Password Strength Analyzer - Project Report

Introduction

The Password Strength Analyzer is a web-based tool that helps users evaluate the strength of their passwords in real-time. It visually displays password strength, provides feedback, and generates custom wordlists for security testing and awareness.

Abstract

The application uses the ZXCVBN library to evaluate passwords based on common patterns, dictionary words, and brute-force complexity. It features a stylish UI with real-time strength updates, estimated cracking time, and suggestions to improve password security. Users can also generate and download custom wordlists based on personal information inputs like name, date of birth, and pet name.

Tools Used

- HTML, CSS, JavaScript
- Tailwind CSS for responsive design
- ZXCVBN library for password strength analysis
- FPDF (for this report generation)

Steps Involved in Building the Project

1. Set up the HTML structure for input fields and output feedback.
2. Applied Tailwind CSS and custom styles for a modern UI.
3. Integrated ZXCVBN.js to analyze password strength.
4. Displayed results dynamically including a strength bar, feedback, and estimated crack time.
5. Implemented a toggle to show/hide password input.
6. Added wordlist generation logic based on user input and leetspeak transformations.
7. Enabled wordlist download as a text file.
8. Final polish with Google Fonts and background gradients.

Conclusion

This project provided a practical understanding of front-end development and real-world password analysis. It reinforces the importance of strong password practices and highlights how even personal information can influence security risks. Future improvements could include database integration and more advanced cracking simulations.