

# Test Plan for VWO App (Login & Dashboard)

## 1. Introduction

This document defines the test strategy, scope, objectives, and execution approach for testing the **Login and Dashboard functionality** of **VWO App (app.vwo.com)**. The primary goal is to **ensure secure authentication, seamless navigation, data integrity, and an intuitive user experience** across different environments.

---

## 2. Scope

### In-Scope

- **Login Page Functionality**
  - User authentication (Valid/Invalid credentials)
  - Password reset and "Forgot Password?" flow
  - "Remember Me" feature validation
  - Multi-device login behaviour
  - Session timeout handling
- **Dashboard Functionality**
  - UI/UX verification
  - User role-based access control
  - Data retrieval accuracy
  - Navigation and responsiveness
  - Integration with backend services
- **Security & Performance Testing**
  - SQL Injection and XSS attack prevention
  - Unauthorized access restriction
  - API response validation for authentication

## Out of Scope

- Third-party integrations unless they directly affect login functionality
  - Non-functional testing like performance and load testing (covered separately)
- 

## 3. Test Objectives

- a) Validate **user authentication mechanisms** (Login, Logout, Forgot Password, SSO)
  - b) Ensure **dashboard accessibility** and correct data loading for different user roles
  - c) Identify and report **functional and UI-related defects**
  - d) Test **session management**, role-based access, and security vulnerabilities
  - e) Verify **responsiveness across different devices and browsers**
- 

## 4. Test Approach

### Functional Testing

- Validate correct login/logout behavior
- Verify error handling for incorrect login attempts
- Ensure the **forgot password flow** sends reset emails correctly
- Test **session expiration and auto logout**

### Regression Testing

- Ensure new feature updates do not break login/dashboard functionality

### Cross-Browser & Device Testing

- Test on **Chrome, Firefox, Edge, and Safari**
- Validate responsiveness on **desktop, tablet, and mobile devices**

### Security Testing

- Attempt SQL Injection and check if it is blocked
- Perform Cross-Site Scripting (XSS) attack tests
- Check role-based access control

### API Testing

- Validate API responses for authentication requests
  - Verify correct error handling in API responses
-

## 5. Test Environment

### Component Details

Browsers	Chrome, Firefox, Edge, Safari
Devices	Desktop, Tablet, Mobile (iOS, Android)
OS	Windows, macOS, Android, iOS
Test Data	Different user roles, valid/invalid credentials

---

## 6. Test Deliverables

- Test Scenarios & Test Cases
  - Test Execution Reports
  - Defect Reports & Logs
  - Final Test Summary Report
- 

## 7. Entry & Exit Criteria

### Entry Criteria:

- Test environment setup is complete
- Required test data is available
- Test cases are reviewed and approved

### Exit Criteria:

- All planned test cases have been executed
  - No high-severity defects remain unresolved
  - Test Summary Report has been submitted
- 

## 8. Risks & Mitigation

Potential Risk	Mitigation Strategy
Login issues in certain browsers	Regular cross-browser testing

API failures causing login failure	Implement robust API monitoring
Security vulnerabilities	Conduct periodic security audits

---

## 9. Conclusion

This test plan aims to validate the **Login and Dashboard functionalities** of the **VWO App**, ensuring a **secure, user-friendly, and stable experience**. The testing process will follow an iterative approach to accommodate **continuous improvements and new feature enhancements**.

---