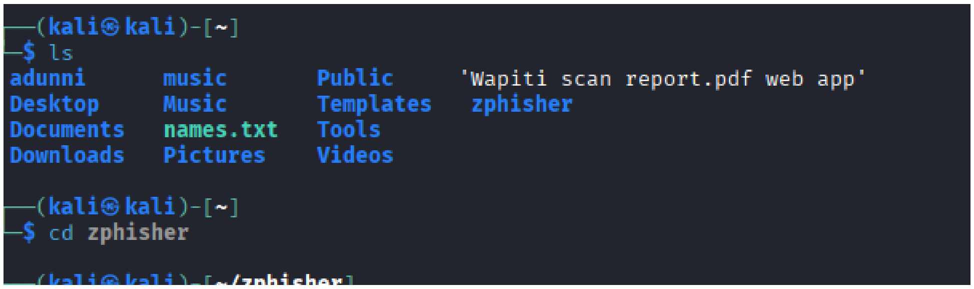
```
┌──(kali㉿kali)-[~/PhishMailer]
└─$ git clone https://github.com/BiZKen/PhishMailer.git
Cloning into 'PhishMailer'...
remote: Enumerating objects: 187, done.
remote: Counting objects: 100% (42/42), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 187 (delta 27), reused 18 (delta 18), pack-reused 145 (from 1)
Receiving objects: 100% (187/187), 148.94 KiB | 1.88 MiB/s, done.
Resolving deltas: 100% (84/84), done.

┌──(kali㉿kali)-[~/PhishMailer]
└─$ cd PhishMailer

┌──(kali㉿kali)-[~/PhishMailer/PhishMailer]
└─$ ls
config.json  LICENSE        Permission.txt  test
Core         Makefile       PhishMailer.py  Version.dat
emails.txt   passwords.txt  README.md

┌──(kali㉿kali)-[~/PhishMailer/PhishMailer]
└─$ python PhishMailer.py
```



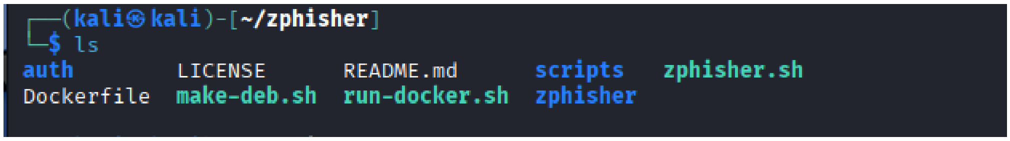
```
┌──(kali㉿kali)-[~]
└─$ git
usage: git [-v | --version] [-h | --help] [-C <path>] [-c <name>=<value>]
           [--exec-path[=<path>]] [--html-path] [--man-path] [--info-path]
           [-p | --paginate | -P | --no-pager] [--no-replace-objects] [--no-l
azy-fetch]
           [--no-optional-locks] [--no-advice] [--bare] [--git-dir=<path>]
           [--work-tree=<path>] [--namespace=<name>] [--config-env=<name>=<en
vvar>]
           <command> [<args>]

These are common Git commands used in various situations:

start a working area (see also: git help tutorial)
   clone      Clone a repository into a new directory
   init       Create an empty Git repository or reinitialize an existing one

work on the current change (see also: git help everyday)
   add        Add file contents to the index
   mv         Move or rename a file, a directory, or a symlink
   restore    Restore working tree files
   rm         Remove files from the working tree and from the index

examine the history and state (see also: git help revisions)
   bisect     Use binary search to find the commit that introduced a bug
   diff       Show changes between commits, commit and working tree, etc
   grep       Print lines matching a pattern
   log        Show commit logs
```



```
┌──(kali㉿kali)-[~]
└─$ ls
adunni      music      Public     'Wapiti scan report.pdf web app'
Desktop     Music      Templates   zphisher
Documents   names.txt  Tools
Downloads   Pictures   Videos

┌──(kali㉿kali)-[~]
└─$ █
```

