

Passerelle - Development #41245

nonce exigé mais inutilisé pour la signature

02 avril 2020 08:34 - Frédéric Péters

Statut:	Fermé	Début:	02 avril 2020
Priorité:	Normal	Echéance:	
Assigné à:		% réalisé:	0%
Catégorie:		Temps estimé:	0:00 heure
Version cible:		Planning:	Non
Patch proposed:	Oui		
Description			
Que ça ne soit plus obligatoire, ou que ça soit testé.			

Révisions associées

Révision 9f6da963 - 02 avril 2020 19:34 - Thomas Noël

signature: do not require nonce if not verified (#41245)

+ some fixes, sync with <http://git.entrouvert.org/hobo.git/tree/hobo/signature.py>

Historique

#1 - 02 avril 2020 10:44 - Thomas Noël

- Fichier 0001-signature-do-not-require-nonce-if-not-verified-41245.patch ajouté
- Statut changé de Nouveau à Solution proposée
- Patch proposed changé de Non à Oui

#2 - 02 avril 2020 13:33 - Thomas Noël

(je suis conscient que c'est juste du code mort mais j'ai pour objectif de garder exactement le même code de signature/vérification dans tous nos modules) (et là, en les relisant, je découvre quelques autres petits bogues)

#3 - 02 avril 2020 13:47 - Thomas Noël

- Statut changé de Solution proposée à En cours

Me suis planté dans la logique, je refais.

#4 - 02 avril 2020 14:12 - Thomas Noël

- Fichier 0001-signature-do-not-require-nonce-if-not-verified-41245.patch ajouté
- Statut changé de En cours à Solution proposée

Voilà la bonne logique, on ne vérifie que si known_nonce n'est pas None (mais on répond bien "False" si nonce n'est pas présent).

J'ai ajouté les tests (en fait ceux de hobo) et synchronisé le code avec hobo au passage. Pour qu'ils fonctionnent on ajoute dans le système de signature la possibilité de ne pas inclure de nonce en envoyant nonce="".

Les tests permettent aussi de voir qu'on ne passait pas known_nonce et timedelta de check_url à check_query, c'est donc fait ici.

Au passage, sign_string a un argument complètement inutile, timedelta, qui n'a pas de sens ici, hop, je supprime, merci.

#5 - 02 avril 2020 18:58 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

#6 - 02 avril 2020 19:35 - Thomas Noël

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

```
commit 9f6da963a4aa424af9c8becf6b9b4a6ddd594fc9
Author: Thomas NOEL <tnoel@entrouvert.com>
Date: Thu Apr 2 10:44:00 2020 +0200
```

```
signature: do not require nonce if not verified (#41245)
```

```
+ some fixes, sync with http://git.entrouvert.org/hobo.git/tree/hobo/signature.py
```

#7 - 07 avril 2020 09:15 - Frédéric Péters

- Statut *changé de Résolu* (à déployer) à *Solution déployée*

Fichiers

0001-signature-do-not-require-nonce-if-not-verified-41245.patch	1,56 ko	02 avril 2020	Thomas Noël
0001-signature-do-not-require-nonce-if-not-verified-41245.patch	7,29 ko	02 avril 2020	Thomas Noël