Documentation module Protector V 3.10

Présentation

Protector est un module très utile qui vous aidera à améliorer la sécurité de votre site XOOPS, son installation est fortement recommandée car il peut vous défendre contre :

- toutes sortes d'attaques de dénis de service (DoS) aspirateurs (gourmands en bande passante), spambots, robots.
- Injection SQL, contamination de variables, bits null, détournement de session (hi-jacking), et toutes sortes de **Cross Site Scripting (XSS), ou le scripting par sites croisés**.
- attaques par force brute et traversée de répertoires
- télé versement (upload) de fichiers image camouflés et d'exécutables
- contrôles des spams dans les liens et commentaires.

Protector enregistre les IPs lors de ces attaques et propose une fourchette de contre-mesures comprenant le bannissement d'IPs, écrans vides, désinfection automatique de tentatives d'injections. Il évalue aussi votre site pour certaines vulnérabilités, fournit des avertissements et des procédures de correction au moyen d'une page spécifique.

Plan

Crédits

L'auteur du module Protector s'appelle GIJOE, il développe des modules et des hacks qui sont compatibles pour les différentes versions de Xoops (série 2.0.x, 2.2.x, XoopsCube, et Xoops JP).

Le module est disponible sur son site http://www.peak.ne.jp/xoops/

Le contenu de ce document est basé largement sur le document, rédigé initialement en anglais par Madfish, puis enrichi par l'équipe Xoops France.

Le support initial fut rédigé à partir du fichier REAME fourni avec le module, texte également disponible dans l'interface d'administration, complété par quelques explications fournies par l'auteur.

1. Installation

L'installation de ce module ne suit pas exactement la procédure standard et quelques fichiers devront être modifiés. Ces modifications complémentaires sont nécessaires pour mettre entièrement en application les améliorations de sécurité recommandées par le module.

1.1 Nouvelle installation

Cette procédure concerne l'installation du module Protector sur un site qui ne disposait pas d'une version de ce module antérieurement. Il est **impératif** d'effectuer ces différentes étapes dans l'ordre où elles sont présentées.

Après avoir décompressé l'archive dans un répertoire temporaire vous serez en présence des dossiers suivants :

/MODULES
/XOOPS_TRUST_PATH

a) copier le dossier *modules* à la racine de votre site
b) créer un autre dossier, avec le nom qu'il vous plaira, **en dehors de la racine de votre site,** dans lequel vous copierez le contenu du dossier XOOPS_TRUST_PATH

exemple :
la racine de votre site est :
/home/xyz/public_html
créez alors un nouveau dossier dans le répertoire
/home/xyz/nouveau_dossier
Ce qui donnera donc l'arborescence suivante :
/home
/xyz
/public_html ← racine de votre site xoops
/nouveau_dossier ← contenu de xoops_trust_path

Si votre hébergement ne vous permet pas de créer ce nouveau dossier en dehors de la racine de votre site, vous pouvez créer ce dossier XOOPS_TRUST_PATH dans un répertoire de votre site, le module fonctionnera mais sera moins sécurisé.

c) modifier les permissions du répertoire nouveau_dossier/modules/protector/configs afin qu'il soit en lecture-écriture (chmod=777). Dans un environnement Windows cela est inutile, mais avec un système d'exploitation linux, vous pouvez effectuer cette opération avec votre logiciel ftp, le plus souvent à l'aide d'un clic droit sur le dossier concerné.
d) Editer le fichier mainfile.php situé à la racine de votre site afin d'y ajouter une nouvelle ligne qui aura pour but de définir la valeur de XOOPS_TRUST_PATH. Le plus simple est d'ajouter cette ligne juste après le « define » de XOOPS_ROOT_PATH.
Ce qui donnerait :

Exemple :

define('XOOPS_ROOT_PATH', '/home/xyz/public_html'); (ligne existante)

define('XOOPS_TRUST_PATH', '/home/xyz/nouveau_dossier'); (nouvelle ligne)

- Il convient maintenant de procéder à l'installation du module. Pour effectuer cette opération, il suffit d'aller dans le menu Administration -> admin system -> modules, et de cliquer sur l'icône du module Protector en bas de la page.

