```
php_value memory_limit 32M
RewriteEngine on
RewriteCond %{HTTP_HOST} ^www.zazki-pezki.ru
RewriteRule ^(.*)$ http://zazki-pezki.ru/$1 [R=301,L]

# Web Optimizer options
<IfModule mod_rewrite.c>
  RewriteEngine On
  RewriteBase /
  RewriteRule ^(.*)\.wo[0-9]+\.(js|php)$ $1.$2
  RewriteRule ^(.*)\.wo[0-9]+\.(jpe?g|png)$ $1.$2
</IfModule>
# Web Optimizer end
AddDefaultCharset utf-8
AddCharset utf-8 *

##
# @version $Id: htaccess.txt 21064 2011-04-03 22:12:19Z dextercowley $
# @package Joomla
# @copyright Copyright (C) 2005 - 2010 Open Source Matters. All rights reserved.
# @license http://www.gnu.org/copyleft/gpl.html GNU/GPL
# Joomla! is Free Software
##


#####################################################
#  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 dissallows changing it in
# your .htaccess file.  If using it causes your server to error out, comment it out (add #
to
# beginning of line), reload your site in your browser and test your sef 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!
#
## Deny access to extension xml files (uncomment out to activate)
#<Files ~ "\.xml$">
#Order allow,deny
#Deny from all
#Satisfy all
#</Files>
## End of deny access to extension xml files
# Block out any script trying to set a mosConfig value through the URL
RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z_]{1,21}(=|\%3D) [OR]
# 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)([^s]*s)+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.
#  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 root, or for an extensionless URL, or the
# requested URL ends with one of the listed extensions
RewriteCond %{REQUEST_URI} (/[^.]*|\.(php|html?|feed|pdf|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
```