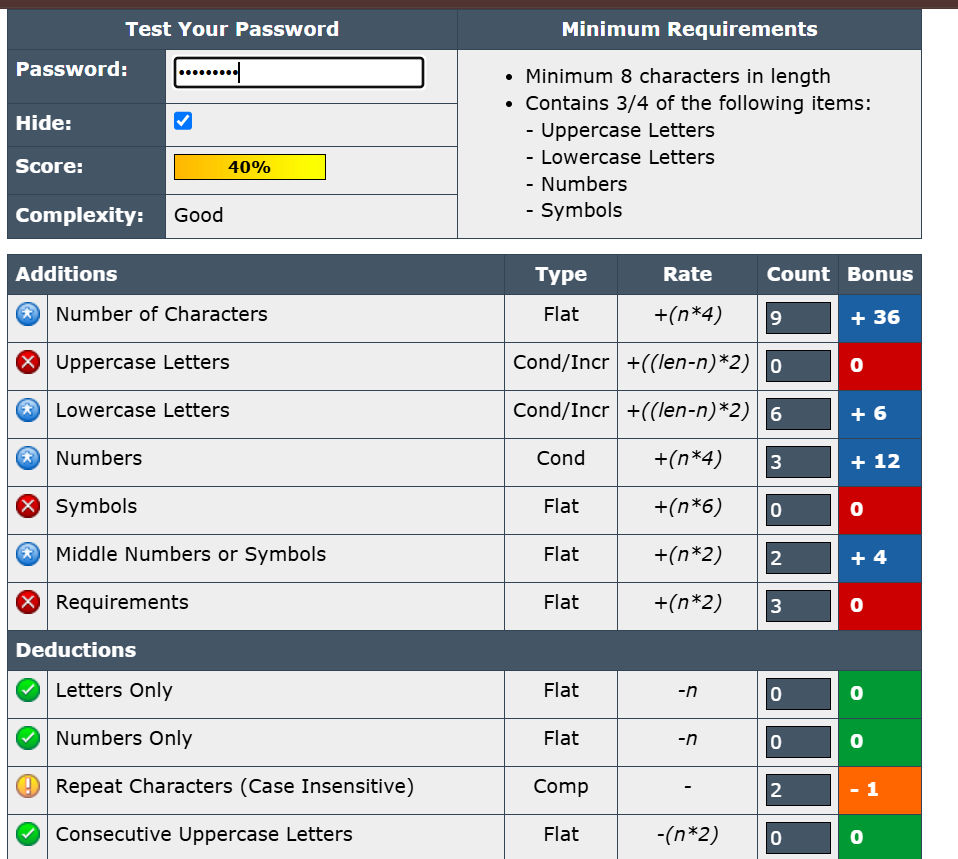
sanika123

This password received a weak rating from the strength checker. It only uses lowercase letters and numbers, making it highly predictable and easy to guess. Since it’s based on a name and common number pattern, it is vulnerable to dictionary and brute force attacks. The estimated crack time was extremely low just a few seconds highlighting its insecurity.

