Entropheus – Advanced Password Strength Analyzer with Wordlist Generator

Introduction :

Passwords remain the primary method of authentication in most systems, yet weak or reused passwords are a top security risk. This project focuses on analysing password strength using both entropy and industry-standard scoring systems, while also generating custom wordlists for use in penetration testing or password audits.

Entropheus is a command-line tool designed to help security testers, analysts, and learners evaluate password robustness and prepare targeted wordlists using personal context. The project combines real-time feedback, scoring, and mutation logic in a lightweight, accessible tool.

Abstract :

Entropheus enables users to:

- Check passwords against an advanced analyser that uses both zxcvbn and entropy calculations
- Receive meaningful feedback about common weaknesses
- Generate highly personalized wordlists based on user inputs (name, DOB, pet, etc.)
- Export wordlists compatible with tools like Hydra, Hashcat, or JohnTheRipper

The tool features a terminal interface inspired by community tools like Zphisher, delivering a professional experience for cybersecurity learners and practitioners.

Tools & Technologies Used :

Tool	Purpose
Python 3.13.5	Core programming language
zxcvbn-python	Password scoring algorithm
math, itertools	Entropy, mutation logic
rich	CLI interface styling
OS & File I/O	Logging and exporting data

Steps Involved in Building the Project :

1. **CLI Interface Development:**
   Designed using the rich Python library to mimic toolkits like Zphisher.
2. **Password Analysis Engine:**
   - Integrated zxcvbn for scoring and feedback.
   - Implemented custom entropy calculations to measure bit strength.
3. **Pattern Feedback Engine:**
   - Detected commonly used sequences like 1234, qwerty, and missing symbols.
4. **Wordlist Generator:**
   - Collected personal inputs like name, pet, and DOB.
   - Applied leetspeak and custom pattern mutation rules.
   - Generated a .txt wordlist with up to 5000 entries.
5. **Logging & Output:**
   - Password strength results are logged in results/session_log.txt.
   - Wordlists are saved in wordlists/generated.txt.

Conclusion :

The Entropheus project successfully demonstrates how password evaluation and wordlist generation can be automated using Python. It highlights the importance of both user behaviour analysis and technical scoring in modern security practices.

The tool is modular, scalable, and can be extended into web dashboards or integrated into red team/blue team pipelines. This project enhanced understanding of password security, entropy models, mutation logic, and ethical hacking methodology.