

```
#

# @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 16954 2010-07-21 22:55:30Z 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>

#####

# #####
```

```
# deny everything*
```

```
<FilesMatch ".*">
```

```
Order Allow,Deny
```

```
Deny from all
```

```
</FilesMatch>
```

```
# but now allow just certain necessary files:
```

```
<FilesMatch ".*\.(mp3|mp4|swf|avi|mpeg|wmv|rm|ra|ram|wmv|epub)$" >
```

```
Order Allow,Deny
```

```
Allow from all
```

```
# tell all downloads to automatically be treated as "save as" instead of launching in an application directly
```

```
# (just uncomment the next 2 lines by removing the '#');
```

```
# ForceType application/octet-stream
```

```
# Header set Content-Disposition attachment
```

```
</FilesMatch>
```

```
IndexIgnore /*
```

```
## NOTE: If you want even greater security to prevent hackers from running scripts in this folder, uncomment the following line (if your hosting company will allow you to use OPTIONS):
```

```
# OPTIONS -Indexes -ExecCGI
```