SOCIAL ENGINEERING
PHISHING SIMULATION

By : Imane TOUIBA

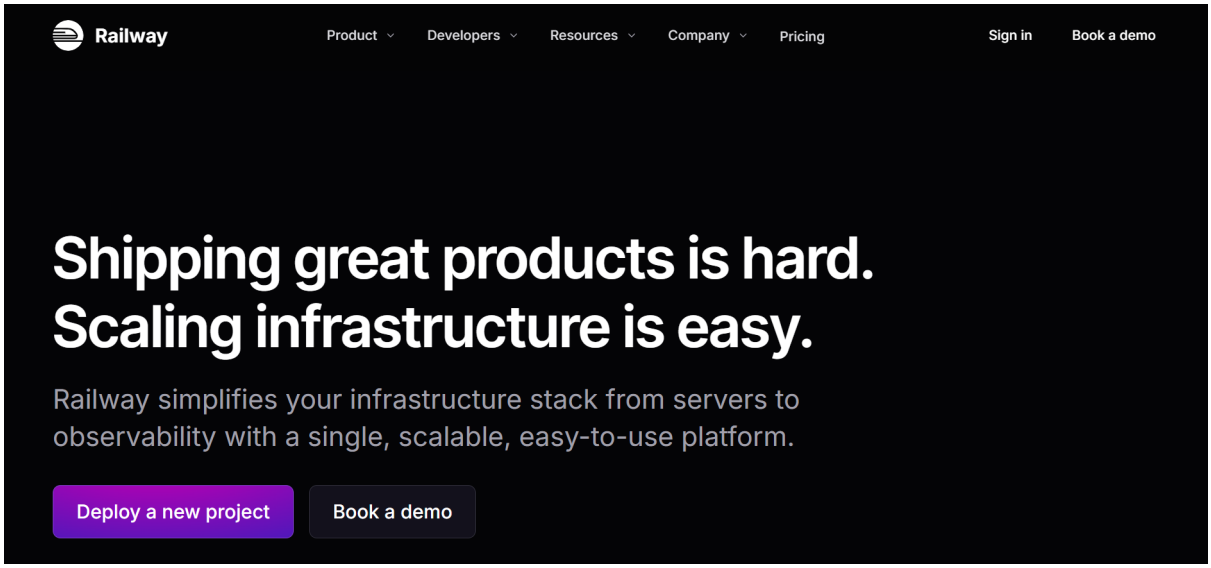
April 19, 2025

1 Introduction

Phishing remains one of the most prevalent cyber threats, exploiting human psychology to bypass technical defenses. With over 90% of data breaches originating from phishing attacks, organizations must prioritize employee awareness and proactive testing. GoPhish, an open-source phishing framework, enables security teams to simulate realistic attacks, assess vulnerabilities, and train users to recognize malicious emails. By deploying GoPhish, this project demonstrates how controlled phishing simulations can strengthen an organization's security posture while measuring employee susceptibility to social engineering tactics.

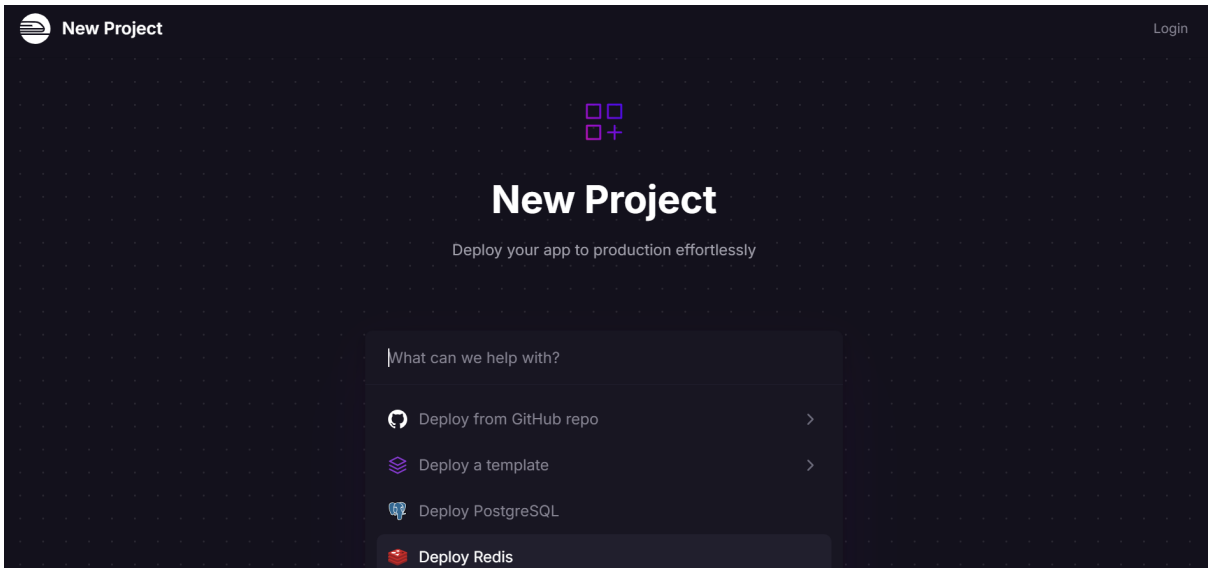
2 Environment Setup

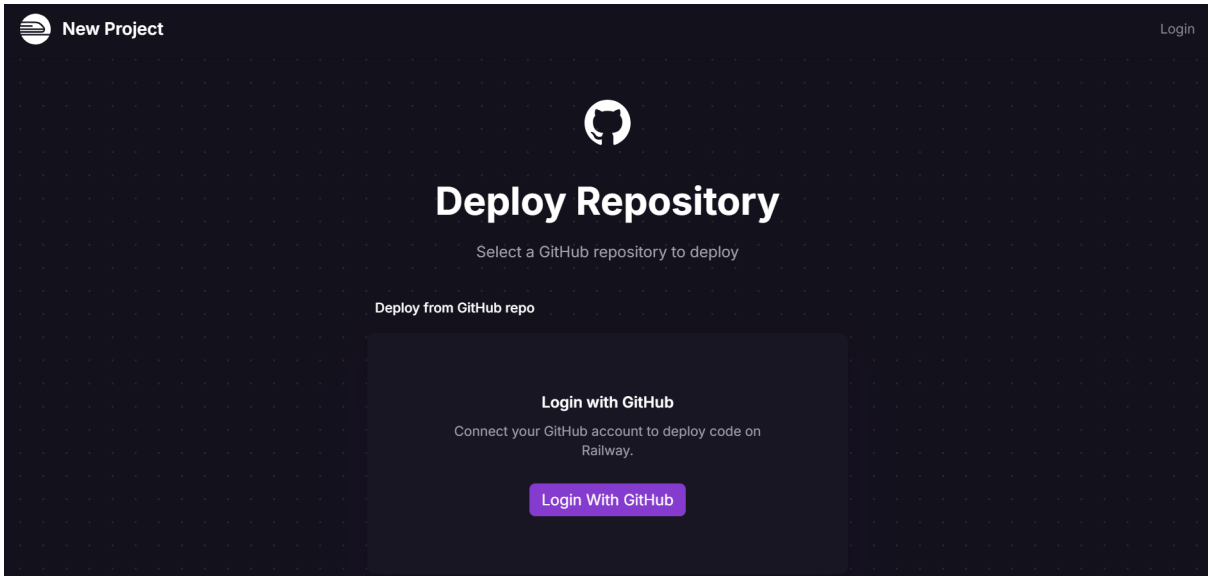
Since emails may be blocked if sent directly from a local machine, I deployed Gophish on Railway (a cloud platform) for reliable email delivery.

