**Password Strength Report**

**Introduction**

Passwords are essential for securing personal and online accounts, but many users still rely on weak or easily guessable passwords. This report evaluates common password vulnerabilities and offers recommendations for stronger password practices.

**Common Password Vulnerabilities**

Many users choose weak passwords like simple words, number sequences, or common patterns that are easy for attackers to guess. Below is a list of common weak passwords:

common\_passwords = [

"password", "123456", "qwerty", "letmein", "welcome", "123456789",

"12345", "abc123", "password1", "iloveyou", "monkey", "qwerty123" ]

These passwords are easily guessed by attackers using brute-force or dictionary-based attacks.

**Password Evaluation Criteria**

1. **Length**: At least 8 characters.
2. **Complexity**: Mix of uppercase, lowercase, numbers, and special characters.
3. **Avoid Common Passwords**: Use passwords not found in common password lists.
4. **Avoid Repeating Patterns**: No repeated characters like "aaaaaa" or predictable sequences like "123456".

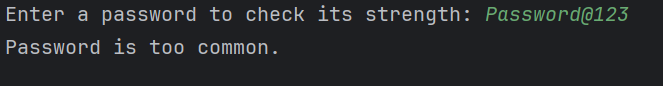
**Recommendations for Stronger Passwords**

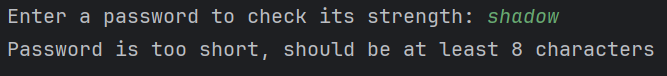
* **Increase Length**: Aim for 12-16 characters.
* **Use Complexity**: Mix letters (uppercase and lowercase), numbers, and symbols.
* **Avoid Common Words**: Don’t use dictionary words or personal information.
* **Use a Password Manager**: Securely store complex passwords.
* **Enable Two-Factor Authentication (2FA)**: Add an extra layer of security.

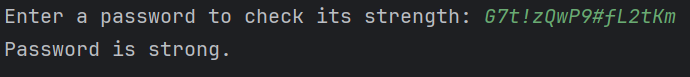
**Example of Strong Passwords:**

* "S!lver$unR@1n21"
* "P@ssw0rdsAre#S@fe"

**Use Case**







**Conclusion**

Weak passwords, like "123456", "password", and "qwerty", are easy for attackers to guess and can lead to account breaches. Many people reuse passwords, so compromising one account can put others at risk.

To improve security, use passwords that are at least 12-16 characters long with a mix of uppercase, lowercase, numbers, and special characters. A **password manager** can help generate and store unique passwords for each account. Additionally, enabling **Two-Factor Authentication (2FA)** provides extra protection even if your password is compromised.

By adopting these practices, you can significantly reduce the risk of unauthorized access and better secure your online accounts.