Password Strength Evaluation Report

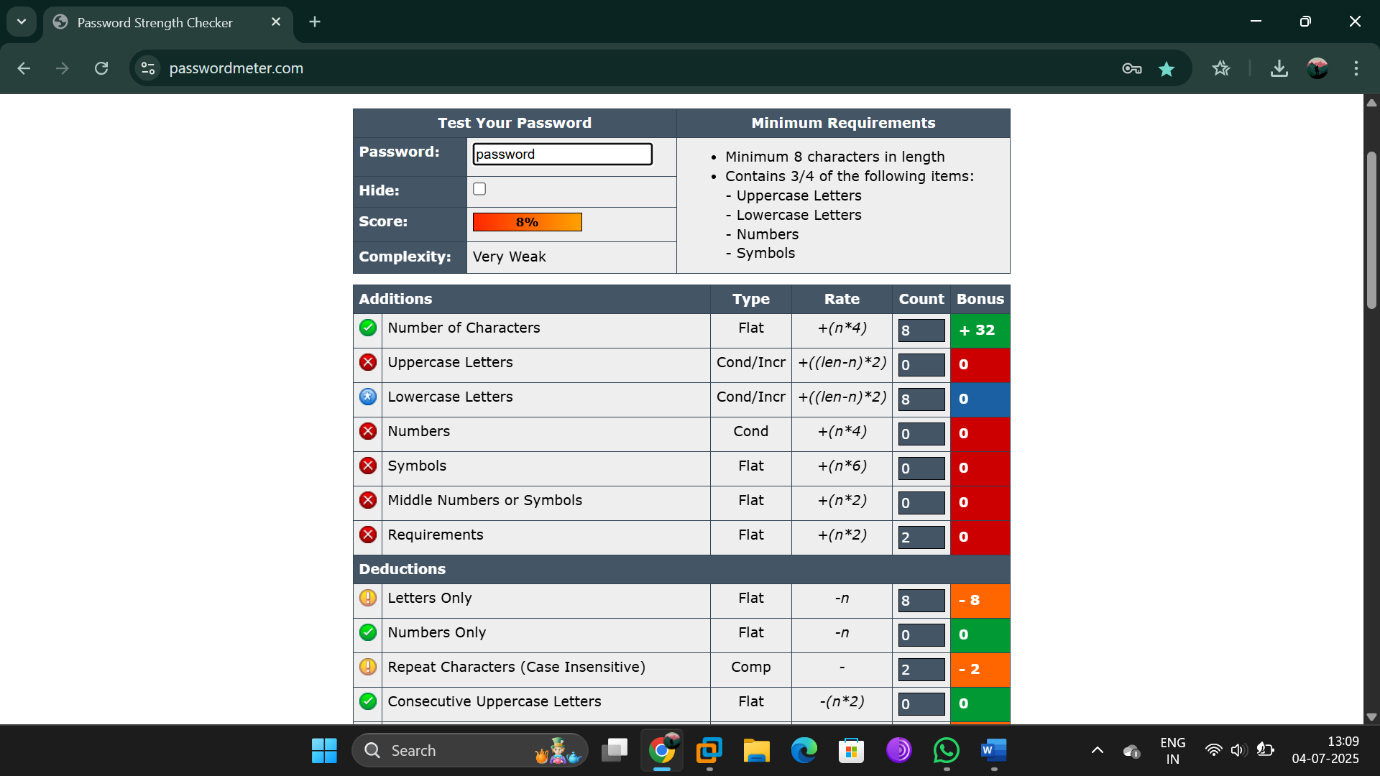
Objective:

Evaluate how password complexity influences security, test several password types using online

