Password Strength Analyzer with Custom Wordlist Generator

Name: Parth Singh
Internship Domain: Cybersecurity
Submission Date: 25 June 2025

---

1. Introduction

This project aims to create a tool that analyzes the strength of a user-provided password and generates a custom wordlist based on personal details. It is designed to demonstrate how predictable patterns in passwords can lead to security vulnerabilities.

---

2. Abstract

The Password Strength Analyzer uses the `zxcvbn` library to evaluate password robustness, estimating how long it might take to crack.
In addition, the project generates a wordlist using user-provided inputs such as name, pet name, and birth year.
This wordlist simulates what an attacker might use in a targeted brute-force or dictionary attack.
The project serves as both a defensive and educational tool in the domain of cybersecurity.

---

3. Tools Used

- Python 3
- `zxcvbn` (for password strength analysis)
- Custom Python scripts (for wordlist generation)
- Text file output (to store the generated wordlist)

---

4. Steps Involved in Building the Project

1. Collected user input for password, name, birth year, and pet name.
2. Used `zxcvbn` to analyze password strength and provide score, crack time, and suggestions.
3. Implemented logic to generate variations of the input data to simulate common password patterns.
4. Saved the generated wordlist to a `.txt` file for inspection.
5. Added clear CLI interface for easy user interaction.

5. Conclusion

This project helps demonstrate how attackers create targeted wordlists using public or personal information.
It also emphasizes the need for strong, unique, and complex passwords.
By analyzing and understanding password weaknesses, users can make informed decisions to enhance their digital security.