w.c.s. - Development #37808

Interdire l'accès à une demande anonyme en frontoffice

20 novembre 2019 11:06 - Thomas Noël

Statut:	Fermé	**Début:**	20 novembre 2019
Priorité:	Normal	**Echéance:**	
Assigné à:	Nicolas Roche	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Oui

Description

Quand on n'est pas connecté et qu'on clique sur l'URL frontoffice d'une demande déposée anonymement, on est renvoyé vers la page de login.

Le but étant que w.c.s. cherche à savoir si la personne devant l'écran a ou pas une fonction lui permettant de voir cette demande.

Mais je pense qu'on frontoffice on pourrait interdire cela, car c'est en backoffice que se passent les actions de traitement.

Je proposerais donc que lorsqu'on est anonyme et qu'on clique sur une URL de demande frontoffice anonyme, alors on reçoive juste un message "accès interdit"

Demandes liées:

Lié à w.c.s. - Development #38077: Accès aux brouillons via le code de suivi	**Fermé**	**29 novembre 2019**

Historique

#2 - 20 novembre 2019 11:09 - Thomas Noël

Une conséquence du comportement actuel : la personne qui a fait une demande anonyme, si elle revient "plus tard" sur l'URL de sa demande, par hasard ou historique de son navigateur, elle va être envoyée vers la page de login... alors que jamais cela ne lui permettra de voir sa demande. (mais elle va quand même tenter de se créer un compte car elle aura l'impression que c'est ce qu'on lui demande, et c'est encore plus d'incompréhension...)

#3 - 20 novembre 2019 11:22 - Stéphane Laget

Surtout cela va poser pb avec les utilisations actuelles.
Si la personne a un compte, on lui envoie par mail directement le lien vers le formulaire, on s'attend alors légitimement à qu'il se connecte pour accéder à sa demande.

#4 - 20 novembre 2019 11:27 - Thomas Noël

Stéphane Laget a écrit :

> Surtout cela va poser pb avec les utilisations actuelles.
> Si la personne a un compte, on lui envoie par mail directement le lien vers le formulaire, on s'attend alors légitimement à qu'il se connecte pour accéder à sa demande.

Si le formulaire est lié à son compte il sera accesssible bien sûr. Je parle ici des demandes déposées anonymement, qui ne sont pas liées à un usager. On envoie même pas l'URL de ces demandes.

#5 - 20 novembre 2019 11:31 - Benjamin Dauvergne

Ça rejoint un peu, mais dans l'autre sens, la solution proposée sur #37095; si un utilisateur est attaché à un formulaire (brouillon ou pas), on force l'authentification si il n'y pas d'utilisateur accès interdit et/ou proposer d'entrer un code de suivi (la dernière solution me parait mieux).

#6 - 20 novembre 2019 12:30 - Nicolas Roche

Oui, sinon je pige pas car je pensais que ce que vous décrivez était déjà pris en compte par #29218.

#7 - 20 novembre 2019 14:54 - Benjamin Dauvergne

Nicolas Roche a écrit :

> Oui, sinon je pige pas car je pensais que ce que vous décrivez était déjà pris en compte par #29218.

On ne parle pas de code de suivi ici (enfin moi un peu), il y a des URLs différentes pour un formulaire qui ont des comportements différents:
1. /slug/<id> pour un brouillon connecté
2. /slug/<id>/ pour un formulaire soumis connecté ou après utilisation du code de suivi
3. /(slug/)?code/<tracking-code/load pour retrouver un formulaire avec tracking code (ensuite ça redirige vers les deux autres URLs)

#29218 ça concerne la 3ème URL pour qu'elle fonctionne même si on est connecté.

Ici on demande à ce que les 2 premières URLs n'invoquent pas d'authentification quand le formulaire visé n'est pas attaché à un utilisateur et moi je rajoute que ce serait bien d'indiquer qu'un code de suivi est nécessaire pour y accéder à ce moment là plutôt que de simplement afficher "Accès interdit".

#8 - 22 novembre 2019 16:00 - Nicolas Roche

- Statut changé de Nouveau à Information nécessaire

- Assigné à mis à Nicolas Roche

- Planning changé de Non à Oui

J'ai essayé en me plaçant au début de *wcs/forms/root.py::FormPage::_q_lookup()* :

```
        # forbidden direct anonymous acces to anonymous formdata on frontoffice
        if get_request().is_in_frontoffice() and not (
                filled.user_id or get_request().user
                or session.is_anonymous_submitter(filled)):
            message = ''
            if filled.get_formdef().enable_tracking_codes:
                message = 'You can access to this page using its tracking code.'
            raise errors.AccessForbiddenError(message)
```

parce qu'après on part dans 2 directions :
ici,

```
        if not filled.is_draft():
...
            return PublicFormStatusPage(self.formdef, filled)
```

ou là

```
        # restore draft
        ...
```

Le problème c'est que l'API passe également par là :

- 'jump/trigger/XXX'
- 'hooks/XXX/'

or les jumps et les hooks ne sont pas détectés par get_request().is_in_api().

#9 - 23 novembre 2019 09:36 - Nicolas Roche

- Fichier 0001-forms-forbidden-direct-anonymous-acces-to-anonymous-.patch ajouté

- Statut changé de Information nécessaire à Solution proposée

- Patch proposed changé de Non à Oui

Avec l'aide de Thomas : je me place à l'autre extrémité, là où on lève l'exception qui renvoie vers la page de login.

#10 - 29 novembre 2019 16:23 - Nicolas Roche

- Fichier 0001-forms-forbidden-direct-anonymous-acces-to-anonymous-.patch ajouté

Rebasé avec les tests sur les accès via le code de suivi (#38073).

#11 - 29 novembre 2019 17:45 - Nicolas Roche

- Lié à Development #38077: Accès aux brouillons via le code de suivi ajouté

#12 - 09 décembre 2019 04:07 - Nicolas Roche

> proposer d'entrer un code de suivi

je suis coincé car pour moi c'est fait par une cellule via combo

> indiquer qu'un code de suivi est nécessaire pour y accéder à ce moment là plutôt que de simplement afficher "Accès interdit".

en fait une indication en plus dans la page d'erreur suffirait ?

#13 - 08 janvier 2020 14:23 - Nicolas Roche

- Fichier 0001-forms-forbidden-direct-anonymous-acces-to-anonymous-.patch ajouté

Rebasé sur les tests et ajout du message dans la page d'erreur.

#14 - 08 janvier 2020 14:25 - Nicolas Roche

- Fichier 0001-forms-forbidden-direct-anonymous-acces-to-anonymous-.patch ajouté

mince, mauvais patch.

#15 - 08 janvier 2020 14:25 - Nicolas Roche

- Fichier 0001-forms-forbidden-direct-anonymous-acces-to-anonymous-.patch supprimé

#16 - 06 octobre 2020 11:26 - Frédéric Péters

- Statut changé de Solution proposée à Fermé

Je ferme tout ça parce que mélangé sur cinq tickets, se partageant plus de 50 commentaires, et que je ne vois pas où ça mène.

Fichiers

0001-forms-forbidden-direct-anonymous-acces-to-anonymous-.patch	3,33 ko	23 novembre 2019	Nicolas Roche
0001-forms-forbidden-direct-anonymous-acces-to-anonymous-.patch	6,07 ko	29 novembre 2019	Nicolas Roche
0001-forms-forbidden-direct-anonymous-acces-to-anonymous-.patch	6,83 ko	08 janvier 2020	Nicolas Roche