**1. Introduction**

**Test Plan ID**: LoginPageTestPlan  
**Test Plan Title**: Login Page Testing for app.vwo.com  
**Test Type**: Functional, Security, Usability, Performance  
**Test Objective**: To ensure the login functionality on the VWO (Visual Website Optimizer) login page is working as expected, secure, and user-friendly.

**Test Scope**:

* Functional Testing
* UI/UX Testing
* Security Testing
* Performance Testing
* Compatibility Testing

**Assumptions**:

* Testers have valid credentials to perform tests.
* App.vwo.com is up and running without any server-side issues.

**2. Test Items**

* **Login Form**: Email input field, Password input field, Submit button, and Remember Me checkbox.
* **Login Process**: Correct and incorrect login, handling of invalid credentials.
* **Error Messages**: Proper display of error messages for invalid credentials.
* **Redirection**: Successful login redirection to the appropriate dashboard page.
* **User Experience (UX)**: Responsiveness and UI elements.
* **Session Management**: Logout, session expiry, and re-login scenarios.

**3. Features to be Tested**

1. **Email Input Field**:
   * Check that the input accepts only valid email formats.
   * Email length should be within valid limits (e.g., 320 characters).
   * Placeholder and input behavior.
2. **Password Input Field**:
   * Password field should mask entered characters.
   * Validate password strength and length.
   * Minimum and maximum password length.
   * Check for visibility toggle (if provided).
3. **Submit Button**:
   * Should only be enabled when both email and password are entered.
   * Ensure clicking the button triggers the correct login behavior.
4. **Login Validation**:
   * Correct login with valid credentials should redirect to the homepage or dashboard.
   * Incorrect login should display an appropriate error message (e.g., "Invalid credentials").
5. **Remember Me Checkbox**:
   * Ensure the "Remember Me" functionality works as expected.
   * Check if it retains the login state upon revisiting the site.
6. **Security**:
   * Check for SQL Injection, Cross-Site Scripting (XSS), and other common vulnerabilities.
   * Ensure HTTPS is enforced for the login page.
7. **Redirection**:
   * Ensure the user is redirected to the correct page upon successful login.
   * Check redirection behavior when incorrect login is attempted.
8. **Session Management**:
   * Ensure that a session is correctly created upon login and terminated after logout.
   * Check session expiry behavior when logged in for long periods.

**4. Features Not to be Tested**

* Backend database integration.
* API-level testing for user authentication.

**5. Test Strategy**

* **Test Types**:
  + **Functional Testing**: Validate that all features, including login, form fields, validation messages, and redirection, work as expected.
  + **Security Testing**: Ensure that the login page is secure from attacks like SQL injection and XSS.
  + **Usability Testing**: Verify that the login page is user-friendly and accessible across devices and screen sizes.
  + **Performance Testing**: Ensure the login page loads within acceptable time limits under varying loads.
  + **Compatibility Testing**: Test the page on different browsers (Chrome, Firefox, Safari, Edge) and mobile devices (iOS, Android).

**6. Test Environment**

* **Platform**: Desktop and Mobile browsers (Chrome, Firefox, Safari, Edge)
* **Operating System**: Windows 10, macOS, Android, iOS
* **Browsers**: Latest versions of Chrome, Firefox, Safari, and Edge.
* **Tools**: Selenium, JMeter (for load testing), Burp Suite (for security testing).

**7. Test Schedule**

| **Test Phase** | **Start Date** | **End Date** | **Responsibility** |
| --- | --- | --- | --- |
| Test Planning | 2025-03-16 | 2025-03-16 | Test Manager |
| Test Design | 2025-03-17 | 2025-03-18 | QA Engineers |
| Test Execution | 2025-03-19 | 2025-03-21 | QA Engineers |
| Defect Reporting | 2025-03-22 | 2025-03-23 | Test Manager |
| Test Closure | 2025-03-24 | 2025-03-24 | Test Manager |

**8. Test Scenarios**

**8.1 Functional Test Scenarios**

| **Test Case ID** | **Test Scenario** | **Expected Result** | **Pass/Fail** |
| --- | --- | --- | --- |
| TC01 | Verify login with valid credentials. | Login should succeed, and the user is redirected to the dashboard. |  |
| TC02 | Verify login with invalid credentials (wrong password). | The system should display an "Invalid credentials" error message. |  |
| TC03 | Verify login with empty email or password. | The system should show validation error for empty fields. |  |
| TC04 | Verify Remember Me functionality works. | The system should retain the login state upon revisiting the site. |  |
| TC05 | Verify successful login redirects to the correct page. | After successful login, user is directed to the correct page. |  |

