This project aims to design a Python-based tool that evaluates password strength and creates custom wordlists for cybersecurity testing. The tool helps identify weak passwords by calculating entropy and analyzing patterns. It also generates personalized wordlists using user-specific details such as names, pets, and dates. This approach helps demonstrate how attackers may exploit personal information in password guessing, while also promoting awareness about secure password creation.

**Tools Used**

1. **Programming Language:** Python 3
2. **Libraries/Modules:**
   * *re* – Regular expression handling for pattern checks
   * *math* – Used for entropy and logarithmic calculations
   * *argparse* – For command-line input arguments
   * *datetime* – To handle dates and extract year patterns
3. **Development Environment:** Visual Studio Code (VS Code)

**Steps Involved in Building the Project**

1. **Password Strength Analysis:**  
   Implemented entropy-based logic to evaluate how complex a password is based on length and character diversity. The strength was categorized into levels from *Very Weak* to *Very Strong*.
2. **Custom Wordlist Generation:**  
   The tool collects user details (like names, pets, years) and automatically creates a list of possible password variations, including leetspeak, capitalization, reversed text, and appended years.
3. **Integration of Functions:**  
   Both password analysis and wordlist creation were combined into one tool for efficiency and better usability.
4. **Export Feature:**  
   The generated wordlist is exported as a .txt file, compatible with password testing tools for ethical hacking practice.
5. **Testing:**  
   Multiple passwords and input combinations were tested to verify accuracy, functionality, and usability.

**Conclusion**

The project successfully demonstrates how password strength can be assessed and how custom wordlists can be generated for ethical password testing. It reinforces the concept of password complexity and the risks of using predictable personal data. The tool serves as an educational resource for cybersecurity students to understand password analysis and the importance of creating strong, unique passwords.