## **Master Test Plan – VWO Application Login Module**

**Project Name**: VWO (Visual Website Optimizer)  
 **Module**: User Authentication – Login  
 **Test Plan Author**: ABIRAMI, QA Tester  
 **Reviewers**: Test Architect, Security Lead, Product Owner  
 **Date**: [12-05-2025]  
 **Approval Status**: Draft | Final

### **1. Business Objective Alignment**

Ensure the login mechanism of VWO enables secure, frictionless access for authorized users while guarding against unauthorized access and fulfilling enterprise-level **security**, **usability**, and **accessibility** standards to maintain platform trust, user retention, and compliance.

### **2. Test Strategy Summary**

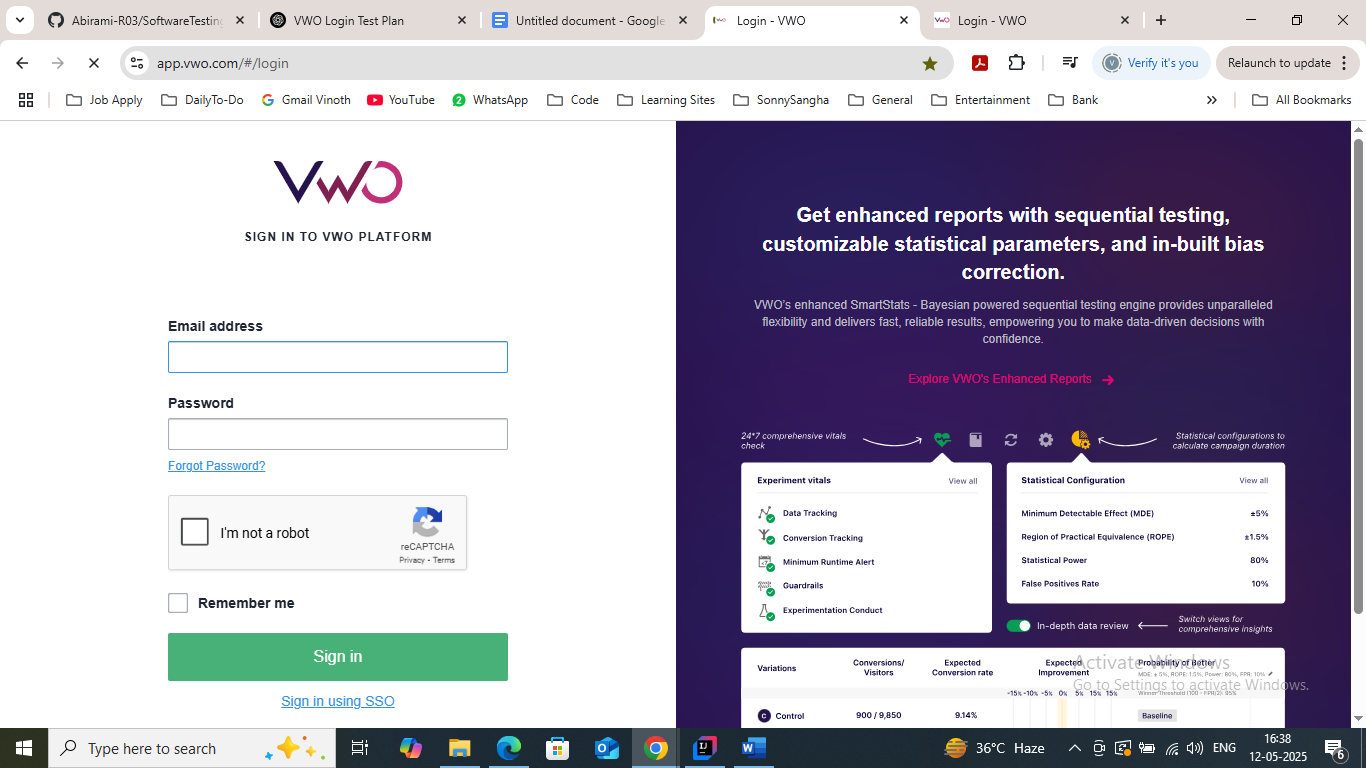
A **risk-based testing** strategy will be employed. Functional, security, usability, and cross-platform validations will be prioritized based on user impact and compliance requirements.

**Testing Types Covered**:

* Functional & UI Validation
* Negative Testing
* Security Testing (OWASP Top 10 focused)
* Accessibility (WCAG 2.1 AA)
* Cross-browser & device compatibility
* Session & Cookie Management
* Input Field Sanitization & Encoding

### **3. In Scope**

* Core login flow (email & password entry, submission, redirection)
* Error handling (invalid credentials, empty inputs, account lock)
* Password visibility toggle
* Forgot password navigation
* Validation against OWASP input vulnerabilities
* Cookie & session behavior post-login
* Localization of error messages (if supported)
* API-level login response validation (optional)



### **4. Out of Scope**

* MFA/OTP (unless enabled)
* SSO/SAML/OAuth integrations
* Signup or registration flows
* Load & concurrency testing of login endpoint

### **5. Assumptions**

* Functional specifications for login behavior are finalized.
* Valid test credentials (including edge cases) are provided.
* Login endpoint is stable and version-locked during testing.
* Environment is integrated with appropriate logging and tracing.

