Hobo - Bug #13914

sécurisation de la configuration par défaut de django-rest-framework

09 novembre 2016 11:51 - Thomas Noël

Statut:	Fermé	**Début:**	09 novembre 2016
Priorité:	Normal	**Echéance:**	
Assigné à:	Thomas Noël	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	

Description

Actuellement hobo **ajoute** l'autorisation par signature pour DRF à des autorisations par défaut (basic et session).

Il serait plus prudent de n'autoriser que les URL signées. Exemple de soucis : les API chrono ouvertes à un user connecté sur chrono, alors qu'on devrait imposer l'accès par signature.

Et, dans la foulée, de fermer par défaut toutes les vues DRF en imposant la permission IsAuthenticated.

Révisions associées

Révision 17c0f375 - 18 novembre 2016 10:04 - Thomas Noël

secure Django Rest Framework auth in django_config_common (#13914)

Historique

#1 - 09 novembre 2016 11:56 - Thomas Noël

- Fichier 0001-secure-Django-Rest-Framework-auth-in-django_config_c.patch ajouté

- Statut changé de Nouveau à En cours

- Patch proposed changé de Non à Oui

#2 - 15 novembre 2016 01:20 - Serghei Mihai

Chrono, corbo exigent déjà la permission rest_framework.permissions.IsAuthenticated, si je ne me trompe pas.

#3 - 15 novembre 2016 07:07 - Thomas Noël

Serghei Mihai a écrit :

> Chrono, corbo exigent déjà la permission rest_framework.permissions.IsAuthenticated, si je ne me trompe pas.

L'idée est ici qu'on utilise DRF pour faire des API Publik, et que celles-ci doivent être toutes protégées par signature : on le précise et on le force donc dans hobo, qui est la glue qui fait de nos logiciels un ensemble nommé "Publik".

Mais dans le code des logiciels qui utilisent DRF, dans chrono, corbo, combo… on peut tout à fait imposer/préciser d'autres permission/authentification. Et c'est même important.

#4 - 15 novembre 2016 09:28 - Serghei Mihai

Ack

#5 - 18 novembre 2016 10:05 - Frédéric Péters

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

Poussé; à rapidement tagguer pour que ça soit bien vérifié sur la recette.

```
commit 17c0f375b5e8e3386baeb241d5138dcce1fa5434
Author: Thomas NOEL <tnoel@entrouvert.com>
Date:   Wed Nov 9 11:54:48 2016 +0100

    secure Django Rest Framework auth in django_config_common (#13914)
```

#6 - 23 décembre 2018 16:01 - Frédéric Péters

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

Fichiers

0001-secure-Django-Rest-Framework-auth-in-django_config_c.patch	1,37 ko	09 novembre 2016	Thomas Noël