Bauhaus-Universität Weimar

Random Password Generator

Project Handover Document

Software Engineering
Summer Semester 2024

Group M
Aditya Kumar Gupta (125904)
Ogunleye Olubunmi Emmanuel (126829)
Ajay Patil (126655)

1. Introduction

This document provides a comprehensive handover of the project "Personalized Random Password Generator." The purpose is to analyze the requirements for ambiguity, incompleteness and imprecision, document resolutions from the handover meeting. And also to provide a brief overview of the implemented features.

2. Requirements Analysis

2.1. Ambiguity Check

- Requirement 1: Generate a password with user-specified length.
    - Issue: Ambiguity in how the length impacts the complexity.
    - Resolution: Clarified that the length should directly correlate with the overall strength of the password by incorporating a mix of character types.
- Requirement 2: Include options for lowercase, uppercase, numbers and special characters.
    - Issue: Ambiguity in what specific special characters are allowed.
    - Resolution: Provided a predefined list of allowable special characters (e.g., !, @, #, $, %, etc.).

2.2. Incompleteness Check

- Requirement 3: Copy to clipboard functionality.
    - Issue: Incomplete description of user interaction.
    - Resolution: Detailed the process: After generating the password, a 'Copy to Clipboard' button appears, which when clicked, copies the password.
- Requirement 4: Password strength measurement.
    - Issue: Incomplete criteria for assessing strength.

- Resolution: Defined the criteria: strength based on length, variety of characters, and entropy, displayed via a label such as "Weak", "Moderate" and "Strong".

2.3. Imprecision Check

- Requirement 5: Provide visual feedback for password strength.
    - Issue: Imprecision in how feedback is visually represented.
    - Resolution: Decided on a textual feedback with color coding, red for weak, yellow for moderate, green for strong.

3. Confirmation of No Issues

- Requirement 6: User-friendly interface for password generation.
    - No Issues: The interface design was clear and no ambiguities or imprecisions were identified. The design was straightforward, providing a simple form for input and a clear output area for the generated password.
- Requirement 7: Secure password generation.
    - No Issues: The requirement was clear and detailed, specifying the use of secure algorithms and random seed generation to ensure password unpredictability.

4. Implemented Features Overview

- Customizable Password Options: Users can customize the password length and choose to include lowercase letters, uppercase letters, numbers, and special characters.
- Random Password Generation: Utilizes a robust algorithm to generate secure passwords based on user preferences.

- Password Strength Measurement: Provides real-time feedback on the strength of the generated password using a descriptive label.
- Copy to Clipboard: Users can easily copy the generated password for use in other applications.
- Visualizations: Visual representations of the password's character composition to help users understand its complexity.

5. Summary of Handover Meeting

During the handover meeting, the following key points were discussed and decisions made:

- Clarified ambiguous requirements regarding character types and password length impact.
- Completed the description of the copy-to-clipboard functionality and password strength assessment criteria.
- Agreed on the visual feedback method for password strength.
- No major issues were found in the user-friendly interface and secure password generation requirements.

6. Contact Information

- Aditya Kumar Gupta
    - Email: aditya.kumar.gupta@uni-weimar.de
- Ogunleye Olubunmi Emmanuel
    - Email: olubunmi.emmanuel.ogunleye@uni-weimar.de
- Ajay Satish Patil
    - Email: ajay.satish.patil@uni-weimar.de