### **6. Entry & Exit Criteria**

| **Entry Criteria** | **Exit Criteria** |
| --- | --- |
| Requirements are signed off | 100% execution of critical test cases |
| Environment is stable and accessible | All critical/major defects closed |
| Test data is available | Test summary report approved |
| Test plan reviewed & approved | Test logs and evidences archived |

### **7. Test Environment Details**

| **Item** | **Description** |
| --- | --- |
| URL | https://app.vwo.com/#/login |
| Environments | UAT / Pre-Prod / Prod |
| Browsers | Chrome (LTS & latest), Firefox, Edge, Safari |
| Devices | Windows, macOS, iOS, Android |
| Tools | Selenium, OWASP ZAP, BrowserStack, Lighthouse |
| CI/CD Integration | Jenkins/GitHub Actions (Optional) |
| Test Mgmt | TestRail / Zephyr / Azure DevOps |
| Logging & Tracing | Browser Console, HAR files, Session logs |

### **8. Test Case Coverage Matrix**

#### **🧪 Functional Scenarios**

| **ID** | **Scenario** | **Priority** | **Risk Level** |
| --- | --- | --- | --- |
| TC01 | Load login page and validate all UI elements | High | Medium |
| TC02 | Login with valid credentials – redirect to dashboard | Critical | High |
| TC03 | Login with invalid password | High | High |
| TC04 | Login with malformed email input | High | High |
| TC05 | Attempt login with empty fields | High | High |
| TC06 | Password masking and visibility toggle | Medium | Low |
| TC07 | Validate error messages and localization (i18n, if supported) | Medium | Medium |
| TC08 | Validate copy-paste behavior in password field | Low | Low |
| TC09 | Redirection to "Forgot Password" page and back | Medium | Low |

#### **🔐 Security Test Cases**

| **ID** | **Scenario** | **Priority** | **Risk Level** |
| --- | --- | --- | --- |
| SEC01 | Attempt login with SQL injection payload (' OR 1=1 --) | Critical | High |
| SEC02 | Validate XSS handling on login inputs | Critical | High |
| SEC03 | Ensure transmission over HTTPS only (SSL cert check) | Critical | High |
| SEC04 | Cookie validation: HttpOnly, Secure, SameSite attributes | High | High |
| SEC05 | Attempt brute-force login and check account lock (rate-limiting) | Critical | High |

#### **♿ Accessibility & UX**

| **ID** | **Scenario** | **Priority** | **Risk Level** |
| --- | --- | --- | --- |
| UX01 | Screen reader compatibility (NVDA, VoiceOver) | Medium | Medium |
| UX02 | Tab order navigation and focus indication | Medium | Low |
| UX03 | Color contrast and error message readability | Medium | Low |

### **9. Test Data Management**

| **User Type** | **Email** | **Password** | **Remarks** |
| --- | --- | --- | --- |
| Valid User | valid@vwo.com | ValidPass123 | Successful login |
| Invalid Email | abc@vwo | ValidPass123 | Invalid format |
| Incorrect User | notexist@vwo.com | Test@123 | Non-existent user |
| Locked User | locked@vwo.com | Test@123 | Should block login |
| Edge User | longinput@vwo.com | 💀🔥🐍💻123 | Special char handling |

Test data to be version-controlled in secure Git repo or Test Data Manager with tagging per environment.

### **10. Traceability Matrix**

(Excerpt)

| **Requirement ID** | **Test Case ID** | **Description** |
| --- | --- | --- |
| REQ-AUTH-001 | TC01–TC05 | Field validations |
| REQ-AUTH-002 | TC02 | Successful login |
| REQ-SEC-001 | SEC01–SEC05 | Security standards (OWASP compliance) |
| REQ-UX-001 | UX01–UX03 | Accessibility & usability |

### **11. Risk Management Plan**

| **Risk** | **Likelihood** | **Impact** | **Mitigation Strategy** |
| --- | --- | --- | --- |
| API behavior changes during test cycle | Medium | High | Continuous sync with Dev; API contracts |
| Browser-specific rendering issues | Medium | Medium | Use BrowserStack to validate |
| Test data contamination across test cycles | Low | High | Reset data via API hooks after each run |
| Incomplete localization coverage | Medium | Low | Add pseudo-localization tests |

### **12. Reporting & Metrics**

**Daily Reporting**:

* Test Case Execution Progress
* Defects by Severity
* Test Coverage % (Requirement-wise)

**Final Metrics**:

* Pass/Fail rate by test type
* Defect density
* Time to detect & time to resolve bugs
* Regressions from previous release

### **13. Sign-Off & Approvals**

| **Role** | **Name** | **Signature / Date** |
| --- | --- | --- |
| QA Lead |  |  |
| Product Owner |  |  |
| Security Auditor |  |  |