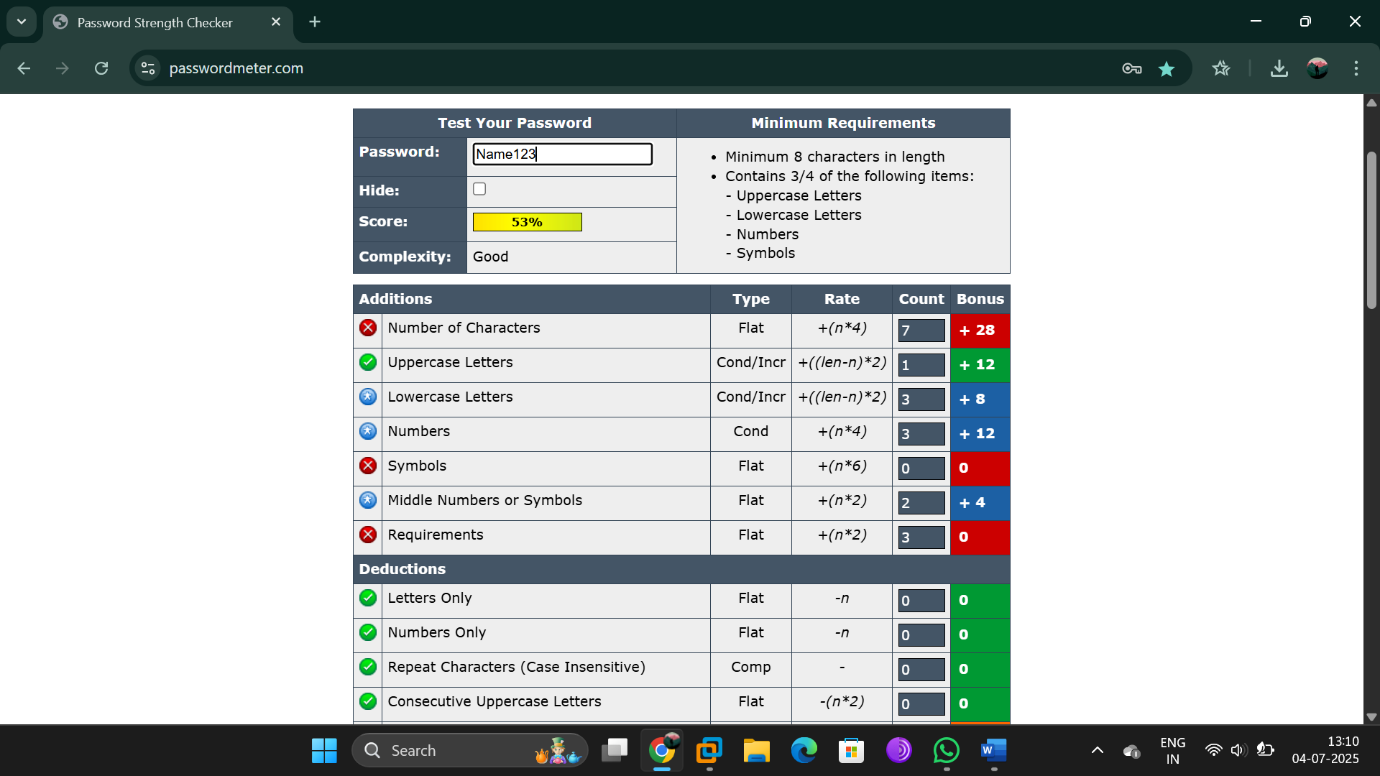
strength checkers, and document attack methods and best practices.

Password Evaluations:

