TASK 2

SOCIAL ENGINEERING & PHISHING ATTACK

🧑‍💻 Intern Name: Jeet Nishad

📧 Email ID: [jeetnishad12@gmail.com](mailto:jeetnishad12@gmail.com)

## 1.Phishing Attack using SEToolkit

## 🎯 Objective:

To simulate a phishing attack using the Social-Engineer Toolkit (SET) in Kali Linux, by cloning a real website and capturing user credentials using a Credential Harvester attack.

## 🧰 Tools Used:

• Kali Linux  
• SEToolkit (Social Engineering Toolkit)  
• Apache Web Server

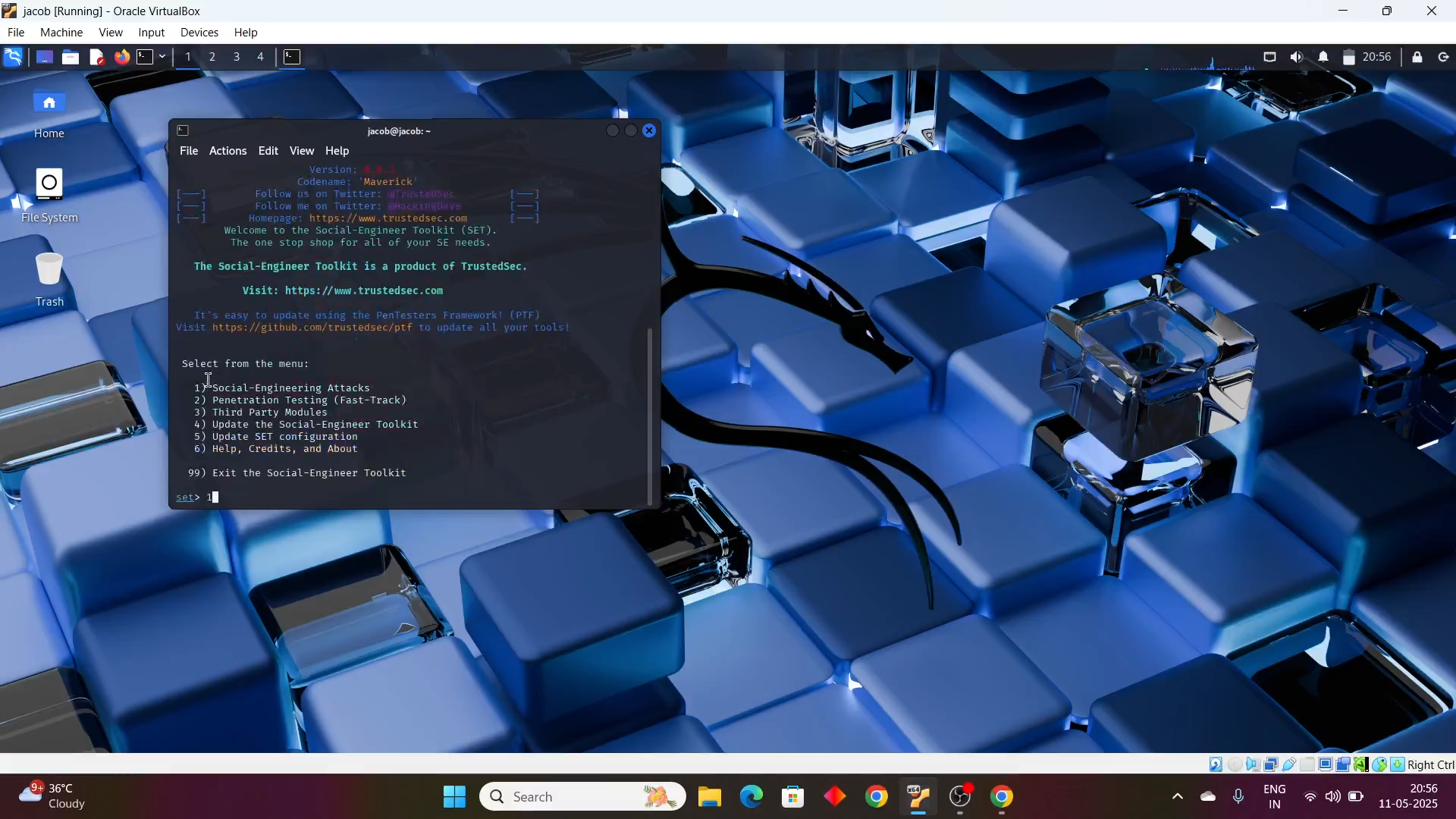
## 🔍 Detailed Steps Performed:

### Launching SEToolkit 🚀

sudo setoolkit  
This command launches the SET interface.

