Title: Week 3 Report

Date:20/06/2023

**Password Manager by Python**

By Sai Harika P , Sai Lavanya K , Revathi M , Rizwana D , Poojitha V

1. **Introduction**:

In this report, we will provide an overview of the progress made during Week 3 of the development of a password manager using Python. The password manager aims to securely store and manage user passwords for various online accounts.

**2. Accomplishments:**

a. Database Integration: During Week 3, we successfully integrated a database system into the password manager project. This allows us to store and retrieve encrypted user passwords securely. We chose SQLite as the database engine due to its lightweight nature and ease of integration with Python.

b. User Interface Improvements: We made significant improvements to the user interface (UI) of the password manager application. We implemented a more intuitive and user-friendly design using the Tkinter library in Python. The UI now includes features such as login, registration, password entry, and retrieval.

c. Encryption and Decryption: To enhance security, we implemented encryption and decryption mechanisms for storing and retrieving passwords from the database. We used the cryptography library in Python to achieve this. The encryption algorithm ensures that passwords are securely stored, even if the database is compromised.

d. Testing and Bug Fixes: We conducted extensive testing during Week 3 to identify and fix any bugs or vulnerabilities. We performed unit tests on different components of the password manager, including user registration, login, password storage, and retrieval. We also addressed any identified issues promptly.

3. **Challenges:**

a. Database Schema Design: Designing an efficient and secure database schema was a challenging task. We needed to carefully plan the structure of the tables and relationships to ensure optimal performance while maintaining data integrity and security. We took help from some sources available from google and python in advance level book from our library.

b. User Interface Design: Creating an intuitive and user-friendly interface required thorough consideration of user experience (UX) principles. We conducted several iterations to improve the UI and gather feedback from users to make it as user-friendly as possible.

4. **Next Steps:**

a. Password Generation: In the upcoming week, we plan to implement a password generation feature within the password manager. This feature will allow users to generate strong and unique passwords for their accounts automatically.

b. Browser Integration: We aim to integrate the password manager with popular web browsers to enable seamless autofill functionality. This will further enhance the user experience and convenience.

c. Multi-Factor Authentication: To strengthen security, we will implement multi-factor authentication (MFA) options in the password manager. Users will have the choice to enable additional authentication methods, such as OTP (one-time password) or biometric authentication.

d. Security: We will conduct a comprehensive security audit of the password manager to identify and address any potential vulnerabilities. This will include code reviews, penetration testing, and threat modelling.

5. **Conclusion:**

Week 3 was productive in terms of database integration, user interface improvements, encryption, and testing. We are making steady progress towards developing a secure and user-friendly password manager. The upcoming week will focus on implementing password generation, browser integration, multi-factor authentication, and conducting a security audit to ensure the reliability and robustness of the application.

Report by

Sai Lavanya K

Email:sailavanya1509@gmail.com