- Si l'installation s'est bien déroulée, vous allez à nouveau modifier votre fichier mainfile.php situé à la racine de votre site pour lui ajouter les deux lignes écrites en rouge comme expliqué dans l'exemple ci-dessous.

```
include XOOPS_TRUST_PATH.'/modules/protector/include/precheck.inc.php';
    if ( !isset( $xoopsOption['nocommon'] ) && XOOPS_ROOT_PATH != '' ){
        include XOOPS_ROOT_PATH."/include/common.php";
    }
include XOOPS_TRUST_PATH.'/modules/protector/include/postcheck.inc.php';
}
?>
```

L'installation est maintenant terminée. N'oubliez pas de changer les permissions sur votre fichier mainfile.php afin qu'il soit en lecture seule (chmod=444).

1.2. Mise à jour à partir de Protector v2.x

Il suffit de suivre les étapes suivantes :

- supprimer les lignes *precheck* et *postcheck* que vous aviez ajouté à la fin de votre fichier mainfile.php lors de l'installation de Protector
- supprimer tous les fichiers situés dans le dossier protector
  XOOPS_ROOT_PATH/modules/protector/
- suivre la procédure décrite dans le chapitre 1.1 pour une nouvelle installation

1.3 Paramétrer le module

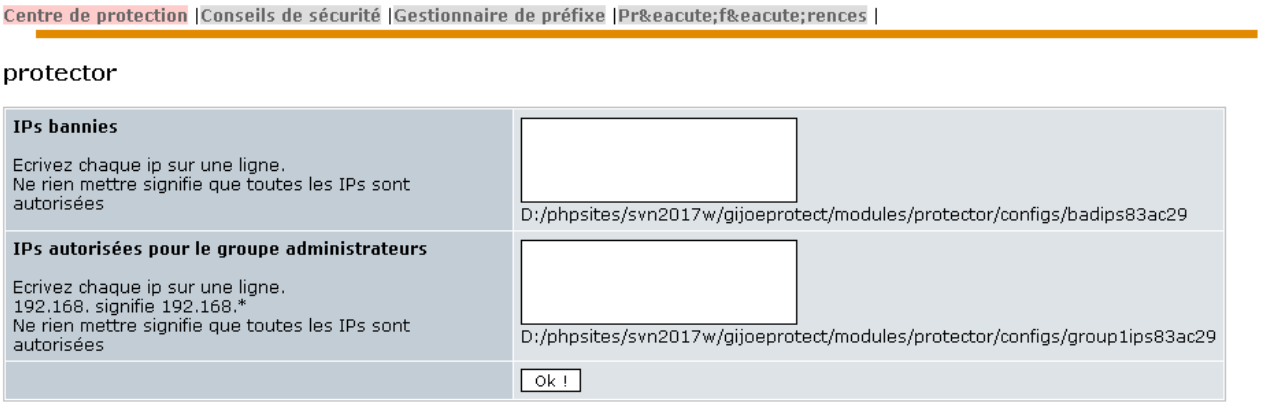
Une fois votre module installé correctement, continuer la procédure pour effectuer les paramétrages adéquats .

- dans la page préférences afin d'adapter la configuration du module à votre environnement
- Consulter la page conseils de sécurité et suivez les recommandations qui vous sont proposées afin d'éliminer la plupart des risques identifiés. Les détails de cette implémentation sont décrits un peu plus loin

