django-mellon - Bug #81211

Middleware : mauvaise détection d'une requête ajax

14 septembre 2023 15:54 - Emmanuel Cazenave

Statut:	Fermé	**Début:**	14 septembre 2023
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

De #81141#note-4, une requête ajax faite depuis wcs vers combo qui n'est pas détectée comme étant ajax, mellon qui tente une authentification passive et échec.

A lire le code il me semble que ça a du marcher via :

```
# Skip AJAX requests
if request.headers.get('x-requested-with') == 'XMLHttpRequest':
    return
```

Mais là point de 'x-requested-with' dans la requête, j'imagine que ça vient d'une évolution de JQuery et que du coup la solution n'est pas du tout dans mellon, mais ce ticket en première approche pour ça ne se perde pas dans les limbes.

Potentiellement des problèmes dans combo où on voit :

```
def is_ajax(request):
    return request.headers.get('x-requested-with') == 'XMLHttpRequest'
```

Demandes liées:

Lié à Authentic 2 - Development #82266: idp_saml2: autoriser les requêtes COR...	**Fermé**	**11 octobre 2023**

Révisions associées

Révision c98d4629 - 14 septembre 2023 16:41 - Benjamin Dauvergne

middleware: check ajax request with sec-fetch-mode header header (#81211)

Historique

#2 - 14 septembre 2023 16:09 - Benjamin Dauvergne

À mon avis on devrait rajouter ça maintenant:

```
sec_fetch_mode = request.headers.get('sec-fetch-mode')
if sec_fetch_mode and sec_fetch_mode != 'navigate':
    return
```

#3 - 14 septembre 2023 16:11 - Benjamin Dauvergne

Mais je me demande quand même comment on fait pour personnaliser le template d'une brique en fonction du statut connecté ou pas d'un utilisateur si une cellule est chargée en ajax, visiblement ça ne marchera jamais si on est pas d'abord connecté au portail. J'ai l'impression qu'on a déjà cette discussion qui avait peut-être menée à détecté ces appels ajax dans mellon.

#4 - 14 septembre 2023 16:25 - Emmanuel Cazenave

Benjamin Dauvergne a écrit :

> À mon avis on devrait rajouter ça maintenant:
> [...]

Ça marcherait sur mon exemple, la requête est faite avec :

```
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
```

#5 - 14 septembre 2023 16:34 - Emmanuel Cazenave

Benjamin Dauvergne a écrit :

> visiblement ça ne marchera jamais si on est pas d'abord connecté au portail.

Oui même analyse ici avec Thomas N.

Sinon juste avant ton message, je m'apprêtais à suggérer de passer systématiquement un ?no-passive-auth dans combo.public.js::combo_load_cell sur l'idée qu'une authent passive ne peut pas marcher en ajax.

#6 - 14 septembre 2023 16:40 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#7 - 14 septembre 2023 16:42 - Benjamin Dauvergne

- Assigné à Benjamin Dauvergne supprimé

Emmanuel Cazenave a écrit :

> Sinon juste avant ton message, je m'apprêtais à suggérer de passer systématiquement un ?no-passive-auth dans combo.public.js::combo_load_cell sur l'idée qu'une authent passive ne peut pas marcher en ajax.

Si vous voulez, mais c'est pas le bon projet :)

#8 - 14 septembre 2023 16:42 - Robot Gitea

- Statut changé de Nouveau à Solution proposée

- Assigné à mis à Benjamin Dauvergne

Benjamin Dauvergne (bdauvergne) a ouvert une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/django-mellon/pulls/8
- Titre : middleware: check ajax request with sec-fetch-mode header header (#81211)
- Modifications : https://git.entrouvert.org/entrouvert/django-mellon/pulls/8/files

#9 - 14 septembre 2023 16:45 - Benjamin Dauvergne

Emmanuel Cazenave a écrit :

> Benjamin Dauvergne a écrit :
>
> > visiblement ça ne marchera jamais si on est pas d'abord connecté au portail.
>
> Oui même analyse ici avec Thomas N.

Je dis ça parce qu'en première analyse je voulais autoriser le passage des requêtes CORS sur /idp/saml2/sso/, car en vrai c'est ça qui bloque, le fait que le endpoint de SSO SAML n'ajoute pas l'entête Allow-CORS (à faire sélectivement certainement, genre en testant que l'entête Origin match le domaine du service SAML demandeur et en posant Allow-CORS: header['origin']). Ce ticket c'est pour garder le statu-quo actuel, c'est déjà bien.

#10 - 14 septembre 2023 16:50 - Robot Gitea

- Statut changé de Solution proposée à Solution validée

Emmanuel Cazenave (ecazenave) a approuvé une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/django-mellon/pulls/8

#11 - 18 septembre 2023 10:41 - Robot Gitea

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

Benjamin Dauvergne (bdauvergne) a mergé une pull request sur Gitea concernant cette demande :

- URL : https://git.entrouvert.org/entrouvert/django-mellon/pulls/8
- Titre : middleware: check ajax request with sec-fetch-mode header header (#81211)
- Modifications : https://git.entrouvert.org/entrouvert/django-mellon/pulls/8/files

#12 - 22 septembre 2023 12:14 - Transition automatique

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

#13 - 11 octobre 2023 15:41 - Benjamin Dauvergne

- Lié à Development #82266: idp_saml2: autoriser les requêtes CORS sur /idp/saml2/sso/ ajouté

#14 - 26 novembre 2023 04:42 - Transition automatique

Automatic expiration