Gmail Login Page Test Scenario

Sr No.	Test Scenario
1	Verify that all the labels and controls including text-boxes, buttons, and links are present on the Login page.
2	Check that the font type and size of the labels and the text written on the different elements should be clearly visible.
3	Verify that the size, color, and UI of the different elements are as per the specifications.
4	Verify that the application's UI is responsive i.e. it should adjust to different screen resolutions and devices.
5	Verify that as soon as the login page opens, by default the cursor should remain on the username textbox.
6	Verify that the user is able to navigate or access the different controls by pressing the 'Tab' key on the keyboard.
7	Check if the password is in masked form when typed in the password field.
8	Check if the password can be copy-pasted or not.
9	Verify that the user is able to login by entering valid credentials and clicking on the 'Login' button.
10	Verify that the user is able to login by entering valid credentials and pressing Enter key.
11	Check that the user is not able to login with an invalid username and password.
12	Verify that the validation message gets displayed in case the user leaves the username or password field as blank.
13	Check that the validation message is displayed in the case the user exceeds the character limit of the user name and password fields.
14	Verify that reset button functionality on the login page. Clicking on it should clear the textbox's content.
15	Verify if there is a checkbox with the label "remember password" on the login page.
16	Verify that closing the browser should not log-out an authenticated user. Launching the application should lead the user to login state only.
17	Verify that there is a limit on the total number of unsuccessful login attempts. So that a user cannot use a brute-force mechanism to try all possible combinations of username-password.
18	Verify that in case of incorrect credentials, a message like "incorrect username or password" should get displayed. Instead of an exact message pointing to the incorrect field. This is because a message like "incorrect password" will help a hacker in knowing that the username is correct. In this way, he will just need to try a different combination on the password field only.
19	Verify the login session timeout duration. So, that once logged-in a user cannot be authenticated for a life-time.
20	Verify that once logged in, clicking the back button doesn't logout the user.
21	Verify if SQL Injection attacks work on the login page. The application should not be vulnerable to SQL injection attacks.
22	Verify that XSS vulnerability should not work on the login page.