**Report: Password Strength Checker Tool**

**1. Introduction**

The **Password Strength Checker Tool** is a user-friendly application designed to evaluate the strength of passwords and provide actionable feedback to users. With increasing cybersecurity threats, creating strong passwords is critical to safeguarding sensitive information. This tool leverages a graphical user interface (GUI) to allow users to test their passwords and receive detailed feedback on their strengths and weaknesses.

The tool is implemented using Python's tkinter library for the GUI and incorporates robust password evaluation criteria, making it an educational and practical utility for enhancing password security awareness.

**2. Features/Characteristics**

The Password Strength Checker Tool includes the following key features:

* **Graphical User Interface (GUI):**
  + A clean, intuitive interface built with tkinter.
  + Visual feedback through color-coded strength levels and progress bars.
* **Password Evaluation Criteria:**
  + Length-based checks (e.g., minimum 8, 12, 17, and 20 characters).
  + Character diversity checks:
    - Presence of uppercase letters.
    - Presence of lowercase letters.
    - Inclusion of special characters.
    - Use of numeric digits.
* **Detailed Feedback:**
  + Displays criteria that are met (with green checkmarks).
  + Highlights missing criteria (with red X marks).
* **Dynamic Progress Bar:**
  + Reflects the overall strength score visually.
* **Color-Coded Strength Levels:**
  + Weak (Red), Okay (Orange), Good (Yellow), Strong (Green).
* **Real-Time Analysis:**
  + Immediate feedback as the user enters a password.

**3. Methodology**

The implementation of the Password Strength Checker Tool follows these steps:

1. **GUI Design:**
   * The tkinter library is used to create a visually appealing interface with labels, entry fields, buttons, and progress bars.
2. **Password Evaluation Logic:**
   * The tool evaluates passwords based on predefined criteria:
     + Length thresholds (>=8, >=12, >=17, >=20).
     + Diversity in character types (uppercase, lowercase, special characters, digits).
   * Each criterion is checked using Python's string manipulation and regular expressions.
3. **Feedback Mechanism:**
   * The tool categorizes passwords into four strength levels:
     + Weak, Okay, Good, Strong.
   * Provides detailed feedback on which criteria are met or missing.
4. **Dynamic Updates:**
   * The GUI dynamically updates the strength level, progress bar, and feedback labels when a password is entered.
5. **Color Coding:**
   * Uses color coding for visual clarity:
     + Green for met criteria.
     + Red for missing criteria.
     + Strength levels are color-coded for easy interpretation.

**4. Results**

The Password Strength Checker Tool was tested with various passwords to evaluate its functionality:

| **Password** | **Strength Level** | **Criteria Met** | **Criteria Missing** |
| --- | --- | --- | --- |
| 123456 | Weak | Length >= 8 | Uppercase, Lowercase, Special |
| Password123 | Okay | Length >= 8, Uppercase, Lowercase | Special Character |
| P@ssw0rd12345 | Good | Length >= 8/12/17, Uppercase, Lowercase, Special Character, Digit | None |
| Str0ngP@ssw0rd! | Strong | All | None |

The tool successfully identified strengths and weaknesses in each password and provided accurate feedback to users.

**5. Conclusion**

The Password Strength Checker Tool is an effective solution for evaluating and improving password security. Its GUI-based approach makes it accessible to users with minimal technical expertise while providing detailed insights into password strength.

**Key Benefits:**

* Educates users on creating strong passwords by highlighting weaknesses.
* Enhances security awareness through real-time feedback.
* Provides a visually engaging experience with intuitive design elements.

**Future Improvements:**

* Integration with external APIs for checking against common password databases.
* Support for additional languages to increase accessibility.
* Implementation of advanced entropy-based strength calculations.

This tool serves as a valuable resource for promoting better password hygiene in both personal and professional settings.

**Submission Details:**

* Submission Date: February 19, 2025
* Group Member Names:

|  |  |
| --- | --- |
| 16010122104 | Kashish Mamania |
| 16010122132 | Sania Parekh |
| 16010122143 | Tanaya Pawar |
| 16010122146 | Sarthak Pokale |