Password Strength Analyzer Using Entropy & Dictionary Checks

Project: ELEVATE LABS – Cybersecurity Intership
Name: Kothamasu Sai Prasad

Introduction

Passwords are the first line of defense in digital security. Weak passwords are highly susceptible to brute-force and dictionary attacks. This project aimed to develop a **web-based Password Strength Analyzer** that evaluates password security in **real-time** and provides actionable suggestions to improve password hygiene.

Abstract

This web application measures password strength using **entropy calculation**, **dictionary-based checks**, and **character diversity**. Users receive instant feedback while typing, and server-side validation ensures accurate scoring and security advice. Weak passwords are flagged, and users are encouraged to create strong, unpredictable passwords or passphrases.

Live Project Link: https://password-strength-analyzer-1jix.onrender.com

Tools Used

- **Python (Flask):** Backend logic and API
- **HTML5 & CSS3:** Frontend structure and styling
- **JavaScript:** Real-time password analysis
- **Gunicorn:** Production WSGI server
- **Dictionary-based password list:** Detect commonly used passwords
- **Windows 10/11:** Development environment

- **Render:** Cloud hosting for public deployment

Project Steps

1. **Setup:** Created Flask backend (app.py) and organized frontend files in templates and static folders. Installed dependencies using requirements.txt.
2. **Backend Implementation:**
   - **Entropy Calculation:** Entropy = Password Length × $\log_2$(Character Set Size)
   - **Strength Scoring:** Converts entropy to a 0–100 score
   - **Dictionary Check:** Flags common passwords as Very Weak
   - **API Endpoint (/api/check)** processes password analysis
3. **Dictionary Attack Detection:** Case-insensitive comparison with a list of common passwords to prevent weak password usage.
4. **Frontend Real-Time Analysis:** JavaScript calculates entropy and updates strength meter, entropy value, password length, and rating instantly.
5. **Server-Side Validation:** Performs full password check, dictionary verification, score calculation, and suggestion generation. Results returned as JSON.

Conclusion

The Password Strength Analyzer demonstrates how cybersecurity principles can be applied to create a **user-friendly, security-focused tool**. Real-time entropy calculation, dictionary checks, and actionable suggestions help users generate strong passwords resistant to attacks.

This project enhanced my understanding of password security fundamentals, entropy-based evaluation, dictionary attack prevention, and secure web application design using Flask.

The application is deployed on **Render**, a cloud hosting platform, and is publicly accessible. Users can test passwords instantly without installing any software. No passwords are stored or logged, ensuring privacy.