```
#
# @copyright Copyright 2003-2016 Zen Cart Development Team
# @license http://www.zen-cart.com/license/2_0.txt GNU Public License V2.0
# @version GIT: $Id: Author: DrByte  Modified in v1.6.0 $
#
# 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.
# Example:
#<Directory "/usr/local/apache/htdocs">
#  AllowOverride Limit Indexes
#</Directory>
################################

# deny *everything*
<FilesMatch ".*\..*">
  <IfModule mod_authz_core.c>
    Require all denied
  </IfModule>
  <IfModule !mod_authz_core.c>
    Order Allow,Deny
    Deny from all
  </IfModule>
</FilesMatch>

# but now allow just *certain* necessary files:
<FilesMatch "(?i).*\.(js|css|jpg|gif|png|html|pdf)$">
  <IfModule mod_authz_core.c>
    Require all granted
  </IfModule>
  <IfModule !mod_authz_core.c>
    Order Allow,Deny
    Allow from all
  </IfModule>
```

```
  </IfModule>
</FilesMatch>

IndexIgnore */*
```