Future Interns

Task 2

Building the password strength analyzer Tool.

Password Strength Analyzer Report:

Introduction

The Password Strength Analyzer is a Python-based desktop application designed to assess and enhance password security. The tool evaluates passwords based on established security criteria and provides feedback to help users create stronger credentials. Additionally, it incorporates SHA-256 hashing for password encryption. This report presents a comprehensive analysis of the tool's functionalities, strengths, areas for improvement, and future development recommendations.

Application Overview:

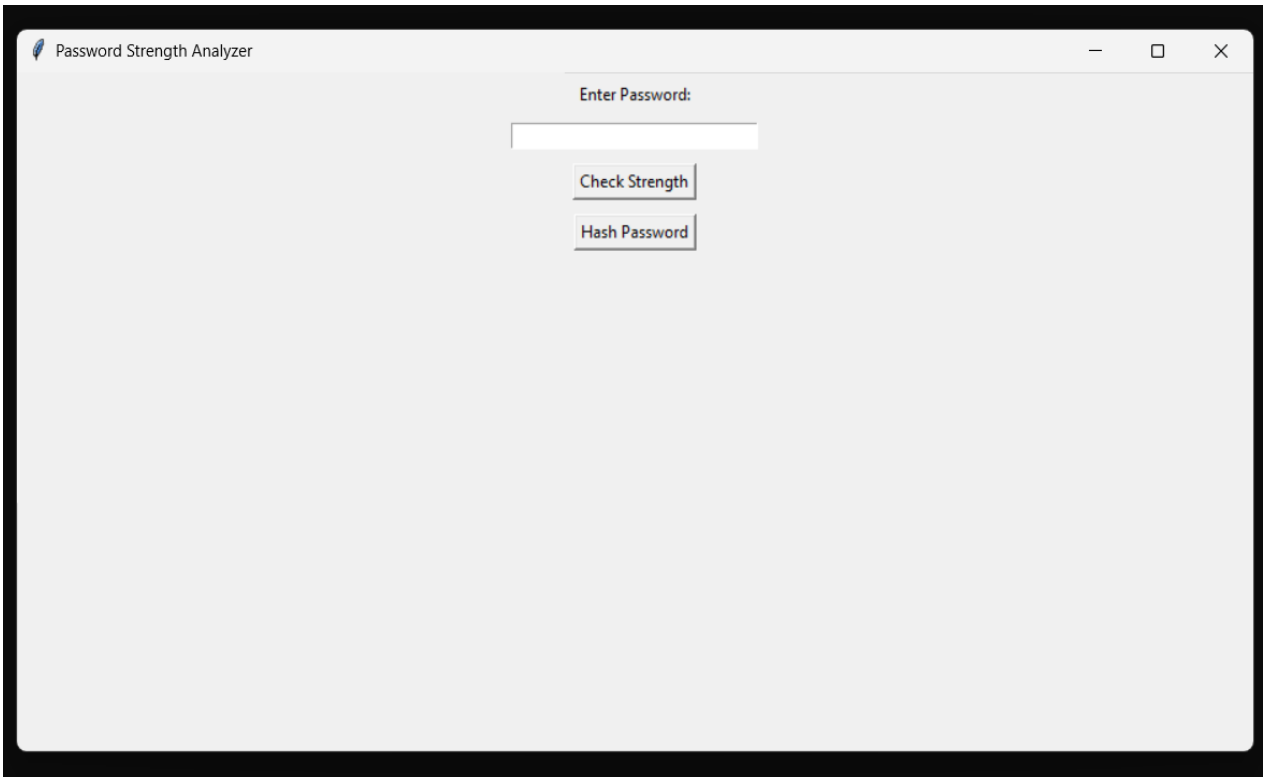
The Password Strength Analyzer consists of the following core features:

1. Password Strength Checking
   - The tool assesses password strength by checking:
     - Minimum length of 8 characters.
     - Inclusion of uppercase and lowercase letters.
     - Presence of numbers and special characters.
   - It categorizes passwords into three levels: Weak, Moderate, or Strong.
2. Password Criteria Display
   - Users receive a pop-up message detailing the password strength requirements:
     - A lowercase letter.
     - A number.
     - A special character.
     - A minimum length of 8 characters.
   - Feedback is provided to help users improve their passwords.
3. Password Hashing
   - The tool generates a SHA-256 hash of the entered password, ensuring additional security by preventing plaintext password storage.
   - The hash value is displayed to users as a security measure.

