Password Strength Analyzer - Documentation

Password Strength Analyzer

A simple yet powerful Python script that analyzes the strength of user passwords using entropy, estimates crack time, detects weaknesses, and suggests a stronger alternative.

Features

- Entropy Calculation - Estimates the unpredictability of the password
- Crack Time Estimation - Approximates how long it would take to brute-force the password at 1 billion guesses/second
- Weakness Detection - Flags issues like common patterns, short length, and poor character variety
- Strong Password Generator - Recommends a highly secure 16-character password
- Batch Password Analysis - Analyzes a list of passwords in one go

Files

- password_analyzer.py - Main script
- README.md - This documentation
- LICENSE - MIT License (optional)

How to Use

1. Requirements
   - Python 3.6 or higher

2. Running the Script (Windows/Mac/Linux)
   Option 1: Run Locally
      python password_analyzer.py
   Option 2: Run Online
      - Replit: https://replit.com/
      - Google Colab: https://colab.research.google.com/

3. Example Output

Password: password123
  Entropy: 59.0 bits

Estimated Crack Time: 6 years

Weaknesses: Common password, Lacks character variety, Low entropy

Stronger Suggestion: Y@6pK#vWz93!qLmX

Customize for Your Input

To analyze your own passwords:

```
passwords = ["YourPasswordHere", "AnotherOne!"]
```

Or make it interactive:

```
passwords = [input("Enter a password to analyze: ")]
```

Weakness Checks Include:

- Too short (<12 characters)
- Common passwords (e.g., password, 123456)
- Only digits or only letters
- Entropy < 60 bits

Sample Strong Passwords Generated:

- gY9$TmZ#1p!vqXWa
- R7#wN2@bVx4!mzPd