

Authentic 2 - Development #43221

retirer les usages de HTTP_REFERER

22 mai 2020 11:51 - Thomas Noël

Statut:	Nouveau	Début:	22 mai 2020
Priorité:	Normal	Echéance:	
Assigné à:		% réalisé:	0%
Catégorie:		Temps estimé:	0:00 heure
Version cible:			
Patch proposed:	Non	Planning:	Non

Description

Parce que ce n'est pas bien génial (facile d'y mettre n'importe quoi) et qu'on pourrait prochainement généraliser l'usage de "Referrer-policy: same-origin"

A priori :

```
src/authentic2/app_settings.py: VALID_REFERERERS=Setting(
src/authentic2/cbv.py:         next_url = request.META.get('HTTP_REFERER') or \
src/authentic2/decorators.py:             origin = request.META.get('HTTP_REFERER')
src/authentic2/saml/common.py:             referer = request.META.get('HTTP_REFERER')
src/authentic2/utils/__init__.py:             referer = request.META.get('HTTP_REFERER')
src/authentic2/views.py:             referer = self.request.META.get('HTTP_REFERER', '')
src/authentic2/views.py:             for valid_referer in app_settings.VALID_REFERERERS:
src/authentic2_idp_cas/views.py:                 referrer = request.META['HTTP_REFERER']
```

Révisions associées

Révision b6b76ee1 - 20 octobre 2022 09:58 - Benjamin Renard

Fix error 500 on CAS logout page if no HTTP Referer is provided (#43221)

License: MIT

Révision 891599f1 - 20 octobre 2022 10:22 - Benjamin Renard

Fix error 500 on CAS logout page if no HTTP Referer is provided (#43221)

License: MIT

Historique

#2 - 22 mai 2020 12:42 - Benjamin Dauvergne

```
src/authentic2/app_settings.py: VALID_REFERERERS=Setting(
```

Je crois que ça n'est jamais utilisé, mais à vérifier, utiliser par utils.check_referer() (utilisé dans la vue de logout pour empêcher un logout direct sur un GET venant d'un autre site) et LoggedInView (pas utilisée non?).

```
src/authentic2/cbv.py:     next_url = request.META.get('HTTP_REFERER') or \
```

Pas utilisé je pense, dans tous les cas où on en a besoin je pense qu'on passe un paramètre next=.

```
src/authentic2/decorators.py:     origin = request.META.get('HTTP_REFERER')
```

Il faut virer les vues JSONP et les remplacer par des appels CORS.

```
src/authentic2/saml/common.py:     referer = request.META.get('HTTP_REFERER')
```

Utiliser dans un error_page(), à virer et afficher les erreurs de manière classique ou au moins uniformisée pour tout a2.

```
src/authentic2/utils/__init__.py: referer = request.META.get('HTTP_REFERER')
```

utils.check_referer() voir premier point.

```
src/authentic2/views.py:     referer = self.request.META.get('HTTP_REFERER', '')  
src/authentic2/views.py:     for valid_referer in app_settings.VALID_REFERERS:
```

LoggedInView() voir premier point.

```
src/authentic2_idp_cas/views.py:     referrer = request.META['HTTP_REFERER']
```

On peut juste remplacer par un redirect sur la vue de logout qui fait la même validation en moins bien (sans avoir connaissance des URLs des SPs CAS), on pourrait aussi poser d'accepter du POST, dans ce cas on reçoit l'entête Origin qui lui n'est jamais bloqué. Comme on déploie jamais de CAS c'est pas super important.

#3 - 15 avril 2021 14:27 - Benjamin Renard

- Fichier 0001-Fix-error-500-on-CAS-logout-page-if-no-HTTP-Referer-.patch ajouté

Benjamin Dauvergne a écrit :

```
src/authentic2_idp_cas/views.py:     referrer = request.META['HTTP_REFERER']
```

On peut juste remplacer par un redirect sur la vue de logout qui fait la même validation en moins bien (sans avoir connaissance des URLs des SPs CAS), on pourrait aussi poser d'accepter du POST, dans ce cas on reçoit l'entête Origin qui lui n'est jamais bloqué. Comme on déploie jamais de CAS c'est pas super important.

Ça semble lié, alors je mets ça ici: aujourd'hui l'URL de déconnexion CAS déclenche une erreur 500 si *HTTP_REFERER* n'est pas disponible:

```
ERROR Internal Server Error: /idp/cas/logout#012Traceback (most recent call last):#012  File "/usr/lib/python3  
/dist-packages/dja  
ngo/core/handlers/exception.py", line 41, in inner#012      response = get_response(request)#012  File "/usr/lib  
/python3/dist-packages/django/core/handlers/base.py", line 187, in _get_response#012      response = se  
lf.process_exception_by_middleware(e, request)#012  File "/usr/lib/python3/dist-packages/django/core/handlers/  
base.py", line 185, in _get_response#012      response = wrapped_callback(request, *callback_args, **ca  
llback_kwargs)#012  File "/usr/lib/python3.7/contextlib.py", line 74, in inner#012      return func(*args, **kwd  
s)#012  File "/usr/lib/python3/dist-packages/authentic2/decorators.py", line 47, in f#012      return f  
unc(request, *args, **kwargs)#012  File "/usr/lib/python3/dist-packages/django/views/generic/base.py", line 68  
, in view#012      return self.dispatch(request, *args, **kwargs)#012  File "/usr/lib/python3/dist-pac  
ages/django/views/generic/base.py", line 88, in dispatch#012      return handler(request, *args, **kwargs)#012  
File "/usr/lib/python3/dist-packages/authentic2_idp_cas/views.py", line 417, in get#012      referrer =  
request.META['HTTP_REFERER']#012KeyError: 'HTTP_REFERER'
```

Le patch ci-joint corrige l'erreur 500, mais ne change pas le comportement actuellement implémenté, à savoir de ne pas déconnecter la personne si le *referrer* ne correspond pas avec un service CAS configuré.

#4 - 12 août 2022 10:51 - Thomas Noël

- Statut changé de Nouveau à Solution proposée

J'ai envoyé le patch dans Jenkins, pour relecture/validation.

#5 - 20 octobre 2022 10:20 - Paul Marillonnet (retour le 15/04)

Ça a été poussé dans main, ce qui déplaît à django-upgrade:

```
diff --git a/src/authentic2_idp_cas/views.py b/src/authentic2_idp_cas/views.py  
index 3e6e9c56..826314ff 100644  
--- a/src/authentic2_idp_cas/views.py  
+++ b/src/authentic2_idp_cas/views.py  
@@ -464,7 +464,7 @@ class LogoutView(View):  
    http_method_names = ['get']  
  
    def get(self, request):  
        -       referrer = request.META.get('HTTP_REFERER')  
+       referrer = request.headers.get('Referer')  
        next_url = request.GET.get('service') or make_url('auth_homepage')  
        if referrer:
```

```
model = Service.objects.for_service(referrer)
```

#6 - 20 octobre 2022 10:22 - Benjamin Dauvergne

- Statut changé de *Solution proposée* à *Nouveau*

Oui j'ai relu et poussé ce fix pour remettre ce ticket à Nouveau, la correction n'ayant pas de rapport et le bug étant évident.

Fichiers

0001-Fix-error-500-on-CAS-logout-page-if-no-HTTP-Referer-.patch 898 octets

15 avril 2021

Benjamin Renard