

Admins - Demande #4474

Renforcer le cloisonnement des applications web sur la vm lamp

09/05/2020 22:42 - Christian P. Momon

Statut:	Fermé	Début:	09/05/2020
Priorité:	Normale	Echéance:	
Assigné à:	Christian P. Momon	% réalisé:	100%
Catégorie:		Temps estimé:	0.00 heure
Version cible:	Mai 2020	Temps passé:	0.00 heure
Difficulté:	2 Facile		
Description			
<p>Lorsque plusieurs applications webs sont hébergées sur la même machine, une précaution élémentaire consiste à interdire au code PHP d'une application d'aller lire ou écrire dans le dossier d'une autre application.</p> <p>Dans Apache, cela passe par le positionnement d'une ligne :</p>			
<pre>php_admin_value open_basedir "/le/chemin/d'ou/ne/pas/sortir"</pre>			
Actuellement :			
<pre>(April) root@lamp:/etc/apache2/sites-enabled[master\$]# grep open_basedir * wc -l 0</pre>			
Demande : ajouter une directive open_basedir dans la conf de toutes les applications PHP sur la vm lamp.			
<pre>000-default.conf [/] site statique apr1.org.conf [X] PHP april-food-inc.april.org.conf [X] site statique audio.april.org.conf [X] site statique boutique.april.org.conf [#] inactif candidats.be.conf [X] site statique corp.april.org.conf [X] site statique diversite.april.org.conf [X] PHP eucd.info.conf [X] PHP expolibre.org.conf [X] PHP formatsouverts.education.conf [X] PHP gspeakup.april.org.conf [X] site statique guide.libreassociation.info.conf [X] site statique (+ 1 page php) libreassociation.info.conf [X] PHP libre-en-fete.net.conf [X] PHP libre-et-accessible.org.conf [X] PHP logiciel-libre.info.conf [X] site statique media.april.org.conf [X] site statique piwik.april.org.conf [X] PHP planet.april.org.conf [X] ~PHP proximite.april.org.conf [X] PHP questionnaires.april.org.conf [X] PHP questionnaires.libreassociation.info.conf [X] PHP spip.libre-en-fete.net.conf [X] PHP statistiques.april.org.conf [X] PHP unitary-patent.april.org.conf [X] site statique v2.expolibre.org.conf [X] ~PHP valise.april.org.conf [-] ancien site valise-new.april.org.conf [X] PHP webmail.april.org.conf [-] /var/lib web site wiki.april.org.conf [-] /var/lib web site www.april.org.conf [X] PHP www.librealire.org.conf [X] redirection</pre>			
Demandes liées:			
Lié à Admins - Demande #3721: Remettre l'application photos.april.org dans la...		Fermé	30/05/2019

Historique

#1 - 09/05/2020 22:50 - Christian P. Momon

- Description mis à jour
- Statut changé de Nouveau à En cours de traitement
- Assigné à mis à Christian P. Momon

Début de la revue systématique.

#2 - 10/05/2020 02:10 - Christian P. Momon

- Description mis à jour
- Statut changé de En cours de traitement à Résolu

Fait.

#3 - 10/05/2020 02:11 - Christian P. Momon

- Lié à Demande #3721: Remettre l'application photos.april.org dans la vm lamp ajouté

#4 - 10/05/2020 09:55 - François Poulain

Merci pour tout ça.

Au fait par rapport à une question posée il y a longtemps, c'est aussi un des intérêts de fpm : on peut avoir une isolation plus forte : 1 id par application (apache ne permet plus ça que je sache), voire éventuellement 1 service par application (systemd permettant d'encadrer les capability et les chemins accessibles). Le open_basedir est mieux que rien mais possède des contournements connus et efficacement documentés.

#5 - 11/05/2020 01:12 - Christian P. Momon

- Sujet changé de Renforcer le cloisonnement des applications web sur la vm lamp à Renforcer le cloisonnement des applications web sur la vm lamp

#6 - 12/05/2020 00:09 - Christian P. Momon

- % réalisé changé de 0 à 100

#7 - 27/05/2020 21:54 - Quentin Gibeaux

- Statut changé de Résolu à Fermé

#8 - 22/08/2020 11:48 - François Poulain

Pour info le openbasedir casse nextcloud. Heureusement il ne devait pas fonctionner. :)

#9 - 22/08/2020 12:43 - Christian P. Momon

Puisque la valise était en fpm, la directive open_basedir devait être inopérante. Suite à [#4034](#), merci d'avoir corrigé :D <3