

Combo - Bug #17173

assurer que user_nameid et user_email ne puissent être forgés dans les urls

24 juin 2017 11:21 - Frédéric Péters

Statut: Fermé	Début: 24 juin 2017
Priorité: Normal	Echéance:
Assigné à:	% réalisé: 0%
Catégorie:	Temps estimé: 0:00 heure
Version cible:	Planning:
Patch proposed: Oui	
Description Pour le moment user_nameid et user_email sont posés uniquement quand l'utilisateur est connecté; avec le post sur la cellule json qui tape toutes les données transmises par l'utilisateur dans le contexte, on peut imaginer un utilisateur non connecté qui ajoute un user_nameid trafiqué dans le formulaire transmis et ça passera. Pour éviter ça, il suffit de toujours définir user_nameid/user_email.	
Demandes liées:	
Lié à Combo - Bug #17172: post : pouvoir utiliser les données transmises dans...	Fermé 24 juin 2017
Lié à Passerelle - Development #17171: json data store : autoriser name_id da...	Fermé 24 juin 2017

Révisions associées

Révision a353802d - 29 juin 2017 08:50 - Frédéric Péters

utils: make sure user_nameid/user_email cannot be forged (#17173)

Révision b1b80dc9 - 29 juin 2017 09:14 - Frédéric Péters

misc: always use a fresh copy of parameters (#17173)

(this is required for tests)

Historique

#1 - 24 juin 2017 11:22 - Frédéric Péters

- Fichier 0001-utils-make-sure-user_nameid-user_email-cannot-be-for.patch ajouté
- Statut changé de Nouveau à En cours
- Patch proposed changé de Non à Oui

#2 - 24 juin 2017 11:22 - Frédéric Péters

- Lié à Bug #17172: post : pouvoir utiliser les données transmises dans l'url appelée ajouté

#3 - 24 juin 2017 11:22 - Frédéric Péters

- Lié à Development #17171: json data store : autoriser name_id dans les actions de modification ajouté

#4 - 26 juin 2017 10:19 - Frédéric Péters

- Fichier 0001-utils-make-sure-user_nameid-user_email-cannot-be-for.patch ajouté

Avec la mise à jour d'un test pour prendre en compte que user_nameid/user_email sont désormais systématiquement disponibles.

#5 - 26 juin 2017 14:32 - Thomas Noël

Ok même si je trouverai plus joli que la ligne user = getattr(context.get('request'), 'user', None) soit placée en dessous du template_vars['user_nameid'] = "

#6 - 29 juin 2017 08:52 - Frédéric Péters

- Statut changé de En cours à Résolu (à déployer)

Avec l'inversion de ligne suggérée.

commit a353802d12e96541c9edbe12ca2181ed49f75b0b
Author: Frédéric Péters <fpeters@entrouvert.com>
Date: Sat Jun 24 11:18:00 2017 +0200

```
utils: make sure user_nameid/user_email cannot be forged (#17173)
```

#7 - 23 décembre 2018 15:18 - Frédéric Péters

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

Fichiers

0001-utils-make-sure-user_nameid-user_email-cannot-be-for.patch	918 octets	24 juin 2017	Frédéric Péters
0001-utils-make-sure-user_nameid-user_email-cannot-be-for.patch	2,24 ko	26 juin 2017	Frédéric Péters