Password Strength Analyzer & Custom Wordlist Generator

Introduction

Weak passwords are one of the top causes of breaches. This project evaluates password strength and generates custom wordlists for awareness and testing.

Abstract

The tool has three modules: - **Analyze**: Evaluates a single password (entropy, ZXCVBN score, crack-time). - **Audit**: Processes a file of passwords and exports results in CSV format. - **Wordlist**: Generates custom wordlists from user metadata (case variants, leetspeak, suffixes, separators, years).

Outputs: JSON for individual analysis, CSV for audits, and `.txt` wordlists.

Tools Used

- Python 3.x
- Libraries: `zxcvbn`, `tqdm`

Steps Involved

1. Set up Python environment and install dependencies.
2. Implement analyzer (entropy + ZXCVBN).
3. Implement audit function to check bulk passwords.
4. Build generator for custom wordlists (meta → variants, suffixes, combos).
5. Test with sample inputs and validate results.
6. Document project with README and screenshots.

Conclusion

The project highlights weaknesses in passwords and shows how attackers might build wordlists. This improves user awareness and strengthens defense. It can be extended with a GUI or Flask web app.