Password Strength Analyzer & Custom Wordlist Generator

Shaik Baji Baba

Elevate Labs

25-08-2025

Company Project Report

Introduction

This project focuses on building a password strength analyzer combined with a custom wordlist generator. The tool provides an evaluation of password complexity while also generating tailored wordlists for cybersecurity testing and awareness purposes.

Abstract

The Password Strength Analyzer & Custom Wordlist Generator is designed to help security teams, developers, and end-users assess password quality and understand common weak patterns. The project also demonstrates how attackers might leverage predictable inputs to generate cracking wordlists, allowing companies to adopt stronger password policies.

Tools Used

1. Python 3.8+ 2. Tkinter (GUI development) 3. zxcvbn (password strength analysis) 4. NLTK (linguistic enhancements) 5. Standard Python libraries (os, itertools)

Steps Involved in Building the Project

1. Environment setup with required libraries.
2. Password strength analysis using zxcvbn with entropy fallback.
3. Collection of user input (names, dates, pets, etc.).
4. Generation of common password patterns (leetspeak, years, combinations).
5. Export of final custom wordlist.
6. GUI implementation for user-friendly interaction.
7. Documentation and packaging for company use.

Conclusion

This project delivers a practical tool for both password strength evaluation and wordlist generation. For Elevate Labs, it highlights awareness in password security, enhances internal cybersecurity training, and can be showcased as part of innovative security solutions. Future work can extend this into enterprise-scale password auditing tools.