Corrigé Activité P1C2

Voici la démarche complète et l'exigence finale à formuler :

Le chef de produit commet ici l'erreur classique de se fier uniquement au *frontend* (l'interface utilisateur) en pensant que cacher le bouton suffit. Si le système génère des liens séquentiels (8754, puis 8755, etc.), un attaquant B2B, même authentifié sur son propre compte, peut facilement lancer un outil automatisé pour parcourir toutes les URL existantes et télécharger les factures de ses concurrents. C'est une faille IDOR par excellence.

Pour corriger cela de manière pérenne et appliquer le principe de "blocage par défaut", vous devez inscrire l'exigence fonctionnelle suivante dans le cahier des charges :

« Pour prévenir toute fuite de données, le système DOIT vérifier côté serveur, à chaque requête de téléchargement, que l'utilisateur actuellement authentifié possède explicitement les droits de propriété ou de lecture sur la facture demandée (via l'invoice_id), et ce conformément aux standards de l'ASVS v5.0. L'affichage ou non du bouton côté client n'est pas une mesure de sécurité valide. »

Pourquoi cette exigence est-elle efficace ?

En exigeant une vérification *côté serveur*, vous vous assurez que même si un attaquant devine l'URL exacte de la facture 8755, le contrôleur vérifiera dans la base de données : "Cet identifiant de session appartient-il au propriétaire de la facture 8755 ?". Si la réponse est non, l'accès est bloqué.

En complément, vous pourriez suggérer à l'équipe de remplacer les ID séquentiels par des UUID (Universally Unique Identifiers, ex: 550e8400-e29b-41d4-a716-446655440000) pour rendre le *force browsing* impossible, tout en maintenant obligatoirement l'exigence de contrôle d'accès serveur comme véritable rempart de sécurité.