App **Tallyroom** Delivered **5 November 2026** Audit **a-sample-01**

SAMPLE

Sample report. The app, its code and every finding are invented to show the format; no real client is described.

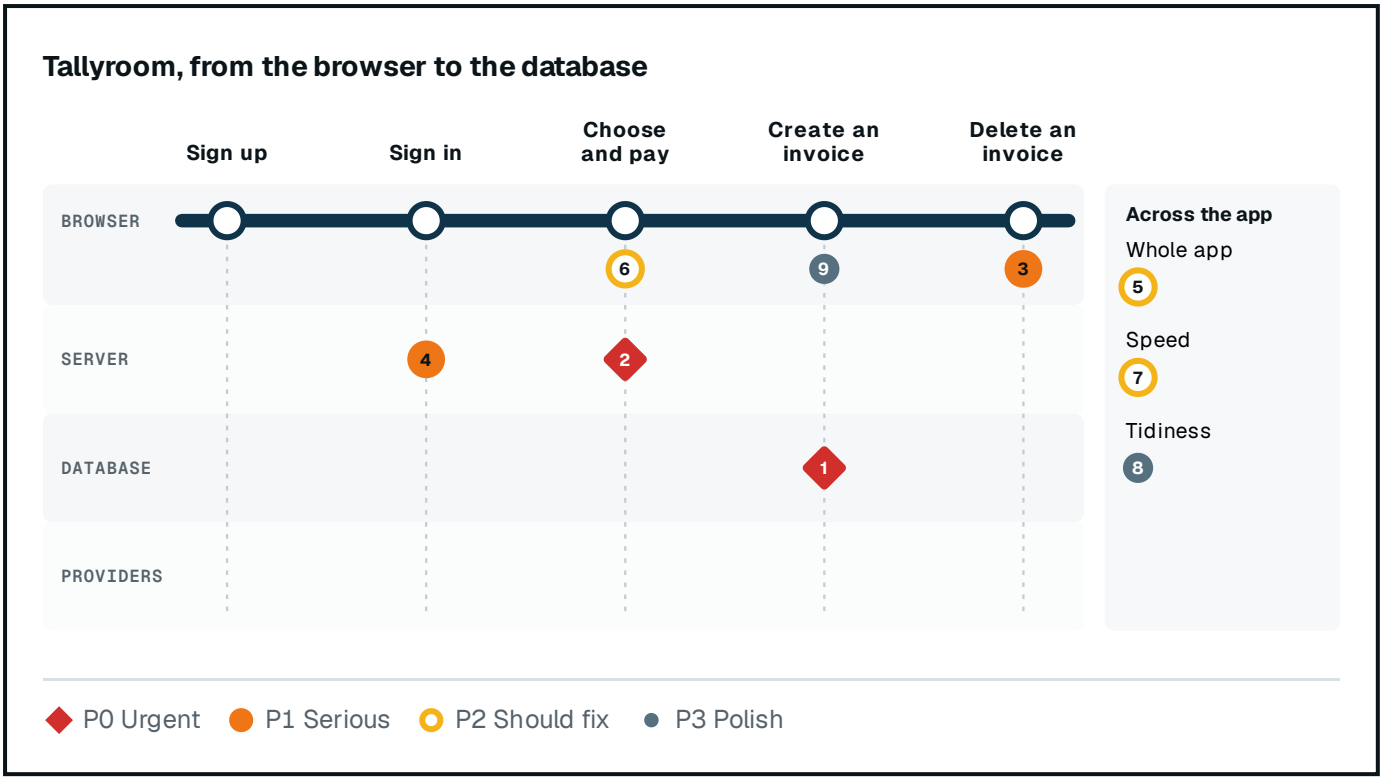
Tallyroom works, and two problems need fixing this week.

Any visitor can read every customer's invoices without signing in, and the checkout lets the browser set the price. Both are quick to fix. The rest of the app is in reasonable shape: sign-up, invoicing and payments work end to end, and nothing leaks your secret keys.

2	2	3	1
Urgent	**Serious**	**Should fix**	**Polish**
Act now	Fix within weeks	Quality and upkeep	When convenient

Where the findings sit

Choose a marker to read its finding. Numbers match the chapters below.



