“Protector” Tutorial

Version 3.04

Table of Contents

"PROTECTOR" TUTORIAL **1**

TABLE OF CONTENTS **2**

PROTECTOR V 3.04 MODULE DOCUMENTATION **3**

1. FUNCTION 3
2. WHAT'S NEW IN V3.04 3
3. MODULE CREDITS & WHERE TO GET A COPY 4
4. INSTALLATION 4
5. ***UPGRADING FROM PROTECTOR V2.X*** 6
6. SETTING UP THE MODULE 6
7. THE PROTECTOR ADMINISTRATION MENU 6
   - *Protect centre (default admin page)* *6*
   - *Security advisory* *8*
   - *Fixing the security risks* *8*
   - *'register_globals': on* *8*
   - *'allow_url_fopen': on* *8*
   - *'session.use_trans_sid": on* *9*
   - *'XOOPS_DB_PREFIX' xoops* *9*
   - *'mainfile.php': missing precheck* *9*
   - *Check if Protector works well* *9*
   - *Prefix manager* *9*
   - *Changing the database table prefix* *10*
   - *Backing up your database* *10*
   - *Deleting duplicate tables* *10*
   - *Preferences* *10*
8. RESCUE: ACCIDENTAL SELF-BANNING 17
9. THE USER SIDE 17
10. BLOCKS 17
11. TEMPLATES 17
12. FILTER PLUGINS 17
    - *postcommon_post_deny_by_rbl.php* *18*
    - *postcommon_post_need_multibyte.php* *18*
13. LICENSE 18
14. ABOUT THIS DOCUMENT 18

Protector V 3.04 module documentation

1. Function

Protector is a very useful module that can help improve the security of your XOOPS site, and is widely regarded as a 'must have' module for all XOOPS websites. Protector is capable of defending against:

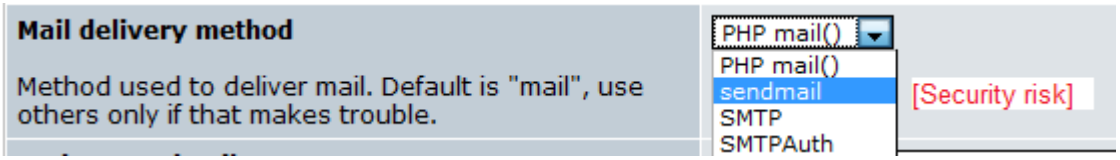
- Some kinds of denial of service (DOS) attacks, bandwidth-hungry crawlers and spambots.
- SQL injection, variable contamination, null bytes, session hijacking, and some kinds of cross-site scripting.
- Brute force attacks and directory traversals.
- Uploading of camouflaged image files and executables.
- Link and comment spammers.

Protector logs the attacking IPs and offers a range of countermeasures including IP bans, blank screens and automatic sanitisation of attempted injections etc. Protector also evaluates your site for certain vulnerabilities and providing warnings about them through a 'security advisory' page, and provides instructions on how to fix them.

2. What's new in V3.04

Version 3.04 adds a check against a recently discovered command-injection vulnerability in PHPmailer, which is one of the mail delivery options available in XOOPS.

The vulnerability specifically affects the 'Sendmail' mail delivery option (which is **not** the default). If you have Sendmail selected then Protector 3.04 will display a warning notice at the top of the screen that says: ***"phpmailer security hole! Change the preferences of mail from "sendmail" to another, or upgrade the core right now! (message by protector)"*.**



As the warning states, you can avoid this vulnerability by going to Administration => Preferences => Mail setup and selecting a different mail delivery option. Please note that

interim security patches are also available from the links below, and that the issue is slated for correction in the next minor releases of XOOPS (2.0.17 and 2.2.5).

- 2.0.16 patch: http://xoopsforge.com/mailer/xoops20-phpmailer.zip
- 2.2.0 patch: http://xoopsforge.com/mailer/xoops22-phpmailer.zip

3. Module credits & where to get a copy

The author of Protector V 3.04 is GIJOE. It is available at his website http://www.peak.ne.jp/xoops/ along with a few other cool modules and hacks (check out TinyD for an excellent and duplicatable content module). This document is based largely on text of the module README file, text available within the module admin areas and some clarifications from GIJOE.

