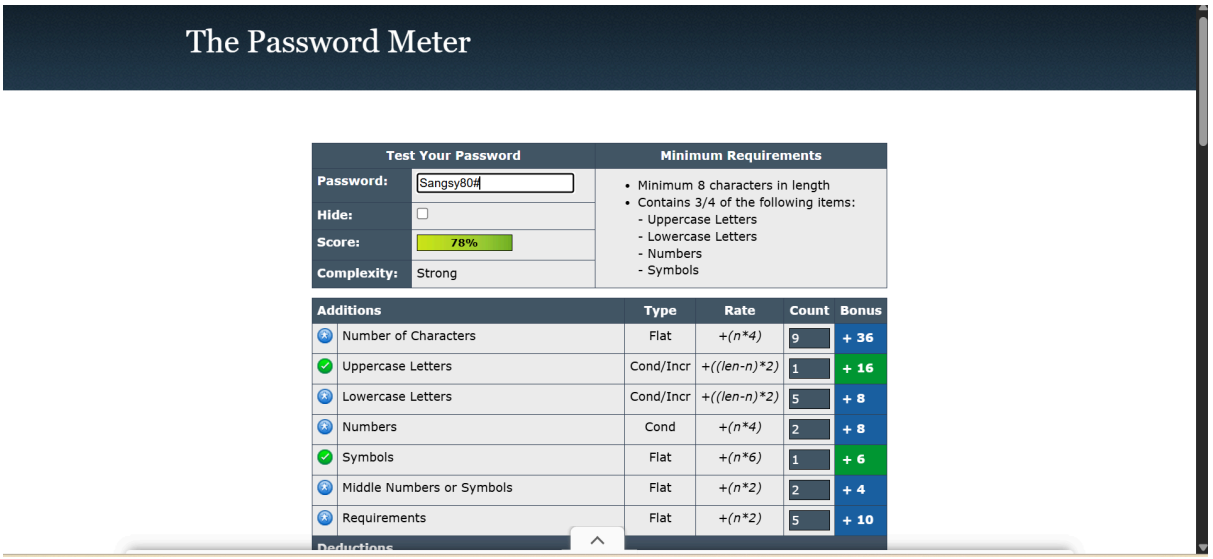
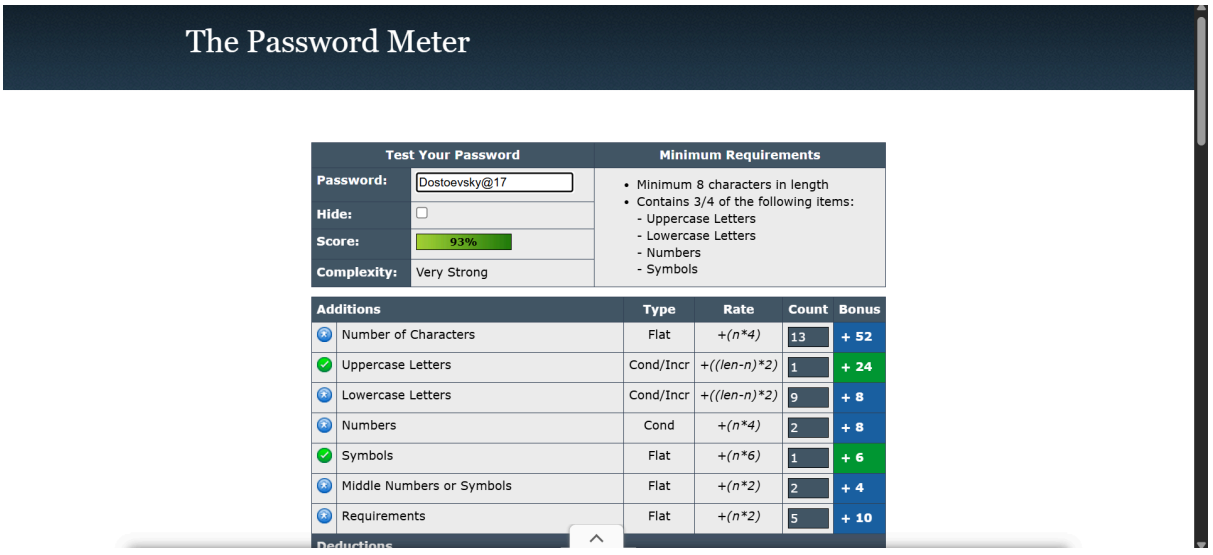
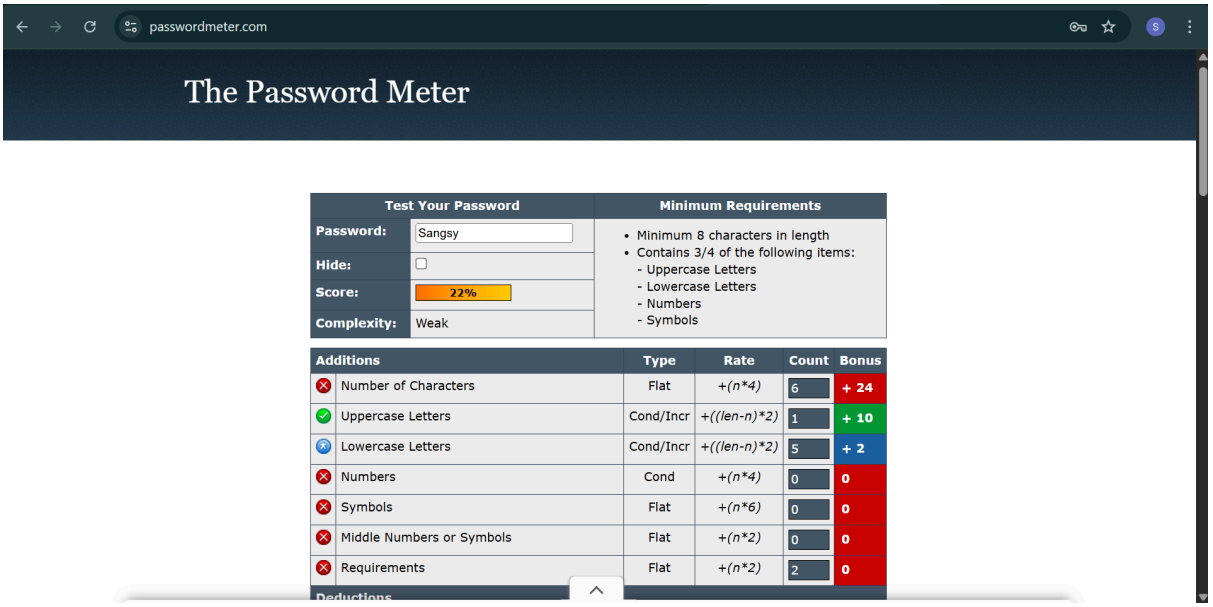
Task 6 : Create a Strong Password and Evaluate Its Strength

