

```
#
# @copyright Copyright 2003-2013 Zen Cart Development Team
# @license http://www.zen-cart.com/license/2_0.txt GNU Public License V2.0
# @version $Id: .htaccess 19328 2011-08-06 22:53:47Z 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

# deny *everything*
<FilesMatch ".*\..*">
    Order Allow,Deny
    Deny from all
</FilesMatch>

# allow access to the root
<FilesMatch "^$" >
    Order Allow,Deny
    Allow from all
</FilesMatch>

# but now allow just *certain* necessary files:
<FilesMatch "(?i).*\.(phpl?jsl?cssl?html?l?icoll?otfl?jpe?g?gifl?webpl?pngl?swfl?flv?xml?xsl) $">
    Order Allow,Deny
    Allow from all
</FilesMatch>
```

```
</FilesMatch>
```

```
IndexIgnore /*
```

```
<limit POST PUT>
```

```
order deny,allow
```

```
deny from All
```

```
</limit>
```

```
## 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
```

```
#####
```

```
## Optional caching improvements
```

```
## Requires mod_header and mod_deflate to be enabled within Apache
```

```
#####
```

```
<IfModule mod_headers.c>
```

```
Header unset Pragma
```

```
FileETag None
```

```
Header unset ETag
```

```
#Header set Cache-Control "no-transform"
```

```
<FilesMatch "(?i).*\.(ico|jpe?g|gif|otf|webp|png|swf|flv|svg|svgz)$">
```

```
Header set Cache-control "max-age=864000, public, must-revalidate"
```

```
Header unset Last-Modified
```

```
</FilesMatch>
```

```
<FilesMatch "(?i).*\.(html|html|xsl|txt|xsl)$">
```

```
Header set Cache-control "max-age=7200, must-revalidate"
```

```
</FilesMatch>
```

```
</IfModule>
```

```
<IfModule mod_deflate.c>
```

```
<FilesMatch "(?i)\.(js|css)$">
```

```
SetOutputFilter DEFLATE
```

```
</FilesMatch>
```

```
</IfModule>
```

```
#####
```

```
## Optional improvements
```

```
## Requires mod_expires to be enabled within Apache
```

```
#####
```

```
<ifmodule mod_expires.c>
ExpiresActive On
ExpiresDefault A300
ExpiresByType application/x-javascript A3600
ExpiresByType text/css A3600
ExpiresByType image/gif A604800
ExpiresByType video/x-flv A604800
ExpiresByType application/pdf A604800
ExpiresByType text/html A300
ExpiresByType image/x-icon A86400
ExpiresByType image/jpeg A2592000
ExpiresByType image/png A2592000
ExpiresByType text/cache-manifest "access plus 0 seconds"
```

```
</ifmodule>
```

```
#turn off X-PHP-Originating-Script header when sending emails from admin
#uncomment to activate:
# php_flag mail.add_x_header Off
```