Project: Password Strength Checker

Introduction:

The "Password Strength Checker" is a web application designed to help users create secure passwords by providing real-time feedback on password strength.

The application visually indicates the password strength and offers a convenient toggle to show or hide the entered password.

This tool aims to enhance password security and usability, making it easier for users to protect their personal and sensitive information.

Objective:

The objective of this project is to develop a user-friendly web application that evaluates and displays the strength of user-generated passwords in real-time. The application aims to:

1. **Educate users** on creating strong, secure passwords by providing immediate visual feedback.

2. **Enhance usability** by offering a feature to toggle the visibility of the entered password.
3. **Promote better security practices** by encouraging the adoption of robust passwords through an intuitive and engaging interface.

Methodology:

Design and Planning:

• Requirement Analysis: Determine the criteria for password strength (e.g., length, character variety, inclusion of special characters).
• User Interface Design: Create a simple and intuitive design for users to input their passwords and receive feedback.

Implementation:

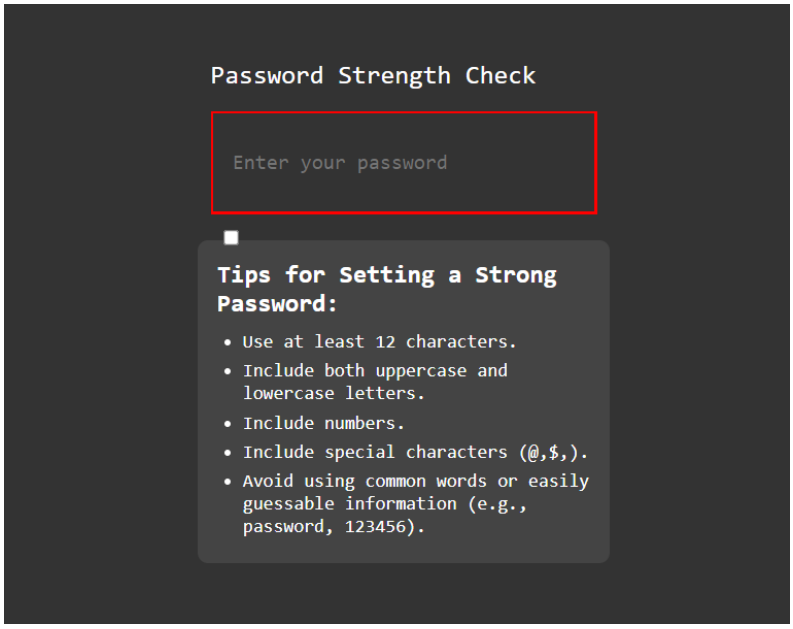
• **HTML** Structure: Develop the basic structure of the application using HTML, including the input field for the password and the area for feedback messages.

• **CSS** Styling: Style the application using CSS to ensure it is visually appealing and easy to use. This includes designing the password strength meter and the feedback messages.

• **JavaScript** Functionality: Implement the core functionality using JavaScript:
Password Strength Calculation: Write a function to evaluate the strength of the password based on predefined criteria.
Real-Time Feedback: Add an event listener to the password input field to provide instant feedback as the user types.
Visibility Toggle: Implement a feature to toggle the visibility of the password (show/hide).

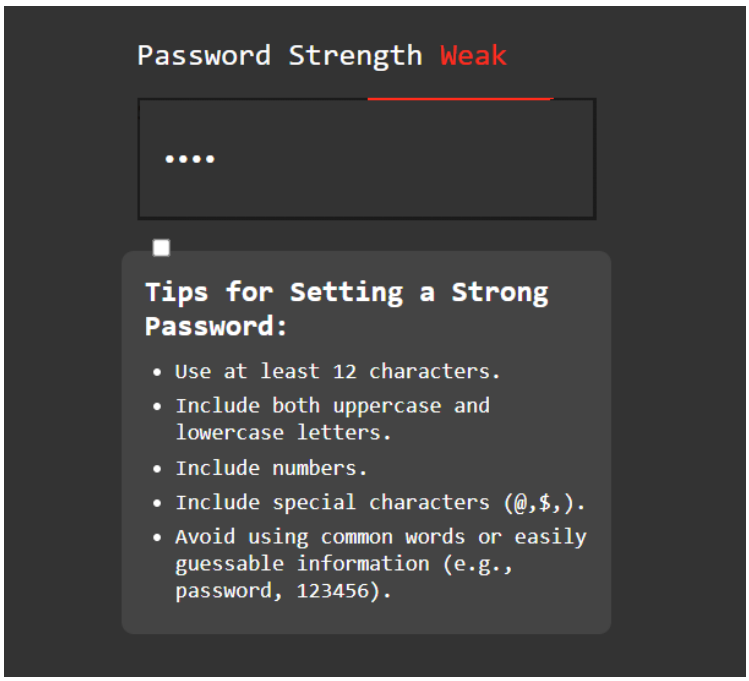
Home Screen:

This is the home screen of the application. It features an input box where you can enter your password and receive real-time feedback on its strength.