Selecting Attack Type 🧠

Selected: 1) Social-Engineering Attacks



### Choosing Website Attack Vectors 🌐

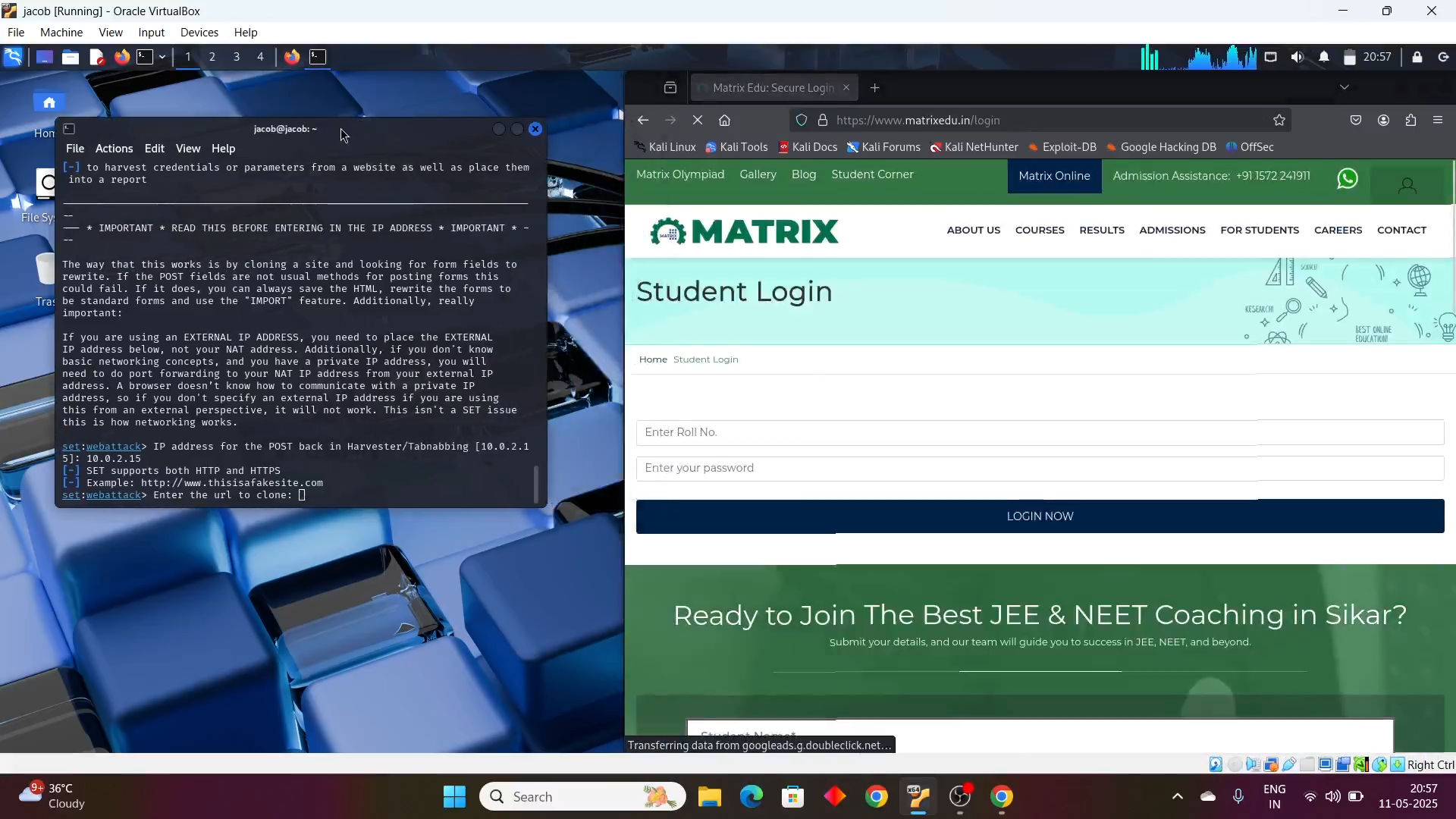
Chose: 2) Website Attack Vectors

### Credential Harvester Method 🪤

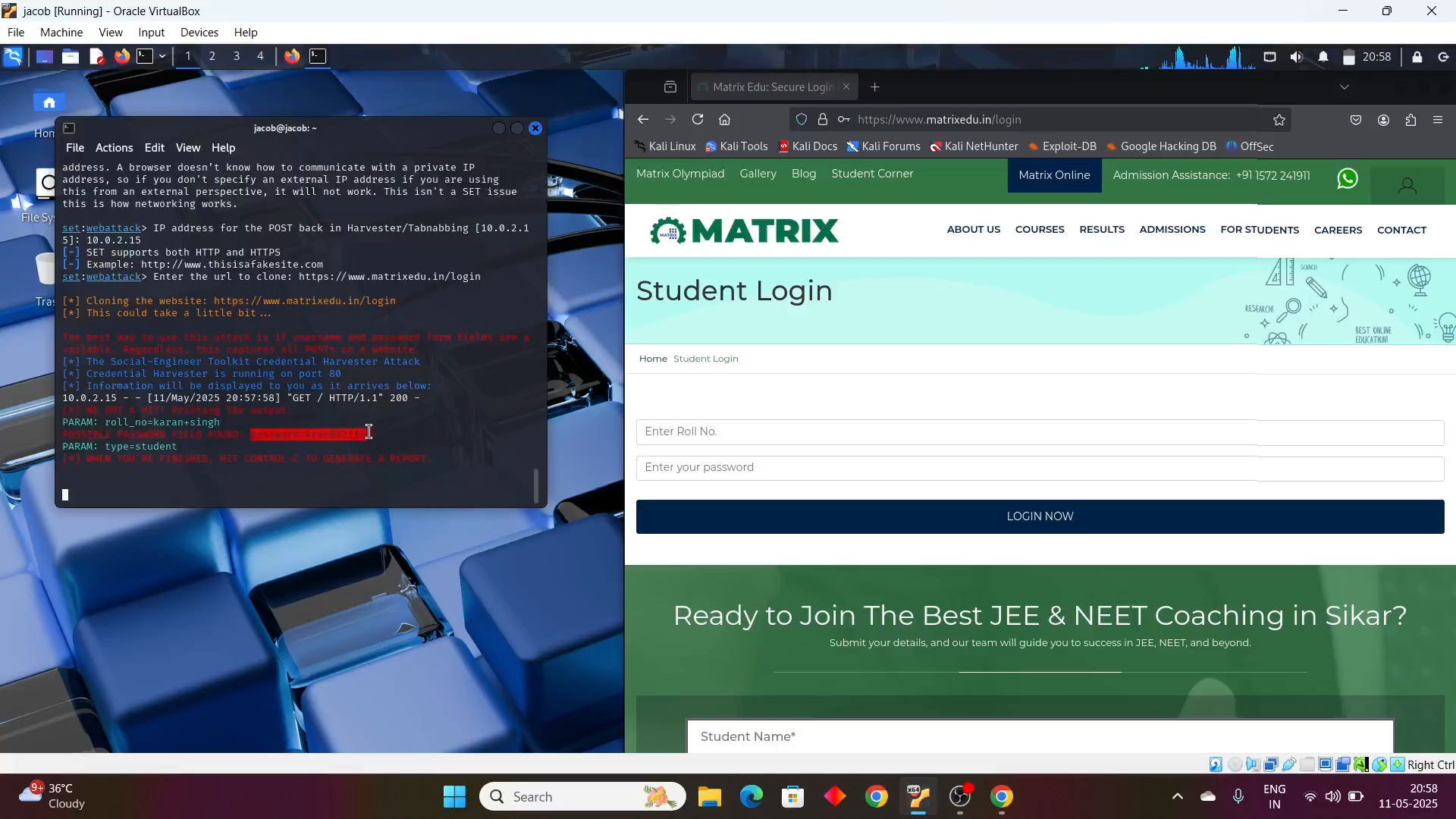
Selected: 3) Credential Harvester Attack Method

### using the Site Cloner Feature 🧬

Selected: 2) Site Cloner  
Entered my local IP address (e.g., 192.168.x.x)  
Cloned a real website (matrixedu.in, etc.)



### Apache Server & Credential Collection 📥

Apache server automatically started and hosted the phishing page.  