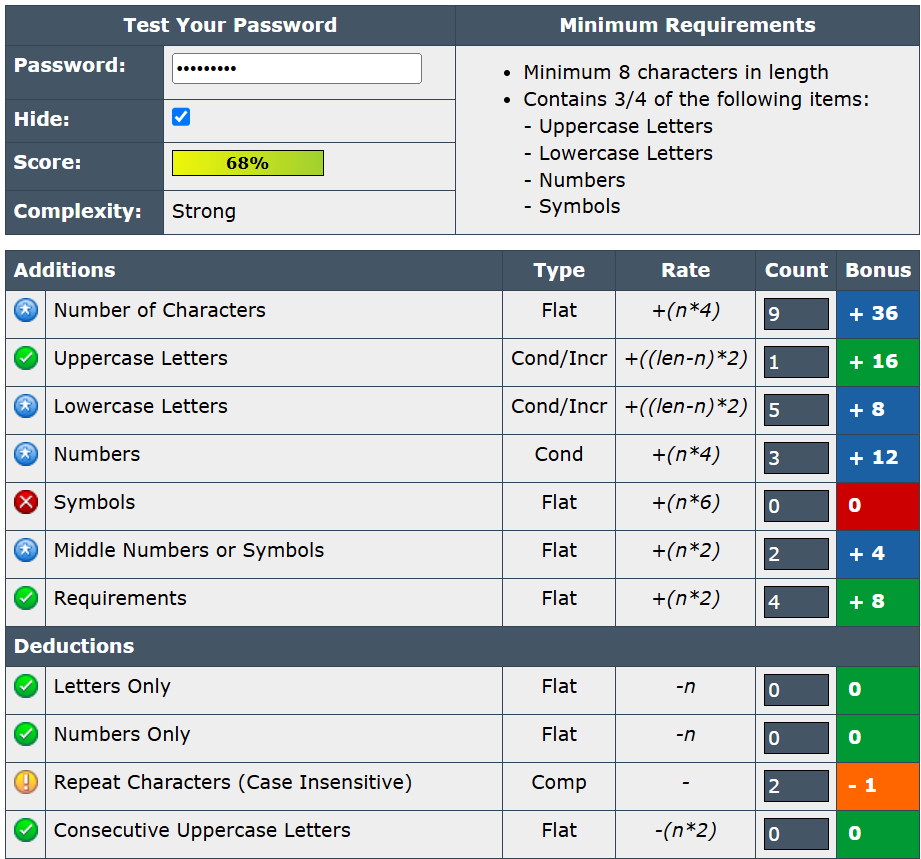


A screenshot of a computer

AI-generated content may be incorrect.

Sanika123

Adding a capital letter improved this password slightly. However, it still follows a predictable structure: a name followed by numbers. The strength checker rated it as moderately weak. It remains susceptible to dictionary attacks and automated tools that guess common combinations of names and birth years. The estimated time to crack was a few seconds to minutes.

