

Rapport d'audit — extrait

EXEMPLE ANONYMISÉ

Réalisé par Corellia SRL — marque Unbroken · scan passif, en lecture seule

Ceci est un vrai rapport d'audit Unbroken, anonymisé. Nom du client, chemins et noms de fichiers ont été retirés ou généralisés. Les constats, gravités, recommandations et efforts estimés sont authentiques. Cet extrait présente **8 constats sur 16** — le rapport complet les détaille tous.

Audit passif. Analyse à distance, en lecture seule, sans modification ni test actif : ce qui est observable dans le code et en surface publique. Les constats issus de l'analyse statique sont à confirmer sur les environnements réels (base de données, console d'hébergement).

Synthèse par gravité

● Critique	2	FAMILLES COUVERTES Sécurité & secrets exposés · Règles d'accès aux données · Tenue sous charge · Dette structurelle · Tests & filet de sécurité · Conformité RGPD · Sauvegardes & restauration · Dépendances & hébergement · Chaîne de déploiement · Infrastructure & configuration de déploiement.
● Important	3	
● Mineur	5	
● Info	6	
Total constats	16	

Constats détaillés — sélection représentative

SÉCURITÉ & SECRETS EXPOSÉS

CRITIQUE Clé privée en clair dans le dépôt

F001

Une clé de compte de service est versionnée en clair — quiconque accède au dépôt (ou à son historique) obtient un accès direct au service.

EMPLACEMENT

```
backend/.../service-account.json:5
```

Recommandation : retirer la clé, la révoquer, purger l'historique git.

Effort estimé : < 1 j

CRITIQUE**Fichier .env présent dans le dépôt**

F004

Des fichiers d'environnement sont versionnés — ils contiennent très probablement des secrets (identifiants, jetons, chaînes de connexion).

EMPLACEMENTS

scripts/migration/.env.acceptance
scripts/migration/.env.integration
scripts/migration/.env.production

Recommandation : retirer du suivi git, ajouter à .gitignore, révoquer les secrets exposés.

Effort estimé : < 1 j

IMPORTANT**Secret potentiel codé en dur**

F002

7 occurrences détectées (hors tests, documentation et commentaires).

EMPLACEMENTS

ci/backend.yml:30
scripts/migration/.env.production:3
scripts/migration/export-1.ps1:13
(+4 autres)

Recommandation : déplacer en variable d'environnement, hors du code versionné.

Effort estimé : < 1 j

DETTE STRUCTURELLE**IMPORTANT****39 fichiers de production volumineux (> 400 lignes)**

F010

Les fichiers/composants trop longs sont difficiles à modifier sans régression (hors tests, mocks et artefacts de maquette).

EMPLACEMENTS

frontend/src/app/dashboard/data-table.component.ts — 1964 lignes
frontend/src/app/users/detail/list.component.ts — 1365 lignes
frontend/src/app/admin/migration-wizard.component.ts — 861 lignes
(+36 autres)

Recommandation : découper en modules/composants ciblés.

Effort estimé : variable

CONFORMITÉ RGPD

MINEUR

Journalisation possible de données personnelles

F015

Des appels de journalisation portent potentiellement sur des données personnelles (intercepteur d'API, écrans d'administration).

EMPLACEMENTS

mobile/src/shared/api/interceptor.ts:145
frontend/src/app/admin/list.component.ts:169
(+3 autres)

Recommandation : ne pas journaliser de données personnelles ; masquer ou omettre.

Effort estimé : faible

TENUE SOUS CHARGE

MINEUR

Image lourde (> 500 Ko)

F008

Une image non optimisée alourdit le chargement, surtout sur mobile.

EMPLACEMENT

mobile/assets/images/cover.jpg – 766 Ko

Recommandation : compresser, servir en WebP/AVIF, dimensionner selon l'usage.

Effort estimé : faible

TESTS & FILET DE SÉCURITÉ

INFO

313 fichiers de test détectés

F013

Un lanceur de tests est déclaré et une base de tests conséquente est présente — bon signe pour la maîtrise des régressions. Reste à confirmer la couverture réelle des chemins critiques.

Vérifications manuelles requises

Non automatisables sans accès aux environnements du client — traitées par l'auditeur lors de l'audit complet.

INFO

Confirmer la RLS / les règles sur la base LIVE

F006

L'analyse statique ne voit que le code. À vérifier sur le projet réel : RLS activée par table, politiques, buckets/stockage publics, grants du rôle « anon », authentification sur chaque route API.

Recommandation : revue en lecture seule de la console du fournisseur.

À vérifier : sauvegardes de la base (fréquence, rétention, restauration à un instant T), sauvegarde du stockage, et surtout qu'une **restauration complète a déjà été testée**. Contrôler aussi la reproductibilité de l'environnement (infrastructure as code).

Recommandation : activer des sauvegardes régulières et tester une restauration de bout en bout.

Conclusion

Ce scan a relevé **2 problèmes critiques** et 3 importants : des risques à traiter en priorité, à commencer par les secrets exposés dans le dépôt.

Aller plus loin

Ce rapport est un scan automatique et **ne remplace pas un audit complet**. Un audit Unbroken examine le code en profondeur (accès aux données, tenue sous charge, dette, tests, RGPD, dépendances, déploiement), rend un **verdict argumenté** — réparer ou reconstruire — et un **plan de correction chiffré**.

Demandez votre audit : www.unbroken.be/contact

Méthodologie

Audit passif appliqué selon les familles suivantes : Sécurité & secrets exposés · Règles d'accès aux données · Tenue sous charge · Dette structurelle · Tests & filet de sécurité · Conformité RGPD · Sauvegardes & restauration · Dépendances & hébergement · Chaîne de déploiement · Infrastructure & configuration de déploiement.