Password Strength Analyzer with Custom Wordlist Generator

1. Introduction

The Password Strength Analyzer with Custom Wordlist Generator is a Python-based tool designed to evaluate the strength of user-provided passwords and generate a custom wordlist based on personal information. The project aids in understanding password security and creating effective wordlists for ethical penetration testing.

2. Abstract

This tool consists of two primary functions: analyzing the strength of any given password using the 'zxcvbn' library, and generating a personalized wordlist file by combining user-specific data such as name, date of birth, and pet's name. It is intended for educational and cybersecurity training purposes.

3. Tools Used

- Python 3.x
- zxcvbn
- argparse
- itertools

4. Steps Involved in Building the Project

1. Developed a CLI-based password analyzer using the 'zxcvbn' library.
2. Created a custom wordlist generator that accepts user inputs: Name, Date of Birth, and Pet Name.
3. Generated multiple permutations of these inputs with common suffixes/prefixes.
4. Stored generated password combinations into a text file ('wordlist.txt').
5. Allowed execution of either functionality via command-line arguments.
6. Tested and verified the tool on various password samples and input combinations.

5. Conclusion

The Password Strength Analyzer with Custom Wordlist Generator successfully demonstrates basic password security assessment and the creation of personalized wordlists useful in penetration testing scenarios. It serves as a simple yet effective tool for understanding password robustness and custom wordlist creation.