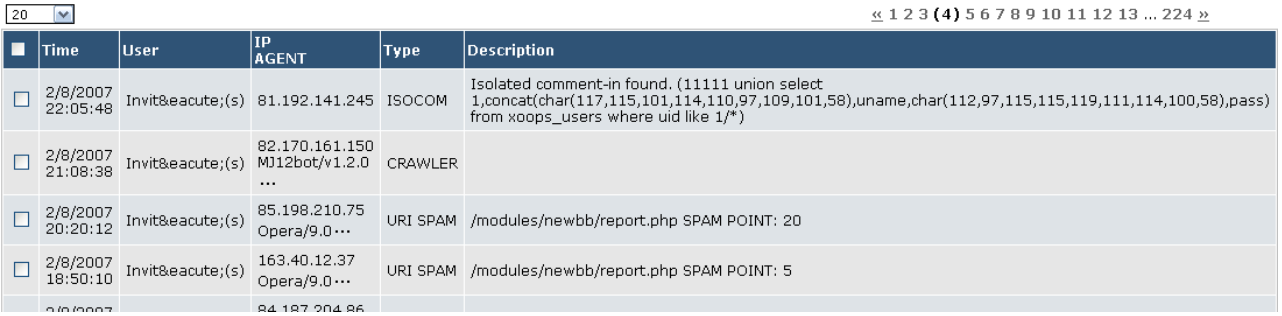
2. Centre de protection

C'est la page par défaut lorsque vous arrivez dans la partie administration du module. Elle vous propose un écran divisé en deux parties.

Sur la première elle fournit un outil pratique pour bannir les IPs qui vous procurent des problèmes.



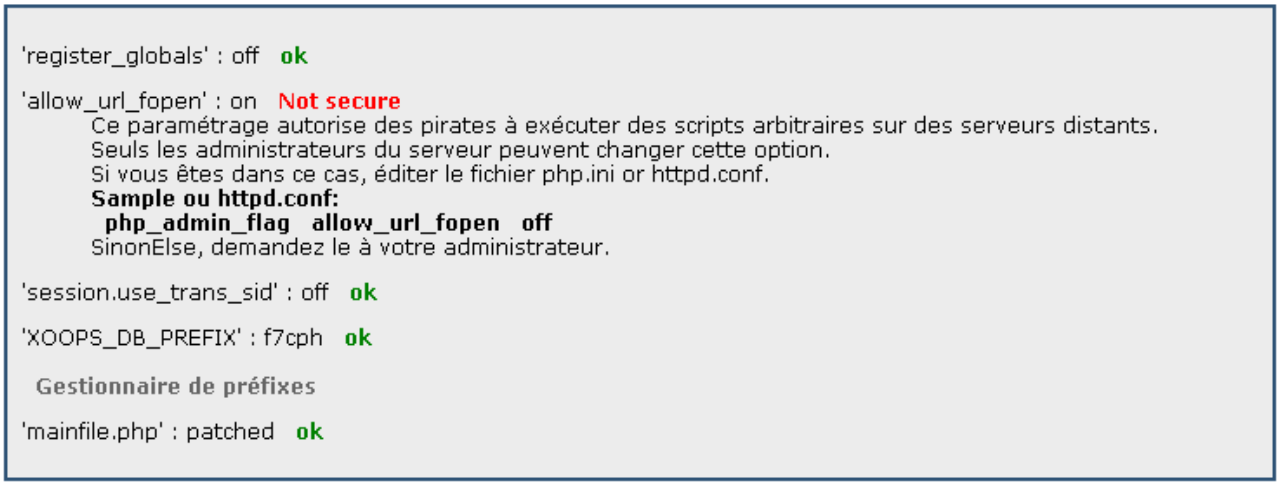
Dans le tableau positionné sur la seconde partie de la page, vous pourrez visualiser la liste des dernières actions du module suite à des incidents qu'il a identifié.



Vous avez la possibilité de supprimer individuellement des enregistrements en cliquant sur la case à cocher en début de ligne, ou en cochant la case à cocher située dans l'en-tête de la colonne pour supprimer tous les enregistrements affichés sur la page, puis valider votre action en cliquant sur le bouton supprimer en bas de la page.

3. Conseils de sécurité

La page « conseils de sécurité » évalue la vulnérabilité de votre site contre des risques de sécurité et propose des conseils pour les corriger comme affiché dans la copie d'écran ci-dessous !



