Infra Chapril - Demande #3145

Faut-il renforcer l'isolation des applications PHP sur la VM lamp ?

10/05/2018 09:02 - Christian P. Momon

Statut:	Nouveau	**Début:**	10/05/2018
Priorité:	Normale	**Echéance:**	
Assigné à:	pitchum .	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Backlog		

Description

Actuellement, sur la VM lamp, il n'y a pas de restriction d'accès entre application PHP installée.
C'est à dire que le code PHP d'une application peut accéder aux fichiers d'une autre application, et même de tout le système.
Exemple : https://date.chapril.org/test.php (qui accède à un fichier dans paste.chapril.org).

D'expérience, il est d'usage d'utiliser la directive **open_basedir** pour augmenter la sécurité :
http://php.net/manual/fr/ini.core.php#ini.open-basedir

De son côté, Didier remonte que la procédure d'installation de paste.chapril.org cite PHP-FPM : https://php-fpm.org/

Pour information : https://paste.chapril.org/phpinfo.php

Question : quel niveau d'isolation voulons-nous ?
1) par défaut : on a confiance dans le code et ce n'est pas grave ;
2) open_basedir : c'est le minimum chez les professionnels ;
3) php-fpm : le maximum est le mieux.

Je suis d'avis d'appliquer open_basedir.

Votre avis ?

Historique

#1 - 10/05/2018 12:06 - Edouard Dausque

4) une machine virtuelle par projet

#2 - 13/05/2018 18:46 - Didier Clermonté

open_basedir actif pour date et paste

#3 - 29/05/2018 15:04 - Denis Dordoigne

Voici ce que je vois habituellement chez mes clients :
- aucune isolation particulière en général
- pour les services accédant à des données sensibles (données personnelles, données de santé, etc.), une machine séparée par service

Chez infini on héberge tous les services de type frama sur les mêmes machines sans isolation particulière, mais on pourrait probablement faire mieux.

#4 - 06/08/2018 16:06 - François Poulain

Je partage l'avis de Edouard.On peut mettre un gloubi boulga de php sur lamp là où ce n'est pas critique, mais les applications qui présentent de la criticité doivent être isolées.

#5 - 21/12/2019 03:02 - Christian P. Momon

- Projet changé de Chapril à Infra Chapril

#6 - 01/04/2020 20:15 - Christian P. Momon

- Version cible mis à Backlog

#7 - 28/02/2021 10:12 - pitchum .

Personnellement je déploie mes applis PHP de la même façon partout :

- un compte unix dédié
- une config php-fpm dédiée
- un compte MySQL ou postgreSQL dédié

Il me semble que ça suffit pour isoler les applis les unes des autres même si elles tournent sur la même VM.

Par exemple, j'ai documenté comment j'ai procédé pour déployer Movim chez Parinux : https://wiki.parinux.org/si/movim#installation

#8 - 07/06/2022 22:54 - pitchum .

- Assigné à mis à pitchum .