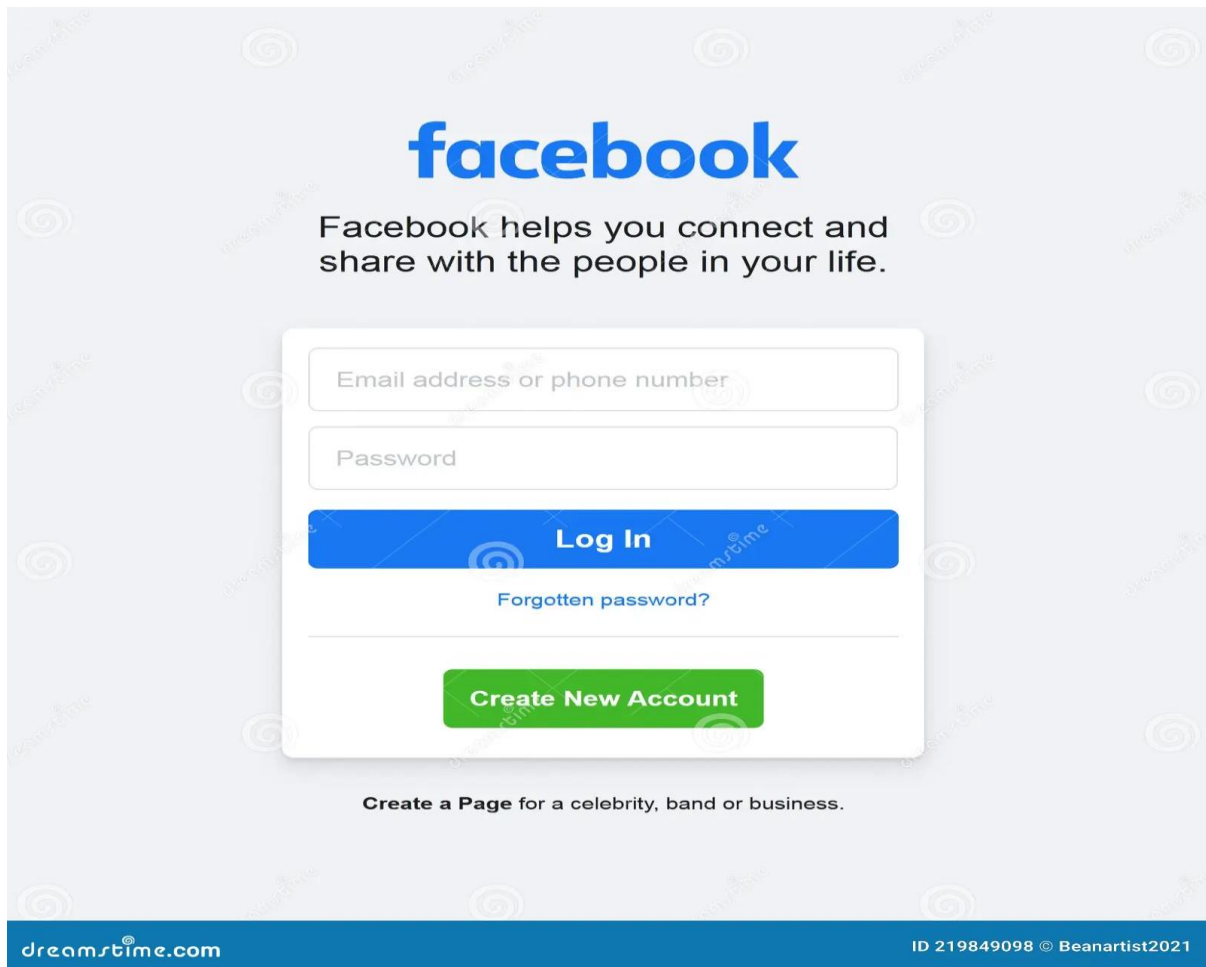


## TEST CASES FOR FACEBOOK LOGIN PAGE



### 1. UI Verification:

1. Verify that the login page URL opens correctly when (<https://www.facebook.com/>) is entered.
2. Verify that the Facebook logo is present on the login page.
3. Verify the **color, shape, size, font, and position** of the Facebook logo.
4. Verify that the tagline is present.
5. Verify the **font, color, and position** of the tagline.
6. Verify that the tagline is free from spelling, grammar, and punctuation errors.
7. Verify that all required labels, input fields, buttons, links, and text are present.
8. Verify that all required elements are **clearly visible**.
9. Verify that all elements (buttons, text, input fields, and links) are **properly aligned** without overlapping.

10. Verify the size of all buttons, links, text, and input fields.
11. Verify that the login page maintains a professional design and layout.
12. Verify that the login page uses consistent font styles across all elements.

## 2. Functionality Verification:

13. Verify the login functionality across different browsers (Chrome, Safari, Edge, Firefox).  
*(Cross-browser testing)*
14. Verify that tooltips are present where applicable.
15. Verify the presence of placeholders in the input fields.
16. Verify the responsiveness of the login page across different screen sizes. *(Responsive Testing)*
17. Verify that the user can log in by pressing the "Enter" key.
18. Verify forward navigation using the "Tab" key.
19. Verify backward navigation using "Shift + Tab".
20. Verify that the user can input a username or email.
21. Verify that the user can input a password.
22. Verify that the password is **masked/encrypted**.
23. Verify that the password becomes visible when the "eye" icon is clicked and re-encrypts when clicked again.
24. Verify that all buttons are clickable and lead to the expected actions.
25. Verify that the "Forgot Password" link redirects to the correct page.

## 3. Field Validation:

26. Verify the **minimum and maximum character limits** for the username/email field.
27. Verify the **minimum and maximum character limits** for the password field.
28. Verify the redirection of all footer links.
29. Verify that the user cannot log in with blank username and password.
30. Verify the **error message** for blank username and password.
31. Verify that the user cannot log in with a blank username and a valid password.
32. Verify the **error message** for blank username and valid password.
33. Verify that the user cannot log in with an invalid username or email format.
34. Verify the **error message** for an invalid email format.

- 35. Verify that the user cannot log in with an incorrect password.
- 36. Verify the **error message** for an incorrect password.
- 37. Verify that the user cannot log in with an old password.
- 38. Verify that the user can log in with a new password.
- 39. Verify that an already-used password cannot be set as the new password.
- 40. Verify that the username, email, or phone number cannot be used as the password.
- 41. Verify that the password meets the required criteria (e.g., one lowercase letter, one uppercase letter, one special character, and at least 8 characters long).

#### **4. Security Verification:**

- 42. Verify the maximum number of unsuccessful login attempts allowed.
- 43. Verify if 2-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) is enabled.
- 44. Verify whether multiple simultaneous sessions are allowed.
- 45. Verify that session timeouts are implemented after a period of inactivity.
- 46. Verify that sensitive data (passwords) is not logged in browser developer tools.
- 47. Verify that the login page uses HTTPS for secure communication.
- 48. Verify that cookies and session tokens are secure and not exposed.
- 49. Verify that the login page is protected against SQL injection and other common attacks.
- 50. Verify that CAPTCHA or similar mechanisms are in place to prevent automated login attempts.