Test Strategy for Amazon.in Login Module

# 1. Introduction

This Test Strategy outlines the approach, methodology, and process for testing the Login Module of Amazon.in. The purpose of the strategy is to ensure that the login module functions as expected under all possible conditions, maintaining both functional integrity and security.

# 2. Objectives

The primary objectives of testing the Login Module are:  
- Ensure Correct Functionality: Verify that users can log in successfully with valid credentials and that errors are appropriately displayed for invalid credentials.  
- Verify Security: Ensure that the login mechanism is secure against common attacks such as SQL injection, XSS, brute force, etc.  
- Cross-Browser & Device Compatibility: Ensure the login feature works across different browsers and devices (desktop, mobile, tablets).  
- Performance & Scalability: Ensure the login module can handle high traffic volumes during peak periods (e.g., Black Friday, Prime Day).

# 3. Scope of Testing

The scope includes testing all components associated with the Login Module:  
- Login with Email, Mobile Number, and OTP  
- Password handling  
- Error messaging and validation  
- Cross-platform compatibility  
- Security testing for threats like SQL injection, XSS, etc.  
- Session Management: Timeouts, CAPTCHA, or Rate-Limiting for repeated failed login attempts  
- UI/UX: Responsive design and user-friendly experience  
  
The following are out of scope:  
- Account creation and registration (handled in separate modules)  
- Payments and transactions after login (handled separately in checkout module)

# 4. Testing Approach

Testing will be carried out following a comprehensive, risk-based approach, which includes the following techniques:  
- Manual Testing: For complex scenarios and exploratory tests where automation isn't feasible.  
- Automated Testing: For regression testing, smoke testing, and repetitive test cases that are executed frequently.  
- Performance Testing: To validate the load, stress, and scalability of the login system.  
- Security Testing: Penetration testing and vulnerability scanning to safeguard the system against potential threats.  
- Usability Testing: To ensure the login flow is intuitive, smooth, and user-friendly.  
- Cross-Platform Testing: Verifying compatibility across different browsers and devices.

# 5. Test Levels

The following test levels will be executed to ensure complete coverage:  
- Unit Testing: Performed by developers to test individual components like login validation logic and security features.  
- Integration Testing: Testing the integration of the login module with other modules (e.g., user account, session management).  
- System Testing: Comprehensive end-to-end testing of the login module.  
- Regression Testing: To validate that existing functionality is not broken after new updates or bug fixes.  
- Acceptance Testing: Conducted by the Product team to validate whether the login module meets the business requirements.

# 6. Test Phases

Test Phases include:  
- Test Planning: Define the test scope, objectives, timelines, resources, tools, and risks.  
- Test Design: Develop detailed test cases, including both positive and negative scenarios. Develop automated test scripts for regression and smoke testing.  
- Test Execution: Execute manual and automated test cases across all test environments.  
- Defect Reporting: Log, track, and prioritize defects based on severity and impact.  
- Test Closure: Prepare the test summary report, including defect trends, test coverage, and overall test execution results.

# 7. Resources

The following resources will be utilized during testing:  
- Testers: A team of 3-4 manual testers and 2-3 automation engineers.  
- Test Environment: The testing will be conducted in the development/staging environments, closely simulating production conditions.  
- Test Tools:   
 - Selenium or Cypress for automated UI testing.  
 - JMeter or LoadRunner for performance testing.  
 - OWASP ZAP or Burp Suite for security testing.  
 - TestRail or Jira for test case management and defect tracking.

# 8. Test Data

Test data will include:  
- Valid Test Data: Real user credentials (email, password, phone number) for valid login scenarios.  
- Invalid Test Data: Invalid email formats, incorrect passwords, empty fields, SQL injection attempts, etc.  
- Boundary Test Data: Long passwords, extremely short emails, very large number of login attempts.  
- Security Test Data: Use of malicious scripts, special characters, invalid OTPs, etc.

# 9. Test Deliverables

The following deliverables will be produced during and after the testing phase:  
- Test Plan Document: Defines the approach and scope of testing.  
- Test Cases: Detailed positive and negative test cases.  
- Test Execution Reports: A summary of executed tests, results, and defect reports.  
- Defect Reports: List of defects identified, with severity levels and status updates.  
- Test Summary Report: A final report covering the overall testing process, results, defect trends, and recommendations.

# 10. Risk and Mitigation

Identified Risks and Mitigation strategies:  
- Risk: Delays in the development of features may impact the testing timeline.  
 Mitigation: Early involvement in development and thorough communication.  
- Risk: Insufficient test coverage on cross-browser and cross-device testing.  
 Mitigation: Use of browser testing tools and real device testing (e.g., BrowserStack).  
- Risk: Insufficient load handling during peak times (e.g., Prime Day).  
 Mitigation: Performance testing to simulate high user load and peak traffic.  
- Risk: Security vulnerabilities in login and password handling.  
 Mitigation: Continuous security testing and code review by security experts.

# 11. Entry and Exit Criteria

Entry Criteria:  
- Test environment is ready and stable.  
- Test cases are reviewed and approved.  
- Required test data is available.  
  
Exit Criteria:  
- All high-priority test cases are executed.  
- All critical defects are resolved, or mitigated with a plan.  
- Test summary report is delivered, indicating the readiness of the product for release.

# 12. Conclusion

This Test Strategy ensures a comprehensive and structured approach to testing the Login Module of Amazon.in. It aligns with business goals and customer needs, focusing on quality, security, and performance to deliver a seamless and reliable user login experience.