http://icietla-ge.ch/voir/spip.php?article134

Ici & Là

Améliorer la sécurité de son site SPIP

- SPIP
- Sécurité
-

Publication date: jeudi 14 juillet 2016

Cet article aborde le thème de la sécurité du CMS SPIP en présentant 4 plugins qui oeuvrent pour assurer la sécurité et 8 articles qui traitent le sujet.

Sommaire

- Plugins
- Plugin FB Antispam - CAPTCHA
- Plugin NoSPAM
- Plugin Notifications
- Points clés pour améliorer (...)
- Références webographiques
- Points clés pour améliorer (...)

Plugins

Quatre plugins sont particulièrement intéressants pour améliorer la sécurité des sites SPIP :

1. les dix lame du bloc Sécurité du plugin Le Couteau Suisse
2. le plugin Notifications
3. le plugin FB Antispam - CAPTCHA pour forums
4. le plugin NoSPAM

Patrice Vanneufville a créé le plugin Le Couteau Suisse dont les dix lame du bloc Sécurité nous intéressent vivement ici. il s'agit de :

1. Ecran de sécurité
2. Fonctions d'autorisations
3. Gestion du JavaScript
4. Limites mémoire
5. Lutte contre le SPAM
6. MailCrypt
7. Mises à jour automatiques
8. Pas de forums anonymes
9. Pas de stockage IP
10. Taille des forums

Dont voici une brève description :

Bloc Sécurité

Lutte contre le SPAM

Tente de lutter contre les envois de messages automatiques et malveillants en partie publique. Certains mots, tout

comme les balises en clair , sont interdits : veuillez inciter vos rédacteurs à utiliser les raccourcis de liens SPIP. La configuration de cet outil antiSPAM vous permet facilement de Lister les séquences interdites et éventuellement de bloquer des adresses IPs.
Action rapide : test interactif de ce filtre (messages et/ou adresses IP) et parcours éventuel de la base de données.

â€”

Ecran de sécurité (toutes versions de SPIP)
L'écran de sécurité est un fichier PHP directement téléchargé sur le site officiel de SPIP, qui protège vos sites en bloquant certaines attaques liées à des trous de sécurité.
Outre la sécurité, cet écran a la capacité réglable de moduler les accès des robots d'indexation aux scripts php, de manière à leur dire de « revenir plus tard » lorsque le serveur est saturé.
En cas de mise à jour officielle, actualisez le fichier distant associé afin de bénéficier de la protection la plus récente.
Fichier distant : facilité de mise à jour et gestion des versions.

â€”

Gestion du javascript
Pour gérer le javascript dans les articles, trois modes sont disponibles :

- jamais : le javascript est refusé partout
- défaut : le javascript est signalé en rouge dans l'espace privé
- toujours : le javascript est accepté partout.

Attention : dans les forums, pétitions, flux syndiqués, etc., la gestion du javascript est toujours sécurisée.

â€”

Mises à jour automatiques
Garde un oeil sur tous vos plugins. Cet outil vous permet de gérer facilement leurs mises à jour, récupérant notamment le numéro de révision contenu dans le fichier svn.revision et le comparant avec celui trouvé sur zone.spip.org. La liste proposée offre la possibilité de lancer le processus de mise à jour automatique de SPIP sur chacun des plugins préalablement installés dans le dossier plugins/auto/.
Cet outil vous informe également des différentes versions officielles disponibles pour SPIP lui-même.

â€”

MailCrypt
Masque tous les liens de courriels présents dans vos textes en les remplaçant par un lien Javascript permettant quand même d'activer la messagerie du lecteur. Cet outil antispam tente d'empêcher les robots de collecter les adresses électroniques laissées en clair dans les forums ou dans les balises de vos squelettes.

â€”

Citations bien balisées
Afin de respecter les usages en HTML dans les contenus SPIP de votre site (articles, rubriques, etc.), cet outil remplace automatiquement les balises par des balises quand il n'y a pas de retour à la ligne.

