14

Conseils pour utiliser Joomla ! en toute sécurité

Joomla!®

CENTRE DE RECHERCHE
SUR L'INFORMATION
SCIENTIFIQUE ET TECHNIQUE

cerist

CONSEILS POUR UTILISER JOOMLA ! EN TOUTE SÉCURITÉ

Un bon contrôle de sécurité est le meilleur moyen de renforcer efficacement la sécurité d'un site web. Joomla !, est un CMS Open Source, qui compte une communauté algérienne assez importante et de nombreux sites .DZ sont réalisés avec ce dernier. Cette rubrique contient une liste de conseils, qui vous permettront de faire un tour d'horizon sur ce qu'il est possible de faire afin d'optimiser la sécurité de son site Joomla! à lire donc et à appliquer bien sur pour une meilleure protection.

1. Téléchargez Joomla! du site officiel

Ne téléchargez jamais Joomla! à partir de sites non officiels, utilisez plutôt les fichiers d'installation téléchargés des sites JoomHYPERLINK **« http://www.joomla.fr/» «http://www.joomla.fr/» a.fr et Joomla.org.**

2. Installez la dernière version

Démarrez sur une base saine en installant la dernière version stable de **« http://www.joomla.org/download.html » Joomla « http://www.joomla.org/download.html »** ! à télécharger comme mentionné précédemment depuis le site officiel.

Pourquoi ? En n'utilisant pas la dernière version stable de Joomla! Votre site est une cible potentielle pour les pirates exploitant des failles de sécurité connues de la version antérieure.

3. Mettez Joomla! régulièrement à jour

La mise à jour régulière du CMS Joomla! est indispensable pour la sécurité du site. L'équipe Joomla! fournit régulièrement des mises à jour qui comprennent des correctifs de sécurité, mises à jour des composants, modules et plug-ins. Il est donc fortement recommandé d'installer la dernière version mais la tenir à jour. Aussi, il est conseillé de mettre à jour les extensions tierces également. De plus, depuis sa version 2.5, la mise à jour du CMS et ses extensions

compatibles se fait en un simple clic. Avant de faire une mise à jour, pensez à faire une sauvegarde.

4. Sauvegarde, Sauvegarde, Sauvegarde (Effectuez des backups réguliers)

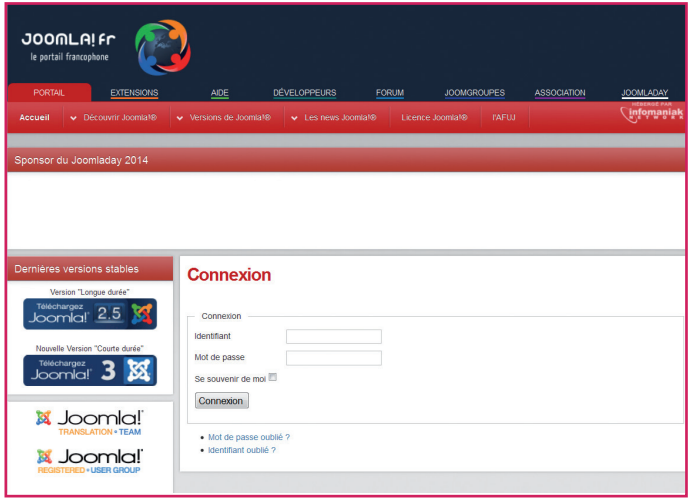
« Mieux vaut prévenir que guérir ! », il est important d'effectuer des backups réguliers : du site et de la base de données. Pensez également à tester les backups que vous planifiez, et stockez-les en lieu sûr. Même si votre site est attaqué, si vous faites des sauvegardes régulières de votre site vous pourrez, dans la grande majorité des cas, le restaurer.