Screenshots

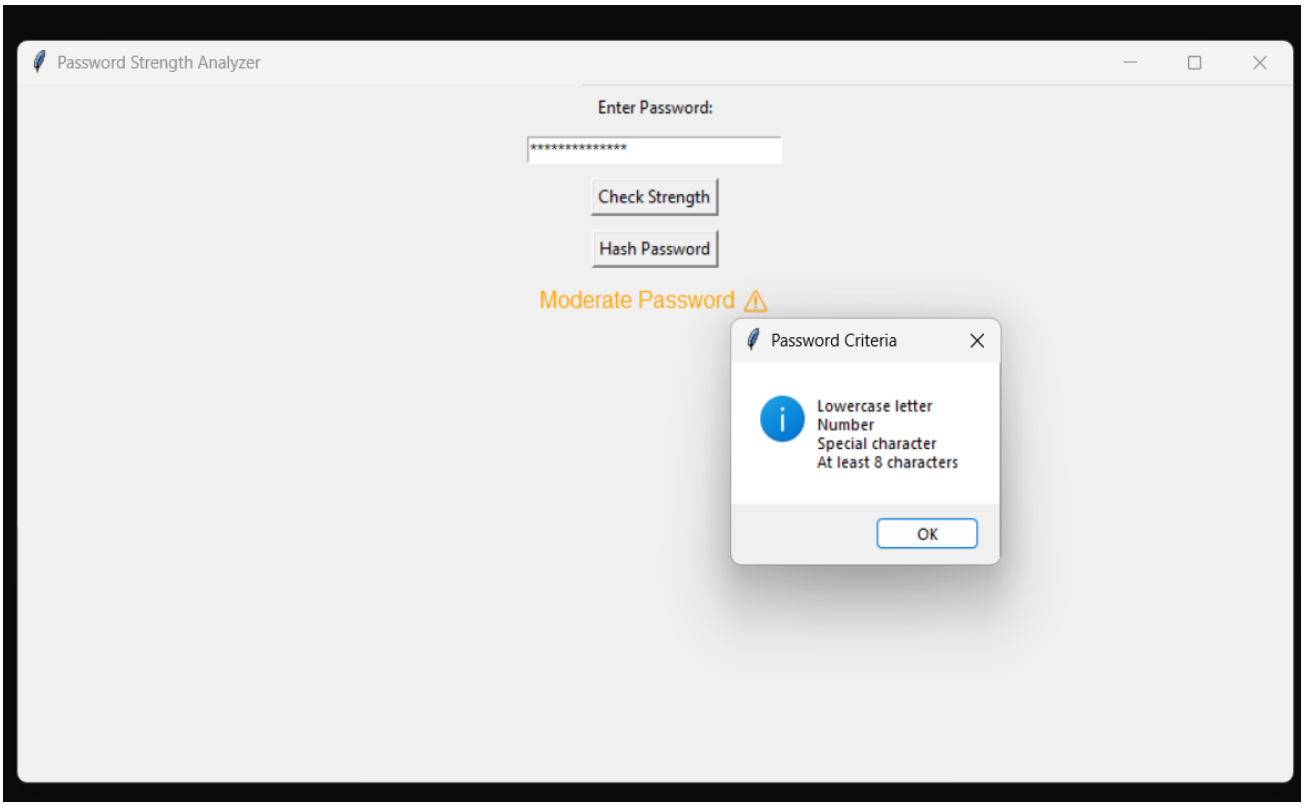
The following images illustrate different aspects of the Password Strength Analyzer:

1. Initial Interface
    - The first screenshot shows the application's main interface, where users can enter a password and select an action.

