Authentic 2 - Development #27823

Avertir par courriel l'utilisateur lorsqu'il demande la suppression de son propre compte

07 novembre 2018 16:53 - Paul Marillonnet

Statut:	Fermé	**Début:**	07 novembre 2018
Priorité:	Normal	**Echéance:**	
Assigné à:	Paul Marillonnet	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Avec donc une suppression en deux temps :
- l'usager demande la suppression de son compte.
- l'usager reçoit par courriel une URL opaque de confirmation de la suppression de son compte.

La validité de l'URL pourrait être limitée dans le temps, par exemple 48h.

Demandes liées:

Lié à Authentic 2 - Development #26910: La suppression d'un utilisateur par l...	**Fermé**	**02 octobre 2018**

Révisions associées

Révision 62441e23 - 02 octobre 2019 11:33 - Paul Marillonnet

accounts: send validation email before self-triggered account deletion (#27823)

Historique

#1 - 07 novembre 2018 16:54 - Paul Marillonnet

- Lié à Development #26910: La suppression d'un utilisateur par lui même doit provoquer l'envoi d'un mail de notification ajouté

#2 - 07 novembre 2018 17:52 - Thomas Noël

A noter qu'actuellement on demande le mot de passe pour valider la suppression, cette étape devra être supprimée (parce que si la personne a accès à son mail, elle peut changer le mot de passe, donc cette vérif du pass devient inutile)

#3 - 18 juillet 2019 15:00 - Paul Marillonnet

Je verrais bien un nouveau modèle pour stocker cette information relative à la demande de suppression de son propre compter par l'usager.

Ce modèle devrait donc contenir :
- Une clé étrangère vers le modèle utilisateur.
- Le code opaque de confirmation de la suppression, de 63 caractères alphanumériques. Ce code opaque servirait à retrouver l'objet à partir du format d'urls. Je vois plutôt d'un paramètre d'urls au sens Django (par exemple /validate-deletion/(?P<opaque_code>|A-Za-z0-9]+)/) plutôt qu'un paramètre de querystring. Ce premier choix est davantage ce qui me vient à l'esprit quand on parle d'URL opaque.
- La date de création de l'objet. Cette date serait utilisée, lorsque la vue de suppression est servie, à vérifier que cet objet a été créé depuis moins de 48h.

#4 - 18 juillet 2019 17:12 - Thomas Noël

Mes 2 cents : s'inspirer plutôt du système utilisé lors de l'enregistrement, cf authentic2/utils.py::build_activation_url . L'URL contient des infos datées et signées, et hop.

#5 - 18 juillet 2019 17:14 - Paul Marillonnet

Ah bein oui, c'est moi qui vaux 2 cents pour ne pas y avoir pensé.
Je vais regarder ça et adapter le code si nécessaire, merci bien.

#6 - 19 juillet 2019 15:45 - Paul Marillonnet

- Statut changé de Nouveau à Information nécessaire

Ce qui m'embête un peu si on s'inspire du code d'activation, c'est qu'on ne stocke plus l'information relative à la demande de suppression.
On vérifierait que le jeton déchiffré correspond à une clé primaire d'usager existant et à un horodatage valide (inférieur à 48h), mais on s'expose à des attaques par force brute dans lesquelles a2 testerait la validité de jetons correspondant potentiellement à des usagers n'ayant jamais émis de demande de suppression de leur compte.

Est-ce que c'est grave docteur ?

#7 - 19 juillet 2019 16:35 - Thomas Noël

Faut calculer l'entropie, comme dirait l'autre. En vrai je n'en sais rien, peut-être que tu soulèves un vrai problème...

#8 - 19 juillet 2019 16:44 - Paul Marillonnet

Le truc évident, discuté de vive voix avec Thomas et Frédéric, c'est de vérifier que l'usager connecté est bien celui dont la clé primaire apparaît dans la signature.

#9 - 19 juillet 2019 16:45 - Paul Marillonnet

- Statut changé de Information nécessaire à En cours

#10 - 22 juillet 2019 21:23 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Le truc évident, discuté de vive voix avec Thomas et Frédéric, c'est de vérifier que l'usager connecté est bien celui dont la clé primaire apparaît dans la signature.

Ça revient à demander le mot de passe, en gros il faut une session ouverte (donc mot de passe) pour pouvoir utiliser le lien de suppression ? Ça me parait superflu, on supprime le compte dont la clé primaire apparaît dans la signature, point (session ouverte ou pas), on peut éventuellement demander confirmation à ce moment là; non c'est même certain qu'il faut le faire[1], et ici on peut rapeller des détails du compte (nom, email, etc..).

[1] Pour les fameux serveurs de mails qui ouvrent les liens.

