Is your app leaking customer data? 25 checks you can run in 15 minutes.

QUICK ANSWER AS OF OCT 2026

The Fix Forward Labs Security Checklist is 25 plain-English checks for business apps built with AI tools like Lovable, Bolt, Replit and Base44. Each one is a test an owner can run in a browser in under a minute, with a red or green answer and what a red result could cost the business. As of October 2026 it covers six areas: who can see your data, keys, logins, payments, backups and ownership.

AI tools got your team to a working app fast. What they tend to skip is the last 20%: who can see what, where the keys live, and what happens on a bad day. These checks show you where you stand. None of them changes anything in your app.

Run these only on apps your company owns or has permission to test. Use two test accounts you create, never a real customer's. A green result on all 25 means none of the common, visible gaps showed up; it doesn't prove the app is secure.

How to read a result: each check ends with Green (nothing to do) or Red (fix it). Count your reds as you go.

A · CHECKS 1–5

Who can see your data

Before you start: create two test accounts with the lowest access level your app has, "Test A" and "Test B", each with one made-up record (a fake customer, job or invoice).

01 **Can someone who isn't logged in see inside the app?**

TEST Logged in, open a page that shows customer or job details and copy its address. Open a private or incognito window and paste it.

☑ GREEN you're sent to the login screen.

■ RED the page or any of its data appears.

IF IT'S RED anyone who gets that link, from a forwarded email or browser history, can read your records. A leak of personal data can trigger breach notices to every affected customer; every US state has a breach-notification law.

02 **Can one user open another user's record?**

`TEST` Logged in as Test A, open A's fake record and copy its address. Log out, log in as Test B and paste the address.

☑ `GREEN` "not found" or "no access".

■ `RED` B can see A's record.

`IF IT'S RED` your clients can see each other's data, and staff can see what their role shouldn't. This is the most common gap in AI-built apps.

TOOL NOTES Lovable and Bolt apps on Supabase: in the Supabase dashboard, every table holding customer data should show Row Level Security (RLS) as enabled, with rules. Lovable's built-in security scan, where your plan shows it, flags tables without them. Base44: check each data table's access rules in the app's data or security settings.

---

03 **What happens when you change the number in the address bar?**

`TEST` As Test A, open a record whose address ends in a number or code, such as `/invoices/1042`. Change it by one (`/1041`, `/1043`) and press Enter.

☑ `GREEN` "not found", or only Test A's own records.

■ `RED` someone else's record appears.

`IF IT'S RED` anyone with an account can walk through every record you have, one number at a time.

---

04 **Are uploaded files open to anyone with the link?**

`TEST` In the app, open an uploaded photo, PDF or contract and copy the file's own address (right-click → Copy link). Paste it into a private window. Try again a day later.

☑ `GREEN` it asks you to log in, or the link has stopped working.

■ `RED` the file opens for anyone, any time.

`IF IT'S RED` signed contracts, IDs, site photos and invoices can be shared or found without anyone noticing.

TOOL NOTES Supabase: under Storage, buckets holding customer files should be private, not public.

---

05 **Has Google indexed pages that should be private?**

`TEST` Search Google for `site:yourapp.com` (use your app's address, including `.lovable.app`, `.bolt.host`, `.replit.app` or `.base44.app` addresses if it ever ran there).

☑ `GREEN` only your public pages appear.

■ `RED` dashboards, customer pages, files or test data appear in results.

`IF IT'S RED` strangers can find your data by searching, and the results can stay in caches after you fix the app.

`B · CHECKS 6–9`

Keys and passwords

06 **Are secret keys visible in your app's code in the browser?**

`TEST` Open your app in Chrome, press F12, then Ctrl+Shift+F (Cmd+Option+F on a Mac) to search every file the page loaded. Search one at a time for `sk_live`, `service_role`, `sk-` and `secret`.

☑ `GREEN` no matches. A Supabase "anon" or "publishable" key showing up is normal and fine.

■ `RED` any `sk_live` Stripe key, Supabase `service_role` key, or AI key starting `sk-`.

`IF IT'S RED` a Stripe secret key lets a stranger issue refunds and read your customers' payment details; an AI key lets them run up your bill. Rotate the key in that service today, then move it out of the browser.

