Password Complexity Checker

import re

def assess\_password\_strength(password):

length\_ok = len(password) >= 8

has\_upper = bool(re.search(r'[A-Z]', password))

has\_lower = bool(re.search(r'[a-z]', password))

has\_digit = bool(re.search(r'\d', password))

has\_special = bool(re.search(r'[!@#$%^&\*(),.?":{}|<>]', password))

score = sum([length\_ok, has\_upper, has\_lower, has\_digit, has\_special])

if score == 5:

strength = "Strong"

elif score >= 3:

strength = "Moderate"

else:

strength = "Weak"

feedback = []

if not length\_ok:

feedback.append("Use at least 8 characters.")

if not has\_upper:

feedback.append("Include at least one uppercase letter.")

if not has\_lower:

feedback.append("Include at least one lowercase letter.")

if not has\_digit:

feedback.append("Include at least one number.")

if not has\_special:

feedback.append("Include at least one special character (!@#$ etc.).")

return {

"strength": strength,

"score": score,

"feedback": feedback

}

if \_\_name\_\_ == "\_\_main\_\_":

user\_input = input("Enter a password to check its strength: ")

result = assess\_password\_strength(user\_input)

print(f"\nPassword Strength: {result['strength']}")

if result['feedback']:

print("Suggestions to improve:")

for suggestion in result['feedback']:

print(f"- {suggestion}")

Output:

