**Password strength Tester**

**Creating a comprehensive password strength tester involves multiple components, including evaluating the password's complexity, length, character diversity, and entropy. We also need to check against common passwords and dictionary-based attacks. Here’s a step-by-step plan to develop this tool:**

 **Password Complexity Evaluation**:

* **Length**: Assess the length of the password.
* **Character Diversity**: Check the presence of lowercase letters, uppercase letters, digits, and special characters.
* **Entropy Calculation**: Estimate the entropy to measure unpredictability.

 **Common Passwords Check**:

* Compare the password against a list of commonly used passwords.

 **Dictionary Attack Check**:

* Compare the password against a list of dictionary words.

 **Feedback and Suggestions**:

* Provide feedback on the weaknesses found.
* Suggest improvements to enhance the password's strength.

**Steps for Using the Code:**

1. **Prepare Common Passwords and Dictionary Files**:
   * Create common\_passwords.txt and dictionary\_words.txt containing common passwords and dictionary words, respectively.
2. **Run the Script**:
   * Run the script with the desired password to test its strength.

**Explanation of Feedback:**

* **Length**: Ensure the password is at least 8 characters long.
* **Character Diversity**: Use a mix of lowercase letters, uppercase letters, digits, and special characters.
* **Entropy**: Aim for higher entropy by increasing length and character variety.
* **Common Passwords**: Avoid using passwords that are commonly used.
* **Dictionary Words**: Avoid using dictionary words as passwords.