Fix these this week

1 **Anyone can read every customer's invoices without signing in**

P0 Urgent · Under a day

2 **A customer can change the price they pay at checkout**

P0 Urgent · Under a day

3 **The Delete invoice button does nothing**

P1 Serious · Under a day

What is solid

Reported as clearly as what is broken: secrets, payments and the main flows held under every check that touched them.

- No secret keys reach the browser, and the git history is clean.
- Stripe webhooks are verified and cannot be replayed to grant access twice.
- Sign-up, sign-in and paying an invoice all work at desktop and phone width.
- Every money amount is stored as whole pence, so totals never drift.

Urgent

2 findings

Two ways in: anyone can read invoices, and the browser sets the price. Close both this week.

1

P0 Urgent

Anyone can read every customer's invoices without signing in

Create an invoice, database | Effort: **Under a day** | Fix in: **week 1**

Why it matters

The invoices table has no access rules, so a stranger with the public app key can download every invoice, client name and amount. That is a data breach you would have to report.

What to do

Fix before anything else. Paste the fix prompt into your coding agent, or ask your developer; it is under an hour of work.

2

P0 Urgent

A customer can change the price they pay at checkout

Choose and pay, server | Effort: **Under a day** | Fix in: **week 1**

Why it matters

The checkout takes the amount from the browser, so anyone who edits the request can pay one pence for a plan that costs forty pounds. You lose money on every such sign-up.

What to do

Fix this week, together with the invoices fix.

Serious

2 findings

A dead button your customers have already met, and nothing stopping password guessing.

3

P1 Serious

The Delete invoice button does nothing

Delete an invoice, browser | Effort: **Under a day** | Fix in: **week 1**

Why it matters

Users click it, nothing happens, and the invoice stays. They lose trust and email you instead, which costs you time on every account.

What to do

Quick fix; include it in this week's round.

4

P1 Serious

Nothing slows down someone guessing passwords

Sign in, server | Effort: **One to three days** | Fix in: **week 2**

Why it matters

An attacker can try thousands of passwords against one account without being stopped. Accounts with weak passwords will eventually be taken over.

What to do

Plan for next week; your developer should do this one.

Should fix

3 findings

Quality and upkeep: errors nobody hears about, a pricing page that breaks on phones, a slow first page.

5

P2 Should fix

When the app breaks, nobody finds out

Across the app: whole app | Effort: **Under a day** | Fix in: **week 2**

Why it matters

Errors that users hit are not recorded anywhere, so you learn about problems only when someone complains, or leaves.

What to do

Worth doing next week; it pays for itself the first time something breaks.

6

P2 Should fix

The pricing table runs off the screen on a phone

Choose and pay, browser | Effort: **Under a day** | Fix in: **week 2**

Why it matters

On a phone the plans scroll sideways and the price of the middle plan is cut off, so visitors on mobile are less likely to sign up.

What to do

Include in next week's round.

7

P2 Should fix

The first page downloads more code than it needs

Across the app: speed | Effort: **One to three days** | Fix in: **week 3**

Why it matters

Visitors wait about four seconds on a phone before the landing page responds, because the whole charting library loads up front. Slow first pages lose sign-ups.

What to do

Later; your developer can do this in a morning.

Polish

1 finding

Polish: leftover sample pages from the builder that make the app look unfinished.

8

P3 Polish

Leftover sample pages from the builder are still live

Across the app: tidiness | Effort: **Under a day** | Fix in: **week 3**

Why it matters

A demo page with fake customers is reachable at /examples. It looks unfinished to anyone who finds it.

What to do

Tidy-up; do it whenever convenient.

Make it easier to use

1 finding

Not defects: one change that would make sending an invoice feel finished, with the reason behind it.

9

P3 Polish

Sending an invoice ends on a toast that disappears

Create an invoice, browser | Effort: **Under a day** | Fix in: **week 3**

Based on: **A likely cost** | UX law: **Peak-End Rule**

Why it matters

After Send, a two-second message says Sent and the page goes back to the invoice list. There is no record on the invoice of when it went or to which address, so a user who looks away has to open their sent mail to check, or sends it twice.

