

```
#
# @copyright Copyright 2003-2010 Zen Cart Development Team
# @license http://www.zen-cart.com/license/2_0.txt GNU Public License V2.0
# @version $Id: .htaccess 16111 2010-04-29 22:39:02Z drbyte $
#
# 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>
#####
```

## DirectoryIndex index.php

```
# prevents inappropriate browsing
<FilesMatch ".*\..*">
    Order Allow,Deny
    Deny from all
</FilesMatch>
<FilesMatch "(^$|^favicon.ico$|.*\.(php|js|css|jpg|gif|png|html)$)">
    Order Allow,Deny
    Allow from all
</FilesMatch>
```

## IndexIgnore \*/\*

```
# Older versions of the mod_security extension in apache may cause "406" errors to appear
during installation.
# If you are running into such problems, simply remove the # from the beginning of the
following lines.
```

Following lines:

```
#SecFilterEngine off
```

```
#SecFilterScanPOST Off
```