Password Strength Tester

IT360 Information Assurance and Security

by

Khalil Elachkham - Mohamed Haroun Cheriha - Mahdi Laafif

April 2023

IT/FIN Junior Students

Tunis Business School

Ben Arous,TUNISIA.

2022-2023

Contents

Chapter 1

Introduction

The security of user passwords is a critical component of any modern web application or online service. Weak or easily guessable passwords can lead to unauthorized access, data breaches, and other security risks. Therefore, it's essential to implement password strength testing to ensure that users are creating strong and secure passwords.

The OWASP (Open Web Application Security Project) is a widely recognized authority in the field of web application security. They provide guidelines for best practices in password strength testing, including minimum password length, complexity requirements, and the avoidance of common password patterns.

In this project, we will be developing a password strength tester that adheres to the OWASP guidelines. Our system will enforce basic password rules while providing user flexibility and encouraging the use of passphrases over standard passwords. By implementing this project, we aim to enhance the security of user passwords and help prevent unauthorized access and data breaches.

In the following sections, we will provide a clear explanation of the main components and functional flow of our password strength tester, as well as discuss implementation details, user testing, limitations and future work, ethical considerations, and references.

Chapter 2

Main Concepts

2.1 Main Concepts

- 1. Password strength testing algorithms: These are mathematical calculations that evaluate the strength of a password. These algorithms are designed to determine how difficult it would be for an attacker to guess or crack a password. OWASP recommends using a combination of techniques, such as entropy calculations, dictionary checks, and rule-based evaluations, to test password strength.

- 2. OWASP guidelines: The Open Web Application Security Project (OWASP) provides guidelines for secure password policies and testing. OWASP provides a comprehensive checklist for testing password strength, which includes many different types of tests, such as testing for common passwords, testing for character repetition, and testing for sequential characters. OWASP guidelines also emphasize the importance of educating users on the importance of strong passwords and password security best practices.

- 3. Password policies: Password policies are the set of rules and requirements that define what constitutes a strong password. OWASP recommends enforcing policies such as minimum password length, required use of special characters, and prohibiting the use of common dictionary words, personal information, or sequential characters. Password policies should be designed to minimize the likelihood of password guessing, cracking, and other types of attacks.

- 4. Passphrases: Passphrases are longer strings of words or sentences that can be used as an alternative to traditional passwords. Passphrases are generally considered more secure

than passwords because they are longer and more difficult to guess or crack. OWASP recommends encouraging the use of passphrases in place of traditional passwords to improve password security.

- 5. User interfaces: User interfaces are the graphical or command-line interfaces through which users interact with the password strength tester. OWASP recommends that user interfaces should be designed to be user-friendly and provide clear feedback to the user. The feedback should indicate the strength of the password, which policies the password meets, and which policies the password does not meet.

2.2 Functional Flow

- 1. User enters password: The user inputs their password into the password strength tester.
- 2. Password is analyzed: The tester uses password policies and strength testing algorithms to analyze the password and determine its strength.
- 3. Results are displayed: The tester displays the results of the analysis to the user, typically in the form of a visual indicator (such as a color-coded bar or a thumbs-up/thumbs-down icon) and a numerical score or rating.
- 4. User is given feedback: The tester provides feedback to the user on how they can improve the strength of their password, such as by using a longer password or including more special characters.