

VIBE96 QUALITY REPORT

Payora

UAE payroll system with GPSSA, WPS, final settlement and employee portal — English and Arabic

Product ID	**B0001-88422**
Builder	**Chow Studio**
Version reviewed	**1.2.2 · released 6 Nov 2026**
Stack	**ASP.NET Core MVC 10 · C# 13 (.NET 10) · SQL Server 2019+**
Built with	**Claude Code**
Review period	**3 Nov 2026 – 6 Nov 2026**

86 / 100

Passed with 2 warnings

Pass mark 75 and no failing check.

Scores

Security	87
Code structure	84
Docs & completeness	80
Dependency health	78
Build & deploy	88

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

✓ **Installed & run**
5 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.
- ! 12 of 15 promised items delivered (setup guide, example config and the rest).
- ✓ Security scored 87/100 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-26-00100. 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 is either an environment-variable reference (docker-compose.yml), a CI-generated random password (ci.yml), or a method signature with CancellationToken (ICustomizationRepository.cs, false positive). appsettings.json holds only a Windows-auth development connection string, and .env.example has empty values. No keys, tokens or private keys were found in the visible files, though the digest is partial.	93	Pass
Dependency vulnerabilities	Every .NET project has a packages.lock.json, locked restore is enabled in Directory.Build.props, and CI and the Dockerfile appear to use it. The excerpts do not include the lockfile or csproj contents, so installed versions could not be checked against advisories. The score is capped at the warning range until those can be reviewed, and a few non-package pins need attention.	78	Warning
Authorisation & access control	A fallback policy requires sign-in on every endpoint, [HasPermission] policies enforce roles, and the settings base controller returns 403 if a derived controller has no permission attribute. Org-scoped queries and a build-time EndpointAuthorizationTests suite point to strong ownership checks. Only a fraction of the 746 files were visible, so the full endpoint list could not be traced and some points are withheld.	88	Pass
Database access rules	The digest shows raw parameterised ADO.NET, an organization-scoped repository convention, 19 migration scripts, a from-scratch schema.sql, and dedicated foreign-key index and performance index migrations. The repository implementations (33 files) and the Administration SQL writers were not included in the excerpts, so I found no evidence of injection or unscoped deletes but could not confirm their absence.	80	Warning
Code structure & duplication	The solution follows a clear Clean Architecture split (Domain, Application, Infrastructure, Web) with features grouped into folders and a shared generic base for settings CRUD controllers, which removes much duplication. The digest shows no copy-pasted modules or dead-code dumps, but a few multi-concern files and hard-coded values would be worth splitting.	84	Pass
Build reproducibility	The solution layout, locked package restores, pinned SDK, pinned SQL Server image and compose start order (db, db-init, app) are coherent, and the setup route creates the database before the app starts. HowToSetup.md and the a project file contents were not in the digest, so prerequisites and framework consistency could only be checked through CLAUDE.md and compose references.	88	Pass

Open warnings

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

Warning 1 **Lockfiles present, but package versions were not shown so a vulnerability audit is not possible**

Every .NET project has a packages.lock.json, locked restore is enabled in Directory.Build.props, and CI and the Dockerfile appear to use it. The excerpts do not include the lockfile or csproj contents, so installed versions could not be checked against advisories. The score is capped at the warning range until those can be reviewed, and a few non-package pins need attention.

Warning 2 **Parameterised ADO.NET and org-scoped design look sound, but most SQL could not be inspected**

The digest shows raw parameterised ADO.NET, an organization-scoped repository convention, 19 migration scripts, a from-scratch schema.sql, and dedicated foreign-key index and performance index migrations. The repository implementations (33 files) and the Administration SQL writers were not included in the excerpts, so I found no evidence of injection or unscoped deletes but could not confirm their absence.

Requirement list

What the builder agreed to deliver before uploading — 12 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	Partial
✓	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
✓	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 5 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 2 warnings shown publicly.

What this report covers — and what it doesn't

- **It covers** version 1.2.2 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-26-00100	1.2.2	6 Nov 2026	**86**	Current
QR-26-00006	1.0.0	4 Oct 2026	**92**	Replaced