Publik - Support #32564

élaboration du menu portail agent et gestion des "cookies tiers"

24 avril 2019 14:47 - Thomas Noël

Statut:	Fermé	**Début:**	24 avril 2019
Priorité:	Normal	**Echéance:**	
Assigné à:	Pierre Cros	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Club:**	Non
Planning:	Non		

Description

Le menu "portail agent" charge des éléments menu.json depuis les différentes briques de Publik. Cela est fait via ajax, en "tâche de fond".

Au premier accès, après un login réussi sur Authentic, ces menu.json passent par le SSO. Comme la session est bonne sur Authentic, ça marche...

Mais si Authentic n'est pas sur le même domaine que les briques, alors il ne reçoit pas son cookie de session (interdiction des cookies tiers) et pense donc que l'utilisateur n'est pas loggué.

La construction du menu échoue alors...

L'accès aux briques reste bon, parce que ce problème de cookie ne se pose que pour les requêtes ajax.

C'est constaté sur Firefox et Chromium avec le mode de protection contre les "cookies tiers" (activé par défaut sur les toutes dernières versions).

Historique

#1 - 24 avril 2019 14:50 - Thomas Noël

Constaté sur :

- https://agents.services.tours.fr/ (idp : https://connexion.services.tours-metropole.fr/)
- https://agendas.mesdemarches.ville-lomme.fr et https://agents.mesdemarches.hellemmes.fr/ (idp : https://connexion.mesdemarches.lille.fr/)

#2 - 24 avril 2019 16:19 - Pierre Cros

Et on doit mettre en prod dans 6 jours à Lille.

#3 - 24 avril 2019 17:12 - Thomas Noël

Comme le soucis est juste sur le portail agent, il est possible de configurer les navigateurs pour ne pas bloquer les cookies tiers (éventuellement dans une whiteliste), et tout fonctionne alors sans soucis.

#5 - 24 avril 2019 17:59 - Benjamin Dauvergne

Thomas Noël a écrit :

> Mais si Authentic n'est pas sur le même domaine que les briques, alors il ne reçoit pas son cookie de session (interdiction des cookies tiers) et pense donc que l'utilisateur n'est pas loggué.

Je ne suis pas certain de cette analyse, on pourrait voir un dump des requêtes notamment le contenu de Origin et Access-Control-Allow-Origin dans les différentes requêtes ?

Requête	Origin	Réponse: Access-Control-Allow-Origin	Réponse: Access-Control-Allow-Credentials	Statut
GET /menu.json	?	?	?	302
GET /idp/saml/sso	?	?	?	302
GET /login/	?	?	?	?

À noter que sur une utilisation de withCredentials Allow-Origin:* est interdit (vur sur https://stackoverflow.com/questions/31465774/chrome-cors-with-302-redirects-and-withcredentials-true).

#6 - 24 avril 2019 18:04 - Benjamin Dauvergne

Aussi les gens qui constatent ce problème pourriez-vous vérifier la valeur de votre politique de sécurité dans (https://support.mozilla.org/en-US/kb/disable-third-party-cookies) FX, si vous avez "All third party cookies" ou autre chose.

#7 - 24 avril 2019 18:05 - Benjamin Dauvergne

Il est clair qu'avec All third party cookies on ne peut à peu près plus rien faire en JSON (ni AJAX ni JSONP) mais ce n'est pas la configuration standard "normalement".

#8 - 24 avril 2019 18:17 - Benjamin Dauvergne

Mais aussi (de https://blog.zok.pw/web/2015/10/21/3rd-party-cookies-in-practice/):

> First of all, when 3rd-party cookies are disabled, browsers do not save, nor send cookies for domains other than the top-level window (current page). This affects all cross-domain requests including resources (e.g. <img> tags), iframes, and XMLHttpRequests (including CORS). This is something that you would expect, actually.
> If there is a cookie that was set previously as a 1st-party, it won't be used.
> Javascript in cross-origin iframe cannot set cookies as well. No exceptions will be thrown, but document.cookie will always return an empty string, even if you set it to something.
> No cookies in CORS requests too, even if you use .withCredentials parameter. Cookie header from server is just ignored.

Le plus important :

> 3rd-level subdomains and sibling 3rd-level subdomains are not considered 3rd-party: foo.example.com can load an iframe pointing to bar.example.com and it will be allowed to set cookies.

#9 - 24 avril 2019 18:18 - Pierre Cros

J'ai "traqueurs tiers" et pas "tous les traqueurs tiers"

#10 - 24 avril 2019 18:51 - Benjamin Dauvergne

Je suis en roue libre c'est du JSONP. J'ai installé FX 66 de unstable mais je n'arrive pas à reproduire, vous auriez des plugins particuliers l'un et l'autre ?

```
firefox:
  Installé : 66.0.1-1
  Candidat : 66.0.1-1
 Table de version :
 *** 66.0.1-1 500
        500 http://ftp.fr.debian.org/debian unstable/main amd64 Packages
        100 /var/lib/dpkg/status
```

#11 - 24 avril 2019 19:02 - Pierre Cros

Oui, je peux pas tester sans eux parce que le truc est down à lille mais j'ai Ublock Origin et Privacy badger qui sont susceptibles de bloquer des choses

#12 - 24 avril 2019 19:03 - Benjamin Dauvergne

Thomas a filé un lien vers Tours (plus haut) où il reproduit le problème sur son FX.

#13 - 24 avril 2019 19:04 - Pierre Cros

sur https://agents.services.tours.fr/ je ne constate aucun problème (mais je n'avais pas testé avant)

#14 - 24 avril 2019 19:09 - Benjamin Dauvergne

J'ai installe uBlock Origin et Privacy Badger (je n'ai pas touché à leurs settings) et ça ne fait rien sur le site de Tours, j'attends le retour de Lille pour tester là aussi.

#15 - 24 avril 2019 19:10 - Benjamin Dauvergne

Pierre Cros a écrit :

> sur https://agents.services.tours.fr/ je ne constate aucun problème (mais je n'avais pas testé avant)

C'est important ça permet déjà d'écarter le FX de Thomas comme "extrêmement casse couille" et mettre le tien dans une catégorie plus normale :)

#16 - 24 avril 2019 19:11 - Pierre Cros

J'ai modifié mon /etc/hosts pour contourner le pb DNS de Lille et ça semble marcher à Lille aussi (sans désactiver mes plugins). Je sais pas ce que tu as fait mais ça me donne de l'espoir, merci !

#17 - 24 avril 2019 19:16 - Benjamin Dauvergne

Pierre Cros a écrit :

> J'ai modifié mon /etc/hosts pour contourner le pb DNS de Lille et ça semble marcher à Lille aussi (sans désactiver mes plugins). Je sais pas ce que tu as fait mais ça me donne de l'espoir, merci !

Je n'ai rien fait, ce n'est pas bon signe :)

#18 - 24 avril 2019 19:33 - Pierre Cros

Je me suis planté désolé, il fallait tester Hellemmes et pas Lille our constater les problèmes, ce que j'ai fait maintenant sur : https://agents.mesdemarches.hellemmes.fr/

Je pense que le coupable est Privacy Badger, ça marche quand je le désactive.

#19 - 26 avril 2019 18:48 - Benjamin Dauvergne

- Statut changé de Nouveau à Information nécessaire

- Assigné à mis à Pierre Cros

On peut fermer ?

#20 - 26 avril 2019 20:33 - Pierre Cros

- Statut changé de Information nécessaire à Fermé