Ethical Phishing Simulation Platform

Introduction

The increase in phishing attacks targeting individuals and organizations highlights the urgent need for awareness and training. This project, Ethical Phishing Simulation Platform, aims to simulate phishing attacks in a secure environment for educational purposes. The goal is to test user awareness and enhance cybersecurity training.

Abstract

This project is a web-based phishing simulation platform built using Flask. It mimics a fake login page to demonstrate how easily users may fall for phishing emails. The system captures user credentials submitted on the form and immediately displays an awareness message. The project helps educate users about the risks of phishing and promotes good security habits.

Tools Used

- Python 3
- Flask Framework
- HTML/CSS
- SQLite (planned for data storage)
- SMTP (planned for email simulation)
- VS Code (for development)

Steps Involved in Building the Project

1. Set up a Flask web server in Python.
2. Created a fake login page using HTML and CSS to mimic a real login interface.
3. Captured user input data (email and password) through POST

request.
4. Logged captured credentials to the terminal for analysis.
5. Displayed an awareness message post-submission to educate the user.
6. (Planned) Integration of SQLite database for logging captured data.
7. (Planned) Sending phishing emails through SMTP for realistic campaigns.

Conclusion

The Ethical Phishing Simulation Platform demonstrates how phishing attacks can be ethically replicated in a controlled environment for training purposes. It successfully simulates a phishing scenario and educates users about the importance of recognizing suspicious links. Future upgrades may include email delivery, dashboards, and automated analytics.