

Title: Password Strength Analyzer and Wordlist Generator

Introduction:

Passwords are the first line of defense in security. This project analyzes password strength and generates a custom wordlist for penetration testing or educational purposes.

Abstract:

The tool evaluates passwords using the zxcvbn library and generates a wordlist using user-provided details like names and dates with variations and leetspeak.

Tools Used:

- Python 3
- zxcvbn (for strength analysis)
- Basic terminal utilities

Steps Involved:

1. Accept user-entered password and analyze its complexity using zxcvbn.
2. Accept user inputs like name, birth year, pet, etc.
3. Generate wordlist using combinations and patterns.
4. Save the generated wordlist to a `.txt` file.

Conclusion:

This project demonstrates how attackers might build wordlists using personal data, and highlights the importance of strong, non-predictable passwords.