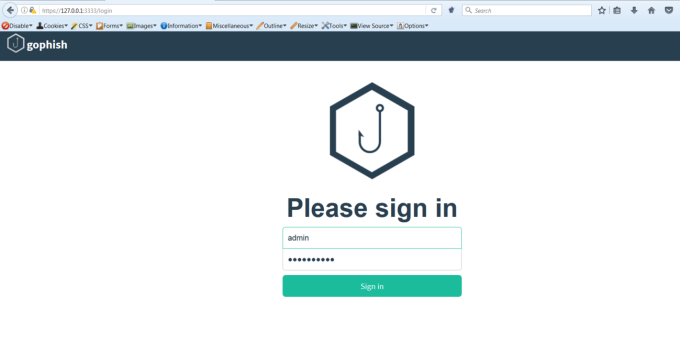
## ✅ Results:

• Successfully created a phishing page using SEToolkit.  
• Realistic cloned page was served using Apache.  
• Login credentials were captured and displayed in terminal logs.

# 2.Phishing Simulation using Gophish

## 🎯 Objective:

To design and execute a full-fledged phishing campaign using Gophish, including creating a landing page, email template, sending profile, and running the campaign to assess awareness among users.



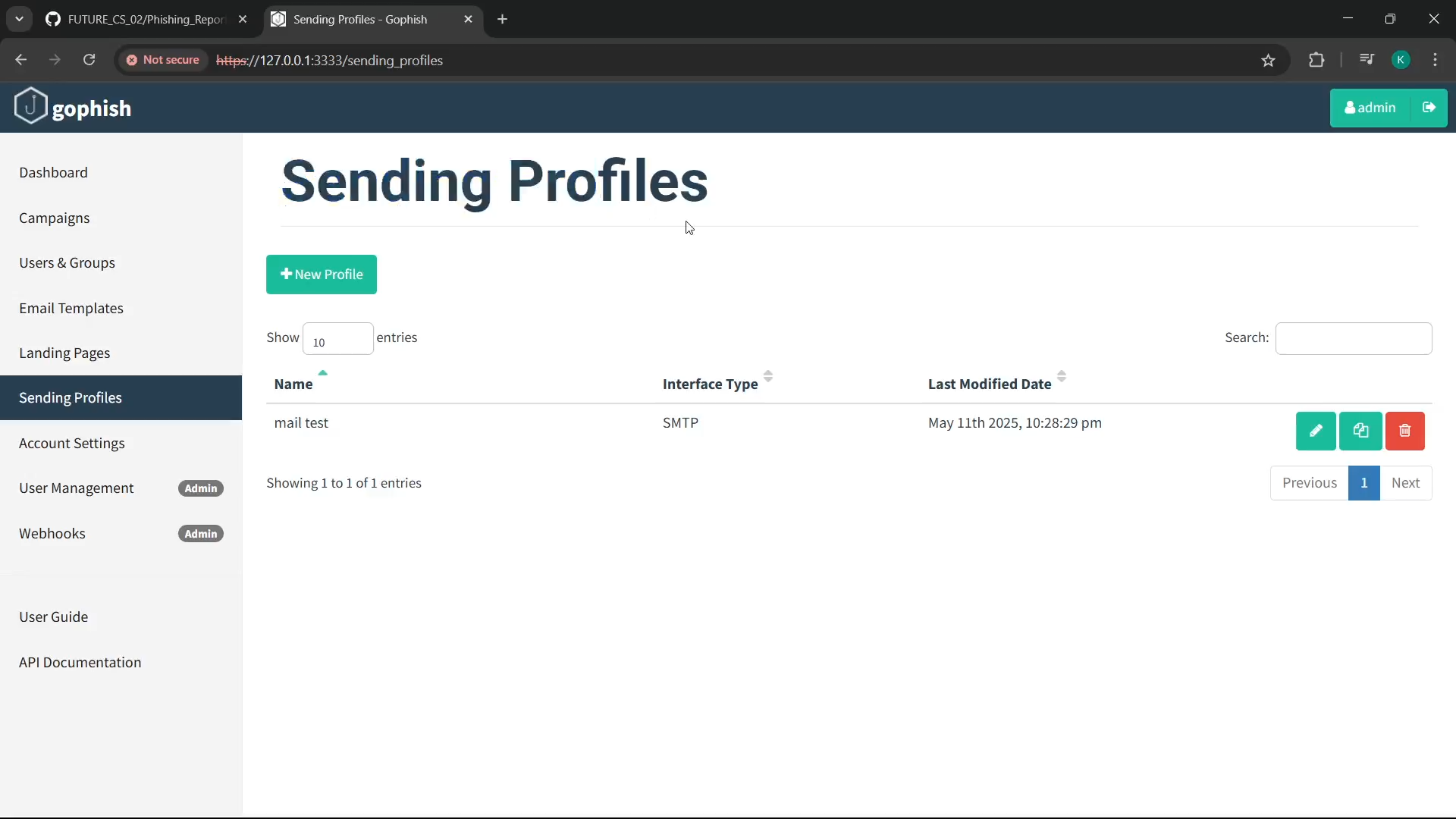
## 🧰 Tools Used:

• Gophish  
• Email SMTP (Gmail: sinxkaran3@gmail.com)  
• HTML Landing Page

## 📝 Step-by-Step Process:

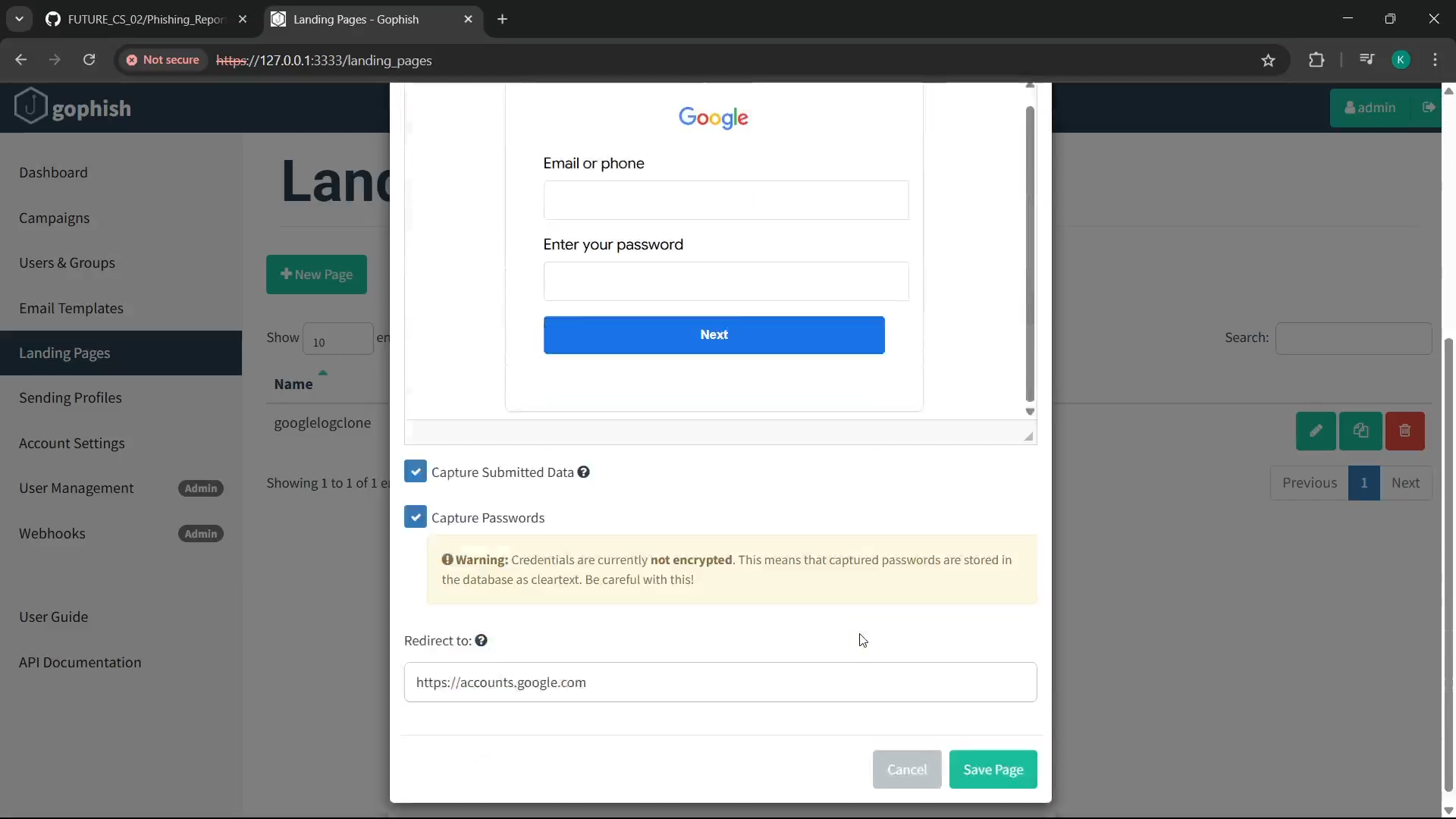
### Creating Sending Profile 💌

Configured Gmail SMTP settings.  
