PROJECT REPORT

Title

Password Strength Analyzer with Custom Wordlist Generator

Introduction

Passwords are the first line of defense in cybersecurity. Weak passwords are vulnerable to dictionary and brute-force attacks. This project focuses on analyzing password strength and educating users about secure password creation by demonstrating how attackers generate password guesses using personal information.

Abstract

This project implements a Password Strength Analyzer using Python and the zxcvbn library. It evaluates passwords based on complexity and predictability. Additionally, a custom wordlist generator is developed to create password combinations using user-provided personal details. The tool helps users understand password security risks and promotes strong password practices.

Tools Used

- Python
- zxcvbn Library
- Command Prompt

Steps Involved in Building the Project

1. Collected password input from the user.

2. Analyzed password strength using zxcvbn scoring.
3. Classified passwords as weak, medium, or strong.
4. Collected user personal details like name, birth year, and pet name.
5. Generated custom password combinations.
6. Saved the generated wordlist into a text file.

Conclusion

The Password Strength Analyzer successfully evaluates password security and demonstrates how predictable passwords can be exploited. This project highlights the importance of strong passwords and helps users understand common password attack techniques used in cybersecurity.