Admins - Demande #1857

Cas du formulaire de login de la page http://www.april.org

08/02/2017 12:57 - Vincent-Xavier JUMEL

Statut:	Fermé	**Début:**	08/02/2017
Priorité:	Élevée	**Echéance:**	
Assigné à:	Benjamin Drieu	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Février 2018	**Temps passé:**	0.00 heure
Difficulté:	2 Facile		

Description

Visiblement https://agir.april.org/issues/1030#note-1 n'a pas été traité et c'est assez fâcheux en terme de sécurité. Maintenant qu'on a des vrais certificats est-ce qu'on ne pourrait pas tout simplement forcer le https:// sur april.org. C'est d'ailleurs ce que ne vont pas tarder à recommander FF et Chromium.

Demandes liées:

Duplique Admins - Demande #1752: Implémenter HTTP Strict Transport Security s...	**Fermé**	**16/06/2016**

Historique

#1 - 08/02/2017 13:06 - François Poulain

Voir https://agir.april.org/issues/1686

Solution: patcher drupal ou changer pour autre chose.

#2 - 08/02/2017 13:34 - Vincent-Xavier JUMEL

Mais tout mettre en https ne résout pas le souci ?

#3 - 08/02/2017 14:38 - François Poulain

Si. Mais perso ça me chagrine que des infos publiques ne soient pas accessibles en clair et nécessitent des tonnes de calculs pour être lisibles.

#4 - 08/02/2017 14:51 - Edouard Dausque

Dans ce cas enlever le formulaire de login et le remplacer par un lien ?

#5 - 08/02/2017 15:09 - Vincent-Xavier JUMEL

François Poulain a écrit :

> Si. Mais perso ça me chagrine que des infos publiques ne soient pas accessibles en clair et nécessitent des tonnes de calculs pour être lisibles.

Sauf qu'on ne sait pas tellement gérer ça autrement pour l'instant. Et personnellement, ça ne me chagrine pas plus que ça, d'autant plus que ça authentifie la source.

#6 - 08/02/2017 19:29 - Quentin CHERGUI

Les temps de calcul pour TLS sont négligeables sur une machine moderne avec le trafic que l'on a.

Et si les cookies de sessions passent en clair ensuite, ça annule en partie l'intérêt de faire du TLS.

Ça ne bloque aucun visiteur de le faire sur la partie publique. Et ça complique la vie à quelqu'un qui veut voir exactement quelles pages un utilisateur a vu (bien que ce soit un risque assez négligeable sur le site de l'April).

Enfin ça préserve des saloperies style proxys transparents qui "optimisent" les pages dont les opérateurs mobiles sont (étaient ?) friands.

En l'état, j'ai du mal à voir quels avantages ça aurait de ne pas le faire.

#7 - 31/01/2018 21:58 - Benjamin Drieu

- Statut changé de Nouveau à Confirmé

- Assigné à mis à Benjamin Drieu

- Priorité changé de Normale à Élevée

- Version cible changé de Backlog à Février 2018

#8 - 06/03/2018 11:20 - Benjamin Drieu

- Duplique Demande #1752: Implémenter HTTP Strict Transport Security sur april.org ajouté

#9 - 06/03/2018 11:21 - Benjamin Drieu

- Statut changé de Confirmé à Résolu

#10 - 07/03/2018 21:16 - Quentin Gibeaux

- Statut changé de Résolu à Fermé