

```
##
# 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 #
# to
# 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

# disable the server signature
ServerSignature Off

# disable directory browsing
Options All -Indexes
# enable directory browsing
#Options All +Indexes

# prevent folder listing
IndexIgnore *

## 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`
#
# 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(?:.*) [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 read for a REQUEST_URI variable via URL
```

```
# 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.

RewriteCond %{REQUEST_FILENAME} !-d
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-l

RewriteRule ^(.+)$ index.php?url=$1 [QSA,L]
```