Test Scenario

In any application, logging in is the process to access an application by an individual who has valid user credentials. Logging in is usually used to enter a specific page, which trespassers cannot see. In this post, we will see “Test Scenarios Login Page”. Testing of the Login page is very important for any application in terms of security aspect.

We usually write test cases for login page for every application we test. Every login page should have the following elements.

1. ‘Email/Phone Number/Username’ Textbox
2. ‘Password’ Textbox
3. Login Button
4. ‘Remember Me’ Checkbox
5. ‘Keep Me Signed In’ Checkbox
6. ‘Forgot Password’ Link
7. ‘Sign up/Create an account’ Link
8. CAPTCHA

Following are the test cases for User Login Page. The list consists of both Positive and Negative test scenarios login page.

Test Cases of a Login Page (Test Scenarios Login Page):

1. Verify that cursor is focused on “Username” text box on the page load (login page)
2. Verify that the login screen contains elements such as Username, Password, Sign in button, Remember password check box, Forgot password link, and Create an account link.
3. Verify that tab functionality is working properly or not
4. Verify that Enter/Tab key works as a substitute for the Sign in button
5. Verify that all the fields such as Username, Password has a valid placeholder
6. Verify that the labels float upward when the text field is in focus or filled (In case of floating label)
7. Verify that User is able to Login with Valid Credentials
8. Verify that User is not able to Login with invalid Username and invalid Password
9. Verify that User is not able to Login with Valid Username and invalid Password

10. Verify that User is not able to Login with invalid Username and Valid Password
11. Verify that User is not able to Login with blank Username or Password
12. Verify that User is not able to Login with inactive credentials
13. Verify that clicking on browser back button after successful login should not take User to log out mode
14. Verify that clicking on browser back button after successful logout should not take User to logged in mode
15. Verify that there is a limit on the total number of unsuccessful login attempts (No. of invalid attempts should be based on business logic. Based on the business logic, User will be asked to enter captcha and try again or user will be blocked)
16. Verify that the password is in encrypted form when entered
17. Verify the password can be copy-pasted
18. Verify that encrypted characters in “Password” field should not allow deciphering if copied
19. Verify that User should be able to login with the new password after changing the password
20. Verify that User should not be able to login with the old password after changing the password
21. Verify that spaces should not be allowed before any password characters attempted
22. Verify that whether User is still logged in after series of actions such as sign in, close browser and reopen the application.
23. Verify that the ways to retrieve the password if the User forgets the password
24. Verify that “Remember password” checkbox is unselected by default (depends on business logic, it may be selected or unselected)
25. Verify that “Keep me logged in” checkbox is unselected by default (depends on business logic, it may be selected or unselected)
26. Verify that the timeout of the login session (Session Timeout)
27. Verify that the logout link is redirected to login/home page
28. Verify that User is redirected to appropriate page after successful login
29. Verify that User is redirected to Forgot password page when clicking on Forgot Password link
30. Verify that User is redirected to Create an account page when clicking on Sign up / Create an account link
31. Verify that validation message is displayed in case when User leaves Username or Password as blank
32. Verify that validation message is displayed in case of exceeding the character limit of the Username and Password fields

33. Verify that validation message is displayed in case of entering special character in the Username and password fields
34. Verify whether the login form is revealing any security information by viewing page source
35. Verify that the login page is vulnerable to SQL injection
36. Verify whether Cross-site scripting (XSS) vulnerability work on a login page. XSS vulnerability may be used by hackers to bypass access controls.

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

37. Verify that whether there is a client-side validation when User doesn't enter CAPTCHA
38. Verify that the refresh link of CAPTCHA is generating new CAPTCHA
39. Verify that the CAPTCHA is case sensitive
40. Verify whether the CAPTCHA has audio support to listen