4. Installation

Installation of the module does **not** follow the standard procedure as a few files must be modified. Additional modifications are necessary to fully implement the security improvements recommended by the module. These are covered in the Security Advisory section below, but for the moment, lets just get it installed.

1. Unzip the compressed archive and you will find two directories inside:

   /XOOPS_TRUST_PATH

   /HTML

2. Upload the **contents** of HTML into the root folder of your website. Basically you want the folder HTML/modules/protector to end up in your_site_root/modules/protector.
3. Create a new folder **outside of your website root** to serve as your 'trust path'. You can call the folder anything you like, but I'll use 'my_trust_path' in this example. If your website root is called public_html, the directory structure would probably look something like this:

   /home

   /my_account

   /public_html [this is the website root, your site is in here]

   /my_trust_path [lies outside the website root]

4. Upload the **contents** of the XOOPS_TRUST_PATH folder into my_trust_path (or whatever you have called it).
5. Change the permissions of my_trust_path/modules/protector/configs to make it writable (777, but on some servers you may be able to write with a more restrictive setting).
6. Edit mainfile.php, which is in your website root folder. You need to define XOOPS_TRUST_PATH as a new constant here by adding a new line. The value should be the physical path to the trust path folder, eg:

```
define('XOOPS_TRUST_PATH',
'/home/my_user_account/my_trust_path');
```

Add the line near the other constant definitions near the top of the file (for example, under XOOPS_ROOT_PATH). If you don't know what the physical path to your trust path folder is, you can see the directory structure in the definition for the XOOPS_ROOT_PATH constant.

7. Go to administration => system => modules and install the module. If you need detailed instructions on installing modules refer to the XOOPS Operation Guide, available from the XOOPs Documentation Site at http://xoopsdocs.net/modules/docs/.
8. You need to add two more lines to mainfile.php as per the red lines in the code example below. You will find it close to the bottom of the file. **Important:** Do not do this until **after** you have installed the module or it will not work.

```
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'
;
```

9. Installation should now be complete. Don't forget to change the permissions on mainfile.php back to read only (444), as this file contains the password to your database account!

5. *Upgrading from Protector V2.x*

Follow these steps:

1. Remove the precheck and postcheck lines for Protector from your mainfile.php.
2. Remove all files under XOOPS_ROOT_PATH/modules/protector/.
3. Upload files in the archive as per the installation procedure steps 2-5 above.
4. Go to admin => system => modules and press the 'upgrade' button for the Protector module.
5. Define the XOOPS_TRUST_PATH as per installation procedure step 6 above.
6. Add two lines for Protector into your mainfile.php, as per installation step 8 and 9 above.