Spoofed email used: sinxkaran3@gmail.com



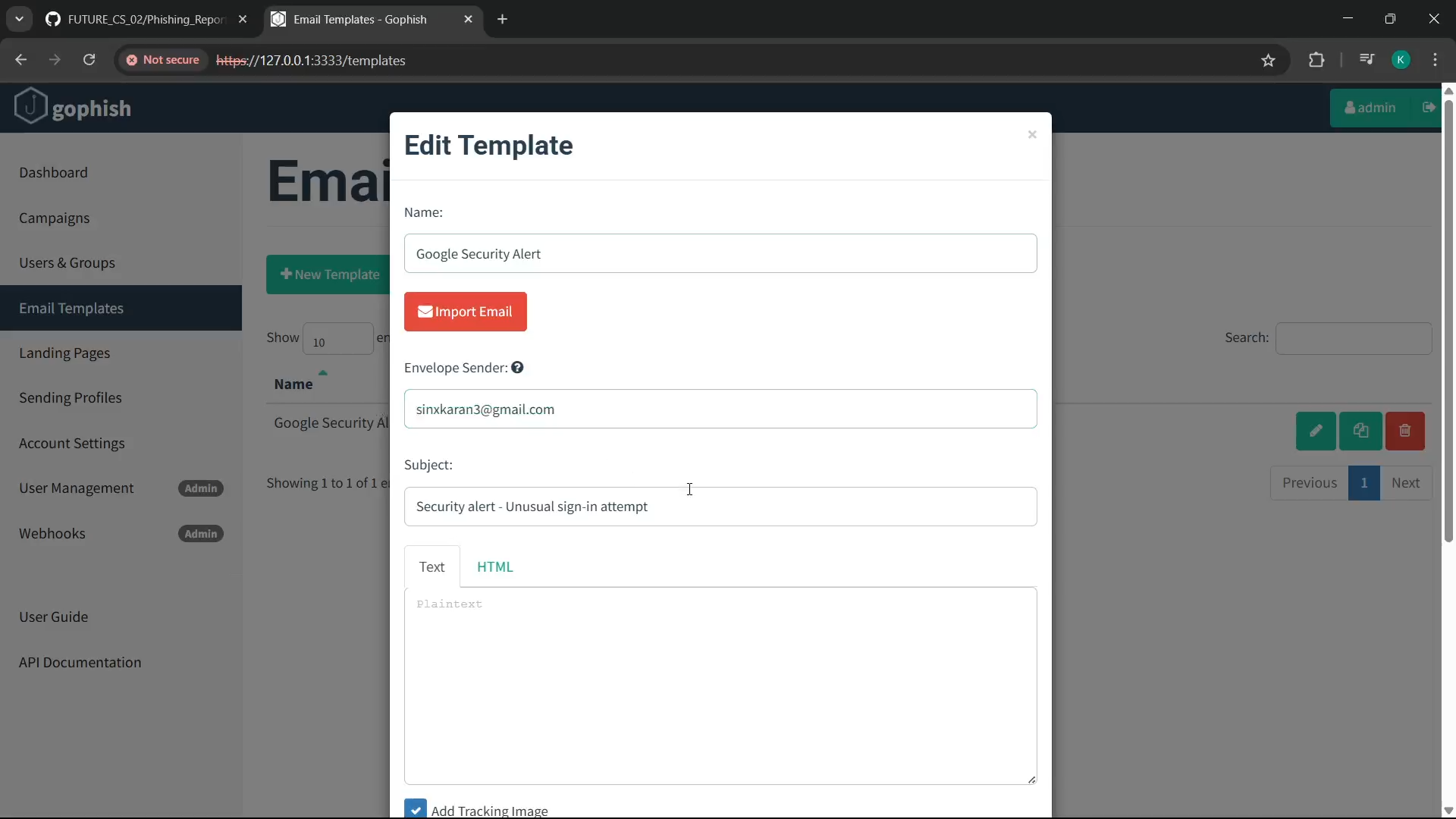
### Building the Landing Page 🖥️

Created a fake login page designed to collect usernames and passwords.



