Project Title: **Password Strength Analyzer & Wordlist Generator.**

Introduction

Passwords remain a primary method of user authentication. Weak passwords are often responsible for security breaches. This project aims to help users understand password security by analyzing strength and simulating how wordlists are created by attackers.

Abstract

The tool provides two core functions: password strength analysis and personalized wordlist generation. It uses the zxcvbn Python library to rate passwords based on entropy and resistance to cracking. It also generates realistic attack wordlists using user information, allowing ethical simulation of password cracking.

Tools Used

- Python 3

- zxcvbn Python library

- Basic file handling

- Regex and string manipulation

Steps Involved

1. Developed `analyzer.py` to evaluate passwords.

2. Used zxcvbn to return crack time, score, and suggestions.

3. Built `wordlist_generator.py` that accepts user inputs (name, DOB, pet).

4. Generated leetspeak, numeric, and year-based variations.

5. Exported combinations to `wordlist.txt`.

Conclusion

The project gave hands-on understanding of password strength, entropy, and how attackers craft custom wordlists using basic information. It also shows how users can improve their password habits and avoid predictable combinations.