6. Setting up the module

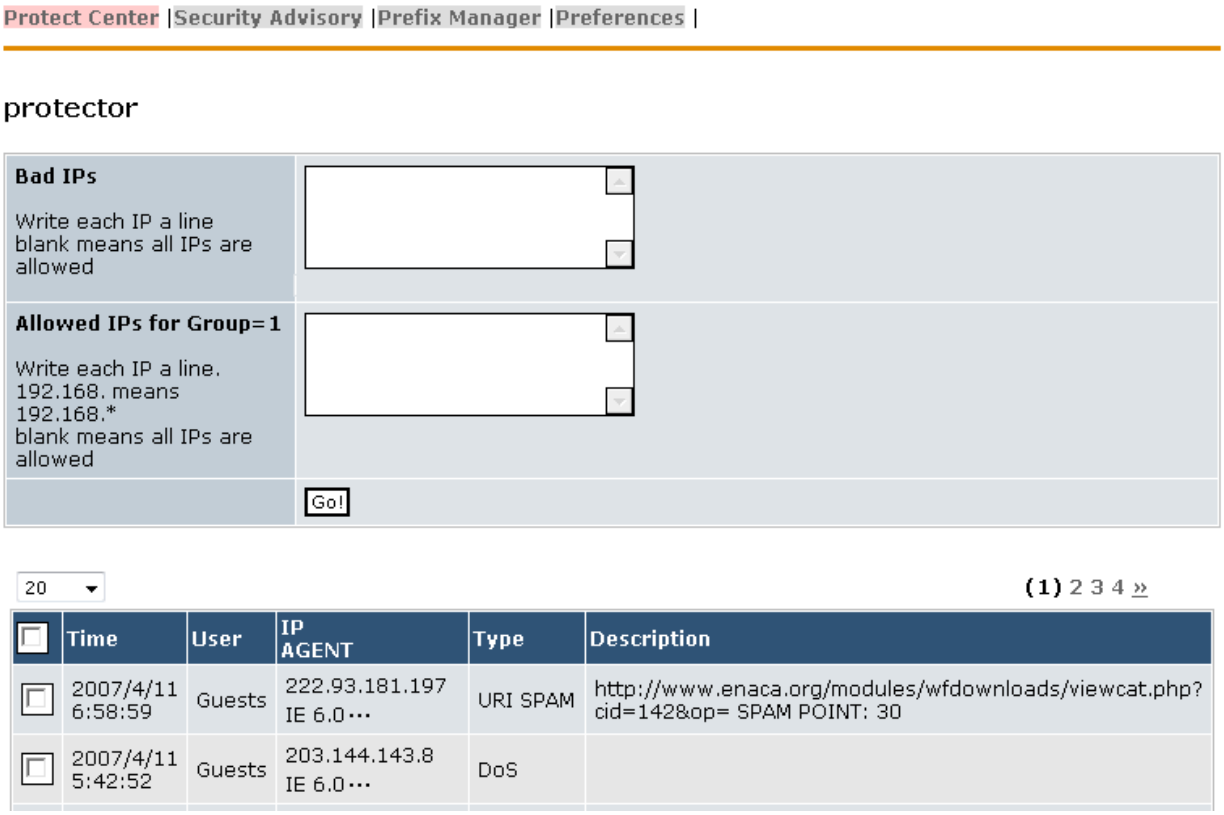
Once you have it installed, the suggested procedure for setting up this module is to:

1. Go to the preferences page and set the module preferences to the recommended state (see the table below). It is worth reading through these carefully.
2. Visit the ‘Security advisory’ section of Protector's administration area and follow the advice there to eliminate as many of the risks that are identified as you can. Details on how to implement the security fixes are described in the 'Security Advisory' section below.

7. The Protector administration menu

➢ Protect centre (default admin page)

The protect centre (below) provides a convenient tool to ban the IP numbers of computers (or people!) that are causing you problems. It also provides a list of all IPs that have been banned to date, including those banned (or at least, reacted to) by the Protector module itself in response to incidents.



