Project Report – Password Strength Analyzer & Custom Wordlist Generator

This project provides a complete tool for analyzing password strength and generating custom attack-focused wordlists using user-supplied personal information. The system is designed for cybersecurity education, password analysis research, and ethical penetration testing.

1. Project Objective

Build a tool capable of evaluating password strength using the zxcvbn library and generating highly targeted custom wordlists based on user metadata.

2. Tools & Technologies Used

- Python
- zxcvbn
- argparse
- tkinter (GUI)
- itertools
- NLP-inspired pattern generation

3. System Features

1. Password Strength Analyzer:
- Entropy calculation
- Crack time estimation
- Feedback and warnings
- Strength score 0–4

2. Custom Wordlist Generator:
- Leetspeak variations
- Capitalization variants
- Common appended patterns like 123, 2024, @, !
- Multi-word combinations
- Export to .txt

3. GUI Support:
- Tkinter interface for non-CLI users

4. Architecture Overview

The application works in 3 main modules:
- Analyzer Module
- Wordlist Generator Module
- CLI/GUI Interface Module

5. Ethical Use Notice

This tool must only be used on systems where you have explicit permission. Unauthorized password cracking is illegal and punishable by law.

6. Conclusion

The Password Strength Analyzer & Custom Wordlist Generator is a practical cybersecurity learning tool with real-world applications in password auditing and secure software development.