**Phishing Simulation**

**User Manual**

**Introduction**

This document provides a step-by-step guide on conducting phishing simulations using the provided system. The guide is structured to help both administrators and users efficiently set up and execute phishing awareness campaigns.

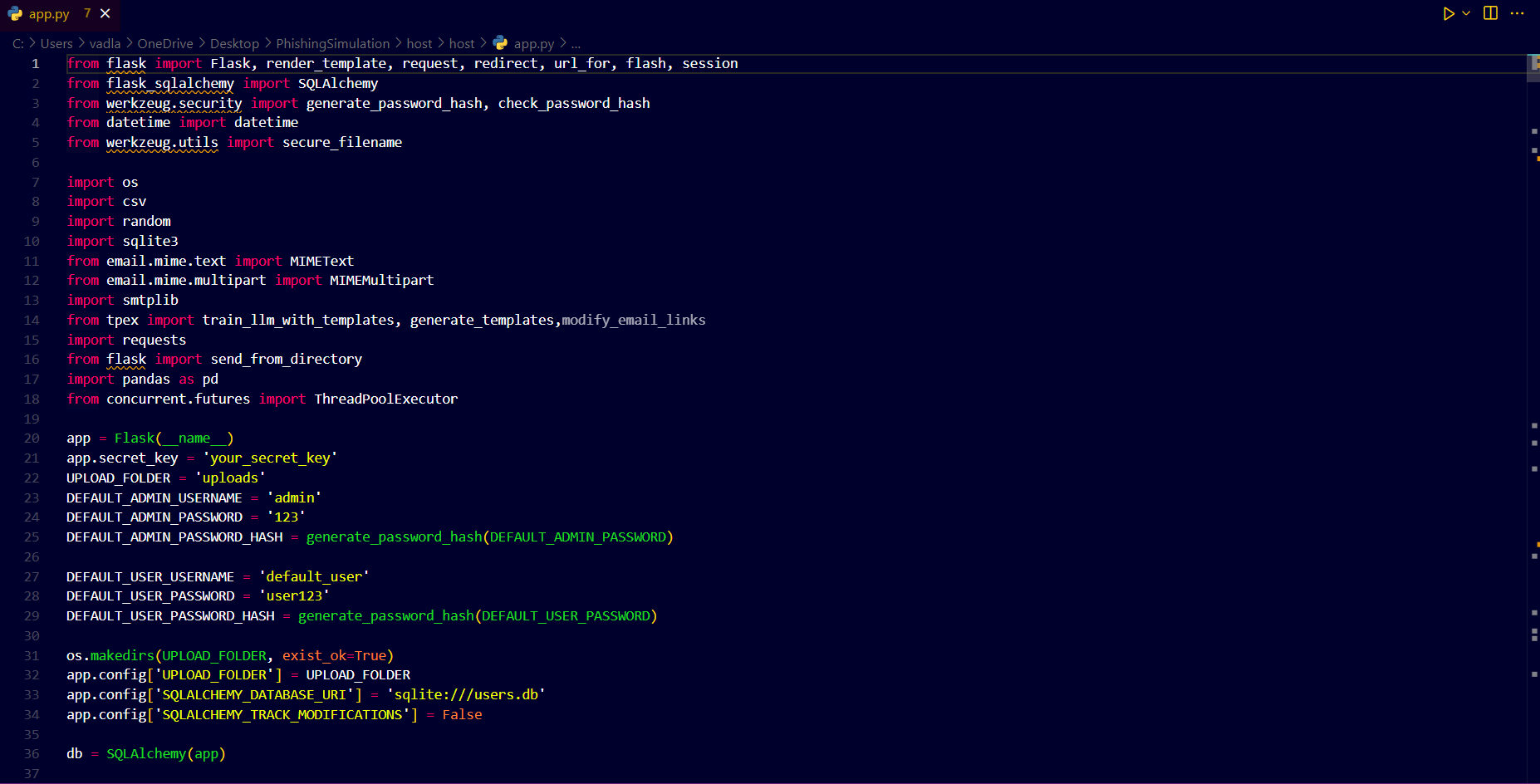
**1.Setting Up the Phishing Simulation**