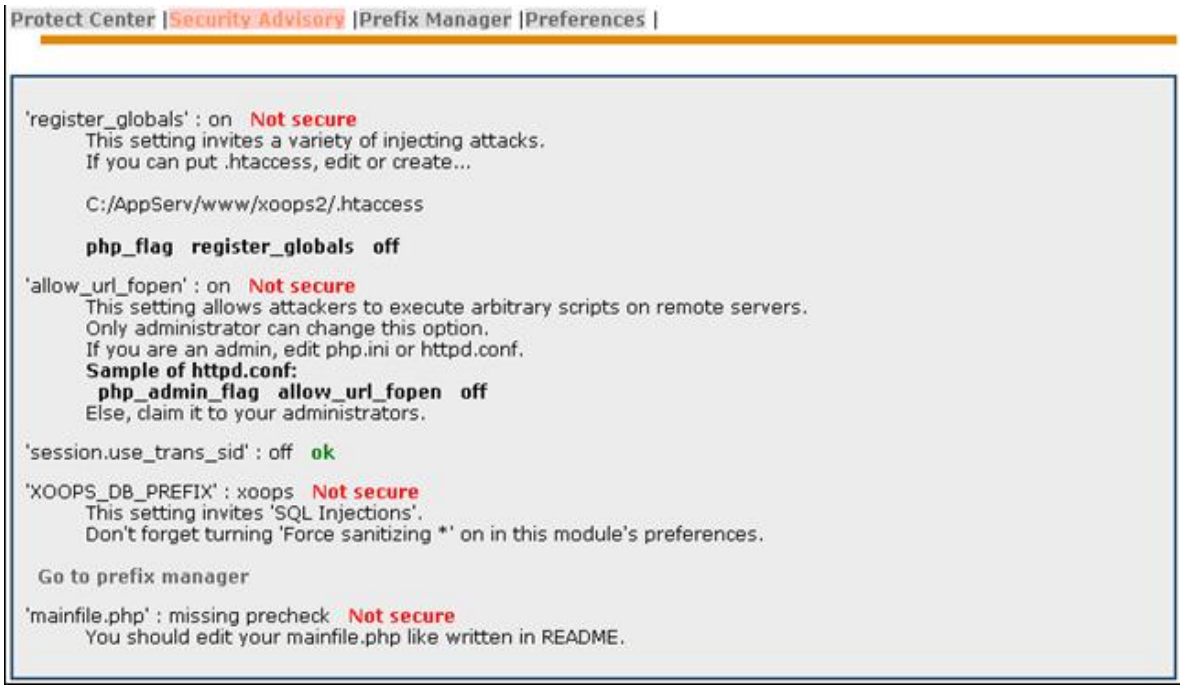
Things that you can do here are:

Option	Function
Bad IPs	You can ban the IPs of troublemakers by entering them in the box, each on a separate line. If you leave this line blank, that means all IPs are allowed.
Allowed IPs for Group=1	Enter allowed IPs for group 1 (webmasters) in this box, each on a separate line. You can allow ranges of IPs, for example entering 192.168. will allow 192.168.*
Log records	Protector keeps a log of IPs that have exceeded the limits of its security policies and triggered a response, as defined in the preferences section. Here you can see the offending IPs, and why they were listed. You can remove records by selecting the checkboxes and clicking the

	'remove' button.

Security advisory

The Security Advisory page evaluates the vulnerability of your site against several



Fixing the security risks

Follow the instructions below to implement security improvements recommended by Protector. Reload the Protect Centre page to check your progress as you go - the red warnings should turn a soothing green.

'register_globals': on

Fixing this issue is very easy. Create a text file called .htaccess. Place it in the root directory of your site. The file only needs to contain one line, as follows:

```
php_flag register_globals off
```

'allow_url_fopen': on

This setting allows attackers to execute arbitrary scripts on remote servers. Unfortunately it may be difficult for you to fix because only an administrator can change this option. If you are renting disk space from a commercial host you need to ask them to make this change for you (and frankly many hosts will refuse to modify a shared

system for your convenience). If you are lucky enough to have access, edit php.ini or httpd.conf and add (or amend) the following line to be:

```
php_admin_flag allow_url_fopen off
```

- **'session.use_trans_sid": on**

Add another line to the .htaccess file in your website root directory, as follows:

```
php_flag session.use_trans_sid off
```

- **'XOOPS_DB_PREFIX' xoops**

This is covered in the section 'Prefix manager', below.

