Combo - Development #35352

fargo, ne pas logger d'erreur de GET sur une 403

10 août 2019 11:47 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	10 août 2019
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Si l'utilisateur n'existe pas dans fargo on obtient une 403, ça ne sert à rien de la logger en erreur ni en warning d'ailleurs.

```
Report

failed to GET https://porte-documents.clissonsevremaine.fr/api/documents/recently-added/?NameID=15
cde3228f7745f08bd55599cdae777a&orig=monespace.clissonsevremaine.fr (403)

Django Version:     1.11.20
Python Executable:     /usr/bin/uwsgi-core
Python Version:     2.7.13
Python Path:

['.',
 '',
 '/usr/lib/python2.7',
 '/usr/lib/python2.7/plat-x86_64-linux-gnu',
 '/usr/lib/python2.7/lib-tk',
 '/usr/lib/python2.7/lib-old',
 '/usr/lib/python2.7/lib-dynload',
 '/usr/local/lib/python2.7/dist-packages',
 '/usr/lib/python2.7/dist-packages']

Server time:     sam, 10 Aoû 2019 09:23:58 +0200
```

Les informations de signature ont disparu des logs à cause de #35225, il faut juste s'en souvenir.

```
Report

failed to GET https://porte-documents.clissonsevremaine.fr/api/documents/recently-added/?NameID=fc
c37bc2ba144264b573feaf3ff1a811&orig=monespace.clissonsevremaine.fr&algo=sha256&timestamp=2019-07-0
6T12%3A20%3A27Z&nonce=8f4a60573d5755adb9da654c66994817L&signature=j/F2R1hLZsOE2cPnTGaDtPsFop28jsH8
SNLNjBuwTfQ%3D (403)

Django Version:     1.11.20
Python Executable:     /usr/bin/uwsgi-core
Python Version:     2.7.13
Python Path:

['.',
 '',
 '/usr/lib/python2.7',
 '/usr/lib/python2.7/plat-x86_64-linux-gnu',
 '/usr/lib/python2.7/lib-tk',
 '/usr/lib/python2.7/lib-old',
 '/usr/lib/python2.7/lib-dynload',
 '/usr/local/lib/python2.7/dist-packages',
 '/usr/lib/python2.7/dist-packages']

Server time:     sam, 6 Jul 2019 14:20:27 +0200
```

Demandes liées:

Lié à Hobo - Development #39911: rest_authentication : lever des exceptions s...	**Fermé**	**14 février 2020**

Révisions associées

Révision 3baed95c - 24 mars 2020 07:57 - Benjamin Dauvergne

fargo: hide user-not-found API errors and only that (#35352)

Historique

#1 - 10 août 2019 11:58 - Benjamin Dauvergne

- Fichier 0001-fargo-do-not-log-403-response-as-errors-35352.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#2 - 13 août 2019 13:59 - Thomas Noël

Je dirais que c'est plutôt à fargo de répondre "vide" dans ce cas (et donc ne faire le 403 que sur les pépins de signature), voire répondre un err:1 ... mais ce n'est pas possible dans fargo car tout se joue trop tôt (Django Rest Framework).

Bref, je ne suis pas chaud, ne pas avoir d'alerte en cas de panne du système de signature, ça m'ennuie un peu. Et je n'ai pas souvenir d'avoir tant rencontré la trace ci-dessus (toi, si ?)

#3 - 13 août 2019 14:02 - Benjamin Dauvergne

Thomas Noël a écrit :

> Je dirais que c'est plutôt à fargo de répondre "vide" dans ce cas (et donc ne faire le 403 que sur les pépins de signature), voire répondre un err:1 ... mais ce n'est pas possible dans fargo car tout se joue trop tôt (Django Rest Framework).

À vrai dire je n'ai même pas trouvé dans le code DRF d'où vient ce 403, c'est une exception PermissionDenied normalement et je n'en vois pas au moment du check d'authentification, on lève un AuthenticationFailed qui devrait donner une 401.

> Bref, je ne suis pas chaud, ne pas avoir d'alerte en cas de panne du système de signature, ça m'ennuie un peu. Et je n'ai pas souvenir d'avoir tant rencontré la trace ci-dessus (toi, si ?)

Oui tous les déploiements avec un fargo dès qu'il y a une cellule dernier document, ça en produit sur les utilisateurs non provisionnés.

#4 - 13 août 2019 14:28 - Thomas Noël

Benjamin Dauvergne a écrit :

> Oui tous les déploiements avec un fargo dès qu'il y a une cellule dernier document, ça en produit sur les utilisateurs non provisionnés.

C'est un peu ça qui m'étonne, les "utilisateurs non provisionnés", c'est pas si fréquent normalement... le cas que je vois c'est dans la seconde après la création du compte, retour sur la page d'accueil qui présente les derniers documents, et boum ?

#5 - 13 août 2019 15:19 - Benjamin Dauvergne

Thomas Noël a écrit :

> Benjamin Dauvergne a écrit :
>
> > Oui tous les déploiements avec un fargo dès qu'il y a une cellule dernier document, ça en produit sur les utilisateurs non provisionnés.
>
> C'est un peu ça qui m'étonne, les "utilisateurs non provisionnés", c'est pas si fréquent normalement... le cas que je vois c'est dans la seconde après la création du compte, retour sur la page d'accueil qui présente les derniers documents, et boum ?

Ben c'est les gens inscrits avant qu'on déploie fargo, à moins d'être sûr de toujours déployer fargo avant toute mise en prod on en aura d'autres, jusqu'à ce qu'on provisionne autrement.

