Release Readiness Report

ShopLab v1.1 · fixed

06 Nov 2026, 09:46 AM IST
Prepared by Sharan L · R2C method

Demonstration report generated automatically from real test runs against ShopLab, a demo application with synthetic data. Not a client engagement.

Go

Ready to release

- No open defects above Low; every requirement passes

18/18	0 · 0 · 0 · 0	70/70	3.1 ms
REQUIREMENTS PASSING	OPEN DEFECTS C · H · M · L	AUTOMATED CHECKS PASSING · 1 SKIPPED BY DESIGN	P95 AT 50 USERS

Executive summary

ShopLab v1.1 can be released. **All 18 requirements pass**, all 14 previously found defects are verified fixed, and no business risk remains open. 4 residual risks are listed below with recommended mitigations; none of them blocks this release.

Business risk register

ID	RISK	LEVEL	STATUS	FAILING REQUIREMENTS
R1	**Customers are charged the wrong amount** Lost revenue, refunds and chargebacks; loss of trust at the point of payment.	High	Mitigated	—
R2	**Customer data is exposed to other users or attackers** Privacy breach, regulatory exposure (GDPR / DPDP) and reputational damage.	High	Mitigated	—
R3	**Accounts are taken over by password guessing** Fraudulent orders on real customers' accounts.	High	Mitigated	—
R5	**The shop slows down at peak traffic** Abandoned carts during campaigns and launches.	High	Mitigated	—
R4	**Stock is oversold** Orders that cannot be fulfilled, cancellations and support cost.	Medium	Mitigated	—

R6	**Phone and assistive-technology users cannot buy** Lost sales and accessibility-law exposure (e.g. European Accessibility Act).	Medium	Mitigated	—
R7	**Shoppers see a different price from the one charged** Complaints and pricing disputes.	Low	Mitigated	—

Requirements traceability

ID	REQUIREMENT	TESTS	STATUS
REQ-01	Customers can sign in with valid credentials	5	pass
REQ-02	Accounts lock after 5 failed sign-in attempts	1	pass
REQ-03	Sign-up validates email format and password strength	12	pass
REQ-04	Product catalogue and search return correct results	4	pass
REQ-05	Listed prices match the system of record	2	pass
REQ-06	Cart quantities are whole numbers from 1 to 10	10	pass
REQ-07	Totals are correct and 8% tax is rounded to the cent	3	pass
REQ-08	A discount code can be used once per order	3	pass
REQ-09	Checkout validates shipping details and places the order	8	pass
REQ-10	Customers can only see their own orders and carts	3	pass
REQ-11	Stock is never oversold, even with simultaneous orders	3	pass
REQ-12	Order data is consistent in the database	2	pass
REQ-13	Product browsing stays under 800 ms (95th percentile) with 50 users	1	pass
REQ-14	Checkout is usable on phones	3	pass
REQ-15	Pages meet WCAG 2.2 AA (labels, contrast, keyboard)	2	pass
REQ-16	Errors are handled safely without exposing internals	3	pass
REQ-17	Security headers and secure session cookies are set	4	pass
REQ-18	User input cannot inject code (SQL or script)	2	pass

Performance

MEASURE (50 USERS, 30 S)	RESULT	TARGET	STATUS
95th percentile response	3.1 ms	< 800 ms	pass
Average response	1.3 ms	—	
Throughput	198.3 requests/s	—	
Error rate	0.00%	< 1%	pass

Test execution

SUITE	PASSED	FAILED	SKIPPED
API + database (pytest)	58	0	0
Browser (Playwright)	11	0	1
Load (k6)	1	0	0

Defects verified fixed

ID	SEVERITY	DEFECT	STATUS
D06	Critical	Any user can read another user's order	verified
D01	High	Account never locks after repeated wrong passwords	verified
D03	High	Same discount code can be applied twice	verified
D05	High	Quantity accepts 0 and negative numbers	verified
D08	High	Stock goes negative under concurrent orders	verified
D14	High	Customer name rendered as HTML (stored XSS)	verified
D02	Medium	Sign-up accepts invalid email and 1-character passwords	verified
D04	Medium	Tax truncated instead of rounded	verified
D07	Medium	Malformed JSON returns 500 with stack trace	verified
D09	Medium	Listed price differs from database	verified
D10	Medium	Product list slow under load	verified
D11	Medium	Place order button off-screen on phones	verified
D12	Medium	Unlabelled fields and low-contrast prices	verified
D13	Low	Missing security headers	verified

Residual risks and recommended mitigations

RISK	SEVERITY	MITIGATION
Passwords use a fast salted hash suited to a demo, not production	Medium	Move to Argon2 or scrypt before handling real customer accounts.
No rate limiting on the sign-in and order APIs	Medium	Add per-IP and per-account rate limits at the edge or in the app.
ShopLab browser tests run on Chromium only	Low	Add Firefox and WebKit projects (already used in the main Playwright suite).
Load measured on a 2-4 core CI runner, not production-like hardware	Low	Repeat the k6 profiles on a staging environment sized like production.

Scope, method and verdict rules

Method (R2C — Risk-to-Confidence): requirements and risks identified → tests designed per risk → automated execution on every change → evidence captured (screenshots, traces, logs) → defects analysed → fixes verified → release decision.

Tools: pytest + requests + jsonschema (API and SQL checks), Playwright + axe-core (browser, phone and WCAG 2.2), k6 (load), GitHub Actions (execution on every change).

Verdict rules: No-Go — any open Critical or High defect, or a failing performance or security requirement. **Go with risks** — only Medium or Low defects open. **Go** — no open defects above Low and every requirement passes.

Source run: local run · Generated by release-report/aggregate.py and render.py · ShopLab is a demonstration application built by Sharan L.