â€”

Taille des forums

Par défaut les messages de forum ne sont pas limités en taille. Si cet outil est activé, un message d'erreur s'affichera lorsque quelqu'un voudra poster un message d'une taille supérieure à la valeur spécifiée, et le message sera refusé.

â€”

Pas de stockage IP

Désactive le mécanisme d'enregistrement automatique des adresses IP des visiteurs de votre site par soucis de confidentialité : SPIP ne conservera alors plus aucun numéro IP, ni temporairement lors des visites (pour gérer les statistiques ou alimenter spip.log), ni dans les forums (responsabilité).

â€”

Pas de forums anonymes

Incite tous les auteurs de messages publics à remplir (d'au moins d'une lettre !) le champ « Votre nom (ou pseudonyme) :» afin d'éviter les contributions totalement anonymes.

Cette fonctionnalité utilise la librairie jQuery.

â€”

Limites mémoire

- **Taille maximale des images, des logos et des documents**. Afin d'alléger la mémoire de votre serveur, SPIP vous permet de limiter les dimensions (hauteur et largeur) et la taille du fichier des images, logos ou documents joints aux divers contenus de votre site. Si un fichier dépasse la taille indiquée, le formulaire enverra bien les données mais elles seront détruites et SPIP n'en tiendra pas compte, ni dans le répertoire IMG/, ni en base de données. Un message d'avertissement sera alors envoyé à l'utilisateur.

Une valeur nulle ou non renseignée correspond à une valeur illimitée.

- **Espace maximal réservé aux copies locales (SPIP 2.0 mini)**. Il s'agit ici l'espace maximal réservé aux fichiers distants que SPIP pourrait télécharger (de serveur à serveur) et stocker sur votre site. La valeur par défaut est de 16 Mo.
- **Calculs d'images avec GD**. Afin d'éviter un dépassement de mémoire PHP dans le traitement des grandes images par la librairie GD2, SPIP teste les capacités du serveur et peut donc refuser de traiter les trop grandes images. Il est possible de désactiver ce test en définissant manuellement le nombre maximal de pixels supportés pour les calculs. La valeur de 1 000 000 pixels semble correcte pour une configuration avec peu de mémoire. Une valeur nulle ou non renseignée entraînera le test du serveur.
- **Qualité de compression (SPIP 2.0 mini)**. La librairie GD2 permet d'ajuster la qualité de compression des images JPG. Un pourcentage élevé correspond à une qualité élevée.

â€”

Sessions anonymes (SPIP 2.1 maxi)

Chaque semaine, cet outil vérifie les sessions anonymes et supprime les fichiers qui sont trop anciens (plus de 2 jours) afin de ne pas surcharger le serveur, notamment en cas de SPAM sur le forum.

Plugin FB Antispam - CAPTCHA pour forums

Fabio propose le plugin **FB Antispam - CAPTCHA pour forums**

Il s'agit d'un simple captcha pour protéger les forums des spams qui envahissent et submergent les bons messages.

Le plugin FBCaptcha ajoute un champs supplémentaire au formulaire pour la rédaction des commentaires de forum. Un code de 4 chiffres est généré de façon aléatoire et ce code doit être saisi par le visiteur pour valider la prise en compte de son commentaire.

Si le code ne correspond pas la saisie est proposée de nouveau avec un message avertissant de l'erreur dans le code.

La version 1.2 ajoute un panneau de configuration, où il est possible de choisir entre trois type de saisie :

1. la copie de 4 caractères,
2. une addition ou
3. une multiplication.

La version 1.2.1 ajoute un lien direct vers le panneau de configuration dans le menu « Configuration », et un choix par défaut si la configuration n'est pas enregistrée.