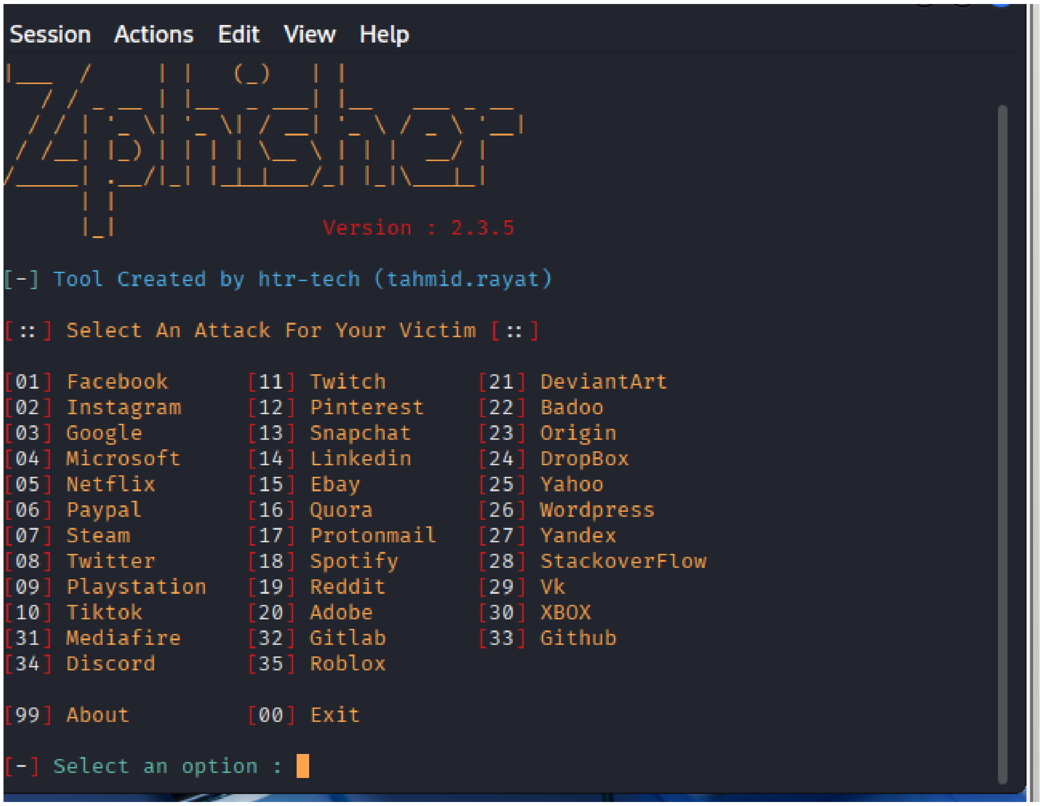


```
──(kali㉿kali)-[~]
─$ ls
adunni      music      Public     'Wapiti scan report.pdf web app'
Desktop     Music      Templates   zphisher
Documents   names.txt  Tools
Downloads   Pictures   Videos

──(kali㉿kali)-[~]
─$ cd zphisher

──(kali㉿kali)-[~/zphisher]
```

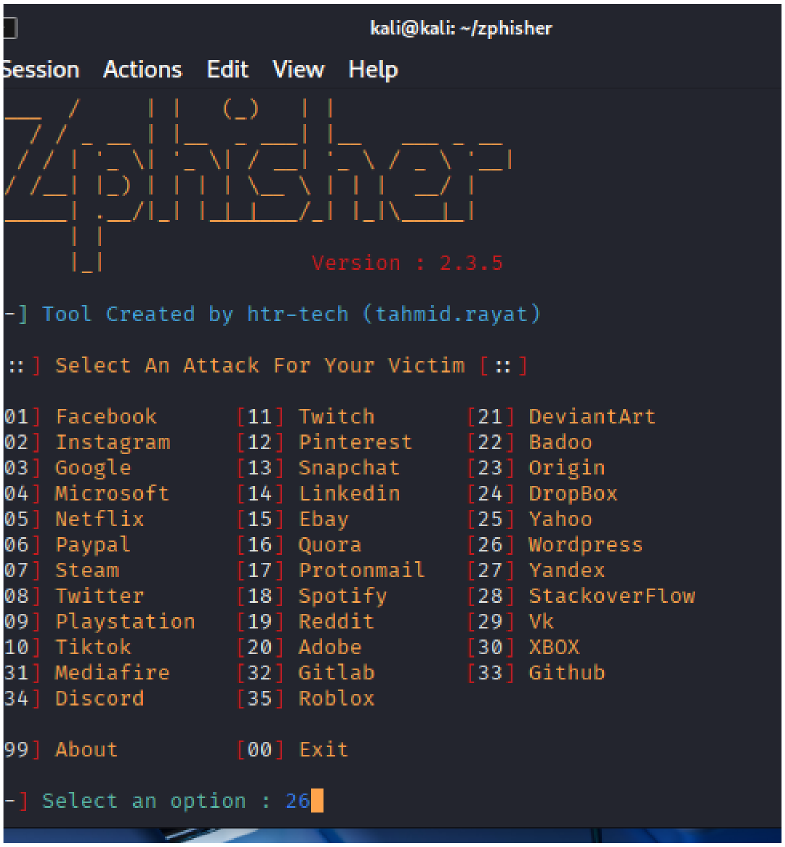


```
┌──(kali㉿kali)-[~/zphisher]
└─$ ls
auth        LICENSE      README.md     scripts   zphisher.sh
Dockerfile  make-deb.sh  run-docker.sh zphisher
```

