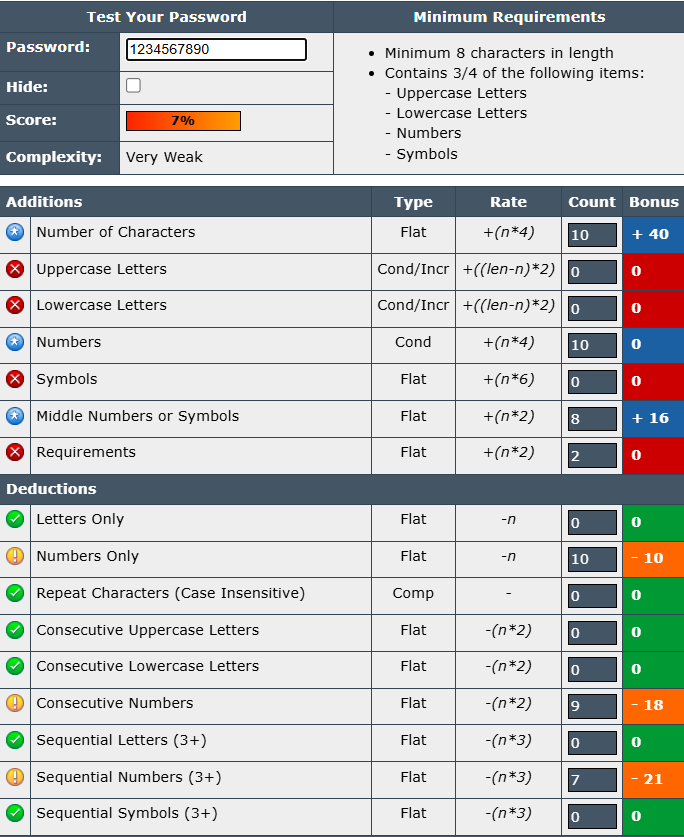
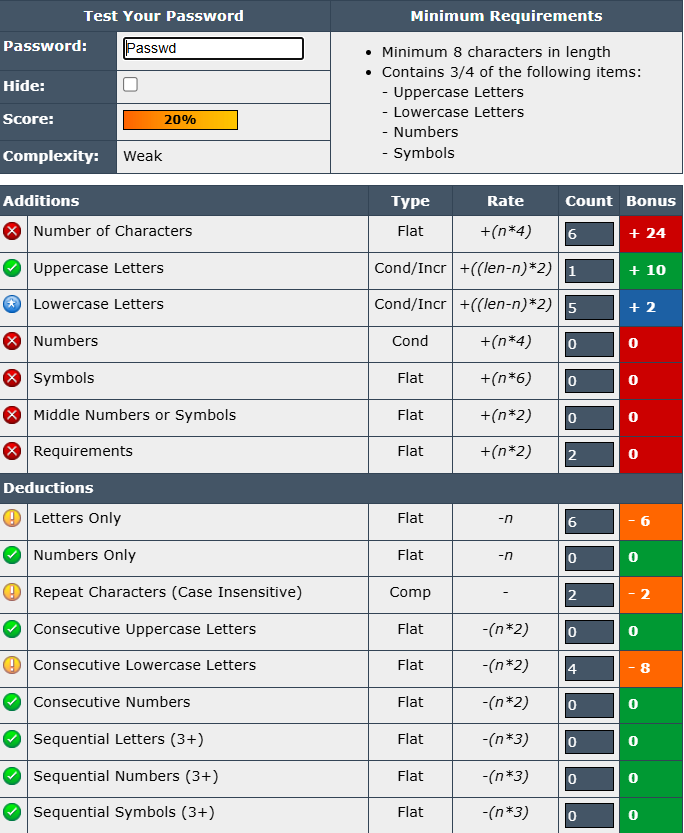
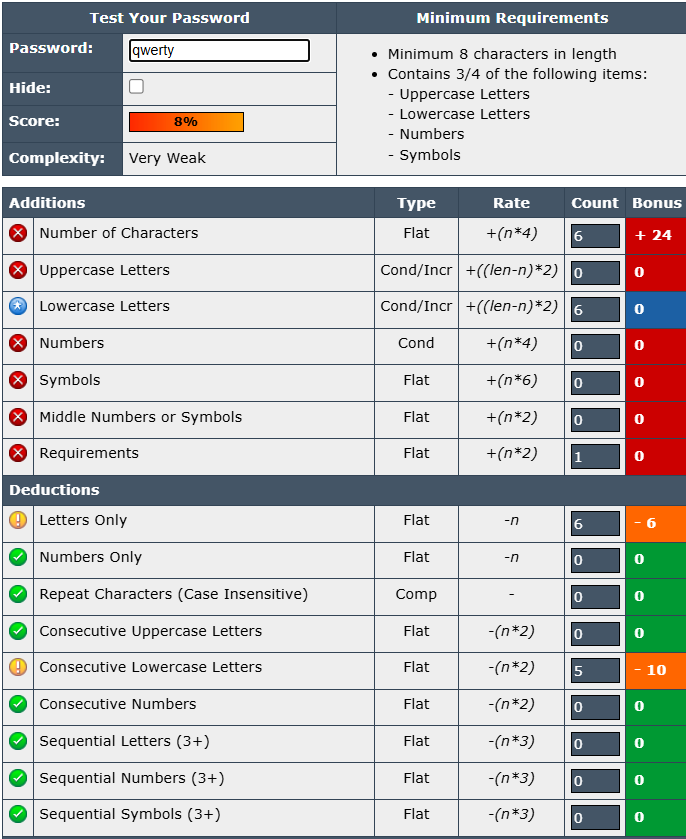
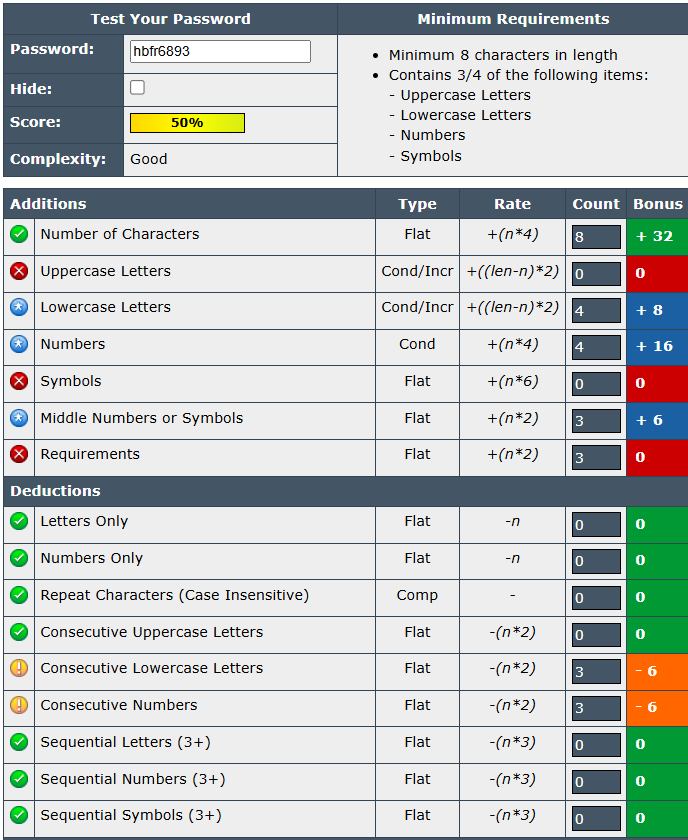
Nandida Valsaraj   
  
