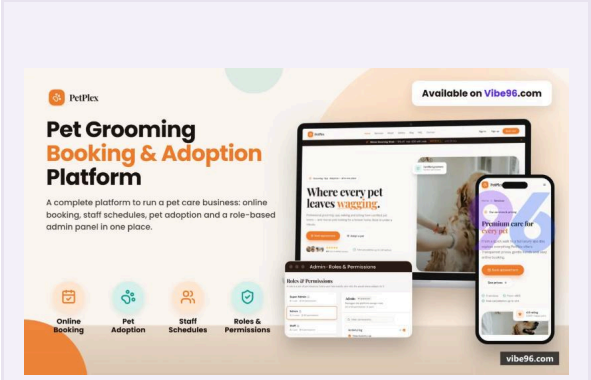


VIBE96 QUALITY REPORT

PetPlex – Pet Grooming Booking & Adoption Platform

Self-hosted grooming booking and pet adoption platform with customer, staff and admin panels for pet care businesses.

Product ID	**B0864-53146**
Builder	**Md Shijan Ali**
Version reviewed	**1.0.0 · released 17 Nov 2026**
Stack	**Next.js 15 (frontend) + Express 5 (API) · TypeScript 5.9 (Node.js 22 LTS) · PostgreSQL 16 with Prisma 7 ORM**
Built with	**Claude Code, Cursor, Lovable, v0 by Vercel**
Review period	**2 Nov 2026 – 17 Nov 2026 · 4 rounds of changes**

79 / 100

Passed with 5 warnings

Pass mark 75 and no failing check.

Scores

Security	77
Code structure	84
Docs & completeness	67
Dependency health	78
Build & deploy	80

✓ **AI code audit**
6 checks · 2 Nov 2026

✓ **Installed & run**
17 Nov 2026

✓ **Demo vs delivered**
17 Nov 2026

✓ **Final sign-off**
17 Nov 2026

At a glance

! Installed and run from the delivered code — 6 of 8 checks answered yes.

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

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

✓ Security scored 77/100 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-26-00142. 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 placeholders, env references or test fixtures; no live API keys, tokens or private keys were found in the visible files. The main concern is docker-compose falling back to a guessable Postgres password ('petplex') if the buyer doesn't set one, plus a few weak example defaults.	88	Warning
Dependency vulnerabilities	Both backend and frontend have package-lock.json files and no wildcard or 'latest' versions. All dependencies use caret ranges, and several version specifiers look unusual or could not be verified from the digest. The lockfiles' installed versions were not visible, so no known critical vulnerability could be confirmed.	78	Warning
Authorisation & access control	The backend declares access (auth, permission, validation) per route through createModuleRouter, and a route-access test exists. Passwords are hashed with bcrypt and refresh tokens are stored as hashes. Only the auth routes were visible in the digest, so most of the 174 endpoints and their ownership checks could not be confirmed.	72	Warning
Database access rules	The backend uses Prisma 7 with a schema split per domain, migrations and a a project file export, and the visible auth schema has foreign keys with cascade rules and indexes. The digest cuts off before any service, queryBuilder, raw SQL or migration file, so I could not confirm there are no string-built queries or unscoped deletes. The score is capped for that missing evidence, plus a few schema gaps visible in auth.prisma.	72	Warning
Code structure & duplication	The project follows a consistent module structure on both sides (backend modules with route/controller/service/validation files, frontend features and views separated), and the CLAUDE.md documents conventions. The visible issues are modest: a hard-coded demo URL appears in configuration examples and the sample env, and the frontend has a large number of similar admin pages that likely repeat CRUD scaffolding.	84	Pass
Build reproducibility	Two independent apps (Next.js frontend, Express/Prisma backend) have manifests, lockfiles, Dockerfiles, compose and env examples that look coherent. HowToSetup.md and several backend files (prisma/, src/config) were not visible in the digest, so some steps cannot be fully verified. A few gaps would trip a clean-machine setup: unpinned runtime versions, a postinstall hook that needs Prisma config, and a mixed zod/ESLint stack.	80	Warning

Open warnings

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

Warning 1 **No real credentials found; weak default DB password fallbacks ship in docker-compose**

All regex candidates are placeholders, env references or test fixtures; no live API keys, tokens or private keys were found in the visible files. The main concern is docker-compose falling back to a guessable Postgres password ('petplex') if the buyer doesn't set one, plus a few weak example defaults.

Warning 2 **Authz design is sound, but only the auth module's routes could be verified; the rest is unreviewable**

The backend declares access (auth, permission, validation) per route through createModuleRouter, and a route-access test exists. Passwords are hashed with bcrypt and refresh tokens are stored as hashes. Only the auth routes were visible in the digest, so most of the 174 endpoints and their ownership checks could not be confirmed.

Warning 3 **Prisma-based access looks sound, but the digest excludes the service files and migrations needed to verify most checks**

The backend uses Prisma 7 with a schema split per domain, migrations and a a project file export, and the visible auth schema has foreign keys with cascade rules and indexes. The digest cuts off before any service, queryBuilder, raw SQL or migration file, so I could not confirm there are no string-built queries or unscoped deletes. The score is capped for that missing evidence, plus a few schema gaps visible in auth.prisma.

Warning 4 **Lockfiles present for both apps; caret ranges and a few version/pinning concerns, no confirmed critical CVE**

Both backend and frontend have package-lock.json files and no wildcard or 'latest' versions. All dependencies use caret ranges, and several version specifiers look unusual or could not be verified from the digest. The lockfiles' installed versions were not visible, so no known critical vulnerability could be confirmed.

Warning 5 **Largely reproducible monorepo; a few unverifiable steps and minor inconsistencies in setup**

Two independent apps (Next.js frontend, Express/Prisma backend) have manifests, lockfiles, Dockerfiles, compose and env examples that look coherent. HowToSetup.md and several backend files (prisma/, src/config) were not visible in the digest, so some steps cannot be fully verified. A few gaps would trip a clean-machine setup: unpinned runtime versions, a postinstall hook that needs Prisma config, and a mixed zod/ESLint stack.

Requirement list

What the builder agreed to deliver before uploading — 10 of 15 met.

!	Complete source for every component	Partial
✓	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	Partial
!	Pinned dependencies without critical CVEs (nice)	Partial
✓	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 17 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	No	
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	No	

Stage 2 — Live demo compared with the delivered code

Completed 17 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 17 Nov 2026 with 5 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.