ensemma

CODEBASE HEALTH CHECK · FINDINGS AND FIX PLAN

What we found in Example Co.'s codebase, and what to fix first

Product	Example Co. web app and API
Review period	2–6 November 2026
Prepared by	Shishir, Ensemma
Version	Sample report

SAMPLE REPORT

Example Co. is a fictional company. This sample shows what a Codebase Health Check report looks like; real reports are confidential.

SUMMARY

The product works and the core is sound. Three issues could hurt you soon: payments can be replayed, checkout has almost no tests, and there are no database backups. All three are fixable in about two weeks.

How each area looks

Security	Fix now	Payment webhook isn't verified; secrets in the repository.
Reliability	Fix now	One database, no backups, no restore tested.
Tests	Fix this month	12 of 14 checkout paths have no tests.
Scalability	Fix this month	Two queries will slow down sharply past about 10× today's traffic.
Architecture	Healthy	Clear structure; easy for new engineers to follow.

The three things to fix first

1. **Verify the payment webhook signature.** Half a day. Stops anyone replaying a payment.
2. **Turn on automated database backups and test a restore.** One day. Today a single failure loses all customer data.
3. **Add tests to the checkout flow.** About a week. Lets you change checkout without fear.

FINDINGS

What we found

SEC-01 Payments can be replayed

Fix now

Where	`api/webhooks/payments.ts`, line 41
What we found	The webhook accepts any request that looks like a payment event. It never checks the provider's signature.
Why it matters	Anyone who sees one real event can send it again and mark unpaid orders as paid.
Fix	Verify the signature with the provider's library before doing anything else.
Effort	Half a day

```
const event = provider.webhooks.constructEvent(rawBody, signature, WEBHOOK_SECRET);
// reject the request if this throws
```

REL-01 No database backups

Fix now

What we found	Production runs on one database instance with backups turned off.
Why it matters	A disk failure or a bad migration loses every customer record, with no way back.
Fix	Enable daily backups with point-in-time recovery, then restore one into a test environment to prove it works.
Effort	One day

TST-01 Checkout is almost untested

Fix this month

What we found	12 of 14 checkout paths have no automated tests, including refunds and discount codes.
Fix	Add tests for every checkout path, starting with refunds. Run them on every pull request.
Effort	About a week

FIX PLAN

A four-week plan, in priority order

WEEK	WORK	FINDINGS	EFFORT
1	Verify payment webhooks; move secrets out of the repository; turn on backups and test a restore	SEC-01, SEC-02, REL-01	3 days
2	Tests for every checkout path; run them on every pull request	TST-01	5 days
3	Rewrite the two slow queries; add the missing indexes; load-test at 10× traffic	SCL-01, SCL-02	4 days
4	Error monitoring and alerts; a short runbook for incidents	REL-02	2 days
	Total		**14 days**

If your team does the work

This report is yours. Every finding has enough detail for your engineers to fix it. We're happy to answer questions for two weeks.

If you'd like us to do it

We can take on the whole plan or part of it, fixed price or time and materials. The Health Check fee is credited in full against work booked within 30 days.

NEXT STEP

Reply to this report or book a call at **ensemma.com**. We'll walk you through it in 30 minutes.