B W O R L D S

RAPPORT D'AUDIT TECHNIQUE

Maison Aubert, réservation et paiement en ligne

Préparé par l'équipe CTO BWORLDS

12 juin 2026

Confidentiel

10 CONSTATS SUR 4 DIMENSIONS

RÉSUMÉ

Maison Aubert est une boutique avec réservation et paiement en ligne, créée avec l'IA. La base est saine : rôles client et gérant séparés, paiement intégré, hébergement géré. L'audit a couvert quatre dimensions, la sécurité, l'intégrité des données, la performance et la conformité.

Il a identifié 1 point critique, 4 points importants et 5 points moyens. Le point critique (une clé de paiement exposée) et l'absence de consentement RGPD sont à refermer avant toute mise en ligne publique. Les correctifs sont simples et la plupart s'appliquent directement depuis votre outil de création.

1	4	5	~99,8 %
CRITIQUE	IMPORTANTS	MOYENS	DISPONIBILITÉ

Aperçu de la plateforme

Stack	Lovable, React + Vite, Supabase (Postgres + Auth), Stripe, Vercel
Application	Boutique, réservation de créneaux et paiement, rôles client et gérant
Disponibilité	~99,8 % sur 30 jours, aucun incident détecté
Temps de réponse	~600 ms en moyenne. Chemin vers la cible de 200 ms identifié
Audit	10 constats sur 4 dimensions, sécurité, intégrité des données, performance, conformité

JALON — « PRÊT À LIVRER »

L'app atteint le niveau de qualité requis pour être livrée au client quand ces quatre conditions sont réunies :

- ✓ **Fait** Disponibilité > 99,5 %
- ○ **À faire** Temps de réponse < 250 ms (cible 200 ms)
- ○ **À faire** 0 point critique
- ○ **À faire** Conformité RGPD couverte

État actuel : 1 / 4 atteint. Cible : avant la mise en ligne publique.

POINT CRITIQUE

CRITIQUE · À CORRIGER · SÉCURITÉ

Clé de paiement exposée côté client

La clé secrète Stripe est incluse dans le code envoyé au navigateur. N'importe quel visiteur peut l'extraire et créer ou rembourser des paiements à votre place. Recommandation : déplacer la clé secrète vers une fonction serveur et ne garder côté client que la clé publique.

`src/lib/stripe.ts · variable VITE_STRIPE_SECRET_KEY`

POINTS IMPORTANTS

IMPORTANT · À CORRIGER · SÉCURITÉ

Cloisonnement des comptes incomplet

La table des réservations n'a pas de règle d'accès par utilisateur. Un client connecté peut lire, via l'API, les réservations et les coordonnées d'un autre client. Recommandation : activer une politique d'accès (RLS) limitant chaque ligne à son propriétaire.

`table reservations · politique RLS manquante`

IMPORTANT · À CORRIGER · INTÉGRITÉ DES DONNÉES

Le chiffre d'affaires du tableau de bord affiche toujours zéro

La requête du tableau de bord interroge une table « commande » au singulier, qui n'existe pas. L'erreur est avalée en silence, le compteur reste donc bloqué à zéro. Le gérant peut croire qu'aucune vente n'a lieu.

`src/pages/Dashboard.tsx:64 · from('commande')`

IMPORTANT · À CORRIGER · INTÉGRITÉ DES DONNÉES

Données parfois périmées après un import

Le cache des disponibilités n'est pas vidé après l'import hebdomadaire des créneaux. Selon le moment, un client peut voir et réserver un créneau déjà pris. Recommandation : invalider le cache à la fin de chaque import.

`src/lib/availability-cache.ts:38`

PERFORMANCE : CHEMIN VERS 200 MS

Réponse actuelle à chaud : ~600 ms, mesurée depuis nos serveurs. Vos visiteurs en France ressentent un peu moins du fait de la proximité. Les principaux goulots et les gains pour atteindre la cible de 200 ms :

CORRECTIF	GAIN
Paginer la liste des réservations (charge les 30 prochaines au lieu de toutes)	**~180 ms**
Supprimer la requête N+1 sur les créneaux (un seul appel groupé)	**~120 ms**
Optimiser et redimensionner les images produits (3,2 Mo → ~400 Ko par page)	**~90 ms**
Mettre en cache la page d'accueil publique (contenu identique pour tous)	**~60 ms**

Charge utilisateur estimée après correctifs : ~190 ms. Cible de 200 ms atteinte.

