Below are the probable test cases for just the login scenario
==========

1. verify the login screen will appear after clicking on a login link or login button.

2. Verify all login-related elements and fields are present on the login page.

3. Verify the alignment of displayed elements on the login screen should be compatible in cross browsers testing.

4. Verify that the size, color, and UI of different elements should match the specifications.

5. Verify that the login page of the application is responsive and aligns properly on different screen resolutions and devices.

6. Verify login page title.

7. After the user login page is open, the cursor should remain in the username text box by default.

8. Verify that there is a checkbox with the label remember password on the login page.

9. Verify the remember me checkbox should mark as checked after clicking on the label text and the check box.

10. verify the user credential remained on the field after clicking remember and get back to the login
screen again.

11. Verify that the user will be able to log in with their account with the correct credential.

12. Verify that the user will get into their dashboard screen after login in with the correct credentials.

13. Verify that the user can access all controls and elements by pressing the Tab key from the keyboard.

14. Verify that the user can log in by entering valid credentials and pressing Enter key.

15. Verify that the user can log in by entering valid credentials and clicking on the login button.

16. Verify that the password entered should be in encrypted form.

17. Verify whether an eye icon is added to the password field or not.

18. Verify that the user can be able to view the password by clicking on the eye icon.

19. There should be an email verification check, as the user verifies the email address then the user is able
to view the dashboard and access features.

20. Add a captcha on the login form to prevent the robot attack.

21. Verify the error message should display after just entering an email address and leaving the password
field blank.

22. Verify the error message should display after just entering a password and leaving the email field blank.

23. Verify the error message should display after entering the invalid credentials.

24. Verify the error message should display after entering an invalid email format.

25. Verify the displayed error message for invalid email format should be correct.

26. Verify the displayed error message grammar should be correct.

27. Verify the displayed error message spell should be correct.

28. Check logged in user should not log out on closing the browser.

29. Verify the login session timeout duration. So, once logged in a user can not be authenticated for a
lifetime.

30. Verify logged-in user doesn’t log out by clicking the back button on the browsers tab.

31. Verify that there is a limit to the total number of unsuccessful login attempts. Therefore, users cannot
use brute force mechanisms to try all possible username-password combinations.

32. Verify logged-in user copies the URL and pastes it into a new browser window, it should redirect to the
login page.

33. Check login by google and all social options for login in the private window separately.

34. As the user signs in, on the home page, there is no need for displaying Sign Up or Try Now, etc (if the
user logged in).

35. Add rate limit on login. After how many attempts user should be able to restrict by the app for the wait.

36. Verify it should not be always in loading in case the user adds an invalid email and password.

37. Verify all the functionalities should be working condition as the user sign-in from social login i-e
Facebook and google.

38. Prevent login page from SQL injection attack.