**Step 1: Navigating to the Host Directory**

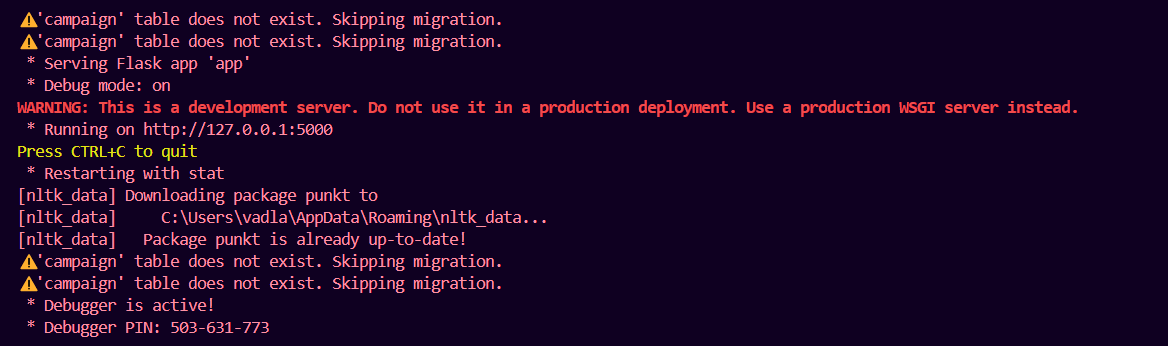
1. Ensure that all required files from the Git Repository are saved.
2. Navigate to the directory: User-Manual-Phishing-Simulation\host\ in order to start the Application.

**Step 2: Running the Application**

1. Open app.py in the host directory.
2. Now, run the script.



1. Once the script is running, a link will be generated: <http://127.0.0.1:5000>.
2. Click on the link while holding the Ctrl key to open it in your browser.



## 

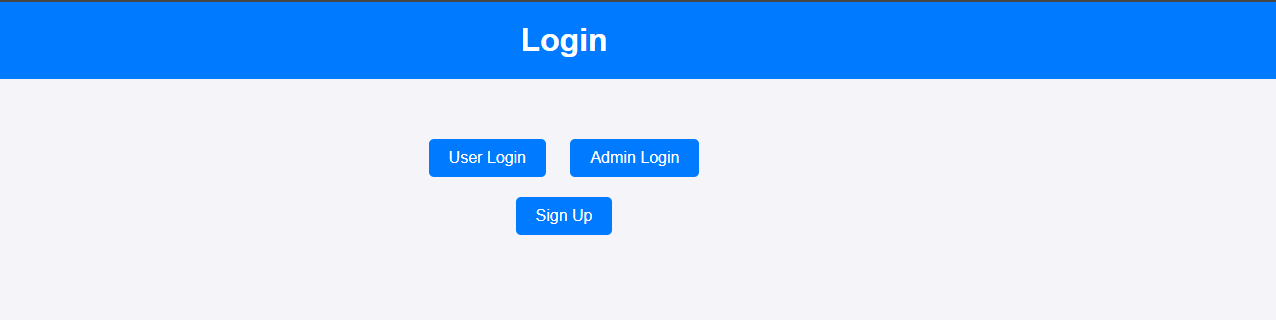
## ****2.Logging In to the System****

### ****Step 1: Redirecting to the Login Page****

1. Once the application is started by clicking on the generated link will redirect you to the login page.
2. Click on the **Login** button to proceed.

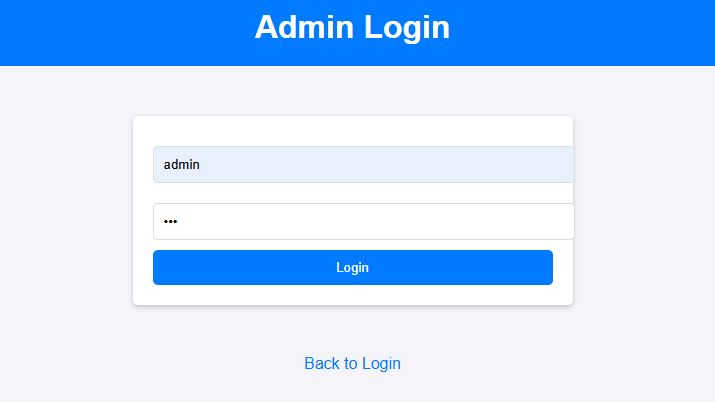


### ****Step 2: Types of Login Credentials****

The system provides two types of login credentials:

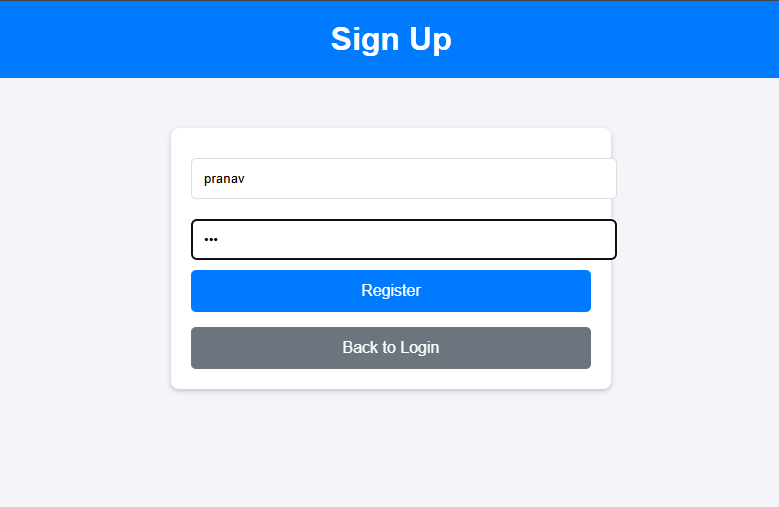
#### **Admin Login:**

* Used by Cyber Guard to monitor phishing campaigns.
* Admin credentials:
  + **Username**: admin
  + **Password**: 123
* Allows viewing, tracking, and managing campaigns.



#### **User Login:**

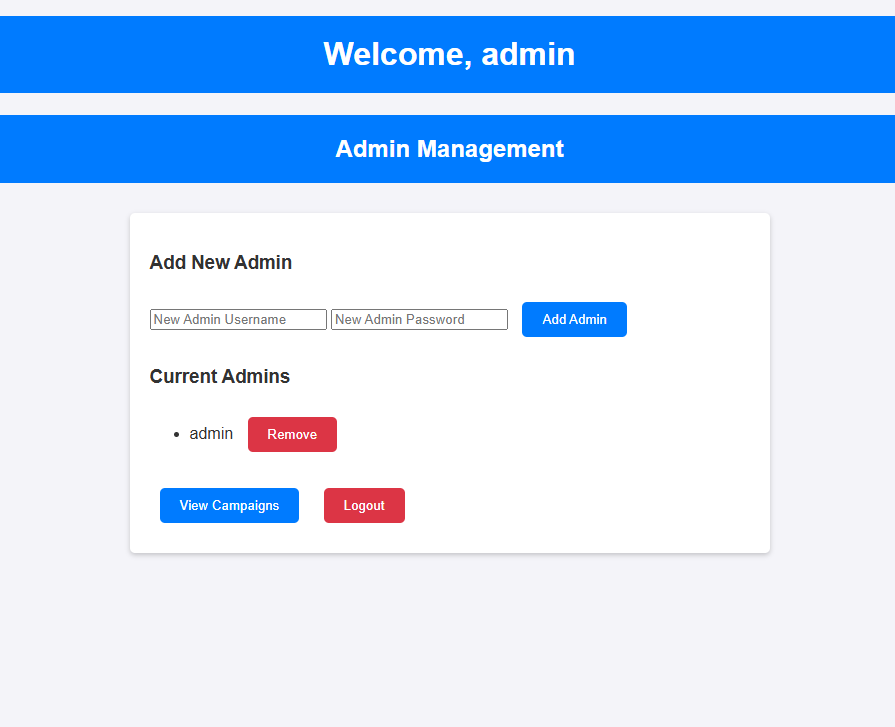
* Used by companies registered for phishing awareness campaigns.
* New companies must sign up before logging in.



