

NOTE OF USE

Module Protect My Shop

Version 1.0.0

Copyright : Librasoft 2015

PRE-REQUISITE

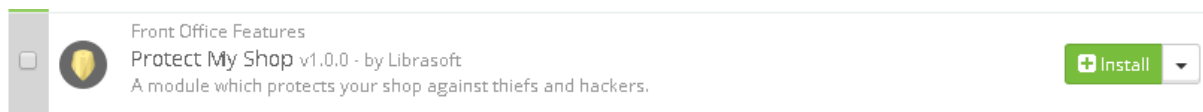
In order to use this module, you need :

- A fonctionnal Prestashop installation at least in version 1.5.

INSTALLATION ON PRESTASHOP

Installation of the module is very simple.

Simply add, or copy the module in your module section, and click on Install.



Once installed, click on Configure to personalize the way the module works.

You can activate one by one, the followings protections :

- **Additional protection of the Back-Office**
 - This protection is implementing secure access via .htaccess on the back office using the login and password that you enter.
- **File protection**
 - This protection prevents the direct download of files considered sensitive. You can add, edit, or disable the type of file to protect in the protection of the files tab.
- **Protecting images**
 - This protection prevents unscrupulous web sites that link to your server pictures they are displaying on their web site. It thus protects your bandwidth. Search engines are not blocked, and can access your images for SEO. You also have the option to add exceptions if you want to allow a particular web site via the hotlinking tab.
- **Protection against SQL injections**
 - This protects your site against all attack attempts through SQL injection. If necessary, you can disable commands to block via the SQL Injection tab. In addition you have the Exception Scripts tab, allowing you to implement exceptions for certain scripts, or particular cases which could be blocked.

- **Protection against XSS injections**
 - This protects your site against all attack attempts through XSS injection. You have the Exception Scripts tab, allowing you to implement exceptions for certain scripts, or particular case which could be blocked.
- **Protection against injections by SHELL commands**
 - This protects your site against all attack attempts by injecting SHELL commands. If necessary, you can disable commands to block via the Injection SHELL tab. In addition you have the Exception Scripts tab, allowing you to implement exceptions for certain scripts, or particular cases which could be blocked.
- **Protection against code injections**
 - This protects your site against all attack attempts throughs code injection. You have the Exception Scripts tab, allowing you to implement exceptions for certain scripts, or particular cases which could be blocked.
- **Protection against website grabber**
 - This protects your site against all known website grabber, to prevent copying and theft of your data. You have the ability to add, edit and disable User-Agents in the blacklist on the Bad-User-Agents tab.
- **Protection against right click of the mouse**
 - This protection prevents the user from using the menu of the right mouse click on your web site, which could allow him to use functions such as ' Save as... ', "Copy-paste "...
- **Protection against copy-paste function**
 - This protection prevents the user from using the function copy - paste of the keyboard. (CTRL-C and CTRL-V), which could allow him to steal the content of your web site.

✓ 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

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

his 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

USAGE

Once activated, the module operates independently. It detects the attempted attacks, blocks them, and redirects the user (or the b0t) to a page stating that his attack was blocked.

Furthermore, the Ip of the attacker is added to the list of banned Ips, you can administer them through the banned IPs tab. Thus, the attacker is banned from your web site, and will no longer carry out other attacks.

An history of attacks is available in the 'History of attacks' tab, if necessary, allowing you to implement a script exception, if block turns out to be a false positive.



QUESTIONS - ANSWERS

Q: Are the legitimate bots as Google are blocked?

A: No, all blocking rules take into account the major search engines, in order to not impacts your SEO.

Q: Once the protection of back office activated, I get a 500 error, what to do?

A: This can happen according to some shared hosting security policies. You will need to manually change the path of the file .htpassword in the .htaccess file located in the admin of your ftp folder. For example, at Online.net, the generated path looks like "[flex/domain/yourdomain/site/www/votre_dossier_admin/.htpassword](#)", you need to change it to "[www/votre_dossier_admin/.htpassword](#)".

Q: On my site, the user must be able to download files .zip, .exe etc. but since the installation of the module, you are redirected to a 403 error.

A: You can choose the types of files to protect or not via the tab "File Protection". Enable or disable a file extension. Here for example the zips files.

Q: I use Prestashop modules, that no longer work since the installation of the module, what to do?

A: See the history of the attacks to determine the rule that triggered a blocking of your module, and then go in the Exception Scripts tab to add an exception for your module. Feel free to contact us in case of need to set a specific exception to your need.

Q: An IP is blocked, and I do not wish it to be, what to do?

A: Go to the tab IPs banned, and remove the IP concerned. Beware, the next attack of this IP, it will be again blocked. To prevent the blocking of this IP permanently, unactive it instead of delete.

Q: Error handling, I am banned myself, how to do ?

A: Log in FTP, delete the .htaccess located in the root of your store, connect you to the BackOffice, go to the banned IPs tab, and remove your IP address from the list.