Password Strength Checker Report

# 1. Introduction

This report provides an overview of the Password Strength Checker, explaining how the tool works, its components, and the logic behind assessing password strength.The checker analyzes a password based on factors like length, complexity, and entropy.

# 2. How the Password Strength Checker Works

## 2.1 Password Complexity

The tool checks for four key elements of complexity: uppercase letters, lowercase letters, numbers, and special characters. A strong password contains a mix of all these elements.

## 2.2 Common Password Check

The checker compares the entered password against a list of common, weak passwords. If the password matches one from this list, it is flagged as weak and users are advised to choose a more unique password.

## 2.3 Repeated Patterns

The tool checks if the password contains any repeated characters or patterns, such as 'aaa' or '111'. Such patterns weaken the password, making it more predictable and easier for attackers to guess.

## 2.4 Entropy Calculation

Entropy is a measure of randomness. Higher entropy means that the password is more difficult to predict. The tool calculates the entropy based on the length of the password and the variety of character sets used (e.g., uppercase, lowercase, numbers, special characters).

# 3. Score and Feedback

Based on the analysis of the password, the tool provides a score that determines the overall strength. Feedback is given to help users improve their password strength, such as increasing its length or adding more complex characters. A score of 5 represents a very strong password, while lower scores indicate areas for improvement.

# 4. Conclusion

The Password Strength Checker provides users with a way to evaluate and improve the security of their passwords. By offering real-time feedback and focusing on length, complexity, and entropy, users are encouraged to create stronger, more secure passwords.