Comment corriger les risques de sécurité ?

En suivant les instructions ci-après vous pourrez mettre en application les améliorations de sécurité recommandées par le module Protector. Actualisez cette page pour vérifier vos progrès, les avertissements écrits initialement en rouge passeront au vert.

3.1 'register_globals': on

La correction de cette faille est très facile à mettre en oeuvre. Il vous suffit de créer un fichier texte que vous allez appeler ***.htaccess*** (ne pas oublier le point devant htaccess). Ensuite copier la ligne écrite en rouge ci-dessous, sauvegarder votre fichier puis transférer le fichier, avec votre logiciel ftp, à la racine de votre site.

Si ce dernier contient déjà un fichier .htaccess à cet endroit, éditez-le et ajoutez cette ligne :

php_flag register_globals off

3.2 'allow_url_fopen': on

Ce paramétrage permet à des personnes malveillantes d'exécuter des scripts arbitraires sur des serveurs distants. Malheureusement cela peut être difficile à corriger parce que seul un administrateur du serveur peut modifier cette option.

Si vous louez un espace disque chez un hébergeur demandez-lui de faire ce changement pour (mais beaucoup de centres serveurs refuseront de modifier leur système partagé pour votre convenance). Si vous avez la chance d'avoir accès à la configuration de votre serveur, éditez le fichier php.ini (ou httpd.conf) et ajoutez ou modifiez la ligne existante pour obtenir ce résultat :

php_admin_flag allow_url_fopen off

3.3 'session.use_trans_sid": on

Ajouter cette ligne dans votre fichier .htaccess qui est situé à la racine de votre site :

php_flag session.use_trans_sid off

3.4 'XOOPS_DB_PREFIX' xoops

Ceci est traité dans la section "Gestionnaire de préfixe" un peu plus loin dans ce document.

3.5 'mainfile.php': missing precheck

Editez votre fichier mainfile.php selon les indications fournies dans la procédure d'installation du module. Cet avertissement ne sera plus affiché si vous suivez scrupuleusement ce qui est indiqué.

3.6 Contrôle de l'action de Protector

Cliquez sur l'un des liens pour tester le module, ce qui devrait vous redirigez vers la page d'accueil, et selon votre paramétrage des lignes devraient être ajoutées dans la log du centre de protection

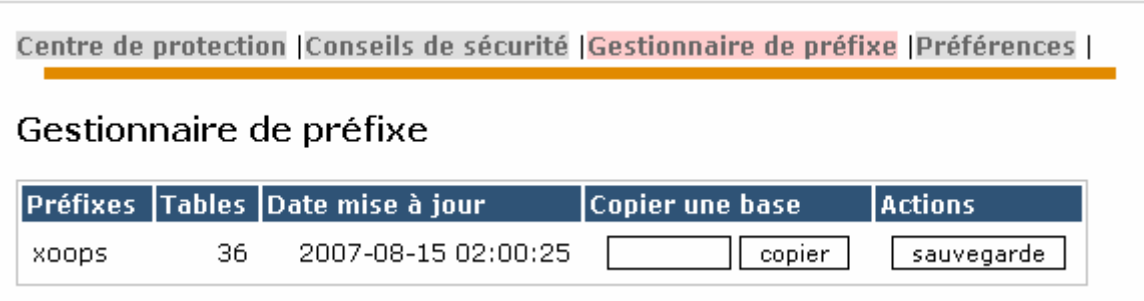
.

4. Gestionnaire de préfixe

Le gestionnaire de préfixe pourra changer le préfixe des tables de votre base de données en recopiant celles-ci avec le préfixe de votre choix tout en procédant à une sauvegarde préalable.

Pourquoi changer ce préfixe ? Lors de l'installation initiale de Xoops, le préfixe xoops est proposé par défaut, et on ne pense pas toujours à le modifier. Le problème est que cela est facilement prévisible et facilite les attaques d'injection SQL – si un hacker trouve une faille sur votre site, il lui sera facile d'intervenir sur votre base de données parce qu'il sera capable de disposer du nom complet des tables. En modifiant le préfixe par quelque chose d'autre, ce sera alors un peu plus difficile pour lui.

