Test Plan for app.vwo.com Login Page and Dashboard

Table of Contents

1. Introduction

1.1 Purpose of the Test Plan

The purpose of this test plan is to outline the approach, resources, and schedule for testing the Login Page and Dashboard of app.vwo.com. The goal is to ensure that both pages are functional, secure, user-friendly, and perform well across different environments and devices.

1.2 Scope of Testing

The scope includes testing the following components:

- Login Page:
- Email Address Field
- Password Field
- "Remember Me" Checkbox
- "Forgot Password" Link
- "Sign In" Button
- "Sign in using SSO" Option
- Error Messages

- Redirects
- Dashboard:
- Navigation Menu
- Widgets and Charts
- User Profile Section
- Notifications
- Search Functionality
- Logout Option

1.3 Objectives

- Validate the functionality of the login page and dashboard.
- Ensure both pages are secure against common vulnerabilities.
- Verify the usability and accessibility of both pages.
- Test the performance of both pages under different load conditions.
- Ensure compatibility across different browsers and devices.

2. Test Environments

2.1 Operating Systems

- Windows 10
- macOS
- Linux

2.2 Browsers

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Safari

2.3 Devices

- Desktop
- Laptop
- Tablet

- Smartphone (iOS and Android)

2.4 Network Conditions

- Wi-Fi
- Cellular
- Wired connections

3. Test Strategy

3.1 Functional Testing

- Login Page:
- Verify login with valid and invalid credentials.
- Test "Remember Me" functionality.
- Test "Forgot Password" functionality.
- Test "Sign in using SSO" option (if applicable).
- Dashboard:

- Verify navigation through the menu.
- Validate widgets and charts display correct data.
- Test user profile updates.
- Check notification functionality.
- Test search functionality.
- Verify logout functionality.

3.2 UI/UX Testing

- Login Page:
- Validate the layout and design.
- Check responsiveness across different screen sizes.
- Verify error messages and their placement.
- Dashboard:
- Validate the layout and design.
- Check responsiveness across different screen sizes.

- Verify the placement and functionality of widgets and charts.

3.3 Security Testing

- Login Page:
- Test for SQL injection vulnerabilities.
- Test for brute force attack prevention.
- Ensure password fields are masked.
- Verify SSL/TLS encryption.
- Dashboard:
- Test for unauthorized access.
- Verify session timeout functionality.
- Ensure sensitive data is not exposed.

3.4 Performance Testing

- Login Page:
    - Test response time under normal and peak load conditions.

    - Simulate multiple users logging in simultaneously.

- Dashboard:
    - Test response time under normal and peak load conditions.
    - Simulate multiple users accessing the dashboard simultaneously.

3.5 Cross-Browser and Cross-Device Testing

Ensure compatibility across all supported browsers and devices for both the login page and dashboard.

3.6 Accessibility Testing

- Login Page:
    - Verify compatibility with screen readers.
    - Check keyboard navigation and focus indicators.
    - Ensure proper contrast ratios for text and background.
- Dashboard:
    - Verify compatibility with screen readers.
    - Check keyboard navigation and focus indicators.

- Ensure proper contrast ratios for text and background.

4. Test Schedule

Task	**Start Date**	**End Date**
Test Plan Creation	Day 1	Day 2
Test Case Creation	Day 2	Day 4
Functional Testing	Day 5	Day 7
UI/UX Testing	Day 5	Day 7
Security Testing	Day 8	Day 9
Performance Testing	Day 10	Day 11
Cross-Browser/Device Testing	Day 10	Day 12
Accessibility Testing	Day 12	Day 13
Defect Reporting & Retesting	Day 14	Day 15
Test Summary Report	Day 14	Day 15

5. Test Deliverables

- **Test Plan:** Document outlining the scope, strategy, and schedule.

- **Test Cases:** Detailed test cases for each functionality of the login page and dashboard.

- **Defect Reports:** Detailed reports of defects found during testing.

- **Test Summary Report:** Summary of testing activities, results, and metrics.

6. Entry and Exit Criteria

6.1 Entry Criteria

- Requirements and design documents are available.
- Test environment is set up and ready for use.
- Test cases are reviewed and approved.

6.2 Exit Criteria

- All test cases have been executed.
- All critical and high-priority defects have been resolved.
- Test summary report is prepared and approved.

7. Tools and Technologies

- **Test Management:** JIRA or TestRail
- **Automation Tools:** Selenium or Cypress
- **Performance Testing:** JMeter or LoadRunner

- **Security Testing:** OWASP ZAP or Burp Suite

- **Accessibility Testing:** Axe or WAVE

8. Risks and Mitigations

Risk	**Mitigation**
Delays in test environment setup	Ensure the environment is ready before testing begins
Resource unavailability	Assign backup resources to avoid delays.
Incomplete or unclear requirements	Conduct regular meetings with stakeholders to clarify requirements.
Time constraints	Prioritize test cases based on risk and business impact.

9. Approvals

The following documents will require approval before proceeding to the next phase:

- Test Plan

- Test Cases

- Test Summary Report

10. Appendix

10.1 Glossary of Terms

- **SQL Injection:** A code injection technique used to attack data-driven applications.

- **Brute Force Attack:** A trial-and-error method used to obtain information such as a user password.

- **SSL/TLS:** Protocols used for securing communication over a computer network.

10.2 References

- Requirements Document for app.vwo.com Login Page and Dashboard

- Design Specifications for app.vwo.com Login Page and Dashboard