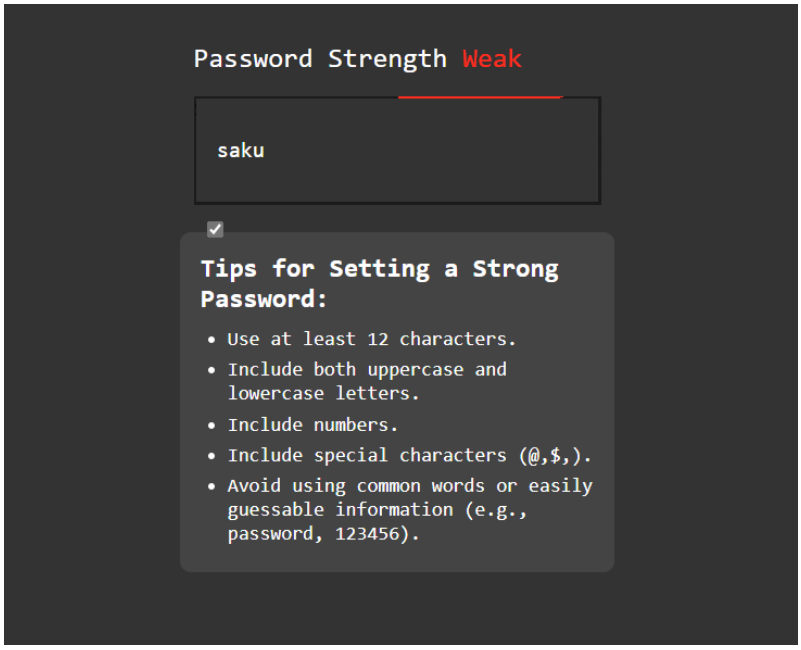
Password is Entered:

This screen shows the application after a password has been entered by the user. By default, the password is hidden for security purposes.



Entered Password is Weak:

This screen displays the application with a password entered by the user. The feedback indicates that the password is weak, helping the user understand that it needs to be strengthened.



Entered Password is Medium:

This screen displays the application with a password entered by the user. The feedback indicates that the password is of medium strength, guiding the user to improve it further for better security.

When Entered Password is Strong:

This screen displays the application with a password entered by the user. The feedback indicates that the password is strong, confirming that it meets the recommended security standards.

Swot Analysis:

Strength:

1. User-Friendly Interface: The application provides an intuitive and simple interface that is easy to use for users of all technical levels.
2. Real-Time Feedback: Users receive immediate feedback on their password strength, allowing them to adjust their passwords on the fly.
3. Enhanced Security Awareness: By visualizing password strength, the application educates users about the importance of strong passwords.

Weaknesses:

1. Limited Criteria: The strength evaluation may not consider all advanced security factors (e.g., common password patterns, dictionary attacks).
2. Visibility Toggle: While useful, the show/hide password feature could pose a security risk if used in an unsecured environment.
3. Static Rules: The criteria for password strength are fixed and may not adapt to evolving security threats or specific organizational policies.

Opportunities:

1. Enhanced Security Features: Integrate additional checks, such as common password blacklist and advanced pattern recognition, to provide more comprehensive feedback.
2. Customization: Allow users or organizations to set their own password strength criteria based on specific needs and policies.
3. Mobile App: Develop a mobile application version for offline use and broader accessibility.

Threats:

1. User Negligence: Users might ignore the feedback and continue using weak passwords, undermining the tool's purpose.
2. Competition: Other similar tools and built-in password managers in browsers and operating systems might reduce its usage.

Conclusion:

The Password Strength Checker project aims to enhance user security by providing an easy-to-use tool that offers real-time feedback on password strength.
By focusing on user education and convenience, the application helps promote better security practices.
Overall, this project serves as a valuable tool in the ongoing effort to improve password security and user awareness.