Voici l'écran que vous découvrirez en cliquant sur le menu Gestionnaire de préfixe



En cliquant sur le bouton ***sauvegarde***, un processus va générer une sauvegarde de votre base de données, il vous proposera d'enregistrer le résultat dans un fichier texte avec l'extension .sql sur votre ordinateur qu'il est conseillé d'accepter.

Cette opération étant réalisée, vous allez maintenant pouvoir saisir un nouveau préfixe dans la colonne ***Copier une base***, cliquez ensuite sur le bouton ***copier*** pour lancer l'action.

> Pour connaître les caractères interdits dans un nom de table vous pouvez consulter la documentation mysql : http://dev.mysql.com/doc/refman/5.0/fr/legal-names.html
>
> Nous attirons votre attention sur cette action va doubler la taille de votre base de données, et il vous est conseillé de vérifier préalablement que cela sera compatible avec les caractéristiques de votre hébergement.

Après l'opération de copie, votre page va se réactualiser avec cette présentation représentée avec la copie d'écran ci-dessous.

On aperçoit maintenant les deux bases de données et dans le tableau ***Queries***, une log sql des différentes requêtes qui ont abouti à ce résultat.

Pour que votre système puisse maintenant utiliser cette nouvelle base de données qui vient d'être clonée avec le nouveau préfixe, il suffit simplement d'éditer le fichier mainfile.php, situé à la racine de votre site pour lui mettre ce nouveau préfixe en remplacement de l'ancien.

Dans l'exemple utilisé ci-dessus, il va donc falloir remplacer :

```
// Table Prefix
define('XOOPS_DB_PREFIX', 'xoops');
```

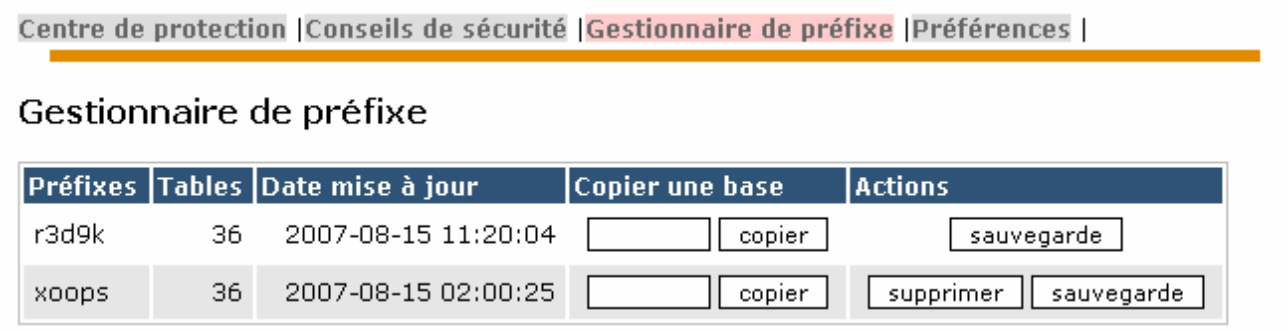
par

```
// Table Prefix
define('XOOPS_DB_PREFIX', 'r3d9k');
```

Après avoir sauvegardé ce fichier, transférez le à la racine de votre site en remplaçant du fichier existant et n'oubliez pas de re-paramétrer ses permissions pour le mettre en lecture seule (chmod=444)

Pour terminer cette opération proprement, il convient maintenant de supprimer la base de données initiale avec le préfixe ***xoops***.

La modification du préfixe dans le fichier mainfile.php a pour conséquence une légère modification de la présentation de l'écran gestionnaire de préfixe :



Il vous est maintenant proposé de cliquer sur le bouton supprimer de la ligne concernant la base de données avec le préfixe xoops pour supprimer cette base qui est maintenant devenue superflue.

