Password Strength Analyzer with Custom Wordlist Generator

By Harini Saladi

2025-07-29

Abstract

This project aims to help users analyze the strength of their passwords while also generating custom wordlists based on user inputs. The tool leverages the zxcvbn library to score passwords and provide feedback, while generating related wordlist entries for use in password auditing or ethical testing. It includes a command-line interface and a GUI (optional) with visualizations for user-friendly analysis.

Tools Used

- Python
- zxcvbn (Password strength estimation)
- NLTK (Natural language processing for word mutations)
- argparse (CLI interface)
- tkinter (for optional GUI)
- matplotlib (for optional visualization)

Architecture Overview

The application is structured into the following modules:
1. CLI Interface: Accepts password and user data via command-line.
2. Analyzer Module: Uses zxcvbn to evaluate password strength.
3. Wordlist Generator: Creates custom wordlist based on inputs, with support for smart mutations.
4. Output Handler: Saves analysis and generated wordlist to text files.
5. GUI (tkinter): Optional graphical interface for analysis and visualization.

Sample CLI Output

Command:
python cli/main.py --password "john123" --inputs john 1999 tiger

Output:
Password Score: 1
Guesses: 4753
Feedback: {'warning': 'This is a very common password.', 'suggestions': ['Add another word or two. Uncommon words are better.']}
Wordlist saved with 9 words.

GitHub Repository

https://github.com/HariniSaladi9/passwordanalyzerr

Conclusion

This tool provides a comprehensive and user-customizable way to evaluate password strength and generate contextual wordlists. With optional GUI and graphing support, the tool can be useful for educational, security research, or penetration testing scenarios.