Internship Project Report
Name: Jaslin Varghese
Date: [15/6/25]

---

1. Introduction

In today's digital world, weak passwords are a major vulnerability. This project aims to assess the strength of user passwords and generate a personalized wordlist that could be used for password cracking simulations or strengthening recommendations.

---

2. Abstract

This project implements a password analysis tool using the `zxcvbn` library, which evaluates password strength and provides real-time feedback. Additionally, it generates a custom wordlist from user-related data like names, dates, and pet names, incorporating common patterns and suffixes. This tool can help both users and penetration testers understand password weaknesses and create stronger alternatives.

---

3. Tools Used

- Python 3
- zxcvbn (for password strength evaluation)
- itertools, file I/O (for wordlist logic)
- tkinter (for GUI)
- Command-line interface (CLI)

---

4. Steps Involved in Building the Project

a. Password Strength Analysis:
User inputs a password, which is evaluated using `zxcvbn`. It returns a strength score (0–4) and improvement suggestions.

b. Wordlist Generation Logic:
Users input data (name, birth year, etc.), and the program creates variations:

- Lowercase, UPPERCASE, Capitalized
- Appending `123`, `@123`, years, etc.
- Combining multiple keywords using permutations

c. File Export:
The wordlist is saved in `.txt` format (`custom_wordlist.txt`) for use in cracking tools or training.

---

5. Conclusion

The tool provides practical insight into password weaknesses and simulates common attack patterns through a customizable wordlist. It can be extended to include leetspeak transformations, password rule enforcement, or a GUI for user-friendliness. This project strengthens the understanding of both password creation and attacker logic.