Combo - Development #33079

traces inutiles fuzzing dans /tracking-code/

14 mai 2019 12:11 - Thomas Noël

Statut:	Fermé	**Début:**	14 mai 2019
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

```
Unsafe redirect to URL with protocol 'file'

Report at /tracking-code/
Unsafe redirect to URL with protocol 'file'

Request Method: POST
Request URL: https://departement06.test.entrouvert.org/tracking-code/
Django Version: 1.11.20
Python Executable: /usr/bin/uwsgi-core
Python Version: 2.7.13
Python Path: ['.', '', '/usr/lib/python2.7', '/usr/lib/python2.7/plat-x86_64-linux-gnu', '/usr/lib
/python2.7/lib-tk', '/usr/lib/python2.7/lib-old',
'/usr/lib/python2.7/lib-dynload', '/usr/local/lib/python2.7/dist-packages', '/usr/lib/python2.7/di
st-packages']
Server time: mar, 14 Mai 2019 11:13:52 +0200
Installed Applications:
''
Installed Middleware:
''

Request information:
USER: ca829e61a2d94ee89a6c2b19148ccf

GET: No GET data

POST:
url = u'file://path/to/file'
cell = u'44'
code = u'{{8*8}}'
```

Demandes liées:

Lié à Hobo - Development #33620: ne pas logguer les "Unsafe redirect"	**Fermé**	**03 juin 2019**

Révisions associées

Révision 6439c43b - 03 juin 2019 12:30 - Frédéric Péters

wcs: raise a bad request when tracking code is missing from request (#33079)

Historique

#1 - 14 mai 2019 12:12 - Thomas Noël

- Sujet changé de trace inutile sur tentative d'url fake sur à trace inutile sur tentative d'url fake sur /tracking-code/ (suite à du fuzzing)

#2 - 14 mai 2019 12:20 - Thomas Noël

- Sujet changé de trace inutile sur tentative d'url fake sur /tracking-code/ (suite à du fuzzing) à traces inutiles fuzzing dans /tracking-code/

Dans la même série, POST sans code :

```
Internal Server Error: /tracking-code/

MultiValueDictKeyError at /tracking-code/
```

```
"'code'"

Request Method: POST
Request URL: https://departement06.test.entrouvert.org/tracking-code/
Django Version: 1.11.20
Python Executable: /usr/bin/uwsgi-core
Python Version: 2.7.13
Python Path: ['.', '', '/usr/lib/python2.7', '/usr/lib/python2.7/plat-x86_64-linux-gnu', '/usr/lib/python2.7/l
ib-tk', '/usr/lib/python2.7/lib-old', '/usr/lib/python2.7/lib-dynload', '/usr/local/lib/python2.7/dist-package
s', '/usr/lib/python2.7/dist-packages']
Server time: mar, 14 Mai 2019 11:57:15 +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/django/views/generic/base.py" in view
  68.             return self.dispatch(request, *args, **kwargs)

File "/usr/lib/python2.7/dist-packages/django/views/decorators/csrf.py" in wrapped_view
  58.         return view_func(*args, **kwargs)

File "/usr/lib/python2.7/dist-packages/combo/apps/wcs/views.py" in dispatch
  41.         return super(TrackingCodeView, self).dispatch(*args, **kwargs)

File "/usr/lib/python2.7/dist-packages/django/views/generic/base.py" in dispatch
  88.         return handler(request, *args, **kwargs)

File "/usr/lib/python2.7/dist-packages/combo/apps/wcs/views.py" in post
  63.         code = request.POST['code']

File "/usr/lib/python2.7/dist-packages/django/utils/datastructures.py" in __getitem__
  85.             raise MultiValueDictKeyError(repr(key))

Exception Type: MultiValueDictKeyError at /tracking-code/
Exception Value: "'code'"
Request information:
USER: AnonymousUser

GET: No GET data

POST:
cell = u'44'

FILES: No FILES data

COOKIES: No cookie data
```

#3 - 02 juin 2019 18:11 - Frédéric Péters

- Fichier 0001-wcs-raise-a-bad-request-when-tracking-code-is-missin.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#4 - 03 juin 2019 10:56 - Thomas Noël

Yep. J'ai mis un peu de temps à relire parce que le ticket au départ parlait d'une alerte à cause de « url = u'file://path/to/file' ». Mais en fait ton patch est tout bien qui gère le manque de "code", que j'indiquais dans la suite du ticket. Tu peux le pousser et on laisse le ticket ouvert, je vais regarder le cas de l'URL mal formattée.

#5 - 03 juin 2019 12:31 - Frédéric Péters

- Statut changé de Solution proposée à En cours

- Patch proposed changé de Oui à Non

Ah oui pas fait gaffe que la trace posée dans le commentaire n'était pas la même,

```
commit 6439c43b482c393320295aa5e0f59c4f317ecfd9
Author: Frédéric Péters <fpeters@entrouvert.com>
Date:   Sun Jun 2 18:11:10 2019 +0200

    wcs: raise a bad request when tracking code is missing from request (#33079)
```

#6 - 03 juin 2019 12:46 - Frédéric Péters

- Statut changé de En cours à Résolu (à déployer)

Pour la partie "unsafe redirect", plutôt hobo, j'ai créé #33620.

#7 - 03 juin 2019 12:46 - Frédéric Péters

- Lié à Development #33620: ne pas logguer les "Unsafe redirect" ajouté

#8 - 04 juin 2019 17:16 - Frédéric Péters

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

Fichiers

0001-wcs-raise-a-bad-request-when-tracking-code-is-missin.patch	1,79 ko	02 juin 2019	Frédéric Péters