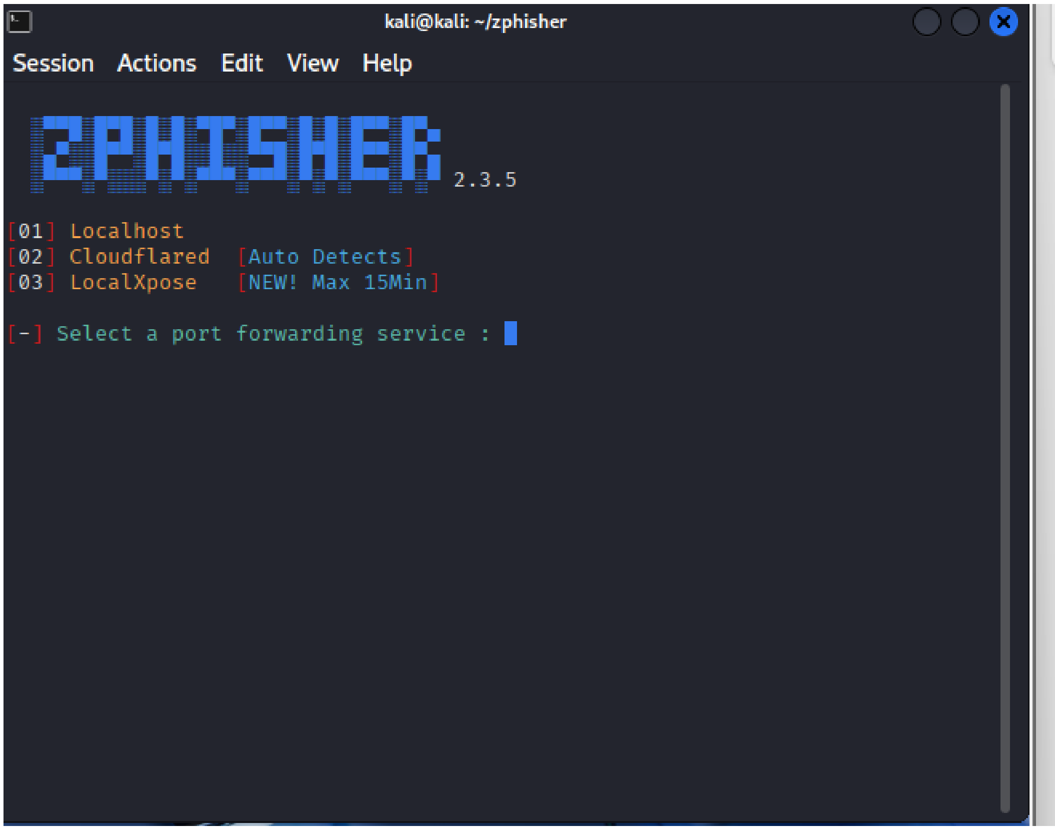
bath



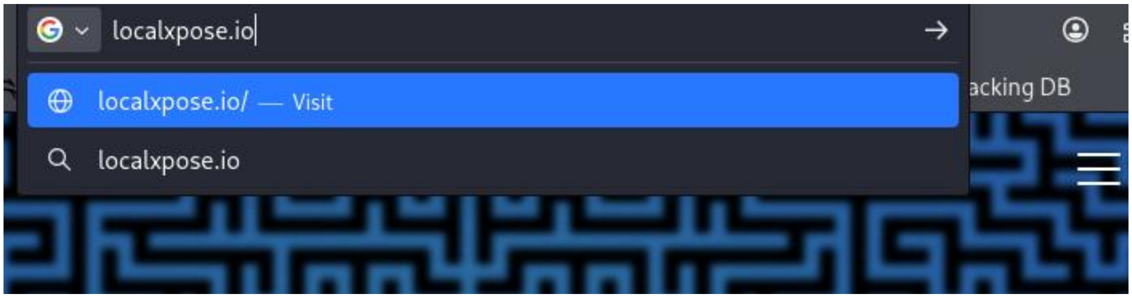
```
|___  /     | |   (_)   | |
   / / _ __ | |__  _ ___| |__   ___ _ __
  / / | '_ \| '_ \| / __| '_ \ / _ \ '__|
 / /__| |_) | | | | \__ \ | | |  __/ |
/_____| .__/|_| |_|_|___/_| |_|\___|_|
      | |
      |_|                Version : 2.3.5

[-] 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] Vk
[10] Tiktok        [20] Adobe         [30] XBOX
[31] Mediafire     [32] Gitlab        [33] Github
[34] Discord       [35] Roblox

[99] About         [00] Exit

[-] Select an option :
```

