Admins - Demande #1752

Implémenter HTTP Strict Transport Security sur april.org

16/06/2016 14:54 - Benjamin Drieu

Statut:	Fermé	**Début:**	16/06/2016
Priorité:	Normale	**Echéance:**	
Assigné à:	Benjamin Drieu	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Backlog	**Temps passé:**	1.00 heure
Difficulté:	3 Moyen		

Description

Voir : https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

D'abord, réfléchir aux implications : quel contenu ne doit pas être servi en HTTPS ?

Commencer par tester un max-age bas pour éviter les problèmes.

Demandes liées:

Lié à Admins - Anomalie #1686: Problèmes SSL TLS sur www.april.org	**Fermé**	**13/03/2016**
Dupliqué par Admins - Demande #1857: Cas du formulaire de login de la page ht...	**Fermé**	**08/02/2017**

Historique

#1 - 20/10/2016 16:02 - François Poulain

Perso ça me semble dangereux si les applications ne sont pas conçues pour. Amha le choix du HSTS doit autant sinon plus relever du concepteur de l'application car c'est lui le seul qui est capable d'attester que c'est conçu pour fonctionner avec.

Par ex. Médiawiki chie ici : #1350 Le site ne serait il pas HS avec HSTS ?

#2 - 23/10/2016 02:27 - Christian P. Momon

Je suis à fond pour le HTTPS-Only Standard qui prône de n'utiliser que du HTTPS pour toutes les pages de tous les sites.

Voir : https://https.cio.gov/

Si un produit bug avec ça, est-ce un bon produit ? Quoiqu'il en soit, le cas par car semble inévitable et même souhaitable.

Question : plutôt que de faire HTTP STS, pourquoi ne pas faire une redirection du flux 80 vers 443 (redirect 301 ou 308) alors à quoi sert HTTP STS ?

Pour information, le redirect est super simple :

https://httpd.apache.org/docs/current/mod/mod_alias.html#redirect

```
<VirtualHost *:80>
        ServerName xxxx ou ServierAlias * ou autre
        Redirect / https://kiwa.devinsy.fr/
</VirtualHost>
```

#3 - 23/10/2016 14:44 - François Poulain

Hum, pour info, tu peux translater toute l'url, pas ne renvoyer qu'à la racine.

#4 - 19/12/2016 17:33 - Christian P. Momon

François Poulain a écrit :

> Hum, pour info, tu peux translater toute l'url, pas ne renvoyer qu'à la racine.

Me semble que l'instruction ci-dessus s'occupe de bien reprendre la partie droite de l'URL :)

#5 - 19/12/2016 17:36 - Christian P. Momon

Aeris souffle sur IRC que le HSTS est mieux que la simple redirection car réduit le risque de mitm.

Ça laisse une possibilité de mitm mais il faut reconnaître que ça la réduit.

Même couper le port 80 laisse une possibilité de mitm.

Possibilité de pré-charger le site en mode HTST : https://hstspreload.org/ . Dans ce cas le mitm semble impossible. Mais bon, ça fait dépendre d'un fichier dont on ne sait pas grand chose de la gestion…

#6 - 19/12/2016 17:45 - François Poulain

> Me semble que l'instruction ci-dessus s'occupe de bien reprendre la partie droite de l'URL :)

Anéfé. La magie apache... ;)

#7 - 19/12/2016 21:39 - Edouard Dausque

Benjamin Drieu a écrit :

> Commencer par tester un max-age bas pour éviter les problèmes.

Et commencer par ne pas mettre la directive includeSubDomains
https://tools.ietf.org/html/rfc6797#section-6.1.2

#8 - 01/02/2017 22:54 - François Poulain

Perso je pense que c'est une erreur tant que ce sera le drupal actuel aux manettes. Cf bug #1686.

#9 - 29/01/2018 21:51 - Frédéric Couchet

- Version cible changé de Sprint Juin 2016 à Backlog

#10 - 06/03/2018 11:19 - Benjamin Drieu

- Statut changé de Nouveau à Résolu

- % réalisé changé de 0 à 100

HSTS a été implémenté sur april.org via NGINX. Le fichier /etc/nginx/hsts.conf doit être inclus par tout virtualhost qui désire forcer l'HSTS.

Par exemple:

```
server {
    listen 443;
    ssl on;

    server_name www.april.org april.org dev.april.org;

    [...]

    include /etc/nginx/hsts.conf;

    [...]
}
```

Pour faciliter la tâche, le fichier /etc/nginx/force-ssl.conf force un site en HTTP à passer en HTTPS et doit être inclus dans la version pur HTTP du virtualhost.

#11 - 06/03/2018 11:20 - Benjamin Drieu

- Dupliqué par Demande #1857: Cas du formulaire de login de la page http://www.april.org ajouté

#12 - 06/03/2018 11:21 - Benjamin Drieu

- Lié à Anomalie #1686: Problèmes SSL TLS sur www.april.org ajouté

#13 - 29/05/2019 12:21 - Quentin Gibeaux

- Statut changé de Résolu à Fermé

#14 - 26/12/2020 02:57 - Christian P. Momon

- Assigné à mis à Benjamin Drieu