

Checklist avant lancement pour les apps créées avec l'IA

12 vérifications à faire vous-même en 20 minutes environ. Pensée pour les apps Lovable, Bolt, Replit et Cursor sur Supabase + Stripe ; les principes valent pour toute stack.

Ne vérifiez que des apps qui vous appartiennent ou que vous êtes autorisé à tester.

Qui voit quoi

8 min

- ☐ 01 **La Row-Level Security est activée sur chaque table.**
Supabase → Advisors → Security Advisor : aucune erreur « RLS disabled ». Commencez par les tables qui contiennent des données utilisateurs.
- ☐ 02 **Aucune policy ne dit `true` sur des données privées.**
Authentication → Policies : une policy SELECT ou UPDATE avec `true` laisse entrer tout utilisateur connecté. Limitez-la au propriétaire ou à son équipe.
- ☐ 03 **Le test à deux comptes passe.**
Créez deux comptes dans deux équipes différentes. Connecté en tant que B, ouvrez une page de A ou changez un identifiant dans l'URL : vous ne devez rien voir.
- ☐ 04 **Un utilisateur ne peut pas s'auto-promouvoir.**
Les colonnes comme `role`, `plan` ou `credits` ne doivent pas être modifiables par l'utilisateur. Vérifiez la policy UPDATE et les droits par colonne de votre table de profils.

Clés et secrets

4 min

- ☐ 05 **Aucune clé secrète dans votre site.**
Ouvrez votre site en production → DevTools → Sources → Ctrl+Maj+F et cherchez `service_role`, `sk_live`, `sk-` et `secret`. Seule votre clé publique (anon / publishable) doit y figurer.
- ☐ 06 **Les clés exposées ont été renouvelées.**
Toute clé passée par le code front, une variable `VITE_` / `NEXT_PUBLIC_` ou l'historique git : renouvelez-la maintenant. Supprimer la ligne ne suffit pas.

Paielements

3 min

- ☐ 07 **Votre webhook Stripe vérifie les signatures.**
Le handler appelle `constructEvent` avec le secret de signature du webhook et rejette tout message non signé.
- ☐ 08 **Le forfait ne change que côté serveur, après paiement.**
La mise à niveau se fait dans le webhook quand `payment_status` vaut `paid`, jamais depuis un clic dans le navigateur.

Fichiers, sauvegardes, inscription

3 min

- ☐ 09 **Les fichiers des utilisateurs sont privés.**
Les buckets qui contiennent des fichiers envoyés ne sont pas publics ; les fichiers passent par des liens signés qui expirent.
- ☐ 10 **Vous avez testé une restauration.**
Les sauvegardes (ou la restauration à un instant T) sont activées, et vous avez restauré une copie au moins une fois, idéalement dans un projet de test.
- ☐ 11 **L'inscription a des garde-fous.**
Confirmation par e-mail activée, mots de passe de 10 caractères minimum, CAPTCHA ou limite de débit sur l'inscription et sur toute fonction IA.

E-mail

2 min

- ☐ 12 **Vos e-mails sont authentifiés.**
SPF et DKIM pour chaque service qui envoie en votre nom, plus un enregistrement DMARC. Vérification gratuite : postlaunch.agency/#email-check

Votre score

12 / 12

Vous êtes devant la plupart des apps créées avec l'IA. Revérifiez après chaque gros changement.

1 à 3 cases vides

Corrigez-les cette semaine. La plupart prennent moins d'une heure.

4 ou plus, ou un doute sur 1 à 3

Faites relire l'app avant d'encaisser plus de paiements.

Un doute sur certains points ? L'audit de mise en production Postlaunch vérifie tout cela et plus encore, preuves et correctifs à prix fixe à l'appui, en 5 jours ouvrés.