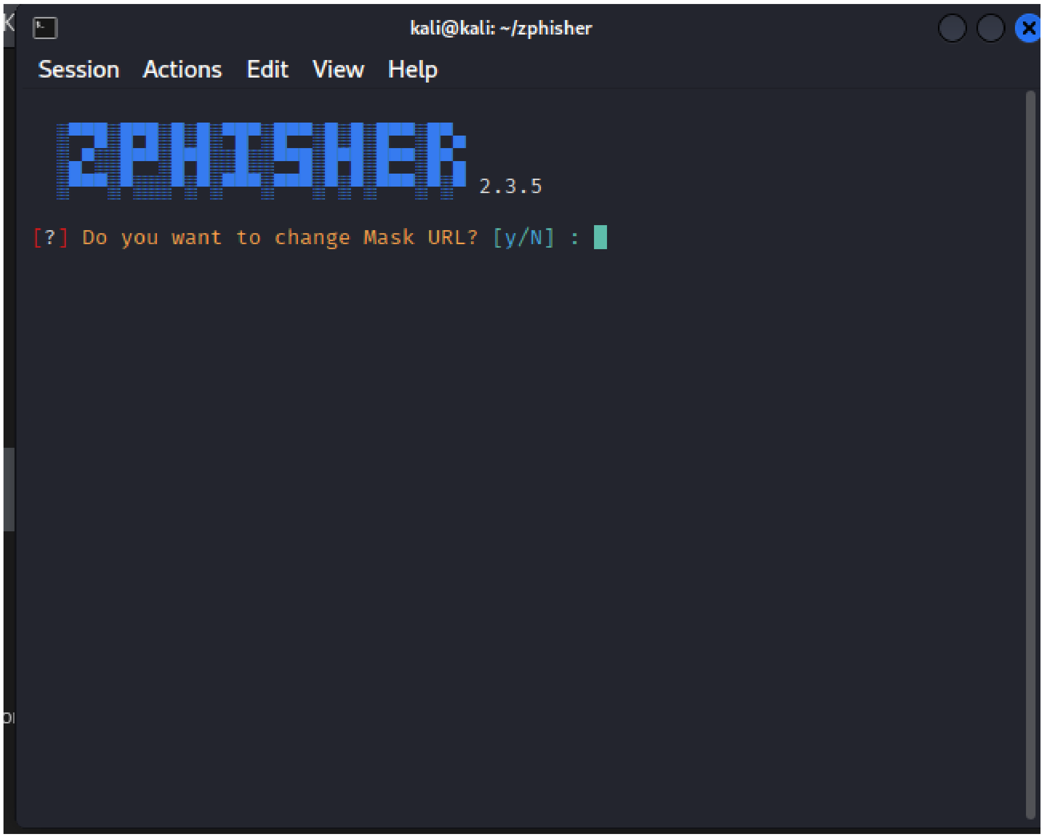


```
___  /     | |   (_)   | |
  / / _ __ | |__  _ ___| |__   ___ _ __
 / / | '_ \| '_ \| / __| '_ \ / _ \ '__|
/ /__| |_) | | | | \__ \ | | |  __/ |
_____| .__/|_| |_|_|___/_| |_|\___|_|
     | |
     |_|                Version : 2.3.5

-] 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] Vk
10] Tiktok        [20] Adobe         [30] XBOX
31] Mediafire     [32] Gitlab        [33] Github
34] Discord       [35] Roblox

99] About         [00] Exit

-] Select an option : 26
```

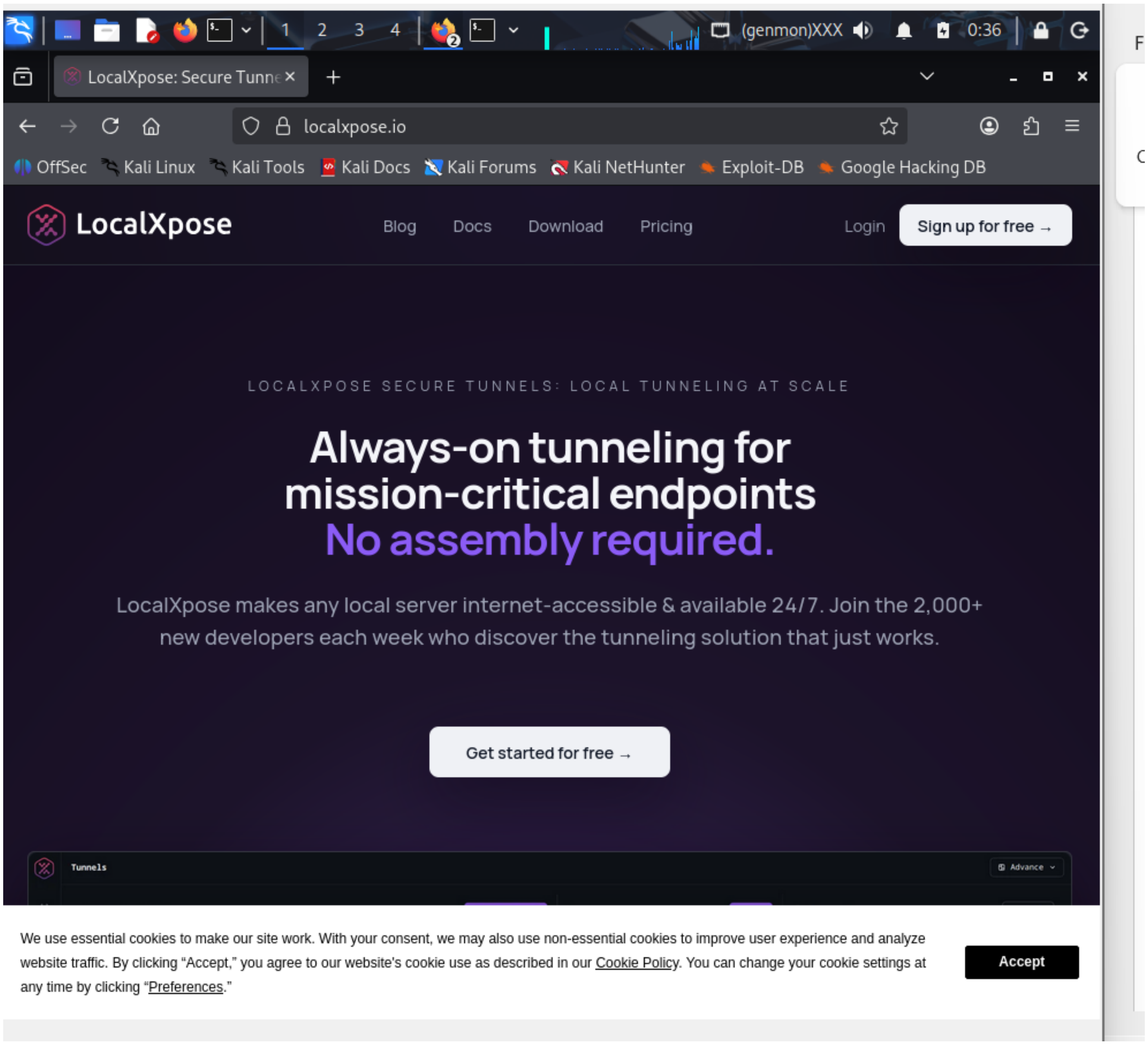


```
ZPHISHER 2.3.5

[01] Localhost
[02] Cloudflared  [Auto Detects]
[03] LocalXpose   [NEW! Max 15Min]

[-] Select a port forwarding service :
```





```
ZPHISHER 2.3.5

[?] Do you want to change Mask URL? [y/N] :
```

