

VIBE96 QUALITY REPORT

GreenRinse

Mobile car-wash management for fleet operators: offline-first washer app, admin dashboard, partner portal.

Product ID	**B0003-25486**
Builder	**Max code**
Version reviewed	**1.2.0 · released 27 Oct 2026**
Stack	**ASP.NET Core 10 + React 18.3 + TypeScript 5.9 · C# 13 / .NET 10 · SQL Server 2019+**
Built with	**Claude Code**
Review period	**25 Oct 2026 – 27 Oct 2026**

77 / 100

Passed with 5 warnings

Pass mark 75 and no failing check.

Scores

Security	74
Code structure	84
Docs & completeness	100
Dependency health	80
Build & deploy	80

✓ **AI code audit**
6 checks · 25 Oct 2026

✓ **Installed & run**
27 Oct 2026

✓ **Demo vs delivered**
27 Oct 2026

✓ **Final sign-off**
27 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.
- ✓ 15 of 15 promised items delivered (setup guide, example config and the rest).
- ! Security scored 74/100 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-26-00072. 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	Every regex candidate in the digest is a placeholder, a setting-key name, or token-handling code, so no real credential was found. Appsettings.json holds no JWT secret and the connection string is a local Windows-auth default. Three warnings: documented demo passwords, a possible demo-credential list in the landing .env, and a seeded admin password.	88	Warning
Dependency vulnerabilities	Lockfiles exist for the frontend (package-lock.json) and every backend project (packages.lock.json), and NuGet versions are centrally pinned. Only package.json of the features package was shown, so no critical known vulnerability could be confirmed. There are a few warnings: workspace deps use "*", React 18.3 and a SignalR 8.0.x client are one major behind the declared .NET 10 stack, and several manifests were not visible.	80	Warning
Authorisation & access control	MaintenanceController is correctly restricted to the SuperAdmin policy, and docs describe role policies and ownership guards (EnsurePartnerAccess). However only one controller was visible in the digest, so per-id ownership checks and authentication on the other ~20 controllers could not be traced. Several smaller risks were visible in the digest.	72	Warning
Database access rules	The digest does not include MaintenanceService.cs, the EF configurations, the query filters, or the SQL scripts, so injection, unscoped deletes and FK indexing could not be verified. The visible signs are mostly good (EF Core with migrations, SuperAdmin-only maintenance endpoints, password re-check before wipe, tenant/partner/soft-delete query filters per CLAUDE.md). The destructive clean and backup paths are the highest-risk unreviewed code, and the schema and migration setup has gaps.	62	Warning
Code structure & duplication	The digest shows a sensible layering (Domain, Application, Infrastructure, Api, Workers) and per-feature folders for controllers, settings keys and frontend apps. The main weaknesses are repeated auth/fetch boilerplate across frontend pages and a few oversized multi-concern files that are hard to navigate, but nothing here is a god file or pervasive copy-paste.	84	Pass
Build reproducibility	The digest shows a coherent .NET 10 solution with central package management, lock files, global.json and .nvmrc, plus a frontend using npm workspaces with pinned versions. Several items could not be confirmed from the excerpts: the Docker files and HowToSetup step order, the Application project, and docker-compose. Duplicated web.config files and unclear migration and seed defaults are minor gaps.	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; demo logins and one committed .env file are weak-default warnings**

Every regex candidate in the digest is a placeholder, a setting-key name, or token-handling code, so no real credential was found. Appsettings.json holds no JWT secret and the connection string is a local Windows-auth default. Three warnings: documented demo passwords, a possible demo-credential list in the landing .env, and a seeded admin password.

Warning 2 **Lockfiles present and pins mostly exact; unverified versions and a wildcard workspace range**

Lockfiles exist for the frontend (package-lock.json) and every backend project (packages.lock.json), and NuGet versions are centrally pinned. Only package.json of the features package was shown, so no critical known vulnerability could be confirmed. There are a few warnings: workspace deps use "*", React 18.3 and a SignalR 8.0.x client are one major behind the declared .NET 10 stack, and several manifests were not visible.

Warning 3 **Visible endpoints are guarded, but most controllers were not shown, so ownership checks are unverified**

MaintenanceController is correctly restricted to the SuperAdmin policy, and docs describe role policies and ownership guards (EnsurePartnerAccess). However only one controller was visible in the digest, so per-id ownership checks and authentication on the other ~20 controllers could not be traced. Several smaller risks were visible in the digest.

Warning 4 **Database rules cannot be fully verified: key data-layer files were not provided, and the destructive clean path needs review**

The digest does not include MaintenanceService.cs, the EF configurations, the query filters, or the SQL scripts, so injection, unscoped deletes and FK indexing could not be verified. The visible signs are mostly good (EF Core with migrations, SuperAdmin-only maintenance endpoints, password re-check before wipe, tenant/partner/soft-delete query filters per CLAUDE.md). The destructive clean and backup paths are the highest-risk unreviewed code, and the schema and migration setup has gaps.

Warning 5 **Largely reproducible; a few unverifiable references and a duplicated config leave small gaps**

The digest shows a coherent .NET 10 solution with central package management, lock files, global.json and .nvmrc, plus a frontend using npm workspaces with pinned versions. Several items could not be confirmed from the excerpts: the Docker files and HowToSetup step order, the Application project, and docker-compose. Duplicated web.config files and unclear migration and seed defaults are minor gaps.

Requirement list

What the builder agreed to deliver before uploading — 15 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	Met
✓	Pinned dependencies without critical CVEs (nice)	Met
✓	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
✓	appsettings.example.json	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 27 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 27 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 27 Oct 2026 with 5 warnings shown publicly.

What this report covers — and what it doesn't

- **It covers** version 1.2.0 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-26-00072	1.2.0	27 Oct 2026	**77**	Current
QR-26-00051	1.0.0	22 Oct 2026	**86**	Replaced