D'une manière générale, vous devez sauvegarder régulièrement votre site. Vous devez le sauvegarder avant et après avoir installé, désinstallé ou mis à jour une extension ou avant et après avoir fait la mise à jour de Joomla! lui-même. Vous devez faire une sauvegarde après avoir créé du contenu. Vous devez faire une sauvegarde avant et après avoir apporté des modifications et surtout, vous devez faire une sauvegarde avant de faire toute intervention dont vous n'êtes pas certain du résultat.

5. Personnalisez le Login et Le Mot de passe

Pendant l'installation de Joomla!, l'identifiant admin est attribué par défaut à l'administrateur du site. La totalité des attaquants et les robots cracker attendent à ce que le nom d'utilisateur de l'administrateur est admin, avec cela la conséquence est qu'un pirate possède déjà une des deux clés pour accéder à votre back office. Il est recommandé de le modifier par un autre identifiant pour vous garantir plus de sécurité.

Pour le mot de passe, il faut choisir des mots de passe solides. Evitez tous les mots simples, votre nom, votre prénom, votre date de naissance, utiliser plutôt des chiffres, caractères spéciaux et lettres en majuscule/minuscule....



6. Protégez le répertoire /administrator

D'origine, Joomla! utilise le répertoire « /administrator » situé à sa racine comme dossier d'administration. Dès lors, il n'est plus un secret pour personne que la page de connexion au back office se situe à l'adresse suivante : http://www.monsite.dz/administrator. Plusieurs solutions s'offrent à vous pour protéger cette page un peu plus convenablement :

- Une protection par IP via .htacess
- Une protection par mot de passe via .htpasswd
- De nombreux plugins et autres solutions tierces pour Joomla! permettent notamment
- de renommer ce dossier, ou d'y ajouter une clé spécifique…

7. Modifiez le préfixe des tables

L'une des recommandations officielles Joomla!, est la modification du préfixe par défaut des tables de votre base de données, pendant l'installation du CMS, il vous propose « jos_ » comme préfixe par défaut, n'hésitez pas à le modifier et utiliser un préfixe de votre choix. En conservant le préfixe « jos_ » connu de tous, vous facilitez l'accès aux pirates désireux d'exploiter les données de votre base.

8. Utilisez des extensions utiles pour la sécurité

Installer un Plugin pour renforcer la sécurité de votre site Joomla! à différents niveaux. Exemple: sentinelle, AdminTools et jSecure Authentication, Akeeba, JMonitoring …

9. Installer des extensions de confiance

Joomla! permet d'étendre ses fonctionnalités à travers des extensions développées par des développeurs tiers dont une partie ne se soucie pas beaucoup de la sécurité, prenez l'habitude de télécharger les extensions à partir du site officiel.
Vous ne devez installer sur votre site que les extensions utiles à son fonctionnement. Beaucoup de débutants installent des extensions pour les tester. Avant d'installer une extension sur votre site, assurez-vous qu'elle sera utile, qu'elle réponde à vos besoins, et installez-la sur un site de tests au préalable afin de l'essayer. Si vous avez sur votre site des extensions inutiles, désinstallez-les.
Savez-vous que chaque extension installée sur un CMS (Joomla! et autres) peut nuire à la sécurité de votre site ? Car chacune d'elle demande de la maintenance donc elle augmente le risque de faille, ainsi chaque extension non à jour est une porte d'entrée pour les attaquants. Vous pouvez également consulter la « Vulnerable Extensions List » qui référence toutes les extensions Joomla! vulnérables.

10. Respectez les permissions des fichiers et répertoires

Vous avez parfois besoin de modifier les fichiers et dossiers de votre site Joomla!, avant de toucher à ces droits, soyez certain de ce que vous faites et/ou demandez conseil à votre hébergeur. Limitez les permissions sur les fichiers et les répertoires, appliquez le principe des « Moindres privilèges ». Pour une question simple de sécurité, ces droits ne doivent JAMAIS être en 777 car un fichier avec permission 777 est lisible, modifiable et exécutable par tous (sauf sur recommandation spéciale de votre hébergeur). Généralement, ils doivent être en 755/705 pour les dossiers et 604/644 pour les fichiers.

