LOGO

Entreprise

Rapport de test d’intrusion

Application Web et Application Mobile

Killian Hoarau

Version	Date
v1.0	01/02/2026

LOGO Entreprise

Rapport de test d’intrusion

Version	Date
v1.0	01/02/2026

LOGO Entreprise

Rapport de test d’intrusion

Version	Date
v1.0	01/02/2026

Résumé exécutif

Entre le 01/01/2026 et le 01/02/2026, un test d’intrusion interne a été réalisé sur Application Web et sur Application Mobile.

Les travaux menés ont inclus des tests d’authentification, des tests d’autorisation, des tests de vulnérabilités applicatives non destructifs, des analyses de surface d’attaque ainsi que de la manipulation contrôlée de requêtes. Pour l’application mobile, une analyse statique et dynamique a également été réalisée, portant notamment sur les permissions, le stockage local et les flux réseau.

Les résultats mettent en évidence plusieurs axes d’amélioration en matière de sécurité, notamment concernant la robustesse des contrôles applicatifs, la gestion des accès et certains mécanismes de protection côté client et côté serveur. Aucune attaque destructive ni déni de service n’a été réalisé, conformément aux règles définies en amont. Les vulnérabilités identifiées présentent des impacts variables, allant de risques d’accès non autorisé à des scénarios de compromission partielle de comptes, selon les contextes.

Globalement, la posture de sécurité observée peut être qualifiée de perfectible. Les applications reposent sur des bases fonctionnelles solides, toutefois plusieurs faiblesses pourraient être exploitées par un attaquant disposant de connaissances techniques modérées. Ces constats soulignent l’importance de renforcer certains contrôles et d’intégrer davantage la sécurité dès les phases de conception et d’évolution.

Ce rapport détaille l’ensemble des vulnérabilités identifiées, accompagnées de preuves minimales, d’une évaluation de leur impact et de recommandations visant à réduire les risques et à améliorer durablement le niveau de sécurité des applications auditées.

LOGO Entreprise

Rapport de test d'intrusion

Version	Date
v1.0	01/02/2026

Introduction

1. Mention légale

Ce rapport contient une liste de découvertes effectuées lors de la période du test d'intrusion. Ce rapport ne doit pas être considéré comme une liste complète de toutes les vulnérabilités.

2. Notation du risque

Dans ce rapport, la sévérité des vulnérabilités identifiées a été évaluée. Le niveau de sévérité est évalué par rapport à la méthodologie d'évaluation des risques d'OWASP [1].

Document 1 : Méthodologie d'évaluation des risques d'OWASP

Sévérité globale du risque				
Impact	Élevé	Moyenne	Élevée	Critique
	Moyen	Faible	Moyenne	Élevée
	Faible	Informative	Faible	Moyenne
		Faible	Moyenne	Élevée
	Probabilité			

Comme il est possible de le voir dans le Tableau 1, la sévérité globale du risque est déterminée en combinant la probabilité d'exploitation avec l'impact que l'exploitation pourrait avoir. Une valeur de 0 à 9 est attribuée pour chacune des 2 variables : 0-2 est défini comme étant "Faible", 3-5 est "Moyenne", 6-9 est "Élevée".

La probabilité dépend de plusieurs facteurs relatifs aux différentes menaces et à la vulnérabilité identifiée. Avec des facteurs tels que le niveau de compétence et les motivations des acteurs malveillants, avec quelle facilité la vulnérabilité peut être exploitée et quelles sont les chances que l'exploitation soit détectée.

L'impact dépend de facteurs techniques et commerciaux tels que : la baisse de confidentialité, d'intégrité et de disponibilité, la

responsabilité, de potentiels dommages financiers, dommages sur l’image de la marque et violations de la vie privée.

Note : N’oubliez pas que l’évaluation de la sévérité est effectuée par Killian Hoarau et les notations peuvent changer d’une source à une autre.

3. Périmètre du test

Le périmètre du test comprend les composants suivants :
- Une application web accessible via Internet
- Une application mobile Android connectée au même socle fonctionnel

Les interfaces d’authentification, de gestion des utilisateurs et de contrôle d’accès associées.

Les tests ont été réalisés sur un environnement de production s’appuyant sur une base de données de test anonymisée. Cette configuration permet de réaliser des tests réalistes tout en limitant les risques pour les données réelles.