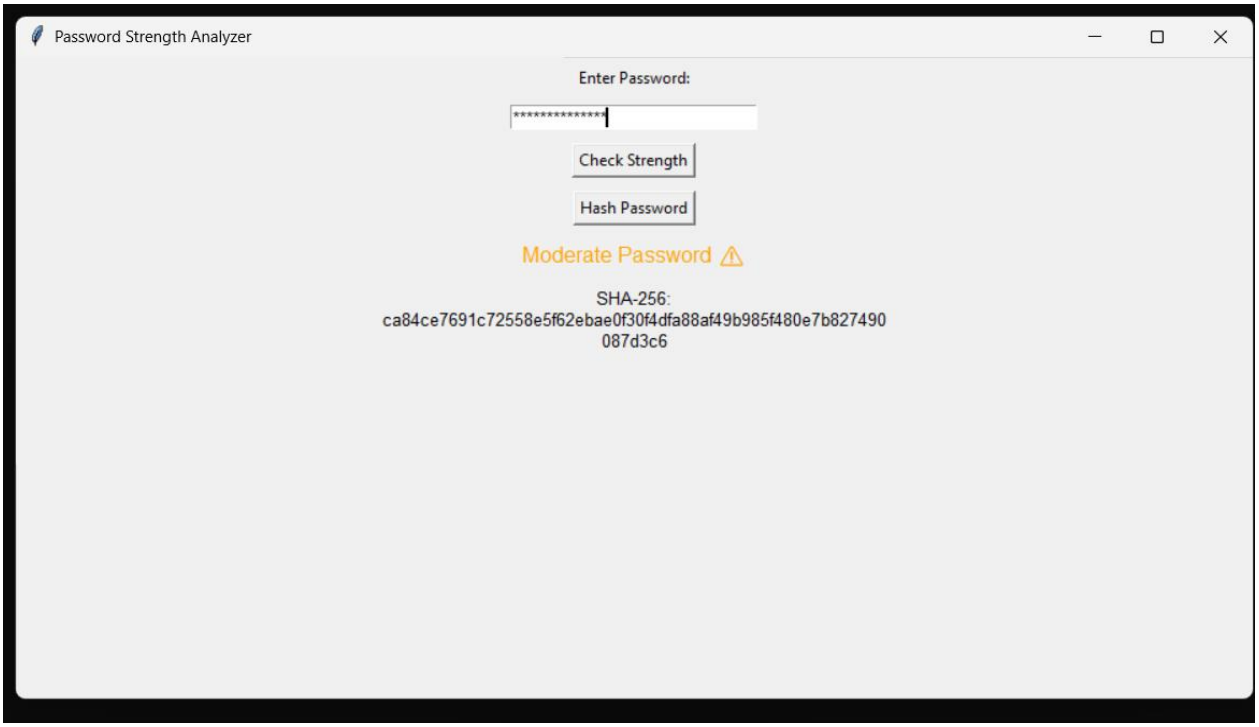


2. Password Strength Evaluation

- The second screenshot captures the system's evaluation of password strength, displaying a 'Moderate Password' message with criteria.



3. Password Hashing
    - The third screenshot displays the SHA-256 hash generated for the entered password.



Strengths of the Application:

- User-Friendly Interface:
    - The simple Tkinter-based GUI ensures ease of use for all users.
- Security Awareness:

    - The password strength evaluation mechanism educates users on secure password practices.
- Secure Hashing:
    - The SHA-256 hashing mechanism prevents plaintext password storage, enhancing security.
- Actionable Feedback:
    - The tool suggests improvements when a password is weak or moderate.

Areas for Improvement:

- More Granular Strength Ratings:
    - The system currently categorizes passwords broadly. Implementing a more detailed rating system (e.g., Weak, Fair, Good, Strong, Very Strong) would improve user feedback.
- Integration with External APIs for Breach Checks:
    - Integrating APIs like 'Have I Been Pwned' could allow users to check whether their password has been compromised in data breaches.
- Blacklist Common Passwords:
    - Adding a database of commonly used weak passwords (e.g., "123456," "password") would help prevent insecure password choices.

- Enhanced Password Recommendations:
    - The tool could dynamically suggest ways to strengthen a password based on the entered input.

Future Enhancements:

To further improve the Password Strength Analyzer, the following updates could be considered:

- Multi-Factor Authentication (MFA) Integration:
    - Adding MFA support would enhance overall security.
- Use of Stronger Hashing Algorithms:
    - Replacing SHA-256 with bcrypt or Argon2 would improve password security.
- Password History Validation:
    - Checking if a password has been used before could prevent credential reuse.
- Cross-Platform Compatibility:
    - Packaging the tool into an executable file using PyInstaller or other tools for broader usability.

Conclusion:

The Password Strength Analyzer is a valuable tool for evaluating and improving password security. By addressing the recommendations outlined in this report, it can evolve into a more robust and comprehensive security tool. Its intuitive interface, secure hashing, and password evaluation features provide a strong foundation for future improvements.

This report serves as a guideline for enhancing the tool's capabilities, ensuring a more secure and user-friendly experience for all users.