Servo - Restaurant Delivery Manager

VIBE96 QUALITY REPORT

Servo - Restaurant Delivery Manager

Complete restaurant operations software: ordering, kitchen, delivery, dine-in and head office in one ASP.NET app

Product ID	**B0001-62641**
Builder	**X1980 Group**
Version reviewed	**1.0.0 · released 4 Oct 2026**
Stack	**ASP.NET Core 9 MVC · C# 12 / .NET 9 · SQL Server 2019+**
Built with	**Claude Code**
Review period	**4 Oct 2026 – 4 Oct 2026**

91 / 100

Passed with 2 warnings

Pass mark 75 and no failing check.

Scores

Security	92
Code structure	82
Docs & completeness	100
Dependency health	95
Build & deploy	92

✓ **AI code audit**
6 checks · 4 Oct 2026

✓ **Installed & run**
4 Oct 2026

✓ **Demo vs delivered**
4 Oct 2026

✓ **Final sign-off**
4 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 92/100 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-26-00007. 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	No actual API keys, passwords or connection strings with real credentials were discovered. The archive ships with local-development defaults (Trusted_Connection, blank passwords) and placeholder patterns that require configuration. Several weak defaults could embarrass a buyer if deployed unchanged: SQL Server connection without encryption enforcement, blank SMTP password, and demo settings that expose internal behavior.	92	Warning
Dependency vulnerabilities	The project uses .NET 9 with NuGet packages. A packages.lock.json exists but was excluded from the digest. All package references in Serveo.Web.csproj use exact version pins (e.g., 9.0.0, 8.0.11). No wildcard or floating versions detected. No known critical vulnerabilities identified in the declared versions.	95	Pass
Authorisation & access control	All mutating endpoints require authentication. Admin routes are protected by [Authorize(Policy)] and permission attributes. Staff sign-in uses bcrypt hashing. Customer authentication is cookie-based with OTP verification. Minor gaps: a few read endpoints (rider earnings, customer order history) lack explicit ownership checks in the query WHERE clause, trusting the controller base class scope.	92	Warning
Database access rules	All SQL goes through a single parameterised execution layer (Db.cs) with no string concatenation of user input. Row-level security enforces branch isolation on ten tables. Schema is complete with temporal tables and foreign keys. Minor: a few foreign keys lack explicit indexes (rider assignments, order items), and one UPDATE in OrderService omits WHERE but is scoped by RLS.	92	Pass
Code structure & duplication	The project demonstrates excellent module boundaries and separation of concerns. Controllers are thin, business logic is centralized in services, and the architecture follows clear patterns. Minor issues include some duplicated authentication/authorization logic across controller base classes, a few hard-coded values that should be configuration, and one oversized JavaScript file that could be split.	82	Pass
Build reproducibility	The project is fully buildable from source with clear prerequisites. The .NET solution, Docker Compose, and database scripts are coherent and reference only included files. Minor documentation improvements needed: HowToSetup.md should specify exact .NET SDK version (9.0.x) and SQL Server edition/version, and the appsettings.example.json reference in README.md points to a file that doesn't exist in the digest.	92	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 and role checks; minor ownership gaps on read endpoints**

All mutating endpoints require authentication. Admin routes are protected by [Authorize(Policy)] and permission attributes. Staff sign-in uses bcrypt hashing. Customer authentication is cookie-based with OTP verification. Minor gaps: a few read endpoints (rider earnings, customer order history) lack explicit ownership checks in the query WHERE clause, trusting the controller base class scope.

Warning 2 **No real credentials found; weak defaults and example patterns need hardening before production**

No actual API keys, passwords or connection strings with real credentials were discovered. The archive ships with local-development defaults (Trusted_Connection, blank passwords) and placeholder patterns that require configuration. Several weak defaults could embarrass a buyer if deployed unchanged: SQL Server connection without encryption enforcement, blank SMTP password, and demo settings that expose internal behavior.

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 4 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 4 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 4 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.