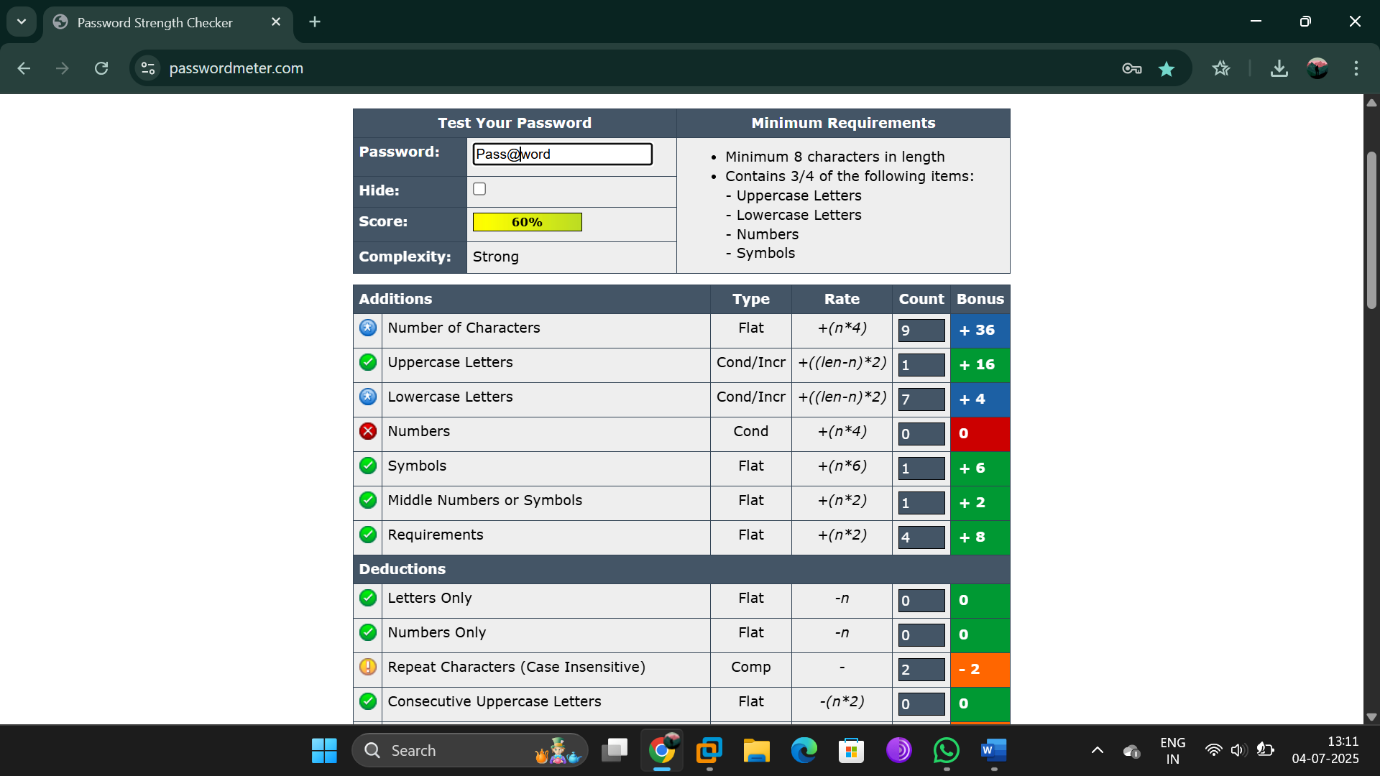
1. password - Basic lowercase . Length: 8. Rating: Weak . Easily guessable.



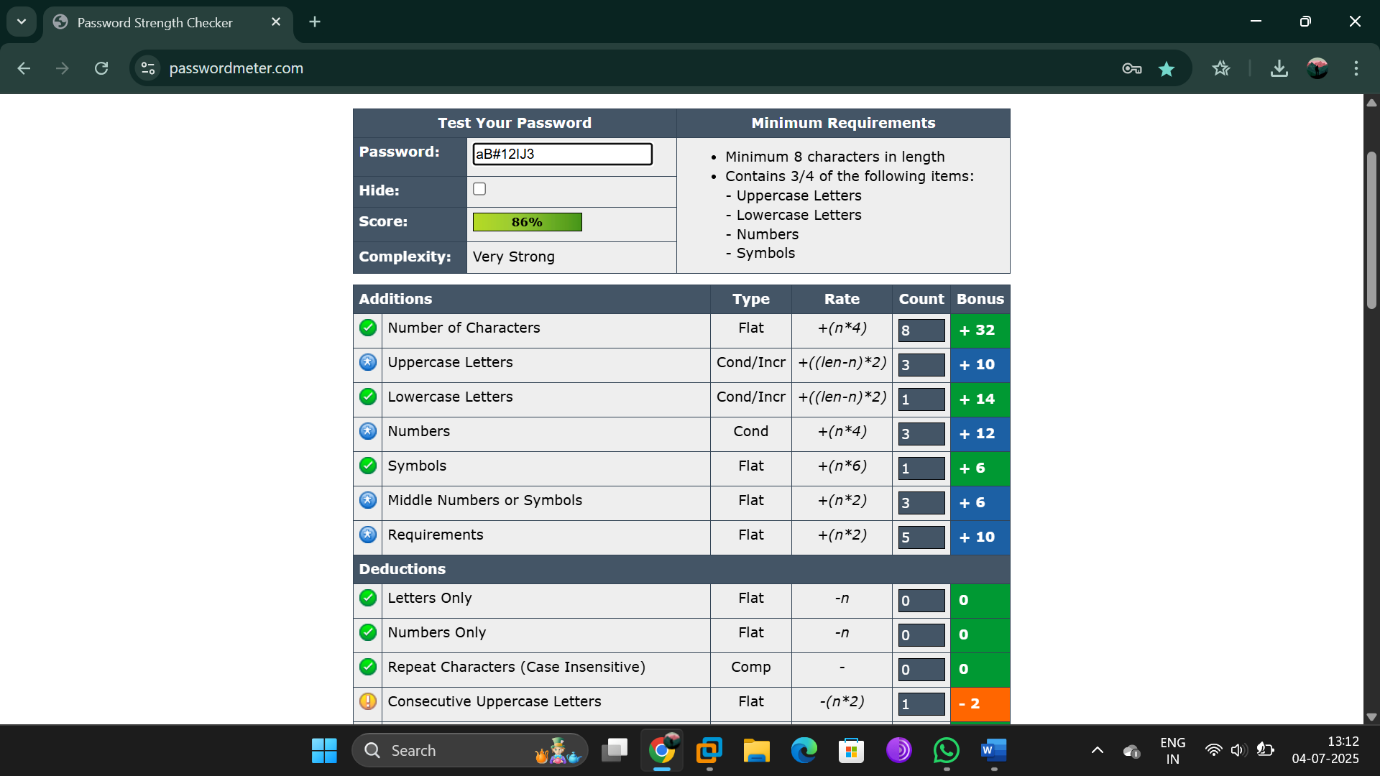
1. Name123 - Common substitution. Rating: Good. Still vulnerable to hybrid attacks.



