Combo - Development #36876

Paiement sans authentification et sans panier

13 octobre 2019 16:24 - Emmanuel Cazenave

Statut:	Fermé	**Début:**	13 octobre 2019
Priorité:	Normal	**Echéance:**	
Assigné à:	Emmanuel Cazenave	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Actuellement dans le parcours utilisateur de paiement authentifié, en revenant de la plateforme de paiement on finit sur la vue 'panier', sur laquelle on peut voir si la transaction est en succès, cliquer sur le lien qui ramène à la démarche, etc.

Plus possible si on est pas authentifié (notre implémentation du 'panier' ne fonctionne que pour un utilisateur authentifié). Il faudra donc revenir sur une vue dédiée genre /lingo/item/(?P<item_id>\d+)/payment-return.

Une visite sur cette vue lorsque le paiement est ok et ce sera redirection vers la démarche (c'est le cas standard, dans lequel la page est invisible pour l'usager).

Si le paiement est 'en attente', on interroge en js le statut du paiement et on dit à l'utilisateur de patienter, et on le redirige vers la démarche quand le paiement est ok (c'est le cas où l'usager est revenu chez nous depuis la plateforme de paiement avant que celle ci nous ait notifié du succès du paiement)

Si le paiement est en erreur on peut également en informer l'utilisateur et lui proposer de retourner à la démarche, qui sera en toujours 'En attente de paiement' et où il pourra retenter un paiement.

Pour l'interrogation du statut de la transaction en js, on a besoin d'une nouvelle vue d'API.

Demandes liées:

Lié à Combo - Bug #9039: paiement sans être loggué	**Fermé**	**19 novembre 2015**
Lié à Publik - Development #32249: Paiements sans voir le panier	**Fermé**	**12 avril 2019**
Lié à Combo - Development #27505: poser les messages notifiant l'échec et l'a...	**Fermé**	**22 octobre 2018**
Lié à Combo - Development #25552: Pouvoir renvoyer l'usager directement vers ...	**Fermé**	**31 juillet 2018**
Dupliqué par Combo - Development #36875: Paiement sans authentification : aju...	**Rejeté**	**13 octobre 2019**

Révisions associées

Révision 266b37db - 16 janvier 2020 11:44 - Emmanuel Cazenave

lingo: check response signature later (#36876)

Révision 36588dd3 - 16 janvier 2020 11:44 - Emmanuel Cazenave

lingo: support anonymous and no basket payment (#36876)

Historique

#1 - 13 octobre 2019 16:25 - Emmanuel Cazenave

- Lié à Bug #9039: paiement sans être loggué ajouté

#2 - 13 octobre 2019 16:46 - Emmanuel Cazenave

Et pour l'inspiration il y a Benj qui avait commencé quelque chose : https://dev.entrouvert.org/issues/32239#note-9 .

#3 - 18 novembre 2019 11:41 - Emmanuel Cazenave

- Lié à Development #32249: Paiements sans voir le panier ajouté

#4 - 17 décembre 2019 13:39 - Emmanuel Cazenave

- Dupliqué par Development #36875: Paiement sans authentification : ajustements dans l'API ajouté

#5 - 19 décembre 2019 19:14 - Emmanuel Cazenave

- Fichier form-inscription-simple-paiement.wcs ajouté

- Fichier Screenshot-2019-12-19 Portail -.png ajouté

- Fichier Screenshot-2019-12-19 Portail -(1).png ajouté

- Fichier workflow-exemple-paiement-en-ligne.wcs ajouté

- Fichier 0001-lingo-support-anonymous-and-no-basket-payment-36876.patch ajouté

- Tracker changé de Support à Bug

- Sujet changé de Paiement sans authentification : vue d'attente après paiement sur la plateforme de paiement à Paiement sans authentification et sans panier

- Statut changé de Nouveau à Solution proposée

- Assigné à mis à Emmanuel Cazenave

- Patch proposed changé de Non à Oui

Pas mal de choses.

