README.md

Project Title:

Password Generator & Strength Evaluator

Overview

The Password Generator & Strength Evaluator is a Python-based command-line tool designed to help users create secure passwords and assess the strength of existing passwords. The program ensures adherence to basic security standards by checking for length, character diversity, and structural strength.

Features

1. Password Generation

- Generates a random password of user-defined length
- Uses uppercase letters, lowercase letters, digits, and punctuation symbols

2. Password Strength Evaluation

- Evaluates password strength based on:
    - Minimum length requirement
    - Presence of lowercase letters
    - Presence of uppercase letters
    - Presence of digits
    - Presence of special characters

- Provides clear feedback for improvement

3. Interactive Menu System

- Simple command-line interface
- Options to generate passwords, evaluate strength, or exit

Technologies / Tools Used

- Python 3.x
- Built-in Python libraries:
    - random for password generation
    - string for character sets

Steps to Install & Run the Project

1. Clone the Repository

```
git clone <your-repo-link>
cd <your-repo-folder>
```

2. Run the Program

```
python password_generator.py
```

(Replace the filename with your actual script name if different.)

Instructions for Testing

Test Case 1: Password Generation

1. Run the script
2. Select option 1
3. Enter a valid length (e.g., 10)
4. Confirm that:
    - A random password is generated
    - Strength evaluation is displayed

Test Case 2: Password Strength Evaluation

1. Run the script
2. Select option 2
3. Enter different test passwords:
    - abc → Weak
    - Abc123 → Moderate
    - A1b2C3!@# → Strong

Test Case 3: Input Validation

- Enter non-numeric values for length
- Enter values less than 4
- Enter an invalid menu choice
  The program should display an error message and re-prompt the user.