- **'mainfile.php': missing precheck**

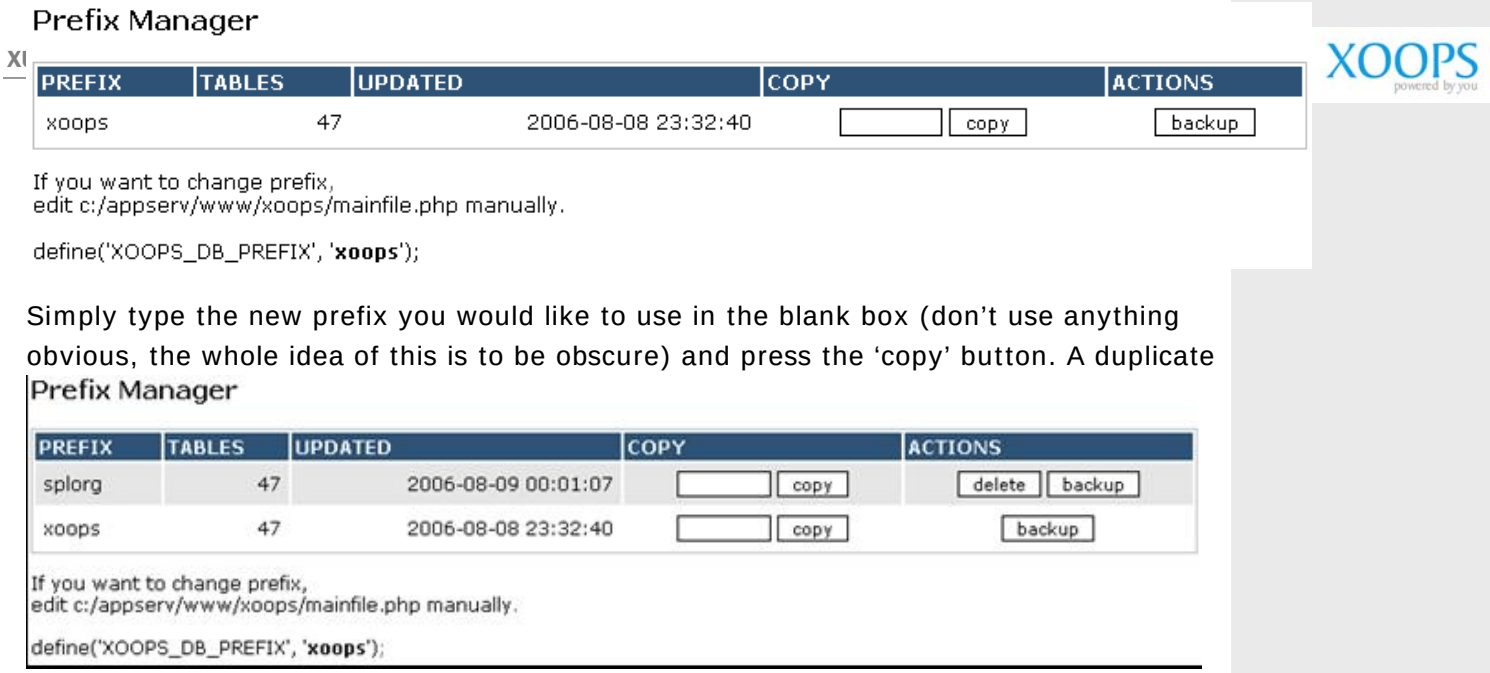
Edit your mainfile.php according to the steps described in the installation procedure (step 8). You shouldn't be seeing this warning if you followed it properly!

- **Check if Protector works well**

Click on a link to test the module – you should get booted back out to the home page, depending on how you set up your preferences. You should also see entries added to the log in the Protect Centre.

Prefix manager

The prefix manager lets you i) change the prefix of your database tables by creating copies with a new prefix of your choice and ii) backup your database. Why would you want to change the prefix? Well, by default the XOOPS installation script sets the prefix as 'xoops'. The problem with this is that it is predictable, facilitating SQL injection attacks - if an attacker finds a hole in your site it will be easier for them to interfere with your database because they will be able to guess the full table names. Changing the prefix to something other than the default makes things a bit more difficult for them.



Simply type the new prefix you would like to use in the blank box (don't use anything obvious, the whole idea of this is to be obscure) and press the 'copy' button. A duplicate

However, to actually use the new set of tables you need to edit the file **mainfile.php** in your root directory, as per the footnote in the image above. Look for the following lines:

// Table Prefix

define('XOOPS_DB_PREFIX', '**xoops**');

Change 'xoops' to whatever your new prefix is and upload your modified mainfile.php. Don't forget to CHMOD the file permissions to 444 (read only in Windows)! Once you have done that, your database will be running on the duplicate tables. Please note that any further changes in your database will not be reflected in the old tables.

