Test Cases for Login Page:

UI Test Scenarios of Login Page:

1. Verify that the login screen contains elements such as Username, Password, Sign in button, Remember password checkbox, Forgot password link, and create an account link.
2. Verify that all the fields such as Username, Password has a valid placeholder.
3. Verify whether all the text boxes have a minimum and maximum length.
4. Verify that the labels float upward when the text fields is in focus or filled (in case of the floating label).
5. Verify to see if the font style and size of the labels, as well as the text on each object are clearly visible.
6. Verify that the application's user interface (UI) is responsive, so it will adapt to different screen resolutions and devices.
7. Verify the login page and all the fields in the login page are displaying without any break in different browsers.

Functional Test Scenarios of Login Page:

1. Verify that cursor is focused on the "Username" text box on the page load (Login Page).
2. Verify that tab functionality is working properly or not.
3. Verify that Enter/Tab key works as a substitute for the Sign-in-Button.
4. Verify that the user is able to Login with valid Credentials.
5. Verify that the user is not able to Login with an invalid Username and invalid password.
6. Verify that the user is not able to log in with an invalid username and valid password.
7. Verify that the user is not able to log in with a valid username and an invalid password.
8. Verify that the user is not able to log in with a blank username or password.
9. Verify that the user is not able to login with inactive credentials.
10. Verify that the reset button clears that data from all the text boxes in the login form.
11. Verify that the login credentials, mainly password stores in a database in an encrypted format.
12. Verify that clicking on the browser back button after successful login should not take the user to log out mode.
13. Verify that validation message is displayed in the case when user leaves username or password as blank.
14. Verify that validation message is displayed in case of exceeding the character limit of the username and password fields.
15. Verify that validation message is displayed in case of entering special character in the username and password fields.
16. Verify that the "Keep me logged in" checkbox is unselected by default (depend on business logic, it may be selected or unselected).
17. Verify that the timeout of the login session (Session Timeout).
18. Verify that the logout link is redirected to login/home page.
19. Verify that User is redirected to appropriate page after successful login.
20. Verify that User is redirected to the Forgot password page when clicking on the Forgot password link.

21. Verify that the user is redirected to the Create an account page when clicking on the SignuP/ Create an account link.
22. Verify that the user Should be able to login with the new password after changing the password.
23. Verify that the user should not be able to login with old password after changing the password.
24. Verify that spaces should not be allowed before any password characters attempted.
25. Verify whether that user is still logged in after a series of actions such as Sign-in, close the browser and reopen the application.
26. Verify that the ways to retrieve the password if the user forgets the password.

Non-Functional Security Test Cases for Login Page:

1. Verify that clicking on the browser back button after successful logout should not take the user to a logged-in mode.
2. Verify that there is a limit on the total number of unsuccessful login attempts (No. of invalid attempts should be based on business logic. Base on the business logic, user will be asked to enter the captcha and try again or user will be blocked).
3. Verify that the password is in encrypted form (masked format) when entered in the password field.
4. Verify the password can be copy-pasted. System shouldn't allow users to copy paste password.
5. Verify that encrypted characters in the "password" field should not allow deciphering if copied.
6. Verify that the "Remember password" checkbox is unselected by default (depends on business logic, it may be selected or unselected).
7. Verify whether the login form is revealing any security information by viewing the page source.
8. Verify that the login page is vulnerable to SQL injection.
9. Verify whether Cross-site Scripting (XSS) vulnerability works on a login page. XSS vulnerability may be used by hackers to bypass access controls.

Performance Test Cases for Login Page:

1. Verify that how much time the application is taking to load the home page after entering the valid user name and password in the login page.

Test Cases for CAPTCHA & Cookies (If there is a captcha on the login page):

1. Verify that whether there is a client-side validation when the user doesn't enter the CAPTCHA.
2. Verify that the refresh link of CAPTCHA is generating the new CAPTCHA.
3. Verify that the CAPTCHA is case sensitive.
4. Verify whether the CAPTCHA has audio support to listen.
5. Verify whether virtual keyboard is available and working properly to enter login credentials incase of banking applications.
6. Verify two-way authentication through OTP is working properly incase of banking applications.
7. Verify SSL certificate is implemented or not.

8. Verify that the user is able to login when the browser cookies are cleared. When the cookies are cleared, system should not allow user to login automatically.
9. Verify the login functionality when the browser cookies are turned off.