

Test Summary Report

Project: E-Commerce Web Application QA Testing

Application Under Test: <http://automationpractice.multiformis.com>

Test Cycle: Functional, Security, Accessibility, Performance & Compatibility

Tested Modules: Registration, Login, Product Search

Test Execution Type: Manual (with security and accessibility tooling where applicable)

Prepared By: QA Team

Document Version: 1.0

1. Executive Summary

This test cycle focused on validating the **Registration**, **Login**, and **Product Search** features of the e-commerce web application. A comprehensive set of functional, security, usability, accessibility, performance, and compatibility test cases were executed across supported browsers and devices.

Overall, **core functionality is partially stable**, but the application **does not meet production-readiness criteria** due to multiple **high-risk security and functional defects**, particularly around authentication security, HTTPS enforcement, password policies, and search reliability.

2. Test Execution Overview

| Metric | Count |
|---------------------------|-------|
| Total Test Cases Executed | 95 |
| Passed | 74 |
| Failed | 13 |
| Blocked | 8 |
| Not Applicable | 2 |
| Pass Rate | ~78% |

3. Module-Wise Summary

3.1 Login Module

Status: **✗ High Risk – Not Production Ready**

Key Observations:

- Core login functionality works correctly for valid credentials.
- Accessibility basics (keyboard navigation) are mostly supported.
- **Critical security gaps were identified.**

Major Issues Identified:

- **✗ No brute-force protection** – unlimited failed login attempts allowed.
- **✗ HTTPS not enforced** – all authentication traffic occurs over HTTP.
- **✗ Logout does not invalidate session properly** – browser back button restores authenticated state.
- **✗ Missing Caps Lock warning** (usability issue).

Blocked Areas:

- Secure cookie flags (HttpOnly, Secure, SameSite).
- Session regeneration after login.
- Screen reader error announcements.
- Backend error handling under 5xx/timeout scenarios.

Overall Login Risk Level: **High**

3.2 Registration Module

Status: **✗ High Risk – Security & Validation Issues**

Key Observations:

- Registration flow works across browsers and devices.
- Accessibility and usability are generally strong.
- **Validation and security controls are insufficient.**

Major Issues Identified:

- **✗ Weak passwords accepted** (e.g., 123, password).
- **✗ Invalid DOB values accepted** (future and unrealistic dates).
- **✗ HTTPS not enforced during registration.**
- **✗ No abuse prevention** (rate limiting / CAPTCHA).

Strengths:

- Duplicate email prevention works.
- Autofill, keyboard navigation, and screen reader support are solid.

- Unicode and special character handling is correct.

Overall Registration Risk Level: High

3.3 Product Search Module

Status:  Medium Risk – Functional Gaps

Key Observations:

- Search is stable across browsers and devices.
- Performance is acceptable under normal load.
- Accessibility support is good.

Major Issues Identified:

-  **Sorting (price low→high / high→low) not functional.**
-  **Out-of-stock items not filtered correctly.**
-  Multi-keyword search relevance issues.
-  Add-to-cart from search results not integrated.

Blocked / Limited Coverage:

- Sort persistence across pagination (insufficient data).
- Invalid price range validation (not testable).
- Large catalog edge cases.

Overall Search Risk Level: Medium

4. Defect Summary

Defects by Severity

| Severity | Count |
|----------|-------|
| Critical | 3 |
| High | 4 |
| Medium | 5 |
| Low | 1 |

Critical / High Impact Defects

- No HTTPS enforcement (Login & Registration)
- No brute-force protection
- Weak password policy
- Session not invalidated on logout
- Broken search sorting
- Invalid DOB accepted during registration

All critical and high-severity defects have been logged in **JIRA** with reproducible steps and evidence.

5. Blockers & Limitations

Some security scenarios could not be fully validated due to environment/tooling limitations:

- Cookie replay and abuse-prevention testing require **Charles Proxy** or equivalent.
 - Backend fault injection (5xx responses) was not available.
 - Insufficient catalog data limited pagination and sorting persistence testing.
-

6. Overall Quality Assessment

| Area | Status |
|----------------------|--------------|
| Functional Stability | ⚠ Partial |
| Security | ✗ Poor |
| Accessibility | ✓ Good |
| Performance | ✓ Acceptable |
| Compatibility | ✓ Good |

7. Release Recommendation

🚫 **DO NOT RELEASE TO PRODUCTION**

Reasons:

- Severe authentication and transport-level security gaps.
- Weak password enforcement.
- Broken core search functionality (sorting & stock handling).
- Session management vulnerabilities.

8. Recommended Next Steps

1. Enforce **HTTPS** across the entire application.
 2. Implement **brute-force protection** and login throttling.
 3. Enforce **strong password policy** during registration.
 4. Fix **session invalidation on logout**.
 5. Repair **search sorting and stock filtering logic**.
 6. Re-run **security regression testing** after fixes.
 7. Conduct a **full re-test of blocked security cases**.
-