Plugin NoSPAM

Cerdic propose le plugin **NoSPAM** pour limiter le risque de spam dans les forums de SPIP. Ce plugin introduit plusieurs mécanismes visant à limiter l'envoi de spams depuis les formulaires de SPIP (forums publics, formulaires de contact, formulaires des pétitions).

Plugin Notifications

Fil a créé le plugin **Notifications** pour envoyer des mails quand les gens s'expriment dans le forum de l'espace privé, sous un article, ou dans la messagerie personnelle...

Ce plugin permet également de notifier le ou les auteurs d'un article lors de la publication de ce dernier.

Plus précisément, parmi ses diverses fonctions, relevons que ce plugin permet :

Articles publiés
Le plugin notifications sait envoyer des mails :

- aux auteurs, lors de la publication de leurs articles.
- aux administrateurs restreints, lors de proposition d'articles dans leur rubrique.

Forums publics
Le plugin notifications sait envoyer des mails :

- aux auteurs (comme le fait SPIP) lorsqu'un message est posté sous leur article
- aux participants d'un fil de discussion, quand quelqu'un parle dans n'importe quel forum public
- aux modérateurs

Il respecte le réglage de modération à priori : dans ce cas seuls les modérateurs sont notifiés lors de l'envoi du forum, les autres étant notifiés lors de sa validation.

On se reportera à l'article original pour les autres fonctions concernant les points :

- Forums privés
- Messagerie
- Signatures de pétition
- Inscription des rédacteurs

Points clés pour améliorer la sécurité des sites SPIP

Voici plusieurs articles intéressants sur le sujet :

OpenStudio, l'éditeur du logiciel libre Thelia présente **8 points clés pour améliorer la sécurité de votre site SPIP**.
Cet article très complet et détaillé passe en revue les points suivants :

1. Disposer d'une version de SPIP à jour
2. Vérifier le paramétrage d'Apache
3. Masquer le type de CMS utilisé
4. Mettre en place une politique de sécurité
5. Contrôler l'accès aux documents de IMG
6. Désactiver les squelettes par défaut et plugins inutilisés
7. Être rigoureux dans l'écriture des squelettes
8. Réaliser un audit régulier

â€”

Le site officiel SPIP spip.net présente l'**Écran de sécurité**.

L'écran de sécurité est un fichier php unique, qui protège vos sites en bloquant certaines attaques liées à des trous de sécurité. Ce système permet de réagir très rapidement lorsqu'un problème est découvert, en colmatant le trou sans pour autant devoir mettre à niveau tout son site ni appliquer un « patch » complexe.

Philosophie
Lorsqu'elle découvre ou qu'on lui signale un « trou » de sécurité, l'équipe de développement de SPIP s'efforce de corriger le problème au plus vite dans sa version de développement et dans ses versions stables, afin de ne plus diffuser de code fautif.

Cependant, la majorité des utilisateurs n'a pas toujours le temps ou la possibilité de faire la mise à jour, et a tendance à peser le pour et le contre face au risque d'avoir, lors d'une mise à jour même minime, des incompatibilités ou des décalages avec le code testé et validé qu'elle a mis en ligne.

Pour un hébergeur, l'information concernant un problème de sécurité est également à double tranchant : d'un côté il ne souhaite pas laisser de « trou » sur un de ses sites hébergés, de l'autre il n'a pas toujours l'autorisation de modifier les sites. Et les mettre hors-ligne n'est bien souvent pas envisageable, sauf chez les hébergeurs cheap ou paranos.

L'écran de sécurité est là pour répondre à cette problématique. Il s'agit d'un fichier php unique et séparé de SPIP, que l'on peut mettre à jour indépendamment du reste du code, et qui est compatible avec toutes les versions de SPIP, même les plus anciennes.

Ce fichier ne se substitue pas a une véritable mise à niveau de votre version de SPIP, mais il peut permettre de bloquer certaines attaques en attendant une migration propre.