5. Préférences

Les options de configuration et le paramétrage recommandé sont résumés dans le tableau ci-dessous. Pour la majorité des cas, vous pouvez conserver le paramétrage par défaut.

Options de configuration	Explications
Temporairement désactivé(oui/non)	Vous pouvez désactiver temporairement Protector si vous rencontrez quelques problèmes. N'oubliez pas de remettre cette option à non quand vous aurez corrigé l'anomalie. Valeur par défaut : non
Niveau de connexion	Les options suivantes sont proposées, mais nous ne disposons pour l'instant d'aucune information sur les conséquences des divers choix proposés : • Aucun • Serein • serein • Complet Valeur par défaut : complet
Temps d'exclusion d'une IP bannie	Saisissez un nombre qui sera exprimé en secondes
IPs fiables	Saisissez les adresses IPs que vous considérez comme fiables. Ceci pourra vous aider afin que Protector ne vous empêche pas de vous connecter. Saisissez les adresses en les séparant avec le caractère | ^ correspond au début de la chaîne $ correspond à la fin de la chaîne.
Nombre de bits de protection de la session IP	Ceci est une mesure de protection contre le vol de session (hijacking). Ce genre d'attaques se produit après l'identification ce qui permettrait à l'attaquant d'assumer le rôle d'un utilisateur (ou administrateur). • Défaut 32 bits – tous les bits sont protégés (l'IP ne peut pas être changée) • Si vous avez une adresse IP dynamique qui évolue dans une fourchette déterminée, vous pouvez définir le nombre de bits correspondants à protéger • Exemple si votre IP se situe entre 192.168.0.0 et 192.168.0.255, utilisez 24 bites. Si un attaquant connaît votre session IP mais a essayé d'accéder depuis l'extérieur de cet intervalle (comme 192.168.2.50) il échouera. L'auteur du module suggère 16 bits comme un valeur médiane pour les sites généraux..
Groupes non autorisés à modifier leur adresse IP au cours d'une session	Ceci est une mesure de protection contre le vol de session (hijacking). Les groupes sélectionnés ne sont pas autorisés à modifier leur adresse IP au cours d'une session. La valeur par défaut est pour le groupe webmasters et il est recommandé de conserver cette option car les conséquences du détournement de la session d'un administrateur peuvent être graves.
Sanitiser les bits null	Le caractère de terminaison '\0' est souvent utilisé dans des attaques malveillantes. Un bit null sera transformé en espace. Conseil : forte recommandation d'activer cette option

Options de configuration	Explications
Ejecter si des fichiers interdits sont uploadés)	Si quelqu'un tente d'uploader des fichiers avec une extension non souhaitée comme .php, il sera éjecté. Conseil : si vous attachez régulièrement des fichiers php dans B-Wiki ou PukiWikiMod, n'activez pas cette option.
Action si une contamination est trouvée	Sélectionner une action lorsque quelqu'un essaiera de contaminer des variables globales système XOOPS. • Aucune – enregistrer seulement • Ecran blanc • Bannir l'ip (temporairement) • Bannir l'ip (définitivement) (Conseil : l'option écran blanc est recommandé).
Action si un commentaire isolé est détecté	Mesure contre les injections SQL Sélectionner une action quand une chaîne isolée "/*" est trouvée : • Aucune – enregistrer seulement • Sanitiser • Ecran blanc • Bannir l'ip (temporairement) • Bannir l'ip (définitivement). 'Sanitiser' signifie ajouter d'autres '*/' à la suite. Conseil : 'sanitiser' est l'option recommandée, cependant la valeur par défaut est aucune que vous pouvez modifier.
Action si une requête UNION est détectée	Mesure contre les injections SQL Sélectionner l'action à effectuer quand une syntaxe de requêtes 'UNION' SQL est trouvée : • Aucune – enregistrer seulement • Sanitiser • Ecran blanc • Bannir l'ip (temporairement) • Bannir l'ip (définitivement). La sanitisation changera "union" en "uni-on", c'est cette option qui est recommandée.
Transformation forcée en nombre entier (intval) de variables comme ID	Cette mesure a pour objectif de contrer un problème dans d'anciens modules de weblog qui ont été corrigés depuis. Tous les appels '*id' seront traités comme un nombre entier. Cette option vous protègera contre certaines attaques XSS et injections SQL. Conseil : activer cette option, cependant celle-ci peut perturber le fonctionnement de certains modules. Valeur par défaut : : non
Protection contre la traversée de répertoires	Elimination de « .. » pour toutes les demandes qui ressemblent à une tentative d'accès par traversée de répertoires. Valeur par défaut : oui
Anti Brute Force	Brute force est une méthode d'analyse de chiffrement dans laquelle toutes les clés possibles sont systématiquement essayées. Le terme de "brute" qualifie parfaitement cette démarche, aussi appelée "recherche exhaustive", effectuée sans grande subtilité.