TOOL NOTES Bolt and other Vite apps: any setting whose name starts with `VITE_` is shipped to the browser, so secrets must never use that prefix. Lovable: secrets belong in Supabase Edge Function secrets. Replit: in the Secrets tool, used only by server code.

---

07 **Are keys or passwords stored in your code repository?**

`TEST` On GitHub, open the repository and use the search box to look for `sk_live`, `service_role`, `password` and a file named `.env`. Check the repository is marked Private.

☑ `GREEN` private, and no keys or `.env` file.

■ `RED` any key or password in the code, or the repository is public.

`IF IT'S RED` automated scanners watch public code for keys, and anyone who ever had access to a private repo has a copy. Rotate every key found.

---

08 **Are passwords and keys shared in chat, email or documents?**

`TEST` Search your team chat, email and shared documents for "password", "API key", "login" and `sk_live`.

☑ `GREEN` shared logins live only in a password manager.

■ `RED` working passwords or keys sit in messages or docs.

`IF IT'S RED` everyone who can read that chat, including former staff and freelancers, holds the keys.

---

09 **Do you know every service the app uses and who holds its keys?**

`TEST` Write down every outside service the app talks to: payments, email, text messages, AI, maps, QuickBooks or the CRM. Next to each, note whose account it is and when the key was last changed.

☑ `GREEN` a complete list, all in company accounts, keys changed since anyone with access left.

■ `RED` you can't complete the list, or a key was created by someone who's gone.

`IF IT'S RED` the person who built it can still use your services, and you can't switch off what you don't know exists.

`C · CHECKS 10–13`

Logins and accounts

10 **Does everyone have their own login?**

`TEST` Ask your team how they get into the app. Look at the app's user list and compare it with the people who actually use it.

☑ `GREEN` one named login per person.

■ `RED` any shared login ("office@", "admin", one password on a sticky note).

`IF IT'S RED` you can't tell who changed or deleted something, and you can't remove one person without locking out everyone.

---

11 **Have people who left lost access?**

`TEST` Open the app's user list (and the builder, hosting and database accounts). Tick off every name against current staff and contractors.

☑ `GREEN` only current people.

■ `RED` any former employee, freelancer or the person who built it still listed.

`IF IT'S RED` people who left still have the keys to your customer data.

```
TOOL NOTES  Supabase: Authentication → Users. Also check team members in Lovable,
Bolt, Replit or Base44 and on GitHub.
```

---

12 **Can a stranger sign up and get in?**

`TEST` In a private window, go to the app's sign-up or login page and try to create an account with a fresh email address of your own.

☑ `GREEN` sign-up is closed, invite-only, or new accounts see nothing until someone approves them.

■ `RED` a stranger's new account can see real data or features.

`IF IT'S RED` the app is open to anyone who finds the address.

`TOOL NOTES` Supabase: Authentication settings include whether new users may sign up. Turn it off for internal tools.

---

13 **Are the accounts behind the app protected with two-step login?**

`TEST` For the AI builder (Lovable, Bolt, Replit, Base44), hosting, database, GitHub, domain and Stripe accounts, check security settings for two-step verification.

☑ `GREEN` on for every account, with recovery codes stored safely.

■ `RED` any account protected by a password alone.

`IF IT'S RED` one reused or phished password hands someone your whole app, including the ability to delete it.

`D · CHECKS 14–17`

Money and payments

Skip this group if the app never touches payments or invoices.

---

14 **Do paid orders in the app match Stripe?**

`TEST` Pick last month. Count the orders or invoices the app shows as paid, then count successful payments in your Stripe dashboard for the same dates.

☑ `GREEN` the numbers match.

■ `RED` they don't, and nobody can explain the gap.

`IF IT'S RED` you're either delivering work nobody paid for or charging people the app doesn't know about.

`TOOL NOTES` Stripe tells the app about payments through webhooks. In Stripe's developer area (Workbench → Webhooks), failed deliveries are a red flag on their own.

---

15 **Does anyone notice failed payments?**

`TEST` In Stripe, filter payments to Failed for the last 30 days. For each one, check what the app shows and whether someone followed up.

☑ `GREEN` every failure shows as unpaid in the app and was chased.

■ `RED` the app shows "paid", or nobody knew.

`IF IT'S RED` revenue is leaking quietly every month.

