# Test Plan & Test Strategy - VWO Platform (Login Module)

## Test Plan

### 1. Objective

Ensure the login functionality works as expected with valid and invalid inputs. Verify security, usability, performance, and compatibility aspects of the login module.

### 2. Scope

In-Scope:  
- Email & Password based login  
- Sign in using SSO  
- Forgot Password flow  
- Remember Me functionality  
- Error messages & validation  
- UI/UX validation of login screen  
  
Out of Scope:  
- Post-login functionalities (dashboard, analytics, etc.)  
- Backend database validation (unless explicitly required)

### 3. Test Scenarios

Positive Scenarios:  
- Valid email + valid password → successful login  
- Valid email + valid password + Remember me → auto-login on next visit  
- Login with SSO → redirects to correct identity provider  
  
Negative Scenarios:  
- Invalid email format (missing @, domain, etc.)  
- Valid email + wrong password → error message  
- Empty fields → validation error  
- SQL injection / special characters in email & password  
- Exceeding max character limits  
  
Boundary Testing:  
- Min/max length of email and password fields  
- Case sensitivity in email & password  
  
Security Scenarios:  
- Brute-force attempt → account lockout  
- Password not visible (masked input)  
- HTTPS encryption check  
- CSRF/XSS vulnerabilities  
- Session timeout after inactivity  
  
Usability Scenarios:  
- Tab order between fields  
- Mobile responsiveness of login page  
- Error message clarity

### 4. Test Data

- Valid registered user credentials  
- Invalid user credentials  
- Email with special characters  
- Test accounts for SSO login

### 5. Entry & Exit Criteria

Entry Criteria:  
- Login page deployed and accessible  
- Test environment ready  
  
Exit Criteria:  
- All critical & high severity bugs fixed  
- >95% test cases passed

### 6. Test Deliverables

- Test Plan  
- Test Cases (manual + automation if required)  
- Test Execution Report  
- Defect Log  
- Final Test Closure Report

## Test Strategy

### 1. Testing Approach

- Manual Testing: Initial validation of UI, UX, field validations, and error messages.  
- Automation Testing: Repeated scenarios like valid login, invalid login, and Remember Me flow.  
- Security Testing: Brute force, SQL injection, XSS testing.  
- Performance Testing: Response time during login.  
- Compatibility Testing: Across browsers and devices.

### 2. Test Levels

- Unit Testing: Field validations, API response codes.  
- Integration Testing: Login API integration with backend, SSO redirection.  
- System Testing: End-to-end login flow validation.  
- Regression Testing: Ensure new changes don’t break login.

### 3. Test Environment

- Staging server with same configuration as production  
- Test accounts provisioned with different roles (admin, user, guest)

### 4. Risk & Mitigation

- Risk: Weak error handling could expose sensitive info.  
 Mitigation: Test for generic error messages.  
  
- Risk: SSO failure due to misconfiguration.  
 Mitigation: Test with multiple identity providers.  
  
- Risk: Performance degradation during peak login.  
 Mitigation: Load test with concurrent users.