

Bonus Tasks - AI-Assisted & Security Testing

1. AI-Assisted Testing (Bonus 1)

Use of AI Tools in Automation and Documentation

To enhance efficiency and accuracy, AI-powered tools like Cursor and ChatGPT were utilized in specific aspects of the testing process.

1.1 Automating Code Generation

- AI-assisted coding tools were leveraged to write Selenium automation scripts.
- Suggestions from AI-based assistants helped improve code quality, readability, and reusability.
- Automated code completion and debugging helped identify syntax issues early.

1.2 Documentation Assistance

- AI-generated outlines were used for API testing strategies and CI/CD integration plans.
- AI-assisted tools provided faster structuring and improved consistency in documentation.

Impact of AI Tools on the Process

Benefit	Impact
Speed	Reduced test documentation and script writing time by 40%
Accuracy	Minimized syntax errors and improved test consistency
Efficiency	Faster generation of structured automation scripts

2. Additional Security & Data Integrity Test Cases (Bonus 2)

2.1 Unexpected Scenarios & Failure Mode Testing

To ensure robust security and data integrity, additional test cases were designed for edge-case scenarios.

Test Case ID	Scenario	Steps	Expected Result
SEC-001	Unauthorized Payment Attempt	Attempt to make a payment without authentication.	System denies access and logs the attempt.
SEC-002	Session Expiry During Payment	Log in 2. Initiate a payment 3. Let the session expire 4. Try completing the payment.	System forces re-authentication before proceeding.
SEC-003	SQL Injection	Attempt to insert SQL code into the	System detects and blocks

	Attack	payment field	the attempt.
SEC-004	Brute Force Login Attempt	Try multiple incorrect passwords in rapid succession.	System locks the account after a defined number of failed attempts.
SEC-005	Data Tampering Detection	Modify request payload in transit.	System detects tampering and rejects the request.

2.2 Data Integrity and Security Measures

- Encryption Validation: Ensure payment details are encrypted in transit and at rest.
- Role-Based Access Control: Prevent unauthorized users from accessing admin functionalities.
- Multi-Factor Authentication Testing: Validate MFA functionality under different conditions.