---

16 **Do refunds and cancellations reach the app?**

`TEST` Find a recent refund or cancelled subscription in Stripe and open the same customer in the app.

☑ `GREEN` the app shows it as refunded or cancelled.

■ `RED` the app still shows it as paid or active.

`IF IT'S RED` you keep serving, shipping or reporting revenue for customers who've left.

---

17 **Do the app's numbers match your books?**

`TEST` Compare last month's revenue or invoice total in the app with QuickBooks or your accounting system.

☑ `GREEN` they match, or the difference is known and explained.

■ `RED` an unexplained gap or double-posted invoices.

`IF IT'S RED` month-end takes hours of manual fixes, and tax and reporting figures can be wrong.

`E · CHECKS 18–21`

Backups and recovery

18 **When was your data last backed up?**

`TEST` Open your database dashboard and find the backups list.

☑ `GREEN` automatic daily backups, the latest within 24 hours.

■ `RED` no backups, or you can't find them.

`IF IT'S RED` one bad update, deleted table or locked account and your customer records are gone for good.

```
TOOL NOTES  Supabase: Database → Backups. Free-plan projects may show no backups
you can restore; paid plans include daily ones. Replit and Base44: check the
database or data settings for backup or export options.
```

---

19 **Has anyone ever restored a backup?**

`TEST` Ask who has restored one, when, and how long it took.

☑ `GREEN` someone restored a backup into a test copy in the last three months.

■ `RED` never tried.

`IF IT'S RED` an untested backup is a hope. You find out it doesn't work on the worst day.

---

20 **Can you undo a bad change to the app itself?**

`TEST` Find where the app's version history lives and name the last version you know was good.

☑ `GREEN` you know how to roll back in minutes.

■ `RED` nobody knows, or every fix is another prompt to the AI.

`IF IT'S RED` a change that breaks the app on a busy day stays broken until someone works out a fix.

```
TOOL NOTES  Lovable and Bolt keep a version history in the editor; Replit has
checkpoints and earlier deployments; GitHub keeps every committed version.
```

---

21 **Is there a copy of your data outside the builder?**

`TEST` Check when your key tables (customers, jobs, invoices) were last exported to a file stored in a company drive.

☑ `GREEN` within the last month.

■ `RED` never.

`IF IT'S RED` if the builder, the hosting account or the person holding it disappears, your data goes with them.

`F · CHECKS 22–25`

Ownership and monitoring

22 **Does your company own every account behind the app?**

`TEST` For the AI builder, hosting, database, domain, GitHub and Stripe, check who the owner is and which email address it uses.

☑ `GREEN` company email addresses, with at least two people from the company as admins.

■ `RED` any account owned by a freelancer's or employee's personal email.

`IF IT'S RED` if it isn't in your company's account, it isn't yours. One falling-out can lock you out of your own app.

---

23 **Could you move the app if you had to?**

`TEST` Check that the code sits in a GitHub account your company owns and that you can download your data.

☑ `GREEN` code in the company's GitHub, data exportable.

■ `RED` the code exists only inside the builder or in someone else's account.

`IF IT'S RED` you can't change hosting, hire a new developer or leave the tool without starting over.

`TOOL NOTES` `Lovable and Bolt can sync to GitHub; Replit projects can be downloaded or connected to Git; with Base44, check whether your plan includes code export.`

---

24 **Who finds out when the app breaks?**

`TEST` Ask: if the app went down at 2 a.m., who would know, and how? Look for an uptime monitor or error alerts.

☑ `GREEN` alerts go to a named person, who hears before customers do.

■ `RED` customers or staff are the alarm.

`IF IT'S RED` every outage runs longer than it needs to, and clients notice before you do.

---

25 **Do you know what the app costs to run each month?**

`TEST` Add up last month's bills: builder plan or credits, hosting, database, AI usage, email and text messages. Check that each service has a spending alert.

☑ `GREEN` a known monthly total and alerts set.

■ `RED` you don't know the total, or a bill has jumped without warning.

`IF IT'S RED` costs grow quietly as you add users, sometimes past what the app saves you.

REDS	WHAT IT MEANS
0	None of the common, visible gaps. Re-run the checklist every quarter and whenever someone leaves.
1	Fix it this week. Most single reds are a setting, not a rebuild.
2 or more	Two or more reds? Send us the app, we'll show you the fix. **Get a free Forward Scan**