Plus complexe que j'avais imaginé à cause de la gestion d'erreurs, à plusieurs endroits lingo redirigeait vers le panier en cas de pépins, dans le parcours sans panier c'est la vue 'basket-item-payment-status' qui prend ça en charge, et pour y arriver plusieurs endroits où on a besoin de connaître l'identifiant de l'item concerné.

'basket-item-payment-status' a besoin d'une vue d'API pour connaître le statut de la transaction : 'api-transaction-status', la vue de paiement d'un item unique 'basket-item-pay-view' qui existait déjà devient accessibles aux utilisateurs anonymes, tout ceci donne le paiement sans authentification.

Avec 'basket-item-pay-view' qui gagne la possibilité de recevoir 'email', 'firstname' et 'lastname' dans la query string, avec ces infos qui navigueront jusqu'à la plateforme de paiement, parce que c'est pas parce qu'on est pas authentifié qu'on a pas le droit de recevoir un mail d'accusé de paiement de la plateforme (je parle de payzen and co).

Sur sur ces trois vues l'identifiant du basket item est chiffré, et là petite interrogation sur la robustesse parce que les signatures produites sont assez courtes, genre 'ab8b8faf' (et voilà j'ai étalé l'intégralité de ma science en matière de chiffrement).

Ci-joint quelques captures de la vue d'attente 'basket-item-payment-status', c'est léger coté présentation (en même temps quand tout va bien on la voit pas, redirection immédiate vers le formulaire), j'ai une réputation de tocard front à tenir, mais je serai ravi de suivre les indications qu'on voudra bien me donner.

Je joins aussi workflow et formulaire utilisé pour qui voudrait faire mumuse. A part ça testé sur payzen, ça me semble marcher pas mal.

#6 - 20 décembre 2019 10:07 - Frédéric Péters

Je serais pour allonger templates/lingo/combo/item-wait-payment.html, qu'il contienne davantage de texte, éventuellement regarder à quelques endroits ce qui se fait, mais en gros quelque chose comme :

> Vous venez d'être redirigé depuis la plateforme de paiement; votre paiement est en cours de traitement, cela devrait prendre quelques secondes et cet écran disparaitra ensuite. Si cet écran persiste, vous pouvez cliquer sur le bouton "continuer" pour retourner sur votre demande de paiement.
>
> (ici mettre en error-notice le message reçu de l'API en cas d'erreur)
>
> [Continuer]

Ça veut dire sortir de l'API le message "Wait a moment...", qui serait dans le template, et dans l'API avoir un statut (attente, ok, erreur), et en cas d'erreur le message d'accompagnement.

À regarder TransactionStatusApiView je me dis aussi que les HttpResponseForbidden pourraient être retournés dans le même format JSON.

La partie javascript, je suis assez pour la placer directement dans le template, plutôt que dans un fichier statique séparé. En ajoutant quelques {% block %} dans le template pour qu'il soit possible d'en modifier le texte sans devoir copier/coller le javascript.

La signature de handle_payment commence à ne plus ressembler à rien,

```
        return self.handle_payment(
            request, regie, [item], [], next_url, email, firstname, lastname, basket=False
        )
```

du coup je passerais tous les paramètres par keyword.

```
            if basket:
                return HttpResponseRedirect(next_url)
            return HttpResponseRedirect(get_single_item_payment_status_view(single_item.pk))
```

Si je comprends bien, je pense que get_single_item_payment_status_view devrait perdre son bout "single_item", qu'on passe systématiquement par elle, même quand il y a un panier.

Par rapport à tous les bouts avec du chiffrement, je me demande dans quelle mesure on ne gagnerait pas à juste faire confiance à la session de l'usager, il y a un petit bout avec lingo_next_url mais j'ai l'impression que ça pourrait être généralisé, avec dans la session un dictionnaire lingo_transactions, genre {transaction.id: {'next_url': ..., 'item_id': ...}}.

#7 - 20 décembre 2019 11:46 - Frédéric Péters

Concernant le message, vu ailleurs, « Veuillez patienter pendant le traitement de votre demande... », je me dis que ça peut être tapé en petit titre au-dessus du texte.