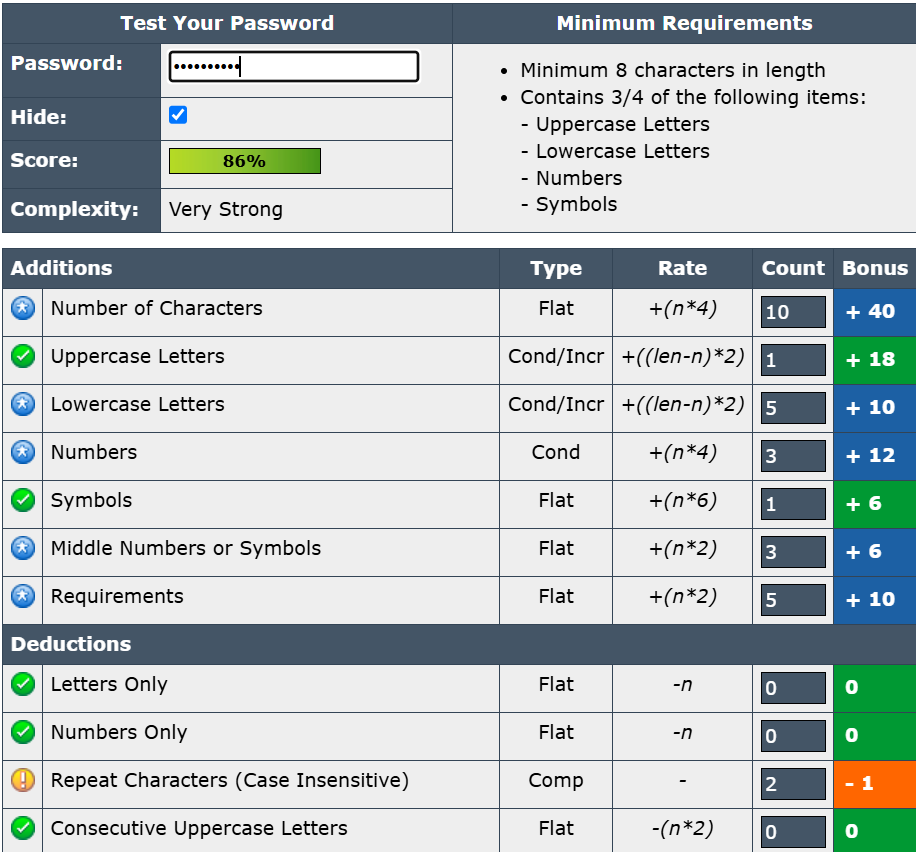


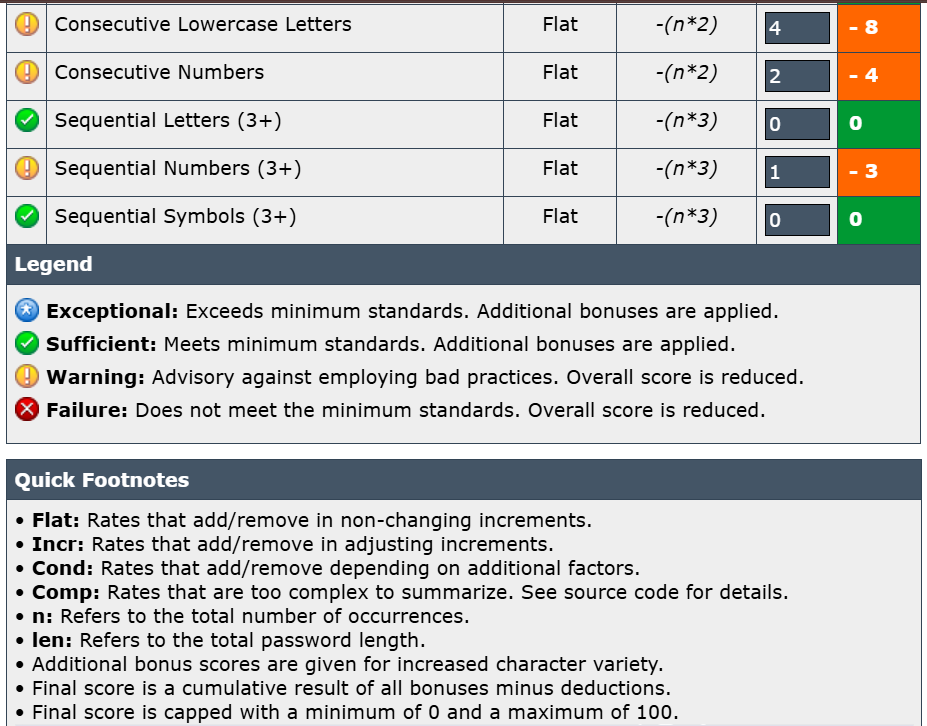
A screenshot of a computer screen

AI-generated content may be incorrect.

Sanika@123

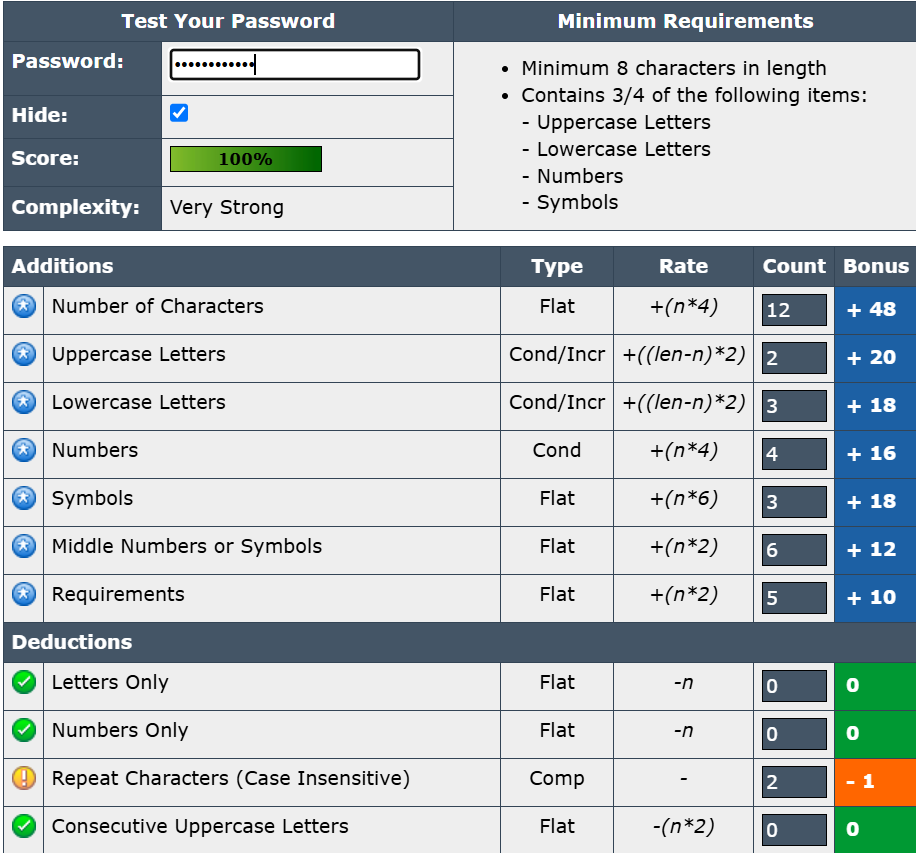
This version introduced a special character (@), which improved its strength. The password now has uppercase and lowercase letters, a number, and a symbol. The strength checker classified it as a stronger password but noted that the structure is still somewhat predictable. Estimated crack time increased to several hours, showing better resistance to basic attacks.





S@niKa!2025#

This password is much stronger and received a high score from the tool. It uses a mix of uppercase and lowercase letters, multiple special characters, and a number. It is longer and not easily guessable. The estimated time to crack this password was several years or more, making it highly resistant to brute force or dictionary attacks.



A screenshot of a computer

AI-generated content may be incorrect.

From this task, I learned that password complexity significantly improves security. Simple passwords even with some variations can be cracked within seconds using brute force or dictionary attacks. Strong passwords include a combination of uppercase and lowercase letters, numbers, symbols, and sufficient length (at least 12–16 characters). The best passwords are unpredictable and avoid personal information like names or birth years. Using tools like password strength checkers helps in understanding weaknesses. In addition, best practices such as using passphrases, password managers, and multi-factor authentication greatly enhance overall password security.