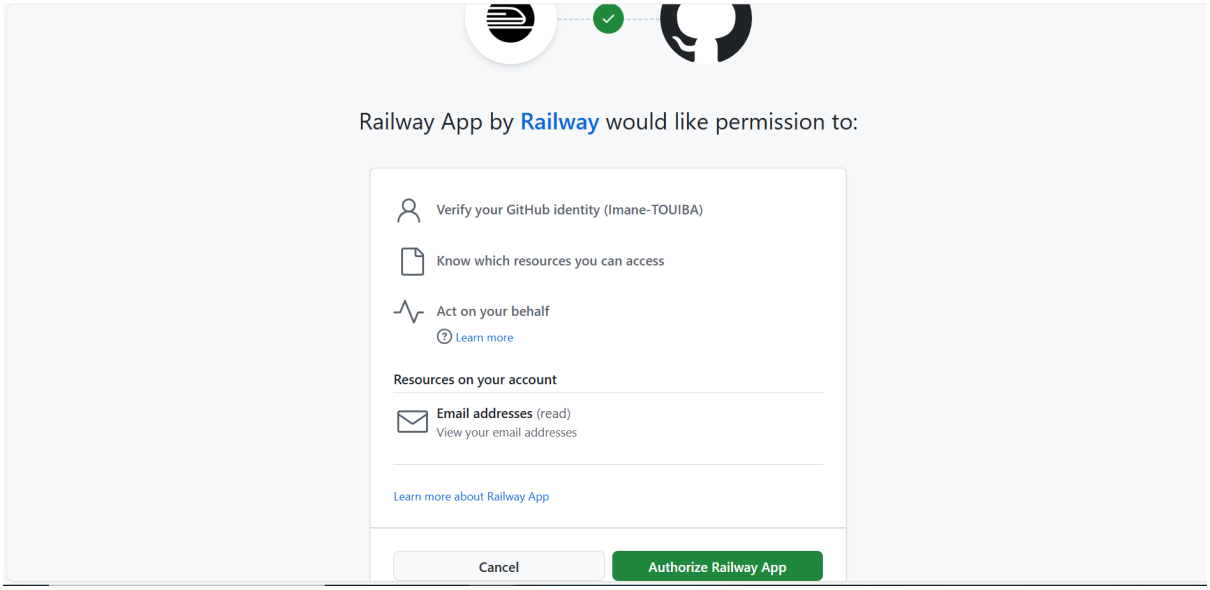


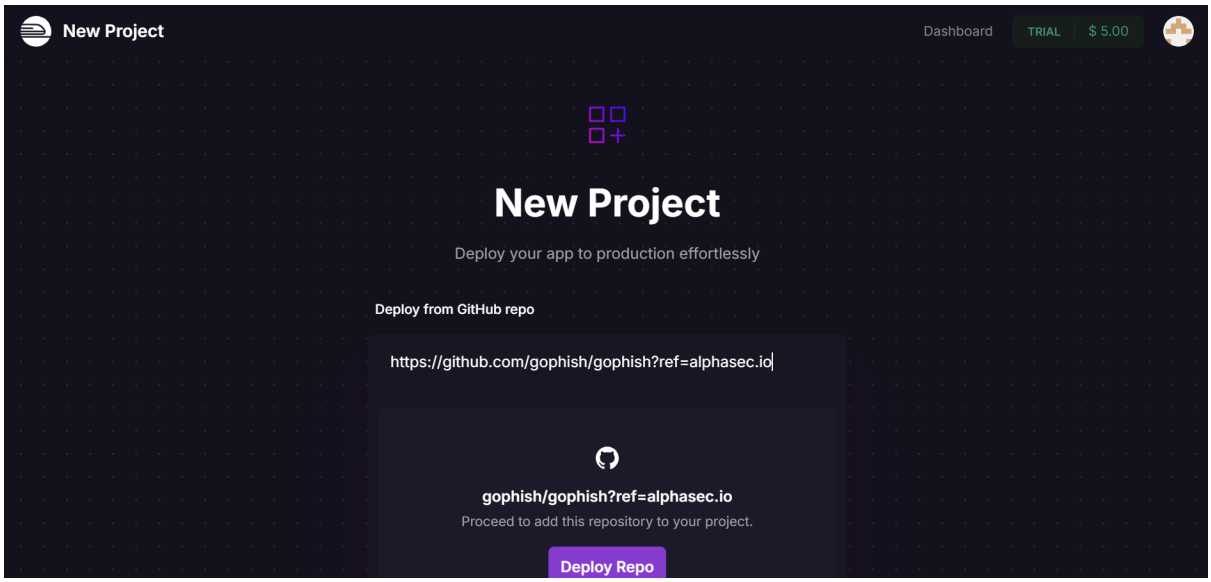
2.1 Deployment via GitHub Repository

Used the official Gophish GitHub repository (https://github.com/gophish/gophish)
Connected the repository to Railway for automated deployment.
Railway built and deployed the Gophish instance.


New Project
Login
New Project
Deploy your app to production effortlessly
What can we help with?
Deploy from GitHub repo
Deploy a template
Deploy PostgreSQL
Deploy Redis


New Project
Login
Deploy Repository
Select a GitHub repository to deploy
Deploy from GitHub repo
Login with GitHub
Connect your GitHub account to deploy code on Railway.
Login With GitHub



