**Manual Testing Report – Payment Gateway Project**

**1. Project Overview**

This project involves manual testing of the **Payment Gateway Application** provided by Guru99:  
🔗 [https://demo.guru99.com/payment-gateway/index.php](https://demo.guru99.com/payment-gateway/index.php?utm_source=chatgpt.com)

The main objective of testing this application is to ensure that:

* Card payment works correctly with valid data.
* Invalid inputs (wrong card, expired card, invalid CVV) are properly handled.
* Amount field accepts only valid numeric inputs.
* Order IDs are generated uniquely for each transaction.
* Transaction history is maintained correctly.
* Security measures like session expiry, logout, and CVV masking are functional.

**2. Test Plan**

* **Application Name:** Guru99 Payment Gateway
* **Testing Type:** Manual Testing (Functional, UI, Error Handling, Security)
* **Environment:** Browsers – Chrome, Firefox, Edge, Safari
* **Tools Used:** Excel/Google Sheets, Screenshot tool
* **In Scope:**
  + Card Payment
  + Amount Validation
  + CVV & Expiry Validation
  + Transaction History
  + Security & Error Handling
* **Out of Scope:**
  + Real banking integration
  + Admin dashboard
* **Entry Criteria:**
  + Application is accessible
  + Test data for valid/invalid cards available
* **Exit Criteria:**
  + All major test cases executed
  + Critical defects fixed or logged
* **Deliverables:**
  + Test Scenarios
  + Test Cases
  + Bug Report
  + Test Summary Report

The test plan defines the overall scope and approach for manual testing of the Guru99 Payment Gateway application. The application will be tested across multiple browsers such as Chrome, Firefox, Edge, and Safari to ensure cross-platform compatibility. Manual testing will cover functional, UI, error handling, and security aspects of the system. Tools like Excel or Google Sheets will be used for tracking test cases and results, along with screenshots for defect reporting. The in-scope features include card payments, amount validation, CVV and expiry date checks, transaction history, and essential security measures. Features like real banking integration and the admin dashboard are considered out of scope for this testing cycle. Entry criteria specify that the application must be accessible and valid test data must be available before execution. Exit criteria state that all major test cases should be executed, and critical defects must either be fixed or logged. Deliverables from this testing process will include detailed test scenarios, structured test cases, a bug report, and a test summary report. This ensures comprehensive coverage and clear documentation of testing outcomes.

|  |  |
| --- | --- |
| **Field** | **Details** |
| **Project Name** | E-Commerce Site Manual Testing |
| **Application URL** | <http://automationpractice.com/index.php> |
| **Tested By** | Ajay A |
| **Testing Type** | Manual Testing (Functional, UI, Regression) |
| **Test Environment** | Web Browsers (Chrome, Firefox, Edge) |
| **Tools Used** | Browser DevTools, Excel/Google Sheets (for test cases), Screenshot tools |
| **Start Date** | 03-Sep-2025 |
| **End Date (est.)** | 04-Sep-2025 |
| **In-Scope Modules** | Login, Registration, Search, Cart, Checkout, Contact Form |
| **Out of Scope** | Payment gateway (not real-time), Admin Panel |
| **Entry Criteria** | Application accessible in browser |
| **Exit Criteria** | All critical test cases executed and major bugs closed |
| **Deliverables** | Test Cases, Bug Report, Test Summary Report |

**3. Test Scenarios**

|  |  |
| --- | --- |
| Scenario ID | Description |
| TS01 | Verify successful payment with valid card details |
| TS02 | Verify error messages for invalid/expired cards |
| TS03 | Verify CVV and expiry field validation |
| TS04 | Verify amount field validation (blank, negative, alphanumeric, boundary values) |
| TS05 | Verify order ID generation for successful payments |
| TS06 | Verify transaction history displays correct details |
| TS07 | Verify security (CVV hidden, session timeout, logout) |
| TS08 | Verify UI alignment and responsiveness |
| TS09 | Verify error handling under invalid inputs |
| TS10 | Verify system response time under load |

**4. Test Cases**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TC ID | Description | Test Steps | Test Data | Expected Result |
| TC01 | Payment with valid card | Enter valid card → Submit | Card: 4111111111111111, Exp: 12/26, CVV: 123, Amount: 500 | Payment successful, Order ID generated |
| TC02 | Invalid card number | Enter invalid card → Submit | Card: 1234567890123456 | Error: “Invalid Card Number” |
| TC03 | Expired card | Enter expired card → Submit | Card Exp: 01/20 | Error: “Card Expired” |
| TC04 | Blank CVV | Leave CVV blank → Submit | CVV: "" | Error: “CVV Required” |
| TC05 | Blank amount field | Leave amount blank → Submit | Amount: "" | Error: “Amount Required” |
| TC06 | Invalid characters in amount | Enter alphabets in amount field | Amount: abc | Error: “Invalid Amount” |
| TC07 | Negative amount | Enter negative value | Amount: -100 | Error: “Invalid Amount” |
| TC08 | Minimum amount boundary | Enter minimum valid amount | Amount: 1 | Payment successful |
| TC09 | Maximum amount boundary | Enter maximum valid amount | Amount: 100000 | Payment processed or error shown |
| TC10 | CVV with <3 digits | Enter 2-digit CVV | CVV: 12 | Error: “Invalid CVV” |
| TC11 | CVV with >3 digits | Enter 5-digit CVV | CVV: 12345 | Error: “Invalid CVV” |
| TC12 | Invalid expiry date | Enter invalid date | Exp: 13/30 | Error: “Invalid Expiry Date” |
| TC13 | Unique order ID check | Make multiple payments | 100, 200 | Unique IDs generated |
| TC14 | Transaction history check | Complete payment → Open history | Order ID: 12345 | Correct details shown |
| TC15 | Transaction history amount | Make a payment of 500 | Amount: 500 | Amount reflected correctly |
| TC16 | CVV hidden | Enter CVV | 123 | CVV masked (•••) |
| TC17 | Session timeout | Stay idle for 10 mins → Submit | N/A | Redirected to login |
| TC18 | Logout clears session | Logout → Use back button | N/A | Redirected to login |
| TC19 | Invalid inputs in all fields | Enter random values | Card: abcd, CVV: xyz | Proper error messages shown |
| TC20 | Load test with multiple users | Simulate multiple payments | 50 users | Response time < 3 sec |

