Task 1 – Password Strength Checker

Description

This project checks how strong a password is by analyzing its length, use of numbers, uppercase, lowercase, and special characters. It helps users create secure passwords that are difficult for hackers to guess.

Tools Used

- Python 3
- Regular Expressions (re module)
- VS Code / PyCharm (for coding)
- Terminal / Command Prompt (for running the script)

Python Code

```
import re

def check_password_strength(password):
    strength = 0
    remarks = ""

    if len(password) < 6:
        remarks = "Password is too short!"
    elif len(password) >= 6:
        if re.search("[a-z]", password):
            strength += 1
        if re.search("[A-Z]", password):
            strength += 1
        if re.search("[0-9]", password):
            strength += 1
        if re.search("[_@$#%^&*!]", password):
            strength += 1

        if strength == 1:
            remarks = "Weak password."
        elif strength == 2:
            remarks = "Moderate password."
        elif strength == 3:
            remarks = "Strong password."
        elif strength == 4:
            remarks = "Very strong password!"

    return remarks
```

```
password = input("Enter your password: ")
print(check_password_strength(password))
```

Code Explanation

- The re module checks patterns in your password.
- The program counts how many categories (uppercase, lowercase, digits, symbols) your password includes.
- It gives you feedback on your password strength.

Output Example

Enter your password: MyPass@123
Very strong password!

Uses

- Ensures data security.
- Helps users generate strong, secure passwords.
- Prevents easy guessing and brute-force attacks.

Summary

The password strength checker is an important tool for cybersecurity awareness. It improves protection by guiding users to create passwords that are difficult to crack.