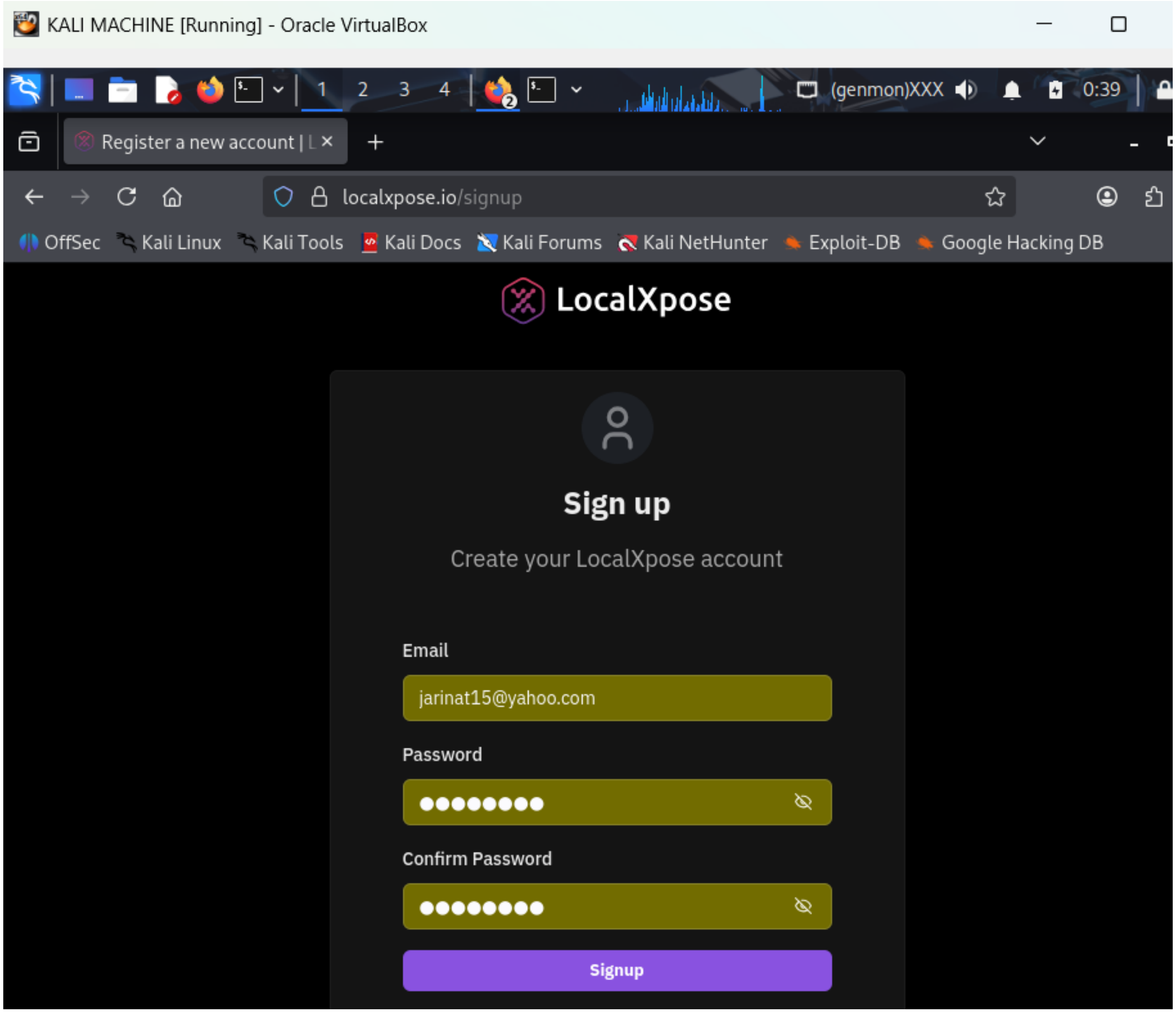


LOCALXPOSE SECURE TUNNELS: LOCAL TUNNELING AT SCALE

Always-on tunneling for mission-critical endpoints No assembly required.

