

Guide de sécurité pour Xoops

Catégorie : Sécurité et pirates

Publié par Fooups le 15/03/2005

Avant tout, vous devez garder à l'esprit qu'il n'existe pas de système sécurisé à 100%. Tout est relatif. Maintenant que c'est dit, il existe certaines choses que vous pouvez faire pour améliorer la sécurité de votre système. Ce guide résume les différentes étapes pour sécuriser votre site à partir d'astuces issues des forums officiels de Xoops.org et du site Xoops-tips.com. La plupart de ces astuces ont déjà été listées sur Xoops-tips, mais pas de façon structurée. Nous espérons (le traducteur aussi) que la présentation structurée de toutes ces astuces, anciennes et nouvelles, apporteront une meilleure compréhension des problèmes de sécurité. Choisir un hébergement Beaucoup d'entre nous ont tendance à diminuer l'importance d'un bon hébergeur et vont là où l'offre est la plus alléchante avec les coûts minimums. Vous devriez avoir une véritable réflexion au moment de choisir une solution d'hébergement. Un bon hébergeur avec une bonne réputation signifie en général une bonne sécurité. Comme la plupart d'entre nous n'avons pas de budget suffisant pour s'offrir un serveur dédié, vous devriez apporter une attention particulière à la sécurité du serveur en entier et des autres sites hébergés. La sécurité des autres sites end du serveur sont aussi important que la sécurité de votre propre site. Peu importe le niveau de sécurité de votre site, si le serveur a subi une attaque via d'autres sites placés sur le même serveur, tous vos efforts pourraient s'avérer inutiles en fin de compte. Les hébergeurs solitaires, revendeurs et petites compagnies devraient en général être évités si vous le pouvez, le plus souvent ils n'ont pas les ressources suffisantes ou les compétences nécessaires pour gérer les serveurs. Comme l'hébergement de sites Internet s'est considérablement développé, le coût d'hébergement n'est plus aussi cher qu'avant. Un bon hébergement vaut largement le surcoût engendré. La face cachée des hébergements ces temps-ci, vous pouvez louer un serveur à un "grossiste" comme n'importe qui pour 200\$ ou moins et devenir revendeur à votre tour. Tant que le revendeur paye ses factures, le grossiste ne s'inquiétera pas de la sécurité du serveur. Quand vous choisissez un revendeur, posez-vous cette question : « Est-ce que l'hébergeur a les compétences pour gérer des serveurs ? » Si votre hébergeur est situé au Royaume-Uni, mais que ses serveurs sont situés au Texas, qu'arriverait-il si votre serveur était hors d'usage ? Vous devriez appeler votre hébergeur, et votre hébergeur devrait appeler le sien pour régler le problème. Espérons que vous aurez une idée. Au moment de choisir un hébergeur, gardez à l'esprit, "Ce que vous payez, c'est ce que vous aurez". Si votre site est important pour vous, ne le mettez pas sur un hébergement à 2\$ par mois. Installation - Choisir le préfixe de la table Pendant le processus d'installation, vous devez choisir un préfixe difficilement identifiable. N'utilisez pas le préfixe par défaut "xoops". Il est trop facile à deviner pour les hackers. Si vous avez installé votre site avec le préfixe « xoops », vous pouvez utiliser le module Protector développé par GIJOE pour le changer. Après l'installation Une fois votre Xoops installé avec succès, n'oubliez pas d'effacer le répertoire "install" et de paramétrer les droits du fichier mainfile.php (chmod 444 ndt). Laisser son répertoire "install" en place et son mainfile.php sans protection, c'est inviter les autres à réinstaller un site Xoops et à prendre le contrôle de votre site. S'il leur prenait l'envie de faire des choses illégales avec, vous seriez responsable des dommages causés.

Installer le module Xoops Protector Une fois l'installation terminée, le premier module que vous

devriez installer est Xoops Protector de GIJOE. Si vous êtes sérieux sur la sécurité de votre site, vous devez installer ce module. Le système Xoops est peut-être le plus sécurisé des CMS. Néanmoins, le noyau ("Core") a ses faiblesses qui pourraient laisser passer des hackers. Cela a été démontré par GIJOE, de loin le meilleur contributeur concernant la sécurité de Xoops. Xoops 2.0.10 intègrera certaines des idées de GIJOE. Mais le module protector est toujours très largement recommandé car il défend à la fois contre des attaques contre le noyau central et les modules. Le module protector peut protéger de différents types d'attaques comme : Déni de Service (DoS); bad crawlers (NdT: robots collectant les adresses email, en vue du spam notamment); injection SQL; Cross-Site Scripting (XSS) (NdT: exploitation de la confiance de l'utilisateur envers un site - utilisateur = victime); system global pollution; session hi-jacking (NdT: renifler le réseau et exploiter des faiblesses de TCP - Protocole de Contrôle des Transmissions, à la base d'Internet dans le couple TCP/IP); null-bytes; mauvaise spécification des chemins de fichier; Cross-Site Request Forgeries (CSRF) (NdT: exploitation de la confiance d'un site envers ses utilisateurs - utilisateur = complice sans le savoir) (ce qui est fatal dans XOOOPS Pour plus d'information, allez sur le site de GIJOE (anglais, ndt): <http://www.peak.ne.jp/xoops/> Déplacer les Username (NOM) et Password (MOT DE PASSE) hors du fichier mainfile.php Une considération supplémentaire au sujet de votre installation de Xoops est de sortir du fichier mainfile.php vos identifiants d'accès à la base de données. Il est toujours plus sûr de conserver les informations sensibles loin dans votre arborescence. Ceci empêchera la révéléation accidentelle de vos données sensibles en cas de dysfonctionnement du serveur comme un arrêt de PHP. Dans ce cas, l'information contenue dans le mainfile.php peut être lue par n'importe qui dans le monde. Pour les détails (anglais, à traduire prochainement) <http://xoops-tips.com/news-article.storyid-1.htm> Protéger le fichier admin.php et le module "system" Xoopsadmin.php est accessible par n'importe qui ce qui pose un problème de sécurité si des hackers souhaitent faire le tour de vos systèmes. Il existe un moyen de se protéger. (en anglais, traduction en cours)

