CIS 641 01 - IP - Systems Analysis and Design (F24)
Final Presentation

PASSWORD STORE MANAGER

Team Members :

Likitha Magham

Swethasarayu Simhadri

Bhavana Arla

Team Roles and Responsibilities:

- **Likitha:** Developer and Tester, responsible for implementing core functionalities and ensuring secure and user-friendly features.
- **Bhavana:** Backend Developer, focused on designing and integrating the SQLite database for secure data management.
- **Swetha:** Frontend Developer, created an intuitive user interface seamlessly connected to the backend.

Introduction :

In today’s digital world, managing multiple passwords is challenging. Many users rely on weak or reused passwords, increasing the risk of breaches. The Password Store Manager offers a secure, user-friendly solution with features like PIN-based authentication and a delete-only mechanism. By prioritizing simplicity and security, it ensures sensitive information remains accessible only to authorized users. This project provides a practical approach to solving a critical issue in digital life

Project Overview:

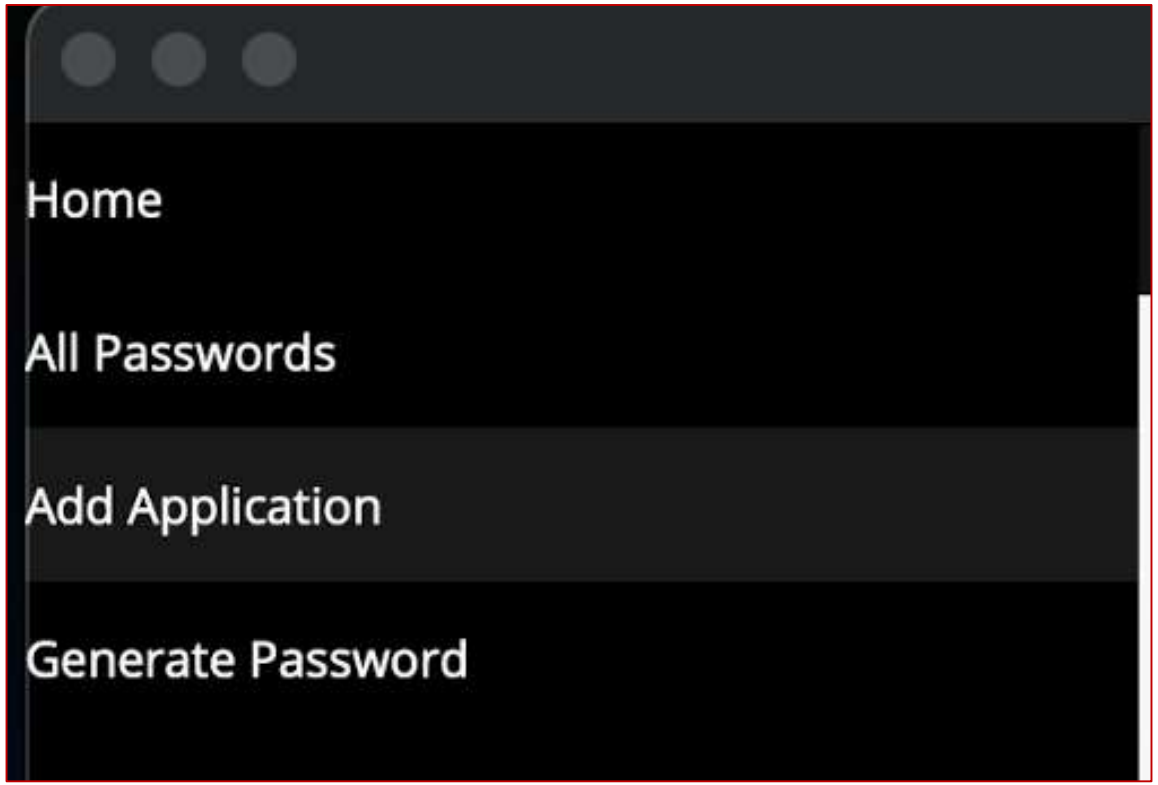
"The Online Password Manager is designed to securely store, generate, and retrieve passwords for users, addressing growing concerns about data breaches and password safety.