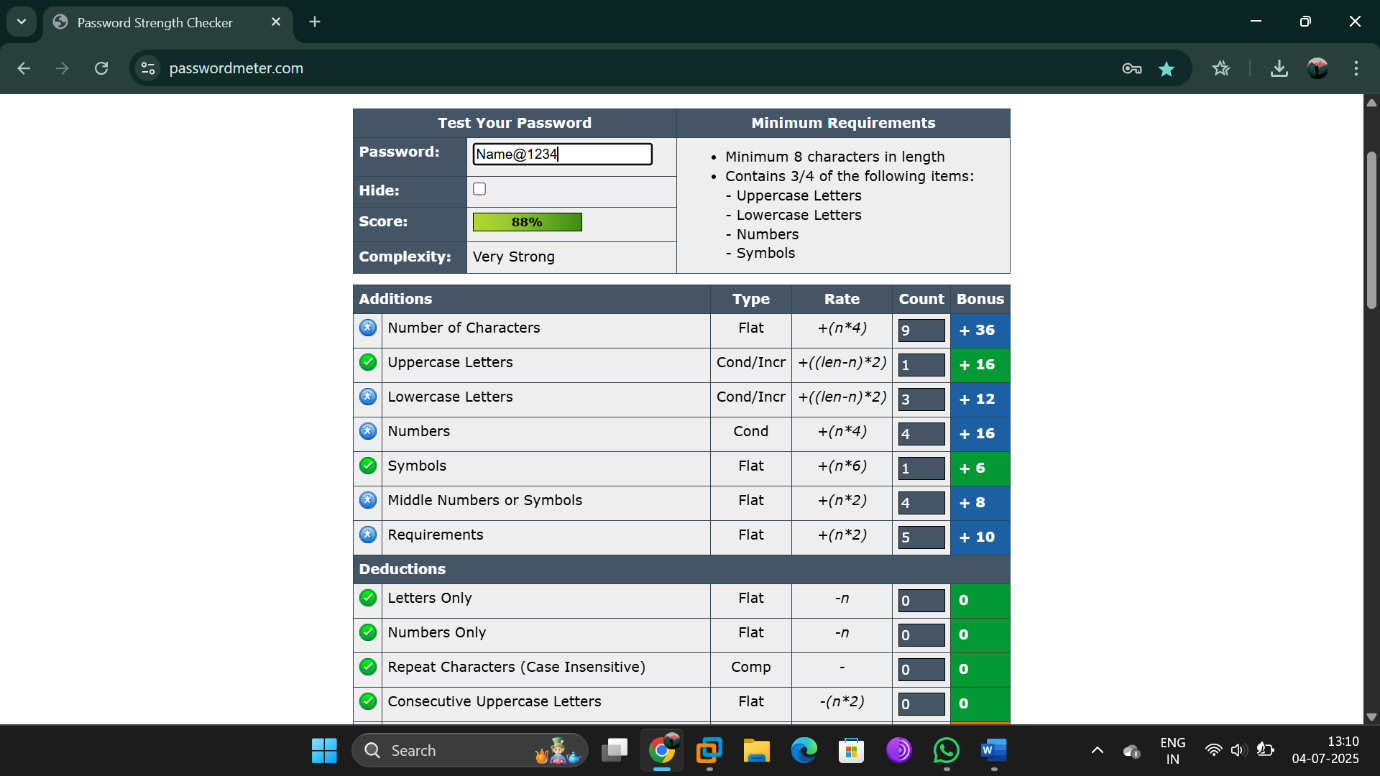
1. Pass@word - Randomized with symbols and letters. Rating: Strong.



