Documentation: Password Strength Checker Group 7

---

1. Project Overview

The **Password Strength Checker** is a web-based tool that helps users assess the strength of their passwords. It evaluates the password based on several criteria such as length, use of uppercase and lowercase letters, numbers, and special characters. The strength of the password is visually indicated through a progress bar and a strength message (Weak, Moderate, or Strong).

This project uses **HTML**, **CSS**, and **JavaScript** to provide an interactive, user-friendly interface.

---

2. Features

- **Password Strength Evaluation**: The password is evaluated against a set of predefined strength criteria.
- **Visual Feedback**: A progress bar and a dynamic strength message show the current strength of the password.
- **Character Requirements**: The app visually indicates which password requirements are met (e.g., length, uppercase letter, number).
- **Responsive Design**: The layout adjusts to different screen sizes for a better user experience on mobile and desktop devices.
- **Colorful Interface**: The interface uses colors (red, orange, green) to indicate the strength of the password.

---

3. Technology Stack

- **HTML**: Used to structure the content of the page.
- **CSS**: Used to style the page, providing a modern and visually appealing design.
- **JavaScript**: Used to implement the password evaluation logic, update the progress bar, and provide dynamic feedback to the user.

---

4. Project Workflow

1. **User Input**: The user enters a password into the password field.
2. **Password Evaluation**: As the user types, JavaScript functions continuously evaluate the password against predefined strength criteria (length, uppercase, lowercase, number, special character).
3. **Progress Bar Update**: The strength of the password is displayed via a progress bar that fills up as more criteria are met.
4. **Strength Message**: A strength message is displayed under the progress bar, indicating if the password is "Weak," "Moderate," or "Strong."
5. **Visual Feedback**: Character requirements (e.g., length, uppercase, special characters) are updated dynamically to show which criteria have been met, with each item turning green when satisfied and red when unmet.

---

5. Strength Criteria

- **Minimum Length**: The password must be at least 8 characters long.
- **Uppercase Letters**: The password must contain at least one uppercase letter (A-Z).
- **Lowercase Letters**: The password must contain at least one lowercase letter (a-z).
- **Numbers**: The password must contain at least one numeric character (0-9).
- **Special Characters**: The password must contain at least one special character (e.g., `!@#$%^&*()`).

---

6. How to Run the Project

1. **Download**: Download the project files (`index.html`, `styles.css`, `script.js`) and place them in the same directory.
2. **Open in Browser**: Open the `index.html` file in any modern web browser (Chrome, Firefox, etc.).
3. **Interact with the App**: Enter a password in the input field to see the strength evaluation.

---

7. Code Explanation

HTML (`index.html`)

- Contains the structure of the page, including a heading, password input field, requirements list, progress bar, and message display area.

- Uses the `<input>` element for the password field and the `<div>` element for the progress bar.

CSS (`styles.css`)

- Provides styling for a modern and responsive interface, including the background, layout, input fields, and color scheme.
- Ensures that the progress bar reflects the password strength by changing its width and color.

JavaScript (`script.js`)

- Contains the logic for evaluating the password against various criteria.
- Updates the progress bar and strength message dynamically based on the password's strength.
- Highlights the requirements (e.g., length, uppercase) in green or red as each criterion is met or unmet.

---

8. Why Password Strength Checkers are Important

Purpose of Password Strength Checker

A password strength checker is essential for ensuring that users create strong passwords that are less likely to be cracked by attackers. Passwords are the primary security mechanism for user accounts, and weak passwords can leave users vulnerable to various attacks, such as brute-force attacks, dictionary attacks, and social engineering.

Why Strong Passwords Matter

- **Protection Against Brute Force Attacks**: Strong passwords make it more difficult for automated scripts to guess the correct password through brute-force attempts, where an attacker tries all possible combinations.
- **Protection Against Phishing and Social Engineering**: Passwords with a variety of characters (letters, numbers, and special characters) are harder to guess and can help protect users from attacks based on guessing or cracking password hints.
- **Account Security**: Strong passwords are a key defense in securing sensitive information, personal accounts, and financial data from unauthorized access.

Where Password Strength Checkers are Used

- **Web Applications**: Most websites and online platforms use password strength checkers to ensure users set secure passwords when creating accounts or changing passwords.
- **Mobile Applications**: Mobile apps often incorporate password strength checkers to guide users in choosing strong, secure passwords.
- **Enterprise Systems**: Many companies use password strength checkers in their internal systems to protect sensitive corporate data and user accounts.
- **Online Banking and E-commerce Sites**: Websites that handle sensitive financial information, such as banking and e-commerce platforms, require strong passwords to prevent unauthorized access.
- **Password Managers**: Password manager tools help users generate strong passwords by using strength checkers, ensuring that passwords are complex and hard to guess.

---

9. Conclusion

The Password Strength Checker project demonstrates how essential it is to ensure password security through clear guidelines and real-time feedback. By using a simple web-based tool, users can easily evaluate and strengthen their passwords to protect their online accounts and personal data. By incorporating password strength evaluation, this tool offers an easy and effective way for users to ensure that their passwords meet security standards.

This project also illustrates the importance of clear UI/UX design to provide immediate, actionable feedback to users, encouraging them to create stronger passwords and reducing security risks in the digital world.