Key Features:

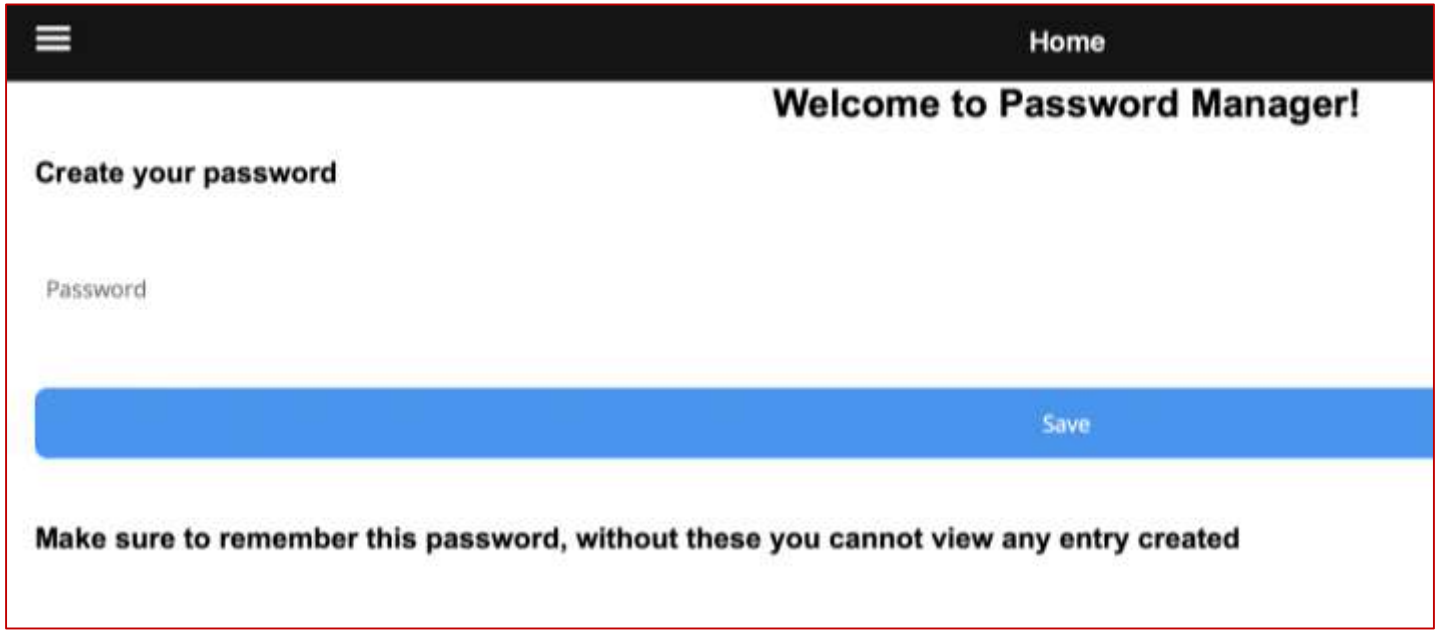
- Password Generator: Creates strong, random passwords for enhanced security.
- Secure Storage: Safely stores passwords in an SQLite database, accessible only through the application.
- Password Retrieval: Allows users to retrieve passwords securely when needed.
- Delete-Only Functionality: Enhances security by enabling users to delete passwords or data but prevents updates or regeneration to avoid unauthorized changes.

