

Test Scenarios For Login Page

1. Leave both the email and password fields blank, click "Login". An error message indicating both fields are required.
2. Enter valid email and password click "Login" to verify the user is successfully logged in.
3. Enter invalid email and password to verify the results.
4. Enter valid email and invalid passwords to verify the results.
5. Enter invalid email and valid passwords to verify the results.
6. Enter an unregistered email, valid password, click "Login”. An error message indicating the email is not found.
7. Enter blank email and valid passwords to verify the results.
8. Verify that the input fields should not accept valid email and a blank password.
9. Leave the email field blank, enter a valid password, click "Login". An error message should indicate the email field is required.
10. Enter a valid email, leave the password field blank, click "Login". An error message should indicate the password field is required.
11. Enter the maximum number of characters allowed for the email, valid password, click "Login." Verify the result a message indicating that the email is too long.
12. Enter valid email, and the maximum number of characters allowed for the password, click "Login". Verify the result of a message indicating the password is too long.
13. Verify that the Login button should successfully Login users after valid credentials.
14. Enter invalid email format (e.g., "userexample.com"), enter valid password, click "Login". Verify an error message indicates “invalid email format”.
15. Enter the same email in different cases (e.g., User@Example.com vs. user@example.com), valid password, click "Login". The system should treat them as identical (email is case-insensitive).
16. Verify that the show password when clicked the actual password should be visible to the users.
17. Enter a password and check the "Show Password" checkbox. Verify that the password is displayed in plain text.
18. Enter a password, check and uncheck the "Show Password" checkbox. Verify that the password should toggle between plain text and hidden format.
19. Verify that the Login button should login successfully on clicking one time.
20. Verify that the input field's password should contain one Uppercase letter, one special character and six characters long .
21. Verify that the input fields should show the error with the red border of the Login button.
22. Verify that the input fields should show the error at the bottom of the Login button.
23. Enter valid email, use the same password with different cases (e.g., Password123 vs. password123), click "Login." Verify that Passwords should be treated as case-sensitive.
24. Leave email and password fields blank. Verify the "Login" button should be disabled until both fields are filled.
25. Attempt to log in with incorrect credentials multiple times (e.g., 5 times). After a certain number of failed attempts, the account should be locked or CAPTCHA should appear.
26. Enter various weak passwords (e.g., "12345," "password") in the password field. Verify that System should indicate that the password is weak.
27. Log in successfully, leave the session idle for a set period. Verify that the session should time out after a period of inactivity.
28. Copy and paste the password from another document into the password field. Verify that the password should be accepted, and login should proceed.
29. Log in successfully, then click the browser back button. Users should remain logged in and not be taken to the login screen again.
30. Turn off the internet connection, enter valid credentials, click "Login." Verify that an appropriate error message should appear indicating no internet connection.
31. Enter valid credentials and press the "Enter" key instead of clicking the "Login" button. Verify that the system should log in the user.
32. Ensure the password is masked with dots or asterisks when typed. Verify Password should not be visible as it is typed.
33. Use the "Tab" key to navigate between the email, password, and "Login" button. Verify that the focus should move in the correct order.
34. Check if the browser autofill suggests previously saved credentials. Verify the Autofill should suggest previously saved login credentials.
35. Attempt to access the login page while already logged in. Verify the system should redirect the user to the home or dashboard page.
36. Log in with the same credentials on multiple devices at the same time. Verify Login should work, or the first session should be invalidated.
37. Attempt to log in using different browsers (Chrome, Firefox, Safari, etc.). Login functionality should work across all supported browsers.
38. Change the account password from another device, then attempt to log in with the old password.Login should fail with the old password.
39. Measure the time taken from clicking "Login" to successfully logging in. Verify the response time should be within acceptable limits.
40. Attempt to log in when the site is under maintenance.Maintenance message should appear.