1.

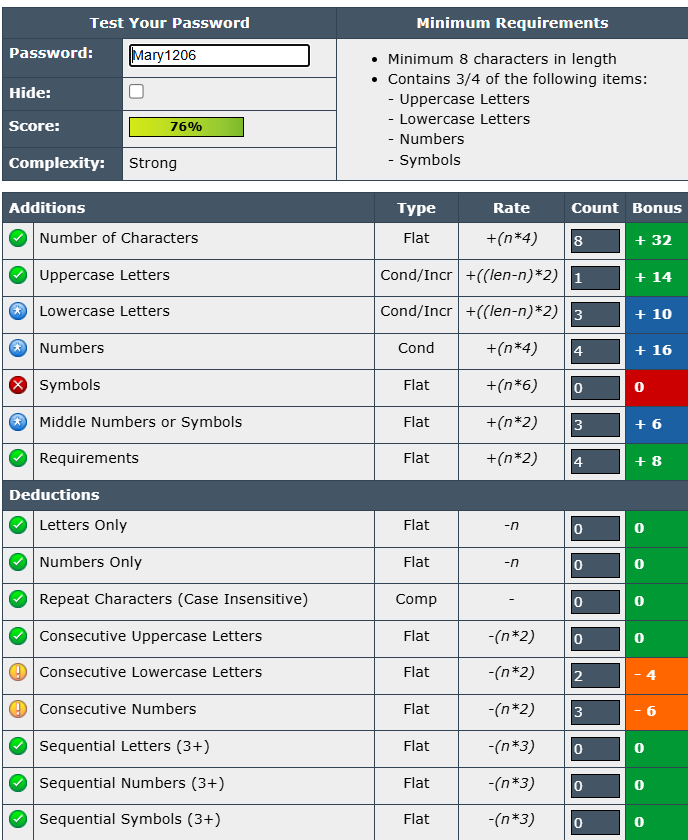
* qwerty
* 1234567890
* Passwd
* Mary1206
* hbfr6893
* Cat34@@L0ve
* S$$pn1m2002
* N12d10Mhu$&i
* We6d!cyt^fuvgibhte&tNem\*

