```
#

# @copyright Copyright 2003-2012 Zen Cart Development Team
# @license http://www.zen-cart.com/license/2_0.txt GNU Public License V2.0

# @version GIT: $Id: Author: DrByte  Wed Jul 4 15:04:12 2012 -0400 Modified in v1.5.1 $
#

# This is used with Apache WebServers

#

# The following blocks direct HTTP requests to all filetypes in this directory recursively, except certain approved exceptions

# It also prevents the ability of any scripts to run. No type of script, be it PHP, PERL or whatever, can normally be executed if ExecCGI is disabled.

# Will also prevent people from seeing what is in the dir. and any sub-directories

#

# For this to work, you must include either 'All' or at least: 'Limit' and 'Indexes' parameters to the AllowOverride configuration in your apache/conf/httpd.conf file.

# Additionally, if you want the added protection offered by the OPTIONS directive below, you'll need to add 'Options' to the AllowOverride list, if 'All' is not specified.

# Example:

#<Directory "/usr/local/apache/htdocs">

#  AllowOverride Limit Options Indexes

#</Directory>

###############################

# deny *everything*

<FilesMatch ".*">
```

```
<FilesMatch ".*">

  Order Allow,Deny

  Deny from all

</FilesMatch>

# but now allow just *certain* necessary files:

<FilesMatch ".*\.(js|css|jpg|JPG|gif|GIF|png|PNG|cur)$">
  Order Allow,Deny

  Allow from all

</FilesMatch>

IndexIgnore */*
```