

Combo - Development #41837

Que faire quand un lien de paiement ne correspond pas à l'utilisateur courant ?

17 avril 2020 16:51 - Benjamin Dauvergne

Statut:	Fermé	Début:	17 avril 2020
Priorité:	Normal	Echéance:	
Assigné à:	Benjamin Dauvergne	% réalisé:	0%
Catégorie:		Temps estimé:	0:00 heure
Version cible:		Planning:	Non
Patch proposed:	Oui		

Description

Discussion suite au souci signalé dans #41827.

Pour l'instant on balance une erreur 403 avec le texte « Mauvaise sélection : paiement non autorisé. » un peu pauvre en information.

Il y a deux cas :

- l'utilisateur est non authentifié, pour une raison que j'ignore le login automatique ne se s'est pas déclenché (la session est actuellement fermée et la page coté w.c.s. toujours visible, le lien est dans un mail, whatever), dans ce cas je pense qu'il faudrait lancer une authentification;
- l'utilisateur n'est pas le même que sur le BasketItem, on devrait le signaler ainsi « ce lien de paiement n'appartient à votre utilisateur » dans une vraie page.

Révisions associées

Révision 832b8188 - 26 juin 2020 11:44 - Benjamin Dauvergne

lingo: allow item payment by any user (#41837)

Historique

#2 - 20 avril 2020 10:32 - Benjamin Dauvergne

- *Projet changé de Combo à Lingo*

#3 - 20 avril 2020 10:50 - Emmanuel Cazenave

Benjamin Dauvergne a écrit :

dans ce cas je pense qu'il faudrait lancer une authentification;

Peut-être hors sujet parce que j'ai pas bien compris les détails mais je tique là dessus parce qu'on veut justement permettre le paiement sans authent depuis peu.

#4 - 20 avril 2020 14:13 - Benjamin Dauvergne

Je sais tout ça mais il y a deux variables: request.user et item.user, pour du paiement sans authent, tel que le code est écrit il faut que item.user soit nul, et là ça marche et je suppose que c'est ce qui est fait actuellement (PS: créer des basketitems sans NameID et donc sans utilisateurs associé).

Mais si item.user n'est pas nul, alors le code impose que request.user ait la même valeur et sinon on a PermissionDenied; je dis juste que plutôt qu'un PermissionDenied il faudrait orienter l'utilisateur :

- soit avec un message d'erreur clair
- soit en lançant une authentification parce que c'est possible

#5 - 22 juin 2020 17:23 - Benjamin Dauvergne

- *Assigné à mis à Benjamin Dauvergne*

#6 - 22 juin 2020 17:42 - Benjamin Dauvergne

- *Fichier 0001-lingo-remove-check-on-item-owner-in-PayView-41837.patch ajouté*

- *Statut changé de Nouveau à Solution proposée*

- *Patch proposed changé de Non à Oui*

J'ai pris le parti de simplifier drastiquement les choses, plus de check sur item.user, la requête est déjà signée à part les éléments, next_url, email, first_name et last_name qui sont purement déclaratifs et n'apportent aucune information à celui qui clique. Même sur l'URL de retour on ne donne pas d'information sur l'élément du panier.

#7 - 22 juin 2020 17:47 - Benjamin Dauvergne

Benjamin Dauvergne a écrit :

J'ai pris le parti de simplifier drastiquement les choses, plus de check sur item.user, la requête est déjà signée à part les éléments, next_url, email, first_name et last_name qui sont purement déclaratifs et n'apportent aucune information à celui qui clique. Même sur l'URL de retour on ne donne pas d'information sur l'élément du panier.

Juste pour justifier tout ça : ça simplifie grandement l'utilisation du paiement que ce soit avec ou sans panier, tous les paiement se comporteront de la même manière réglant les tickets #41827 à Toulouse et #42525 au SICTIAM (utilisateur non connecté/connecté avec un utilisateur différent voulant payer un item attaché à un utilisateur).

À noter que si un utilisateur différent de celui de l'item est connecté, son profil sera utilisé (email, first_name, last_name) et la transaction attaché à son compte; actuellement on a pas de cellule pour présenter les transactions attachées à un compte (le champ Transaction.user ne sert donc pas à grand chose il me semble), seul le propriétaire du BasketItem, s'il y en a un, verra qu'il est bien payé et l'éventuelle démarche associée.

#8 - 22 juin 2020 17:59 - Frédéric Péters

actuellement on a pas de cellule pour présenter les transactions attachées à un compte

On a, LingoRecentTransactionsCell.

#9 - 22 juin 2020 18:29 - Benjamin Dauvergne

Frédéric Péters a écrit :

actuellement on a pas de cellule pour présenter les transactions attachées à un compte

On a, LingoRecentTransactionsCell.

Ok dans ce cas je propose d'étendre son comportement au moins pour les BasketItem, on liste aussi les transactions liées à des BasketItem de l'utilisateur en cours; pour les remote_items le cas n'est pas possible (ça passe par PayView).

#10 - 24 juin 2020 11:15 - Benjamin Dauvergne

Branche à jour avec modification de LingoRecentTransactionsCell pour afficher les transactions dont on est le payeur ou qui concernent un item qui nous appartient et adaptation des tests.

#11 - 25 juin 2020 15:44 - Serghei Mihai

Cela me semble plus clair de définir l'attribut transactions_queryset dans la classe et lui attribuer la requete Transaction.objects.... Et éviter ainsi le if not hasattr(self, 'transactions_queryset').

#12 - 25 juin 2020 18:53 - Benjamin Dauvergne

Serghei Mihai a écrit :

Cela me semble plus clair de définir l'attribut transactions_queryset dans la classe et lui attribuer la requete Transaction.objects.... Et éviter ainsi le if not hasattr(self, 'transactions_queryset').

Je vais virer le hasattr(), je pensais que le contenu serait réutilisé. Il y a une partie dynamique qui dépend du contexte, ça ne peut pas être un attribut de la classe, une property à la rigueur.

#13 - 25 juin 2020 18:55 - Benjamin Dauvergne

Branche à jour (property non en fait, toujours la dépendance sur le contexte).

#14 - 26 juin 2020 11:22 - Serghei Mihai

- Statut changé de Solution proposée à Solution validée

#15 - 26 juin 2020 11:45 - Benjamin Dauvergne

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

commit 832b8188f9f280fc83cbcc328c3beaf9fc77d
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date: Mon Jun 22 17:40:56 2020 +0200

lingo: allow item payment by any user (#41837)

#16 - 27 juin 2020 18:16 - Frédéric Péters

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

Fichiers

0001-lingo-remove-check-on-item-owner-in-PayView-41837.patch	876 octets	22 juin 2020	Benjamin Dauvergne
--	------------	--------------	--------------------