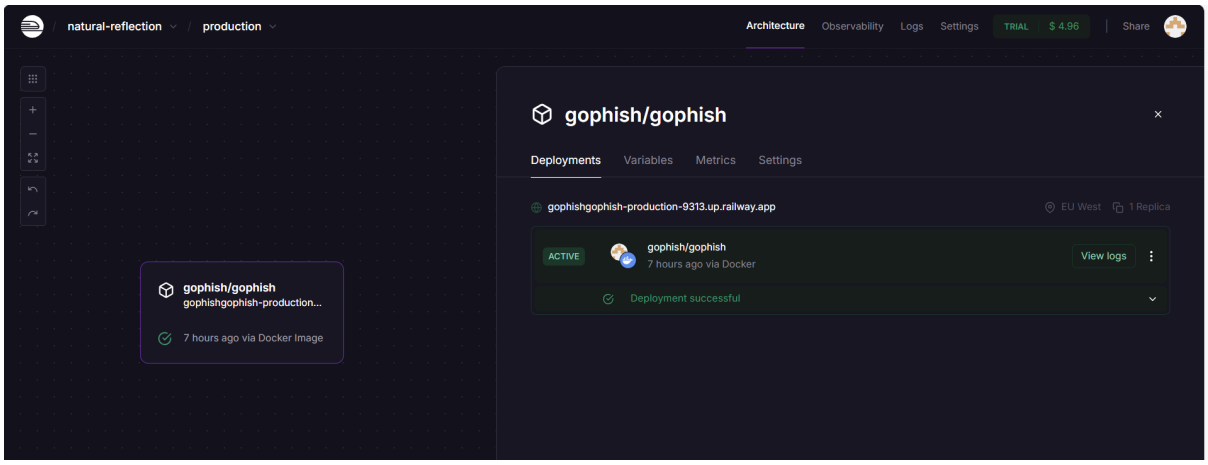


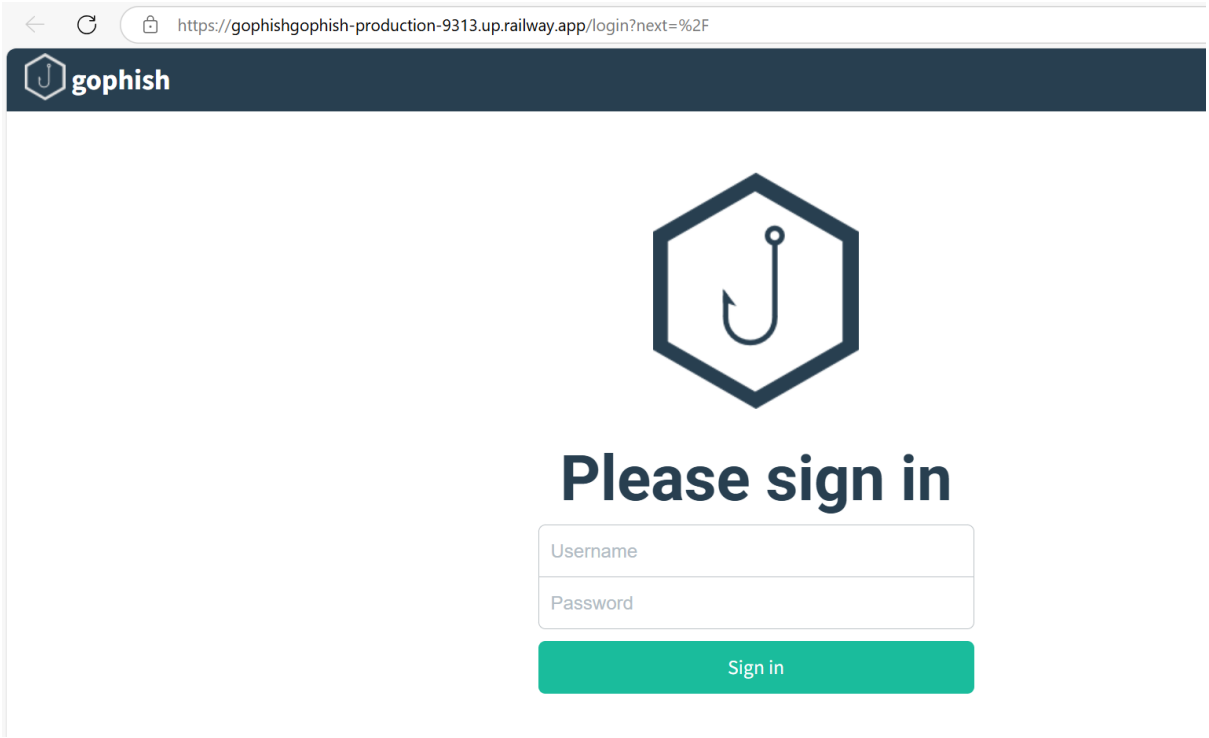
2.2 Accessing Gophish

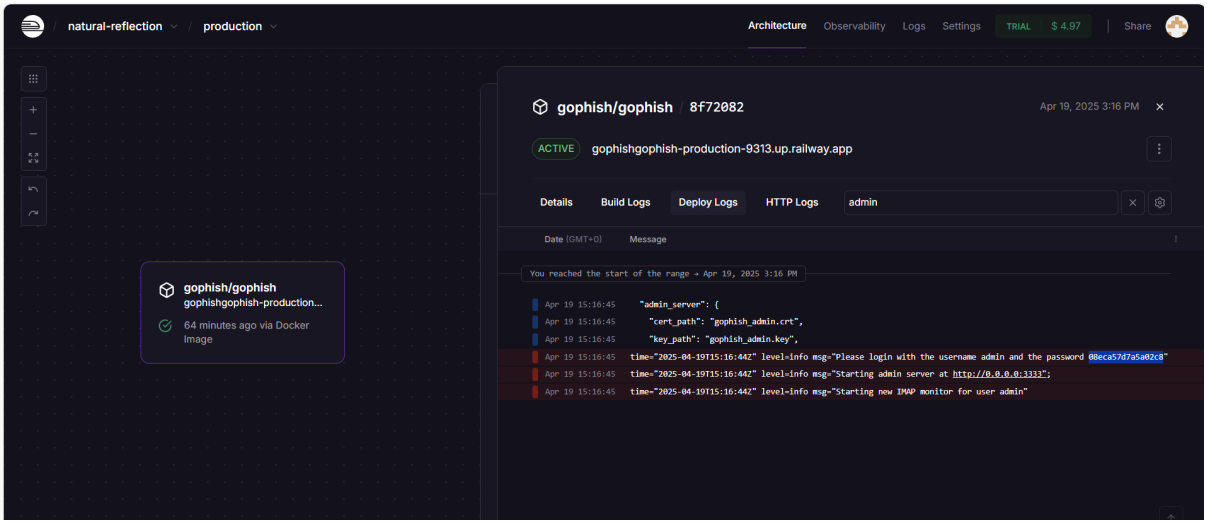
After deployment, Railway provided a public URL for the Gophish server.

Navigated to the URL in a web browser to access the Gophish dashboard.

Retrieved login credentials (admin username and password) from Railway's logs or environment variables.

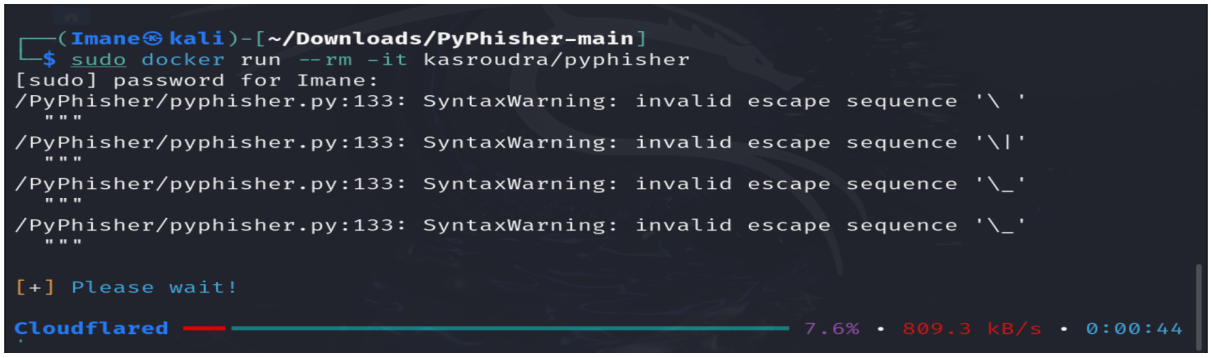

natural-reflection
production
Architecture
Observability
Logs
Settings
TRIAL
$ 4.96
Share
gophish/gophish
Deployments
Variables
Metrics
Settings
gophishgophish-production-9313.up.railway.app
EU West
1 Replica
ACTIVE
gophish/gophish
7 hours ago via Docker
View logs
Deployment successful
gophish/gophish
gophishgophish-production...
7 hours ago via Docker Image

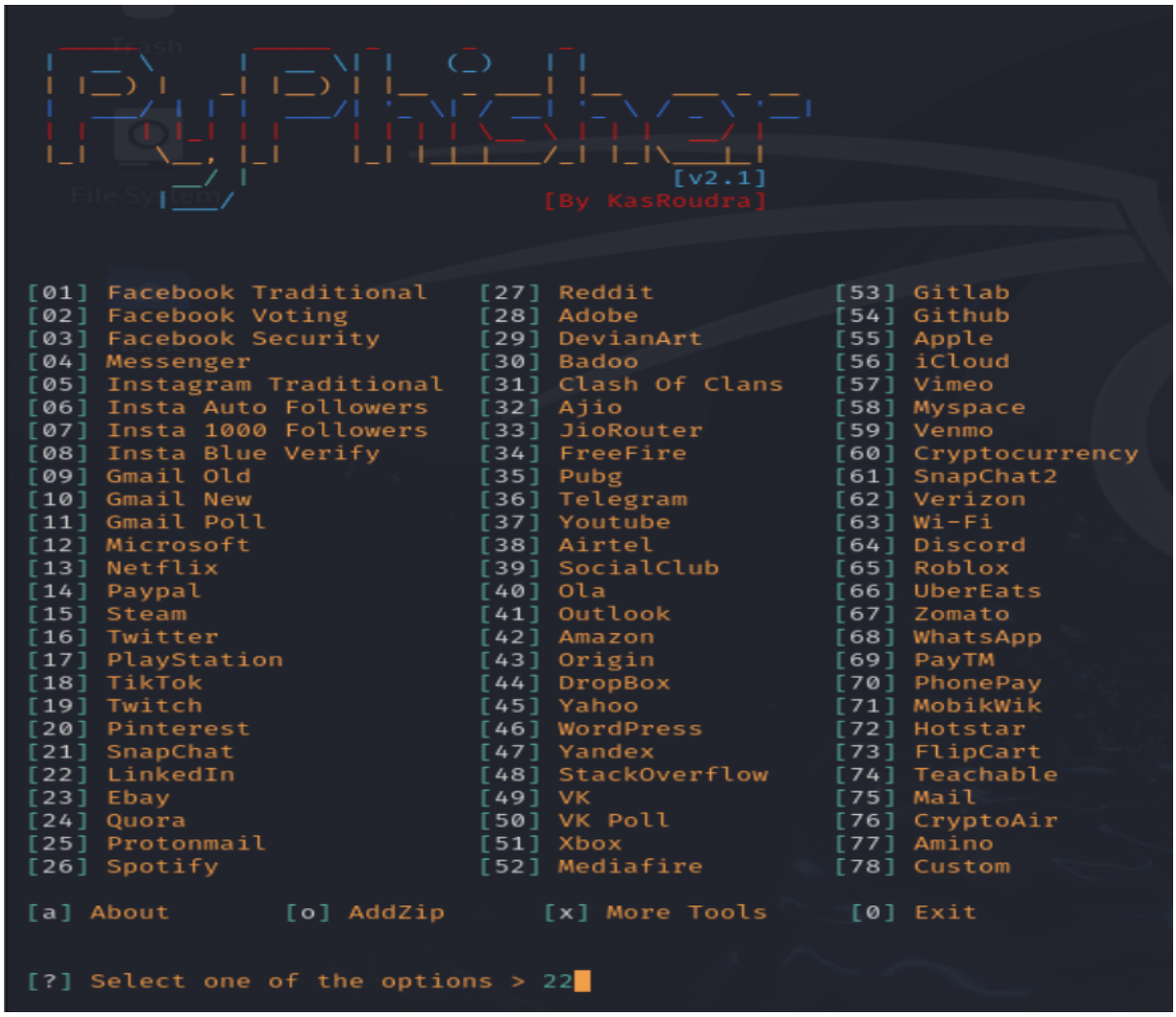

https://gophishgophish-production-9313.up.railway.app/login?next=%2F
gophish
Please sign in
Username
Password
Sign in


