# Password Strength Analyzer with Custom Wordlist Generator

## Introduction

In the modern digital landscape, passwords are the first line of defense against unauthorized access. However, many users continue to use weak or predictable passwords, putting their data at risk. This project aims to provide a practical tool that not only analyzes password strength but also helps generate customized wordlists that could be used in penetration testing or ethical hacking practices.

## Abstract

This project focuses on creating a dual-purpose application:  
1. A Password Strength Analyzer that evaluates the complexity of a given password using entropy and pattern analysis.  
2. A Custom Wordlist Generator that creates a list of possible passwords based on user-provided personal data (e.g., name, birth year, pet name) and common password patterns.  
  
The tool helps users assess password quality while demonstrating how easily guessable passwords can be derived from personal data. It features both a command-line and GUI interface, making it accessible to beginners and useful for cybersecurity learners.

## Tools Used

- Python: Core programming language  
- Tkinter: GUI development  
- zxcvbn: Password strength estimation  
- NLTK: Optional, for word processing  
- argparse: Command-line interface  
- PowerShell / Terminal: Running and testing the script

## Steps Involved in Building the Project

1. Setup Environment:  
 - Install Python and necessary libraries using pip  
2. Design GUI:  
 - Built using tkinter to allow users to enter password and personal data  
3. Implement Password Strength Analysis:  
 - Used zxcvbn to analyze entropy, crack time, and feedback  
4. Generate Wordlist:  
 - Created variations using personal data and saved them in a .txt file  
5. Testing:  
 - Verified outputs using PowerShell or terminal

## Conclusion

The Password Strength Analyzer with Custom Wordlist Generator provides users with a deeper understanding of password security. It shows how personal data can be exploited to generate possible passwords, thereby encouraging stronger password practices. The project demonstrates both defensive and offensive aspects of cybersecurity, making it a valuable learning tool for students and ethical hackers.