**Password Strength Checker**

**1.Abstract**

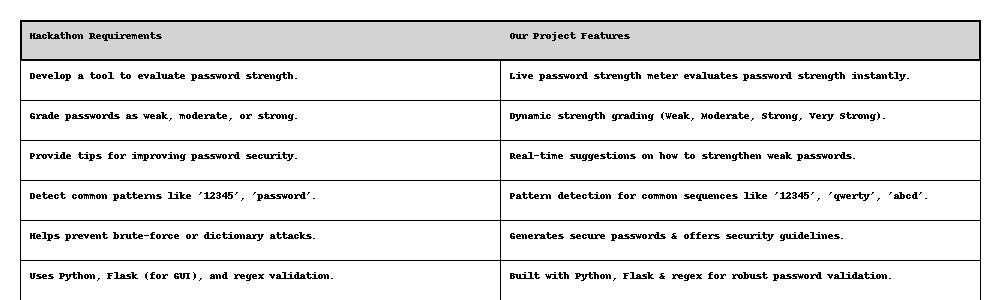
With increasing cybersecurity threats, weak passwords are one of the easiest entry points for attackers.

This project provides a Password Strength Checker, a simple yet effective tool that evaluates password strength, offers recommendations

for improvement, and detects common weak patterns. Built with Flask, JavaScript, and Regex-based validation, this tool helps users create

secure passwords while ensuring an interactive and user-friendly experience.

**2. Problem Statement vs. Our Project**



**3. Technology Stack**

- Backend: Flask (Python)

- Frontend: HTML, CSS, JavaScript

- Validation: Regex (Python)

- Styling & Animations: CSS (Transitions, Hover Effects)

- User Interface Enhancements: Dark Mode, Smooth Transitions, Live Strength Meter

- Password Generation: Python Random Library

**4. Features & Functionality**

- Real-time Password Strength Meter - Updates dynamically as users type.

- Password Visibility Toggle - Show/Hide password functionality.

- Generate Secure Password - One-click button for generating strong passwords.

- Dark Mode Toggle - User-friendly theme switcher.

- Live Feedback & Suggestions - Helps improve weak passwords instantly.

- Smooth Animations & Transitions - Enhanced UI experience.

**5. How to Use**

1. Enter a password in the input field.

2. Check the live strength meter to see if it's Weak, Moderate, Strong, or Very Strong.

3. Use the "View" button to toggle password visibility.

4. Follow password guidelines displayed below the input field.

5. Click "Check Strength" to manually validate your password.

6. Click "Generate Strong Password" to get a secure, random password.

7. Switch between Light & Dark Mode using the Dark Mode button.

**6. Potential Impact**

- Enhancing Security - Helps users create stronger passwords, reducing the risk of hacking & brute-force attacks.

- Preventing Weak Passwords - Detects commonly used passwords like "password123", "qwerty", and "abcdef".

- Educating Users - Provides real-time feedback & tips to guide users toward better password practices.

- Accessible & User-Friendly - Simple, lightweight, and easy to use for everyone, from beginners to security-conscious users.

**7. Installation & Deployment**

Prerequisites:

- Python (v3.6+)

- Flask (Python Framework)

- Basic Web Browser (Chrome, Firefox, Edge, etc.)

**Installation Steps:**

**7.1 Clone the Repository:**

git clone https://github.com/your-repo/password-strength-checker.git

cd password-strength-checker

**7.2 Install Flask:**

pip install flask

**7.3 Run the Flask Server:**

python app1.py

**7.4 Open in Browser:**

http://127.0.0.1:5000/

**8. Future Enhancements**

- Integration with 'Have I Been Pwned' API to check leaked passwords.

- Customizable password rules (Users set their own strength criteria).

- Browser extension version for quick password validation.

**9. Conclusion**

This project successfully meets all hackathon requirements by providing a secure, interactive, and

user-friendly password strength checker. With real-time validation, regex-based security checks, and a password generator, this tool

empowers users to create strong passwords and enhance their digital security.