Smart Password Audit Tool – Project Report

1. Introduction

The Smart Password Audit Tool is a cybersecurity-focused desktop application built with Python and Tkinter. Its primary purpose is to help users evaluate password strength, detect vulnerabilities, and suggest improvements using AI-driven insights.

2. Abstract

The project analyzes passwords based on entropy, breach history, pattern detection, and real-time typing behavior. It enhances user security awareness by providing visual feedback, graphical strength representation, and live password suggestions. Additional features include dark mode, password logging, encryption, report export, and email integration.

3. Tools Used

- Python 3.x
- Tkinter (GUI)
- zxcvbn (password strength)
- requests
- matplotlib
- ReportLab
- Cryptography
- smtplib
- PyInstaller

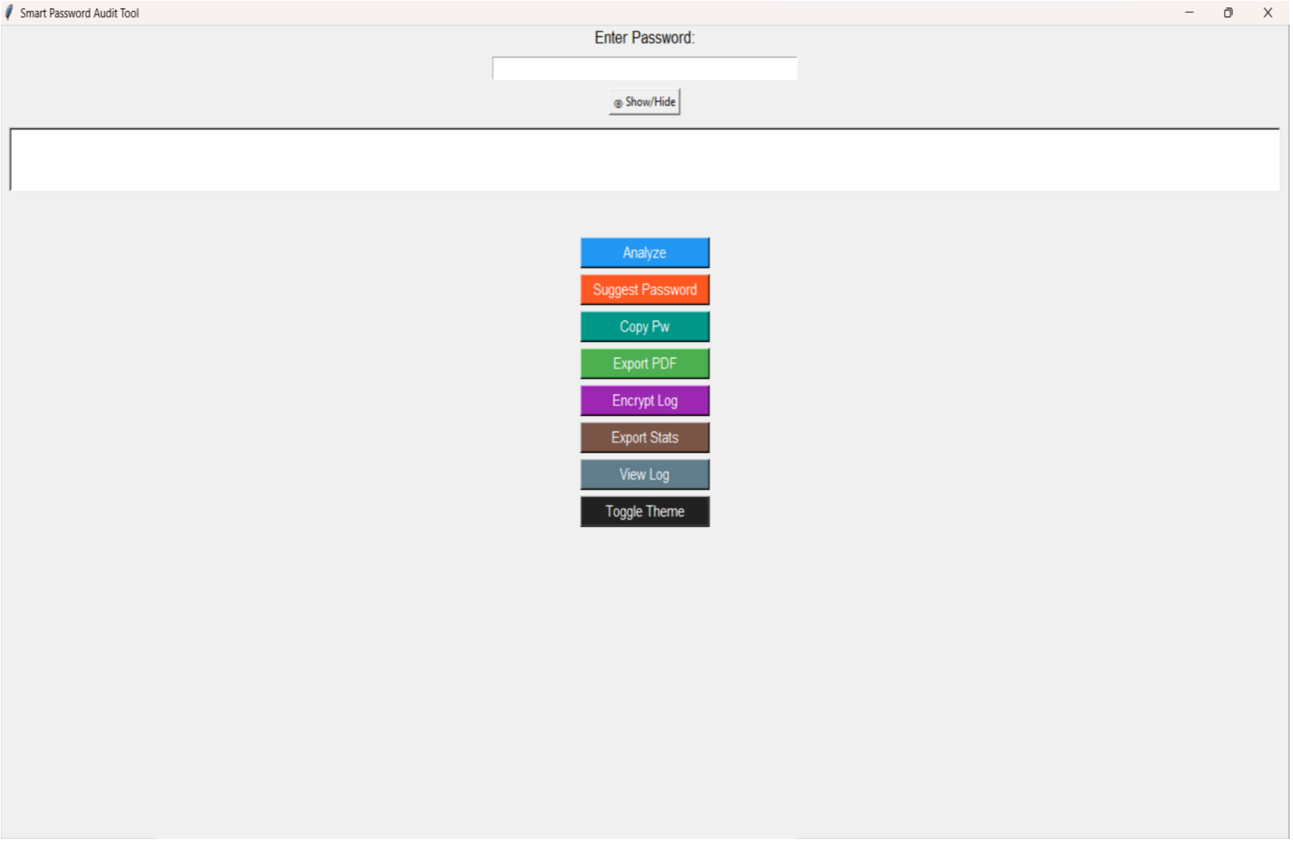
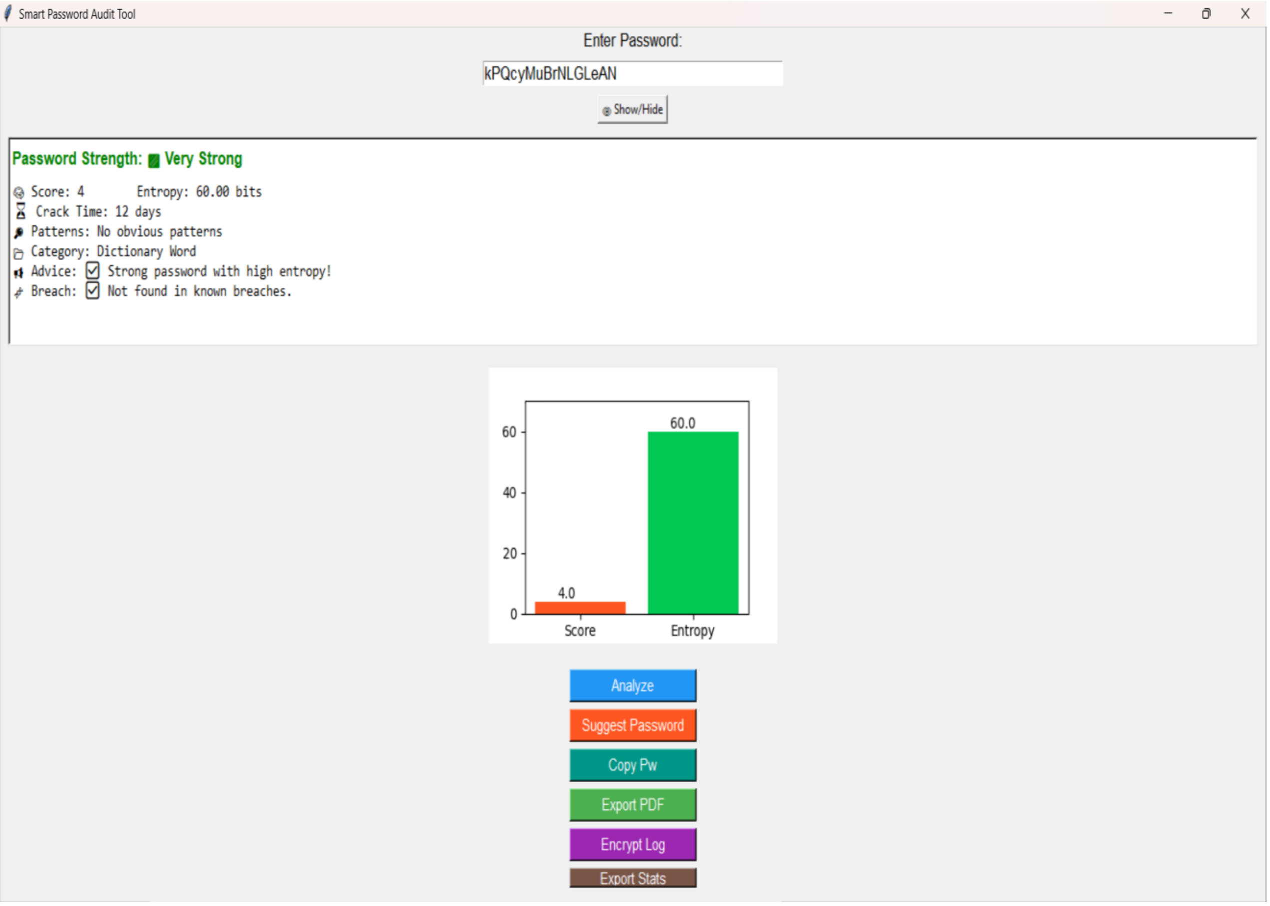


Figure 1: Main Application Interface

4. Steps Involved in Building the Project

- Designed UI with Tkinter for password input, buttons, and dynamic labels.
- Integrated zxcvbn to analyze password strength and crack time.
- Added breach check API (Have I Been Pwned) for leak detection.
- Implemented entropy and pattern analysis.
- Integrated PDF/wordlist export and email alerts.
- Applied dark mode switch and strength-based color feedback.
- Compiled project to .exe using PyInstaller.



Enter Password: kPQcyMuBrNLGLeAN

```
Password Strength: 🟩 Very Strong

Score: 4        Entropy: 60.00 bits
⌛ Crack Time: 12 days
Patterns: No obvious patterns
Category: Dictionary Word
Advice: ☑ Strong password with high entropy!
Breach: ☑ Not found in known breaches.
```

Figure 2: Password Analysis and Breach Check Output

5. Conclusion

This project successfully demonstrates how AI and simple UI elements can empower users to generate and evaluate strong passwords. By combining real-time feedback, graphical representation, and breach awareness, the tool acts as a practical cybersecurity aid. It can be further extended with mobile or web-based integration.