What to do

Do it when convenient; it is a small change.

What this rests on

Sending is the moment the app earns its keep. When it ends without a lasting confirmation, users check by hand or send the same invoice again.

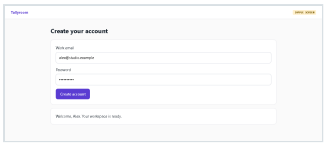
Functionality and usability

Sign-up works everywhere; choosing a plan and sending an invoice struggle on a phone; deleting an invoice is broken.

Sign up

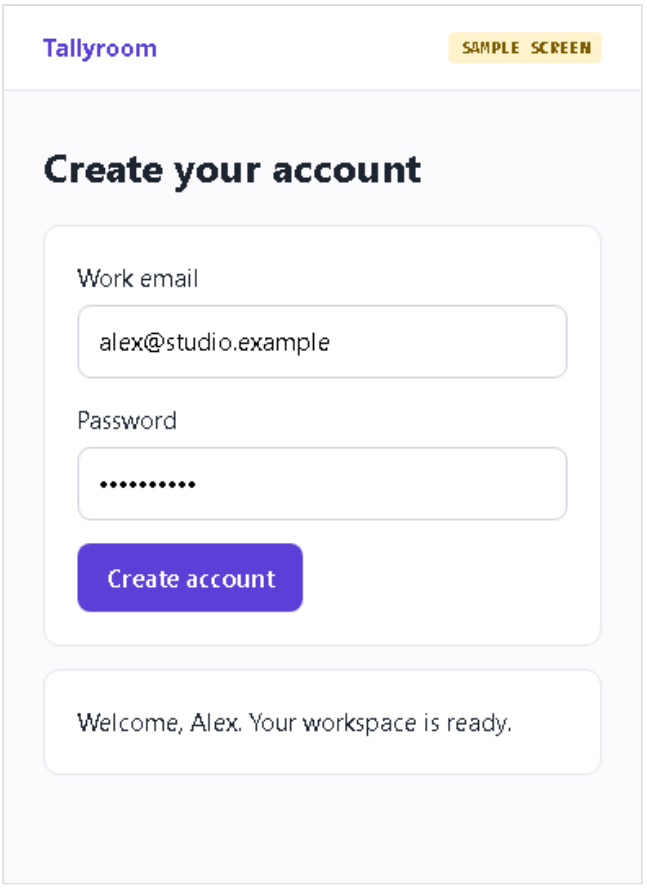
Desktop: Account created, welcome screen shown.

Phone: Works; the form fits the screen.



Desktop, 1280px

■ Works



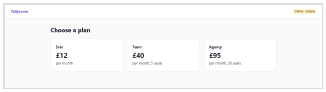
Phone, 390px

■ Works

Choose a plan

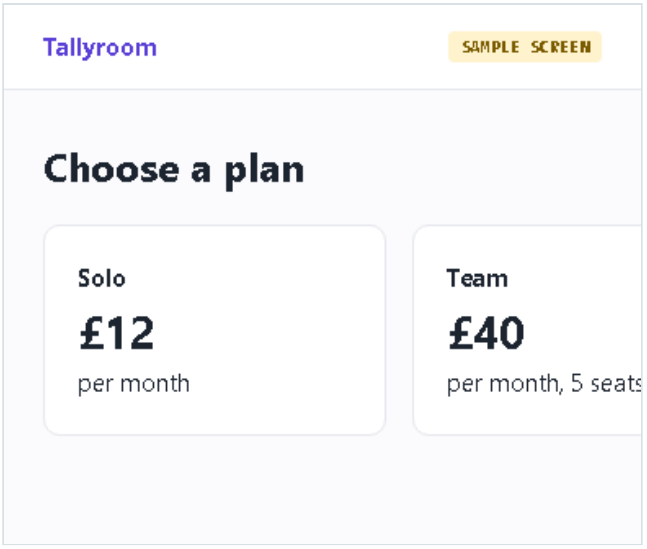
Desktop: Plans readable side by side.

Phone: Table runs off the screen; see finding F-006.