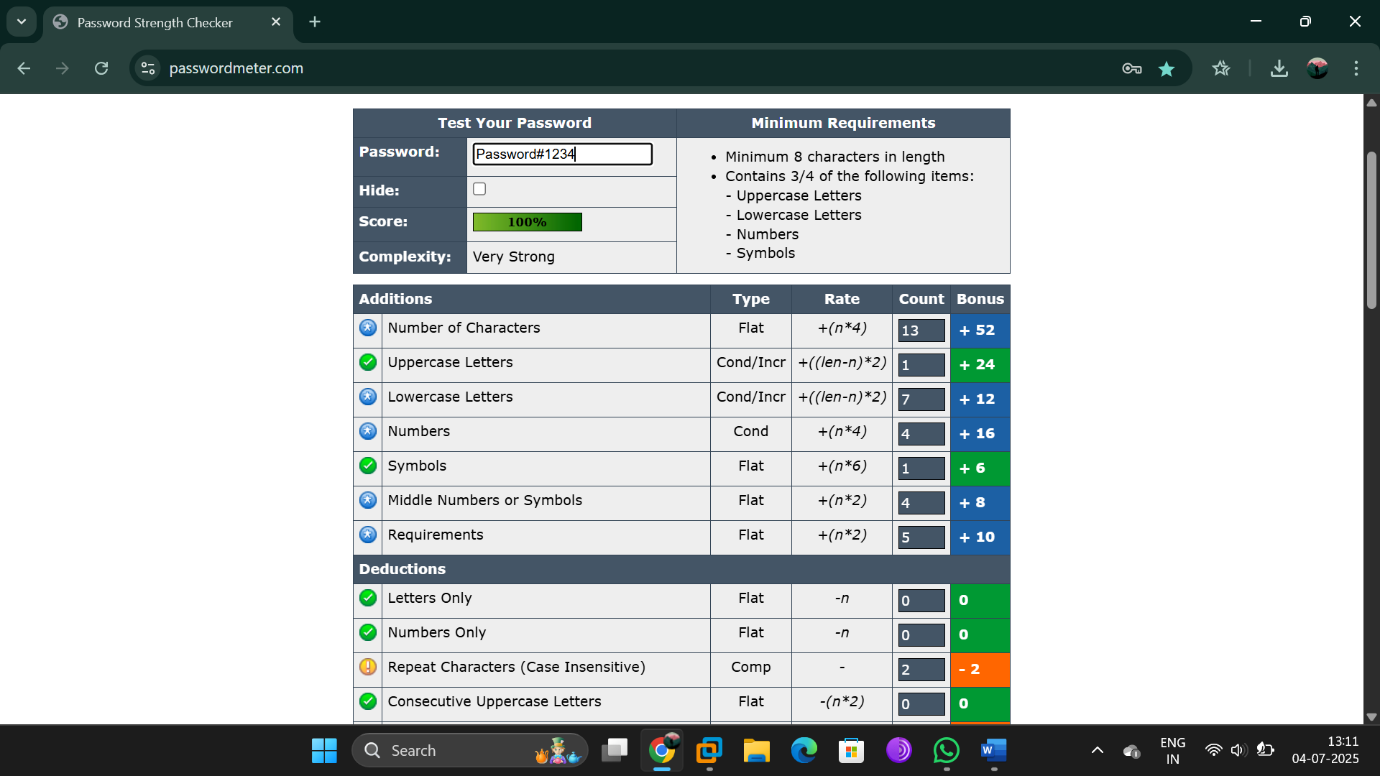
1. aB#12IJ3 - Secure – High complexity. Rating: Very Strong.



