**Task 6: Create a Strong Password and Evaluate Its Strength**

**Objective**

The objective of this task is to understand the characteristics of strong passwords, evaluate them using online password strength checkers, and learn best practices for creating secure passwords.

**Tools**

* Online Password Strength Checkers:
  + passwordmeter.com
  + security.org password strength tester
  + Kaspersky Password Checker

**Methodology (Steps Followed)**

1. **Created multiple passwords** with different complexity levels.
2. Used a mix of **uppercase, lowercase, numbers, symbols, and different lengths**.
3. Tested each password using password strength checkers.
4. **Recorded scores** and feedback provided by the tools.
5. Identified **best practices** for strong password creation.
6. Wrote **tips and lessons learned**.
7. Researched common **password attacks** (brute force, dictionary, phishing).
8. Summarized how **password complexity impacts security**.

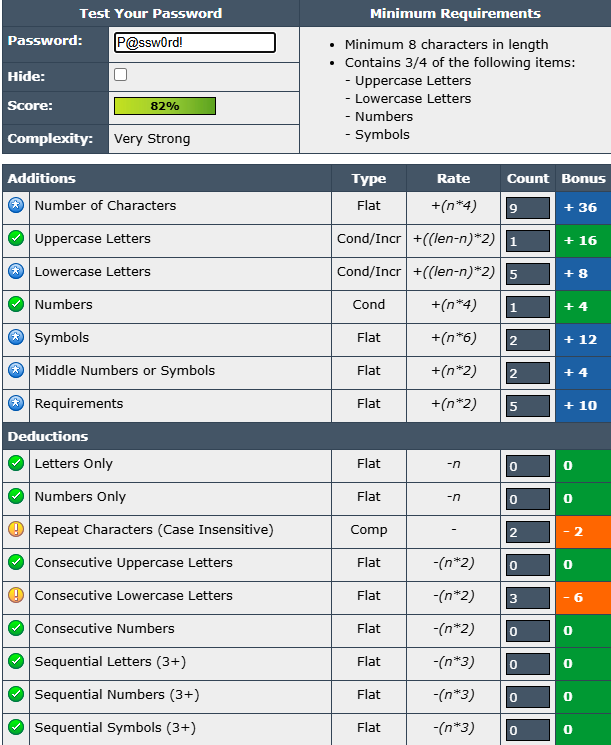
**Password-12345**



**Password-** **Password!23**

****

**Password- P@ssw0rd!**



**Password- Tr0ub4dor&3**

****

**Password- G$7vL!p#rX8zQ2kM**

****

### Best Practices for Creating Strong Passwords

* Use **at least 12–16 characters**.
* Mix **uppercase, lowercase, numbers, and symbols**.
* Avoid **dictionary words** and predictable substitutions (like "Password123").
* Use **passphrases** made of random words (e.g., “Blue!River9Horse$Sky”).
* Do **not reuse** the same password across multiple accounts.
* Enable **two-factor authentication (2FA)** where possible.

### Tips Learned from Evaluation

* Length improves strength more than complexity alone.
* Substituting letters with numbers (e.g., "P@ssw0rd") is no longer effective, as attackers account for these.
* Random combinations or unique passphrases are significantly stronger.
* Password managers help generate and store strong passwords securely.

### Research on Common Password Attacks

* **Brute Force Attack**: Tries all possible combinations until success. Long and complex passwords resist this.
* **Dictionary Attack**: Uses common words/phrases. Avoid dictionary words to prevent this.
* **Credential Stuffing**: Attackers use leaked username-password pairs. Unique passwords for every site protect against this.

### Conclusion

Password complexity directly impacts security. **Long, unique, and random passwords** are the strongest defense against brute force and dictionary attacks. Combining this with **2FA** greatly enhances protection.