Desktop, 1280px

Works



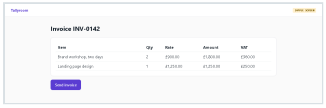
Phone, 390px

Broken

Create and send an invoice

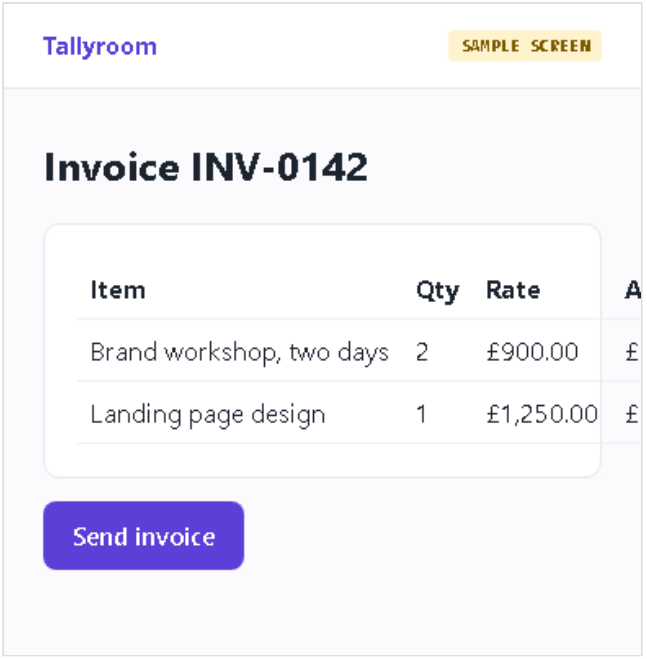
Desktop: Created and sent in under a minute.

Phone: Works, but the line-item table needs sideways scrolling.



Desktop, 1280px

Works



Phone, 390px

Works with problems

Delete an invoice

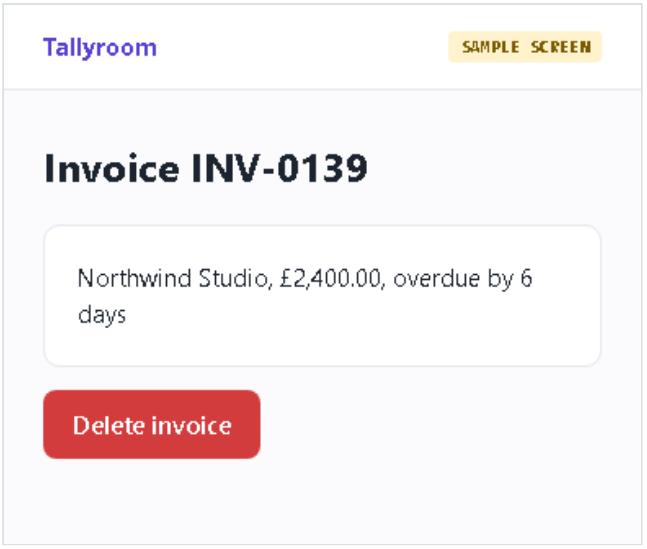
Desktop: Button does nothing; see finding F-003.

Phone: Same as desktop.



Desktop, 1280px

Broken



Phone, 390px

Broken

Fix plan

Three weeks, in an order where each fix clears the way for the next.

This week

Close the two ways in: data readable without login, and the price set by the browser. Then the dead button.

- 1. Anyone can read every customer's invoices without signing in
- 2. A customer can change the price they pay at checkout
- 3. The Delete invoice button does nothing

Next week

Stop password guessing, start hearing about errors, fix the phone pricing page.

