## Project Title

Password Manager and Two-Factor Authentication Script

### Overview :

The Password Manager and Two-Factor Authentication Script is a secure and user friendly solution designed to help users manage their passwords and enhance the security of their accounts .This project combines HTML, CSS, Bootstrap, and Python Flask to create a comprehensive password management system.

The Two-Factor Authentication Script adds an extra layer of security to user logins .It generates time-based one-time passwords (TOTPs) and supports additional 2FA methods like email verification codes. By implementing this script, users can authenticate themselves through a combination of their passwords and a temporary code, significantly reducing the risk of unauthorized access to their accounts.

The project aims to provide users with a convenient and reliable solution for password management while reinforcing the security of their accounts. By utilizing modern web technologies and industry-standard encryption practices, this system aims to enhance user experience and promote better cyber security practices.

Please note that the following sections will provide more in-depth information about the project , including its architecture, implementation details, and usage guide.

### Technologies Used :

The technologies i have used to develop the password manager and two-factor authentication script

are :

* HTML
* CSS
* Bootstrap
* Python (flask,smtp,threading,sqlite3,random,pandas)

# Password Manager

### Introduction :

The Password Manager is a crucial component of this project, providing users with a secure and convenient solution for managing their passwords. With the increasing number of online accounts and the need for strong and unique passwords, it can be challenging to remember them all. The purpose of the Password Manager is to alleviate this burden by offering features that simplify password management and enhance security.

The Password Manager allows users to generate strong and random passwords that are resistant to common cracking techniques .These passwords are securely stored in our database , ensuring that sensitive information remains protected. When users need to access their passwords, the Password Manager provides a retrieval mechanism that allows easy access to the stored credentials.

Overall, the Password Manager aims to simplify password management and bolster account security by providing a robust set of features. By generating strong passwords, securely storing them, offering password retrieval ,this component empowers users to take control of their password hygiene and protect their sensitive information.

### Architecture :

The Password Manager follows a client-server architecture, with the frontend components (HTML, CSS, Bootstrap) responsible for the user interface and the backend implemented using Python Flask, handling the business logic and data storage.The overall architecture consists of several key components and their interactions.

## 1. Client-Side:

The client-side components include the HTML templates, CSS style sheets , and Bootstrap framework. These components create an intuitive and visually appealing user interface, providing users with a seamless experience while interacting with the Password Manager. The home page serves as the entry point, presenting users with a login form. If users don't have an account, they can sign up using the provided option.

## 2. Server-Side :

The server-side of the Password Manager is implemented using Python Flask, a micro web framework. Flask handles the incoming requests from the client-side and processes them accordingly. It manages the application routes, handles form submissions, and communicates with the underlying database.

### 3. Database:

A database is used to store user account information, encrypted passwords, and other relevant data The database can be implemented using a suitable database management system (DBMS) SQLite. The user account information, including username and hashed password etc.., is stored securely to prevent unauthorized access.

### 4. Password Management:

The Password Manager offers three primary functionalities for users: adding new passwords, viewing saved passwords, and managing passwords. When users choose to add a new password, they are presented with a form where they can enter the relevant details. This information is then securely stored in the database, ensuring the confidentiality and integrity of the stored passwords.

# Usage Guide :

### 1. Login or Sign Up:

* Open the Password Manager application in your web browser.
* On the home page, you will see a login form. If you already have an account, enter your email and password, then click the "Login" button to access your account.
* If you don't have an account, click on the "Sign Up" option. Fill in the required details, such as your desired username and password, and click "Sign Up" to create a new account.
* After successful login or signup, you will be directed to the main dashboard of the Password Manager.

### 2. Generate and Store Passwords :

* To generate a strong and secure password, navigate to the "Add Password" option.
* Fill in the necessary details, such as the website or application name, email, and password.
* Click on the "Generate Password" button to generate a random and strong password.
* Once generated, the password will be displayed in a secure field.
* Click the "Save" or "Add" button to store the password securely in the Password Manager.

### 3.Retrieve Passwords:

* To retrieve a stored password, go to the "View Passwords" or "Saved Passwords" section.
* Here, you will see a list of all your stored passwords, along with the associated website or application names.
* Click on the password entry to reveal the password.

### 4 .Manage Passwords:

* To manage your passwords, navigate to the "Manage Passwords" or "Password Management" section.
* Here, you can view and delete your stored passwords.
* To delete a password, locate the corresponding entry and click on the delete icon or the "Delete" button. Confirm the deletion if prompted.

Remember to regularly log out of your Password Manager account and keep your login credentials secure. It is also advisable to use strong and unique passwords for both your Password Manager account and any other accounts you manage with it.

# Two-Factor Authentication

## 1. Account Creation with Two-Factor Authentication:

When a user creates a new account, they will be prompted to provide their email address along with the other required details.

After entering the email address, the system will generate a unique one-time password (OTP) and send it to the provided email address .

The user should check their email inbox, including the spam folder, for the OTP.

### 2. OTP Validation during Account Creation:

On the account creation page, the user will find an input field to enter the OTP received in their email.

They should copy the OTP from their email and paste it into the OTP input field.

Upon clicking the "Validate OTP" or "Submit" button, the system will compare the entered OTP with the generated OTP.

### 3.Successful OTP Validation:

If the entered OTP matches the generated OTP, the system will validate the OTP and proceed with creating the user's account.

The user will receive a success message indicating that their account has been created successfully.

They can then proceed to log in to their newly created account using their email and password.

### 4.Failed OTP Validation:

If the entered OTP does not match the generated OTP, the system will display an error message indicating that the OTP is incorrect.

The user will be prompted to enter the correct OTP and click the "Validate OTP" or "Submit" button again.

They can retry entering the OTP until a successful match is made.