natural-reflection
production
Architecture
Observability
Logs
Settings
TRIAL
$ 4.97
Share
gophish/gophish
gophishgophish-production...
64 minutes ago via Docker Image
gophish/gophish
8f72082
Apr 19, 2025 3:16 PM
ACTIVE
gophishgophish-production-9313.up.railway.app
Details
Build Logs
Deploy Logs
HTTP Logs
admin
Date (GMT+0)
Message
You reached the start of the range → Apr 19, 2025 3:16 PM
Apr 19 15:16:45 "admin_server": {
Apr 19 15:16:45 "cert_path": "gophish_admin.crt",
Apr 19 15:16:45 "key_path": "gophish_admin.key",
Apr 19 15:16:45 time="2025-04-19T15:16:44Z" level=info msg="Please login with the username admin and the password 08eca57d7a5a02c8"
Apr 19 15:16:45 time="2025-04-19T15:16:44Z" level=info msg="Starting admin server at http://0.0.0.0:3333"
Apr 19 15:16:45 time="2025-04-19T15:16:44Z" level=info msg="Starting new IMAP monitor for user admin"

https://gophishgophish-production-9313.up.railway.app/reset_password?next=%2F
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
gophish
Reset Your Password
Save Password

3 PyPhisher


(Imane㉿kali)-[~/Downloads/PyPhisher-main]
$ sudo docker run --rm -it kasroudra/pyphisher
[sudo] password for Imane:
/PyPhisher/pyphisher.py:133: SyntaxWarning: invalid escape sequence '\ '
/PyPhisher/pyphisher.py:133: SyntaxWarning: invalid escape sequence '\|'
/PyPhisher/pyphisher.py:133: SyntaxWarning: invalid escape sequence '_'
/PyPhisher/pyphisher.py:133: SyntaxWarning: invalid escape sequence '_'
[+] Please wait!
Cloudflared 7.6% • 809.3 kB/s • 0:00:44


[v2.1]
[By KasRoudra]
[01] Facebook Traditional
[02] Facebook Voting
[03] Facebook Security
[04] Messenger
[05] Instagram Traditional
[06] Insta Auto Followers
[07] Insta 1000 Followers
[08] Insta Blue Verify
[09] Gmail Old
[10] Gmail New
[11] Gmail Poll
[12] Microsoft
[13] Netflix
[14] Paypal
[15] Steam
[16] Twitter
[17] PlayStation
[18] TikTok
[19] Twitch
[20] Pinterest
[21] SnapChat
[22] LinkedIn
[23] Ebay
[24] Quora
[25] Protonmail
[26] Spotify
[27] Reddit
[28] Adobe
[29] DevianArt
[30] Badoo
[31] Clash Of Clans
[32] Ajio
[33] JioRouter
[34] FreeFire
[35] Pubg
[36] Telegram
[37] Youtube
[38] Airtel
[39] SocialClub
[40] Ola
[41] Outlook
[42] Amazon
[43] Origin
[44] DropBox
[45] Yahoo
[46] WordPress
[47] Yandex
[48] StackOverflow
[49] VK
[50] VK Poll
[51] Xbox
[52] Mediafire
[53] Gitlab
[54] Github
[55] Apple
[56] iCloud
[57] Vimeo
[58] Myspace
[59] Venmo
[60] Cryptocurrency
[61] SnapChat2
[62] Verizon
[63] Wi-Fi
[64] Discord
[65] Roblox
[66] UberEats
[67] Zomato
[68] WhatsApp
[69] PayTM
[70] PhonePay
[71] MobikWik
[72] Hotstar
[73] FlipCart
[74] Teachable
[75] Mail
[76] CryptoAir
[77] Amino
[78] Custom
[a] About
[o] AddZip
[x] More Tools
[0] Exit
[?] Select one of the options > 22

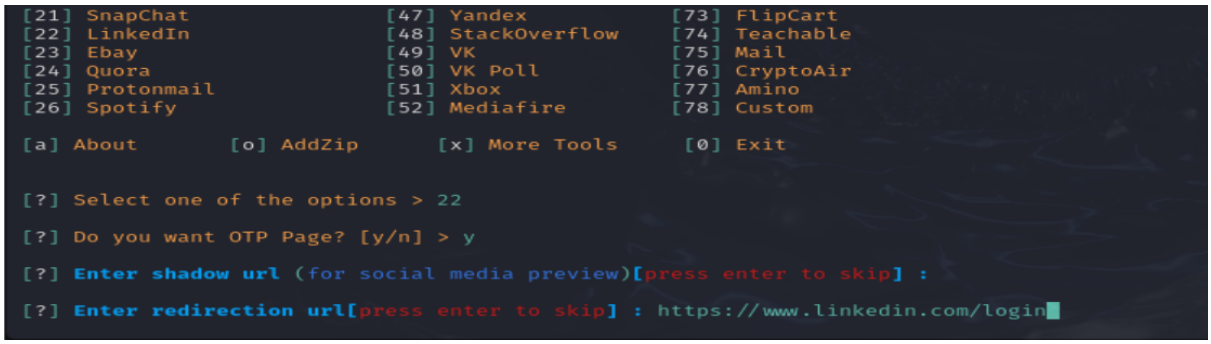
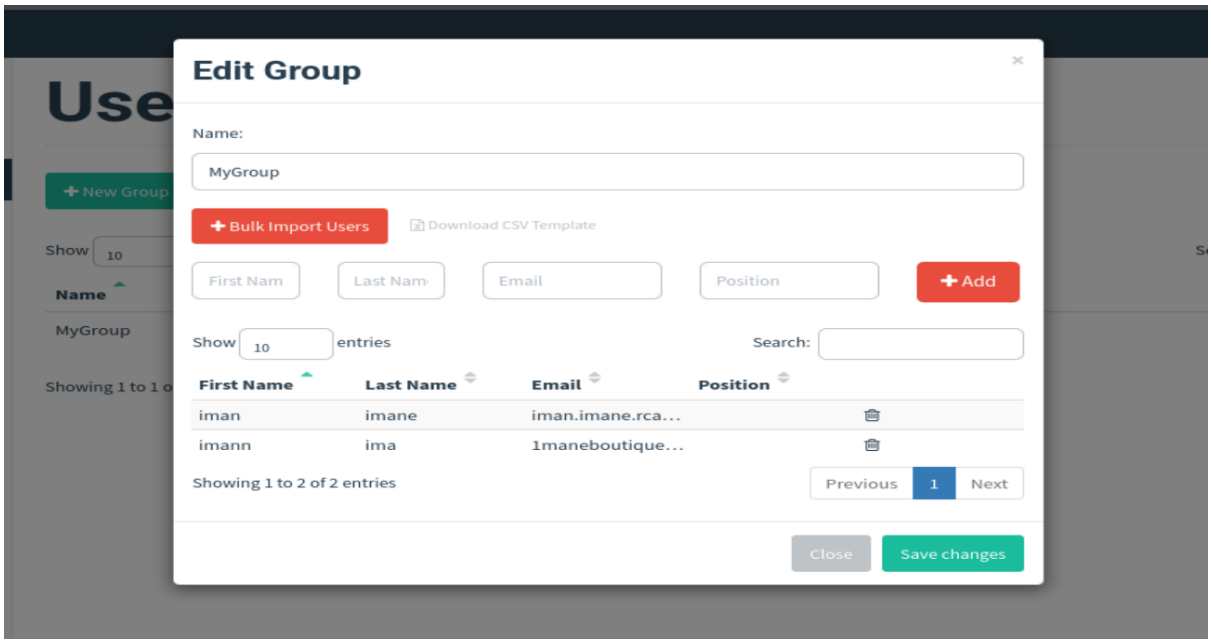
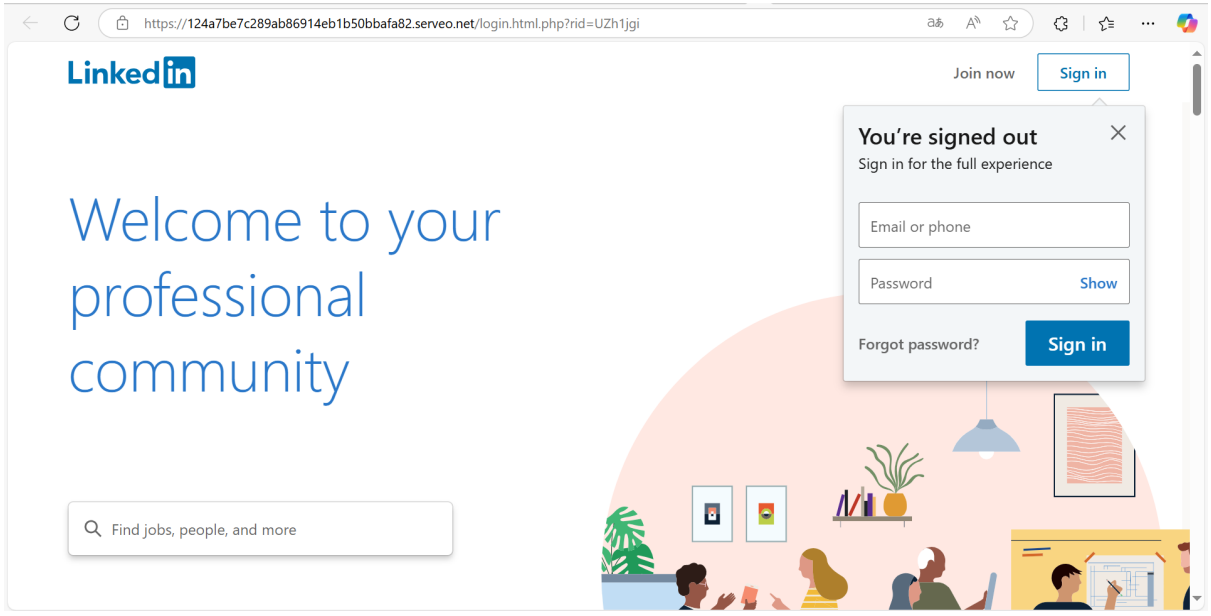


