This report has been replaced by QR-26-00113 — a newer version of the product was reviewed.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	**1.3.0 · released 6 Nov 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	**3 Nov 2026 – 6 Nov 2026**

77 / 100

Passed with 5 warnings

Pass mark 75 and no failing check.

Scores

Security	78
Code structure	82
Docs & completeness	87
Dependency health	72
Build & deploy	72

✓ **AI code audit**
6 checks · 3 Nov 2026

✓ **Installed & run**
6 Nov 2026

✓ **Demo vs delivered**
6 Nov 2026

✓ **Final sign-off**
6 Nov 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 78/100 with no failing check.

! 5 open warnings — explained in part 1.

Check this report is genuine. Scan the code or open vibe96.com/report/QR-26-00103. 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 regex candidates are environment variable references, empty .env.example placeholders, or Cloudflare secret bindings, so no real key, token or connection string is committed. The one notable item is a demo-mode endpoint that intentionally exposes the admin password, which is safe only if buyers never enable it with real data.	92	Pass
Dependency vulnerabilities	Node a project file pins every direct dependency exactly and package-lock.json is committed, with no wildcard ranges. Two devDependencies are pre-release (beta) builds, and the declared stack (Vite 8.0.0, React 19.3.1) conflicts with the pinned Vite 8.3.4, so versions could not be verified against advisories. No known critical vulnerability was identified.	72	Warning
Authorisation & access control	The README documents a shared guard in createHavenServer that sits before every data route. Only health, public-config and login are public, and sessions are HMAC-signed with timing-safe comparisons. I could not inspect the route code in a project file, so the guard is unverified. The demo deliberately publishes its admin password, which is acceptable only if it never reaches production.	82	Warning
Database access rules	The files that decide this check (a project file, a project file, a project file, a project file) were not included in the excerpts, so I could not confirm that queries are parameterized or that the schema is complete. The documentation claims parameterized Neon storage and atomic versioned updates, and the visible code shows no string-built SQL. That is a claim, not proof, so the score is held at a middle value until the SQL can be read.	60	Warning
Code structure & duplication	The project separates storage, HTTP app, seed data and feature components, which keeps most concerns apart. The main structural cost is that startup validation and environment parsing live in the entry point rather than the shared app, and several values such as port 5177 are repeated across files. File sizes for the larger React modules were not in the digest, so they could not be assessed.	82	Warning
Build reproducibility	The Node project has a lockfile, pinned dependencies, a multi-stage Dockerfile and compose with required-variable guards, so a clean build is likely. However, version claims conflict across the declared stack, README and package.json, the build depends on beta Cloudflare packages, and HowToSetup.md was not visible to verify step order and prerequisites.	72	Warning

Open warnings

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

Warning 1 Pinned deps with lockfile, but beta/pre-release tooling and unverifiable versions; no known critical CVE

Node a project file pins every direct dependency exactly and package-lock.json is committed, with no wildcard ranges. Two devDependencies are pre-release (beta) builds, and the declared stack (Vite 8.0.0, React 19.3.1) conflicts with the pinned Vite 8.3.4, so versions could not be verified against advisories. No known critical vulnerability was identified.

Warning 2 Single-admin API appears guarded, but a project file was not shown and the demo password is public by design

The README documents a shared guard in createHavenServer that sits before every data route. Only health, public-config and login are public, and sessions are HMAC-signed with timing-safe comparisons. I could not inspect the route code in a project file, so the guard is unverified. The demo deliberately publishes its admin password, which is acceptable only if it never reaches production.

Warning 3 **Database layer not visible in digest; injection and schema checks cannot be verified, score capped**

The files that decide this check (a project file, a project file, a project file, a project file) were not included in the excerpts, so I could not confirm that queries are parameterized or that the schema is complete. The documentation claims parameterized Neon storage and atomic versioned updates, and the visible code shows no string-built SQL. That is a claim, not proof, so the score is held at a middle value until the SQL can be read.

Warning 4 **Mostly reproducible; version drift, beta deps and unverified HowToSetup limit confidence**

The Node project has a lockfile, pinned dependencies, a multi-stage Dockerfile and compose with required-variable guards, so a clean build is likely. However, version claims conflict across the declared stack, README and package.json, the build depends on beta Cloudflare packages, and HowToSetup.md was not visible to verify step order and prerequisites.

Warning 5 **Reasonable module layout; config validation duplicated across entry points and paths hard-coded in several places**

The project separates storage, HTTP app, seed data and feature components, which keeps most concerns apart. The main structural cost is that startup validation and environment parsing live in the entry point rather than the shared app, and several values such as port 5177 are repeated across files. File sizes for the larger React modules were not in the digest, so they could not be assessed.

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	Partial
✓	Database script or migrations	Met
✓	Authentication and roles on every mutating endpoint	Met
✓	Pinned dependencies without critical CVEs (nice)	Met
✓	Documentation set (nice)	Met
!	Working live demo	Partial
✓	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 6 Nov 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 6 Nov 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 6 Nov 2026 with 5 warnings shown publicly.

What this report covers — and what it doesn't

- **It covers** version 1.3.0 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