SAMPLE REPORT · OUR OWN APP

Leak Check: our own production client portal

Next.js · Postgres · Stripe · behind a Cloudflare Tunnel | Outside-in review, owner-authorized, cross-checked against source | Tools: REA reverse-engineering suite, headless Chrome, HTTP probing

Bottom line: the app holds up well. Nothing secret ships to the browser, private areas can't be reached without a valid login, and forged webhooks and login links are rejected. We found **one medium issue** (the app also loaded over unencrypted HTTP), fixed with a single setting, and two low-priority hardening items. All three were fixed within a day.

Findings

#	FINDING	SEVERITY	FIX EFFORT
1	App and login form load over plain HTTP, with no redirect to HTTPS	Medium · Fixed same day	2 minutes (one setting)
2	No Content-Security-Policy header	Low · Fixed next day	1–2 hours
3	Marketing site missing HSTS and Permissions-Policy headers	Fixed same day	5 minutes
4	Anyone can write to the analytics and error-log endpoints	Info	Optional
5	Public health check reports database status	Info	None needed

1. Plain-HTTP access to the app Medium

What we saw: `http://app.…/login` returned the full login form over HTTP. The main website redirected to HTTPS, but the app's own address didn't.

Why it matters: a visitor who follows an `http://` link on public Wi-Fi can have the page read or swapped for a fake. Two things limit the damage: the login cookie is marked `Secure`, so sessions can't be stolen this way, and returning visitors are protected by HSTS.

Fix: turn on "Always Use HTTPS" in the DNS/CDN provider, then confirm `http://` returns a 301 redirect.

2. No Content-Security-Policy Low

What we saw: no CSP header. Uploaded files already get a strict sandbox policy.

Why it matters: a CSP is the safety net if a cross-site-scripting bug ever appears. The current risk is low because the code never injects raw HTML.

Fix: add a nonce-based policy, ship it in report-only mode for a week, then enforce it.

Result: fixed the next day with a nonce-based policy. It was tested on a separate copy of the app in a real browser before it went live, then checked again on the live site.

What passed

- ✓ **No secrets in the browser.** 694 KB of shipped JavaScript and all public pages were scanned: no payment, cloud or AI keys, no database addresses, no internal server names.
- ✓ **Source code stays private.** All 15 source-map files return "not found", and live page inspection found none declared.
- ✓ **Nothing to steal from browser storage.** The app keeps no tokens in localStorage, sessionStorage or IndexedDB.
- ✓ **Private areas are locked.** The admin and client dashboards redirect to login. A fake session cookie and the known Next.js bypass header (CVE-2025-29927) were both refused.
- ✓ **Every hidden endpoint holds.** All 12 API routes refuse unauthenticated requests, and file downloads check ownership.
- ✓ **Forged webhooks are rejected.** Unsigned and fake-signature payment and phone webhooks get 400/401.

- ✓ **Login can't be abused.** Forged login links are rejected, the login form doesn't reveal who has an account, and requests are rate-limited.
- ✓ **No cross-site access.** Requests from an attacker's website get no CORS permission.
- ✓ **Strong cookie and header basics.** The session cookie is HttpOnly, Secure and SameSite. HSTS, X-Frame-Options and nosniff are set, and the server type isn't revealed.

Coverage & limits

This Leak Check covers what is reachable **without logging in**. Per-customer data isolation was confirmed by reading the code, not by live testing with customer accounts; that's part of the Full Audit. We ran no load or denial-of-service tests and touched no real customer data. Every check is backed by saved evidence (REA evidence IDs and raw HTTP responses), available on request.

Golden Rock · San Antonio, Texas · hello@goldenrockadvancements.com · goldenrockadvancements.com/audit
Leak Check $499 · Quick Scan $299 · Full Audit $1,200–$1,500 · Android App Review $1,500–$3,500. This is a security review, not legal advice or a guarantee against breaches.