Developing a Password Strength Checking Tool

Cade Garcia, c.garcia21@icloud.com, Chaminade University, Data Science Analytics and Visualization

Introduction

Cyber attacks are a growing threat trying to gain access to valuable data. Many common hacking techniques involves cracking weak passwords. Your data is important and your password is your first line of defense to keep it secure. In this project, I researched password entropy to create an application that evaluates password strength in order to improve your security.

Methods and Programs

Password entropy is the strength of a password, measured by how unpredictable it is. The greater the entropy, the more effective the password is against all types of attacks.

Entropy is calculated by:

Eq.

$$E = log2\ (R^L)$$

- E = password entropy, measured in bits.
- R = the range of characters.
- L = the number of characters in a password.

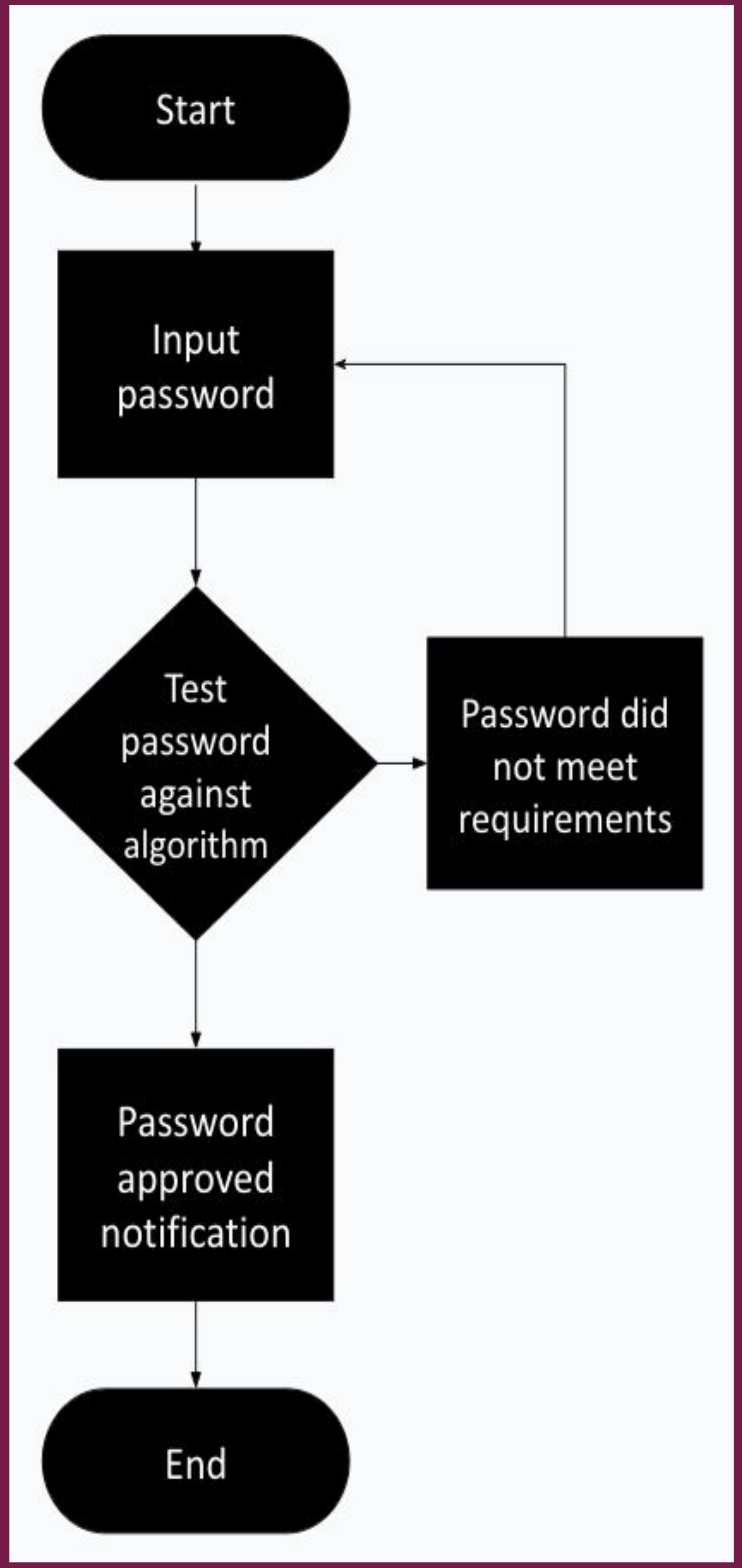
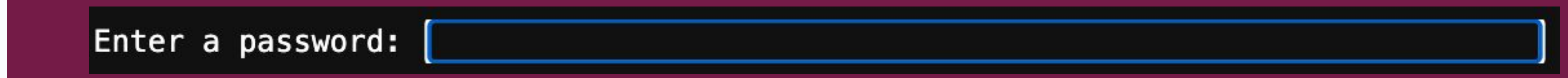
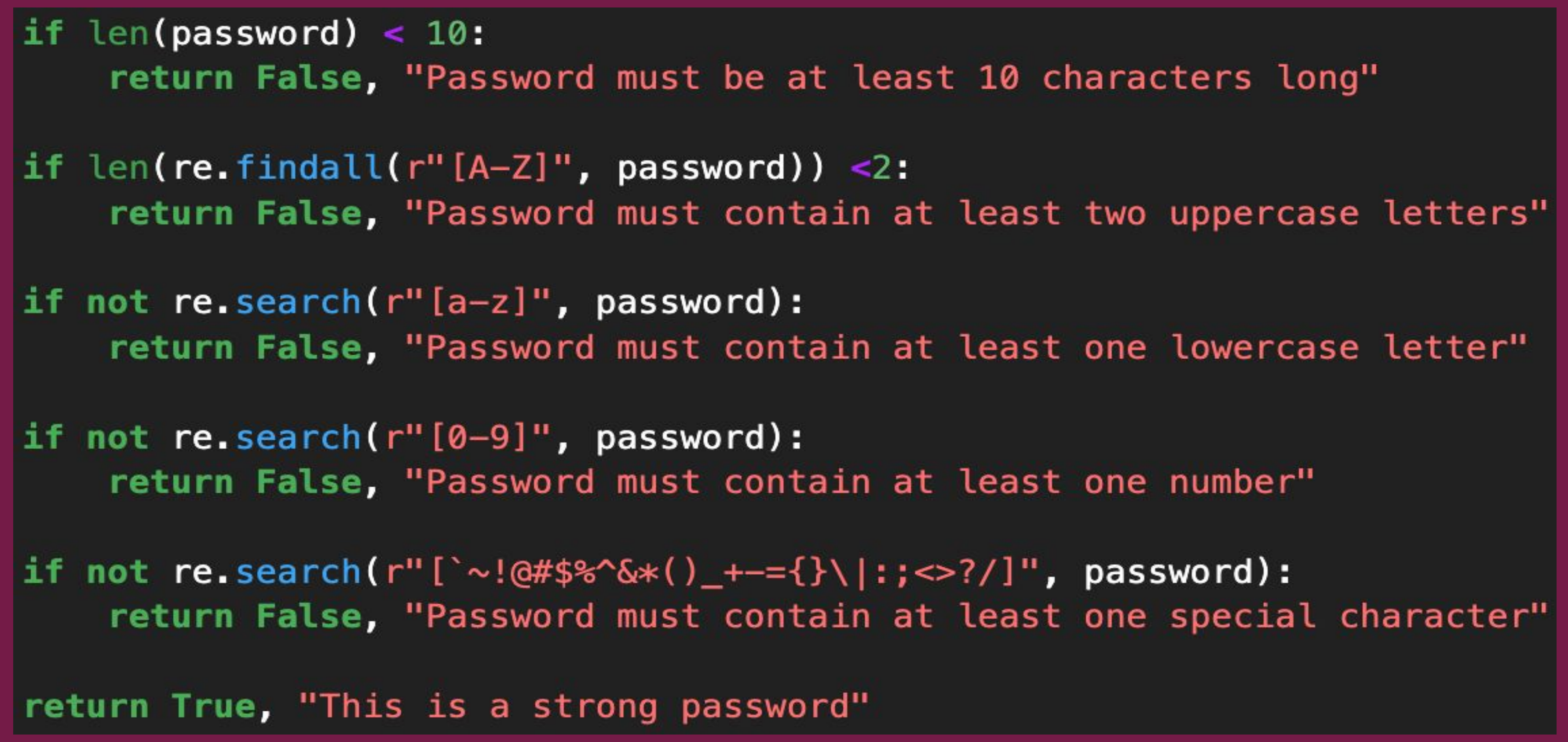

