Name: satya chaitanya yerninti

Email: satyachaitanya21@gmail.com

Objective: Understand what makes a password strong and test it against password strength tools.

Tools used: passwordmeter.com

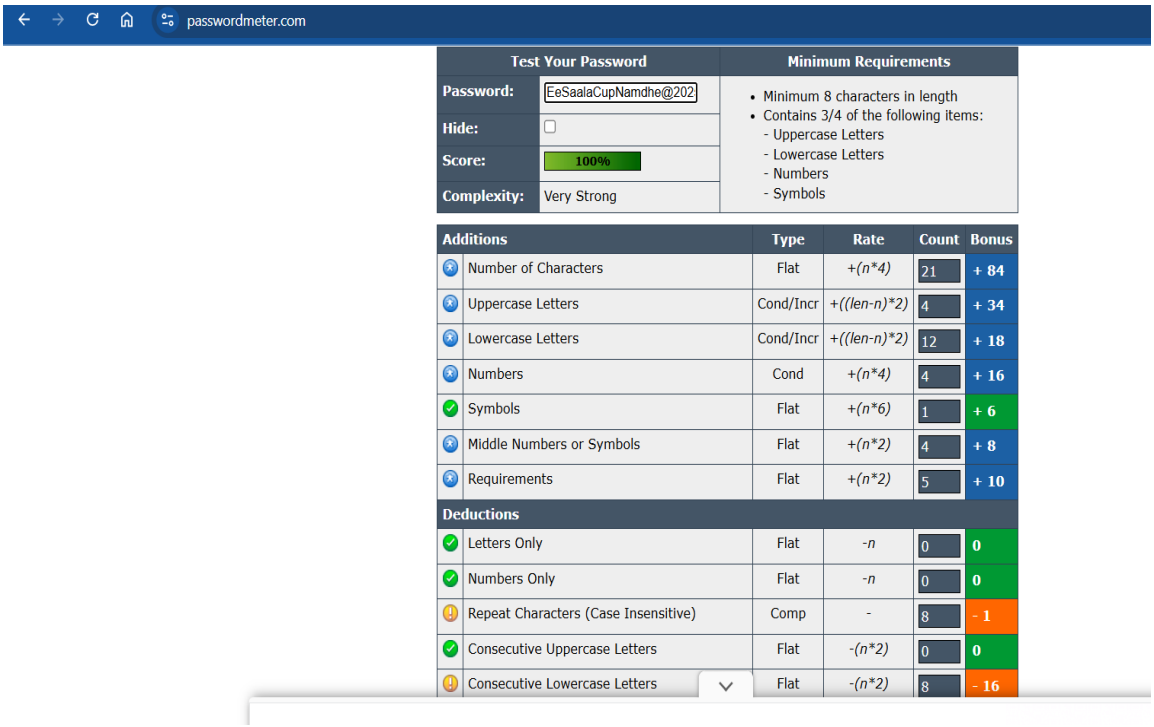
Password strengthening:

Password strengthening involves creating long, unique passwords with a mix of uppercase letters, lowercase letters, numbers, and symbols. It is also crucial to use a password manager to store unique passwords for each account and enable multi-factor authentication whenever possible. Avoid using personal information, common words, or predictable patterns that are easy for attackers to guess.

Creating a strong password

- **Make it long:** Aim for at least 12 characters, with 14 or more being even better.
- **Use a mix of character types:** Combine uppercase and lowercase letters, numbers, and special symbols (e.g., @, #, %).
- **Avoid personal information:** Don't use birthdays, names, addresses, or pet names that can be easily found online.
- **Don't use common words or patterns:** Steer clear of dictionary words, consecutive letters (like "abc"), or repeated characters (like "aaa").
- **Consider a passphrase:** A memorable phrase made of several random words is often longer and more secure than a single password (e.g., "CoffeeTableBookSunshine").

Keeping strong password



Weak password