CONFORMITÉ

IMPORTANT À CORRIGER CONFORMITÉ

Consentement aux cookies et mentions légales absents

Le site dépose des cookies de mesure d'audience sans recueillir le consentement, et ne publie ni politique de confidentialité ni mentions légales. Ces éléments sont obligatoires en France. Le risque est juridique autant que commercial pour votre client. Recommandation : bandeau de consentement et pages légales avant la mise en ligne.

`absence de bandeau de consentement · pages /mentions et /confidentialite`

POINTS MOYENS

#	POINT	DIMENSION
1	CORS ouvert (origine *) sur les fonctions edge. À restreindre au domaine de production.	Sécurité
2	L'import des créneaux fait confiance aux données envoyées par le navigateur sans les revalider côté serveur.	Intégrité des données
3	Aucune sauvegarde automatique : la base est en plan gratuit. Confirmer le passage en plan payant.	Fiabilité
4	Pas de page d'erreur. En cas de panne, l'utilisateur voit une page blanche sans explication.	Fiabilité
5	Les emails de confirmation partent sans limite de débit, un pic peut épuiser le quota d'envoi.	Fiabilité

CE QUI FONCTIONNE BIEN

Des bases solides

- Séparation claire des rôles client et gérant
- Paiement délégué à Stripe, aucune donnée de carte stockée chez vous
- Disponibilité élevée : ~99,8 % sur 30 jours, aucun incident
- Règles d'accès (RLS) déjà en place sur la majorité des tables
- Hébergement géré et déploiements automatiques
- Surveillance des erreurs déjà connectée

PLAN D'ACTION PRIORITAIRE

Classé par impact. Les points 1 à 4 sont à traiter avant la mise en ligne publique (jalon « prêt à livrer »).

#	ACTION	IMPACT	EFFORT
1	Déplacer la clé de paiement secrète vers une fonction serveur	**Critique**	Petit
2	Activer une règle d'accès par utilisateur sur les réservations	**Important**	Trivial
3	Ajouter le bandeau de consentement et les pages légales (RGPD)	**Important**	Moyen
4	Paginer les réservations et corriger la requête N+1 (vers 200 ms)	**Important**	Petit
5	Corriger la requête du chiffre d'affaires (« commandes » au pluriel)	**Important**	Trivial
6	Vider le cache des disponibilités après chaque import	Important	Petit
7	Confirmer le passage en plan payant et activer les sauvegardes	Moyen	Trivial
8	Restreindre le CORS au domaine de production	Moyen	Trivial
9	Ajouter une page d'erreur et optimiser les images produits	Moyen	Petit

Légende des efforts. Trivial = changement de configuration ou correctif d'une à deux lignes. Petit = moins d'une heure. Moyen = 2 à 4 heures.

EN RÉSUMÉ

Aucun chantier lourd. Les points 1 à 4 referment le risque critique, la fuite de données, la conformité et la performance, et font passer l'app au-dessus du jalon « prêt à livrer ». La plupart s'appliquent directement depuis votre outil de création. On reste disponibles pour vous accompagner sur chacun.

Restez tranquille, dans la durée

Une fois le jalon « prêt à livrer » atteint, l'app ne s'arrête pas de vivre. BWorlds, votre tiers de confiance technique, la surveille en continu et la ré-audite chaque mois sur les sept piliers. Vos clients restent rassurés, vous gardez l'esprit tranquille.

- ✓ Audit mensuel complet sur les 7 piliers, un rapport comme celui-ci
- ✓ Surveillance continue : disponibilité, erreurs, sessions
- ✓ Remédiation guidée, prête pour votre outil de création
- ✓ Vue claire de tout votre portefeuille client

bworlds.co/studio