Group Name: Future Engineers
Team Members: Eesha Asad, Totti Nguyen, Ena Salazar, Alan Gonzalez

Test Cases

Test Case 1: Verify Customizable Password Length

Test Case Description: Ensure the system generates a password of the user-specified length.

Pre-conditions: User is on the password generator interface.

Test Steps:

1. Navigate to the password generator interface.
2. Use the slider or input field to specify a desired password length (e.g., 12 characters).
3. Click the "Generate Password" button.

Expected Result: The system generates and displays a password exactly 12 characters long.

Actual Result:

Post-conditions: A password of the specified length is generated and displayed.

Pass/Fail Criteria: Pass if the generated password is 12 characters long; fail otherwise.

Test Case 2: Verify Selectable Character Types

Test Case Description: Ensure the system generates a password including the user-selected character types.

Pre-Conditions: User is on the Password Generator Interface

Test Steps:

1. Navigate to the password generator interface
2. Select desired character types (e.g., uppercase, numbers, and symbols).
3. Click the “Generate Password” button
4. Verify that the password does not contain any unselected character types.

Expected Result: The system generates and displays a password containing the selected character types

Actual Result:

Post-Condition: A password containing the selected character types is generated and displayed.

Pass/Fail Criteria: Pass if the password includes the selected character types; fail otherwise

Group Name: Future Engineers
Team Members: Eesha Asad, Totti Nguyen, Ena Salazar, Alan Gonzalez

Test Case 3: Password Strength Indicator

Test Case Description: Ensure the password strength indicator adjusts according to the complexity of the generated password

Pre-conditions: User is on the password generator interface.

Test Steps:

1. Navigate to the password generator interface
2. Specify password generation criteria (e.g., length, character types).
3. Observe the password strength indicator as the password is generated

Expected Result: The strength indicator accurately reflects the complexity of the password (e.g., weak, medium, strong).

Post-conditions: The strength indicator reflects the complexity of the generated password.

Pass/Fail Criteria: Pass if the indicator's feedback matches the password complexity; fail otherwise.

Test Case 4: Copy to Clipboard Functionality

Test Case Description: Verify that users can successfully copy the generated password to their clipboard.

Pre-conditions: A password has been generated.

Test Steps:

1. Generate a new password using the application.
2. Click the "Copy to Clipboard" button/icon
3. Paste the contents of the clipboard into a text editor.

Expected Result: The pasted content matches the generated password.

Actual Result:

Post-conditions: The generated password is copied to the clipboard.

Pass/Fail Criteria: Pass if the pasted content is identical to the generated password; fail otherwise.

Group Name: Future Engineers
Team Members: Eesha Asad, Totti Nguyen, Ena Salazar, Alan Gonzalez

Test Case 5: Regenerate Password

Test Case Description: Ensure users can regenerate a password without restrictions.

Pre-conditions: An initial password has been generated.

Test Steps:

1. Generate an initial password.
2. Re-click the “Generate Password” button.
3. Compare the newly generated password with the initial one.

Expected Result: The new password is different from the initial password and meets the specified criteria.

Post-conditions: A new password is generated and is different from the initial one.

Pass/Fail Criteria: Pass if the new password is different and complies with the set criteria; fail otherwise.

Test Case 6: Cross-Browser Compatibility

Test Case Description: Verify the password generator works consistently across different web browsers.

Pre-conditions: Password generator is accessible in multiple web browsers.

Test Steps:

1. Open the password generator in multiple web browsers (e.g. Chrome, Firefox, Safari).
2. Generate a password in each browser with the same criteria.
3. Observe the functionality and layout.

Expected Result: The application functions correctly and appears consistent across browsers.

Actual Result:

Post-conditions: The application functions correctly and appears consistent across browsers.

Pass/Fail Criteria: Pass if functionality and appearance are consistent; fail otherwise.

Group Name: Future Engineers
Team Members: Eesha Asad, Totti Nguyen, Ena Salazar, Alan Gonzalez

Test Case 7: Mobile Responsiveness

Test Case Description: Ensure the password generator interface is responsive and functional on mobile devices.

Pre-conditions: Password generator is accessed on a mobile device.

Test Steps:

1. Open the password generator on a mobile device.
2. Generate a password with specified criteria
3. Navigate through each different feature and option

Expected result: The interface adjusts to the screen size, and all features are accessible and functional

Actual Result:

Post-conditions: The interface is responsive and functional on the mobile device.

Pass/Fail Criteria: Pass if the interface is responsive and features work as expected; fail otherwise

Test Case 8: Security of Generated Passwords

Test Case Description: Test the security of the generated passwords using strong cryptographic algorithms.

Pre-conditions: A set of passwords has been generated.

Test Steps:

1. Generate a set of passwords with the application.
2. Analyze the generated passwords for patterns or weaknesses with tools like ent (a command-line utility), regular expressions algorithms, or libraries like zcxvbn to assess the strength of the generated passwords.

Expected Result: Passwords show no discernible patterns and meet high security standards.

Post-conditions: The generated passwords are analyzed and deemed secure without detectable patterns or weaknesses.

Pass/Fail Criteria: Pass if passwords are secure and random; fail if any patterns or predictability are detected.