## ****3.Admin Dashboard Overview****

### ****Monitoring Campaigns****

1. After logging in as an admin, you can view all active phishing campaigns.
2. The dashboard provides insights into:
   * Registered companies
   * Running campaigns
   * Performance metrics

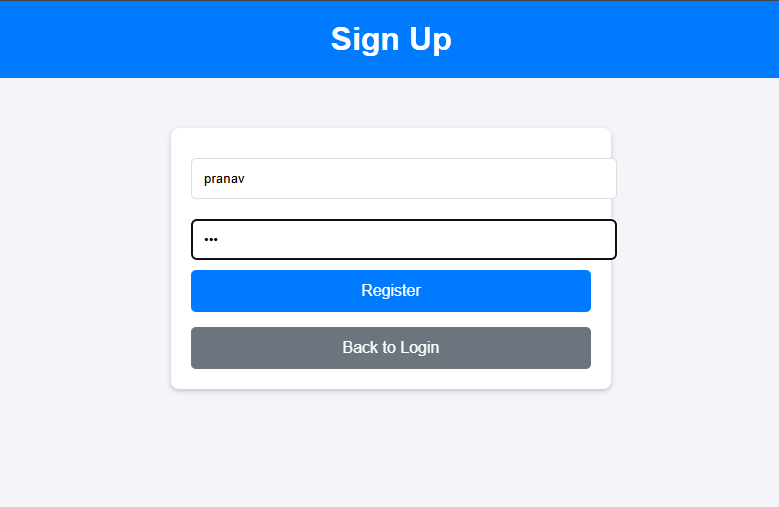


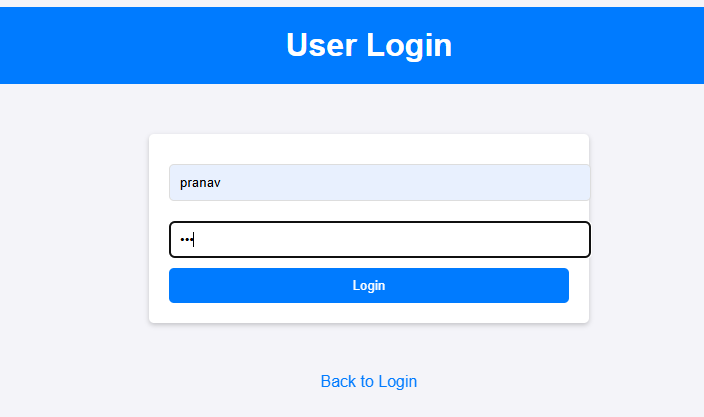


## ****4.Registering a New Company****

### ****Step 1: Sign-Up Process****

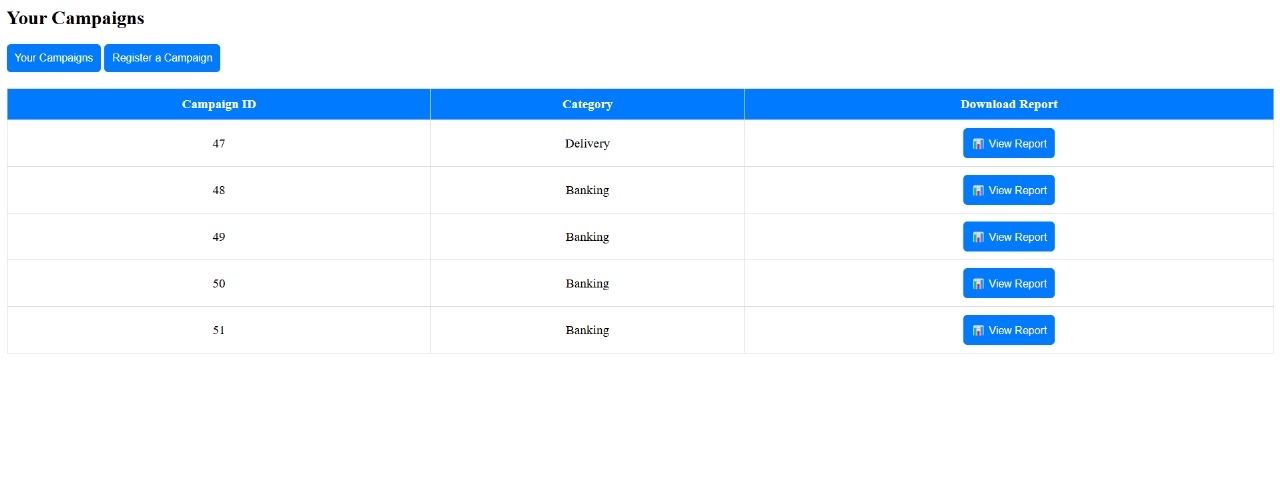
1. If a company is new, it must go through the sign-up process.
2. Provide the necessary details to create a user account.
3. Once signed up, log in using the newly created credentials.



