

Strong Password Detection

Ngoan Vo

Professor Lewis Heuermann

CYB333 – Security Automation

Project Goal

This Strong Password Detection project aims to enhance security measures by developing a tool capable of analyzing and identifying weak passwords. This tool aids individuals and organizations in strengthening their digital defenses against potential security breaches resulting from password vulnerabilities.

The link to my GitHub repository: <https://github.com/Ngoan-Vo/Strong-Password-Detection>

The Problem I Am Solving

Weak passwords pose a significant risk to cybersecurity as they are susceptible to various forms of attacks such as brute-force attacks and dictionary attacks. These attacks can compromise sensitive data leading to financial losses, reputational damage, and privacy breaches. By creating the tool that can detect weak passwords, I aim to mitigate these risks and promote better password among users.

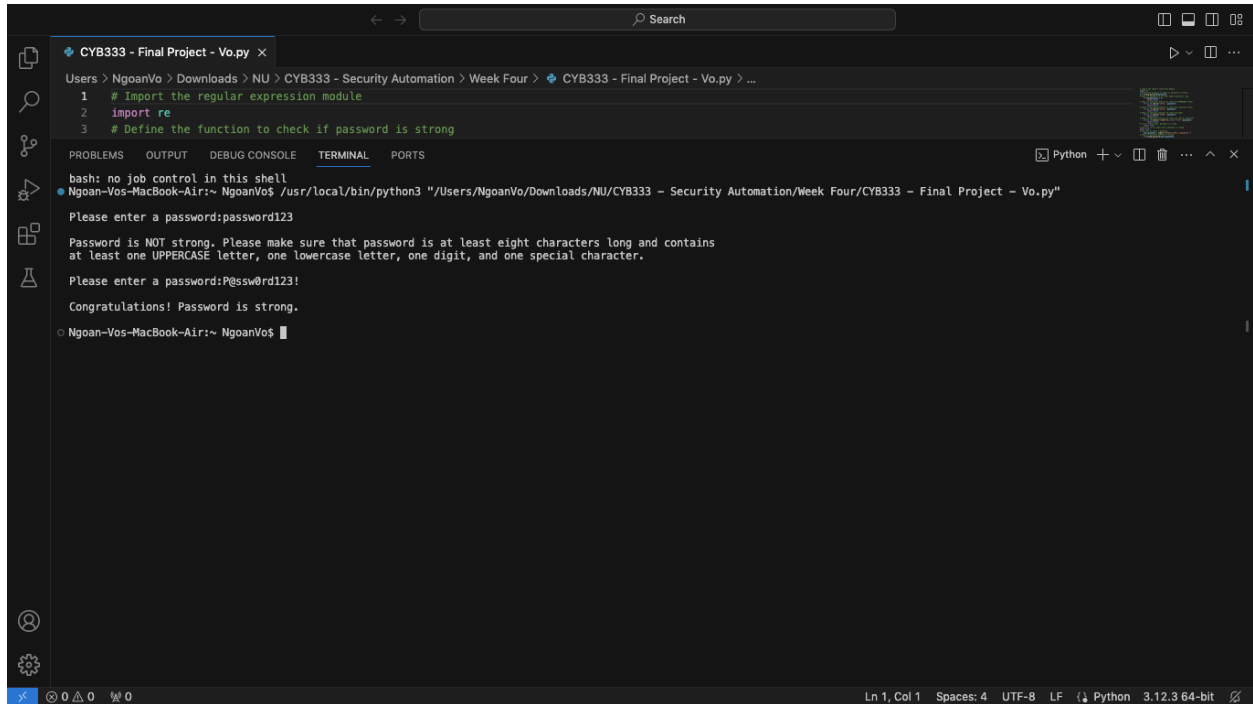
Expected Outcomes

The expected outcome of this project is the development of a robust and user-friendly tool capable of analyzing passwords for strength and identifying potential vulnerabilities. The tool highlights areas where passwords can be improved to enhance security.

The Tool and Demonstration

The Strong Password Detection tool is designed to analyze the strength of passwords. Upon inputting a password, the tool utilizes sophisticated algorithms to assess its complexity and length. It then generates recommendations for improving password security. For demonstration purposes, let's consider a scenario where a user enters the password "P@ssw0rd123!" The tool

promptly evaluates this password and provides feedback indicating its strength as strong due to its combination of length, uppercase letters, lowercase letters, numbers, and special characters.



The screenshot shows a Visual Studio Code editor window with a file named 'CYB333 - Final Project - Vo.py'. The code in the editor is as follows:

```
1 # Import the regular expression module
2 import re
3 # Define the function to check if password is strong
```

The terminal output shows the execution of the script. It starts with a shell prompt, followed by the command to run the script. The script prompts the user to enter a password. The user enters 'password123', and the script outputs: 'Password is NOT strong. Please make sure that password is at least eight characters long and contains at least one UPPERCASE letter, one lowercase letter, one digit, and one special character.' The user then enters 'P@ssw0rd123!', and the script outputs: 'Congratulations! Password is strong.'

References

Severance, C. R., Blumenberg, S., & Hauser, E. (2016). *Python for Everybody: Exploring Data in Python 3: CreateSpace Independent Publishing Platform*

Seitz, J. (2015). Black hat Python: Python programming for hackers and pentesters

ITProTV. (n.d.). <https://app.acilearning.com/course/version-control/github-repository>