**Positive Tests:**

1. Verify that the user can successfully log in with valid credentials.
2. Check that the password visibility toggle works correctly, allowing the user to see the password when clicked.
3. Ensure that the "Forgot your password?" button is functional and redirects to the password reset form.
4. Validate that the success message appears when the user successfully resets their password.
5. Confirm that the login form displays appropriate placeholder text for the username and password fields.
6. Test that the error message is displayed when incorrect login credentials are entered.

**Negative Tests:**

1. Attempt to log in with an incorrect username and/or password and verify that an error message is displayed.
2. Check the behavior when the username or password fields are left empty and the user tries to submit the form.
3. Test the login process with a username that exceeds the character limit (if applicable) and ensure that it fails gracefully.
4. Verify that the password reset form does not submit if the email field is left empty.
5. Attempt to access the application without proper authorization and confirm that the user is redirected to the login page.

**Creative Test Scenarios:**

1. Simulate a scenario where the user enters valid credentials but the server is down, and check how the application handles the error.
2. Test the application’s response when a user tries to log in multiple times in quick succession with incorrect credentials, ensuring that it does not lock the account unexpectedly.
3. Verify the behavior of the application when a user switches from the login form to the password reset form and back, ensuring that the state is preserved correctly.
4. Check how the application behaves when a user tries to log in from different devices simultaneously with the same credentials.
5. Test the application’s accessibility features by navigating the login and password reset forms using only keyboard shortcuts.