#6 - 13 août 2019 15:24 - Thomas Noël

Benjamin Dauvergne a écrit :

> Thomas Noël a écrit :
>
> > Benjamin Dauvergne a écrit :

> > > Oui tous les déploiements avec un fargo dès qu'il y a une cellule dernier document, ça en produit sur les utilisateurs non provisionnés.
>
> > C'est un peu ça qui m'étonne, les "utilisateurs non provisionnés", c'est pas si fréquent normalement... le cas que je vois c'est dans la seconde après la création du compte, retour sur la page d'accueil qui présente les derniers documents, et boum ?
>
> Ben c'est les gens inscrits avant qu'on déploie fargo, à moins d'être sûr de toujours déployer fargo avant toute mise en prod on en aura d'autres, jusqu'à ce qu'on provisionne autrement.

« authentic hobo_provision --users » et hop

#7 - 12 février 2020 13:53 - Benjamin Dauvergne

Je ne suis pas tellement d'accord, supposer que le provisionning des usagers fonctionne à 100% en temps réel c'est casse gueule, je pense que ce patch est utile.

#8 - 12 février 2020 15:06 - Thomas Noël

Benjamin Dauvergne a écrit :

> Je ne suis pas tellement d'accord, supposer que le provisionning des usagers fonctionne à 100% en temps réel c'est casse gueule, je pense que ce patch est utile.

Fargo a aussi un front, donc on a aussi du provisionning via SAML (et pour le coup "100% temps réel") dès que la personne clique sur "mes documents". Je reste pas chaud à cacher les 403 (et comme dit plus haut je préférerais qu'on creuse hobo/rest_authentication.py pour voir si vraiment on peut envoyer un err:1 quand l'utilisateur n'existe pas... même si j'ai pas vu de chemin pour faire ça)

#9 - 12 février 2020 17:31 - Benjamin Dauvergne

J'ai trouvé l'origine de la 403 (ça convertit en 403 tout ce qui est 401 mais ne vient pas d'un mode d'authentification HTTP classique, i.e. via un entête Authorization, parce que c'est des nazis du code HTTP) :

```
    def handle_exception(self, exc):
        """
        Handle any exception that occurs, by returning an appropriate response,
        or re-raising the error.
        """
        if isinstance(exc, (exceptions.NotAuthenticated,
                            exceptions.AuthenticationFailed)):
            # WWW-Authenticate header for 401 responses, else coerce to 403
            auth_header = self.get_authenticate_header(self.request)
```

```
            if auth_header:
                exc.auth_header = auth_header
            else:
                exc.status_code = status.HTTP_403_FORBIDDEN
```

On pourrait passer par une erreur APIException et faire une 401 avec err=1 en loucedé, ça t'irait ? Mais ça va devoir aller dans hobo.

#10 - 12 février 2020 19:52 - Benjamin Dauvergne

- Statut changé de Solution proposée à Information nécessaire

- Assigné à changé de Benjamin Dauvergne à Thomas Noël

#11 - 13 février 2020 00:55 - Thomas Noël

- Assigné à changé de Thomas Noël à Benjamin Dauvergne

> On pourrait passer par une erreur APIException et faire une 401 avec err=1 en loucedé, ça t'irait ? Mais ça va devoir aller dans hobo.

Oui, que ça soit dans hobo/rest_authentication.py c'est le bon endroit. Et cela grâce à un raise d'une APIException avec un detail={err:1, err_desc:"user-not-found"} et status_code=401, pour arriver ici dans le code de DRF :

```
def exception_handler(exc, context):
```

```
    if isinstance(exc, exceptions.APIException):
        headers = {}
```

```
        if getattr(exc, 'auth_header', None):
            headers['WWW-Authenticate'] = exc.auth_header
        if getattr(exc, 'wait', None):
            headers['Retry-After'] = '%d' % exc.wait

        if isinstance(exc.detail, (list, dict)):
            data = exc.detail
        else:
            data = {'detail': exc.detail}

        set_rollback()
        return Response(data, status=exc.status_code, headers=headers)
</per>

Et donc dans combo, petit patch quand même : quand on appelle une API DRF on saura qu'un 401 avec un payload e
rr=1, on sait que ça peut arriver (soucis de provisionning sur un nouveau compte) : loguer juste en info, ou a
u pire warning.

J'ai bon ?
```

#12 - 13 février 2020 08:03 - Benjamin Dauvergne

Thomas Noël a écrit :

> Et donc dans combo, petit patch quand même : quand on appelle une API DRF on saura qu'un 401 avec un payload err=1, on sait que ça peut arriver (soucis de provisionning sur un nouveau compte) : loguer juste en info, ou au pire warning.
>
> J'ai bon ?

Yep c'est ça l'idée.

#13 - 14 février 2020 16:57 - Benjamin Dauvergne

- Lié à Development #39911: rest_authentication : lever des exceptions spécifiques en cas d'échec ajouté

#14 - 22 mars 2020 12:09 - Benjamin Dauvergne

- Fichier 0001-fargo-hide-user-not-found-API-errors-and-only-that-3.patch ajouté

- Statut changé de Information nécessaire à Solution proposée

#15 - 23 mars 2020 15:30 - Thomas Noël

- Statut changé de Solution proposée à Solution validée

#16 - 24 mars 2020 07:57 - Benjamin Dauvergne

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

```
commit 60add2525c032ec2e7608d9d43ec8bc0923b5ee7
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Sun Mar 22 12:07:14 2020 +0100

    fargo: hide user-not-found API errors and only that (#35352)
```

#17 - 31 mars 2020 20:15 - Frédéric Péters

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

Fichiers

0001-fargo-do-not-log-403-response-as-errors-35352.patch	2,25 ko	10 août 2019	Benjamin Dauvergne
0001-fargo-hide-user-not-found-API-errors-and-only-that-3.patch	3,02 ko	22 mars 2020	Benjamin Dauvergne