Combo - Bug #24147

crash sur post d'un tracking code avec un id de cellule invalide

29 mai 2018 16:34 - Frédéric Péters

Statut:	Fermé	**Début:**	29 mai 2018
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	

Description

Ça n'arrive pas mais un outil d'intrusion fait ça et amène des traces,

```
  File "/usr/lib/python2.7/dist-packages/combo/apps/wcs/views.py", line 41, in post
    cell = TrackingCodeInputCell.objects.get(id=request.POST['cell'])
  File "/usr/lib/python2.7/dist-packages/django/db/models/manager.py", line 127, in manager_method
    return getattr(self.get_queryset(), name)(*args, **kwargs)
  File "/usr/lib/python2.7/dist-packages/django/db/models/query.py", line 325, in get
    clone = self.filter(*args, **kwargs)
  File "/usr/lib/python2.7/dist-packages/django/db/models/query.py", line 679, in filter
    return self._filter_or_exclude(False, *args, **kwargs)
  File "/usr/lib/python2.7/dist-packages/django/db/models/query.py", line 697, in _filter_or_exclu
de
    clone.query.add_q(Q(*args, **kwargs))
  File "/usr/lib/python2.7/dist-packages/django/db/models/sql/query.py", line 1310, in add_q
    clause, require_inner = self._add_q(where_part, self.used_aliases)
  File "/usr/lib/python2.7/dist-packages/django/db/models/sql/query.py", line 1338, in _add_q
    allow_joins=allow_joins, split_subq=split_subq,
  File "/usr/lib/python2.7/dist-packages/django/db/models/sql/query.py", line 1209, in build_filte
r
    condition = self.build_lookup(lookups, col, value)
  File "/usr/lib/python2.7/dist-packages/django/db/models/sql/query.py", line 1102, in build_looku
p
    return final_lookup(lhs, rhs)
  File "/usr/lib/python2.7/dist-packages/django/db/models/lookups.py", line 105, in __init__
    self.rhs = self.get_prep_lookup()
  File "/usr/lib/python2.7/dist-packages/django/db/models/lookups.py", line 143, in get_prep_looku
p
    return self.lhs.output_field.get_prep_lookup(self.lookup_name, self.rhs)
  File "/usr/lib/python2.7/dist-packages/django/db/models/fields/__init__.py", line 727, in get_pr
ep_lookup
    return self.get_prep_value(value)
  File "/usr/lib/python2.7/dist-packages/django/db/models/fields/__init__.py", line 985, in get_pr
ep_value
    return int(value)
ValueError: invalid literal for int() with base 10: ';import time;time.sleep(4000/1000);'
```

Révisions associées

Révision d245938e - 29 mai 2018 16:47 - Frédéric Péters

wcs: do not crash on POST with invalid cell identifiers (#24147)

Historique

#1 - 29 mai 2018 16:35 - Frédéric Péters

- Fichier 0001-wcs-do-not-crash-on-POST-with-invalid-cell-identifie.patch ajouté

- Statut changé de Nouveau à En cours

- Patch proposed changé de Non à Oui

#2 - 29 mai 2018 16:39 - Frédéric Péters

- Projet changé de Publik à Combo

#3 - 29 mai 2018 16:46 - Emmanuel Cazenave

ack

#4 - 29 mai 2018 16:47 - Frédéric Péters

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

```
commit d245938ecc28027df3aba217a66e254ee5637b63
Author: Frédéric Péters <fpeters@entrouvert.com>
Date:   Tue May 29 16:34:45 2018 +0200

    wcs: do not crash on POST with invalid cell identifiers (#24147)
```

#5 - 29 mai 2018 17:15 - Christophe Siraut

Ack.

#6 - 23 décembre 2018 15:10 - Frédéric Péters

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

Fichiers

0001-wcs-do-not-crash-on-POST-with-invalid-cell-identifie.patch	2,08 ko	29 mai 2018	Frédéric Péters