PASSWORD STRENGTH CHECKER

1.Importance of Strong Passwords in Cybersecurity

Strong passwords are the cornerstone of cybersecurity, acting as a primary defense against unauthorized access to sensitive information. Weak passwords can pose significant risks, making systems vulnerable to various cyber threats such as brute force attacks, dictionary attacks, and password guessing. These attacks exploit passwords that lack complexity, making them easier to crack and compromising personal data, financial information, and even critical systems.

2.Risks Associated with Weak Passwords

Weak passwords typically lack complexity—they might be short, easily guessable, or lack a combination of letters, numbers, and special characters. They are susceptible to being cracked using automated tools that rapidly try different combinations, eventually breaching the system's security. This can lead to unauthorized access, data breaches, identity theft, and financial losses for individuals or organizations.

3.Objectives of the Project

The project aims to create a tool that assesses password strength in real-time. By evaluating various parameters such as length, combination of characters, and complexity, it provides immediate feedback on the strength of entered passwords. Through visual indicators and textual feedback, users can understand the strength of their passwords and receive recommendations for improving them.

4.Technical Implementation

The code integrates a password strength checker. It dynamically evaluates the entered password and categorizes it into weak, medium, or strong based on length and character complexity. It uses regular expressions to match lowercase letters, digits, and special characters to determine the strength level. The script updates visual indicators and text feedback to inform users about the strength of their passwords.

This tool empowers users to create stronger passwords by visually displaying the strength level and offering suggestions to enhance their security posture.

4.1 HTML Structure:

The HTML structure comprises a form containing an input field for entering the password.

It includes visual indicators (weak, medium, strong) and a text field to display the strength assessment.

4.2 JavaScript Functionality:

Variables:

The script declares variables to target HTML elements and define regular expressions for weak, medium, and strong password criteria.

Trigger Function:

The trigger() function executes on every keystroke within the password input field.

It evaluates the entered password against predefined criteria to determine its strength level.

Based on the password's length and character composition, it sets different classes (weak, medium, strong) and displays corresponding strength indicators and textual feedback.

Additionally, it allows users to toggle password visibility by clicking the "SHOW"/"HIDE" button.

Password Strength Assessment:

Weak Passwords:

Passwords with insufficient length or lacking certain character types (lowercase letters, digits, or special characters) are categorized as weak.

Medium Passwords:

Passwords meeting certain length and character criteria, even if not all, fall under the medium category.

Strong Passwords:

Passwords fulfilling all criteria (length, lowercase letters, digits, and special characters) are classified as strong.

5. Condition Evaluation:

>The script uses conditional statements to categorize the password strength into weak, medium, or strong based on length and character complexity.

>Weaknesses are determined by insufficient length or the absence of specific character types.

Medium strength is assigned if certain criteria are met, and strong strength is assigned only when all criteria are fulfilled.