

```
order allow,deny
deny from 89.69.121.189
deny from 89.72.154.41
deny from 5.9.2.67
deny from 5.255.253.67
deny from 5.248.247.173
deny from 31.146.244.60
deny from 212.129.43.127
deny from 62.4.27.67
deny from 188.240.88.17
#deny from 195.154.43.217
#deny from 195.242.115.171
#deny from 193.151.106.171
deny from 155.133.18.167
deny from 95.135.145.205
#deny from 46.149.89.212
#deny from 46.149.87.25
#deny from 46.149.82.33
#deny from 46.149.92.160
#deny from 46.119.122.226
deny from 23.95.128.112
deny from 23.95.197.29
deny from 23.94.163.39
deny from 23.95.197.79
deny from 198.23.179.174
allow from all
```

```
##
# @package Joomla
# @copyright Copyright (C) 2005 - 2013 Open Source Matters. All rights reserved.
# @license GNU General Public License version 2 or later; see LICENSE.txt
##
```

```
##
# READ THIS COMPLETELY IF YOU CHOOSE TO USE THIS FILE!
#
# The line just below this section: 'Options +FollowSymLinks' may cause problems
# with some server configurations. It is required for use of mod_rewrite, but may already
# be set by your server administrator in a way that disallows changing it in
# your .htaccess file. If using it causes your server to error out, comment it out (add #
+-
```

```
10
# beginning of line), reload your site in your browser and test your self url's. If they
work,
# it has been set by your server administrator and you do not need it set here.
##

## Can be commented out if causes errors, see notes above.
Options +FollowSymLinks

## Mod_rewrite in use.

RewriteEngine On

## Begin - Rewrite rules to block out some common exploits.
# If you experience problems on your site block out the operations listed below
# This attempts to block the most common type of exploit 'attempts' to Joomla!
#
# Block out any script trying to base64_encode data within the URL.
RewriteCond %{QUERY_STRING} base64_encode(?:.*) [OR]
# Block out any script that includes a <script> tag in URL.
RewriteCond %{QUERY_STRING} (<|%)3C(?:.*)+cript.*(%)3E [NC,OR]
# Block out any script trying to set a PHP GLOBALS variable via URL.
RewriteCond %{QUERY_STRING} GLOBALS(=| \[| \[0-9A-Z]{0,2}) [OR]
# Block out any script trying to modify a _REQUEST variable via URL.
RewriteCond %{QUERY_STRING} _REQUEST(=| \[| \[0-9A-Z]{0,2})
# Return 403 Forbidden header and show the content of the root homepage
RewriteRule .* index.php [F]
#
## End - Rewrite rules to block out some common exploits.

## Begin - Custom redirects
#
# If you need to redirect some pages, or set a canonical non-www to
# www redirect (or vice versa), place that code here. Ensure those
# redirects use the correct RewriteRule syntax and the [R=301,L] flags.
#
## End - Custom redirects

##
# Uncomment following line if your webserver's URL
# is not directly related to physical file paths.
# RewriteRule /(.*) /$1 [R=301,L]
```

```
# Update Your Joomla! Directory (just / for root).
##

# RewriteBase /

## Begin - Joomla! core SEF Section.
#
RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
#
# If the requested path and file is not /index.php and the request
# has not already been internally rewritten to the index.php script
RewriteCond %{REQUEST_URI} !^/index\.php
# and the request is for something within the component folder,
# or for the site root, or for an extensionless URL, or the
# requested URL ends with one of the listed extensions
RewriteCond %{REQUEST_URI} /component/|(|/[^\.]*)\.(php|html?!feed|pdf|vcf|raw))$ [NC]
# and the requested path and file doesn't directly match a physical file
RewriteCond %{REQUEST_FILENAME} !-f
# and the requested path and file doesn't directly match a physical folder
RewriteCond %{REQUEST_FILENAME} !-d
# internally rewrite the request to the index.php script
RewriteRule .* index.php [L]
#
## End - Joomla! core SEF Section.
php_flag display_errors off
php_value display_errors 0
php_value error_reporting 30711

Redirect 302 /filtr http://dostavka24.cn.ua/zavedenia
```