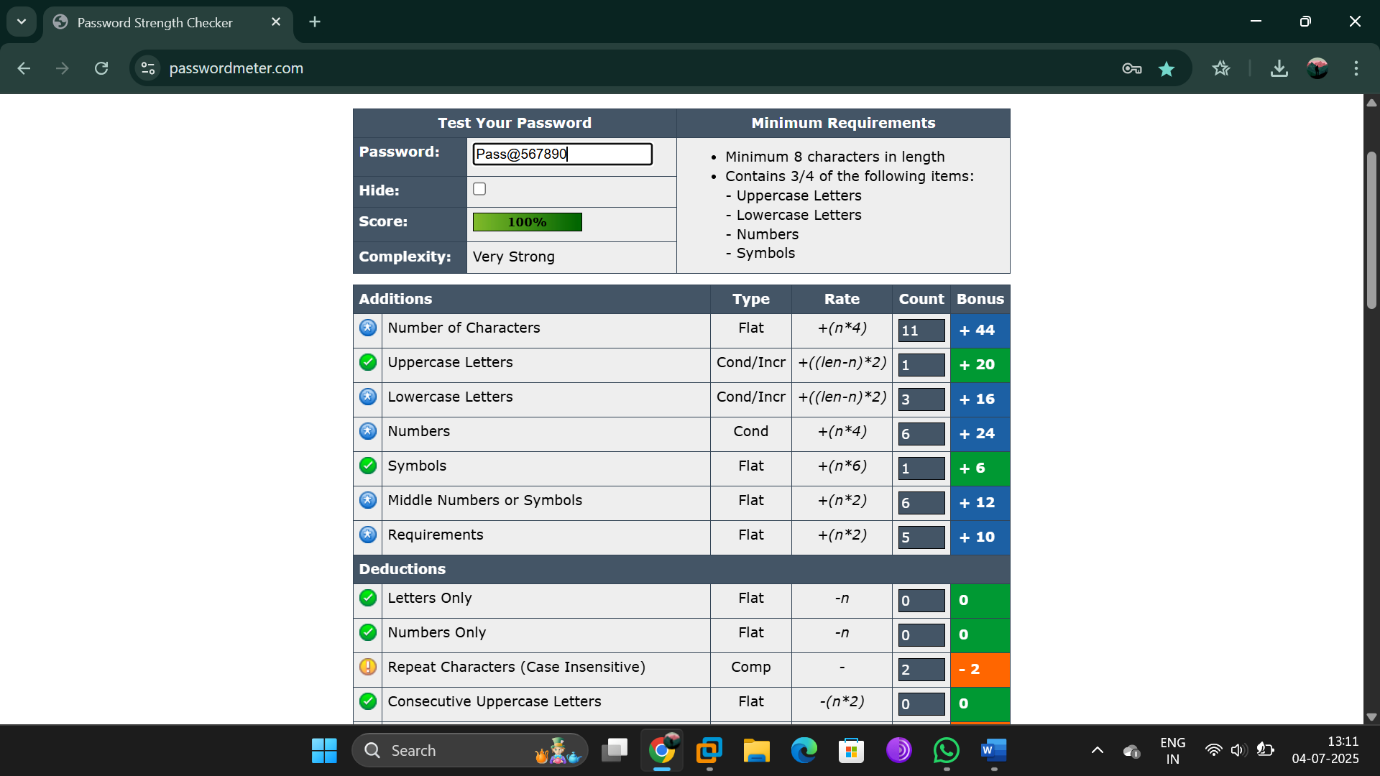
1. Name@1234 - letter, numeric, symbols . Rating: Very Strong.



