Advanced Password Tool – Project Report

Abstract

This project developed a desktop application named Advanced Password Tool, allowing users to analyze password strength, generate random secure passwords, and create customizable wordlists for security testing. Developed in Python with Tkinter, the tool incorporates modules such as zxcvbn for pattern-aware scoring, entropy calculations, and breach detection via Have I Been Pwned.

Introduction

Weak or reused passwords remain a leading security issue. The tool addresses this by offering entropy-based metrics, breach detection, and pattern analysis combined with a clean GUI for accessible usage.

Tools Used

Python 3.x, Tkinter, zxcvbn-python (for scoring), secrets and random modules, ReportLab (for PDF reporting), pytest (for testing), PyInstaller (for packaging)

Steps Involved

1. Requirement gathering and modular design 2. Implemented core modules: analyzer (entropy + breach), generator (secure passwords), wordlist builder (transforms with combinatorial limits) 3. Built Tkinter GUI with tabbed interface and theme toggling 4. Added CLI script (cli.py) and used PyInstaller for creating a single-file executable 5. Wrote unit tests to ensure reliability

Conclusion

The Advanced Password Tool delivers functional and secure utility for password strength evaluation, generation, and tailored wordlists. Its GUI and executable packaging enhance accessibility, while future enhancements could include vault features, mnemonic generation, or CLI expansions.