Test Plan for VWO Login Page

Created by: Sushma S

---

1. Objective

Ensure that the VWO login page delivers secure, fast, and intuitive user authentication. This plan validates all critical functionalities, performance, usability, and security aspects to support digital marketers, product managers, and developers.

---

2. Scope

Features to Test:

- **User Authentication:**
  - Valid login/logout
  - Error handling for invalid credentials
  - "Forgot Password" and account recovery flows
- **UI & Usability:**
  - Responsive design and layout consistency
  - Input field validations (masking, character limits)
  - Accessibility compliance (keyboard navigation, screen reader support)
- **Security:**
  - HTTPS enforcement, session management, and data encryption
  - Protection against injection attacks and XSS
- **Performance:**
  - Page load times under varying network conditions
  - Stress handling during peak access

---

3. Inclusions

- **Functional Testing:** Verification of login processes, error messages, and session termination.
- **Usability Testing:** Assessment of UI design, responsiveness, and user experience.
- **Security Testing:** Evaluation of encryption, authentication protocols, and vulnerability scans.
- **Performance Testing:** Load testing, response time measurement, and stress testing.

---

4. Exclusions

- Backend API performance (covered under separate API test plans).

- Post-login application features (e.g., dashboards, analytics).
- Administrative functionalities not exposed to end users.

---

5. Test Environments

Operating Systems:

- Windows 10/11, macOS (Monterey+), Ubuntu Linux

Browsers:

- Google Chrome (Latest 3 versions)
- Mozilla Firefox (Latest 3 versions)
- Microsoft Edge (Latest version)
- Safari (Latest version)

Devices:

- Desktop Computers & Laptops
- Tablets & Smartphones (iOS and Android)

Network Conditions:

- Wi-Fi, wired LAN, cellular (4G/5G)
- Simulated low bandwidth & high latency scenarios

Security Protocols:

- Multi-Factor Authentication (if enabled)
- Secure HTTPS connections and session timeouts

---

6. Defect Reporting Procedure

Identification:

- Monitor deviations in functionality, UI inconsistencies, slow responses, and security flaws.

Reporting:

- Capture screenshots/logs and detail reproduction steps.
- Assign severity (Critical, Major, Minor) and priority.
- Log defects in JIRA with clear descriptions and attachments.

Tracking:

- Update defect statuses and retest fixes until closure.

---

7. Test Strategy

Test Case Creation:

- Develop scenarios using equivalence partitioning, boundary value analysis, decision tables, and state transition testing.
- Incorporate exploratory and error guessing techniques to uncover edge cases.

Testing Phases:

1. **Smoke Testing:** Quick run-through of core functionalities (page load, login/logout).
2. **Detailed Functional Testing:** Step-by-step execution of all defined test cases.
3. **Regression Testing:** Automated scripts (e.g., Selenium) to ensure new changes don't break existing functionality.
4. **Security & Performance Testing:** Use tools (e.g., OWASP ZAP, JMeter) to assess vulnerabilities and response times.

Best Practices:

- Context-driven testing based on real user scenarios.
- Shift-left approach to catch defects early.
- End-to-end flow simulation to mimic actual user journeys.

---

8. Test Schedule

Task	Duration
Test Plan & Case Creation	3 Days
Test Environment Setup	1 Day
Smoke & Functional Testing	4 Days
Regression & Automation Run	2 Days
Security & Performance Testing	2 Days
Defect Resolution & Retest	3 Days
Test Summary Report	1 Day

---

9. Test Deliverables

- **Test Plan Document:** This document detailing the overall strategy.
- **Test Scenarios & Cases:** Detailed, executable test cases.
- **Defect Reports:** Logs from JIRA with screenshots and reproduction steps.
- **Automation Scripts:** (Where applicable) for regression testing.
- **Final Test Summary Report:** Coverage, defect statistics, and recommendations.

10. Entry and Exit Criteria

Entry Criteria:

- Finalized requirements and design documents are available.
- Test environment is configured and accessible.
- Test data (valid/invalid credentials) is prepared.

Exit Criteria:

- All critical and major test cases executed.
- All defects logged, resolved, and retested.
- Test summary report completed and approved by stakeholders.

---

11. Tools

- **Defect Tracking:** JIRA
- **Automation Testing:** Selenium/Cypress
- **Performance Testing:** JMeter
- **Security Testing:** OWASP ZAP (or similar)
- **Documentation:** Microsoft Word/Excel or Confluence
- **Debugging:** Browser Developer Tools and Snipping Tool

---

12. Risks and Mitigations

Risk	Mitigation Strategy
Unstable network or test environment	Use backup environments; simulate various network conditions.
Incomplete test data	Prepare synthetic data sets; verify credentials in advance.
Browser/version discrepancies	Regularly update browsers; run cross-browser tests in parallel.
Tight timelines	Prioritize high-impact test cases; allocate backup resources.

---

13. Approvals

- **Test Lead:** Sushma S
- **QA Manager:** Manager ABC
- **Product Manager:** Prod Man 123
- **Development Team:** Dev001