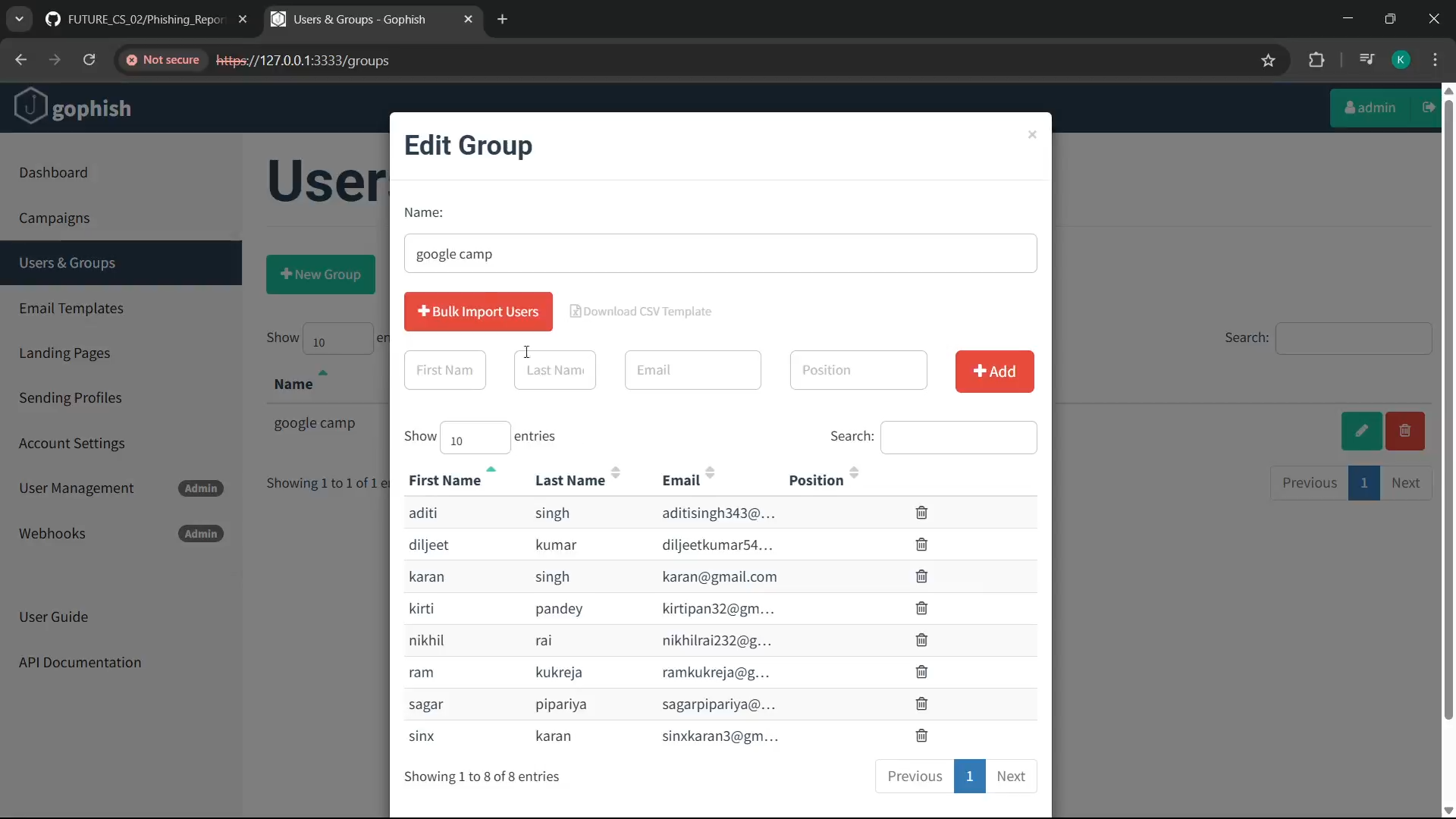
### Designing Email Template ✉️

Crafted phishing email with a convincing message.



