w.c.s. - Development #38079

Forcer l'authentification sur un brouillon auquel un utilisateur est attaché.

29 novembre 2019 13:10 - Nicolas Roche

Statut:	Fermé	**Début:**	29 novembre 2019
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

reprend le patch proposé dans #37095

Demandes liées:

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

Historique

#1 - 29 novembre 2019 15:05 - Nicolas Roche

- Fichier 0001-forms-force-authentication-on-user-drafts-38079.patch ajouté

- Statut changé de Nouveau à En cours

- Patch proposed changé de Non à Oui

Première version :
ne pas autoriser un utilisateur non connecté à charger un code de suivi associé à un utilisateur.

#2 - 29 novembre 2019 17:20 - Nicolas Roche

- Fichier 0002-forms-enforce-authentication-on-user-drafts-38079.patch ajouté

- Statut changé de En cours à Solution proposée

dans #37095 :

> Il restera le cas d'un brouillon commencé non connecté et repris en mode connecté

Pour moi tout ça découle d'un cas plus général :
celui d'un brouillon repris en mode connecté par un autre utilisateur que celui qui l'a commencé (connecté ou pas).

Sauf que cela entraîne une régression :
les agents utilisant un code de suivi pour accéder à une demande sont à présent redirigés en backoffice.

#3 - 29 novembre 2019 17:46 - Nicolas Roche

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

#4 - 29 novembre 2019 18:25 - Thomas Noël

Selon moi ça ne va pas marcher dans le cadre d'un SSO :

1. je suis connecté wcs via SSO, donc j'ai une session sur l'IDP
2. je veux aller sur un brouillon qui appartient à qqun d'autre
3. je suis renvoyé sur login (dans l'idée que je dois changer de user)
4. login me renvoie vers l'IdP
5. j'ai une session sur l'IdP : il répond immédiatement et me renvoie sur le formulaire
6. et donc je reviens sur l'étape 2 : ça boucle

Bref, le seul cas où ça marche c'est quand je ne suis pas encore loggué (le cas codé actuellement).

#5 - 05 décembre 2019 12:21 - Nicolas Roche

Effectivement, le login ne force pas les utilisateurs déjà authentifiés à se reloguer.
La redirection est mise en place dans wcs/forms/root.py::TrackingCodeDirectory::load(). Ce que je constate à l'usage (entre 2 usagers) c'est :

1. je suis connecté wcs via SSO, donc j'ai une session sur l'IDP
2. je veux aller sur un brouillon qui appartient à qqun d'autre (appel à load)
3. je suis renvoyé sur login (dans l'idée que je dois changer de user)
4. login me renvoie vers l'IdP
5. j'ai une session sur l'IdP : il répond immédiatement et me renvoie sur le formulaire
6. j'accède directement à la ressource
7. l'accès m'est interdit : page d'interdiction WCS qui invite à retourner sur l'acceuil

#6 - 05 décembre 2019 13:55 - Thomas Noël

Nicolas Roche a écrit :

> Effectivement, le login ne force pas les utilisateurs déjà authentifiés à se reloguer.
> La redirection est mise en place dans wcs/forms/root.py::TrackingCodeDirectory::load(). Ce que je constate à l'usage (entre 2 usagers) c'est :
>
> 1. je suis connecté wcs via SSO, donc j'ai une session sur l'IDP
> 2. je veux aller sur un brouillon qui appartient à qqun d'autre (appel à load)
> 3. je suis renvoyé sur login (dans l'idée que je dois changer de user)
> 4. login me renvoie vers l'IdP
> 5. j'ai une session sur l'IdP : il répond immédiatement et me renvoie sur le formulaire
> 6. j'accède directement à la ressource
> 7. l'accès m'est interdit : page d'interdiction WCS qui invite à retourner sur l'acceuil

C'est exactement ce que j'ai décrit ci-dessus, hein. Donc, faut rien faire, juste refuser l'accès dans ce cas.

#7 - 05 décembre 2019 17:06 - Nicolas Roche

oui et non,

```
<<<
6. et donc je reviens sur l'étape 2 : ça boucle
---
6. j'accède directement à la ressource
>>>
```

il y a bien un aller retour sur l'IDP mais pas de boucle

#8 - 06 décembre 2019 00:08 - Thomas Noël

Nicolas Roche a écrit :

> oui et non,
> [...]
> il y a bien un aller retour sur l'IDP mais pas de boucle

Je veux dire : ça change pas le user. On revient sur wcs sans que rien n'ai changé. Bref, on peut pas changer de user, et comme dit en réunion de lundi, sur les brouillons, c'est pas grave, c'est même mieux. Un brouillon attaché à un user ne doit rester accessible qu'à celui-ci (donc soit il est déjà loggué et ça passe, soit il n'est pas loggué et on force le log avec un retour vers le formulaire). On revient donc à l'essence du ticket : forcer l'auth sur un brouillon auquel un utilisateur est attaché.

#9 - 08 janvier 2020 15:13 - Nicolas Roche

- Fichier 0001-forms-force-authentication-if-anonymous-use-user-tra.patch ajouté

rebasé, pour alimenter la discussion sur le problème de pré-remplissage des champs.
(juste pour information, ce patch n'est pas sensé être poussé en l'état)

Si la demande a été initialisée par un utilisateur, on force la connexion avec cet utilisateur ; si un autre utilisateur est déjà logué, alors on affiche une page d'erreur : "Accès interdit".

Si la demande a été initialisée anonymement, pas de changement : on pré-rempli avec les champs de l'utilisateur actuellement en session.
(et donc potentiellement avec des données propres aux agents)

#10 - 11 février 2020 14:27 - Nicolas Roche

- Fichier 0003-tracking_code-correct-tests-on-formdata-access-38073.patch ajouté

- Fichier 0002-forms-force-authentication-if-using-another-user-s-t.patch ajouté

- Fichier 0001-tracking_code-add-tests-on-formdata-access-38073.patch ajouté

Rebasé en retirant mes tests : seul 0002 sera éventuellement poussé.

#11 - 11 février 2020 14:59 - Frédéric Péters

(tu peux ne pas attacher les patchs qui sont à ignorer)

#12 - 12 février 2020 12:06 - Nicolas Roche

- Fichier 0001-forms-force-authentication-if-using-another-user-s-t.patch ajouté

ok

#13 - 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-force-authentication-on-user-drafts-38079.patch	5,85 ko	29 novembre 2019	Nicolas Roche
0002-forms-enforce-authentication-on-user-drafts-38079.patch	3,78 ko	29 novembre 2019	Nicolas Roche
0001-forms-force-authentication-if-anonymous-use-user-tra.patch	8,08 ko	08 janvier 2020	Nicolas Roche
0002-forms-force-authentication-if-using-another-user-s-t.patch	4,56 ko	11 février 2020	Nicolas Roche
0003-tracking_code-correct-tests-on-formdata-access-38073.patch	3,1 ko	11 février 2020	Nicolas Roche
0001-tracking_code-add-tests-on-formdata-access-38073.patch	17,1 ko	11 février 2020	Nicolas Roche
0001-forms-force-authentication-if-using-another-user-s-t.patch	4,55 ko	12 février 2020	Nicolas Roche