De fait, cet écran peut être activé au niveau du serveur sur l'ensemble des scripts php (SPIP ou pas), et garantit, s'il est à jour, que toutes les failles connues de quelque version de SPIP que ce soit sont impossibles à exploiter. D'où son nom d'« écran » : il se place entre le visiteur et SPIP, et vérifie que le visiteur n'est pas en train d'essayer d'exploiter une attaque connue.

Lorsqu'une nouvelle faille est découverte, il suffit donc de mettre à jour cet écran pour parer toute attaque via ladite faille ; ça laisse le temps de mettre à jour les scripts SPIP à tête reposée au moment idoine.

â€”

La liste des articles de mise à jour de sécurité est listée sur la page **SPIP-core**
Présente toutes les alertes de failles sécurité découvertes et corrigées sur SPIP.

â€”

Le dernier exemple d'alerte de failles sécurité découvertes et corrigées sur SPIP date du 10 mars 2016 : L'équipe de SPIP-Contrib **Mise à jour CRITIQUE de sécurité - Sortie de SPIP 3.1.1, SPIP 3.0.22 et SPIP 2.1.29**. en voici la teneur :

Deux failles de sécurité ont été découvertes récemment dans SPIP :

1. une faille critique permettant l'injection de code PHP (merci à g0uZ et sambecks, team root-me)
2. une faille secondaire permettant l'injection d'objets par unserialize (merci à Gilles Vincent)

Ces failles sont sérieuses et affectent toutes les versions de SPIP. Il est impératif de mettre à jour votre site SPIP dès que possible.

Pour les sites qui ne peuvent pas être immédiatement mis à jour, il est nécessaire d'installer la version 1.2.4 de l'écran de sécurité qui corrige la faille critique http://www.spip.net/fr_article4200.html

Annonce complète et détails https://blog.spip.net/789

â€”

Le site Apprendre SPIP - http://spippourlesnuls.fr présente une page intitulée **Sécurité - méfiance sur Internet** dont la teneur essentielle est :

La première sécurisation porte sur la gestion et l'enregistrement des mots de passe nécessaires aux auteurs : bien sûr, ceux-ci sont enregistrés de façon haschée et salée, ce qui signifie que le mot de passe n'est pas géré en clair (texte dactylographié), mais encodé par une fonction (MD5 et maintenant SHA), avec en plus l'apport d'un grain de sel aléatoire, qui interdit le décodage direct.
Par ailleurs, SPIP propose un système de récupération de son accès privé par l'intermédiaire du mail déclaré à chaque auteur, ce qui reporte la sensibilité d'accès sur ce dernier.

Parmi les failles de sécurité courantes sur le Web, la défiguration est l'une des plus visibles en termes de communication et de buzz, et mise en évidence par le CERTA.

En plus de mises-à-jour du core fréquentes, SPIP dispose désormais d'un programme Â« ecran de securité Â» pour protéger des failles XSS...

Un assez bon gage de sécurité de ce CMS, souvent choisi par des experts, peut s'en déduire quand on s'aperçoit qu'un nombre important de sites de sécurité sont sous SPIP : spyworld-actu.com/..

Mais assez souvent, on constatera une attaque indirecte, c'est-à-dire que ce n'est pas le site lui-même qui est compromis, mais une machine cliente, souvent celle utilisée pour des mises-à-jour, qui se fait voler les accès FTP : voir Des cas..... résolus ! PHP5.

â€”

Le site cimarronweb.com présente une page dédiée à la sécurité intitulée **Sécurité des sites SPIP - mise à jour de sécurité**. elle traite les questions de :

- L'écran de sécurité
- La mise à jour des plugins via la lame Â« Mise à jour automatique Â» du plugin Le couteau suisse.

