Password Strength Tester

Aymen MSADDAK
Moona SAADAOUI
Husin KHLIF
Aya ARFAOUI

April 27, 2025

1 Introduction

Authentication (AuthN) is the process of verifying that an individual, entity, or website is who or what it claims to be by determining the validity of one or more authenticators (such as passwords, fingerprints, or security tokens) that are used to support this claim. One of the most common and essential means of authentication is passwords.

2 Main Concepts

A key concern when using passwords for authentication is the strength of the password. A "strong" password policy makes it difficult or even improbable for one to guess the password through either manual or automated means. Following the OWASP guidelines for password security, here are some of the password strength characteristics:

- Password length:
  - passwords shorter than 8 characters are considered to be weak
  - passwords should have at least 16 characters
- Letters case: a mixture of both upper and lower cases
- A mixture of diverse letters and numbers
- Inclusion of at least one special character: ! @ ?]
- Do not use:
  - names (family, pets, middle names, etc.)
  - dates (birthdays, anniversaries, etc.)
  - personal information
  - dictionary words
  - a series of characters
  - a keyboard series of characters (qwerty, poiuy, etc.)

3 Passphrases Vs Passwords

- Passphrases: is a longer sequence of random words or a meaningful sentence, making it easier to remember but harder to crack.
- Passwords: is a short, typically complex string of characters (letters, numbers, and symbols) used to authenticate a user.

4 Common Attacks

- Brute-force Attacks: The attacker tries every possible combination of characters until the correct one is found. This attack is effective against simple and short passwords.
- Dictionary Attacks: the attacker uses a precompiled list of commonly used passwords such as 'password123' or 'azerty', etc. This attack is effective against passwords that consist of predictable words or phrases.

- Rainbow Table Attacks: Precomputed tables of hashed passwords are used to reverse-engineer the password from a hash. Effective against systems that store password in unsalted hashes.

5 Functional Flow

Step by step process of how a password strength tester operates:

- The user enters a password.
- The system checks the regex and pattern.
- The system applies complexity rules.
- The entropy score is calculated.
- Feedback is generated:
  - password strength result: color bar
  - provide tips for a strong password
  - suggest a strong password

6 Theoretical Aspects

6.1 Algorithms

- String Pattern Matching: using Regex pattern matching, for example, to detect common dictionary words.
- Password Complexity Evaluation: assign a score variable to measure the complexity of the password, based on the OWASP standards and rules.
- Rules enforcing algorithm: define the minimum criteria for the password to be considered secure and usable, example: set minimum length, number of digits to include, etc.
- Entropy calculation: To estimate password strength, we may use Shannon entropy, or OWASP-style estimation based on character variety and length.

6.2 Protocols

- OWASP Authentication Guidelines.
- TLS.
- PBKDF2 / bcrypt / Argon2.
- Content Security Policy (CSP).

7 Advantages and Limitations of Password Strength Tester

7.1 Advantage

- Fully OWASP-compliant.
- Encourage passphrases, not just complexity.
- Provide educational and actionable feedback.
- Highlight weak points in real time.

7.2 Limitations

- Do not guarantee protection against reused passwords unless connected to a breach database.
- Cannot detect cleverly hidden personal info (e.g., reverse names).
- Limited to front-end checks (not actual password storage).