Objective: Understand what makes a password strong and test it against password strength tools.
Tools: Online free password strength checkers (e.g., passwordmeter.com).
Deliverables: Report showing password strength results and explanation.

To understand the importance of password security, multiple passwords with varying levels of complexity were tested using **passwordmeter.com**, an online password strength checker. The objective was to observe how password length, character variety, and structure affect overall password strength and resistance to common attacks.







Password Testing Results

1. Password: “Sangsy”

- **Length:** 6 characters
- **Score:** 22%
- **Complexity:** Weak

Observations:

- Contains uppercase and lowercase letters only.
- Does not meet the minimum length requirement (8 characters).
- Lacks numbers and symbols.
- Fails most security requirements.

Security Risk:
This password is highly vulnerable to **dictionary attacks** and **brute force attacks** due to its short length and predictable structure.

2. Password: “Sangsy80#”

- **Length:** 9 characters
- **Score:** 78%
- **Complexity:** Strong

Observations:

- Includes uppercase letters, lowercase letters, numbers, and symbols.
- Meets minimum length and character diversity requirements.
- Shows significant improvement over the weak password.

Security Impact:
This password provides better resistance against brute force attacks due to increased length and character variety, making it harder to guess or crack.

3. Password: “Dostoevsky@17”

- **Length:** 13 characters
- **Score:** 93%
- **Complexity:** Very Strong

Observations:

- Contains uppercase and lowercase letters, numbers, and symbols.
- Long length significantly increases entropy.
- Meets all recommended security requirements.

Security Impact:
This password is highly resistant to **brute force** and **dictionary attacks**. The combination of length and complexity makes it suitable for securing sensitive accounts.

Key Learnings & Best Practices

- **Password length is critical**: Longer passwords drastically increase the time required for brute force attacks.
- **Character diversity matters**: Using uppercase, lowercase, numbers, and symbols significantly improves strength.
- **Avoid simple or common words**: They are easily cracked using dictionary attacks.
- **Middle placement of numbers/symbols** improves strength compared to appending them at the end.
- **Strong passwords reduce attack success rate**, even if attackers use advanced tools.

Impact of Password Complexity on Security

Password complexity directly affects security by increasing the number of possible combinations an attacker must try. Weak passwords can be cracked in seconds, while strong and complex passwords can take years or even centuries to break using brute force techniques.

Conclusion

The evaluation clearly shows that **password strength increases with length and complexity**. Weak passwords pose serious security risks, while strong passwords significantly enhance protection against common password-based attacks. Adopting best practices in password creation is essential for maintaining secure authentication systems.