Figure 1: Enter Caption





4 Gophish configuration

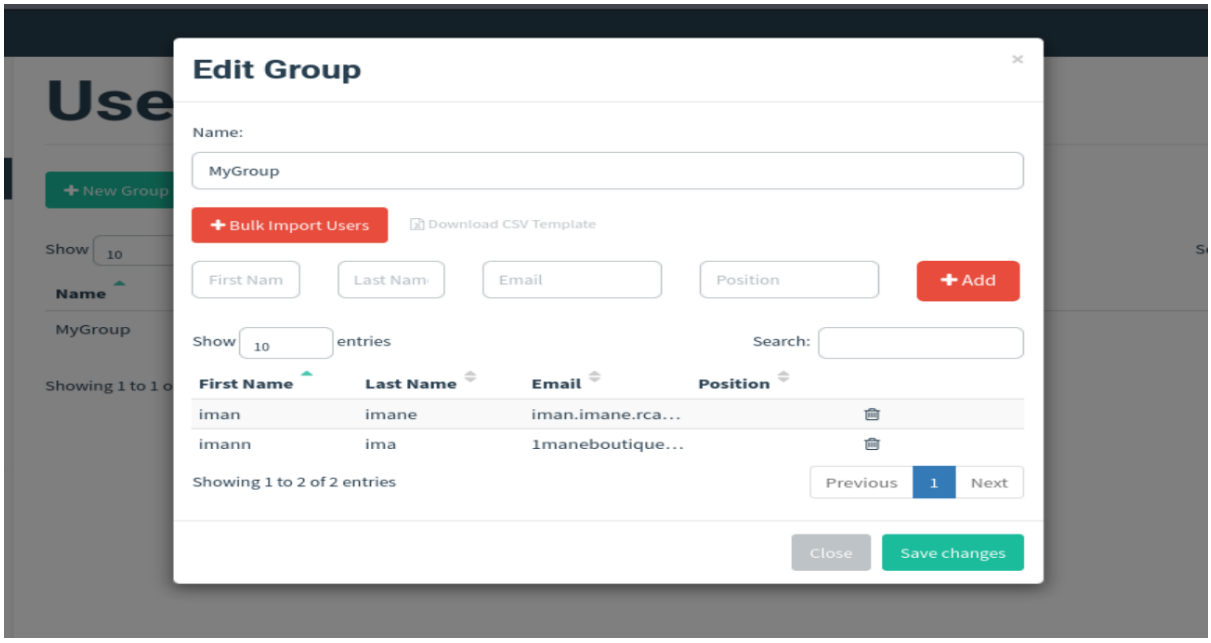
After logging in, I configured the following components for the phishing campaign:

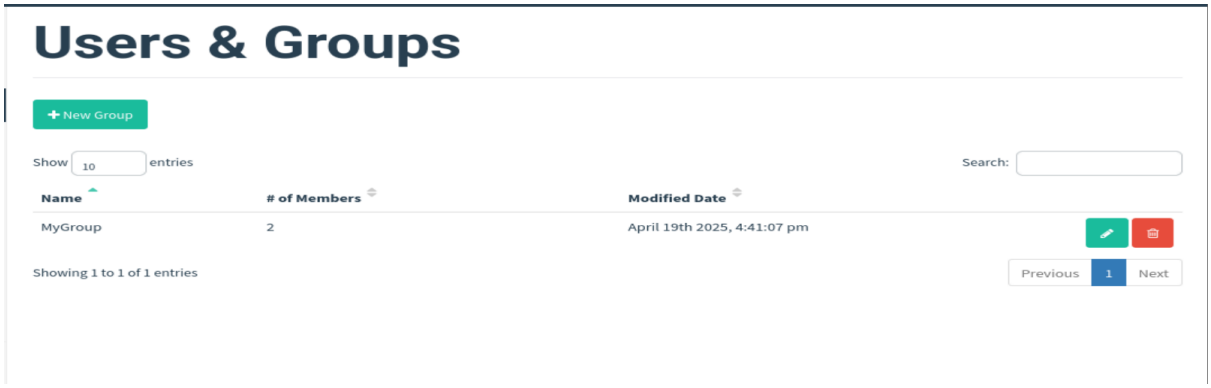
Groups and Users Purpose: Define the target recipients.

Action Taken:

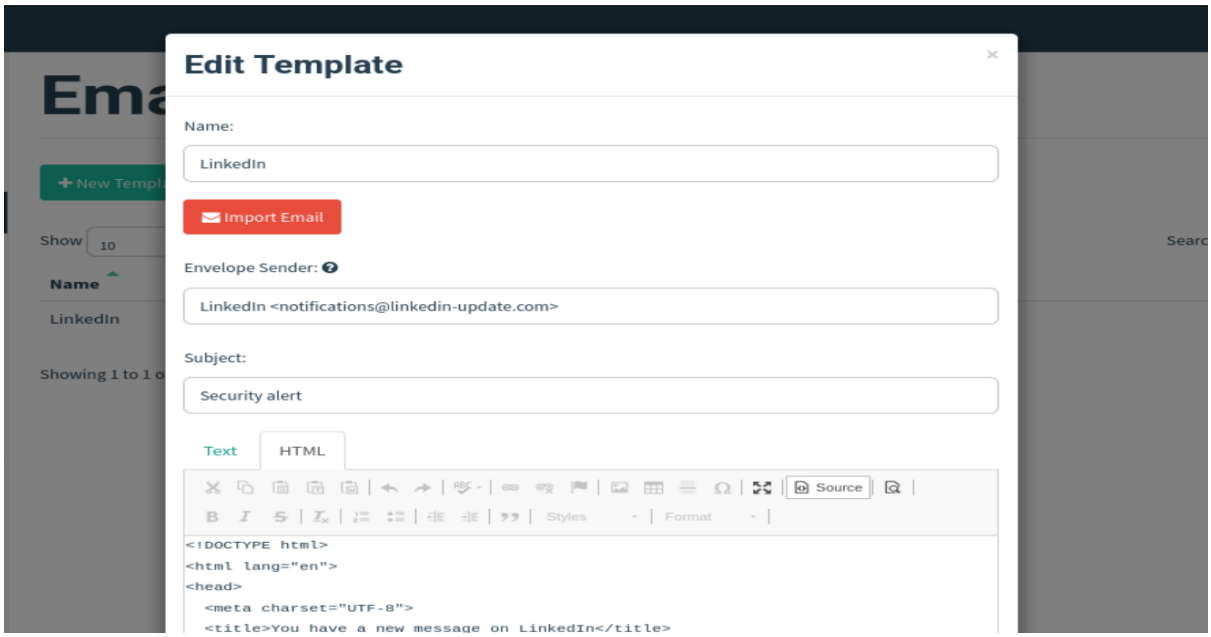
Created group "MyGroup" containing 2 test users.

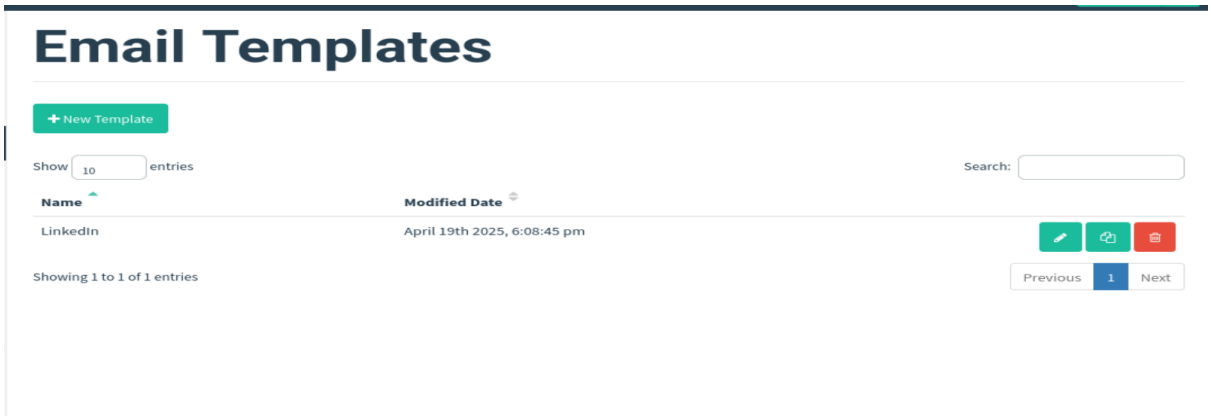
Manually added target emails (There is also the possibility to import a CSV file containing target emails).



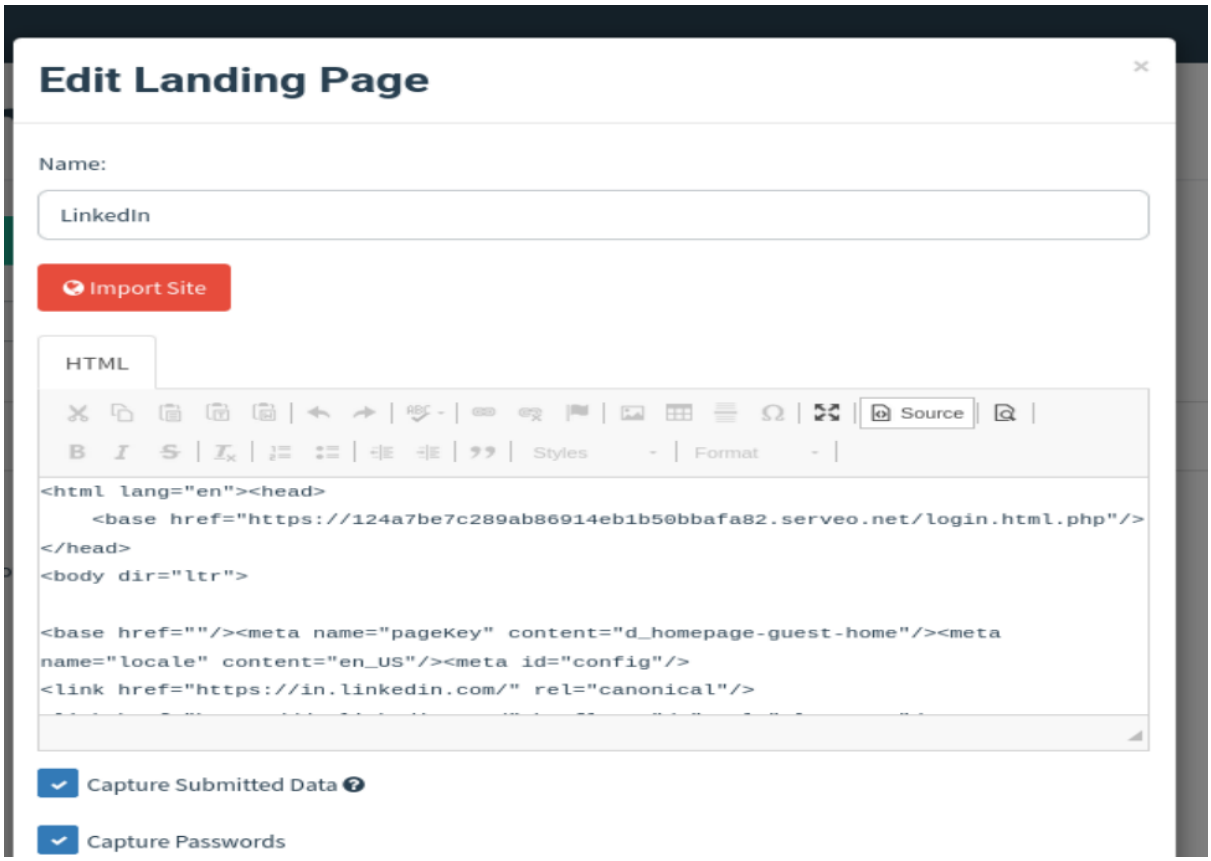


Email Template Design Template Name: "LinkedIn"
Sender Address: Spoofed as LinkedIn <notifications@linkedin-update.com>
Subject Line: "Security alert" to induce urgency
HTML Body: Cloned LinkedIn notification email

