Password Complexity Checker

Overview

The Password Complexity Checker is a Python-based tool designed to evaluate the strength of passwords. It provides feedback on password strength and highlights areas for improvement based on predefined criteria.

Features

- Checks if a password meets the following complexity requirements:
  - Minimum length of 8 characters
  - Contains at least one digit
  - Contains at least one uppercase letter
  - Contains at least one lowercase letter
  - Contains at least one special character (e.g., `!@#$%^&*(),.?\":{}|<>`)
- Categorizes passwords as **Strong**, **Moderate**, or **Weak** based on the number of criteria met.
- Provides detailed feedback for passwords that do not meet all requirements.

Requirements

- Python 3.6 or higher

Usage

1. Run the program:
   ```
   python password_complexity_checker.py
   ```
2. Enter a password when prompted, and the tool will evaluate its strength and provide feedback.
3. To exit the tool, type `exit` when prompted for a password.

Example

Input:

```
Enter a password to check (or type 'exit' to quit): P@ssw0rd
```

Output:

```
Password strength: Strong
```

Input:

```
Enter a password to check (or type 'exit' to quit): pass123
```

Output:

```
Password strength: Weak
Issues:
- Password must contain at least one uppercase letter.
- Password must contain at least one special character (!@#$%^&*(),.?\":{}|<>).
```

License

This project is licensed under the MIT License. See the LICENSE file for details.

Acknowledgments

- Python's `re` module for regular expressions.