Publik - Support #31842

pas d'authentification passive mellon dans Combo

29 mars 2019 10:54 - Serghei Mihai

Statut:	Fermé	**Début:**	29 mars 2019
Priorité:	Normal	**Echéance:**	
Assigné à:	Serghei Mihai	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Club:**	Non
Planning:	Non		

Description

Je fais le ticket ici, à ranger ensuite au bon endroit.

Si un formulaire wcs requiert l'authentification, l'usager est rédirigé vers authentic et revient ensuite sur le formulaire en étant connecté.
Si ensuite l'usager va sur Combo il peut ne pas être connecté.

C'est genant dans les cas ou le formulaire (et son workflow) ajoute des montants à payer dans le panier, et rédirige l'usager directement vers le paiement: Combo. Combo signale alors que l'usager n'est pas connecté.

Cela peut se produire dans des cas ou il y a des appels ajax pour récupérer les badges des cellules comme "Panier" ou "Notifications", instanciées quelque part dans Combo.
L'appel ajax passe par l'authentification passive, le cookie "MELLON_PASSIVE_TRIED" sans pourtant que l'authentification aboutisse.

Je joins un log HAR de Firefox qui illustre le parcours.

On voit à la fin Authentic faire une 302 avec :

```
Location: https://citoyen-combo.entrouvert.lan/accounts/mellon/login/?SAMLart=AAQAAIelNeK1%2Bphtfd
VV%2F6BObd7IOSNNRTQwMkFFMDU4MzAzNjQyOTk3RUQ%3D&RelayState=1a0033f7-c6d1-49c2-95ad-29497f9b1b32
```

mais le navigateur ne suit pas la rédirection et leve le message d'alerte:

```
Cross-Origin Request Blocked: The Same Origin Policy disallows reading the remote resource at http
s://connexion-authentic.entrouvert.lan/idp/saml2/sso?SAMLRequest=jZNfT9swFMW%2FSmQJ3lLnTwuJlxQFWqR
K24TGtIe9IONewFJiB99rWr49bquirJHQniL94nPPPcdJhbJre9F4ejG%2F4NUDUrTtWoNi%2F6Jm3hlhJWoURnaAgpS4b358F
9kkEb2zZJVt2UDytUIigiNtzVECtmYvRD0KzjebzQQMOevfwqGJsh1n0WpRs4eiScvmcjktLpub5CLNkuJiObst8iS%2FTpo0y
1n0BxyGsTULLkGE6GFlkKShgJK0jJM8zsrfSSmmhUjLvyxahKjaSNqrjisoawxsA4plaCQso9VwpVYartc93wXNOKJl0a11Cvb
11exJtgg797uQU7%2FBkcyrnUDst3LzTy9N9h1MHHI%2B2lMXqZT1hpB30LbWhAfJtSTJKz6cVR2ub7klMLv8OK%2FAihCBHrx
r%2F9Oq12G88fGjXD8D8qtePsPZ7PpstqjTc9n13wYgOwX5KZidgjQZkfHYMRk5ZSOrbFrxYdxDN%2F%2FWcSA%2Fw5e4WtzZV
qv3qAmNbm4cSAo3RM4D45%2FS4Y8w%2FwA%3D&RelayState=1a0033f7-c6d1-49c2-95ad-29497f9b1b32&SigAlg=http%
3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signature=Pnwn6cNd%2BO9DiFFPy6%2BHvZ%2Fhy%2F6q
cjM46si%2Bs3NzHf91jCM5AlUZl00mPibGX6klPpYlBPDWQoRcS%2BtsUvcPPEJetURAjtPtdv%2BZRA70ae5H0fREmzOa56DJ
SwPkd%2F5oyD%2BydpSHm7S2oqPO8%2FCkVDObfJE3PJiuuLL7TVF0Sxg%3D. (Reason: CORS header ‘Access-Control
-Allow-Origin’ missing).
```

Historique

#2 - 29 mars 2019 11:00 - Frédéric Péters

> CORS header ‘Access-Control-Allow-Origin’ missing

Peut-être pas ça mais au moins une piste, Authentic est particulier dans sa gestion dynamique de l'entête, cf src/authentic2/cors.py. (et on peut imaginer le navigateur ayant déjà fait une première requête et ayant mémorisé une valeur différente pour l'entête).

(les autres modules passent par hobo/middleware/cors.py qui tape tous les services déclarés dans Hobo dans l'entête).

#3 - 29 mars 2019 12:15 - Benjamin Dauvergne

Authentic ne supporte pas les requêtes CORS en dehors de /api/user/, il me semble (le contenu de cors.py n'est utilisé que par le décorateur JSONP dans decorators.py, qui n'est utilisé que par un seul endpoint /api/user/).

Le seul truc qui marche c'est les chargements via <script/> comme sur les backoffice.

~~Je n'ai pas trop d'idée, soit on rend tout authentic CORS compatible avec un middleware, et je n'ai pas toutes les implications au niveau sécurité en tête, soit poupouf.~~

Mais en fait CORSMiddleware est aussi chargé par authentic donc je ne vois pas trop d'où vient le problème... peut-être faut-il déclarer explicitement le support des redirections (vague souvenir de la spécification CORS).

#4 - 29 mars 2019 12:20 - Benjamin Dauvergne

Trouvé: https://developer.mozilla.org/fr/docs/Web/HTTP/CORS#Requ%C3%AAtes_pr%C3%A9liminaires_et_redirection

Mais comme CORSMiddleware passe avant PassiveAuthenticationMiddleware et court-circuite explicitement la génération des réponse il ne devrait pas y avoir de redirection sur les pré-requêtes... je suis perdu.

#5 - 01 avril 2019 11:14 - Benjamin Dauvergne

Serghei si tu peux chercher un peu plus pour voir où ça merde dans le circuit, c'est cool.

#6 - 01 avril 2019 11:17 - Serghei Mihai

- Assigné à mis à Serghei Mihai

Oui, je prend.

#7 - 11 mai 2019 17:22 - Frédéric Péters

- Statut changé de Nouveau à Fermé

C'est #32395.

Fichiers

Archive 19-03-29 10-48-37.har	2,92 Mo	29 mars 2019	Serghei Mihai