Authentic 2 - Development #25579

bouton "Se souvenir de moi" / remember me

03 août 2018 15:51 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	03 août 2018
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	

Description

L'option sera à activé dans les settings "A2_USER_REMEMBER_ME=<durée en secondes>", ce sera la durée de la prolongation de session par défaut quand le bouton est utilisé.

Pour chaque ou on aura par ailleurs un paramétrage remember_me qui pourra être différent et par défaut à None. 0 désactivera le comportement.

Pour l'implémentation:

- ajout d'une case à cocher quand l'option est activée (bool(remember_me) is True)
- si case cochée on calcule now() + timedelta(seconds=<remember_me>) et on pose une expiration explicite pour la session
- on pose remember_me=True dans la session pour se souvenir que cette option est activée

Cela aura une influence en SAML sur le sessionNotOnOrAfter, à voir si on réduit celle-ci à quelque chose de plus raisonnable (disons au pire le minimum en expiry_date et now()+24H); l'idée étant de ne pas laisser des sessions ouvertes sans fins dans chaque application.

Révisions associées

Révision 99a7b14b - 03 août 2018 18:52 - Benjamin Dauvergne

add a remember me button (fixes #25579)

It simply use session.set_expiry() to augment the session duration.

Historique

#2 - 03 août 2018 16:39 - Benjamin Dauvergne

Référence owasp: https://www.owasp.org/index.php/PHP_Security_Cheat_Sheet#Remember_Me

Je ne pense pas que ce soit utile de recopier leur façons de faire, parce que Django gère déjà l'expiration des sessions au niveau du modèle les stockant.

#3 - 03 août 2018 16:51 - Emmanuel Cazenave

Pas compris la différence entre zéro et None pour l'option.

#4 - 03 août 2018 17:16 - Benjamin Dauvergne

- Fichier 0001-add-a-remember-me-button-fixes-25579.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

Bon je passe outre mes propres tergiversations, voilà un patch.

#5 - 03 août 2018 17:17 - Benjamin Dauvergne

Bon finalement c'est plus compliqué, les sessions django ne stocke pas une date absolu mais une durée, à chaque sauvegarde de la session, le max_age/expires est recalculé à partir de la date courante et de cette durée, ainsi que l'attribute expire_date du modèle en base.

Coté authentic on a le middleware ViewRestrictionMiddleware qui vérifie si l'utilisateur à un password_reset en cours qui fait ça toutes les 10s mais pour cela stocke en session la date du dernier check et donc toutes les 10s on a forcément une nouvelle sauvegarde de session, en gros à chaque accès ou presque on en reprend pour A2_USER_REMEMBER_ME secondes.

Je ne sais pas si c'est extrêmement gênant.

PS: commentaire écrit avant de soumettre le patch.

#6 - 03 août 2018 17:19 - Benjamin Dauvergne

Emmanuel Cazenave a écrit :

> Pas compris la différence entre zéro et None pour l'option.

Pour l'instant je n'ai pas implémenté la restriction par OU, je garde ça sous le coude.

Par défaut le champ OU.remember_me serait à None, ne faisant rien qu'appliquer le comportement global, une durée quelconque remplacerait la durée configurée par A2_USER_REMEMBER_ME, et une valeur de 0 désactiverait remember_me pour cet utilisateur, il aurait les sessions normales.

#7 - 03 août 2018 17:50 - Emmanuel Cazenave

En publik devinst, le boutton 'remember me' n'apparait pas.

#8 - 03 août 2018 18:07 - Benjamin Dauvergne

Bizarre, ici ça marche bien, tu as bien mis A2_USER_REMEMBER_ME=1234 dans ton local_settings.py ou idem ?

#9 - 03 août 2018 18:22 - Emmanuel Cazenave

- Statut changé de Solution proposée à Solution validée

voilà c'est mieux avec le setting.

#10 - 03 août 2018 18:55 - Benjamin Dauvergne

- Statut changé de Solution validée à Résolu (à déployer)

- % réalisé changé de 0 à 100

Appliqué par commit authentic2|99a7b14bf0e038eb6973dcd0d459713a8ea323bc.

#11 - 13 décembre 2018 22:35 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

0001-add-a-remember-me-button-fixes-25579.patch	5,97 ko	03 août 2018	Benjamin Dauvergne