**8.2 Security Test Scenarios**

| **Test Case ID** | **Test Scenario** | **Expected Result** | **Pass/Fail** |
| --- | --- | --- | --- |
| TC06 | Test for SQL Injection in the email and password fields. | The application should not be vulnerable to SQL Injection attacks. |  |
| TC07 | Test for Cross-Site Scripting (XSS) vulnerability. | The application should not allow script injection via input fields. |  |
| TC08 | Verify HTTPS encryption for the login page. | The login page should load using HTTPS. |  |

**8.3 Usability Test Scenarios**

| **Test Case ID** | **Test Scenario** | **Expected Result** | **Pass/Fail** |
| --- | --- | --- | --- |
| TC09 | Verify UI consistency across devices. | UI should adjust appropriately for different screen sizes. |  |
| TC10 | Verify readability and font size for form fields. | Text should be easily readable, and the form should be accessible. |  |

**8.4 Performance Test Scenarios**

| **Test Case ID** | **Test Scenario** | **Expected Result** | **Pass/Fail** |
| --- | --- | --- | --- |
| TC11 | Load testing for login page (500 users). | The page should load within acceptable time limits for 500 concurrent users. |  |
| TC12 | Stress testing with 1000 users logging in simultaneously. | The system should handle the load without crashing or slowing down drastically. |  |

**8.5 Compatibility Test Scenarios**

| **Test Case ID** | **Test Scenario** | **Expected Result** | **Pass/Fail** |
| --- | --- | --- | --- |
| TC13 | Verify login functionality on Chrome (latest version). | Login functionality should work without issues. |  |
| TC14 | Verify login functionality on Firefox (latest version). | Login functionality should work without issues. |  |
| TC15 | Verify login functionality on Safari (latest version). | Login functionality should work without issues. |  |
| TC16 | Verify login functionality on mobile (iOS and Android). | Login should work seamlessly across mobile browsers. |  |

**9. Entry and Exit Criteria for Test Execution**

**Entry Criteria:**

* Test environment is set up and stable.
* Test data is ready, including valid and invalid user credentials.
* Test cases are written, reviewed, and ready for execution.
* All dependencies and prerequisites are resolved (e.g., backend integration is available).
* Test environment configuration is verified to match the production environment.
* The testing team has been briefed on the scope, tools, and methodologies.

**Exit Criteria:**

* All planned test cases have been executed successfully.
* All critical and high-priority test cases have passed.
* No high-severity defects remain unresolved (unless risks are accepted by the relevant stakeholders).
* All defects have been logged, reviewed, and closed or deferred appropriately.
* Test results are documented, and any deviations from the expected behavior have been recorded and communicated.
* Test logs, defect reports, and other documentation are complete and shared with stakeholders.

**10. Entry and Exit Criteria for Test Closure**

**Entry Criteria:**

* Test execution is complete for all test cases.
* All critical defects are resolved or have been accepted as risks.
* Test reports are generated and reviewed for completeness and accuracy.
* All stakeholders have been informed of any open issues or risks.
* Test cases, scenarios, and test data are finalized and documented.

**Exit Criteria:**

* All tests are complete, and the quality of the product meets the agreed-upon acceptance criteria.
* The final test report is prepared, covering test results, defect status, and overall quality assessment.
* Test deliverables (such as test logs, defect reports, and other relevant documents) have been submitted to stakeholders.
* Stakeholders have reviewed and approved the final results and test closure.

**11. Defect Reporting Procedure**

1. **Identify Defect**: When a defect is found during test execution, it must be documented immediately with sufficient detail for reproduction.
2. **Log Defect**: Report defects in the defect management tool (e.g., JIRA, Bugzilla) including:
   * Title/ID
   * Description
   * Steps to reproduce
   * Expected vs. actual results
   * Severity and priority
   * Screenshots or logs (if applicable)
3. **Defect Triage**: The defects are reviewed, prioritized, and assigned to the appropriate team (e.g., development).
4. **Fix and Retest**: After the defect is resolved, retest to verify the fix.
5. **Close Defect**: Once the fix is validated, the defect is closed.

**12. Test Deliverables**

* **Test Plan Document**: The current test plan document.
* **Test Cases/Scenarios**: A detailed list of test cases for login functionality.
* **Test Execution Report**: A report summarizing the results of test execution, including pass/fail status.
* **Defect Logs**: Detailed logs of any defects found during testing.
* **Test Closure Report**: A final report summarizing the test process, results, and overall quality assessment.

**13. Tools**

* **Automation Tools**: Selenium, Cypress (for automated functional testing)
* **Load Testing Tools**: JMeter, LoadRunner
* **Security Testing Tools**: Burp Suite, OWASP ZAP
* **Defect Tracking Tools**: JIRA, Bugzilla, or any other internal defect tracking tool.
* **Test Case Management Tools**: TestRail, QTest

**14. Approval**

* **Test Manager**: [Test Manager Name]  
  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* **Development Lead**: [Development Lead Name]  
  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* **Product Owner**: [Product Owner Name]  
  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_