**VWO Platform Login Page Test Plan**

**1. Introduction**

This test plan focuses on thorough validation of the VWO platform login page functionality, security, and user experience. The plan includes test scenarios, test cases, and acceptance criteria appropriate for a QA professional with 2+ years of experience.

**2. Test Scope**

* Email/password login functionality
* SSO login functionality
* Password recovery process
* New user registration ("Start a free trial")
* "Remember me" functionality
* UI/UX aspects
* Responsiveness and compatibility
* Security considerations

**3. Test Scenarios and Test Cases**

**3.1 Functional Testing**

**Email/Password Authentication**

1. **Valid Login**
   * Enter valid email and password
   * Verify successful login and redirect to dashboard
   * Expected: User logged in successfully
2. **Invalid Login - Wrong Email**
   * Enter non-existent email and any password
   * Expected: Error message indicating invalid credentials
3. **Invalid Login - Wrong Password**
   * Enter valid email with incorrect password
   * Expected: Error message indicating invalid credentials
4. **Empty Fields Validation**
   * Submit with empty email field
   * Submit with empty password field
   * Submit with both fields empty
   * Expected: Appropriate validation error messages
5. **Email Format Validation**
   * Enter improperly formatted emails (missing @, missing domain, etc.)
   * Expected: Format validation error message
6. **Password Field Behavior**
   * Verify password is masked during entry
   * Check if copy/paste functionality works
   * Expected: Password appears as dots/asterisks, copy/paste works properly
7. **Case Sensitivity**
   * Verify email field is case-insensitive
   * Verify password field is case-sensitive
   * Expected: Login successful with different email casing, fails with incorrect password casing

**"Remember Me" Functionality**

1. **Remember Me - Checked**
   * Login with "Remember me" checked
   * Close browser and reopen
   * Expected: Email field pre-populated, login session preserved (if applicable)
2. **Remember Me - Unchecked**
   * Login with "Remember me" unchecked
   * Close browser and reopen
   * Expected: Email field empty, session not preserved

**SSO Authentication**

1. **SSO Login Flow**
   * Click "Sign in using SSO"
   * Verify redirect to SSO provider
   * Complete SSO authentication
   * Expected: Successful redirect back to VWO with authenticated session
2. **SSO Error Handling**
   * Test SSO with incorrect credentials or permissions
   * Expected: Appropriate error messages displayed

**Password Recovery**

1. **Forgot Password Functionality**
   * Click "Forgot Password?"
   * Enter valid email
   * Expected: Success message confirming password reset email sent
2. **Password Reset Invalid Email**
   * Enter non-existent email in password recovery
   * Expected: Generic message to protect from email enumeration
3. **Password Reset Link Validation**
   * Verify password reset link expiration
   * Test password complexity requirements on reset
   * Expected: Links expire appropriately, password requirements enforced

**New User Registration**

1. **Free Trial Link**
   * Click "Start a free trial"
   * Verify redirect to registration page
   * Expected: Proper redirection to sign-up flow

**3.2 UI/UX Testing**

1. **Visual Elements**
   * Verify VWO logo displays correctly
   * Check form field labels and positioning
   * Validate button styling and hover states
   * Expected: All elements match design specifications
2. **Form Field Behavior**
   * Check tab order between fields
   * Test field focus and blur events
   * Verify Enter key submits the form
   * Expected: Intuitive navigation between fields
3. **Error Message Display**
   * Verify positioning, styling, and clarity of error messages
   * Check accessibility of error states
   * Expected: Clear, visible error messages that guide user action

**3.3 Compatibility Testing**

1. **Browser Compatibility**
   * Test on Chrome, Firefox, Safari, Edge
   * Expected: Consistent behavior across browsers
2. **Device Compatibility**
   * Test on desktop, tablet, mobile viewports
   * Expected: Responsive layout with all functionality preserved
3. **OS Compatibility**
   * Test on Windows, macOS, iOS, Android
   * Expected: Consistent behavior across operating systems

**3.4 Security Testing**

1. **Input Sanitization**
   * Test SQL injection in email and password fields
   * Test XSS vulnerability with script inputs
   * Expected: Properly sanitized inputs, no security vulnerabilities exposed
2. **Brute Force Protection**
   * Test multiple failed login attempts
   * Expected: Account lockout or CAPTCHA after defined attempts
3. **Session Management**
   * Check session timeout behavior
   * Verify session invalidation after logout
   * Expected: Sessions expire appropriately, cannot access after logout
4. **HTTPS Verification**
   * Verify secure connection
   * Check certificate validity
   * Expected: Valid HTTPS with current certificate
5. **Password Storage**
   * Review password handling (if applicable)
   * Expected: One-way hashing with salt

**3.5 Performance Testing**

1. **Login Response Time**
   * Measure time to authenticate and redirect
   * Expected: Response within 2 seconds under normal conditions
2. **Concurrent User Logins**
   * Simulate multiple concurrent login attempts
   * Expected: System handles multiple logins without degradation

**4. Test Environment**

**Required Resources**

* Multiple browsers (Chrome, Firefox, Safari, Edge)
* Desktop, tablet, and mobile devices
* Test accounts with various permission levels
* SSO test accounts/configuration
* Network throttling tools for performance testing

**5. Risk Assessment**

1. **High Risk Areas**
   * Password recovery flow (security implications)
   * SSO integration points (third-party dependency)
   * Session management (security implications)
   * Brute force protection (security vulnerability)
2. **Mitigation Strategies**
   * Extra test cycles on high-risk areas
   * Security-focused code reviews
   * Regular penetration testing
   * Monitoring failed login attempts in production

**6. Exit Criteria**

* All test cases executed with 100% pass rate
* No high or critical severity bugs open
* Security vulnerabilities addressed
* Performance meets response time requirements

**7. Test Deliverables**

* Test case documentation with results
* Bug reports for identified issues
* Security assessment report
* Performance metrics report
* Final test summary report

**8. Regression Testing Approach**

* Full regression suite execution after any login page changes
* Focused regression on affected areas for backend authentication changes
* Automated test suite for critical login paths

**9. Automated Testing Recommendations**

**Automation Priority**

1. Valid login scenarios
2. Invalid login scenarios
3. Password recovery flow
4. SSO authentication flow
5. Security tests (brute force protection, session management)

**Tools Recommendation**

* Selenium/Playwright for UI testing
* JMeter/k6 for performance testing
* OWASP ZAP for security testing
* REST API clients for direct authentication API testing