Password Strength Analyzer with Custom Wordlist Generator

Introduction:

In the realm of cybersecurity, weak passwords remain one of the most exploited vulnerabilities. This project aims to tackle this issue by developing a Python-based tool that analyzes password strength and generates custom wordlists for use in penetration testing simulations.

Abstract:

This tool evaluates password strength using the zxcvbn library, which calculates entropy and patterns based on user input. Additionally, it generates a personalized wordlist using inputs such as names, dates, and pet names, incorporating common mutations like leetspeak and numeric suffixes. The tool is designed to be beginner-friendly and educational.

Tools Used:

- Python 3.x
- zxcvbn (for password strength estimation)
- argparse (for CLI interface)
- Custom Python logic for wordlist generation

Password Strength Analyzer with Custom Wordlist Generator

Steps Involved in Building the Project:

1. Installed necessary libraries including zxcvbn using pip.
2. Created a CLI using argparse to accept password inputs and base words for wordlist.
3. Implemented password evaluation logic using zxcvbn.
4. Built the custom wordlist generator using patterns, years, and leetspeak transformations.
5. Added file writing logic to export the wordlist to a .txt file.

Conclusion:

This project has practical value in both personal security awareness and professional cybersecurity training. It demonstrates how even simple tools can be powerful in evaluating and strengthening password policies. This tool also introduces students to concepts like entropy, password cracking, and user-driven data mutation, all within an ethical framework.