Options de configuration	Explications
	Cette option empêche des attaques de ce type pour tenter une connexion en définissant le nombre de tentatives Ici vous pouvez définir le nombre de tentatives de tentatives de connexion autorisées pour un invité dans un intervalle de 10 minutes. Si quelqu'un échoue dans sa tentative au delà de ce nombre, son adresse IP sera bannie La valeur par défaut est 10
Modules à exclure du contrôle DoS/Crawler	Protector peut bannir des adresses IPs qui semblent être à l'origine d'attaques DoS (*) ou des aspirateurs qui consomment des ressources excessives. Cependant, vous pouvez exclure différents modules de cette protection en écrivant leurs noms ici. Séparez le nom de chaque module avec ce caractère |. Cette option est utile pour les modules de chat par exemple. (*) Le "Denial-of-service" ou déni de service est une attaque très évoluée visant à rendre muette une machine en la submergeant de trafic inutile
Délai de réaction aux rechargements fréquents de page	Contre-mesure pour les attaques 'touche F5' : Saisissez une valeur en secondes pour les tentatives par rechargement de page et par les aspirateurs. La valeur par défaut est de 60 secondes.
Nombre de tentatives F5 autorisées	Contre-mesure pour les attaques DoS : Cette valeur détermine le nombre de rechargements au delà duquel la connexion est considérée comme une attaque malicieuse au cours du délai fixé dans l'option ci-dessus. La valeur par défaut est 10.
Action si une attaque F5 est détectée	Sélectionner l'action à réaliser si une attaque Dos/F5 est détectée : • Aucune – enregistrer seulement • Mise en veille • Ecran blanc • Bannir l'ip (temporairement) • Bannir l'ip (définitivement). • Refus par htaccess (function expérimentale) La valeur par défaut est un écran blanc. Si vous voulez utiliser le refus par htaccess vous avez besoin de paramétrer XOOPS_ROOT_PATH/.htaccess accessible en lecture-écriture, ce qui est un risque aussi.
Nombre de tentatives pour qu'un crawler soit reconnu comme malicieux	Défense contre des crawlers-aspirateurs malicieux (comme bots chasseurs d'e-mails): La valeur détermine le nombre d'accès au delà duquel le crawler est considéré comme malicieux. La valeur par défaut est 30.
Users-Agents autorisés	Un perl regex pattern pour les User-Agent. Vous pouvez employer ceci pour empêcher Protector de réagir accidentellement contre les robots intéressants de type Google.

