DevFest Challenge - Password strength (Easy)

Introduction

Passwords are the first line of defense against unauthorized access to our valuable information. A great way to help our users choose a strong password is to provide a visual indicator of its strength.

Problem Statement

Aiming to sensitize the users of a banking app of how crucial choosing a good password is to protect their financial details, it has been decided to add a new feature to help users see how strong is their password as well as a visual indicator of it.

This challenge's goal is to implement a password strength calculator that calculates how much time it would take to crack a password, with a colored indicator and display it to the user.

Requirements

1. The solution must be implemented only using HTML, CSS & JS.
2. The use of external libraries is strictly prohibited.

Expectations

- We expect a working solution that respects the requirements and is implemented in a user friendly way that is visually appealing.

Evaluation

This challenge has maximum points of 5 for implementing a working solution.

Notes

- You can assume the average number of attempts per second is**2 Billion attempt per second**.
- To calculate the time, you need to know which type of characters the user introduced, the length of the password, and finally the number of possible combinations :

> For a password of length 8, using only lower case letters, the number of possible combinations is $$26^8 combinations$$ Assuming the number of attemps per second is 2 Billion : $$T= \frac{26^8}{2000000000}

> seconds.$$

- You can consider that there are 3 levels of strength :
    - Weak : **timeToCrack ≤ 3 weeks**.
    - Medium : **3 weeks < timeToCrack ≤ 400 years**.
    - Strong : **timeToCrack > 400years**
- This challenge should a little over one hour to complete.