**ParaBank Customer Login Test Scenarios**

**Scenario: Login with Valid Credentials**

* **Given:** a user is on the login page
* **When:** they log in with a valid username and password
* **Then:** the user is redirected to the account overview

**Scenario: Login with Invalid Password**

* **Given:** a user is on the login page
* **When:** they log in with a valid username and an invalid password
* **Then:** an error message "Invalid username or password" is displayed

**Scenario: Login with Invalid Username**

* **Given:** a user is on the login page
* **When:** they log in with an invalid username and a valid password
* **Then:** an error message "Invalid username or password" is displayed

**Scenario: Submit Login Form with Empty Fields**

* **Given:** a user is on the login page
* **When:** they submit the login form with empty fields
* **Then:** a validation message prompts the user to enter credentials

**Scenario: Submit Login Form with Whitespace-Only Input**

* **Given:** a user is on the login page
* **When:** they submit the login form with whitespace-only input
* **Then:** a validation message prompts the user to enter valid data

**Scenario: Navigate to Forgot Login Info Page**

* **Given:** a user is on the login page
* **When:** they click the “Forgot login info?” link
* **Then:** the user is redirected to the account recovery page

**Scenario: Navigate to New User Registration Page**

* **Given:** a user is on the login page
* **When:** they click the “Register” link
* **Then:** the user is redirected to the new user registration page

**Scenario: Attempt Login with SQL Injection**

* **Given:** a user is on the login page
* **When:** they attempt to log in with an SQL injection payload
* **Then:** the input is rejected, and an error message is shown

**Scenario: Attempt Login with XSS Script**

* **Given:** a user is on the login page
* **When:** they attempt to log in with an XSS script
* **Then:** the input is sanitized and no script is executed

**Scenario: Verify Password Masking**

* **Given:** a user is on the login page
* **When:** they enter a password
* **Then:** all characters are hidden as '●' or '\*'

**Scenario: Verify Keyboard Navigation**

* **Given:** a user is on the login page
* **When:** they navigate the form using only the keyboard
* **Then:** all fields and buttons are accessible in a logical order

**Scenario: Mobile Responsiveness**

* **Given:** a user is on a mobile device
* **When:** they access the login page
* **Then:** the page adapts to the screen size with a proper layout

**Scenario: Account Lockout after Failed Attempts**

* **Given:** a user is on the login page
* **When:** they attempt to log in 5 consecutive times with incorrect credentials
* **Then:** an "Account locked" message is displayed

**Scenario: Verify Audit Log Entry**

* **Given:** a user attempts to log in
* **When:** the login attempt is processed
* **Then:** an entry is recorded in the audit log with a timestamp, username, and status

**Scenario: Verify Session Management**

* **Given:** a user has successfully logged in
* **When:** their session is managed
* **Then:** a session token is generated and is invalidated upon logout