Guide de sÃ©curitÃ© pour Xoops

CatÃ©gorie : SÃ©curitÃ© et pirates

PubliÃ© par Fooups le 15/03/2005

Avant tout, vous devez garder Ã¡ l'esprit qu'il n'existe pas de systÃªme sÃ©curisÃ© Ã¡ 100%. Tout est relatif. Maintenant que c'est dit, il existe certaines choses que vous pouvez faire pour amÃ©liorer la sÃ©curitÃ© de votre systÃªme. Ce guide rÃ©sume les diffÃ©rentes Ã©tapes pour sÃ©curiser votre site Ã¡ partir d'astuces issues des forums officiels de Xoops.org et du site Xoops-tips.com. La plupart de ces astuces ont dÃ©jÃ¡ Ã©tÃ© listÃ©es sur Xoops-tips, mais pas de faÃ§on structurÃ©e. Nous espÃ©rons (le traducteur aussi) que la prÃ©sentation structurÃ©e de toutes ces astuces, anciennes et nouvelles, apporteront une meilleure comprÃ©hension des problÃªmes de sÃ©curitÃ©. Choisir un hÃ©bergement Beaucoup d'entre nous ont tendance Ã¡ diminuer l'importance d'un bon hÃ©bergeur et vont lÃ¡ oÃ¹l'offre est la plus allÃªchante avec les coÃ»ts minimums. Vous devriez avoir une vÃ©ritable rÃ©flexion au moment de choisir une solution d'hÃ©bergement. Un bon hÃ©bergeur avec une bonne rÃ©putation signifie en gÃ©nÃ©ral une bonne sÃ©curitÃ©. Comme la plupart d'entre nous n'avons pas de budget suffisant pour s'offrir un serveur dÃ©diÃ©, vous devriez apporter une attention particuliÃªre Ã¡ la sÃ©curitÃ© du serveur en entier et des autres sites hÃ©bergÃ©s. La sÃ©curitÃ© des autres sites end du serveur sont aussi important que la sÃ©curitÃ© de votre propre site. Peu importe le niveau de sÃ©curitÃ© de votre site, si le serveur a subit une attaque via d'autres sites placÃ©s sur le mÃªme serveur, tous vos efforts pourraient s'avÃ©rer inutiles en fin de compte. Les hÃ©bergeurs solitaires, revendeurs et petites compagnies devraient en gÃ©nÃ©ral Ãªtre Ã©vitÃ©s si vous le pouvez, le plus souvent ils n'ont pas les ressources suffisantes ou les compÃ©tences nÃ©cessaires pour gÃ©rer les serveurs. Comme l'hÃ©bergement de sites Internet s'est considÃ©rablement dÃ©veloppÃ©, le coÃ»t d'hÃ©bergement n'est plus aussi cher qu'avant. Un bon hÃ©bergement vaut largement le surcoÃ»t engendrÃ©. La face cachÃ©e des hÃ©bergements ces temps-ci, vous pouvez louer un serveur Ã¡ un "grossiste" comme n'importe qui pour 200$ ou moins et devenir revendeur Ã¡ votre tour. Tant que le revendeur paye ses factures, le grossiste ne s'inquiÃªtera pas de la sÃ©curitÃ© du serveur. Quand vous choisissez un revendeur, posez-vous cette question : Ã¢â‚¬Å“Est-ce que l'hÃ©bergeur a les compÃ©tences pour gÃ©rer des serveurs ?Ã¢â‚¬Â• Si votre hÃ©bergeur est situÃ© au Royaume-Uni, mais que ses serveurs sont situÃ©s au Texas, qu'arriverait-il si votre serveur Ã©tait hors d'usage ? Vous devriez appeler votre hÃ©bergeur, et votre hÃ©bergeur devrait appeler le sien pour rÃ©gler le problÃªme. EspÃ©rons que vous aurez une idÃ©e. Au moment de choisir un hÃ©bergeur, gardez Ã¡ 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 hÃ©bergement Ã¡ 2$ par mois. Installation - Choisir le prÃ©fixe de la table Pendant le processus d'installation, vous devez choisir un prÃ©fixe difficilement identifiable. N'utilisez pas le prÃ©fixe par dÃ©faut "xoops". Il est trop facile Ã¡ deviner pour les hackers. Si vous avez installer votre site avec le prÃ©fixe Ã¢â‚¬Å“xoopsÃ¢â‚¬Â•, vous pouvez utiliser le module Protector dÃ©veloppÃ© par GIJOE pour le changer. AprÃªs l'installation Une fois votre Xoops installÃ© avec succÃªs, n'oubliez pas d'effacer le rÃ©pertoire "install" et de paramÃ©trer les droits du fichier mainfile.php (chmod 444 ndt). Laisser son rÃ©pertoire "install" en place et son mainfile.php sans protection, c'est inviter les autres Ã¡ rÃ©installer un site Xoops et Ã¡ prendre le contrÃ´le de votre site. S'il leur prenait l'envie de faire des choses illÃ©gales avec, vous seriez responsable des dommages causÃ©s.