LocalXpose makes any local server internet-accessible & available 24/7. Join the 2,000+ new developers each week who discover the tunneling solution that just works.

We use essential cookies to make our site work. With your consent, we may also use non-essential cookies to improve user experience and analyze website traffic. By clicking “Accept,” you agree to our website's cookie use as described in our Cookie Policy. You can change your cookie settings at any time by clicking “Preferences.”



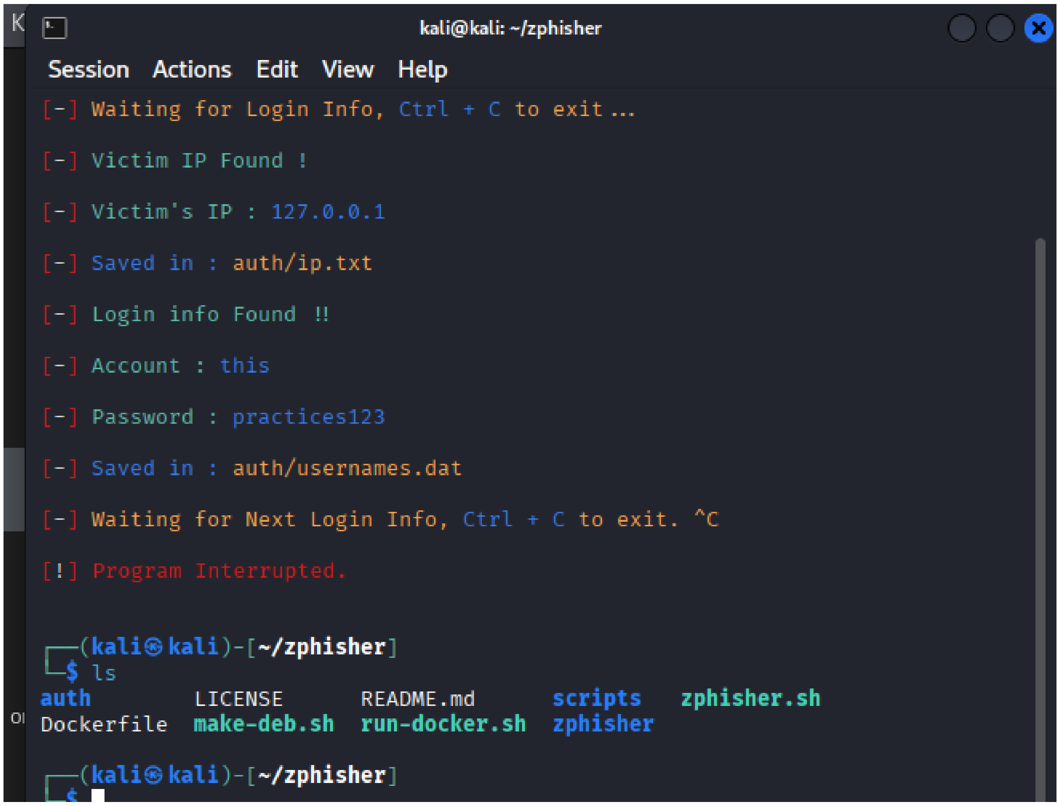
Sign up

Create your LocalXpose account

Email: jarinat15@yahoo.com

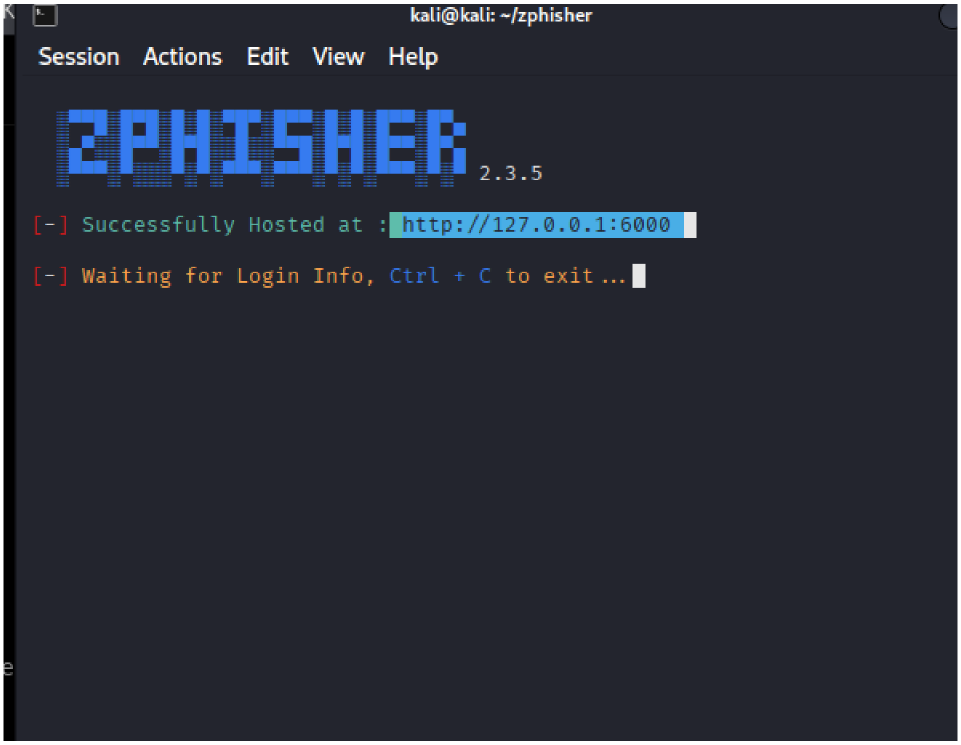
Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

