**Group 5 Password Manager Application**

**Group Members:** Ash Burks, Chris Stewart, Kelsey Hodge, Ryan Gossage

**Requirements Section**

**Personas**

* User Persona
  + People who need a tool to easily lookup and update passwords
  + People who need to frequently change complex passwords, possibly for multiple accounts at work for example
* Hacker Persona
  + Person who wants to gain unauthorized access to users passwords to steal their login information for various accounts. Wants to exploit weak security measures in order to gain unauthorized access.

**User Stories**

* User
  + I want to store my passwords in one secure location so they are easy to access and secure.
  + I want to easily copy passwords so I don’t have to manually type them in each time.
  + I want to be able to query my passwords.
* Hacker
  + I want to find weak passwords to break into user accounts and steal data.
  + I want to gain unauthorized access using stolen passwords.

**Functional Documentation**

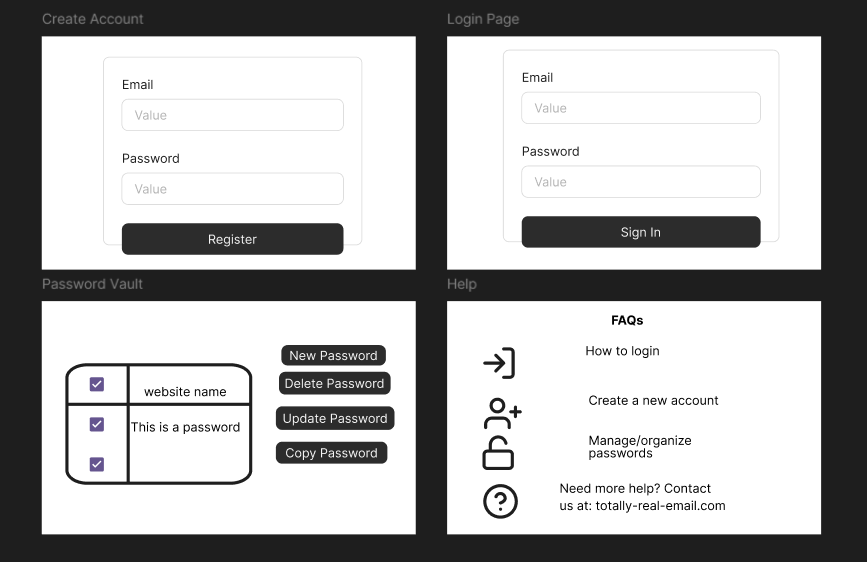
* Allow users to register and login to the password manager
* Ensure no duplicate accounts are created
* Enforce a registration password complexity requirement: At least 8 characters with at least one uppercase character, one lowercase character, one number, and one special character. If the password does not meet the requirements, the user will be prompted again.
* Authenticate the users credentials, and deny access if this fails.
* Track login attempts and deny access after three failed attempts
* Allow users to manage, access, and organize their passwords securely. As well as add, update, delete, and copy passwords through the web interface.
* Display list of password entries in a form or table which are obscured until clicked on
* Allow user to query password entities through a form
* Utilize a database to store user account credentials and password credentials (SQL, or potentially PHP)
* Push and pull from web server to an SQL database

**Help Documentation**

* Create an account - Instructions for registering and setting up an account
* Create account password following complexity rules - Instructions for password complexity requirements.
  + At least 8 characters with at least one uppercase character, one lowercase character, one number, one special character.
* Login to an account - Instructions for logging in with the password created at registration
* Manage/Organize passwords - Instructions for adding, updating, copying, and deleting passwords after successful login.
* Contact support email ([totally.real.email@gmail.com](mailto:totally.real.email@gmail.com)).

**Mockup**

1. Create Account Page
   1. Field for Email
   2. Field for Password
   3. Register button
2. Login Page
   1. Field for Email
   2. Field for Password
   3. Submit button
3. Password Vault Page
   1. List of stored passwords (or stored Website accounts with an option to reveal the password?)
   2. New Password button
   3. Delete Password button
   4. Update Password button
   5. Copy Password button
4. FAQs Page
   1. List of frequently asked questions with help documentation



**Security Measures**

* User password authentication (3 failed attempts locks them out)
* Encryption (hashed AES-256 encryption/end to end)
* HTTPS connection
* Password strength checks (at least 8 characters with at least one uppercase, one lower case, one number, and one special character).

**Help Documentation Section:**

**Getting Started Guide**

**Welcome to Password Manager**

Our password manager helps you securely store and manage all your passwords in one place. Follow the steps below to get started.

**Creating Your Account**

Registration Steps

1. Click the "Register" button on the homepage
2. Enter your email address
3. Create a strong master password (see guidelines below)
4. Confirm your master password
5. Complete the registration process

**Creating a Strong Master Password**

Password Requirements

* Minimum 8 characters long
* Must include at least one uppercase letter
* Must include at least one lowercase letter
* Must include at least one number
* Must include at least one special character
* Should not be used for any other accounts

**User Guide**

**Using Your Password Manager**

Adding a New Password

1. Click the "Add New Password" button in the dashboard
2. Enter the website name
3. Enter your username for that website
4. Enter your password
5. Click Save to store the entry

Editing a Password

1. Click the "Edit" button next to the password entry
2. Modify the desired fields
3. Enter your master password to confirm changes
4. Click Save to update the entry

Deleting a Password

1. Click the "Delete" button next to the password entry
2. Enter your master password to confirm deletion
3. Click Delete to remove the entry

**AI Usage Documentation**

I asked the chatbot to provide the PHP code for linking the frontend and backend/database of a password manager web application as well as advising on where in the code stack the security measures and validations should be located (frontend or backend). The AI provided the initial PHP code along with the related HTML/CSS for the structure and style of our web application as described, as well as indicated the security measures should be integrated into the PHP configuration which allows the front and back end to communicate. Next I went through several iterations of testing the application where I had to specify specific changes to be made based upon the original design of our app and resolutions for errors as I encountered them.