OPENCLASSROOMS

Corrigé Activité P1C8

La proposition du chef de produit, bien qu'orientée vers le confort de l'utilisateur, crée deux vulnérabilités critiques de la catégorie A07 qui permettraient un piratage instantané des comptes clients B2B.

Voici le veto technique et l'exigence de correction que vous devez formuler pour l'équipe Produit :

L'exposition d'un jeton de session dans l'URL est une pratique extrêmement dangereuse. Les URL sont souvent stockées en clair dans l'historique du navigateur du client, dans les logs des serveurs web intermédiaires, ou encore envoyées à des sites tiers via l'en-tête HTTP "Referer". Un attaquant pourrait simplement regarder par-dessus l'épaule de la victime (shoulder surfing), copier l'URL, ou fouiller l'historique d'un ordinateur partagé pour usurper immédiatement la session du client.

De plus, une session sans date d'expiration (qui n'est pas fermée automatiquement) laisse une fenêtre d'attaque permanente en cas d'oubli de déconnexion, ce qui arrive fréquemment sur des postes informatiques en entreprise.

Pour corriger ces défaillances, voici le garde-fou obligatoire à inscrire dans les spécifications :

"Le système NE DOIT JAMAIS exposer les identifiants de session dans l'URL. Le système DOIT utiliser exclusivement des cookies sécurisés (marqués avec les attributs Secure et HttpOnly) pour transporter le jeton. Enfin, toutes les sessions DOIVENT être automatiquement invalidées par le serveur après un délai d'inactivité strict, sans attendre une action manuelle de l'utilisateur."

N'imposez pas de rotation arbitraire des mots de passe aux utilisateurs (ex: les forcer à changer de mot de passe tous les 90 jours). Les standards modernes du NIST ont prouvé que cette pratique frustre les utilisateurs, qui se contentent d'ajouter un chiffre à la fin de leur mot de passe ("MotDePasse1" devient "MotDePasse2"), facilitant grandement les attaques par bourrage hybride. Forcez la réinitialisation uniquement si vous suspectez une compromission de la base de données.