

## banner.chapril.org - Demande #3134

### Forcer la bannière par text replace nginx

06/05/2018 19:05 - Quentin Gibeaux

<b>Statut:</b>	Fermé	<b>Début:</b>	06/05/2018
<b>Priorité:</b>	Normale	<b>Echéance:</b>	
<b>Assigné à:</b>	Christian P. Momon	<b>% réalisé:</b>	0%
<b>Catégorie:</b>		<b>Temps estimé:</b>	0.00 heure
<b>Version cible:</b>	Mise en production Chapril		

**Description**

Il est possible d'injecter une bannière chapril en réalisant un text replace sur la réponse reçue par bastion avec ce genre de configuration nginx dans un location / :

```
sub_filter '</body>' '<h1>Miaou !</h1></body>';
sub_filter_once on;
```

Cependant, cela n'est pas exécuté lorsque le contenu renvoyé semble zipé par le serveur http distant, il est possible de contourner ce problème via deux solutions :

- 1/ désactiver le module deflate sur le serveur http
- 2/ forcer un paramètre proxy\_set\_header Accept-Encoding "";

Cependant, cette seconde solution crée des problèmes sur un service comme date.chapril.org : tout les liens sont cassés et apparaissent comme "http://lamp..."

### Historique

#### #1 - 07/05/2018 01:09 - Christian P. Momon

Lors que je me connecte à listes.chapril.org :  
- je tombe sur la page <https://sympa.cluster.chapril.org/sympa/lists> :/  
- y a un miaou en bas à gauche.

#### #2 - 07/05/2018 11:35 - Quentin Gibeaux

Le nginx n'avait pas été reloadé

#### #3 - 07/05/2018 11:42 - Quentin Gibeaux

Pour info : <http://www.bortzmeyer.org/gzip-compression-apache.html>

#### #4 - 07/05/2018 14:52 - Christian P. Momon

Je confirme la résolution du problème suite au Nginx reload \o/

#### #5 - 08/05/2018 19:28 - Christian P. Momon

Actuellement, le code de la bannière est inclus depuis un fichier. J'approuve (centralisation...).

Ce fichier a pour nom « banniere-chapril ». Proposition d'appliquer un nommage uniquement en anglais par souci d'homogénéité et de cohérence. Suggestion de renommer en « chapril-banner ».

#### #6 - 09/05/2018 11:58 - Quentin Gibeaux

- Version cible mis à Mise en production Chapril

#### #7 - 09/05/2018 21:58 - Christian P. Momon

À propos du non chargement du CSS dans pouet.chapril.org, en regardant les logs réseaux (inspecteur Firefox) :

```
21:34:34,895 Content Security Policy: Les paramètres de la page ont empêché le chargement d'une ressource à
https://www.chapril.org/Banner/chapril-banner.css (« style-src https://paste.chapril.org »). 1 (source inconnue)
```

Du coup, recherche web : <https://www.bart-konieczny.com/fr/blog/securete-des-applications-web/explication-content-security-policy>

Et ça se confirme :

```
cpm@ocmstar (21:53:28) ~ 21 > curl -v https://pouet.chapril.org/about 2>&1 |grep -i security
< Content-Security-Policy: default-src 'none'; font-src 'self'; media-src 'self'; style-src 'self' 'unsafe-inline'; script-src 'self'; img-src 'self' data:;
connect-src 'self' wss://pouet.chapril.org; frame-ancestors 'none';
```

Hypothèses :

- 1) désactiver le CSP : oui, mais où ?
- 2) ajouter des location dans la conf nginx pour faire croire que les ressources sont locales.

#### #8 - 09/05/2018 22:12 - Christian P. Momon

Dans /etc/nginx/sites-enabled/pouet.chapril.org :

```
location / {
    add_header Referrer-Policy "strict-origin-when-cross-origin";
    add_header Content-Security-Policy "default-src 'none'; font-src 'self'; media-src 'self'; style-src 'self' 'unsafe-inline'; script-src 'self'; img-src 'self'
data:; connect-src 'self' wss://pouet.chapril.org; frame-ancestors 'none';";
    try_files $uri @proxy_static @proxy;
}
```

#### #9 - 09/05/2018 23:54 - Christian P. Momon

J'ai appliqué la solution n°2 (mettre les ressources en relatif) et ça semble bien fonctionner.

L'inconvénient est qu'il faut deux include par fichier de configuration (1 pour le location /Banner et un pour les filter), pas très joli.

#### #10 - 01/11/2018 11:36 - Christian P. Momon

- Statut changé de Nouveau à Résolu

Solution technique validée.

#### #11 - 01/11/2018 15:13 - Edouard Dausque

- Statut changé de Résolu à Fermé

#### #12 - 21/12/2019 03:11 - Christian P. Momon

- Projet changé de Chapril à banner.chapril.org

- Assigné à mis à Christian P. Momon