Installer le module Xoops Protector Une fois l'installation terminÃ©e, le premier module que vous

devriez installer est Xoops Protector de GIJOE. Si vous Ãªtes sÃ©rieux sur la sÃ©curitÃ© de votre site, vous devez installer ce module. Le systÃªme Xoops est peut-Ãªtre le plus sÃ©curisÃ© des CMS. NÃ©anmoins, le noyau ("Core") a ses faiblesses qui pourraient laisser passer des hackers. Cela a Ã©tÃ© dÃ©montrÃ© par GIJOE, de loin le meilleur contributeur concernant la sÃ©curitÃ© de Xoops. Xoops 2.0.10 intÃ©grera certaines des idÃ©es de GIJOE. Mais le module protector est toujours trÃ¨s largement recommandÃ© car il dÃ©fend Ã¡ la fois contre des attaques contre le noyau central et les modules. Le module protector peut protÃ©ger de diffÃ©rents types d'attques comme : DÃ©ni 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 globals pollution; session hi-jacking (NdT: renifler le rÃ©seau et exploiter des faiblesses de TCP - Protocole de ContrÃ´le des Transmissions, Ã¡ la base d'Internet dans le couple TCP/IP); null-bytes; mauvaise spÃ©cification 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 XOOPS Pour plus d'information, allez sur le site de GIJOE (anglais, ndt): http://www.peak.ne.jp/xoops/ DÃ©placer les Username (NOM) et Password (MOT DE PASSE) hors du fichier mainfile.php Une considÃ©ration supplÃ©mentaire au sujet de votre installation de Xoops est de sortir du fichier mainfile.php vos identifiants d'accÃ¨s Ã¡ la base de donnÃ©es. Il est toujours plus sÃ»r de conserver les informations sensibles loins dans votre arborescence. Ceci empÃªchera la rÃ©vÃ©lation accidentelle de vos donnÃ©es sensibles en cas de dysfonctionnement du serveur comme un arrÃªt de PHP. Dans ce cas, l'information contenue dans le mainfile.php peut Ãªtre lue par n'importe qui dans le monde. Pour les dÃ©tails (anglais, Ã¡ traduire prochainement) http://xoops-tips.com/news-article.storyid-1.htm ProtÃ©ger le fichier admin.php et le module "system" Xoopsadmin.php est accessible par n'importe qui ce qui pose un problÃªme de sÃ©curitÃ© si des hackers souhaitent faire le tour de vos systÃªmes. Il existe un moyen de se protÃ©ger. (en anglais, traduction en cours) http://xoops-tips.com/news-article.storyid-9.htm
ProtÃ©ger le rÃ©pertoire Theme Vous pouvez protÃ©ger les fichiers de vos thÃªmes des curieux. DÃ©tails ci-dessous (nglais, traduction en cours) : http://xoops-tips.com/news-article.storyid-25.htm
DÃ©sactiver la liste des rÃ©pertoires (disable directory listing) Si votre hÃ©bergeur vous autorise Ã¡ dÃ©sactiver la liste des rÃ©pertoires, mettez le Ã¡ ON. Si votre hÃ©bergeur ne vous permet pas de telle manipulation, crÃ©ez un fichier index.html avec le contenu suivant : script>history.go(-1); Chargez-le dans tous les rÃ©petoires de votre site Xoops (SAUF A LA RACINE ou DANS les rÃ©pertoires de vos modules). La version de base de Xoops stock fournit ce fichier index.html dans la majoritÃ© des rÃ©pertoires. Assurez-vous que chaque rÃ©pertoire en dispose. ProtÃ©ger l'adresse Email de l'administration Vous ne devriez jamais, en aucun cas, rÃ©vÃ©ler 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 livrÃ©s avec le pack xoops.org, ndt) Faites particuliÃªrement attention aux modules tiers. Il peut exister des failles de sÃ©curitÃ© que les dÃ©veloppeurs n'ont pas dÃ©tectÃ©. Si vous utilisez un module tiers, assurez-vous de bien vÃ©rifier les mises Ã¡ jour et les fixes de sÃ©curitÃ©, et vÃ©rifiez rÃ©guliÃªrement 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 sÃ©curitÃ©. Sauvegardez votre site et son contenu La sauvegarde devrez Ãªtre considÃ©rÃ©e comme l'un des aspects le plus important de protection et de sÃ©curitÃ© de votre site. Des sauvegardes rÃ©guilÃªres et le tÃ©lÃ©chargement complet du site devraient Ãªtre une routine. Si votre contenu change quotidiennement, vous devriez sauvegarder quotidiennement votre base de donnÃ©es. S'il ne change pas aussi frÃ©quemment, alors une sauvegarde hebdomadaire peut Ãªtre une solution. De la mÃªme faÃ§on, pour les fichiers du site, une sauvegarde mensuelle devrait Ãªtre suffisante. Ou