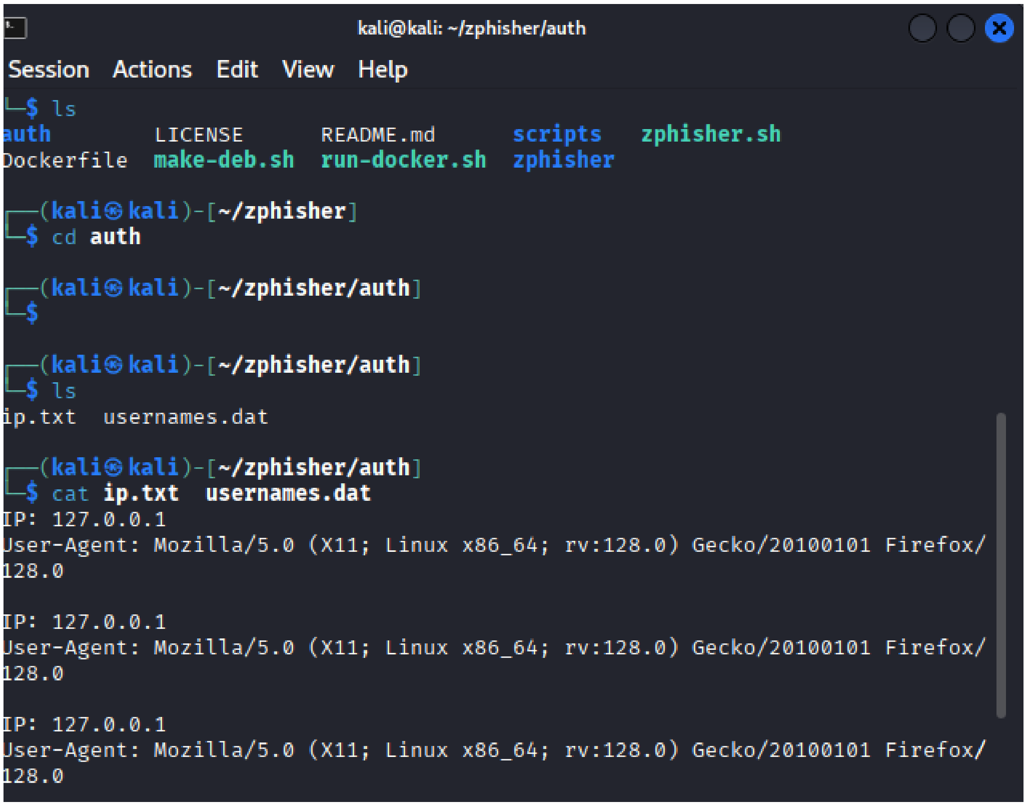


```
[-] Waiting for Login Info, Ctrl + C to exit ...

[-] Victim IP Found !

[-] Victim's IP : 127.0.0.1

[-] Saved in : auth/ip.txt

[-] Login info Found !!

[-] Account : this

[-] Password : practices123

[-] Saved in : auth/usernames.dat

[-] Waiting for Next Login Info, Ctrl + C to exit. ^C

[!] Program Interrupted.


┌──(kali㉿kali)-[~/zphisher]
└─$ ls
auth        LICENSE     README.md     scripts   zphisher.sh
Dockerfile  make-deb.sh run-docker.sh zphisher

┌──(kali㉿kali)-[~/zphisher]
```