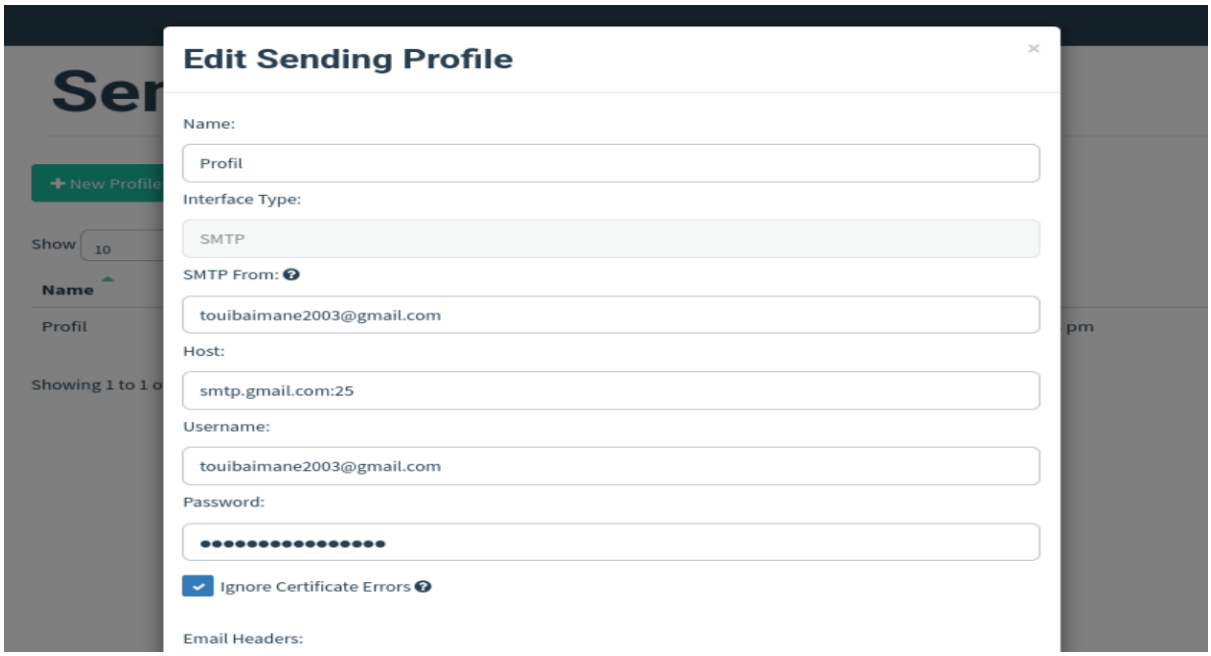




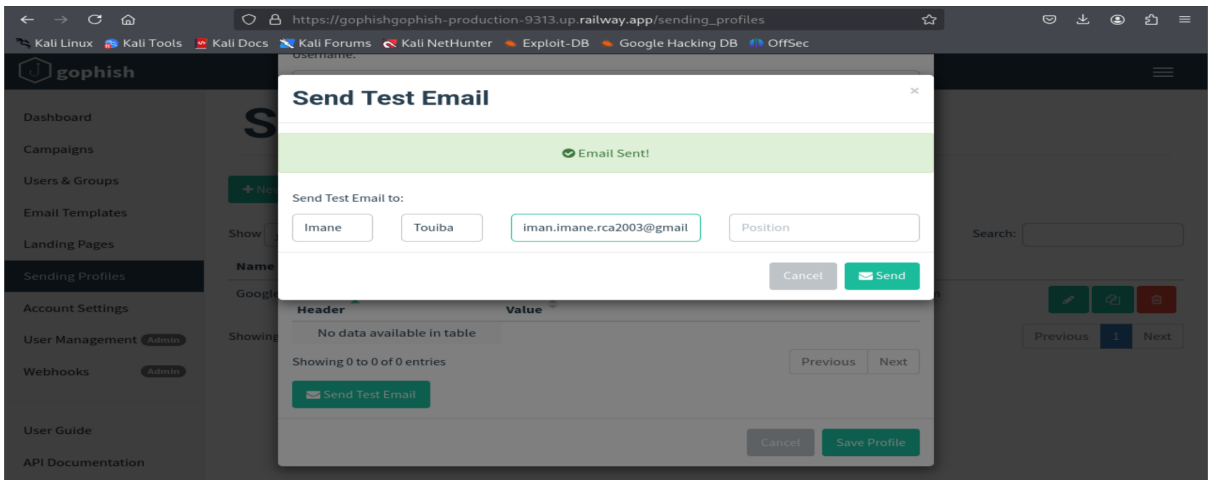
Landing Page Integration Page Name: "LinkedIn"
Source: Pyphisher-generated page hosted at: https://124a7be7c289ab8691 4eb1b50bbafa82.serveo.net/ login.html.php

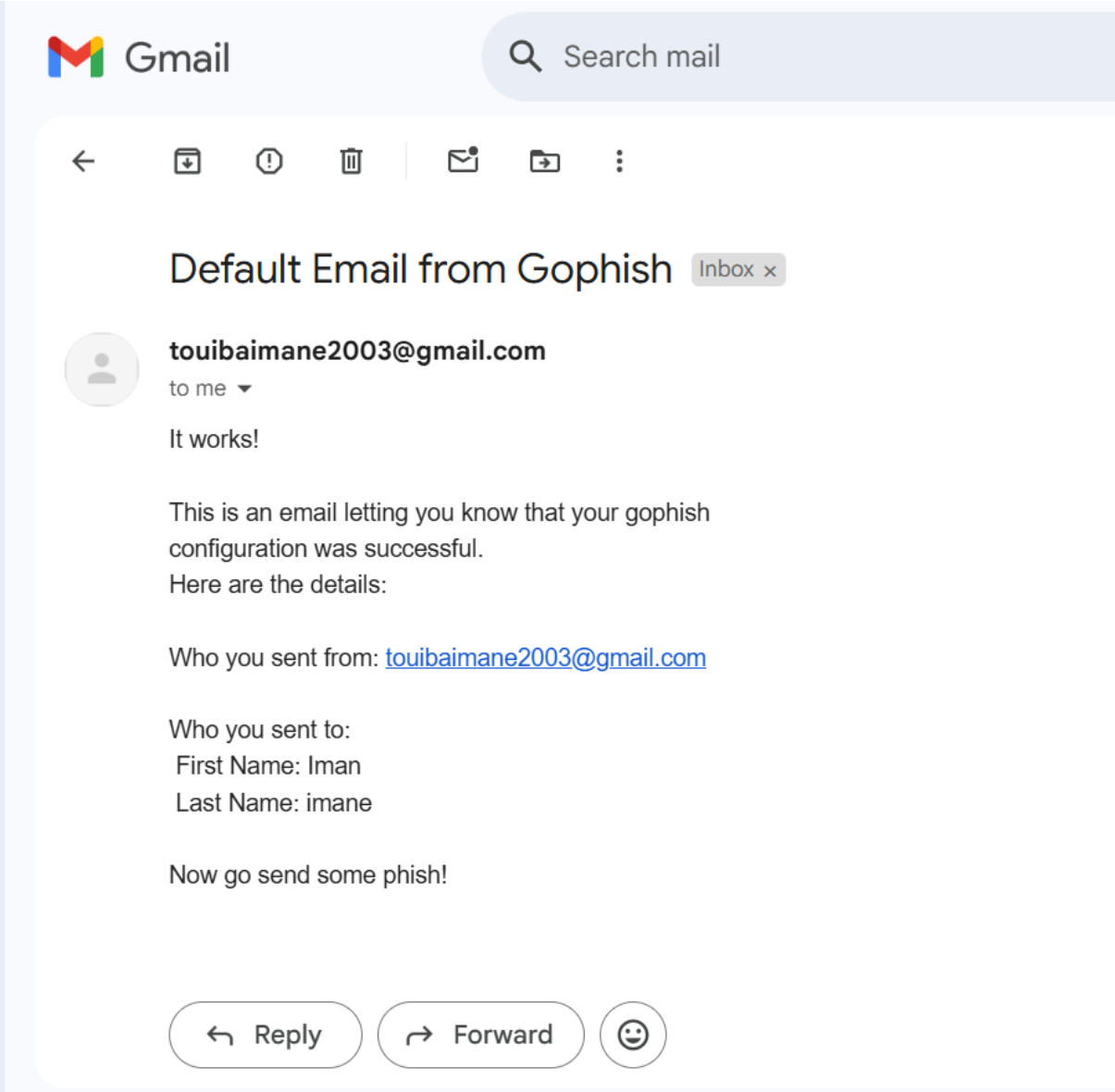


SMTP Server: Gmail (smtp.gmail.com:25)
Sender Identity: My email address
Security Note: Certificate errors ignored (not recommended for production)

