w.c.s. - Development #9005

Les utilisateurs "administrateur du site" n'ont pas accès à toutes les APIs

17 novembre 2015 11:34 - Benjamin Dauvergne

Statut:	Rejeté	**Début:**	17 novembre 2015
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

Ça rend assez difficile l'écriture d'un outil qui synchronise w.c.s. avec autre chose (par exemple ElasticSearch), l'utilisateur utilisé pour faire les requêtes devant appartenir à tous les rôles.

Historique

#1 - 17 novembre 2015 11:34 - Benjamin Dauvergne

- Tracker changé de Bug à Development

#2 - 17 novembre 2015 11:35 - Benjamin Dauvergne

- Fichier 0001-api-admin-can-access-all-formdatas-9005.patch ajouté

- Patch proposed changé de Non à Oui

#3 - 17 novembre 2015 11:41 - Benjamin Dauvergne

- Fichier 0001-api-admin-can-access-all-formdatas-9005.patch ajouté

En simplifiant un peu le control-flow.

#4 - 17 novembre 2015 11:45 - Benjamin Dauvergne

- Fichier 0001-api-admin-can-access-all-formdatas-9005.patch supprimé

#5 - 17 novembre 2015 11:46 - Benjamin Dauvergne

Le deuxième patch était too much il laissait les utilisateurs non-admin voir le formdata complet ce qui n'est pas voulu.

#6 - 17 novembre 2015 13:39 - Frédéric Péters

Je ne suis pas sûr, j'espérais (un petit peu) préserver les accès à l'API de l'utilisation de is_admin. Tu peux te contenter d'assigner les rôles pour le moment, qu'on ait le temps de se poser pour réfléchir à l'accès aux API ?

#7 - 17 novembre 2015 15:34 - Benjamin Dauvergne

Frédéric Péters a écrit :

> Je ne suis pas sûr, j'espérais (un petit peu) préserver les accès à l'API de l'utilisation de is_admin. Tu peux te contenter d'assigner les rôles pour le moment, qu'on ait le temps de se poser pour réfléchir à l'accès aux API ?

Oui j'ai déjà cliqué nerveusement dans authentic et donc ça appelle une action de masse coté authentic.

#8 - 17 novembre 2015 15:47 - Benjamin Dauvergne

Pour moi les paramètres email/NameID sur système de signature ne sont pas là pour la sécurité (de toute façon un combo "piraté" a accès à tout en prenant n'importe quel rôle de n'importe quel utilisateur) mais pour simuler pour un combo ce qu'un utilisateur a effectivement le droit de voir. Dans la plupart des cas une signature sans utilisateur désigné devrait donner un accès complet aux données, c'est déjà le cas il me semble pour les APIs sur les utilisateurs ou sur les rôles.

Donc je serais pour que si on a is_url_signed() and not get_user_from_api_query_string() qui est vrai, on ait les pleins droits. D'ailleurs je vais faire une proposition pour une révision constitutionnelle.

#9 - 06 décembre 2015 14:29 - Benjamin Dauvergne

- Patch proposed changé de Oui à Non

#10 - 10 juin 2016 13:13 - Benjamin Dauvergne

A priori abandonné en faveur du mode anonyme, si tout le monde est d'accord je rejette.

#11 - 24 septembre 2019 11:23 - Benjamin Dauvergne

- Statut changé de Nouveau à Rejeté

- Assigné à Benjamin Dauvergne supprimé

Sur le fond j'ai raison (la restriction actuelle n'améliore pas la sécurité, c'est juste bloquant).

Fichiers

0001-api-admin-can-access-all-formdatas-9005.patch	1,18 ko	17 novembre 2015	Benjamin Dauvergne