Start
Input password
Test password against algorithm
Password did not meet requirements
Password approved notification
End

Figure 1 Application design

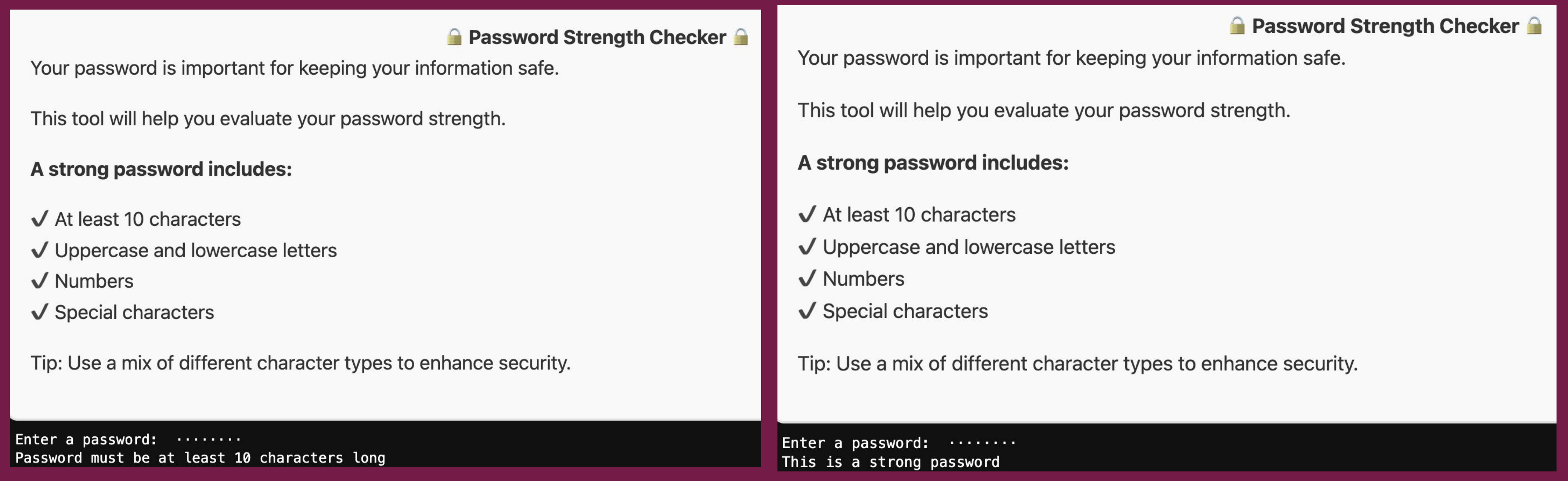
Inputs algorithm and outputs



```
Enter a password:
```



```
if len(password) < 10:
    return False, "Password must be at least 10 characters long"

if len(re.findall(r"[A-Z]", password)) <2:
    return False, "Password must contain at least two uppercase letters"

if not re.search(r"[a-z]", password):
    return False, "Password must contain at least one lowercase letter"

if not re.search(r"[0-9]", password):
    return False, "Password must contain at least one number"

if not re.search(r"[`~!@#$%^&*()_+-={}\|:;<>?/]", password):
    return False, "Password must contain at least one special character"

return True, "This is a strong password"
```



🔒 **Password Strength Checker** 🔒

Your password is important for keeping your information safe.

This tool will help you evaluate your password strength.

A strong password includes:

✓ At least 10 characters
✓ Uppercase and lowercase letters
✓ Numbers
✓ Special characters

Tip: Use a mix of different character types to enhance security.

```
Enter a password:  ········
Password must be at least 10 characters long
```

🔒 **Password Strength Checker** 🔒

Your password is important for keeping your information safe.

This tool will help you evaluate your password strength.

A strong password includes:

✓ At least 10 characters
✓ Uppercase and lowercase letters
✓ Numbers
✓ Special characters

Tip: Use a mix of different character types to enhance security.

```
Enter a password:  ········
This is a strong password
```

Figure 2 Application outputs

Methods

- Built with Python & Jupyter Notebook
- Uses OS & Pandas packages for data handling
- Checks password strength using entropy (60+ bits = strong)

Resources Used

https://www.researchgate.net/profile/Keng-Siau-2/publication/327571329_Cybersecurity_Personal_Information_and_Password_Setup/links/5b9734644585153a53264273/Cybersecurity-Personal-Information-and-Password-Setup.pdf
https://www.researchgate.net/profile/Andras-Keszthelyi/publication/293518235_About_Passwords/links/56c75bf208ae5488f0d2ce5a/About-Passwords.pdf
https://www.sciencedirect.com/science/article/abs/pii/S0167404816300657
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6234434

Discussion and Future works

To mitigate common cyber risks, the code checks user-input against public datasets of frequently compromised passwords. Then, the code iterates for each condition– if the input does not meet the requirement, the user is prompted to fix their password and try again. When all the requirements are met, they will have created a strong password. In entropy terms, 10 characters long with 87 different possible characters will calculate to 64.43 bits which is considered a strong password. The next steps for this project would be to prevent other common password mistakes that compromise security such as reusing passwords

Acknowledgements

I want to thank the Data Science program and Dr. Rylan Chong for supporting this project. This work was partially supported by the grant numbers HRD-2217242 (INCLUDES Alliance ALL SPICE) and PEARL DUE-2030654 (S-STEM). The content is solely the responsibility of the authors and does not necessarily represent the official views of NSF.