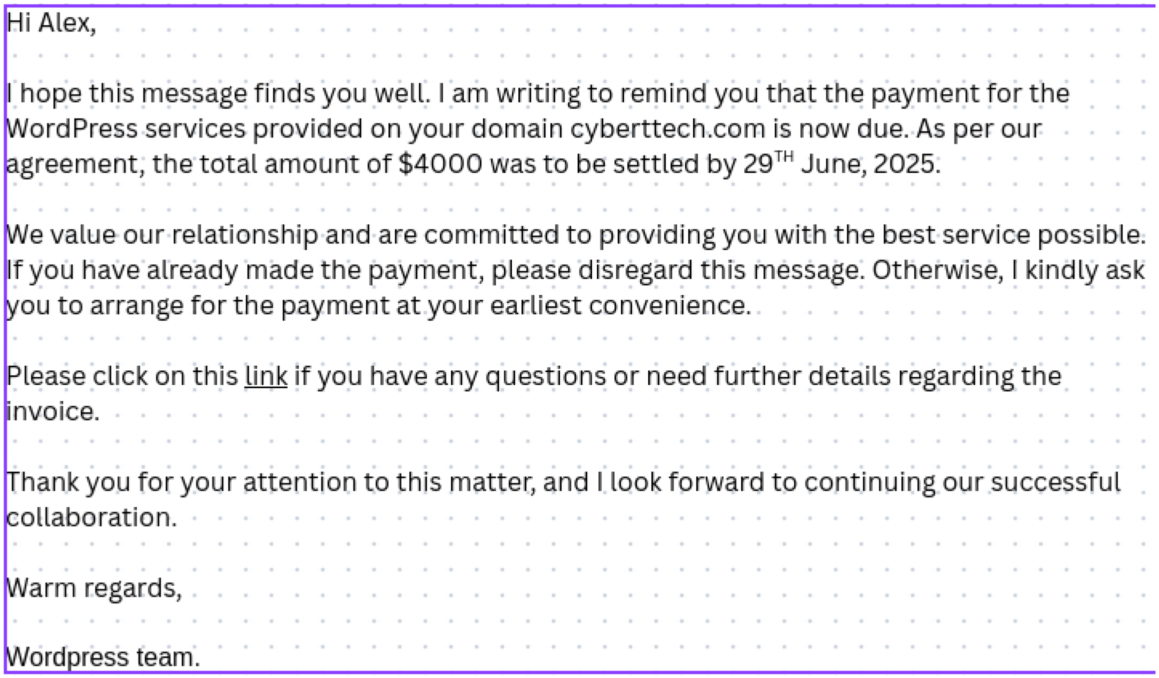
cat



```
2.3.5

[-] Successfully Hosted at : http://127.0.0.1:6000

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



```
└─$ ls
auth        LICENSE      README.md      scripts    zphisher.sh
Dockerfile  make-deb.sh  run-docker.sh  zphisher

┌──(kali㉿kali)-[~/zphisher]
└─$ cd auth

┌──(kali㉿kali)-[~/zphisher/auth]
└─$

┌──(kali㉿kali)-[~/zphisher/auth]
└─$ ls
ip.txt  usernames.dat

┌──(kali㉿kali)-[~/zphisher/auth]
└─$ cat ip.txt  usernames.dat
IP: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/
128.0

IP: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/
128.0

IP: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/
128.0
```



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 · Metrics

Before training, phishing simulations showed **higher click rates, higher credential submissions, and lower reporting**.

Department	Employees Tested	Link Clicks	Credential Submissions	Phishing Reports	Click Rate (%)	Submission Rate (%)	Report Rate (%)
Sales	30	10	4	3	33.3%	13.3%	10.0%
Marketing	40	15	6	5	37.5%	15.0%	12.5%
IT	35	12	3	4	34.3%	8.6%	11.4%

Post-training results shows clear **positive improvement**:

- Click rate dropped from ~35% → ~15–20%.
- Credential submissions dropped from 13% → almost 0%.
- Report rate increased from ~10–12% → 33–47%.

Department	Employees Tested	Link Clicks	Credential Submissions	Phishing Reports	Click Rate (%)	Submission Rate (%)	Report Rate (%)
Sales	30	5	1	10	16.7%	3.3%	33.3%
Marketing	40	8	0	19	20.0%	0.0%	47.5%
IT	35	5	0	14	14.3%	0.0%	40.0%

7 · Analysis

- Sales: Moderate click rate (16.7%) with 1 credential submitted. Improvement is needed in recognizing malicious login requests.
- Marketing: Higher click rate (20%), but zero credentials submitted — showing employees are stopping before full compromise. Reporting rate (47.5%) was the highest across all teams.
- IT: Lowest click rate (14.3%) with strong reporting (40%), suggesting high awareness levels.

8 · Recommendations

- Targeted Follow-Up Training for Sales team on credential phishing indicators.
- Reinforcement Sessions for all employees highlighting the importance of reporting suspected emails.
- Quarterly Simulations to measure sustained improvement and meet ISO 27001 awareness control.
- Gamified Awareness Programs (leaderboards, recognition for reporting) to encourage higher vigilance.

9 · Conclusion

The phishing simulation confirms that recent awareness training is producing measurable improvements in employee security behavior. Credential submission attempts have been reduced to near zero, while reporting of suspicious emails has increased significantly across departments. These outcomes demonstrate clear progress toward building a stronger security culture. With continued reinforcement through targeted training, regular simulations, and engagement initiatives, the organization is well positioned to further minimize phishing risks and maintain compliance with ISO 27001 requirements