â€”

Dans son artilce **Réglages de sécurité pour SPIP** , Philippe Giron aborde :

- Le problème du spam et propose d'utiliser le plugin NoSpam.
- Le plugin Notification
- Le bloc Sécurité du plugin Le couteau suisse qui aujourd'hui présente les lames :
  1. Ecran de sécurité
  2. Fonctions d'autorisations
  3. Gestion du JavaScript
  4. Limites mémoire
  5. Lutte contre le SPAM
  6. MailCrypt
  7. Mises à jour automatiques
  8. Pas de forums anonymes
  9. Pas de stockage IP
  10. Taille des forums

â€”

Cerdic aborde **La sécurité** en traitant les thèmes :

- Qu'est-ce que la sécurité ?
- La problématique actuelle
- Politique actuelle
- Les injections SQL
- La communication

Références webographiques

Plugins

Quatre plugins sont particulièrement intéressants pour améliorer la sécurité des sites SPIP :

1. Les dix lame du bloc Sécurité du plugin Le Couteau Suisse
2. Notifications
3. FB Antispam - CAPTCHA pour forums
4. NoSPAM

- **Les dix lame du bloc Sécurité du plugin Le Couteau Suisse**
  4 mai 2007 - par Patrice Vanneufville
  http://contrib.spip.net/Le-Couteau-Suisse#securite
  http://plugins.spip.net/couteau_suisse.html
  1. Ecran de sécurité
  2. Fonctions d'autorisations
  3. Gestion du JavaScript
  4. Limites mémoire
  5. Lutte contre le SPAM
  6. MailCrypt
  7. Mises à jour automatiques
  8. Pas de forums anonymes
  9. Pas de stockage IP
  10. Taille des forums

- **Notifications**
  23 juillet 2007 - par Fil
  http://contrib.spip.net/Notifications
  http://plugins.spip.net/notifications.html

- ***Notifications avancées***
  8 novembre 2011 - par RastaPopoulos
  http://contrib.spip.net/Notifications-avancees-3981

http://plugins.spip.net/notifavancees.html

- **FB Antispam - CAPTCHA pour forums**
  26 octobre 2013 - par Fabio
  http://contrib.spip.net/FB-Antispam-CAPTCHA-pour-forums
  http://plugins.spip.net/fbantispam.html

- **NoSPAM**
  20 novembre 2008 - par Cerdic
  http://contrib.spip.net/NoSPAM
  http://plugins.spip.net/nospam.html

Points clés pour améliorer la sécurité des sites SPIP

Voici plusieurs articles intéressants sur le sujet :

- **8 points clés pour améliorer la sécurité de votre site SPIP**
  Par : OpenStudio, éditeur du logiciel libre Thelia
  avril 2012
  http://www.openstudio.fr/lab/8-points-clefs-pour-ameliorer-la.html

- **Écran de sécurité**
  Août 2009 â€" mis à jour le : 13 mars
  http://www.spip.net/fr_article4200.html

- **SPIP-core**
  Présente toutes les alertes de failles sécurité découvertes et corrigées sur SPIP.
  http://contrib.spip.net/SPIP-core#pagination_articles

- **Mise à jour CRITIQUE de sécurité - Sortie de SPIP 3.1.1, SPIP 3.0.22 et SPIP 2.1.29**
  Dernier exemple en date d'alerte de failles sécurité découvertes et corrigées sur SPIP.
  10 mars 2016 - par L'équipe de SPIP-Contrib
  http://contrib.spip.net/Mise-a-jour-CRITIQUE-de-securite-Sortie-de-SPIP-3-1-1

- **Sécurité - méfiance sur Internet**
  http://spippourlesnuls.fr/?Securite,148

- **Sécurité des sites SPIP - mise à jour de sécurité**
  vendredi 23 janvier 2015
  http://www.cimarronweb.com/spip.php?article86

- **Réglages de sécurité pour SPIP**
  mercredi 14 janvier 2015 par Philippe Giron
  http://internet22.catholique.fr/Reglages-de-securite-pour-SPIP

- **La sécurité**
  par Cerdic, 4 mars 2006 - Dernière modification de cette page le 3 janvier 2008
  http://contrib.spip.net/La-securite