#8 - 23 décembre 2019 13:28 - Emmanuel Cazenave

- Fichier 0001-lingo-support-anonymous-and-no-basket-payment-36876.patch ajouté

- Tracker changé de Bug à Development

Frédéric Péters a écrit :

> Si je comprends bien, je pense que get_single_item_payment_status_view devrait perdre son bout "single_item", qu'on passe systématiquement par elle, même quand il y a un panier.

Hmm non non, le parcours classique avec retour sur le panier après paiement ou en cas d'erreur doit continuer à pouvoir marcher.
C'est pour ça que handle_payment gagne un paramètre 'basket', qui est passé à False dans le parcours sans panier (ie: passage par BasketItemPayView), True par défaut (ie: passage par PayView).

Dans le même esprit, ReturnView choisis de rediriger vers le panier ou vers la vue d'attente en fonction de "request.GET.get('item-id')".

> Par rapport à tous les bouts avec du chiffrement, je me demande dans quelle mesure on ne gagnerait pas à juste faire confiance à la session de l'usager, il y a un petit bout avec lingo_next_url mais j'ai l'impression que ça pourrait être généralisé, avec dans la session un dictionnaire lingo_transactions, genre {transaction.id: {'next_url': ..., 'item_id': ...}}.

J'avais envisagé ça mais je l'avais écarté parce qu'il y plusieurs situations d'erreur où on doit rediriger vers la vue d'attente alors qu'on a pas encore d'identifiant de transaction disponible.

> À regarder TransactionStatusApiView je me dis aussi que les HttpResponseForbidden pourraient être retournés dans le même format JSON.

Vu sur jabber avec Fred, pas évident avec Jquery d'aller piocher le message d'erreur dans le JSON en cas d'erreur 4XX, on laisse tomber.

J'ai tenu compte de tout le reste.

#9 - 23 décembre 2019 13:38 - Frédéric Péters

> > Si je comprends bien, je pense que get_single_item_payment_status_view devrait perdre son bout "single_item", qu'on passe systématiquement par elle, même quand il y a un panier.
>
> Hmm non non, le parcours classique avec retour sur le panier après paiement ou en cas d'erreur doit continuer à pouvoir marcher.

Oui, mais pour moi cette vue de statut y a aussi son sens, parce qu'il est utile d'attendre la notification du site de paiement : j'imagine de mon côté que dans toutes les situations le retour du site de paiement soit vers cette vue, qu'une fois le paiement obtenu, elle redirige, vers ce qui sera opportun.

#10 - 23 décembre 2019 15:43 - Benjamin Dauvergne

J'ai l'impression que le cas UnsignedPaymentException n'est pas pris en compte ici, c'est justement le cas où le retour par redirect n'est pas suffisant pour valider la transaction et où il faudrait tomber sur une page qui poll combo pour voir si on a reçu un retour asynchrone (tous les autres cas sont des erreurs où on peut considérer la transaction comme ayant échouée). Il me semble que c'est le cas avec TIPI (sûr, mais bon même le retour asynchrone n'est pas secure), ogone et paybox. Avec payzen ça n'arrive jamais, la signature est obligatoire en synchrone (redirect) et asynchrone (webhook) et avec payfip/tipi web-service ça n'arrivera pas non plus car on doit valider dès le retour via l'API web-service.

#11 - 24 décembre 2019 13:45 - Emmanuel Cazenave

- Fichier 0001-lingo-check-response-signature-later-36876.patch ajouté

- Fichier 0002-lingo-support-anonymous-and-no-basket-payment-36876.patch ajouté

Passage par la vue 'payment-status' pour tout le monde et gestion du cas de réponse non signé dans las ReturnView.

#12 - 08 janvier 2020 10:39 - Emmanuel Cazenave

- Fichier out.ogv ajouté

Avec la vidéo de réclame (de review).

#13 - 09 janvier 2020 10:26 - Serghei Mihai

Dans:

```
display_error($('#transaction-status').data('error'))
```

je ne vois pas d'element avec l'id transaction-status dans le template.