11. Supprimez les fichiers et dossiers non utilisés

Après chaque installation de Joomla!, supprimer le dossier d'installation et ne vous contentez pas de le renommer, supprimez également tous les fichiers non utilisés de votre template.

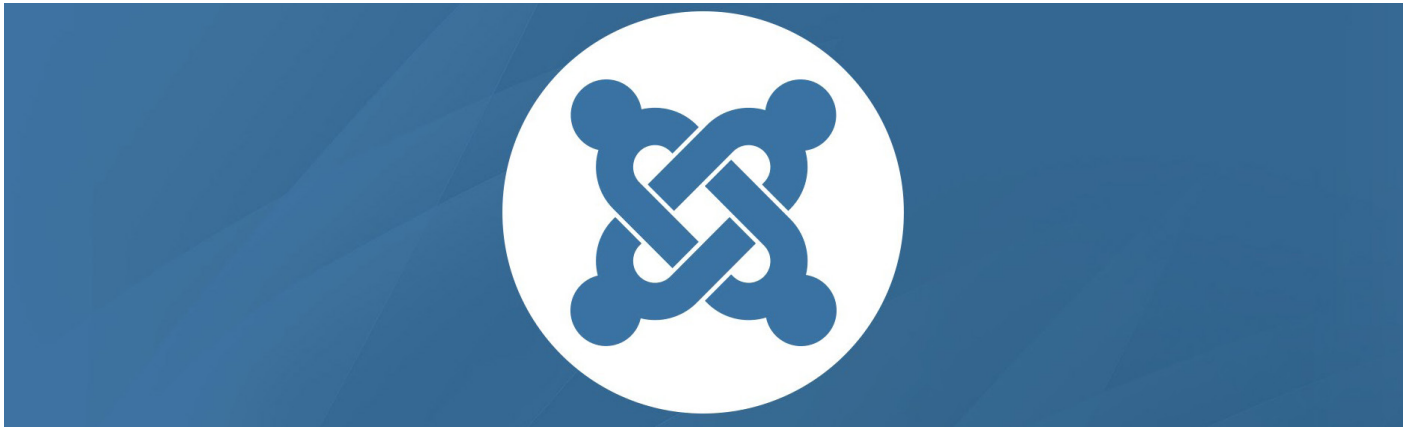
12. Utilisez le fichier Htaccess (Bloquez l'accès à tous les fichiers sauf index.php et index2.php)
Si vous n'avez pas un fichier htaccess, dans votre dossier Joomla!, vous devez renommer le fichier htaccess.txt fourni avec votre package d'installation Joomla! en .Htaccess.

13. Choisissez autant que possible le SSH (ou SFTP) au lieu du FTP.

14. Ne copiez-collez pas de texte provenant d'ailleurs dans vos articles sans nettoyer le code

15. Limitez autant que possible l'utilisation des iFrames (qui sont des portes ouvrant une page externe dans votre site)

16. Assurez-vous que vous exécutez votre site internet sur PHP 5.2 ou une version plus récente
Même si vous respectez à la lettre toutes ces règles, vous devez garder en tête que le risque 0 n'existe pas. Il y a toujours une chance, aussi infime qu'elle soit que vous vous fassiez hacker. Dans ce cas, vous aurez fait la majorité du travail surtout si vous respectez la règle des sauvegardes régulières. Ces



conseils représentent une ébauche concernant la sécurité d'un site propulsé sous Joomla! Pour apprendre plus il faut consulter la documentation **« http://docs.joomla.org/Category:Security_Checklist » « http://docs. joomla.org / Category:Security_Checklist » « http://docs.joomla.org/Category:Security_Checklist » « http://docs.joomla.org / Category : Security_Checklist » ! « http://docs.joomla.org/Category:Security_Checklist » sur « http://docs.joomla.org/Category : Security_Checklist » la sécurité.**