

NOTICE D'UTILISATION

Module Protect My Shop

Version 1.0.0

Copyright : Librasoft 2015

PRE-REQUIS

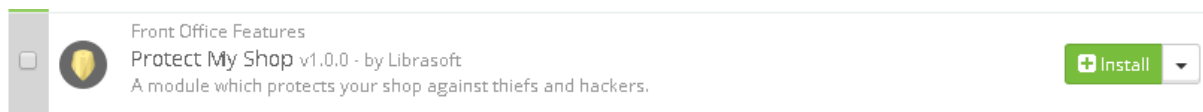
Afin d'utiliser ce module il vous faut :

- Une installation fonctionnelle de Prestashop en version 1.5 ou plus.

INSTALLATION SUR PRESTASHOP

L'installation du module sur Prestashop est très simple.

Ajoutez ou copiez le module dans votre section modules et cliquez sur Installer.



Une fois installé cliquez sur Configurer pour personnaliser le comportement du module.

Vous pouvez activer individuellement plusieurs protections :

- **Protection supplémentaire du Back-Office**
 - Cette protection met en place un accès sécurisé via .htaccess sur le back-office en utilisant le login et mot de passe que vous saisissez.
- **Protection des fichiers**
 - Cette protection empêche le téléchargement direct des fichiers jugés sensibles. Vous pouvez ajouter, modifier ou désactiver le type de fichier à protéger dans l'onglet protection des fichiers.
- **Protection des images**
 - Cette protection empêche les sites web indéliés de faire un lien vers votre serveur pour afficher vos images sur leur site web. Cela protège ainsi votre bande passante. Les moteurs de recherche ne sont pas bloqués, et peuvent accéder à vos images pour le référencement. Vous avez également la possibilité d'ajouter des exceptions si vous souhaitez autoriser un site web en particulier via l'onglet hotlinking.
- **Protection contre les injections SQL**
 - Cette protection protège votre site contre toutes les tentatives d'attaque par injection SQL. Vous pouvez, au besoin, désactiver les commandes à bloquer via l'onglet Injection SQL. De plus vous disposez de l'onglet Exception Scripts, qui vous permet de mettre en place des exceptions pour certains scripts, ou cas particulier qui pourrait être bloqués.

- **Protection contre les injections XSS**
 - Cette protection protège votre site contre toutes les tentatives d'attaque par injection XSS. Vous disposez de l'onglet Exception Scripts, qui vous permet de mettre en place des exceptions pour certains scripts, ou cas particulier qui pourrait être bloqués.
- **Protection contre les injections Commandes SHELL**
 - Cette protection protège votre site contre toutes les tentatives d'attaque par injection de commandes SHELL. Vous pouvez, au besoin, désactiver les commandes à bloquer via l'onglet Injection SHELL. De plus vous disposez de l'onglet Exception Scripts, qui vous permet de mettre en place des exceptions pour certains scripts, ou cas particulier qui pourrait être bloqués.
- **Protection contre les injections de code**
 - Cette protection protège votre site contre toutes les tentatives d'attaque par injection de code. Vous disposez de l'onglet Exception Scripts, qui vous permet de mettre en place des exceptions pour certains scripts, ou cas particulier qui pourrait être bloqués.
- **Protection contre les aspirateurs de site web**
 - Cette protection protège votre site contre tous les aspirateurs de site connus à ce jour, afin d'empêcher la copie et le vol de vos données. Vous disposez de la possibilité d'ajouter, modifier, désactiver des User-Agents dans la liste noire sur l'onglet Bad-User-Agents.
- **Protection Clic-droit de la souris**
 - Cette protection empêche l'utilisateur d'utiliser le menu du clic droit de la souris sur votre site web, qui pourrait lui permettre d'utiliser les fonctions comme « Enregistrer sous... », « Copier-Coller »...
- **Protection Copier-Coller**
 - Cette protection empêche l'utilisateur d'utiliser la fonction copier-coller du clavier. CTRL-C et CTRL-V, qui pourrait lui permettre de voler le contenu de votre site web.



Module(s) installed successfully.



