**MINI PROJECT**

**\*Create a Password Strength Indicator for a login page of our website.**

# ABSTRACT

The project "Password Strength Indicator for a Login Page" is aimed at enhancing the security of user accounts by providing a visual indicator of the strength of passwords during the registration or login process on a website. Password security is crucial in safeguarding user data and preventing unauthorized access. The proposed solution utilizes Python to assess and display the password strength, classifying it as weak, medium, or strong based on several criteria, including length and character complexity.

# PROGRAM

import re  
  
def check\_password\_strength(password):  
 # Define criteria  
 min\_length = 8  
 min\_uppercase = 1  
 min\_lowercase = 1  
 min\_digits = 1  
 min\_special\_chars = 1  
  
 strength = 0  
  
 # Check length  
 if len(password) >= min\_length:  
 strength += 2  
 elif len(password) >= 6:  
 strength += 1  
  
 # Check uppercase letters  
 if len(re.findall(r'[A-Z]', password)) >= min\_uppercase:  
 strength += 1  
  
 # Check lowercase letters  
 if len(re.findall(r'[a-z]', password)) >= min\_lowercase:  
 strength += 1  
  
 # Check digits  
 if len(re.findall(r'\d', password)) >= min\_digits:  
 strength += 1  
  
 # Check special characters  
 if len(re.findall(r'[!@#$%^&\*]', password)) >= min\_special\_chars:  
 strength += 1  
  
 return strength  
  
  
password = input("enter your password: ")  
strength = check\_password\_strength(password)  
  
if strength >= 4:  
 print("Strong password")  
elif strength >= 2:  
 print("Medium password")  
else:  
 print("Weak password")

# EXPLANATION

The project "Password Strength Indicator for a Login Page" aims to improve the security of user accounts by providing a visual representation of the strength of passwords during the registration or login process on a website. This system evaluates the quality of a user's chosen password and classifies it into one of three categories: weak, medium, or strong, based on specific criteria.

Here's a more detailed explanation of the project:

* Password Length Assessment: The first and most basic criterion for evaluating password strength is its length. Passwords are considered strong if they are longer than 8 characters, as longer passwords tend to be more secure. Passwords that are between 6 and 8 characters are categorized as medium in strength, while those with less than 6 characters are labeled as weak. This initial assessment helps users understand the importance of a sufficient password length.
* Character Complexity: In its current form, the project primarily focuses on password length. However, future iterations of this system can be enhanced by considering additional factors that contribute to password strength. These factors may include the presence of both uppercase and lowercase letters, digits, and special characters. For example, a password with a combination of uppercase letters, lowercase letters, digits, and special characters is typically more secure and can be rated as strong.

In conclusion, this project offers a practical solution to the critical issue of password security in the context of website authentication. By visually indicating password strength, users are empowered to make informed decisions when creating or changing their passwords. Ultimately, this project contributes to improving the overall security of the website and protecting sensitive user data. It's a user-friendly and valuable addition to any website's login page, promoting both security and a positive user experience.

Top of Form