Project Report: Password Strength Analyzer and Custom Wordlist Generator

Abstract

Passwords are a critical component of cyber security and act as the first line of defense in protecting digital systems. However, weak and predictable passwords are still widely used by users, making systems vulnerable to cyber-attacks. This project focuses on analyzing password strength and generating custom wordlists using user-provided information. The password strength analyzer evaluates passwords based on entropy and common patterns, while the wordlist generator demonstrates how attackers create password lists using personal data. The main objective of this project is to spread awareness about password security and promote the use of strong passwords.

Introduction

In today's digital world, password-based authentication is used in almost every application, including social media, banking systems, and enterprise networks. Despite advancements in security technologies, weak passwords remain one of the major causes of security breaches. Attackers exploit weak passwords using dictionary attacks and brute-force techniques. This project demonstrates how password strength can be evaluated and how easily passwords can be predicted when users rely on personal information. The project helps users understand cyber security risks related to password misuse.

Tools Used

The following tools and technologies were used in this project:

- Python Programming Language
- zxcvbn Password Strength Estimation Library
- Basic File Handling Techniques

Steps Involved in Building the Project

1. The user enters a password to be analyzed.
2. The password strength analyzer evaluates the password using the zxcvbn library.

3. The system displays the password strength score and estimated crack time.
4. The user provides personal details such as name, birth year, and pet name.
5. A custom wordlist is generated using common patterns and combinations.
6. The generated wordlist is saved in a text file for demonstration purposes.

Conclusion

This project successfully demonstrates the importance of strong passwords in cyber security. By analyzing password strength and generating custom wordlists, users can clearly understand how attackers exploit weak and predictable passwords. The project emphasizes the need for strong password policies and secure authentication practices. It also provides practical insight into password security concepts and helps in building awareness among users.