w.c.s. - Development #55858

auth http basic pour l'API de création de demande

27 juillet 2021 13:55 - Frédéric Péters

Statut:	Fermé	**Début:**	27 juillet 2021
Priorité:	Normal	**Echéance:**	
Assigné à:	Lauréline Guérin	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Pour le moment cette API impose encore la signature.

Demandes liées:

Lié à w.c.s. - Development #20624: Permettre l'accès http/auth à la plupart d...	**Fermé**	**12 décembre 2017**

Révisions associées

Révision e44cf60a - 27 septembre 2021 09:52 - Lauréline Guérin

api: add basic auth support to forms submit (#55858)

Historique

#1 - 13 septembre 2021 14:32 - Mikaël Ates (de retour le 29 avril)

- Lié à Development #20624: Permettre l'accès http/auth à la plupart des API ajouté

#2 - 14 septembre 2021 12:03 - Lauréline Guérin

- Assigné à mis à Lauréline Guérin

#3 - 14 septembre 2021 15:05 - Lauréline Guérin

note: création de fiche traité dans #54350

#4 - 14 septembre 2021 15:05 - Lauréline Guérin

- Sujet changé de auth http basic pour l'API de création de demande/fiche à auth http basic pour l'API de création de demande

- Description mis à jour

#5 - 14 septembre 2021 15:51 - Lauréline Guérin

- Fichier 0001-api-add-basic-auth-support-to-forms-submit-55858.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#6 - 16 septembre 2021 09:39 - Benjamin Dauvergne

- Statut changé de Solution proposée à En cours

Est-ce qu'on a écrit quelque part les règles d'accès implicites qu'on souhaite pour les api-user ? Est-ce que c'est juste équivalent aux signatures ou bien on cherche à avoir des règles d'accès plus fin ?

Parce que je vois que ceux-ci ont des rôles, que dans le cas de submit() ces rôles ne sont contrôlés que dans le cas de la soumission backoffice, reproduisant le comportement en utilisant les signatures. Sauf que les signatures permettent de se faire passer pour n'importe qui sans contrôle, donc c'est un contrôle purement logique qui est fait, pour ne pas simuler une soumission avec un utilisateur qui ne pourrait pas le faire directement en BO.

Si meta.get('backoffice-submission') alors aucun contrôle n'est fait, et donc on a aucun contrôle d'accès sur les ApiUser faisant des submit qui peuvent donc simuler des soumissions en front en prenant l'identité de n'importe qui (via json_input['user']).

Le code m'a l'air ok, ma question porte plus sur l'objectif qui aurait du être discuté avant de passer à l'implémentation.

Dans le fond je me demande si c'est ce qu'on veut, sachant que les ApiUser ont été introduit pour justement rendre plus fin le contrôle d'accès, malheureusement dans un cas très restreint qui est celui du chatbot du CD06 devant avoir accès uniquement aux données anonymisés de tous les formulaires d'un utilisateur. Mais si je prends ce cas, on va donner la possibilité au chatbot de faire des soumissions, et je sais qu'on ne veut pas ou

alors seulement sur certains (ça n'a pas été évoqué).

#7 - 20 septembre 2021 14:55 - Frédéric Péters

Je dirais le premier truc facile, c'est que s'il y a des rôles posés sur l'ApiAccess il faut alors les prendre en compte. Sur la situation ici je dirais que ça signifie les regarder par rapport à backoffice_submission_roles, et ne pas autoriser autre chose que l'enregistrement "saisie backoffice".

Par contre, s'il n'y a pas de rôles posés, je ne sais pas encore trop si ça doit être tout autoriser, ou pas. Je tendrais à pencher pour l'option de ne rien autoriser de particulier, parce que ce sera plus facile de changer ça pour finalement accepter des trucs que de fermer une API qui aurait été trop ouverte.

Pour moi donc, ici, l'accès HTTP auth Basic pour la création de demande, on lui pose comme limite que le paramétrage de l'accès API doit préciser ces rôles en accord avec formdef.backoffice_submission_roles, je dirais aussi qu'on peut dans ce cas ne pas avoir meta/backoffice-submission, i.e. avoir quelque chose comme :

```
          meta = json_input.get('meta') or {}
-         if meta.get('backoffice-submission'):
+         if meta.get('backoffice-submission') or (user and user.is_api_user):
```

#8 - 23 septembre 2021 10:10 - Lauréline Guérin

- Fichier 0001-api-add-basic-auth-support-to-forms-submit-55858.patch ajouté

- Statut changé de En cours à Solution proposée

#9 - 24 septembre 2021 09:13 - Frédéric Péters

- Statut changé de Solution proposée à Solution validée

#10 - 27 septembre 2021 10:27 - Lauréline Guérin

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

```
commit e44cf60a88fc81fc9221f879b9f83a75d1b5253d
Author: Lauréline Guérin <zebuline@entrouvert.com>
Date:   Tue Sep 14 15:49:48 2021 +0200

    api: add basic auth support to forms submit (#55858)
```

#11 - 27 septembre 2021 21:18 - Frédéric Péters

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

Fichiers

0001-api-add-basic-auth-support-to-forms-submit-55858.patch	9,4 ko 14 septembre 2021	Lauréline Guérin
0001-api-add-basic-auth-support-to-forms-submit-55858.patch	12,1 ko 23 septembre 2021	Lauréline Guérin