- **Backing up your database**

Just press the 'backup' button and you will be prompted to download an SQL file of your database.

- **Deleting duplicate tables**

Since having duplicate sets of tables increases the size of your database so you might like to get rid of excess copies once you are sure the new set is working well. You can delete the old copies by pressing the 'delete' button (good idea to back them up locally first in case you later discover you need them). Note that you cannot delete the prefix/tables that are currently in use.

Preferences

The configuration options and recommended settings for Protector are summarised in the table below. For the most part, you can just leave the settings at the defaults.

Module configuration option	Function
Temporarily disabled (yes/no)	You can turn Protector off temporarily if you are having problems. Don't forget turn it back on when you have fixed the problem. Default is 'no'.
Reliable IPs	Enter IPs that you consider 'reliable' eg. your own. These IPs will not be banned by Protector, which can help stop you locking yourself out. Set IPs you can rely separated with | . ^ matches the head of string, $ matches the tail of string.
Logging level	Options (default is 'full') are: • None. • quiet. • Quiet (this is quieter than 'quiet'). • Full.

Module configuration option	Function
Protected IP bits for the session	This is an anti session hijacking measure that limits how far IP bits can move within a session. • Default 32 bit - all bits are protected (IP cannot change). • If you have a dynamic IP that moves within a known range, you can set the number of protected bits to roughly match. • For example, if your IP can move in the range of 192.168.0.0 to 192.168.0.255, set 24 bit here. If a cracker knew your session IP but tried to access from outside this range (say 192.168.2.50) they would fail. The author of the module suggests 16 bit as a balanced value for general use.
Groups not allowed to move their IP in a session	Anti session hijacking measure. Selected groups are not permitted to change their IP in a session. The default is 'webmasters' and it is recommended to leave it that way as the consequences of an administrator's session getting hijacked could be quite severe.
Sanitizing null-bytes	The terminating character "\0" is often used in malicious attacks. A null-byte will be changed to a space if this option is on (which is the default, and it is highly recommended to leave it this way).
Exit if bad files are uploaded (yes/no)	If someone tries to upload files which have risky extensions like .php , Protector exits XOOPS. If you often attach php files into B-Wiki or

	PukiWikiMod you may need to turn this off to avoid problems.
Action if contamination is found	Select the action when someone tries to contaminate system global variables into your XOOPS. Options are: • None – only logging. • Blank screen. • Ban the IP. The recommended option is blank screen (default).
Action if an isolated comment-in is found	Anti SQL injection measure. Select the action when an isolated "/*" is found. Options are: • None (only logging). • Sanitizing. • Blank screen. • Ban the IP. "Sanitizing" means adding another "*/" in the tail, and is the recommended option. However the default is 'none (only logging)'. You might want to change this.

Module configuration option	Function
Action if a UNION is found	Anti SQL injection measure. Select the action when the UNION syntax of SQL is found. Options are: • None (only logging). • Sanitizing. • Blank screen. • Ban the IP. "Sanitizing" means changing "union" to "uni-on". This is the default and recommended option.
Force intval to variables like id	This measure was to guard against a problem in an older weblog module, which has since been patched. All requests with names such as "*id" will be treated as integers. This option protects you from some kind of XSS and SQL Injections. It is recommended to turn this option on, but it can cause problems with some modules. The default is 'off'.
Protection from Directory Traversals	This setting eliminates ".." from all requests that look like attempted directory traversals. Options are to turn this on (yes) or off (no). The default setting is on.
Anti Brute Force	Here you can set the number of times you allow guests to try to login with 10 minutes. If someone fails to login in excess of this limit their IP will be banned. This prevents people mounting brute force attacks against logins. The default value is 10.
Modules out of DoS/Crawler checker	Protector can ban IPs that seem to be mounting DoS attacks or crawlers that