### Launching the Campaign 🚀

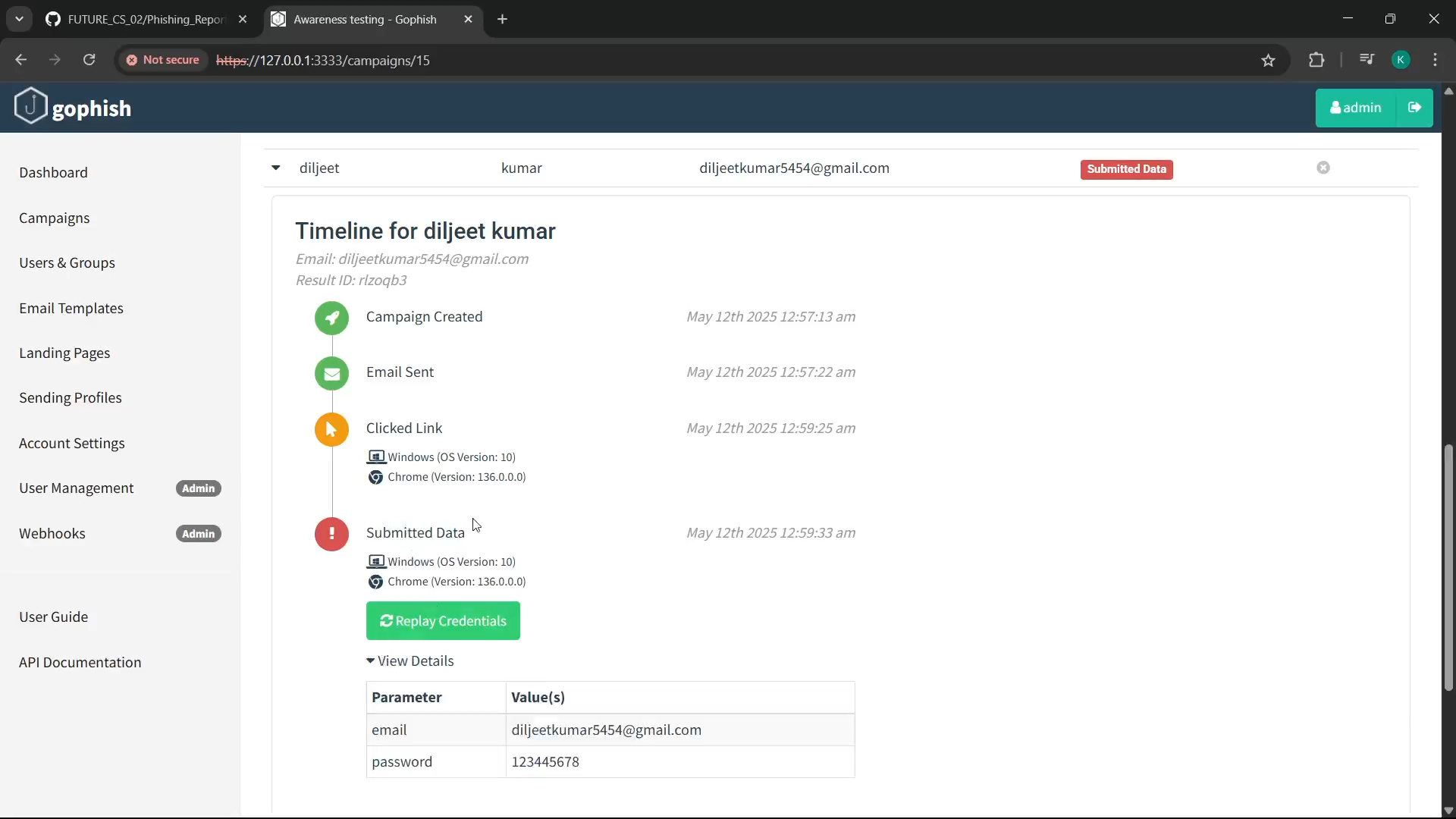
Campaign Name: Awareness Testing  
Target: 8 Emails



### Monitoring Campaign Performance 📊

Emails Sent: 8  
Emails Opened: 3  
Credentials Captured: 3





## ✅ Results:

• Phishing simulation completed successfully.  
• User interaction tracked through open and click rates.  
• Demonstrated real-world risk of phishing threats.

# 📌 Conclusion

Both SEToolkit and Gophish were effectively used to demonstrate real-world phishing attacks and simulations.  
- SEToolkit helped clone a website and collect sensitive data.  
- Gophish provided full simulation with tracking and analytics.  
  
🔒 This highlights the urgent need for regular security awareness training and stronger email protection measures within organizations.