Project Timeline

1. Flyout Pages:

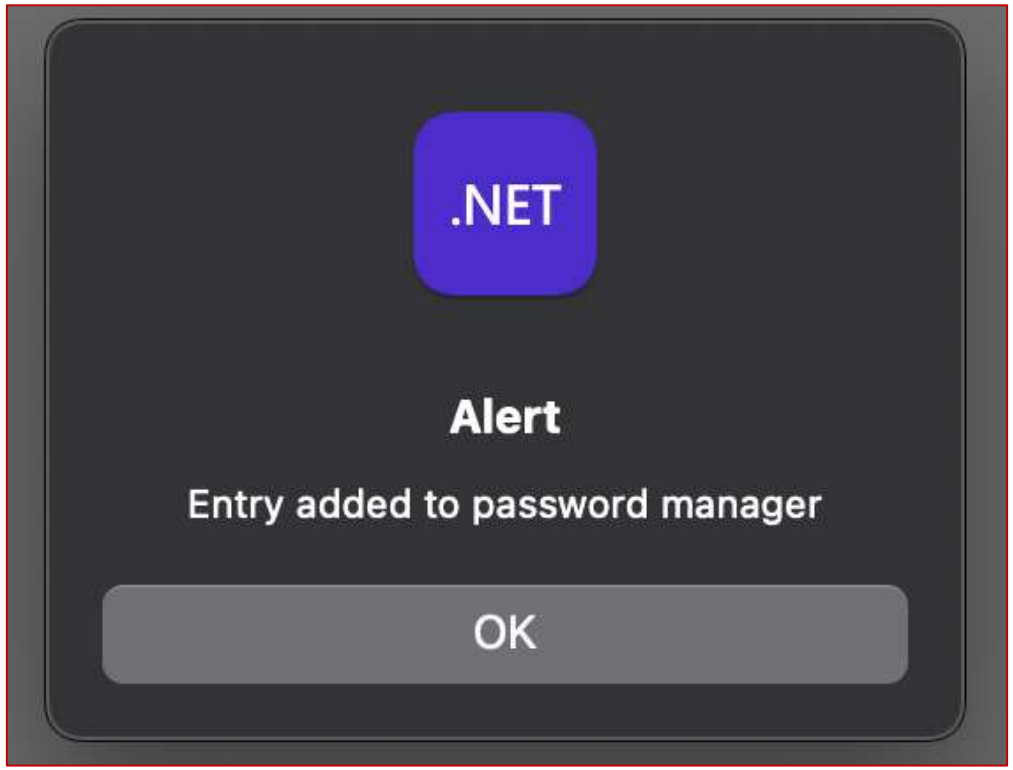


2.Home page asks for a Password or Pin setup:

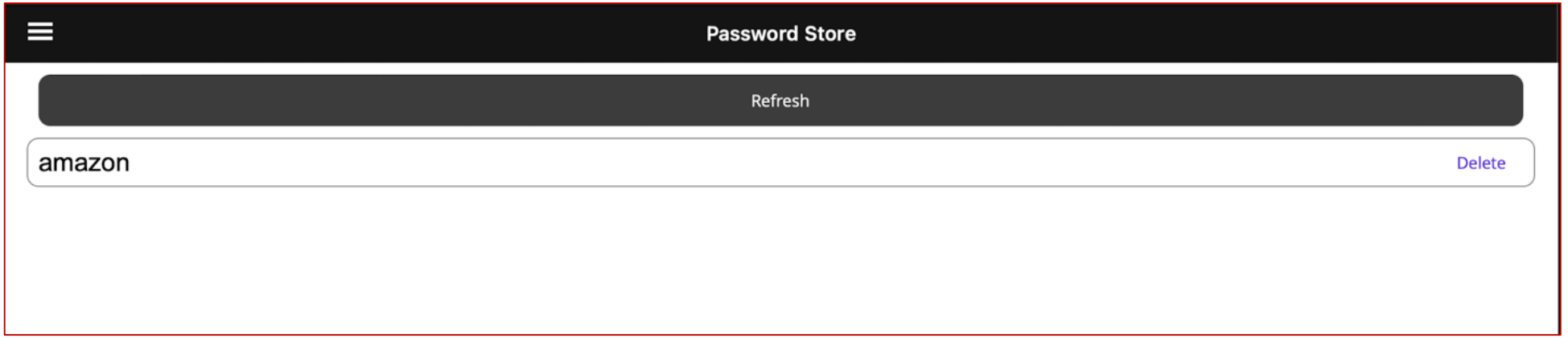


3.Add application page lets you add the application name and password:

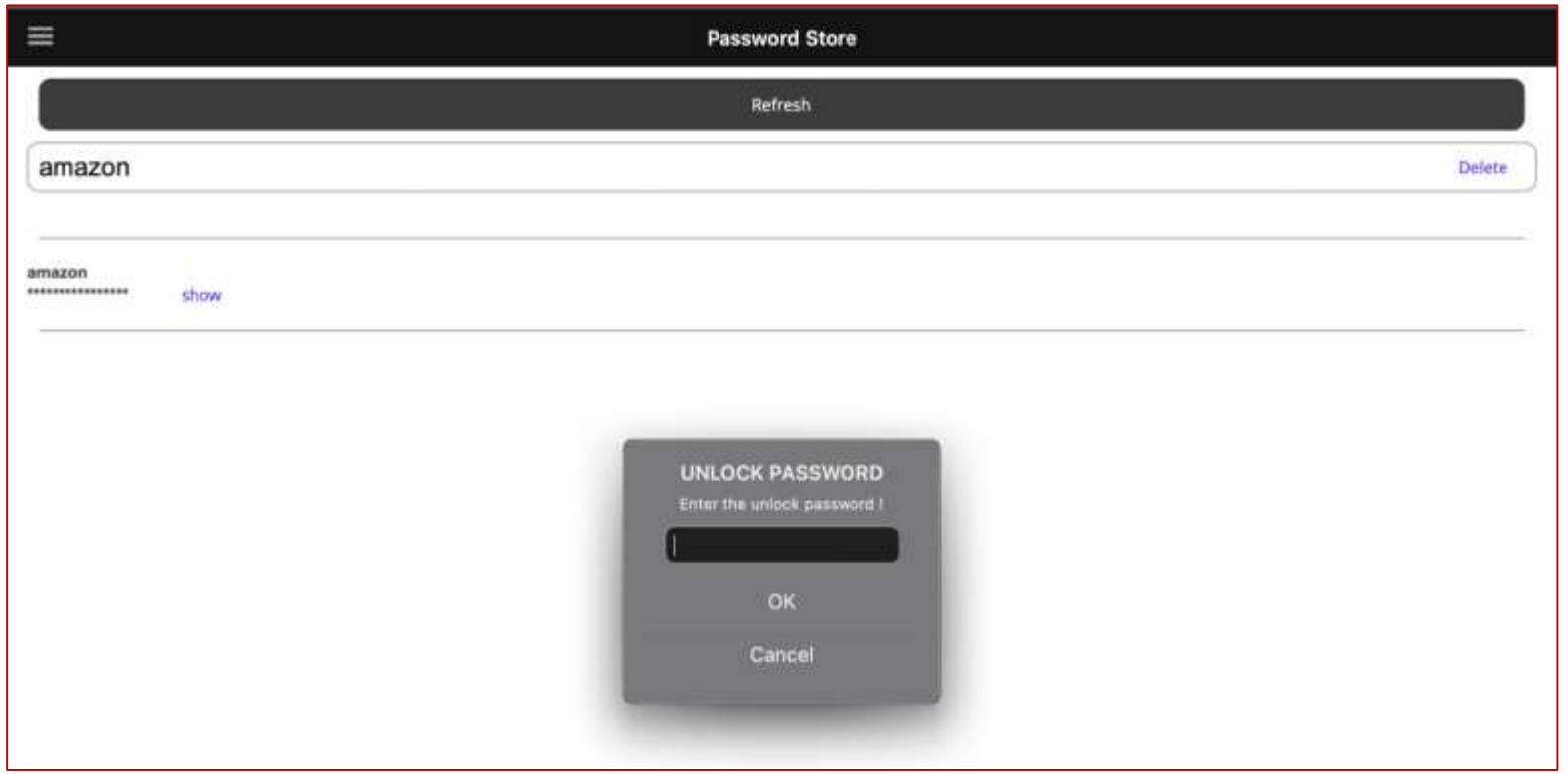
4. Application gives the Acknowledgement that the entry is added to the password manager:



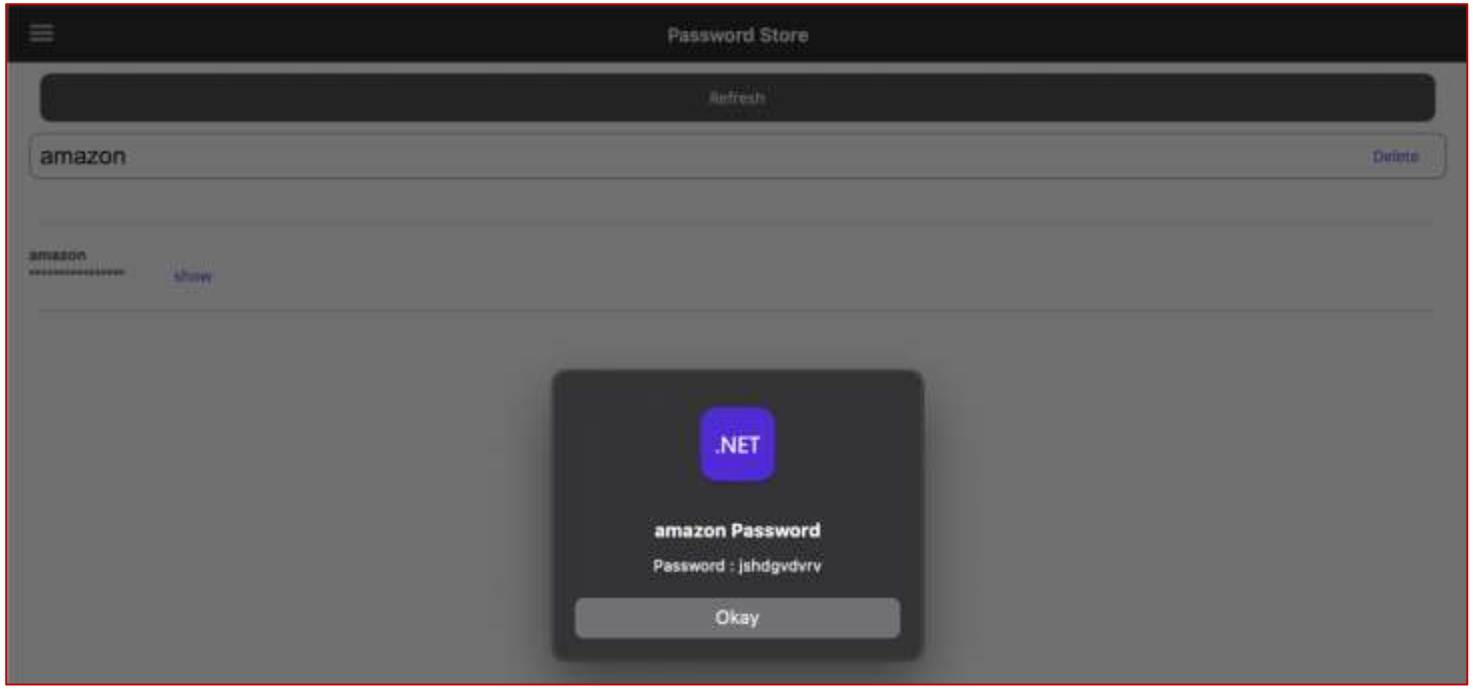
5. Added entry is shown in the Password store:



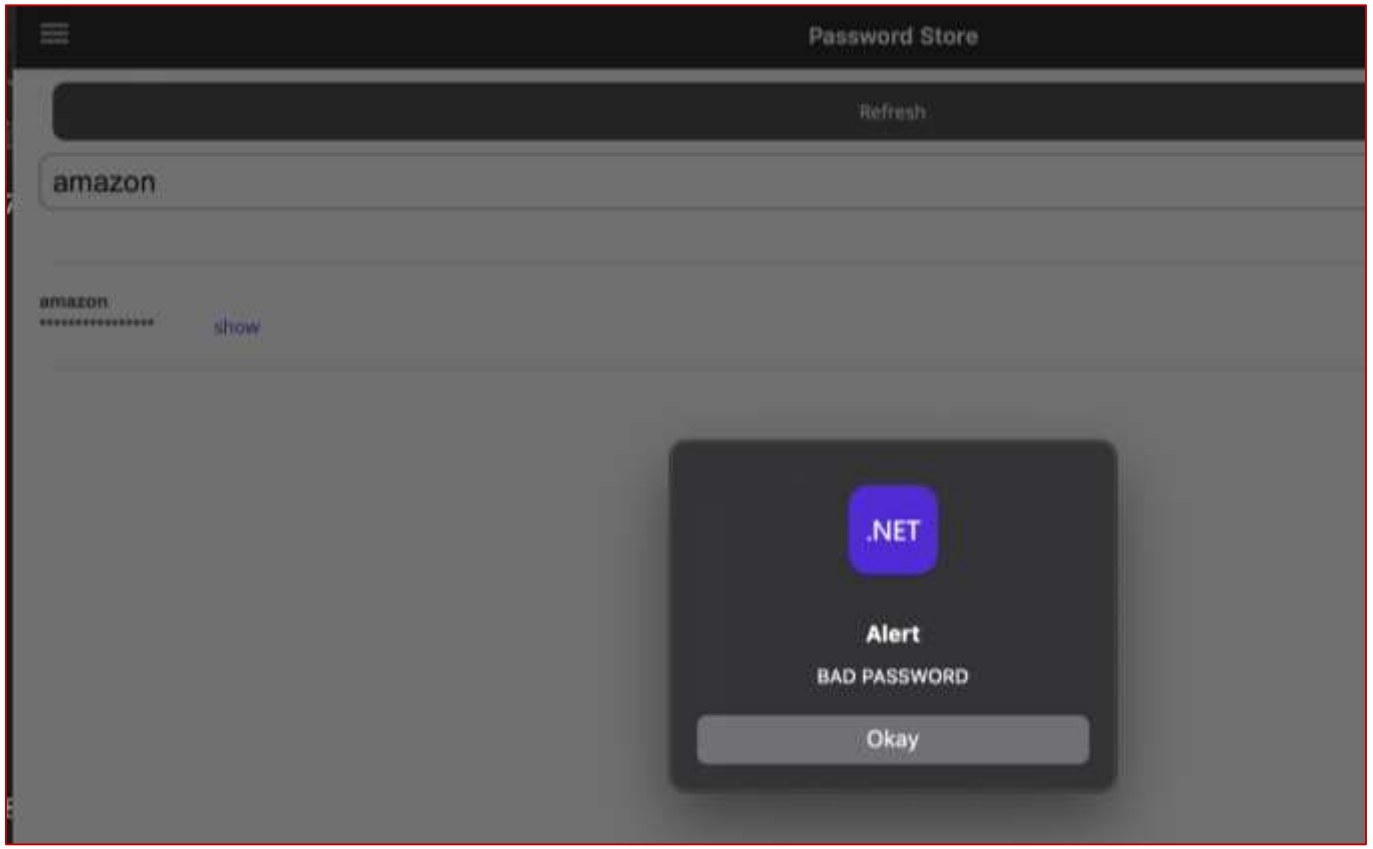
6.If the user wants to see the password, the application asks for a pin that is set-up by the user in the starting page:



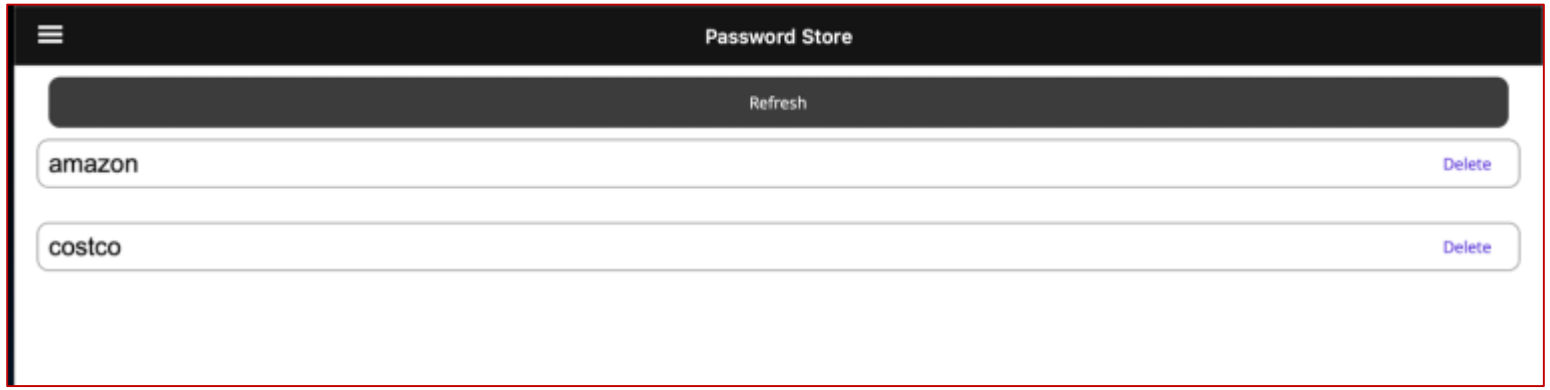
7.After user enters the correct pin, the password will be visible.

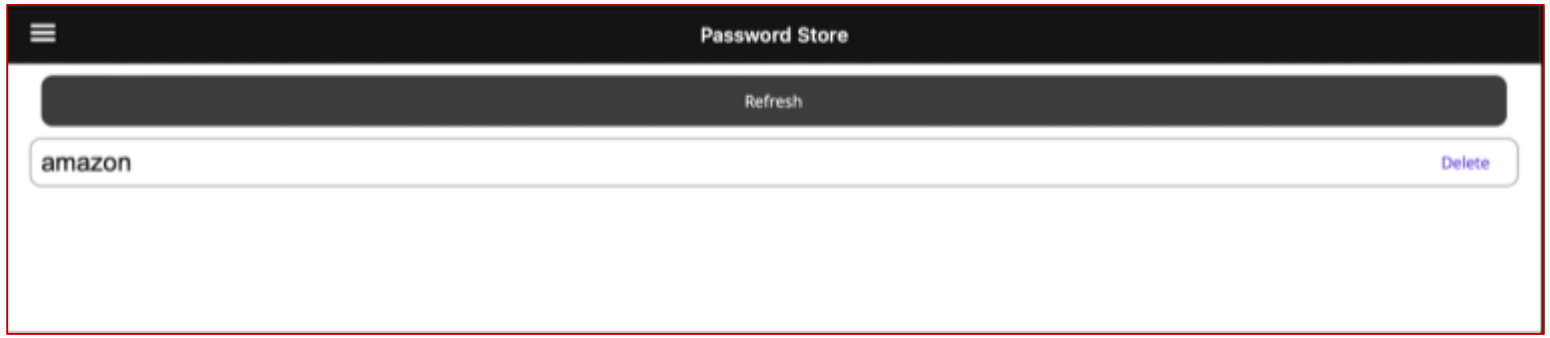


8.If the user enters the wrong pin, then application shows an alert message that the entered pin is bad:

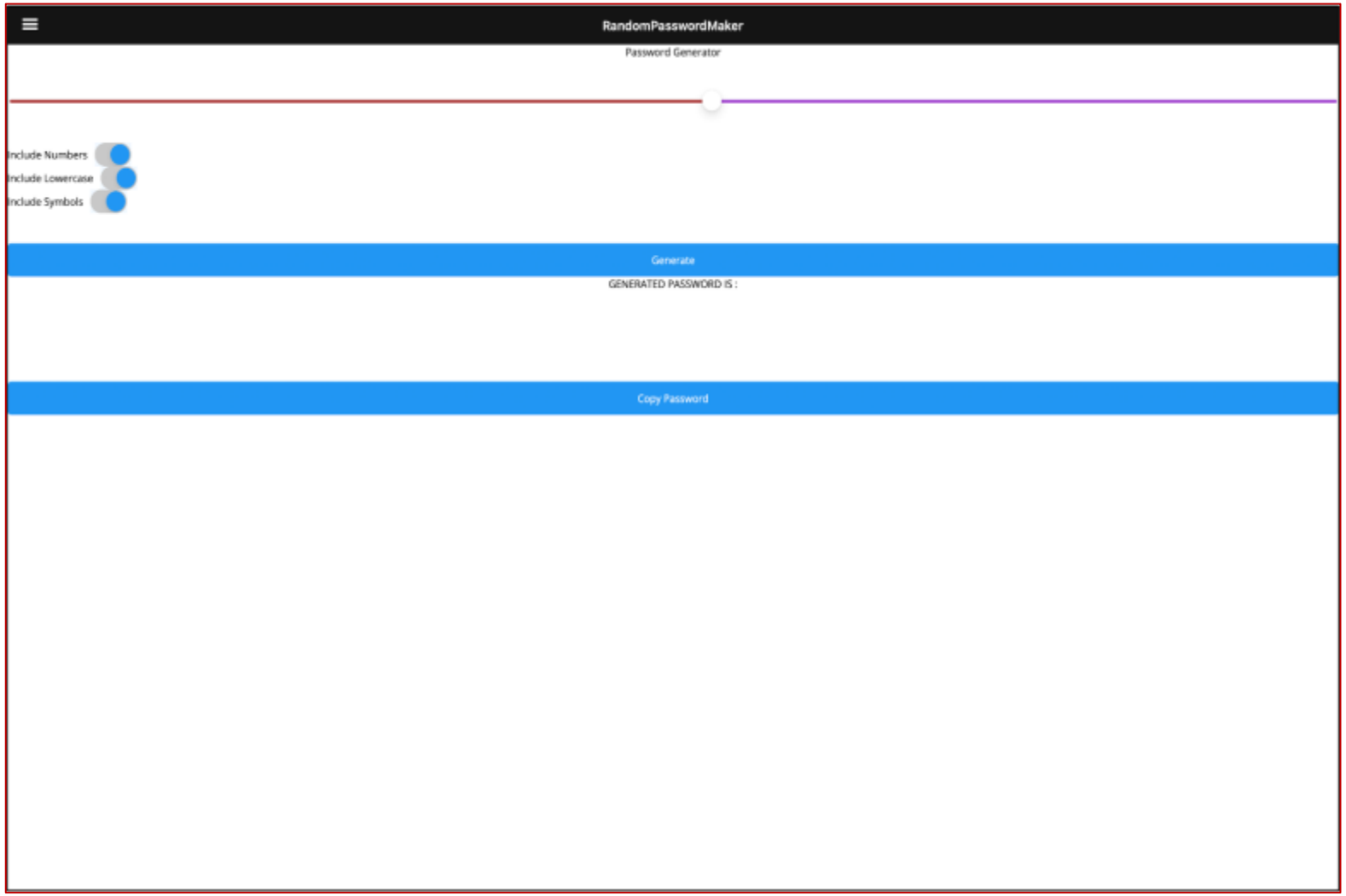


9. If the user wants to remove any saved passwords, he can directly delete those from the Password Store





10.Random Password Generator Page:



Thank You