	consume excessive resources (see below). However, you can exclude individual modules from this protection by entering their directory names here. Separate multiple modules with a | character. This option is useful for things like chat modules.
Watch time for high loadings (sec)	This value specifies the watch time for high / frequent reloading (F5 attack) and high loading crawlers. The default is 60 seconds.
Bad counts for F5 Attack	Measure against DoS attacks. This value specifies the number of reloads (within the watch period above) that must be made before an IP is considered to be making a malicious attack. The default 10.
Action against F5 Attack	What do you want to do when an F5/DoS attack is detected? Options are: • None (only logging). • Sleep. • Blank screen. • Ban the IP. • Deny by htaccess (an experimental feature). The default response is a blank screen. If you want to use the deny by htaccess feature you need to set XOOPS_ROOT_PATH/.htaccess as writable. However, please note that this entails some risk in itself.
Module configuration option	**Function**
Bad counts for crawlers	Measure against high loading web crawlers or bots. The value set here specifies the number of access attempts that can be made before a crawler is considered to be 'badly behaved', ie.

	consuming too many resources. The default is 30 reloads.
Action against high loading crawlers	What do you want to do when a 'bad' crawler is detected? Options are: • None (only logging). • Sleep. • Blank screen. • Ban the IP. • Deny by htaccess (experimental feature). The default response is a blank screen.
Welcomed User-Agent	A perl regex pattern for User-Agent. You can use this to prevent Protector from accidentally reacting against 'good'crawlers, such as those from Google. If it matches, the crawler is never considered as a high loading crawler. The default is: /(msnbot|Googlebot|Yahoo! Slurp)/i
Groups never registered as Bad IP	A user who belongs to the group specified here will never be banned. The default is 'webmasters', and it is recommended to leave it this way.
Disable dangerous features in XOOPS	This option can be used to protect against some known bugs and security holes. This is largely relevant to old versions of xoops as these have been closed in recent versions (if you are running an old version of XOOPS you should consider upgrading it). The default is xmlrpc, other options are xmlrps + 2.0.9.2 bugs, or none.
enable anti-XSS (BigUmbrella)	This protects you from some attacks via cross-site scripting (XSS) vulnerabilities. But it is not 100% . The default is no

	(off), probably a good idea to turn it on.
anti-SPAM: URLs for normal users	You can set a limit on how many URLs will be tolerated in POST data from registered users (eg. in forum posts and comments) other than administrators. If the POST contains too many URLs it is considered to be spam. The default is 10. If you want to disable this feature, set it as 0.
anti-SPAM: URLs for guests	As above, but for anonymous (guest) users. The default in this case is 5. Set it to 0 if you want to disable this feature.

8. Rescue: Accidental self-banning

If you somehow manage to ban yourself from your own site (most people seem to achieve this at least once :) go to XOOPS_TRUST_PATH/modules/protector/configs and delete the files in there. One of them contains the 'banned IP' data so getting rid of it (or better, editing it to remove your own IP) will restore your access to the site. Note that deleting it will also restore access of all other banned users, so editing it is a better idea if you aren't in a hurry.

In previous versions of Protector there was a facility to set a “rescue password”, but this has been removed in V3.

9. The user side

There is no user-side functionality associated with this module. All interaction is through the administration side. Only site administrators should have access to this module.

10. Blocks

There are no blocks associated with this module (there were in earlier versions, but no longer).

11. Templates

There are no user-side templates associated with this module.

12. Filter plugins

There are two plugins distributed with the module. To install them, copy the files in XOOPS_TRUST_PATH/modules/protector/filters_disabled/ into the adjacent /filters_enabled folder.

- **postcommon_post_deny_by_rbl.php**

An anti-SPAM plugin. All posts from IPs registered within RBL will be rejected. This plugin can slow the performance of posts, especially in chat modules.

- **postcommon_post_need_multibyte.php**

An anti-spam plugin that only works for multibyte Japanese, Traditional Chinese, Simplified Chinese and Korean language sites. Basically, posts without multi-byte characters will be rejected.

13. License

Protector V3.04 is released under the GNU General Public License (GPL). For more information about the GPL visit: http://www.gnu.org/copyleft/gpl.html.

14. About this document