faites une sauvegarde ad hoc Ã¡ chaque modification majeure de votre site. Equilibre entre attirer le chaland et sÃ©curitÃ© Certains Xoopsers sont tentÃ©s d'ouvrir leur site Ã¡ 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 Ã¡ faible valeur ajoutÃ©e, peu importe vos mÃ©thodes pour les attirer. Maintenir un site sans modÃ©ration est une invitation pour des ennuis. TÃ´t ou tard, vous le regretterez. Conserver votre Noyau de Xoops Ã¡ jour Utilisez les derniÃªres mise Ã¡ jour. Les dÃ©veloppeurs corrigent des dysfonctionnements et des failles de sÃ©curitÃ©. Avec les derniÃªres mises Ã¡ jour, vous diminuez des erreurs ou des failles de sÃ©curitÃ©s potentiels. N'ayez aucune illusion, si vous avez une faille de sÃ©curitÃ©, elle sera exploitÃ©e contre votre site. Les failles de sÃ©curitÃ© ont Ã©tÃ© et seront exploitÃ©es si vous ne faites pas de mises Ã¡ jour. PHP et MySQL Depuis que Xoops utilise PHP et MySQL, il a aussi hÃ©ritÃ© de leurs faiblesses respectives. MySQL nÃ©cessite PHP pour envoyer, en clair, le pseudo et le mot de passe. Ce qui, vous l'imaginez, crÃ©er des casse-tÃªtes pour la sÃ©curitÃ©. Si votre session est attaquÃ©e (hijacked), alors votre base de donnÃ©es est vulnÃ©rable. Il n'y a pas de conseils Ã©vidents pour Ã©viter cela. Nous le mentionnons pour que vous en soyez informÃ©. Si votre hÃ©bergeur vous autorise Ã¡ faire tourner PHP incgi-wrap, vous pouvez l'utiliser. Mais attention si votre site est trÃªs actif, vous le ralentirez. Contenu du Cache Si vous vendez du contenu, vous devez installer les lignes suivantes dansl'en-tÃªte de votre fichier theme.html METAÂ NAME= "ROBOTS"Â CONTENT="NOARCHIVE"> Cela empÃªchera 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 vÃ´tre, vous n'avez aucun contrÃ´le dessus. Attention en utilisant ce code, la plupart des moteurs de recherche sont contre le URL cloaking. Malheureusement, la technique de cloaking est utilisÃ©e dans la balise noarchive. Votre site risque d'Ãªtre Ã©tiquetÃ© par les moteurs de recherche comme "dÃ©linquant du cloaking" et votre classement sera alors dÃ©prÃ©ciÃ© par ces mÃªmes moteurs. Autres astuces pour un site Xoops plus sÃ»r Si vous avez suivi toutes les suggestions, votre site devrait Ãªtre relativement bien sÃ©curisÃ©. Comme nous vous le disions en introduction, ne soyez pas trop sÃ»r de votre sÃ©curitÃ©. Une bonne pratique est toujours de vÃ©rifier les statistiques quotidiennes de connexions et de rechercher d'Ã©ventuels problÃªmes et de prendre les mesures qui s'imposent. En espÃ©rant que ce guide sera utile Ã¡ tous ll! ndt : moi aussi.