This report has been replaced by QR-26-00113 — a newer version of the product was reviewed.



VIBE96 QUALITY REPORT

Haven — Small Hotel Front Desk & Room Booking

Front-desk software for independent hotels with 5–50 rooms, managing reservations, check-ins and guest payments.

Product ID	**B0183-36274**
Builder	**Redowan Ahmed Farhan**
Version reviewed	**1.0.0 · released 26 Oct 2026**
Stack	**React 19.3.1 + Vite 8.0.0 · JavaScript (Node.js 24+) · SQLite bundled with Node.js 24+; optional Neon PostgreSQL 17 (verified)**
Built with	**OpenAI Codex**
Review period	**24 Oct 2026 – 26 Oct 2026**

94 / 100

Passed with 2 warnings

Pass mark 75 and no failing check.

Scores

Security	96
Code structure	82
Docs & completeness	87
Dependency health	95
Build & deploy	95

✓ **AI code audit**
6 checks · 24 Oct 2026

✓ **Installed & run**
26 Oct 2026

✓ **Demo vs delivered**
26 Oct 2026

✓ **Final sign-off**
26 Oct 2026

At a glance

✓ Installed and run from the delivered code — 8 of 8 checks answered yes.

✓ Live demo compared with the delivered code — 7 of 7 checks answered yes.

! 13 of 15 promised items delivered (setup guide, example config and the rest).

✓ Security scored 96/100 with no failing check.

! 2 open warnings — explained in part 1.

Check this report is genuine. Scan the code or open vibe96.com/report/QR-26-00066. The online copy always shows the latest status.

PART 1

AI code audit

The full source archive was read by our AI auditor against each check. It reads the code — it does not run it; running it is part 2.

CHECK	WHAT WE FOUND	SCORE	RESULT
Secrets & credentials	All credential references are either placeholders ([hidden], SESSION_SECRET=, your-verified-domain.com) or environment variable instructions. The regex candidates flagged documentation patterns and Docker Compose variable syntax, not actual secrets. No committed .env files, API keys, or connection strings with real values were found.	100	Pass
Dependency vulnerabilities	All production dependencies are pinned in package-lock.json with no known critical vulnerabilities. React 19.3.1, Vite 8.0.0, and other packages are current stable releases. Minor outdated devDependencies (Playwright 1.64.1 vs 1.49+, ESLint 10.13.0 vs 10.18+) are acceptable for a recent project.	95	Pass
Authorisation & access control	All data-changing endpoints require signed admin session with proper bcrypt password hashing. Login is rate-limited. The only gap is that authenticated users can read any guest record by ID without ownership checks, though this is a single-admin system where all staff share one password.	95	Warning
Database access rules	SQL queries use parameterized statements throughout, preventing injection. Schema has proper foreign keys and constraints. However, foreign key columns lack explicit indexes in SQLite/Postgres schemas, and one DELETE statement in server.mjs lacks a WHERE clause (though it's scoped by table design). These are performance and safety warnings, not critical flaws.	92	Warning
Code structure & duplication	The project demonstrates good separation of concerns with clear module boundaries: frontend components, server routes, storage layer, and tests are appropriately isolated. Files are reasonably sized and focused. Minor issues include duplicated documentation files across directories and some configuration duplication in .env.example files, which do not impact production code quality.	82	Pass
Build reproducibility	The project is fully reproducible with consistent dependencies and proper exclusions. All package references resolve, Docker configuration is coherent, and build artifacts are excluded. Minor issues: HowToSetup.md is missing from Node Project folder (only in docs/), and the setup document could clarify the .env configuration step happens before npm ci.	95	Pass

Open warnings

Problems that did not stop the listing. They stay on the product page until a later version fixes them.

Warning 1 **Strong authentication on all mutating endpoints; minor ownership gap on guest reads**

All data-changing endpoints require signed admin session with proper bcrypt password hashing. Login is rate-limited. The only gap is that authenticated users can read any guest record by ID without ownership checks, though this is a single-admin system where all staff share one password.

Warning 2 **Database access is mostly safe; missing foreign key indexes and one unscoped DELETE**

SQL queries use parameterized statements throughout, preventing injection. Schema has proper foreign keys and constraints. However, foreign key columns lack explicit indexes in SQLite/Postgres schemas, and one DELETE statement in server.mjs lacks a WHERE clause (though it's scoped by table design). These are performance and safety warnings, not critical flaws.

Requirement list

What the builder agreed to deliver before uploading — 13 of 15 met.

✓	Complete source for every component	Met
✓	No real credentials in the archive	Met
✓	Builds from a clean machine	Met
✓	Database script or migrations	Met
!	Authentication and roles on every mutating endpoint	Partial
!	Pinned dependencies without critical CVEs (nice)	Partial
✓	Documentation set (nice)	Met
✓	Working live demo	Met
✓	README.md	Met
✓	HowToSetup.md	Met
✓	CLAUDE.md (or AGENTS.md) (nice)	Met
✓	CHANGELOG.md (nice)	Met
✓	.env.example	Met
✓	a project file	Met
✓	a project file (nice)	Met

PART 2

Human review

Reviewers from the Vibe96 team in Dubai worked through each question below; a final reviewer signed it off.

Stage 1 — Installed and run from the delivered code

Completed 26 Oct 2026

A reviewer installed the product on a clean machine, following only the guide that ships with it.

QUESTION	ANSWER	REVIEWER'S NOTE
Packages restored without errors	Yes	
Solution builds clean	Yes	
Database created from the shipped script or migrations	Yes	
First sign-in works with the documented steps	Yes	
Setup guide is accurate and complete	Yes	
Every module in the feature list opens and works	Yes	
No real secrets in the archive	Yes	
Branding and company details can be changed without code	Yes	

Stage 2 — Live demo compared with the delivered code

Completed 26 Oct 2026

A second reviewer checked that what the listing and demo show is what the buyer receives.

QUESTION	ANSWER	REVIEWER'S NOTE
Demo URL is reachable	Yes	
Demo credentials work	Yes	
Demo runs the same version as the archive	Yes	
All five differentiators are visible in the demo	Yes	
Screenshots match the demo	Yes	
Nothing in the demo is missing from the code	Yes	
Datasheet claims are accurate	Yes	

Changes asked for during review

None — approved on the first round.

Sign-off: approved for sale on 26 Oct 2026 with 2 warnings shown publicly.

What this report covers — and what it doesn't

- **It covers** version 1.0.0 exactly as the buyer downloads it: the source archive, the setup guide and the live demo on the dates above.

- **It is not** a penetration test, a performance or load test, or a legal review of third-party package licences.
- **Scores are a point in time.** Libraries age; a later version is audited again and gets its own report.
- **Your setup matters.** Hosting, configuration and changes made after purchase are outside this review.
- **How the score is made:** each AI check is scored 0–100 and weighted (security counts most). A listing needs 75 or more, no failing check, and the human review passed.
- **Always try the live demo** before buying, and ask the builder questions from the product page.

Report history

REPORT	VERSION	DATE	SCORE	STATUS
QR-26-00113	1.4.0	11 Nov 2026	**79**	Current
QR-26-00103	1.3.0	6 Nov 2026	**77**	Replaced
QR-26-00066	1.0.0	26 Oct 2026	**94**	Replaced