HARBOVA SECURITY REPORT

demo-app.lovable.app

Deep Audit (sample) · July 13, 2026

We found 4 issues that matter, including 1 critical. The most serious lets anyone read your users' data using only the public key in your front-end. All four are fixable in a day, and none require rebuilding.

F
34/100

1 Critical	**2** High	**1** Medium	**0** Low

Findings

CRITICAL Database · A01 Broken Access Control

1. Your database is readable by anyone (RLS off)

What we found. Using only the public key that ships in your front-end, we read live rows from the profiles and orders tables. Anyone on the internet can download this data right now.

Evidence: GET /rest/v1/profiles?limit=1 → 200 with rows

How to fix it. Enable Row Level Security on every table and add policies so each user can only read their own rows. The exact SQL is included in your fix pack.

HIGH Secrets · A05 Security Misconfiguration

2. API key exposed in the front-end bundle

What we found. A third-party service key was hard-coded in your JavaScript. Anyone can extract it and run charges against your account.

Evidence: sk-l••••a1b2 (in JavaScript bundle)

How to fix it. Move the key to a server-side environment variable, proxy the call through an API route, and rotate the exposed key now.

HIGH Auth · A01 Broken Access Control

3. Admin page has no login

What we found. The /admin route renders the dashboard without checking who is asking.

How to fix it. Add a server-side auth check that runs before the page renders and redirects anyone who is not an admin.

MEDIUM Surface · A05 Security Misconfiguration

4. Missing security headers

What we found. No Content-Security-Policy, no clickjacking protection, and HSTS is not set.
How to fix it. Add a small set of response headers. The exact config for your framework is included.

What passed

✓ Served over HTTPS
✓ No exposed .env or .git files

Re-test & verification. On Audit + Fix engagements, every issue above is re-tested after remediation and this report is reissued showing each item closed and verified. This report reflects the state of the in-scope assets at the time of testing and is not a certified penetration test.