Authentic 2 - Development #34115

Le ?next= se perd à la création de compte

18 juin 2019 14:06 - Frédéric Péters

Statut:	Fermé	**Début:**	18 juin 2019
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Création d'un compte via l'API, avec send_registration_email_next_url = xxx; ce xxx se trouve bien repris dans l'URL mentionnée dans le message, https://.../accounts/password/reset/confirm/...?next=xxx. Mais à la validation de ce formulaire, je ne me trouve pas envoyé vers xxx.

Révisions associées

Révision 26be52b4 - 04 juillet 2019 17:17 - Benjamin Dauvergne

whitelist send_registration_email_next_url using HMAC signature (#34115)

Historique

#1 - 18 juin 2019 20:36 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#2 - 18 juin 2019 20:37 - Benjamin Dauvergne

- Fichier 0001-tests-test-users-API-with-send_registration_email_ne.patch ajouté

- Tracker changé de Bug à Development

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

Déjà un test pour montrer que ça marche mais il faut que l'URL qui est passé soit whitelistée.

#3 - 19 juin 2019 09:29 - Frédéric Péters

On peut envisager quelque chose au niveau de l'API, répondre en erreur quand send_registration_email_next_url contient une URL qui ne sera pas prise en compte ? Ou logguer le fait que ? (ou bien sûr qu'une URL transmise par l'API soit prise en compte, même si elle n'a pas été explicitement déclarée).

#4 - 19 juin 2019 15:50 - Benjamin Dauvergne

- Fichier 0001-whitelist-send_registration_email_next_url-using-HMA.patch ajouté

Voilà voilà.

#5 - 02 juillet 2019 11:11 - Paul Marillonnet

```
@@ -894,6 +899,11 @@ def good_next_url(request, next_url):
         return True
     if same_origin(request.build_absolute_uri(), next_url):
         return True
+    signature = request.POST.get(constants.NEXT_URL_SIGNATURE) or request.GET.get(constants.NEXT_URL_SIGNATUR
E)
+
+    if signature:
+        return crypto.check_hmac_url(settings.SECRET_KEY, next_url, signature)
```

Question de principe j'aurais bien vu cet ajout de code remonter plus haut la fonction good_next_url : s'il y a une signature, il faut la vérifier. Si la signature ne colle pas, même pour un next sur une ressource de même origine, c'est qu'il y a une embrouille.

#6 - 02 juillet 2019 13:52 - Benjamin Dauvergne

Paul Marillonnet a écrit :

> [...]
>
> Question de principe j'aurais bien vu cet ajout de code remonter plus haut la fonction good_next_url : s'il y a une signature, il faut la vérifier. Si la signature ne colle pas, même pour un next sur une ressource de même origine, c'est qu'il y a une embrouille.

Si on était la NSA je te dirai oui, mais l'avantage que j'y vois c'est que les cas qui marchent déjà ne sont pas impactés et comme le bloquage des URLs de redirection n'est pas non plus une énorme avancée dans la sécurité ça me parait suffisant de dire que les signatures c'est en option du système actuel.

#7 - 03 juillet 2019 09:13 - Paul Marillonnet

- Statut changé de Solution proposée à Solution validée

Benjamin Dauvergne a écrit :

> Si on était la NSA je te dirai oui

Quand ils nous commanderont une GRU il faudra penser à revenir sur ce ticket.

#8 - 04 juillet 2019 17:17 - Benjamin Dauvergne

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

```
commit 26be52b49f64fb1a67677b2def1bc962a96f0226
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Tue Jun 18 20:36:26 2019 +0200

    whitelist send_registration_email_next_url using HMAC signature (#34115)
```

#9 - 05 juillet 2019 01:15 - Frédéric Péters

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

Fichiers

0001-tests-test-users-API-with-send_registration_email_ne.patch	1,74 ko	18 juin 2019	Benjamin Dauvergne
0001-whitelist-send_registration_email_next_url-using-HMA.patch	6,56 ko	19 juin 2019	Benjamin Dauvergne