<http://xoops-tips.com/news-article.storyid-9.htm>

Protéger le répertoire Theme Vous pouvez protéger les fichiers de vos thèmes des curieux. Détails ci-dessous (anglais, traduction en cours) : <http://xoops-tips.com/news-article.storyid-25.htm> Désactiver la liste des répertoires (disable directory listing) Si votre hébergeur vous autorise à désactiver la liste des répertoires, mettez le à ON. Si votre hébergeur ne vous permet pas de telle manipulation, créez un fichier index.html avec le contenu suivant : `script>history.go(-1);` Chargez-le dans tous les répertoires de votre site Xoops (SAUF A LA RACINE ou DANS les répertoires de vos modules). La version de base de Xoops stock fournit ce fichier index.html dans la majorité des répertoires. Assurez-vous que chaque répertoire en dispose. Protéger l'adresse Email de l'administration Vous ne devriez jamais, en aucun cas, révéler l'adresse d'administration de Xoops en dehors de vos membres. Si vous utilisez le module Xoopsheadline, merci de lire cette astuce pour la cacher : (en anglais, en cours de traduction)

<http://xoops-tips.com/news-article.storyid-51.htm> Les modules tiers (non livrés avec le pack xoops.org, ndt) Faites particulièrement attention aux modules tiers. Il peut exister des failles de sécurité que les développeurs n'ont pas détectées. Si vous utilisez un module tiers, assurez-vous de bien vérifier les mises à jour et les fixes de sécurité, et vérifiez régulièrement les forums Xoops. Le module Xoops protector offre une protection, mais il est toujours possible que ce ne soit pas suffisant contre d'importante faille de sécurité. Sauvegardez votre site et son contenu La sauvegarde devrez être considérée comme l'un des aspects le plus important de protection et de sécurité de votre site. Des sauvegardes régulières et le téléchargement complet du site devraient être une routine. Si votre contenu change quotidiennement, vous devriez sauvegarder quotidiennement votre base de données. S'il ne change pas aussi fréquemment, alors une sauvegarde hebdomadaire peut être une solution. De la même façon, pour les fichiers du site, une sauvegarde mensuelle devrait être suffisante. Ou

faites une sauvegarde ad hoc à chaque modification majeure de votre site. Equilibre entre attirer le chaland et sécurité Certains Xoopsers sont tentés d'ouvrir leur site à tous, hackers inclus, dans le but d'attirer des membres sur leur site. Notre conseil est "SURTOUT PAS !!!!!" Les membres resteront avec vous aussi longtemps que vous offrirez un contenu ou un service original et unique. Ils ne resteront pas si votre contenu est peu attractif ou à faible valeur ajoutée, peu importe vos méthodes pour les attirer. Maintenir un site sans modification est une invitation pour des ennuis. Tôt ou tard, vous le regretterez. Conserver votre Noyau de Xoops à jour Utilisez les dernières mises à jour. Les développeurs corrigent des dysfonctionnements et des failles de sécurité. Avec les dernières mises à jour, vous diminuez des erreurs ou des failles de sécurité potentiels. N'ayez aucune illusion, si vous avez une faille de sécurité, elle sera exploitée contre votre site. Les failles de sécurité ont été et seront exploitées si vous ne faites pas de mises à jour. PHP et MySQL Depuis que Xoops utilise PHP et MySQL, il a aussi hérité de leurs faiblesses respectives. MySQL nécessite PHP pour envoyer, en clair, le pseudo et le mot de passe. Ce qui, vous l'imaginez, crée des casse-têtes pour la sécurité. Si votre session est attaquée (hijacked), alors votre base de données est vulnérable. Il n'y a pas de conseils évidents pour éviter cela. Nous le mentionnons pour que vous en soyez informé. Si votre hébergeur vous autorise à faire tourner PHP incgi-wrap, vous pouvez l'utiliser. Mais attention si votre site est toujours actif, vous le ralentirez. Contenu du Cache Si vous vendez du contenu, vous devez installer les lignes suivantes dans l'en-tête de votre fichier theme.html `META NAME="ROBOTS" CONTENT="NOARCHIVE">` Cela empêchera les visiteurs de vous voler votre contenu. Mais si vous bannissez une adresse IP, ils pourront toujours faire une copie du contenu par en cliquant sur une version en cache sur Google (ou tout autre moteur de recherche). Les versions cache viennent des serveurs de moteurs de recherche, pas du vôtre, vous n'avez aucun contrôle dessus. Attention en utilisant ce code, la plupart des moteurs de recherche sont contre le URL cloaking. Malheureusement, la technique de cloaking est utilisée dans la balise noarchive. Votre site risque d'être étiqueté par les moteurs de recherche comme "délinquant du cloaking" et votre classement sera alors dégradé par ces mêmes moteurs. Autres astuces pour un site Xoops plus sûr Si vous avez suivi toutes les suggestions, votre site devrait être relativement bien sécurisé. Comme nous vous le disons en introduction, ne soyez pas trop sûr de votre sécurité. Une bonne pratique est toujours de vérifier les statistiques quotidiennes de connexions et de rechercher d'éventuels problèmes et de prendre les mesures qui s'imposent. En espérant que ce guide sera utile à tous !! ndt : moi aussi.