Protect My Shop

[Settings](#) [Attacks History](#) [Banned Ips](#) [Files Protection](#) [Scripts Exception](#) [Hotlinking Exception](#) [Bad User-Agents](#) [Sql Injection](#) [Shell Injection](#)

⚙️ SETTINGS

Secured Access for the backoffice

☐ YES☒ NO*An additional secured access will be added to the backoffice using following login/password.*

* Administration Login

demo@librasoft-demo.fr

This is the login that will be used for the secure access of the BackOffice. For example : secureadmin

* Administration Password

🔒

This is the password that will be used for the secure access of the BackOffice. For example : mysupersecurepasswordever

Protection for your files

☐ YES☒ NO*This feature avoids direct download of all your important files (templates, binary, plugins,...).*

Protection for your pictures

☐ YES☒ NO*This feature avoids hotlinking of your pictures to preserve bandwidth.*

Protection against SQL Injection

☐ YES☒ NO*this feature blocks all SQL Injection attempts.*

Protection against XSS Injection

☐ YES☒ NO*This feature blocks all XSS Injection attempts.*

Protection against SHELL Injection

☐ YES☒ NO*This feature blocks all SHELL Injection attempts.*

Protection against CODE Injection

☐ YES☒ NO*This feature blocks all CODE Injection attempts.*

Protection against Website Grabber

☐ YES☒ NO*This feature blocks all known Website grabber that steal your data.*

Protection against Right-Click

☐ YES☒ NO*This feature blocks the right click of the mouse.*

Protection against Copy-Paste

☐ YES☒ NO*This feature blocks the copy-paste function.*

Save

FONCTIONNEMENT

Une fois les options de protection activées, le module fonctionne de façon autonome. Il détecte les tentatives d'attaques, les bloque, et redirige l'utilisateur ou le b0t vers une page lui indiquant que son attaque a été bloquée.

De plus, l'Ip de l'attaquant est ajoutée dans la liste des Ips bannies, que vous pouvez administrer via l'onglet IPs bannies. Ainsi, l'attaquant est banni de votre site web, et ne pourra plus procéder à d'autres attaques.

Un historique des attaques est disponible dans l'onglet « Historique des attaques », vous permettant le cas échéant, de mettre en place une exception de script, si un blocage s'avère être un faux positif.

QUESTIONS - REPONSES

Q : Est-ce que les b0ts légitimes comme ceux de Google sont bloqués ?

R : Non, toutes les règles de blocages prennent en compte les principaux moteurs de recherche, afin de ne pas impacter votre référencement.

Q : Une fois la protection du back office mise en place, j'ai une erreur 500, que faire ?

R : Cela peut arriver selon les politiques de sécurité de certains hébergement mutualisé. Il faut modifier manuellement le chemin du fichier .htpassword, dans le fichier .htaccess situé dans le dossier admin de votre ftp. Par exemple, chez Online.net, le chemin généré ressemble à « /flex/domain/votre_domaine/site/www/votre_dossier_admin/.htpassword », il vous faut le changer en « /www/votre_dossier_admin/.htpassword ».

Q : Sur mon site, l'utilisateur doit pouvoir télécharger des fichiers .zip, .exe etc... mais depuis l'installation du module, on est redirigé vers une erreur 403.

R : Vous pouvez choisir les types de fichiers à protéger ou non via l'onglet « Protection des fichiers ». Activez ou désactivez une extension de fichier. Ici par exemple les fichiers zips.

Q : J'utilise des modules Prestashop, qui ne fonctionnent plus depuis l'installation du module, que faire ?

R : Consultez l'historique des attaques afin de déterminer la règle qui a déclenché un blocage de votre module, puis rendez-vous dans l'onglet Exception Scripts afin d'ajouter une exception pour votre module. N'hésitez pas à nous contacter en cas de besoin pour définir une règle d'exception spécifique à votre besoin.

Q : Une IP est bloquée, et je ne souhaite pas qu'elle le soit, que faire ?

R : Allez dans l'onglet IPs bannies, et supprimer l'IP concernée. Attention, à la prochaine attaque de cette IP, elle sera à nouveau bloquée. Pour empêcher le blocage de cette IP de façon définitive, désactivez là au lieu de la supprimer.

Q : Erreur de manipulation, je me suis banni moi-même, comment faire ?

R : Connectez-vous en FTP, supprimer le .htaccess situé à la racine de votre boutique, connectez-vous au BackOffice, allez dans l'onglet IPs bannies, et supprimez votre adresse IP de la liste.