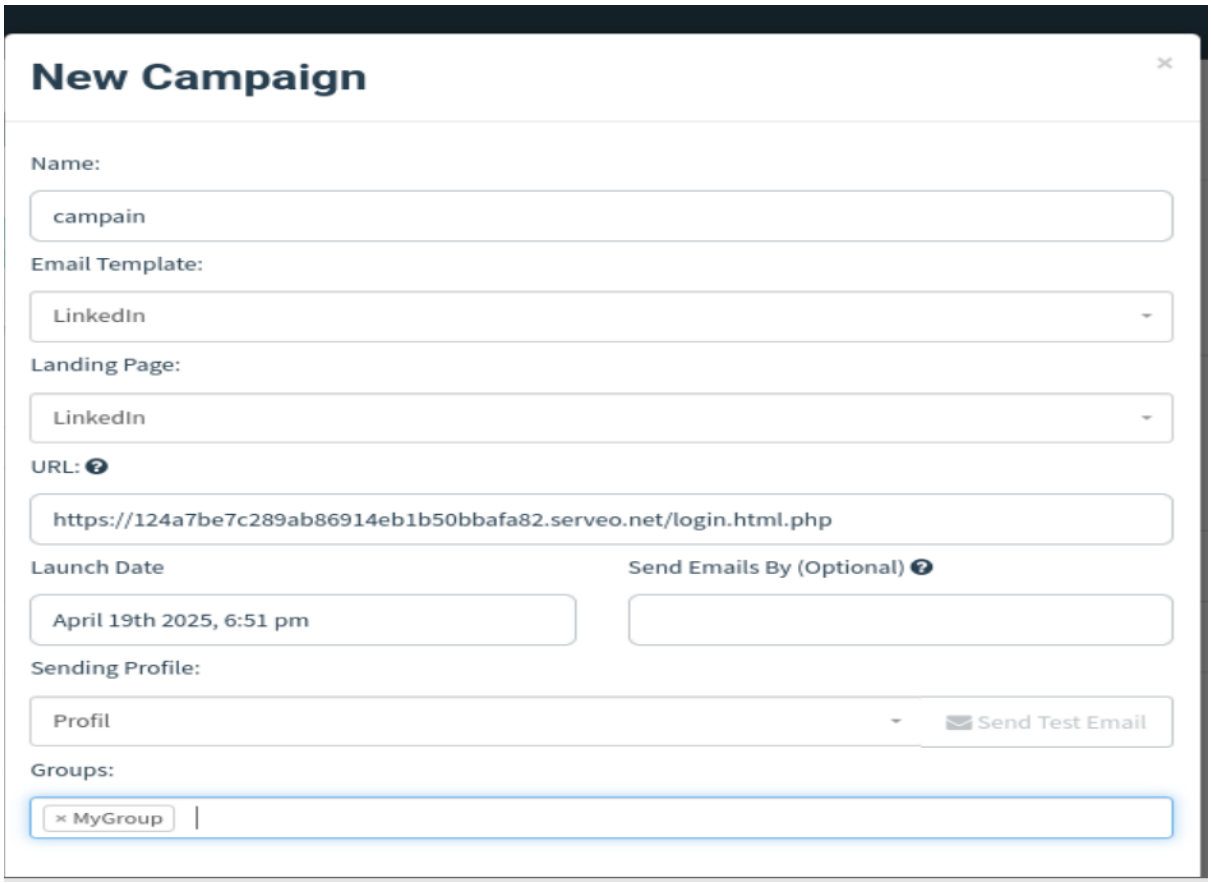


Sending test email to verify that the GoPhish configuration is functioning correctly



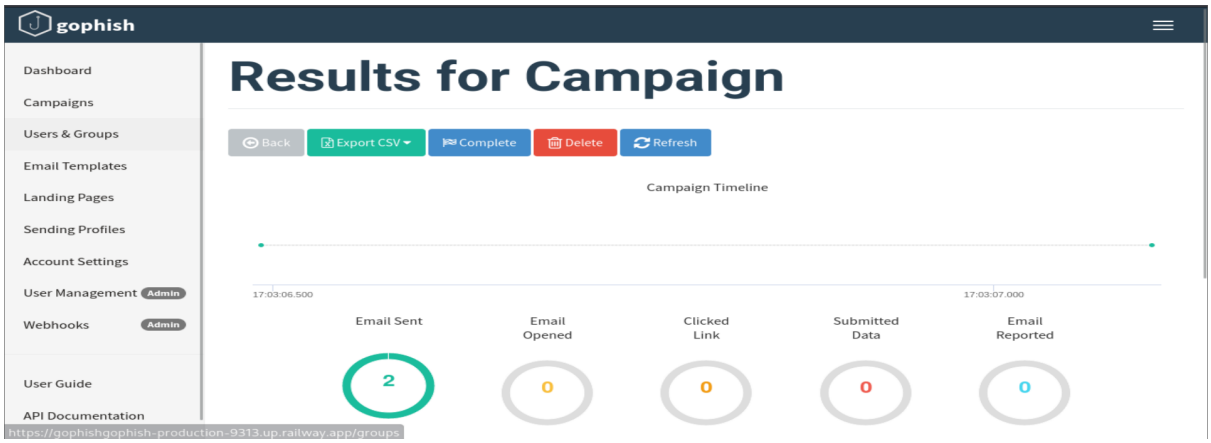


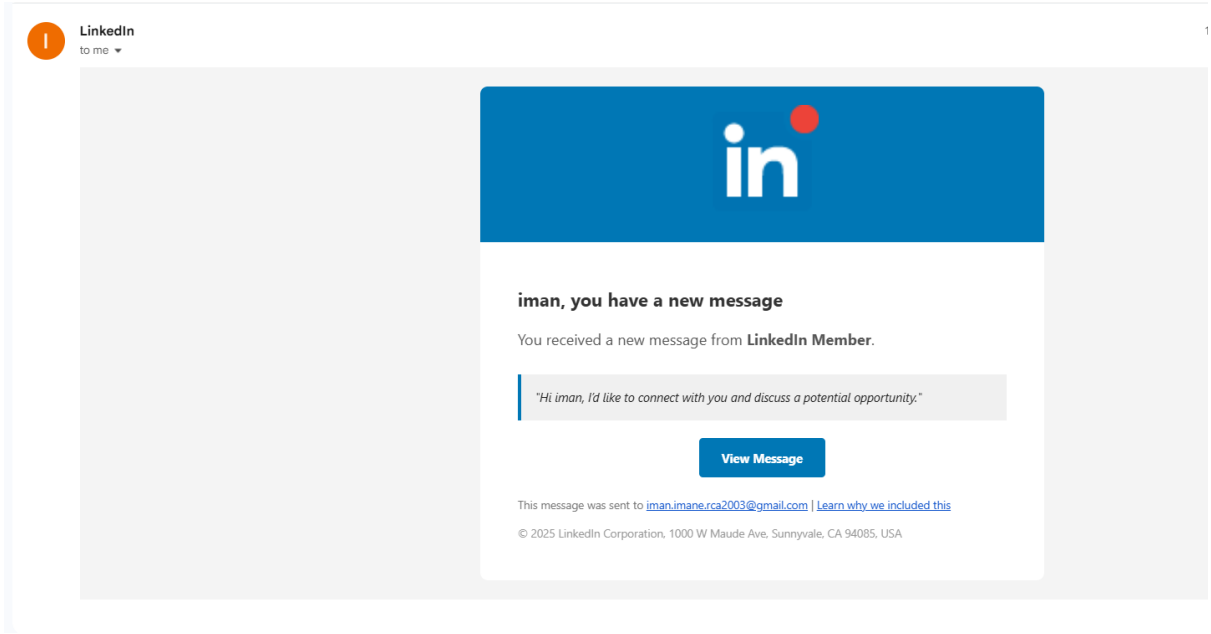
Campaign Launch Name: "campain"
Parameters:
Linked to "LinkedIn" email template and landing page
Scheduled for April 19th 2025, 6:51 PM
Assigned to "MyGroup" recipients



5 Phishing attack

After launching the campaign, GoPhish successfully delivered the spoofed LinkedIn emails to both test users. One user clicked the link and submitted credentials (username:, password: password) through the Pyphisher-generated landing page, which were captured in creds.txt.


gophish
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Account Settings
User Management
Admin
Webhooks
Admin
User Guide
API Documentation
Results for Campaign
Back
Export CSV
Complete
Delete
Refresh
Campaign Timeline
17:03:06.500
17:03:07.000
Email Sent
2
Email Opened
0
Clicked Link
0
Submitted Data
0
Email Reported
0
https://gophishgophish-production-9313.up.railway.app/groups


LinkedIn
to me
iman, you have a new message
You received a new message from LinkedIn Member.
"Hi iman, I'd like to connect with you and discuss a potential opportunity."
View Message
This message was sent to iman.imane.rca2003@gmail.com | Learn why we included this
© 2025 LinkedIn Corporation, 1000 W Maude Ave, Sunnyvale, CA 94085, USA

Imane@kali: ~/Downloads/PyPhisher-main
File Actions Edit View Help
PyPhisher Data
[*] LinkedIn Username: 00000000
[*] Password: password
[•] Saved in creds.txt
[+] Waiting for next.....Press Ctrl+C to exit
[√] Victim login info found!
PyPhisher Data
[*] LinkedIn Username: iman.imane.rca2003@gmail.com
[*] Password: password
[•] Saved in creds.txt
[+] Waiting for next.....Press Ctrl+C to exit