

```
#
# @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 Tue Aug 28 16:48:39 2012 -0400 New 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.
# Example:
#<Directory "/usr/local/apache/htdocs">
# AllowOverride Limit Options Indexes
#</Directory>
#####

<Limit GET POST PUT>
  <IfModule mod_authz_core.c>
    Require all denied
  </IfModule>
  <IfModule !mod_authz_core.c>
    Order Allow,Deny
    Deny from all
  </IfModule>
</Limit>

## NOBODY SHOULD BE SNOOPING IN THIS FOLDER

# 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>
```

```
deny from all
</IfModule>
</FilesMatch>

IndexIgnore */*
```