**5. Bug Report**

|  |  |  |  |
| --- | --- | --- | --- |
| **Bug ID** | **Description** | **Severity** | **Status** |
| BUG01 | Expired card accepted | Critical | Open |
| BUG02 | Negative amount accepted | Major | Open |
| BUG03 | CVV accepts more than 3 digits | Major | Open |
| BUG04 | Invalid expiry date (13/30) accepted | Major | Open |
| BUG05 | UI fields overlap in mobile view | Minor | Open |
| BUG06 | Session does not expire after timeout | Critical | Open |

**6. Test Summary Report**

* **Testing Duration:** 3 days (04–Sep–2025 to 06–Sep–2025)
* **Total Test Cases:** 20
* **Passed:** 14
* **Failed:** 6
* **Blocked:** 0

The testing activity was conducted over a duration of three days, from 04–Sep–2025 to 06–Sep–2025. A total of 20 test cases were designed and executed to validate the functionality, usability, and performance of the application. Out of these, 14 test cases passed successfully, indicating that the majority of the core features are working as expected. Six test cases failed, highlighting certain functional gaps and defects that need immediate attention from the development team. No test cases were blocked, which shows that the test environment and prerequisites were properly configured. The failures mainly relate to edge scenarios and integration issues, which can be resolved with targeted fixes. The overall pass percentage indicates a reasonably stable product, though improvements are required before release. The test coverage was adequate and ensured validation across critical modules. The testing team has documented the defects and shared them for resolution. In conclusion, the system is partially stable but requires further defect fixes and re-testing before moving to production.

**Defect Statistics:**

* Total Defects: 6
* Critical: 2 | Major: 3 | Minor: 1
* Status – Open: 6 | Closed: 0

During the testing phase, a total of six defects were identified and reported. Out of these, two defects were categorized as critical, directly impacting the core functionality of the application. Three defects were classified as major, affecting important features but not causing a complete system failure. One defect was marked as minor, having a low impact and limited effect on the overall system performance. At the time of reporting, all six defects remain in the open status, with none marked as closed. This indicates that the defects have been successfully captured but are still pending resolution from the development team. The presence of critical defects emphasizes the need for urgent fixes before the system can move forward. Major defects also require attention to ensure smooth user experience and prevent functionality breakdowns. The minor defect, although less severe, should also be resolved to maintain overall quality. The defect statistics provide clear insight into the stability of the system and help prioritize defect fixing activities. Overall, the data highlights the importance of immediate corrective actions and re-testing efforts.

**Observations:**

* Expired/invalid card validation weak.
* Amount and CVV validation need improvement.
* Session timeout not functional.
* UI layout issues on mobile view.

During the testing process, several key issues were observed that impact both functionality and user experience. The validation for expired and invalid cards was found to be weak, allowing certain invalid inputs to bypass checks. Similarly, the amount and CVV fields require stronger validation to prevent incorrect or fraudulent data entry. Another major concern is that the session timeout feature is not functioning, which poses a potential security risk for unattended sessions. In addition, UI layout issues were identified on mobile devices, leading to poor responsiveness and usability challenges. These issues collectively reduce the overall reliability and security of the system. Strengthening input validations will help safeguard against fraud and data inconsistencies. Fixing the session timeout problem is critical to ensuring user account protection. Addressing mobile view layout problems will enhance the customer experience across platforms. The defects have been documented and prioritized for development fixes. Overall, these issues must be resolved to achieve a secure, user-friendly, and production-ready payment system.

**Conclusion:**  
The overall testing results indicate that the core payment flow is functioning correctly when valid inputs are provided. This confirms that the primary transaction process is stable under normal conditions. However, multiple critical issues related to validation and security were identified during testing. These defects pose significant risks if left unresolved, as they may lead to data breaches, unauthorized access, or financial inconsistencies. Given the sensitivity of payment systems, such vulnerabilities must be addressed on priority. The presence of these defects suggests that while the functional backbone is strong, the application is not yet production-ready. Additional rounds of regression and security testing will be required once fixes are implemented. Only after closing all critical and major defects can the system be considered safe for deployment. The testing team recommends delaying the release until these issues are resolved. In conclusion, the product shows promise but needs immediate defect resolution to ensure reliability, security, and compliance.