Sysadmins of the North - httpBL{} class

httpBL{} class readme

<?php echo 'How to use httpbl.class.php'; ?>

Contents

Sysadmins of the North - httpBL{} class

Introduction

Why this PHP class

As a system administrator for the webhosting company VEVIDA, I deal with unwanted HTTP traffic on a daily basis. Customer websites are hacked, comment forms and forums are flooded with spam, and so on.

There are quite a few blacklists available, but for as far as I know most are intended for SMTP traffic, not HTTP. Two of such HTTP blacklists which do exists, are Project Honey Pot and StopForumSpam. A lot of "offending" IP addresses are listed in these blacklists, so why not use them? Both blacklists offer *Application Programming Interfaces* or API's, to query their databases. Also, both have lists of written implementations, or plugins; here and here, contributed by the community.

One thing I missed (or couldn't find) is an implementation which can use **both** databases, and offers support for the creation of a local blacklist. This local blacklist can be used to reduce remote lookups and decreases the load on both external databases. So I decided to create such an implementation.

The blacklist can be used with either **IIS 7** and **7.5** *IP Address and Domain Restrictions* module, stored in a *web.config* file, or stored in a flat text file for use with *.htaccess* files. Both **Helicon ISAPI_Rewrite 3** and **Apache mod_rewrite** support a **RewriteMap** directive, therefor the blacklist and usage should be **cross platform**.

About Project Honey Pot

Project Honey Pot is the first and only distributed system for identifying spammers and the spambots they use to scrape addresses from your website. Using the Project Honey Pot system you can install addresses that are custom-tagged to the time and IP address of a visitor to your site. If one of these addresses begins receiving email we not only can tell that the messages are spam, but also the exact moment when the address was harvested and the IP address that gathered it.

Project Honey Pot was created by Unspam Technologies, Inc — an anti-spam company with the singular mission of helping design and enforce effective anti-spam laws.

About StopForumSpam

We provide lists of spammers that persist in abusing forums and blogs with their scams, ripoffs, exploits and other annoyances*. We provide these lists so that you don't have to endure the never ending job of having to moderate, filter and delete their rubbish.

We provide a "free for use" site where you can check registrations and posts against our database. We list known forum and blog spammers, including IP and email addresses, usernames, how busy they are and, in some cases, evidence of their spam.

Sysadmins of the North - httpBL{} class

Configuration and file locations

The PHP class httpBL requires a number of files. They are described in detail here.

- **Config.ini**: this file holds the configuration settings and the file should therefor be placed in a location where the webserver cannot read. For VEVIDA, this is the database folder. The path to the config.ini file is defined on line 6 in httpbl.class.php:

  ```
  public $configfile = "path/to/config.ini”;
  ```

The config.ini configuration file uses the php.ini syntax. This means every line starting with a semi colon (;) is a comment and is ignored.

In the config.ini file, a few settings MUST BE SET:

- Blfileloc - location of the blacklist.txt file
- Bllogfileloc - location of the blacklist log file
- webconfigFile - location of the web.config file, if available
- use_webconfigFile - use web.config or not (1 or 0)
- PHPaccesskey - Project Honey Pot accesskey (**mandatory!**)
- SFSaccesskey - StopForumSpam accesskey (**mandatory!**)
- minDayinBl - number of days since last activity (read API documentation)
- minThreatLevel - minimal threat level (read API documentation)

the **blacklist.txt** file and its **logfile** (I called it *bl_log*.txt) should both be placed in the same location as **config.ini**, so it cannot be read by the web server. The **web.config** file is only for usage with IIS 7 / 7.5. Place the file **httpbl.class.php** in the webroot, so it can be included in your **.php** files.

All files (blacklist.txt, bl_log.txt, and web.config) **have to be writable!**

Usage

We need to include het httpbl.class.php file in our .php files and fire up the class:

```
require_once(‘httpbl.class.php’);
$mybl = new httpBL();
```

You can use the **ipcheck.php** script to test the class, or simply use the functions:

- `_retrieve_IP_address_status_SFP()`
- `_retrieve_IP_address_status_PHP()`
- `_retrieve_remote_IP_address()`

```
if($mybl->_retrieve_IP_address_status_SFP($mybl->_retrieve_remote_IP_address()) &&
($mybl->_retrieve_IP_address_status_PHP($mybl->_retrieve_remote_IP_address())))
{
	// IP address is listed, so block it or show them a nice message
	header("HTTP/1.0 403 Forbidden"); die();
}
```

The function **$mybl->_retrieve_remote_IP_address()** looks up the visitors IP address, which then is run through the functions **$mybl->_retrieve_IP_address_status_SPF** (look up in StopForumSpam database), and **$mybl->_retrieve_IP_address_status_PHP** (look up in Project Honey Pot database).

Logic

The logic behind all is as follows:

1. a visitor visits your website;
2. The IP address of the visitor is looked up in the local blacklist.txt file and (if set up) web.config file
    a. IP address found? Block the visitor and log the visit attempt
    b. IP address not found? Look up the IP address in StopForumSpam and Project Honey Pot databases
3. If the IP adress is found in either one of the databases:
    a. write the IP address in the local blacklist.txt file and (if set up) web.config file
    b. log the visit attempt.
    c. block the visitor

When the web.config file is in use, there is nothing more you have to do. A visitor will receive the 403 Forbidden message automatically by IIS.

If web.config is not in use, and Helicon ISAPI_Rewrite or Apache mod_rewrite is, you have to set up a **RewriteMap** configuration. This is explained on this page (in Dutch, but you'll get the idea):

- ISAPI_Rewrite als soort van Web Application Firewall (WAF)

Open the .htaccess file and change the line starting with "RewriteMap" to reflect your situation. Save the file and upload it to your webroot.

As said before, this **should** be cross platform compatible between Helicontech ISAPI_Rewrite and Apache mod_rewrite's **.htaccess files**.

The RewriteMap only has to be defined once in your **.htaccess** file, it'll reread the blacklist.txt file when a new entry is written to it.

Sysadmins of the North - httpBL{} class

Disclamer and support

The files and code are “AS IS”. It functions quite well in my various test environments, and live here on http://www.saotn.nl. Yes, you are monitored ;-). I cannot, and will not, guarantee it’ll function in your specific environment. I cannot be held responsible or liable for any damages caused by these scripts. Use them on your own risc.

Change line 70 in httpbl.class.php to query different blacklists, for instance bl.spamcop.net, cbl.abuseat.org or zen.spamhaus.org.

For what it’s worth:
Project Honey Pot and StopForumSpam are great initiatives in my opinion. If you decide to use this PHP class, and you register on both websites for API-keys, **please support them by making a donation**. Also, give them some exposure on your website, for instance in a blog post. Thank you.