#14 - 09 janvier 2020 15:49 - Emmanuel Cazenave

- Fichier 0001-lingo-check-response-signature-later-36876.patch ajouté

- Fichier 0002-lingo-support-anonymous-and-no-basket-payment-36876.patch ajouté

Bien vu merci, c'est corrigé pour :

```
display_error($('#transaction-error').data('error'))
```

#15 - 12 janvier 2020 17:48 - Frédéric Péters

- Lié à Development #27505: poser les messages notifiant l'échec et l'aboutissement du paiement uniquement si la rédirection est faite vers combo ajouté

#16 - 12 janvier 2020 17:49 - Frédéric Péters

- Lié à Development #25552: Pouvoir renvoyer l'usager directement vers l'historique d'une demande (form_url) lorsque l'usager paye en ligne dans le cadre d'une démarche ajouté

#17 - 13 janvier 2020 08:21 - Emmanuel Cazenave

Ce que je propose ici me semble résoudre #27505, il y a redirection systématique vers /api/lingo/transaction-status/ sur laquelle on reste au moins 3 secondes justement pour afficher les messages :

```
$('#wait-msg').text($('#wait-msg').data('continue'))
// wait a little to show messages
setTimeout(function(){location.href=next_url}, 3000);
```

#18 - 13 janvier 2020 17:20 - Serghei Mihai

Yep, les messages seront affichés sur cette page.

#19 - 14 janvier 2020 11:10 - Serghei Mihai

- Statut changé de Solution proposée à Solution validée

Vas-y, pousse et envoie en recette. Ça nous laissera le temps de voir et corriger les éventuels pépins.

#20 - 14 janvier 2020 11:18 - Benjamin Dauvergne

Pour ça :

```
        if user:
            item.regie.compute_extra_fees(user=item.user)
```

Il faudrait péter une erreur si en fait c'est nécessaire (le code derrière est déjà super permissif en fait...), avec par exemple :

```
        if user:
            ...
        else:
            if item.regie.extra_fees_ws_url:
                raise Exception(...)
```

ou alors fait en sorte que extra_fees fonctionne aussi sans user (et si ça ne plaît pas au web-service derrière il pètera une erreur qu'il faudra récupérer ce qui n'est pas le cas actuellement, c'est juste ignoré)

Pourquoi utiliser aes_hex_encrypt plutôt que les fonctions crypto[1] de Django (dumps et loads) ? surtout que le chiffrement ne me parait pas nécessaire s'agissant de références opaques, une signature suffit.

J'ai un peu du mal à voir la différence entre transaction_id et publik-payment j'ai l'impression que ça fait un peu la même chose (référencé la transaction en cours), sachant qu'on a aussi transaction.order_id pour ça, on multiplie les identifiants.

[1]: https://docs.djangoproject.com/fr/3.0/topics/signing/

#21 - 14 janvier 2020 11:19 - Benjamin Dauvergne

- Statut changé de Solution validée à En cours

#22 - 14 janvier 2020 12:17 - Benjamin Dauvergne

Donc je rajoute que je verrai bien l'utilisation direct de transaction.id comme identifiant pour la vue statut du paiement, next_url pouvant être stocké dedans (on génère une transaction par tentative de paiement donc ça va bien) et items lui étant déjà lié, on a besoin de rien d'autre. Au niveau de handle_response on pourrait vérifier que transaction.order_id correspond avec response.order_id. Ça fait que handle_response n'aura plus besoin de retourner transaction et pourra simplement le prendre en paramètre.

#23 - 14 janvier 2020 18:58 - Emmanuel Cazenave

- Fichier 0001-lingo-check-response-signature-later-36876.patch ajouté

- Fichier 0002-lingo-support-anonymous-and-no-basket-payment-36876.patch ajouté

- Statut changé de En cours à Solution proposée

Benjamin Dauvergne a écrit :

> Il faudrait péter une erreur si en fait c'est nécessaire (le code derrière est déjà super permissif en fait...), avec par exemple :

Tenu compte.

> Pourquoi utiliser aes_hex_encrypt plutôt que les fonctions crypto[1] de Django (dumps et loads) ? surtout que le chiffrement ne me parait pas nécessaire s'agissant de références opaques, une signature suffit.

Tenu compte.

