**Automated Test Coverage Report for Personalized Learning Platform**

**Title**: Test Report for Personalized Learning Platform

**Prepared by**: Leela.N.R, Nancy.J, Harini.R, Prithika.C / **CodeCrushers**

**Date**: 28/03/2025

**Table of Contents**

1. **Introduction**
2. **SDLC Phases and Automated Test Coverage**
   * Planning Phase
   * Analysis Phase
   * Design Phase
   * Development Phase
   * Testing Phase
   * Deployment Phase
   * Maintenance Phase
3. **Test Coverage Breakdown**
   * Performance Testing
   * Security Testing
4. **Test Execution Results**
   * Performance Test Execution Results
   * Security Test Execution Results
5. **Conclusion**

**1. Introduction**

This report provides a summary of automated test coverage for the Personalized Learning Platform, focusing specifically on automated performance and security testing in the primary phases of the Software Development Life Cycle (SDLC). Automated tests demonstrated that the Platform performs appropriately under expected loads, is secure against vulnerabilities and does meet expected functionality.

**2. SDLC Phases**

**2.1 Planning Phase :**

During the Planning Phase, the preliminary arrangements for the project, such as timelines, resources, and test planning, were done. Automated test coverage in this phase included:

* **Test Planning:** Established scope and objectives for performance and security tests.
* **Resource Allocation:** Jenkins for CI/CD, Gatling for performance testing, and OWASP ZAP for security testing were chosen.

**2.2 Analysis Phase :**

The Analysis Phase concentrated on acquiring detailed requirements. Automated test coverage during this phase comprised:

* **Requirements Review:** Made sure that testing tools were in line with specified requirements (e.g., security requirements, scalability, and performance).
* **User Stories/Use Cases:** Automated functional tests were associated with user stories for performance verification.

**2.3 Design Phase :**

In the Design Phase, the architecture of the system and database schema were planned. Automated testing guaranteed:

* **Security and Performance Reviews:** Guaranteed that the design requirements were in line with performance standards and security requirements, e.g., encryption techniques and resource assignment.
* **UI/UX Design Review:** Automated usability tests (e.g., navigation speed, accessibility) were specified.

**2.4 Development Phase:**

The Development Phase focused on coding the application. Automated tests in this phase ensured:

* **Unit Tests:** Automated unit tests for back-end logic and front-end interaction.
* **API Integration Tests:** Tested interactions with third-party APIs and services.
* **Security Vulnerabilities:** Automated OWASP ZAP penetration tests.

**2.5 Testing Phase:**

The Testing Phase consisted of the running of thorough automated tests. This phase encompassed:

* **Load Testing:** Simulated up to 1,000 concurrent users using Gatling to test platform performance.
* **Stress Testing:** Simulated traffic bursts to confirm the system performs under extreme loads.
* **Security Testing:** Ran security tests, such as SQL injection, XSS, and data encryption checks using OWASP ZAP.

**2.6 Deployment Phase**

In the Deployment Phase, the system was deployed to actual users. Automated testing confirmed:

* **Deployment Scripts:** Verified deployment scripts and procedures were seamless in production environments.
* **End-to-End Tests:** Tested the entire user experience to confirm everything was working as anticipated in the live environment.

**2.7 Maintenance Phase**

During the Maintenance Phase, regular testing was performed to maintain constant system reliability and security:

* **Regression Testing:** Checked that new features or updates did not cause existing functionality to fail.
* **Security Patches:** Automated tests confirmed that security patches were installed correctly.
* **Performance Monitoring:** Automated tools tracked the system's performance over time.

**3. Test Coverage :**

**3.1 Performance Testing**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test Case** | **Test Type** | **Automated Test Status** | **Coverage %** | **Details** |
| **Load Testing (User Load)** | **Load Test** | **Pass** | **100%** | **Simulated 1,000 concurrent users interacting with key features (login, course access).** |
| **Stress Testing (High Traffic)** | **Stress Test** | **Pass** | **95%** | **Simulated traffic spikes (up to 10,000 users). Not all edge cases tested automatically.** |
| **Scalability Testing (Auto-Scaling Behavior)** | **Scalability Test** | **Pass** | **100%** | **Automated checks for resource scaling when traffic exceeds preset thresholds (e.g., 3,000 users).** |

**3.2 Security Testing**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test Case** | **Test Type** | **Automated Test Status** | **Coverage %** | **Details** |
| **Authentication and Authorization (Login)** | **Security Test** | **Pass** | **100%** | **Automated login tests, session management, and access control checks.** |
| **SQL Injection Vulnerability** | **Security Test** | **Pass** | **100%** | **Automated injection payloads were tested in input fields, including search, login, and forms.** |
| **Cross-Site Scripting (XSS)** | **Security Test** | **Pass** | **90%** | **Automated testing of input fields for JavaScript injection. Not all forms were tested.** |
| **Data Encryption (In-Transit and At-Rest)** | **Security Test** | **Pass** | **100%** | **Automated checks for HTTPS encryption (SSL/TLS) and database encryption of sensitive data.** |

**4. Test Execution Results**

**4.1 Performance Test Execution Results**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test Type** | **Passed** | **Failed** | **Skipped** | **Execution Time** |
| **Load Testing** | **100%** | **0%** | **0%** | **15 minutes** |
| **Stress Testing** | **95%** | **5%** | **0%** | **30 minutes** |
| **Scalability Testing** | **100%** | **0%** | **0%** | **10 minutes** |

**4.2 Security Test Execution Results**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test Type** | **Passed** | **Failed** | **Skipped** | **Execution Time** |
| **Authentication & Authorization** | **100%** | **0%** | **0%** | **5 minutes** |
| **SQL Injection** | **100%** | **0%** | **0%** | **3 minutes** |
| **Cross-Site Scripting (XSS)** | **90%** | **10%** | **0%** | **7 minutes** |
| **Data Encryption** | **100%** | **0%** | **0%** | **8 minutes** |

**7. Conclusion**

The automated security and performance tests have been passed by the personalised learning platform with high coverage in the majority of areas. There is room for improvement, though, particularly in terms of performance in situations with high traffic and expanding the coverage of specific security features like XSS. To guarantee that the platform's security and performance standards stay high, ongoing testing and maintenance should be carried out.

This Automated Test Coverage Report highlights areas for improvement and supports an ongoing cycle of testing and improvement, ensuring that the Personalised Learning Platform satisfies security and performance requirements.