Authentic 2 - Development #70816

Suivre les bonnes pratiques pour la fonctionnalité "Se souvenir de moi"

28 octobre 2022 11:59 - Benjamin Dauvergne

Statut:	Nouveau	**Début:**	28 octobre 2022
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

Ça n'est pas du tout implémenté comme il faut (my bad), augmenter la durée des sessions est une très mauvaise idée. Déjà au niveau sécurité mais ça enlève aussi des évènements login pour correctement l'utilisation du service.

En suivant les recommandations (mélange d'OWASP et de lectures sur stackmachin) on devrait faire comme cela :

Mise en place

Si la case à cocher "Se souvenir de moi" est cochée :

- générer une valeur aléatoire X
- créer un jeton (authentic2.models.Token) de type "rememberme" avec une durée de vie adaptée (disons 3 mois), lier ce jeton au compte (ça vaut la peine d'ajouter une colonne user, nullable, à Token) indexé par le hash sha256 tronqué de X à 128bits (UUID(bytes=hashlib.sha256(random_value).digest()[:16])).
- ne pas toucher à la durée de vie des sessions
- poser un cookie RememberMe, HttpOnly, Secure, SameSite=Lax avec la valeur de X

L'utilisation d'un hash empêche qu'une fuite de donnée au niveau de la base de donnée ne donne accès à l'application. Idéalement les session_id devraient être gérés de la même façon mais c'est un autre sujet.

Utilisation

Sur la page de login, si cookie RememberMe présent prendre le hash256 tronqué de sa valeur de sa valeur, en faire un uuid comme plus haut et chercher un jeton correspondant:

- si trouvé, connecter le compte associé, et rediriger immédiatement
- si non trouvé, supprimer le cookie et continuer normalement.

Suppression

Sur toute déconnexion ou changement de mot de passe, supprimer tous les jetons remember-me. C'est gênant pour les gens qui utilisent deux terminaux, un en se loggat normalement et l'autre via ce cookie, mais je ne vois de moyen de rendre ça sûr et à la fois facilement gérable, ne pas les supprimer c'est risqué que des jetons traînent sans l'utilisateur ne s'en rende compte et ajouter un écran pour les gérer un par un c'est une usine à gaz pour les utilisateurs qui ont autre chose à faire.

Il faut prévoir la migration des sessions existantes vers ce mécanisme, elles sont faciles à détecter, une clé remember_me=True est posée dans la session. Si cette clé est présente remettre une durée normale à la session et poser le cookie.