**TASK – 6**

***CYBERSECURITY INTERN***

MADHAV P RAJEEV

[Madhavrajeev93@gmail.com](mailto:Madhavrajeev93@gmail.com)

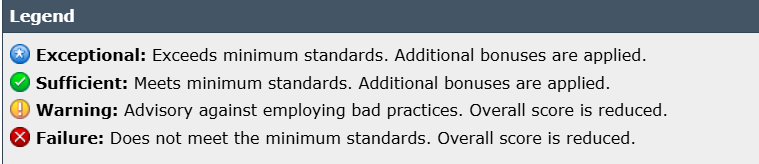
**Password Strength Checker :**

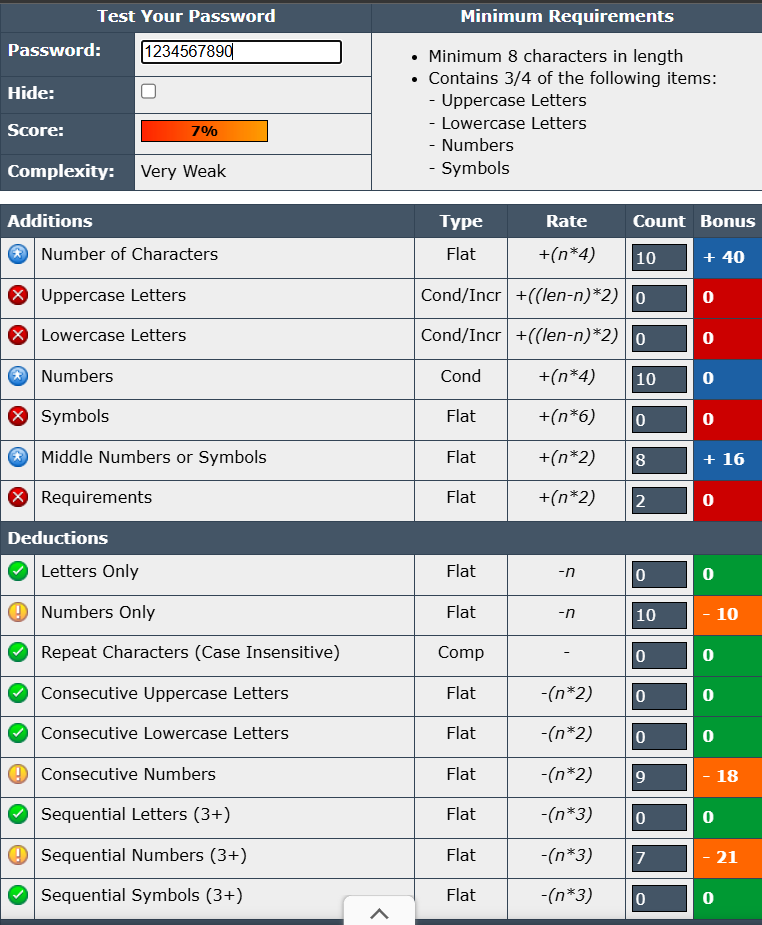
Strength of the password Analysed using <https://passwordmeter.com>

**Password Samples:**

* Password@123
* PaSwORD\_!23
* @w33ewjn7t1738£
* 1234567890

**Results:**

****

****

****

****

****

**Detailed Research: Password Attacks**

1. Overview of attack types

Brute-force attack

* What: Attacker tries every possible combination until the correct password is found.
* Where used: Offline (attacker has a hash/database) and online (login form).
* Characteristics: Guaranteed to find password eventually; cost and time grow exponentially with password length and character set.

Dictionary attack

* What: Attacker tries likely passwords from a precompiled list (wordlists, leaked passwords, common patterns).
* Where used: Very effective for weak human-chosen passwords. Often combined with mangling rules (e.g., append numbers, leet substitutions).
* Characteristics: Much faster than full brute force when users pick words, names, or predictable variations.

Credential stuffing

* What: Uses breached username/password pairs from one site against other sites (automated reuse attempts).
* Where used: Online. Targets services where users commonly reuse credentials. Often uses large-scale automation and IP/proxy rotation.
* Characteristics: High success rate when users reuse passwords; low effort for attacker.

Related techniques

* Rainbow tables: Precomputed hash → password tables to invert common hashes quickly (mitigated by unique salts).
* Hybrid attacks: Combine dictionary with brute-force suffix/prefix additions.
* Phishing & social engineering: Trick users into revealing credentials — orthogonal but often more effective than technical attacks.
* Keylogging / malware: Capture typed passwords directly.

**Best practices for creating strong passwords**:

1. **Use a mix of characters** – Combine uppercase letters, lowercase letters, numbers, and special symbols (e.g., @, #, $, !) to increase complexity.
2. **Make it long** – Aim for at least **12–16 characters**. Longer passwords are exponentially harder to crack.
3. **Avoid common words or patterns** – Don’t use easily guessable information like password123, birthdays, or repeated sequences (abcd, 1111).
4. **Use passphrases or random combinations** – A series of unrelated words or a random string of characters is more secure (e.g., Tiger!Blue7$Rocket).
5. **Unique passwords for each account** – Never reuse passwords across multiple accounts; this prevents a breach on one service from compromising others.