Random Password Generator

By: Harshita Vachhani (B23EE1026)

Introduction:

This project was prepared to design a program that would be able to calculate the strength of passwords based on criteria such as the presence of numbers, uppercase and lowercase letters, special characters, and length. Additionally, it offers an option to suggest a randomly generated strong password.

Implementation Process:

1) Password Generation Function: The create_password function generates random passwords by selecting characters from predefined character sets and arranging them in a random order.
2) Strength Calculation Function: The strength function evaluates the strength of user-entered passwords based on various criteria, such as length and character diversity.
3) User Interaction: The program provides a menu-driven interface for users to input their passwords, calculate their strength, and generate random passwords.

Challenges Faced:

1) Ensuring Randomness:

   One challenge was ensuring the randomness of generated passwords to enhance security.

2) User Input Validation: Validating user input to ensure it meets minimum criteria for password strength posed another challenge.
3) Optimization: Optimizing the program for efficiency and performance while maintaining simplicity and usability was a continuous effort throughout the implementation process.

Potential Improvements:

User Interface Enhancements: Improving the user interface to make it more intuitive and user-friendly would enhance the overall user experience.

Conclusion:

The Random Password Generator project offers a solution to the challenge of creating strong and secure passwords. By automating the password generation process and providing users with tools to evaluate password strength, this project contributes to enhance online security. Future enhancements and refinements can further improve the project's functionality and usability.