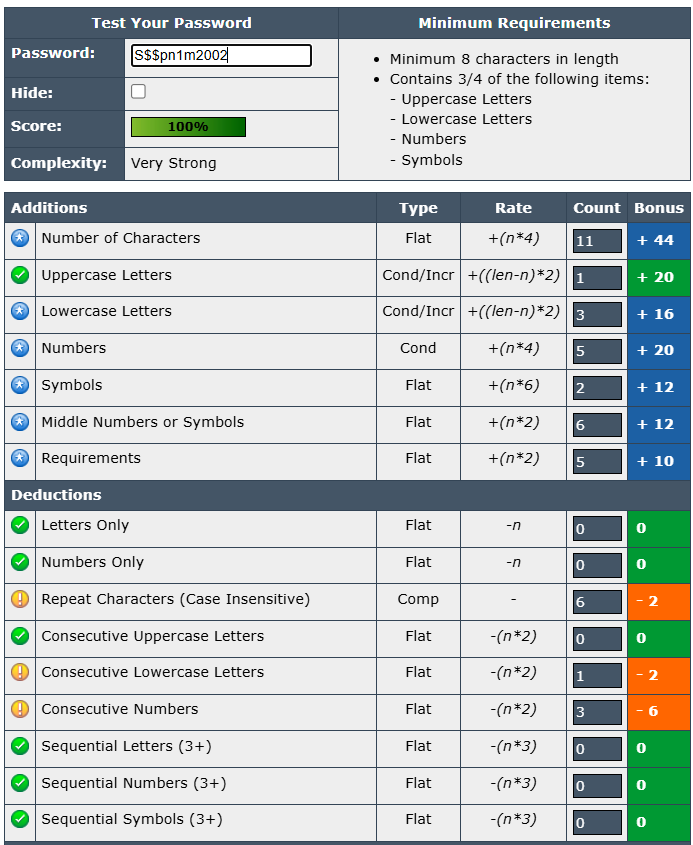
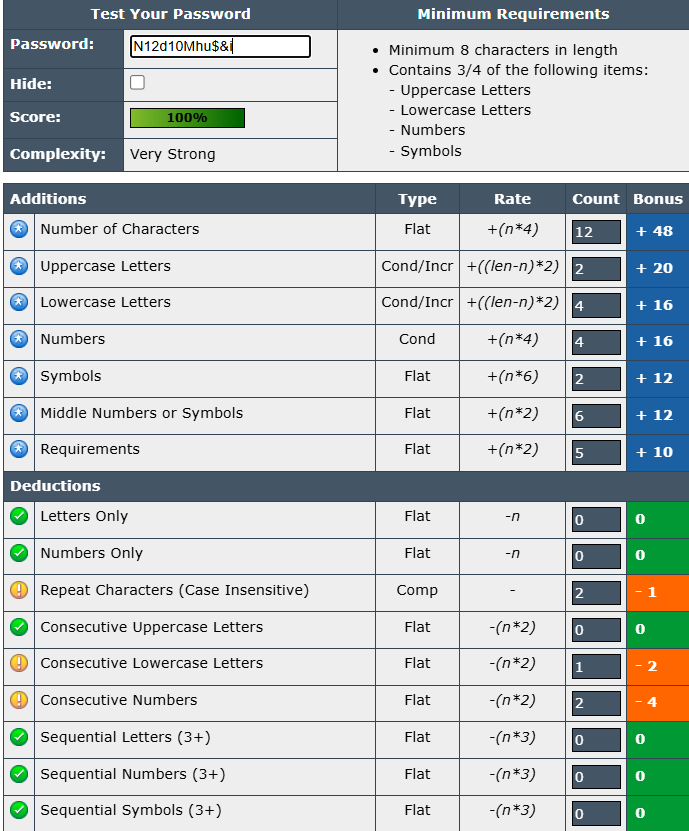
4.









5.

* To create strong passwords prioritize length(atleast 12 characters).
* Use a mix of uppercase, lowercase, numbers, and symbols.
* Don’t reuse passwords across multiple accounts or sites .
* Avoid personal information (name, birthday, address, or other personal details).
* Avoid dictionary words or phrases.
* Utilize password managers.
* Regulary update passwords.
* Enable 2FA

6.

* Longer passwords always scored higher
* Random combinations were stronger than meaningful phrases or words.
* Repeated characters or patterns lowered the score
* Adding symbols like @, #, !, and & significantly increased strength scores.

7. Common password attacks include

* Brute force : a trial-and-error method used by attackers to guess passwords, encryption keys, or other sensitive information by systematically trying all possible combinations.
* Phishing: a type of cyberattack where malicious actors deceive individuals into revealing sensitive information, often through fraudulent emails, messages, or websites.
* Credential stuffing: a type of cyberattack where cybercriminals use lists of stolen usernames and passwords (often obtained from data breaches) to try and access other online accounts.
* Pasword spraying: a form of brute-force cyberattack in which threat actors attempt to access large numbers of accounts (usernames) with a few commonly used passwords.
* Keylogging: also known as keystroke logging, is the process of secretly recording the keys pressed on a keyboard.
* Man-in-the-middle attacks: attack is a type of cyberattack where an attacker secretly intercepts and relays communications between two parties, potentially altering the communication or stealing sensitive information.

8. Password complexity dramatically increases the time needed for an attacker to crack a password. A simple 8-character password like password1 can be guessed in seconds, while a 16-character complex password with mixed characters can take centuries to crack using brute force.