> Donc je rajoute que je verrai bien l'utilisation direct de transaction.id comme identifiant

Tenu compte, plus de nouveau uuid, je me base sur l'identifiant de transaction (par contre je ne me suis pas lancé dans le changement d'interface de handle_return etc, le patch est déjà bien gros).

#24 - 15 janvier 2020 14:35 - Serghei Mihai

J'ai pas d'autres remarques sauf:

Dans PaymentStatusView

```
        try:
            transaction = Transaction.objects.get(pk=transaction_id)
        except Transaction.DoesNotExist:
```

on ne devrait pas poser rechercher uniquement les transactions qui ne sont pas marquées comme payées, genre:

```
transaction = Transaction.objects.exclude(status__in=(eopayment.PAID, eopayment.ACCEPTED)).get(pk=transaction_id)
```

#25 - 15 janvier 2020 15:27 - Benjamin Dauvergne

Pour ne justement pas faire la même erreur que Saga on devrait contrôler que des notifications successives pour une même transaction sont cohérentes ; et là attention pour des prélèvements différés il me semble qu'en plus il y en a plusieurs avec des statuts différents, mais ça dépasse certainement le cadre de ce ticket.

#26 - 15 janvier 2020 15:37 - Emmanuel Cazenave

Serghei Mihai a écrit :

> on ne devrait pas poser rechercher uniquement les transactions qui ne sont pas marquées comme payées, genre:
> [...]

Le plus commun est justement d'arriver sur cette vue alors que la transaction est payée : je paye, la transaction est marquée payée par callbackview ou returnview, j'arrive sur PaymentStatusView où on me dit que tout va bien et que je vais être redirigé, je suis redirigé vers le formulaire.

#27 - 16 janvier 2020 11:39 - Serghei Mihai

- Statut changé de Solution proposée à Solution validée

Ok, go.

#28 - 16 janvier 2020 11:54 - Emmanuel Cazenave

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

```
commit 36588dd35739bee1a9ed90ea9a59136591302342
Author: Emmanuel Cazenave <ecazenave@entrouvert.com>
Date:   Tue Dec 24 13:42:47 2019 +0100

    lingo: support anonymous and no basket payment (#36876)

commit 266b37db6fa1894059af0c4e033ecb69763d83ff
Author: Emmanuel Cazenave <ecazenave@entrouvert.com>
Date:   Tue Dec 24 13:41:48 2019 +0100

    lingo: check response signature later (#36876)
```

#29 - 16 janvier 2020 14:15 - Frédéric Péters

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

Fichiers

form-inscription-simple-paiement.wcs	2,92 ko	19 décembre 2019	Emmanuel Cazenave
Screenshot-2019-12-19 Portail -.png	94,6 ko	19 décembre 2019	Emmanuel Cazenave
Screenshot-2019-12-19 Portail -(1).png	95,1 ko	19 décembre 2019	Emmanuel Cazenave
workflow-exemple-paiement-en-ligne.wcs	5,19 ko	19 décembre 2019	Emmanuel Cazenave
0001-lingo-support-anonymous-and-no-basket-payment-36876.patch	28,5 ko	19 décembre 2019	Emmanuel Cazenave
0001-lingo-support-anonymous-and-no-basket-payment-36876.patch	28,5 ko	23 décembre 2019	Emmanuel Cazenave
0001-lingo-check-response-signature-later-36876.patch	2,4 ko	24 décembre 2019	Emmanuel Cazenave
0002-lingo-support-anonymous-and-no-basket-payment-36876.patch	34,2 ko	24 décembre 2019	Emmanuel Cazenave
out.ogv	7,61 Mo	08 janvier 2020	Emmanuel Cazenave
0001-lingo-check-response-signature-later-36876.patch	2,4 ko	09 janvier 2020	Emmanuel Cazenave
0002-lingo-support-anonymous-and-no-basket-payment-36876.patch	34,2 ko	09 janvier 2020	Emmanuel Cazenave
0001-lingo-check-response-signature-later-36876.patch	2,4 ko	14 janvier 2020	Emmanuel Cazenave
0002-lingo-support-anonymous-and-no-basket-payment-36876.patch	34,6 ko	14 janvier 2020	Emmanuel Cazenave