#11 - 05 août 2019 16:25 - Paul Marillonnet

- Fichier 0001-accounts-send-validation-email-before-self-triggered.patch ajouté

- Statut changé de En cours à Solution proposée

- Patch proposed changé de Non à Oui

Benjamin Dauvergne a écrit :

> [1] Pour les fameux serveurs de mails qui ouvrent les liens.

Dont j'ignorais l'existence :)

#12 - 05 août 2019 16:36 - Paul Marillonnet

- Statut changé de Solution proposée à En cours

L'affichage des erreurs lors de la suppression n'est pas hyper clean. Peux mieux faire. Je recommence.

#13 - 06 août 2019 15:19 - Paul Marillonnet

- Fichier 0001-accounts-send-validation-email-before-self-triggered.patch ajouté

- Statut changé de En cours à Solution proposée

Paul Marillonnet a écrit :

> L'affichage des erreurs lors de la suppression n'est pas hyper clean. Peux mieux faire. Je recommence.

En fait, je craignais que, dans le cas général, le message de toute ValidationError remontée lorsqu'on teste la validité de l'URL contenant le jeton de suppression ne doive pas être présenté à l'écran de l'usager, mais la lecture du code et de la doc Django me rassure sur la banalité de la chose.

Je maintiens mon patch (modulo un correctif d'échappement HTML, qui faisait planter les tests).

#14 - 06 août 2019 15:21 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> Benjamin Dauvergne a écrit :
>
> > [1] Pour les fameux serveurs de mails qui ouvrent les liens.
>
> Dont j'ignorais l'existence :)

C'est une marotte de Thomas.

#17 - 18 septembre 2019 11:23 - Frédéric Péters

Sur la forme,

> account_deletion_code_body.txt

Ça va faire une première ligne super longue.

> accounts_delete_validation.html

Je dégagerais la partie sur le possessif et ferais plutôt "You are about to delete the account of {{full_name}}. This will remove all related personal data and you won't be able to log in with this account anymore."

+ {% trans "Delete" %} → Confirm Deletion.

~~

Sur le code je n'arrive pas trop à dire s'il y a eu relecture à l'occasion des commentaires précédents.

(et si oui, je serais pour pousser ainsi, avec ou sans les changements aux gabarits, qui pourront toujours sinon être gérés dans publik-base-theme).

#18 - 19 septembre 2019 15:23 - Paul Marillonnet

- Fichier 0001-accounts-send-validation-email-before-self-triggered.patch ajouté

Frédéric Péters a écrit :

> Sur la forme,

Merci, pris en compte ici.

> Sur le code je n'arrive pas trop à dire s'il y a eu relecture à l'occasion des commentaires précédents.

Prise en compte des remarques de mon côté, oui, mais relecture, je ne sais pas.

#19 - 19 septembre 2019 15:49 - Benjamin Dauvergne

Je relis.

- plutôt que accounts_plain_message, tu peux utiliser messages.info(request, message) et rediriger vers la homepage,
- DeleteView: ne pas balancer des mails sur un simple GET de /accounts/delete/, il faut un formulaire et un POST, que supprimer son compte prenne 3 clicks au lieu de 2 n'est pas bien grave, l'important c'est de pas se rater et ne pas ouvrir un moyen d'inonder les gens de mails,
- accounts_delete_validation.html : j'ai pas moyen sûr d'avoir un template sans utilisateur donc ce que tu fais est bon (remplacer user dans ctx[])

#20 - 19 septembre 2019 17:14 - Paul Marillonnet

- Fichier 0001-accounts-send-validation-email-before-self-triggered.patch ajouté

Benjamin Dauvergne a écrit :

> Je relis.
> [...]

Bien vu, merci. C'est corrigé ici.

#21 - 27 septembre 2019 20:45 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

- Assigné à mis à Paul Marillonnet

#22 - 02 octobre 2019 11:35 - Paul Marillonnet

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

```
commit 62441e234071a08c013cbc3190e2a9c7b4f25962
```

```
Author: Paul Marillonnet <pmarillonnet@entrouvert.com>
Date:   Thu Jul 18 15:09:30 2019 +0200

    accounts: send validation email before self-triggered account deletion (#27823)
```

#23 - 03 octobre 2019 15:15 - Frédéric Péters

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

Fichiers

0001-accounts-send-validation-email-before-self-triggered.patch	19,3 ko	05 août 2019	Paul Marillonnet
0001-accounts-send-validation-email-before-self-triggered.patch	19,4 ko	06 août 2019	Paul Marillonnet
0001-accounts-send-validation-email-before-self-triggered.patch	18,6 ko	19 septembre 2019	Paul Marillonnet
0001-accounts-send-validation-email-before-self-triggered.patch	19,5 ko	19 septembre 2019	Paul Marillonnet