

OkToShip

LAUNCH AUDIT / ILLUSTRATIVE-EXAMPLE

Your audit, with evidence.

Readiness: 64 / 100. Coverage: 75%.

ILLUSTRATIVE SAMPLE. Synthetic findings for a made-up app; not a real customer audit.

A clean scan is not a guarantee of security. Findings describe the tested scope at the time of this scan. Suspected means proof is incomplete. Untested checks are not passes.

Coverage.

bundle_secrets: completed. No findings in the inspected sample bundle.

logged_out_read: completed. Approved synthetic profiles table.

account_read_replay: completed. Dedicated User A and User B; synthetic test-owned row.

write_replay: untested. Staging and disposable write scope were not supplied.

Findings.

HIGH / PROVEN

Profiles are readable without signing in.

ILLUSTRATIVE: a logged-out GET /rest/v1/profiles returned HTTP 200 and 3 synthetic rows. Email sample: a***@example.test. No secret values included.

FIX / Review every SELECT policy that applies to anon. Allow private profile reads only when the authenticated user owns the row. Recheck after the repair.

HIGH / PROVEN

User B can read A's profile.

ILLUSTRATIVE: GET /rest/v1/profiles?id=eq.test-profile-a returned HTTP 200 and A's synthetic row while using dedicated User B's session. No production customer data.

FIX / Enforce ownership on the server or database policy. Test that A can read their row, B is denied A's row, and logged-out reads are denied.