Options de configuration	Explications
	En cas de correspondance, le crawler n'est jamais banni La valeur par défaut est : /(msnbot|Googlebot|Yahoo! Slurp)/i
Groupes dont l'adresse IP ne sera jamais bannie	Un utilisateur qui appartient à l'un des groupes sélectionnés ne sera jamais banni. La valeur par défaut est webmasters, et il est recommandé de conserver cette option.
Désactiver les fonctions dangereuses dans XOOPS	Cette option peut être employée pour se protéger contre quelques bogues et trous connus de sécurité. C'est en grande partie approprié à de vieilles versions des xoops. La valeur par défaut est xmlrpc, les autres options sont xmlrps et quelques bugs de la 2.0.9.2 .
Activer la protection anti-XSS (BigUmbrella)	Ceci vous protège contre presque toutes les attaques par l'intermédiaire des vulnérabilités de XSS. Mais il n'est pas sur à 100%. La valeur par défaut est non, ce serait une meilleure idée de l'activer.
anti-SPAM: nombre d'URLs pour les membres	Vous pouvez fixer une limite sur le nombre d'urls qui sont tolérées dans les données d'un POST (dans un forum ou des commentaires) émis par les membres de votre site, en dehors des administrateurs. Si le message contient plus d'urls que la limite fixée il sera considéré comme du spam. La valeur par défaut est 10, pour désactiver cette fonction il suffit de mettre 0.
anti-SPAM: nombre d'URLs pour les invités	Même règle que ci-dessus mais qui s'applique aux visiteurs anonymes. La valeur par défaut est 5, pour désactiver cette fonction il suffit de mettre 0.

6. Suppléments

6.1 Sauvetage : bannissement accidentel

Si vous vous retrouvez banni de votre propre site (cela arrive au moins un fois à la plupart des gens) allez dans le répertoire XOOPS_TRUST_PATH/modules/protector/configs et supprimez les fichiers qui sont présents.

L'un d'entre eux contient les adresses IP bannies, si vous pouvez l'éditer et retirer votre adresse IP, vous pourrez retrouver l'accès à votre site.

Veuillez noter qu'en supprimant ces fichiers de configuration, cela donnera accès à tous les autres utilisateurs interdits, il est donc meilleur de pouvoir juste supprimer son adresse ip.

Dans les versions précédentes de Protector existait une fonctionnalité de récupération qui a été supprimée dans les versions 3.x de ce module.

6.2 Coté utilisateur

Ce module ne fournit pas de fonctionnalités pour les utilisateurs. Toutes les manipulations s'effectuent dans l'administration du module. Seuls les administrateurs doivent pouvoir accéder à celui-ci.

6.3 Blocs

Il n'y a pas de blocs associés avec ce module.

6.4 Templates

Ce module ne possède pas de templates.

6.5 Extensions de filtre

Deux extensions sont livrées avec le module. Pour les installer copy les fichiers situés dans le dossier XOOPS_TRUST_PATH/modules/protector/filters_disabled/ dans le dossier adjacent /filters_enabled.

postcommon_post_deny_by_rbl.php

C'est une extension anti-SPAM. Tous les posts émanant d'IPs enregistrées sur un serveur RBL(*) seront rejetées. Cette extension peut ralentir la performance des messages, notamment dans les modules de chat.
Par expérience cette installation est à manier avec précaution sous peine de voir affluer des plaintes des membres de votre site qui se retrouveraient bannis car ils utilisent, le plus souvent à leur insu, une adresse IP dynamique qui aura été bannie sur un serveur RBL
(*) Définition RBL : http://fr.wikipedia.org/wiki/Anti-spam#RBL_.28Realtime_Blackhole_List.29

Le début du fichier liste quelques adresses de serveurs RBL, celles précédées du caractère # ne sont pas actives et sont considérées comme du commentaire. Il n'est pas forcément conseillé d'activer tous les serveurs pour ne pas trop ralentir la performance de votre site lors des envois par vos membres.

postcommon_post_need_multibyte.php

C'est également une extension anti-spam mais réserve à ceux qui utilisent des caractères multi-octets comme le japonais, chinois traditionnel et simplifié, coréen. Les posts sans caractères multi-octets seront rejetés.

6.6 Paramétrage de Protecteur pour plusieurs sites

Il est possible de paramétrer ce module afin qu'il puisse gérer plusieurs sites localisés sur le même serveur. XOOPS_TRUST_PATH peut être partagé par plusieurs sites xoops.

6.7 License

Protector 3.10 est livré avec la licence GNU General Public License (GPL). Pour plus d'information sur GPL visitez : http://www.gnu.org/copyleft/gpl.html.