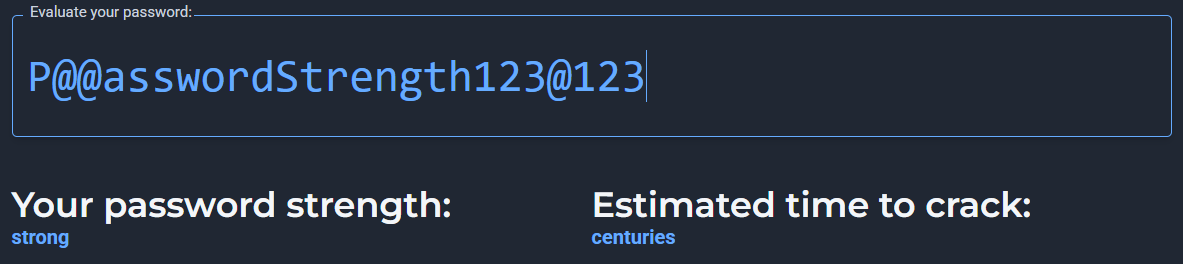
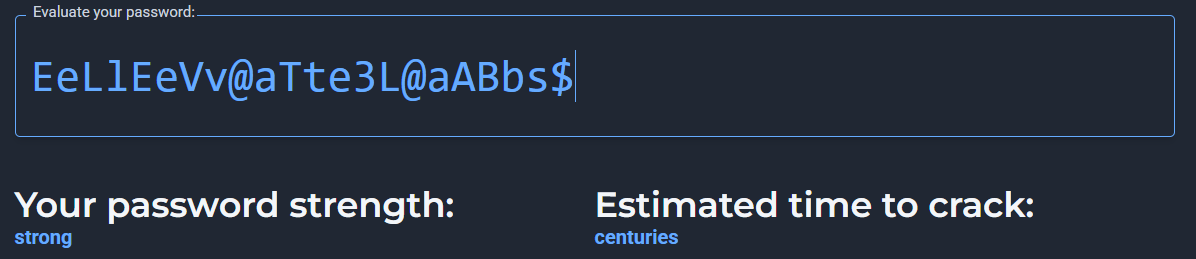
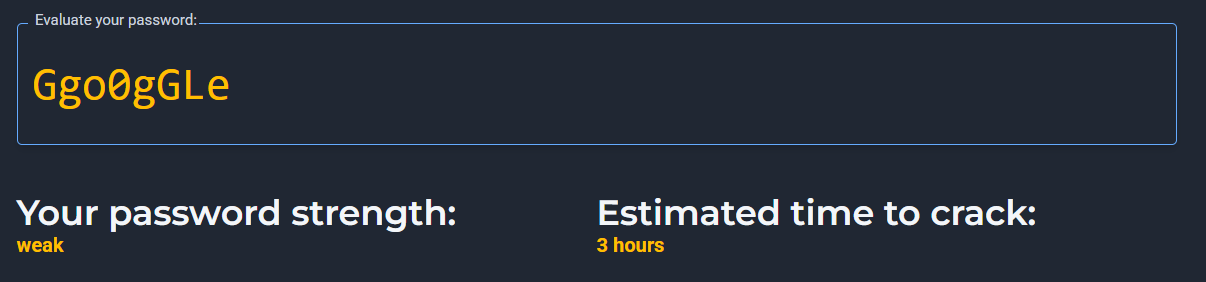
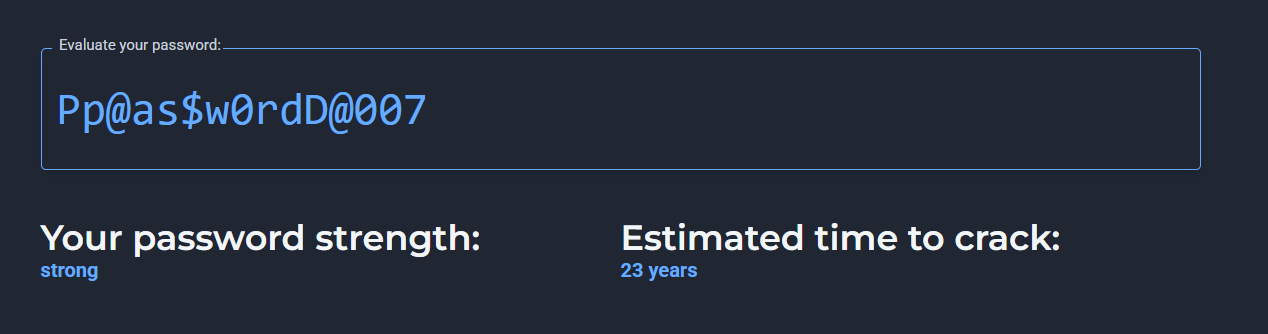
Password Security Evaluation Report

# Tool Evaluation Screenshots









# 1. Scores and Feedback from the Tool

Based on the analysis from the uploaded evaluation tool screenshots, the results show the effectiveness of the tested passwords in terms of strength, entropy, and resistance against common password attacks. Higher scores generally indicate stronger resistance to brute-force or dictionary-based guessing, while lower scores highlight weak or easily predictable choices. Feedback typically emphasizes the length, use of mixed character sets, and avoidance of common words or sequences.

# 2. Best Practices for Creating Strong Passwords

From the evaluation, several best practices for building strong passwords emerge:

* • Use a mix of uppercase, lowercase, numbers, and special characters.
* • Ensure passwords are at least 12–16 characters long.
* • Avoid dictionary words, names, birthdays, or common patterns.
* • Use passphrases (a sequence of unrelated words) for easier memorization.
* • Change passwords regularly and do not reuse the same password across accounts.
* • Consider using a password manager to generate and securely store complex passwords.

# 3. Tips Learned from the Evaluation

The tool demonstrated that short or simple passwords were scored poorly, while longer, more complex ones showed higher resistance to attacks. The evaluation reinforced the idea that even a slight increase in password length dramatically improves security. It also showed that predictable substitutions (e.g., 'P@ssw0rd') provide little benefit as attackers commonly anticipate them.

# 4. Common Password Attacks

The two most common password attacks include:

* • Brute Force Attack: systematically trying every possible combination of characters until the correct password is found. Its success depends on password length and complexity.
* • Dictionary Attack: uses precompiled lists of words, phrases, or common passwords to guess quickly. Simple or common passwords are highly vulnerable.

Other attacks include credential stuffing (using leaked credentials from breaches) and social engineering (tricking users into revealing passwords).

# 5. How Password Complexity Affects Security

Password complexity plays a crucial role in resisting attacks. A complex password with a mix of characters exponentially increases the number of combinations an attacker must try. For example, an 8-character lowercase-only password has just 26^8 possibilities, while an 8-character password with uppercase, lowercase, numbers, and symbols has over 95^8 possibilities. This makes brute-force attacks impractical. Similarly, dictionary-based attacks become less effective when a password avoids recognizable words or patterns.