Corrigé Activité P1C11

Le comportement actuel de l'application est un exemple parfait de "Failing Open" en matière de divulgation d'informations. En renvoyant la trace technique complète à l'utilisateur final, l'application facilite grandement la tâche d'un cybercriminel en phase de reconnaissance. Si ce problème survient en production, un attaquant saura exactement quelles tables attaquer pour voler les données des clients.

Pour corriger ce défaut de résilience de manière systémique, vous devez rédiger et imposer la politique de gestion des erreurs suivante au sein du cadre d'exigences de TechNova :

"Afin de prévenir toute fuite d'informations sensibles et de garantir la résilience du système, l'application DOIT attraper (catch) les exceptions à la source via un gestionnaire global. Il est formellement INTERDIT de faire remonter des traces techniques (stack traces) ou des erreurs de base de données au client. En cas de crash, le système DOIT afficher un message standardisé et générique à l'utilisateur final, tout en journalisant les détails complets en interne pour alerter les administrateurs."

En imposant ce garde-fou, vous obligez l'équipe à séparer le traitement technique de l'affichage public. L'utilisateur ne verra plus qu'un message inoffensif, tandis que l'équipe de sécurité recevra une alerte détaillée contenant l'erreur SQL pour pouvoir corriger le bug sous-jacent.

Ne concevez jamais de ressources sans limites au sein de vos architectures ; imposez des quotas (rate limiting) pour prévenir l'épuisement total de la mémoire ou des bases de données lors d'exceptions répétées en boucle par un attaquant.