Des comptes de test ont été fournis afin de permettre la réalisation de tests authentifiés. Ces comptes incluent différents niveaux de privilèges, permettant de tester les mécanismes de contrôle d’accès et de séparation des rôles.

Les éléments suivants sont explicitement exclus du périmètre de cette mission :
- Tests de déni de service
- Attaques par force brute non encadrées
- Ingénierie sociale
- Exploitation destructive

4. Méthodologie

La mission a été réalisée selon une approche inspirée de la méthodologie PASSI, combinée aux bonnes pratiques de tests d’intrusion applicatifs et aux recommandations OWASP.

Le test s’est déroulé selon les phases suivantes :
- Analyse fonctionnelle et compréhension des applications
- Cartographie des surfaces d’attaque
- Tests d’authentification et de gestion de session
- Tests de contrôle d’accès
- Tests de vulnérabilités applicatives non destructifs

- Analyse spécifique de l'application mobile (statique et dynamique)

Synthèse des résultats

Les travaux réalisés ont permis d'identifier plusieurs vulnérabilités affectant l'application web et l'application mobile. Ces vulnérabilités présentent des niveaux de sévérité variables, allant de faiblesses informatives à des vulnérabilités de sévérité élevée.

La majorité des vulnérabilités identifiées concerne la gestion des accès, des mécanismes d'authentification et certains contrôles applicatifs. Aucune vulnérabilité critique permettant une compromission complète immédiate du système n'a été identifiée lors de cette mission.

Voici un récapitulatif du nombre de découvertes effectuées par niveau de sévérité :

Sévérité	Informative	Faible	Moyenne	Élevée	Critique
Nombre	0	0	0	2	0

Voici la liste détaillée des découvertes avec leur niveau de sévérité :

Découverte	**Sévérité**
WEB-01 : Faiblesse dans le contrôle d'accès à certaines fonctionnalités	Élevée
MOB-01 : Stockage local insuffisamment protégé de données applicatives	Élevée

Détails des découvertes

1. Application Web

WEB-01 : Faiblesse dans le contrôle d'accès à certaines fonctionnalités

Sévérité : Élevée

Description

Certaines fonctionnalités de l'application web ne mettent pas en œuvre des contrôles d'accès suffisamment stricts. Un utilisateur authentifié avec des privilèges limités peut accéder à des ressources ou actions normalement réservées à des profils plus élevés.

Impact

Cette vulnérabilité pourrait permettre un accès non autorisé à des fonctionnalités sensibles et conduire à une élévation de privilèges.

Preuve

Une manipulation contrôlée des requêtes HTTP permet d'accéder à une ressource restreinte sans les droits appropriés [2].

Document 2 : Capture d'écran des requêtes

<CAPTURE D'ÉCRAN>

Recommandations

Mettre en place des contrôles d'accès systématiques côté serveur et s'assurer que chaque action sensible vérifie explicitement les autorisations de l'utilisateur.

2. Application Mobile

MOB-01 : Stockage local insuffisamment protégé de données applicatives

Sévérité : Élevée

Description

L’analyse de l’application mobile a mis en évidence la présence de données applicatives stockées localement sans protection suffisante.

Impact

En cas d’accès physique ou logique à l’appareil, un attaquant pourrait accéder à des informations sensibles.

Preuve

Un fichier d’état de session a été identifié dans le stockage applicatif et contenait des informations lisibles en clair (identifiant utilisateur, paramètres applicatifs). Les valeurs ont été masquées dans la capture [3].

Document 3 : Capture d’écran du fichier

<CAPTURE D’ÉCRAN>

Recommandations

Utiliser des mécanismes de stockage sécurisé fournis par le système d’exploitation et limiter les données stockées localement au strict nécessaire.

Recommandations globales

Il est recommandé de renforcer les mécanismes de contrôle d’accès, de centraliser la gestion des autorisations et de renforcer la validation côté serveur.

Une attention particulière devrait être portée à la sécurisation des flux, à la gestion des sessions et aux pratiques de développement sécurisé.

La mise en place de tests de sécurité réguliers et l’intégration de la sécurité dès les phases de conception sont également recommandées.

Conclusion

Ce test d’intrusion a permis d’identifier plusieurs vulnérabilités affectant les applications auditées.

Bien que les applications reposent sur des bases fonctionnelles solides, certaines faiblesses pourraient être exploitées par un attaquant.

La correction des vulnérabilités identifiées et la mise en œuvre des recommandations formulées permettront d’améliorer significativement le niveau de sécurité global.