

Authentic 2 - Development #33087

NoReverseMatch sur logout avec next \"backend

14 mai 2019 14:01 - Thomas Noël

Statut:	Fermé	Début:	14 mai 2019
Priorité:	Normal	Echéance:	
Assigné à:	Benjamin Dauvergne	% réalisé:	0%
Catégorie:		Temps estimé:	0:00 heure
Version cible:		Planning:	Non
Patch proposed:	Oui		
Description			
C'est dans le cadre d'un fuzzing, mais la réponse est assez bizarre.			
<pre>Internal Server Error: /logout/ NoReverseMatch at /logout/ Reverse for '\"backend' not found. '\"backend' is not a valid view function or pattern name. Request Method: GET Request URL: https://connexion-xxx.test.entrouvert.org/logout/?local=ok&next=%5c%22backend Django Version: 1.11.20 Python Executable: /usr/bin/python Python Version: 2.7.13 Python Path: ... Server time: mar, 14 Mai 2019 12:54:30 +0200 Installed Applications: '' Installed Middleware: '' Traceback: File "/usr/lib/python2.7/dist-packages/django/core/handlers/exception.py" in inner 41. response = get_response(request) File "/usr/lib/python2.7/dist-packages/django/core/handlers/base.py" in _legacy_get_response 249. response = self._get_response(request) File "/usr/lib/python2.7/dist-packages/django/core/handlers/base.py" in _get_response 187. response = self.process_exception_by_middleware(e, request) File "/usr/lib/python2.7/dist-packages/django/core/handlers/base.py" in _get_response 185. response = wrapped_callback(request, *callback_args, **callback_kwargs) File "/usr/lib/python2.7/dist-packages/authentic2/views.py" in logout 575. response = utils.redirect(request, next_url) File "/usr/lib/python2.7/dist-packages/authentic2/utils.py" in redirect 326. include=include, exclude=exclude, fragment=fragment, resolve=resolve) File "/usr/lib/python2.7/dist-packages/authentic2/utils.py" in make_url 271. url = resolve_url(to, *args, **kwargs) File "/usr/lib/python2.7/dist-packages/django/shortcuts.py" in resolve_url 147. return reverse(to, args=args, kwargs=kwargs) File "/usr/lib/python2.7/dist-packages/django/urls/base.py" in reverse 91. return force_text(iri_to_uri(resolver._reverse_with_prefix(view, prefix, *args, **kwargs))) File "/usr/lib/python2.7/dist-packages/django/urls/resolvers.py" in _reverse_with_prefix 497. raise NoReverseMatch(msg)</pre>			

```
Exception Type: NoReverseMatch at /logout/
Exception Value: Reverse for '"backend' not found. '"backend' is not a valid view function or pattern name.
Request information:
USER: AnonymousUser

GET:
local = u'ok'
next = u'\'"backend'

POST: No POST data

FILES: No FILES data

COOKIES: No cookie data
```

Demandes liées:

Copié depuis Authentic 2 - Bug #33086: crash sur mauvaise URL next lors du lo...

Rejeté

14 mai 2019

Révisions associées

Révision 7be25fff - 04 juillet 2019 13:10 - Benjamin Dauvergne

views: validates logout next URL (#33087)

Historique

#1 - 14 mai 2019 14:02 - Thomas Noël

Même genre avec next=(:

```
NoReverseMatch at /logout/
Reverse for '(' not found. '(' is not a valid view function or pattern name.
```

```
Request Method: GET
Request URL: https://connexion-departement06.test.entrouvert.org/logout/?local=ok&next=(
```

#2 - 14 mai 2019 14:03 - Thomas Noël

Et plus amusant :

```
Internal Server Error: /logout/

NoReverseMatch at /logout/
Reverse for 'amsterdam' not found. 'amsterdam' is not a valid view function or pattern name.
```

```
Request Method: GET
Request URL: https://connexion-departement06.test.entrouvert.org/logout/?local=ok&next=amsterdam
```

#3 - 14 mai 2019 16:21 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#4 - 14 mai 2019 17:04 - Benjamin Dauvergne

- Fichier 0001-spring-cleaning-32934.patch ajouté
- Fichier 0002-views-validates-logout-next-URL-33087.patch ajouté
- Tracker changé de Bug à Development
- Statut changé de Nouveau à Solution proposée
- Patch proposed changé de Non à Oui

À appliquer après [#32934](#).

Ce patch évite aussi d'utiliser `utils.redirect()` qui doit être réservé à un usage interne, `shortcuts.redirect()` suffit pour un des URLs bruts.

Ça valide toutes les URLs next vis à vis de la whitelist dynamique, mais bon normalement personne n'est sensé appeler notre URL de logout à part authentic.

#5 - 14 mai 2019 17:11 - Benjamin Dauvergne

- Copié depuis Bug #33086: crash sur mauvaise URL next lors du logout ajouté

#6 - 02 juillet 2019 15:46 - Benjamin Dauvergne

- Fichier 0001-views-validates-logout-next-URL-33087.patch ajouté

Rebasé.

#7 - 02 juillet 2019 16:26 - Paul Marillonnet

La vue logout perd la possibilité de choisir le garabit à rendre, alors qu'il est toujours présent dans la vue login. Ça me plaît moyen d'avoir cette possibilité pour l'une de ces deux vues mais pas pour l'autre.

#8 - 02 juillet 2019 21:27 - Benjamin Dauvergne

Paul Marillonnet a écrit :

La vue logout perd la possibilité de choisir le garabit à rendre, alors qu'il est toujours présent dans la vue login. Ça me plaît moyen d'avoir cette possibilité pour l'une de ces deux vues mais pas pour l'autre.

On ne s'en sert pas, c'est du vieux code, la plupart des paramètres de vue sont inutiles, ça date de nos débuts en Django, j'essayais d'écrire les vues comme les vues générique des contribs django mais ça ne sert à rien.

#9 - 03 juillet 2019 09:15 - Paul Marillonnet

- Statut changé de Solution proposée à Solution validée

Benjamin Dauvergne a écrit :

On ne s'en sert pas, c'est du vieux code

(Est-ce qu'on aurait pas intérêt à créer un ticket de nettoyage de ce vieux code ?)

#10 - 03 juillet 2019 10:07 - Benjamin Dauvergne

Paul Marillonnet a écrit :

Benjamin Dauvergne a écrit :

On ne s'en sert pas, c'est du vieux code

(Est-ce qu'on aurait pas intérêt à créer un ticket de nettoyage de ce vieux code ?)

Je préfère qu'on réécrive chaque vue progressivement.

#11 - 04 juillet 2019 13:11 - Benjamin Dauvergne

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

```
commit 7be25fff6998b0db94c1d36e6454055bcc20dad8
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date: Tue May 14 16:56:14 2019 +0200
```

```
views: validates logout next URL (#33087)
```

#12 - 05 juillet 2019 01:15 - Frédéric Péters

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

Fichiers

0001-spring-cleaning-32934.patch	725 ko	14 mai 2019	Benjamin Dauvergne
0002-views-validates-logout-next-URL-33087.patch	2,43 ko	14 mai 2019	Benjamin Dauvergne
0001-views-validates-logout-next-URL-33087.patch	2,39 ko	02 juillet 2019	Benjamin Dauvergne