Archers Password Inventory (A.P.I.)

Dax Tangco - CPE, dax_axis_tangco@dlsu.edu.ph
Yuan Obias - IE, yuan_obias@dlsu.edu.ph
Aron Zuniga - CPE, aron_zuniga@dlsu.edu.ph

Abstract

The Password Manager project aims to offer a secure and user-friendly solution for managing passwords, addressing the challenge of remembering numerous passwords for various accounts. This application is designed to enhance security and convenience with a simple and intuitive graphical user interface (GUI).

Key features include:

- **Login**: Users must log in with a registered username and password to access their saved accounts.
- **Registration**: Users can create an account by providing a username, password, and confirmation password.
- **Account Reset**: Each registered account will have a reset key for password recovery, stored locally by the user.
- **Data Storage**: Usernames and passwords are stored in an encrypted database to ensure security.
- **Add Password**: Users can store new passwords with associated service names and usernames, optionally encrypted.
- **Retrieve Password**: Allows users to securely retrieve stored passwords by providing the service name and optional key.
- **Edit Password**: Users can update saved usernames or passwords as needed.
- **Delete Password**: Users can remove stored passwords by specifying the service name and associated key.
- **Generate Password**: Users have the option to generate secure passwords to meet various platform requirements.

The project also features a table view displaying all stored services and corresponding usernames, without showing passwords. This design balances accessibility and security, helping users manage their passwords efficiently.

Introduction

In today's digital world, managing multiple accounts with unique passwords is a common challenge. Users often struggle with tracking and remembering passwords for different platforms, leading to security risks and frustration. Existing password management solutions address some of these issues, but there is still a need for a more user-friendly and secure option.

Our target users are individuals who find password management challenging and have difficulty recalling passwords for various accounts. These users face problems such as forgetting passwords, reusing weak passwords, and encountering the tedious process of password recovery. Our app aims to solve these issues by storing and managing passwords securely, allowing easy access to credentials without compromising security.

This application is significant because it addresses a crucial aspect of digital security. By offering features such as password generation, encrypted storage, and easy retrieval, our app enhances overall account security and encourages essential cybersecurity habits. This practical and reliable password storage solution helps users avoid the hassle of data breaches and promotes better cybersecurity practices, ultimately contributing to a safer digital environment.

Functionalities

Persona	Description	Benefit
Business Entities	**Feature 1: Registration / Login** The program stores the data of different users that have registered. It will allow the user to login and see their saved passwords. Business Entities can utilize this in order to keep the sets of passwords of their employees secure.	The password manager can store multiple different data depending on the different users that logged in. This makes the program more secure. The user can save their data and access it with the same account.
Cybersecurity Worker	**Feature 2: Encrypted Database** The application provides secure storage and management of multiple	The passwords will be in a secure database and will not be easily accessed by hackers. This will keep the data of each user secure. The encryption method is

	passwords. It generates strong, unique passwords for various accounts and saves them in an encrypted database for easy retrieval. This encryption method is simple but effective and can be utilized effectively in other situations or projects by Cybersecurity workers.	beneficial for workers who deal with cybersecurity related issues.
New Internet Users	**Feature 3:User-friendly UI** The program has a clean and simple user interface with intuitive controls for adding, retrieving, and deleting passwords. Overall, it shows all the elements in an organized manner, and it is easy to follow. There are always new internet users that may get confused. The UI is designed in this way to make it understandable and easy to follow for new users.	Users can easily manage their passwords without a steep learning curve, improving the overall user experience. This will make it more accessible to new users or people who are not used to the internet yet.
Students	**Feature 4: Filter / Search feature** The table in the UI shows all saved passwords, which are masked for security. Users can search for specific platforms to retrieve or delete passwords. However, they will require a key that they will make, in order to filter and search for their passwords. Students may have to organize their passwords in different applications, websites, institutions, etc.	Users can efficiently manage and find their passwords, saving time and effort in maintaining their credentials. The filtering and searching feature can aid students in looking for passwords efficiently.

Walkthrough

Run the password manager:

```
API
```

User Registration:

Click on the 'Register' button.
Fill in the username, password, and confirm the password.
A message box will display the reset key. Copy this key for password recovery purposes.

User Login:

Enter your registered username and password.
Click on the 'Login' button to access the password manager interface.

Forgot Password:

Click on the 'Forgot Password' button.
Enter your username, reset key, new password, and confirm the new password.
Click on the 'Confirm' button to reset your password.

Password Manager Interface:

Add new credentials by entering the alias, platform, username, and password, then click 'Add'.
View stored credentials by selecting an entry and clicking 'Show'.
Edit credentials by selecting an entry, making changes, and clicking 'Edit'.
Delete credentials by selecting an entry and clicking 'Delete'.
Log out by clicking the 'Log Out' button.

Security

Password Hashing: User passwords are hashed using SHA-256 before storing in the database.
Encryption: Stored passwords are encrypted using AES-256 to ensure security.
Reset Key: A reset key is generated and encrypted using AES-256 for secure password recovery.

Video Walkthrough:
https://drive.google.com/file/d/1ZXxl0lLBrbDuvulj3TxdPxTHH38RX_8W/view?usp=sharing