w.c.s. - Bug #69958

Il n'est plus possible d'imprimer les fichiers attachés dans firefox depuis l'ajout d'un entête Content-Security-Policy

06 octobre 2022 15:55 - Benjamin Dauvergne

Statut:	Fermé	**Début:**	06 octobre 2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Cette modification suite au ticket #67872 empêche le chargement d'une image dans la boite de dialogue d'impression (pas de prévisualisation et impression vide) :

```
commit 69ab751d323fac6ee0db1b01956724767617c568
Author: Frédéric Péters <fpeters@entrouvert.com>
Date:   Tue Aug 2 11:09:43 2022 +0200

    misc: do not transform, and restrict, uploaded HTML files (#67872)

diff --git a/wcs/forms/common.py b/wcs/forms/common.py
index 9bb14cd3c..8e0bf2580 100644
--- a/wcs/forms/common.py
+++ b/wcs/forms/common.py
@@ -94,6 +94,11 @@ class FileDirectory(Directory):
             else:
                 raise errors.TraversalError()

+        # force potential HTML upload to be used as-is (not decorated with theme)
+        # and with minimal permissions
+        response.filter = {}
+        response.set_header('Content-Security-Policy', 'default-src \'none\';')
+
         if file.content_type:
             response.set_content_type(file.content_type)
         else:
```

J'imagine qu'un Content-Security-Policy: default-src 'self' ou bien 'https://la-meme-url/' marcherait peut-être...

Demandes liées:

Lié à w.c.s. - Bug #67872: traitement des fichiers HTML uploadés à travers un...	**Fermé**	**02 août 2022**

Révisions associées

Révision 2f7db76f - 11 octobre 2022 13:48 - Benjamin Dauvergne

misc: add img-src CSP to fix printing on Firefox (#69958)

On firefox the CSP is applied to the printing dialog box of the browser, if it's
too restrictive it cannot print an image file.

Historique

#2 - 06 octobre 2022 15:55 - Benjamin Dauvergne

- Lié à Bug #67872: traitement des fichiers HTML uploadés à travers un champ fichier ajouté

#3 - 06 octobre 2022 16:00 - Benjamin Dauvergne

Plutôt ajouter, img-src '<url de l'image>' ou alors img-src 'self'.

#4 - 06 octobre 2022 16:01 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#5 - 06 octobre 2022 16:04 - Benjamin Dauvergne

- Fichier 0001-mics-add-img-src-csp-to-attaches-files-to-permit-pri.patch ajouté

- Tracker changé de Bug à Development

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

Il faudrait vérifier que ça permet d'imprimer des PDF aussi...

#6 - 10 octobre 2022 09:48 - Frédéric Péters

- Statut changé de Solution proposée à En cours

> Il faudrait vérifier que ça permet d'imprimer des PDF aussi...

(en attente de cette vérification, alors ?)

#7 - 10 octobre 2022 13:09 - Frédéric Péters

En fait non, vraiment, pour les fichiers HTML téléchargés on voudrait appliquer la pire politique, pas même leur permettre d'image.

De ce que je lis ici là il y a Firefox qui se marche dessus et applique la politique d'un fichier téléchargé à la page qui l'intègre.

Il me semble y avoir davantage à comprendre.

#8 - 10 octobre 2022 14:36 - Benjamin Dauvergne

Ok j'ai ouvert un ticket sur bugzilla.

https://bugzilla.mozilla.org/show_bug.cgi?id=1794395

#9 - 10 octobre 2022 20:14 - Benjamin Dauvergne

Benjamin Dauvergne a écrit :

> Ok j'ai ouvert un ticket sur bugzilla.
>
> https://bugzilla.mozilla.org/show_bug.cgi?id=1794395

J'ai testé dans chrome, il n'y pas ce bug, en attendant les agents à Tours ne peuvent plus imprimer les pièces jointes (on peut faire passer ça pour une mesure écolo à la rigueur) :/

#10 - 10 octobre 2022 22:01 - Benjamin Dauvergne

- Assigné à Benjamin Dauvergne supprimé

#11 - 10 octobre 2022 22:54 - Frédéric Péters

De manière transitoire, la Content-Security-Policy pourrait être posée uniquement sur ce qui est text/html, voire à l'inverse explicitement pas posée sur les image/*.

#12 - 11 octobre 2022 03:05 - Benjamin Dauvergne

L'impression de PDF n'est pas bloquée par ce souci sous firefox.

~~J'ai relu le ticket #67872, et un truc qui n'est pas pris en compte c'est que pour tempfile il n'y pas de travail sur content-disposition alors que pour la vue des fichiers attachés il y en a un qui fait qu'il est quasiment impossible d'afficher un fichier HTML (mais on pourrait imaginer un fichier bien foutu qui trompe libmagic de notre coté mais qui soit reconnu comme un fichier HTML par le navigateur, qui sait) et qui rend le response.filter = {} assez inutile dans ce cas. Je verrai bien un content-disposition: attachment sur la vue tempfile, ça me parait plus logique.~~ PS: Et en fait ça n'arrive pas non plus parce que le widget d'upload met un <a download=...> en fait l'audit à la base de tout ça est complètement nul.

Dans tous les cas la CSP encore plus restrictive 'img-src %s;' % get_request().build_absolute_uri() permet l'impression et ne me semble pas permettra de charger une image dans un fichier HTML (à part lui même, mais je ne vois pas bien ce qu'on risque qu'on ne risque pas déjà en chargeant bêtement une image).

#13 - 11 octobre 2022 03:13 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#14 - 11 octobre 2022 03:13 - Benjamin Dauvergne

- Fichier 0001-misc-add-img-src-CSP-to-fix-printing-on-Firefox-6995.patch ajouté

- Statut changé de En cours à Solution proposée

#15 - 11 octobre 2022 12:29 - Frédéric Péters

- Tracker changé de Development à Bug

- Statut changé de Solution proposée à Solution validée

Il y a une suppression de ligne vide dans le premier chunk, tu peux la remettre avant de pousser ?

(je passe en qualification "bug" pour être explicite sur le fait que ça puisse être poussé pour ce cycle).

#16 - 11 octobre 2022 13:49 - Frédéric Péters

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

Je l'ai envoyé moi-même.

```
commit 2f7db76ffd197df03bb3bfac365084837e5e3819
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
Date:   Thu Oct 6 16:03:37 2022 +0200

    misc: add img-src CSP to fix printing on Firefox (#69958)

    On firefox the CSP is applied to the printing dialog box of the browser, if it's
    too restrictive it cannot print an image file.
```

#17 - 11 octobre 2022 16:14 - Transition automatique

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

#18 - 11 octobre 2022 17:20 - Benjamin Dauvergne

Benjamin Dauvergne a écrit :

> Ok j'ai ouvert un ticket sur bugzilla.
>
> https://bugzilla.mozilla.org/show_bug.cgi?id=1794395

Et quelqu'un a réagit mais me demande un lien pour reproduire le souci, https://bugzilla.mozilla.org/show_bug.cgi?id=1794395 ... sont chiants ces dév.

#19 - 11 décembre 2022 04:42 - Transition automatique

Automatic expiration

Fichiers

0001-mics-add-img-src-csp-to-attaches-files-to-permit-pri.patch	1,05 ko	06 octobre 2022	Benjamin Dauvergne
0001-misc-add-img-src-CSP-to-fix-printing-on-Firefox-6995.patch	1,96 ko	11 octobre 2022	Benjamin Dauvergne