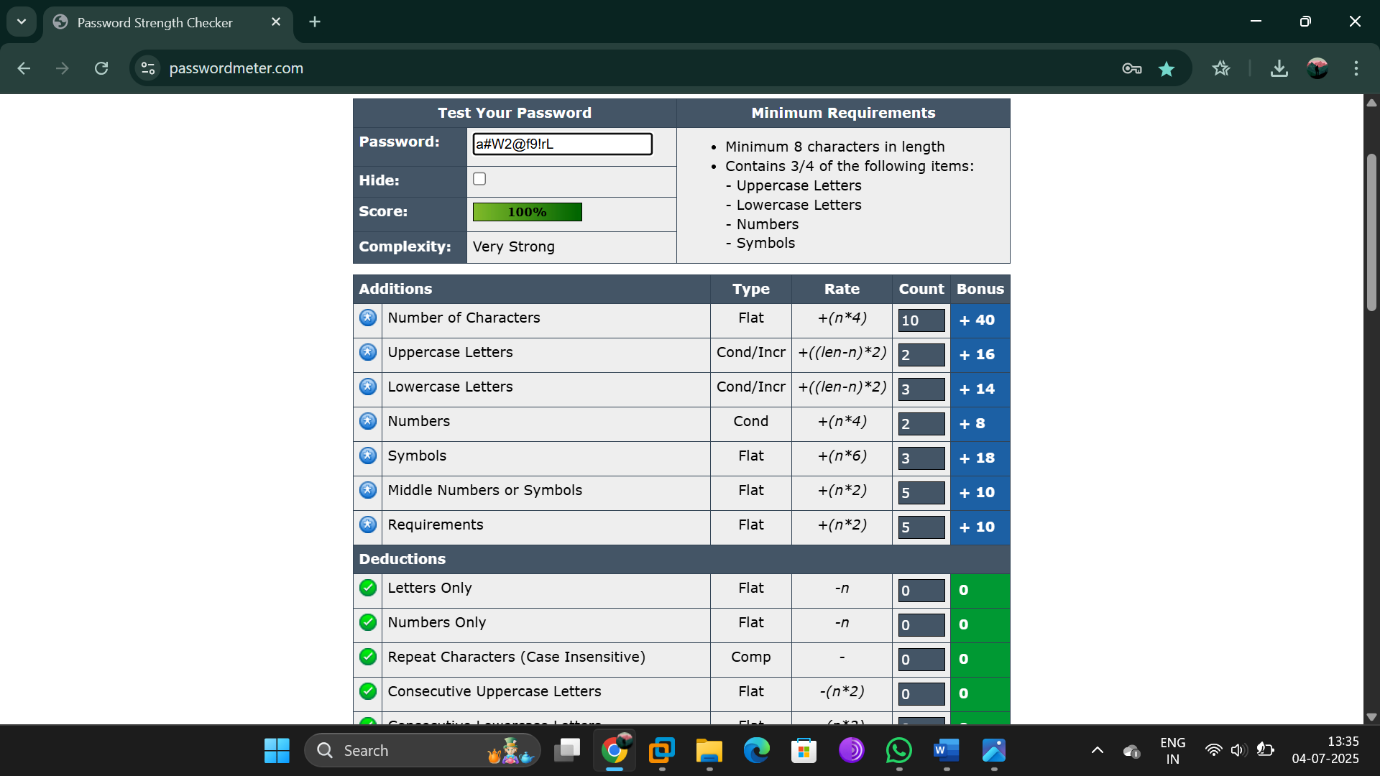
1. Password#1234 - High complexity. Rating: Very Strong.



1. Pass@567890 - High complexity. Rating: Very Strong



1. a#W2@f9!rL - high complexity. Rating: Very Strong



Best Practices for Strong Passwords:

- Use 12-16+ characters.

- Combine upper/lowercase, numbers, and symbols.

- Avoid dictionary words, names, or common patterns.

- Use password managers.

- Enable multi-factor authentication (MFA).

Common Attack Methods:

- Brute-force: Tries all combinations.

- Dictionary: Uses known word lists.

- Credential Stuffing: Tests leaked combinations.

- Hybrid Attacks: Mixes known words with symbols.

Password Complexity & Security

Greater complexity and length increase resistance to cracking.

Example: 'Pass123!' is crackable in minutes; 'RainCloud$42\*Secure' may take centuries.

Key Takeaways:

- Randomness and length provide better security than substitutions.

- Avoid reuse and predictability.

- Password managers simplify complex password usage.