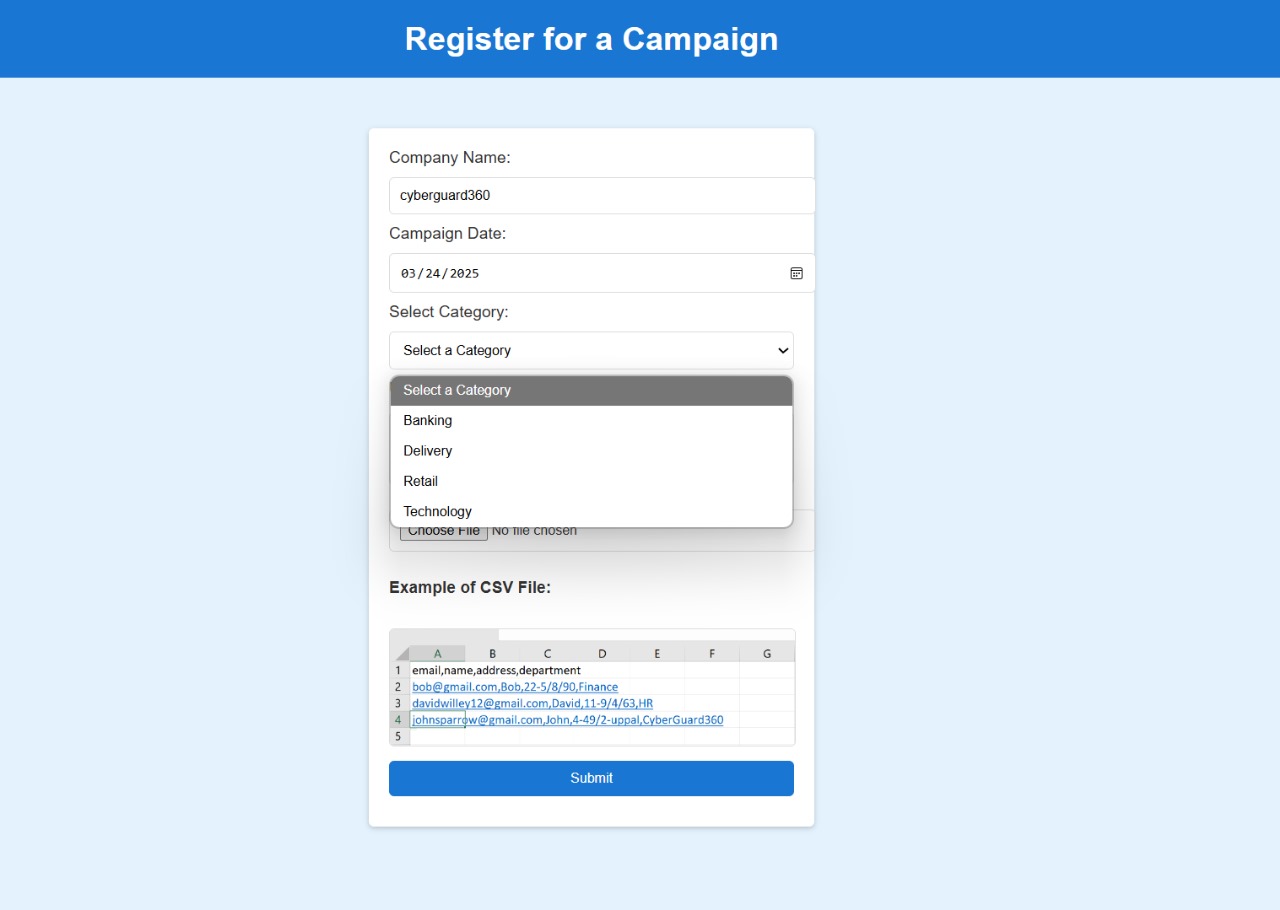


### ****Step 2: Running a Phishing Awareness Campaign****

1. After logging in as a user, access the campaign dashboard.
2. Click on ***Register a campaign***



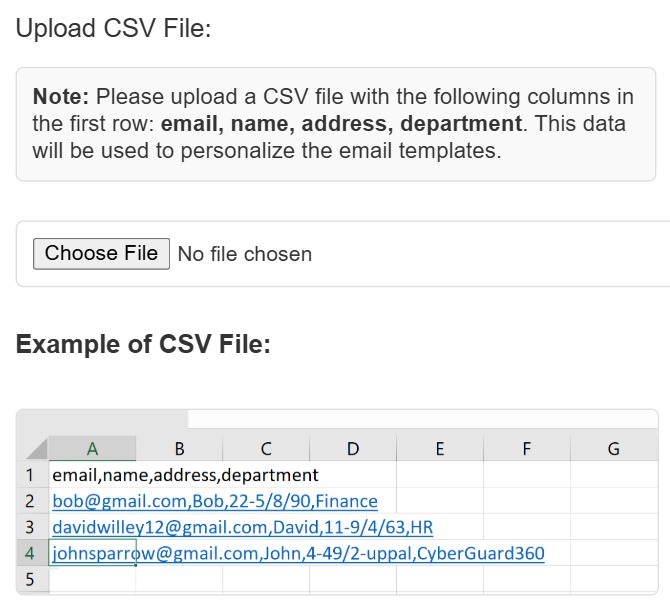
1. Enter the required details
   * Company name
   * Campaign date
   * Category of Phishing Email Templates



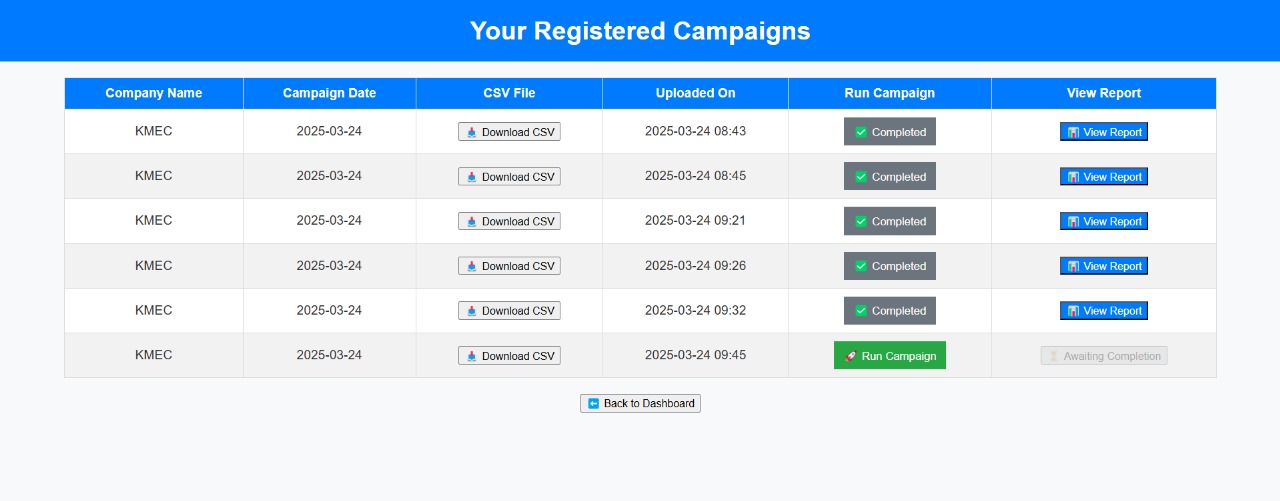
* + Upload the csv file (which consists of the details of the targeted audience)

Make sure you fill the details of the target audience details with only commas and not with spaces or any other characters

Note- The csv file should have the following first row mentioned as email,name,address,department and the respective target audience details in the following rows as shown in the below picture



1. On clicking on the submit button you are directed to the dash board again.
2. Click on the ***Your Campaigns*** button.
3. Click **Run Campaign** to initiate the phishing simulation.



1. Monitor campaign progress and employee responses through the dashboard.
2. Review reports and analytics to assess phishing awareness effectiveness.

### 

## ****Conclusion****

This guide provides a clear walkthrough for both admins and users to set up, monitor, and execute phishing awareness campaigns effectively. Ensure that all processes are followed correctly to maximize the impact of the simulation.