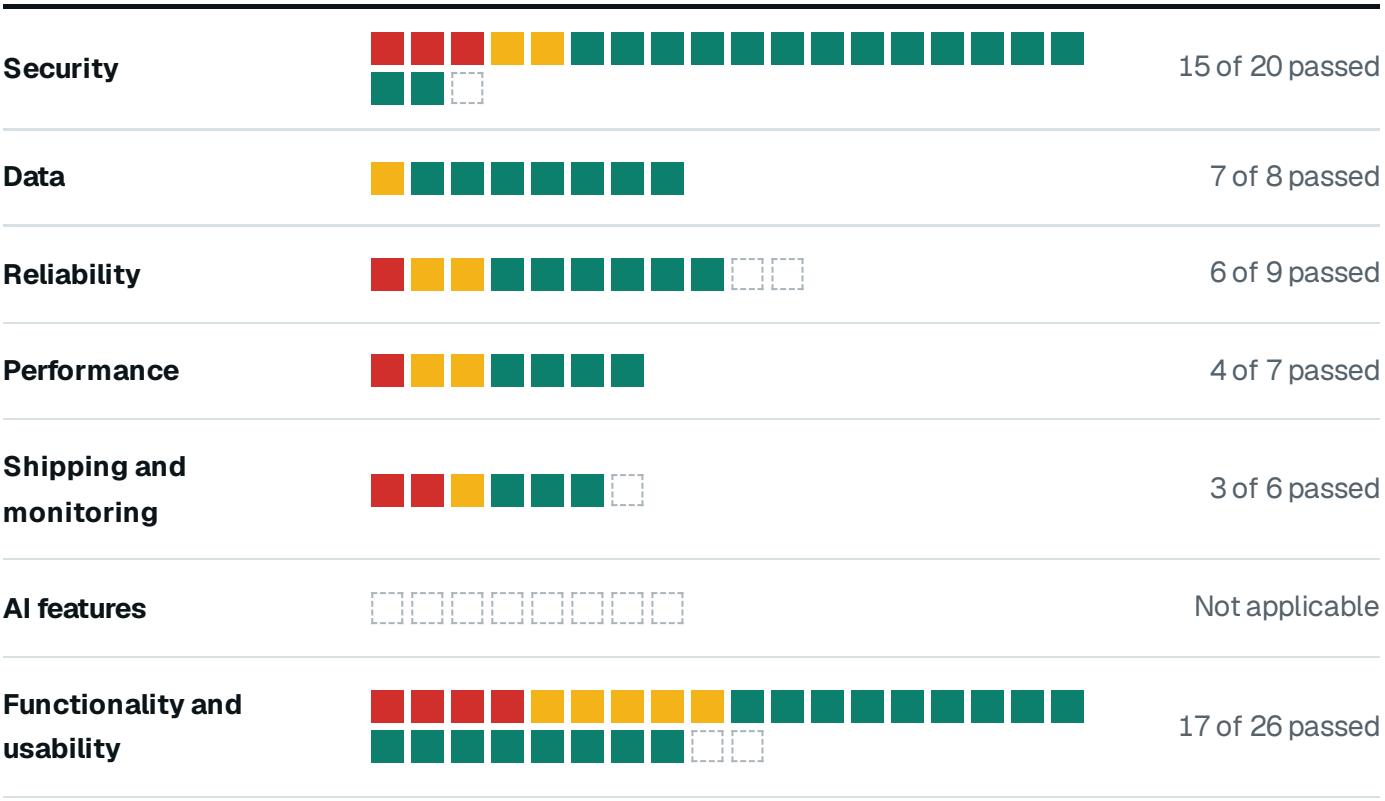
- 4. Nothing slows down someone guessing passwords
- 5. When the app breaks, nobody finds out
- 6. The pricing table runs off the screen on a phone

When convenient

Speed, tidy-up, and a clearer end to sending an invoice.

- 7. The first page downloads more code than it needs
- 8. Leftover sample pages from the builder are still live
- 9. Sending an invoice ends on a toast that disappears

Every check, one mark each



Graded against the Qodeup Check Catalogue v1.4: 76 of 90 checks apply to this app.

Auditor's statement

Qodeup examined Tallyroom's code, database rules and live app against the Qodeup Check Catalogue v1.4.

Every finding was found by the audit crew and challenged by a verifier against its evidence. Every urgent and serious finding was reviewed again, blind, by an independent second model. A senior engineer read the report and signed it.

Orezi Emeotu, founder, Qodeup Africa

Signed 5 November 2026

Report version 1, audit `a-sample-01`

What happens next

- → Free re-check of the P0 items by 5 December 2026.
- → 30-minute walkthrough call, booked for 6 November.
- → Qodeup can fix everything in weeks 1 and 2 as a fixed-price sprint; the quote is attached separately.