w.c.s. - Bug #10194

comportement quand le module feedparser (pour _sanitizeHTML) est absent

04 mars 2016 09:38 - Frédéric Péters

Statut:	Fermé	**Début:**	04 mars 2016
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:	v1.36		
Patch proposed:	Oui	**Planning:**	

Description

dans le WysiwygTextWidget on fait :

```
            if _sanitizeHTML:
                self.value = _sanitizeHTML(self.value, get_request().charset, 'text/html')
            else:
                self.value = str(htmlescape(self.value))
```

mais ça fait que le résultat si _sanitizeHTML est absent est trop quoté :

```
>>> print str(htmlescape('<p>hello</p>'))
&lt;p&gt;hello&lt;/p&gt;
```

C'était fait volontairement pour éviter qu'on puisse taper n'importe quoi comme HTML mais ce n'est pas terrible comme comportement; on pourrait ne pas afficher le ckeditor et considérer que l'html n'est pas géré dans ce cas, ou prendre la valeur comme elle vient.

Révisions associées

Révision b187f5b2 - 04 mars 2016 14:54 - Frédéric Péters

misc: don't escape html if _sanitizeHTML is absent (#10194)

Historique

#1 - 04 mars 2016 10:03 - Thomas Noël

> prendre la valeur comme elle vient.

y'a un risque ?

#2 - 04 mars 2016 10:07 - Frédéric Péters

> y'a un risque ?

Il doit y avoir moyen que d'ouvrir ou fermer trop de et que le résultat soit que le formulaire de login n'apparaisse pas. (on peut dire qu'il l'aura bien cherché)

#3 - 04 mars 2016 10:51 - Thomas Noël

Ok, pas de risque de sécurité (i.e. on n'utilise nulle part ça pour gérer du html saisi par un inconnu). Je dirais donc que oui, « prendre la valeur comme elle vient ».

#4 - 04 mars 2016 11:03 - Frédéric Péters

- Fichier 0001-misc-don-t-escape-html-if-_sanitizeHTML-is-absent-10.patch ajouté

- Statut changé de Nouveau à En cours

- Patch proposed changé de Non à Oui

#5 - 04 mars 2016 11:35 - Frédéric Péters

- Fichier 0001-misc-don-t-escape-html-if-_sanitizeHTML-is-absent-10.patch ajouté

Avec changement au test qui vérifiait qu'on échappait bien le texte…

#6 - 04 mars 2016 14:52 - Thomas Noël

Ack

#7 - 04 mars 2016 14:55 - Frédéric Péters

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

```
commit b187f5b23e2bcfa11e40e335eaed7e3c30509955
Author: Frédéric Péters <fpeters@entrouvert.com>
Date:   Fri Mar 4 11:02:25 2016 +0100

    misc: don't escape html if _sanitizeHTML is absent (#10194)
```

#8 - 04 mars 2016 18:05 - Thomas Noël

- Version cible mis à v1.36

#9 - 04 avril 2016 10:10 - Thomas Noël

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

0001-misc-don-t-escape-html-if-_sanitizeHTML-is-absent-10.patch	894 octets	04 mars 2016	Frédéric Péters
0001-misc-don-t-escape-html-if-_sanitizeHTML-is-absent-10.patch	1,72 ko	04 mars 2016	Frédéric Péters