

## Common HTACCESS File Directives for WordPress

.HTACCESS files are used in UNIX based web servers to provide instructions to a web server that are in addition to the server's configuration. The most common usage for this in WordPress is to enable permalinks. Permalinks are a feature that "rewrite" the traditional WordPress URLs to more user and search engine friendly ones. A typical WordPress URL will look like <http://www.myblog.com/?P=1> to ones like <http://www.myblog.com/my-first-post>.

WordPress also uses the HTACCESS directives to do things like give your blog a WWW or non-WWW extension. For example, <http://myblog.com> versus <http://www.myblog.com>. This is known as canonicalization in search engine terms.

The standard WordPress HTACCESS file will have the following entry:

```
# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
</IfModule>
# END WordPress
```

### Other HTACCESS Common Entries

Many configurations of Apache (web server) will have a line in them for providing special instructions for the interoperation of PHP version 4 and PHP version 5. If yours has it in there, this is fine:

```
AddHandler php5-script .php
```

### WordPress Plugins

Some WordPress Plugins will put additional directives in the main HTACCESS file or they will place their own HTACCESS file in their plugin directory. WP-SuperCache is

a performance plugin that puts a lot of information in the HTACCESS file. When I first saw this, all of the references to mobile phone names really caught my attention. This is all fine, however, as they simply get mobile users to the right place. If you are running WP-SuperCache, you will have this big entry in your HTACCESS file:

```
# BEGIN supercache <IfModule mod_mime.c>
<FilesMatch "\.html\.gz$">
ForceType text/html
FileETag None
</FilesMatch>
AddEncoding gzip .gz
AddType text/html .gz
</IfModule>

RewriteCond %{HTTP_USER_AGENT} !^.*(2.0\
MMP|240x320|400X240|AvantGo|BlackBerry|Blazer|Cellphone|Danger|DoCoMo|E
laine/3.0|EudoraWeb|Googlebot-
Mobile|hiptop|IEMobile|KYOCERA/WX310K|LG/U990|MIDP-2.|MMEF20|MOT-
V|NetFront|Newt|Nintendo\ Wii|Nitro|Nokia|Opera\ Mini|Palm|PlayStation\
Portable|portalmmm|Proxinet|ProxiNet|SHARP-TQ-GX10|SHG-
i900|Small|SonyEricsson|Symbian\ OS|SymbianOS|TS21i-
10|UP.Browser|UP.Link|webOS|Windows\ CE|WinWAP|YahooSeeker/M1A1-
R2D2|iPhone|iPod|Android|BlackBerry9530|LG-TU915\ Obigo|LGE\
VX|webOS|Nokia5800).*
<IfModule mod_deflate.c>
SetEnvIfNoCase Request_URI \.gz$ no-gzip
</IfModule>
<IfModule mod_headers.c>
Header set Vary "Accept-Encoding, Cookie"
Header set Cache-Control 'max-age=300, must-revalidate'
</IfModule>
<IfModule mod_expires.c>
ExpiresActive On
ExpiresByType text/html A300
</IfModule>
# END supercache
```

## Individual Plugin Directories

Many plugins will place their own HTACCESS file in the top of their own plugin directory. Though the reasons can vary, I have placed a couple of common ones so you can see what they look like.

### WP-DBBackup

```
<Files ~ ".*\..*">
order allow,deny
deny from all
</Files>
```

### Si-Captcha

```
deny from all
```

## Evil Usage of a 301 Redirect

So, if all of these HTACCESS files and plugin entries are OK, what is it that you should be looking for? In short, a 301 redirect to a site you don't know. These look like:

```
redirectMatch 301 ^(.*)$ http://www.domain.com
```

or

```
redirectMatch permanent ^(.*)$ http://www.domain.com
```

or

```
redirect 301 /index.html http://www.domain.com/index.html
```

or

```
redirect permanent /index.html http://www.domain.com/index.html
```

If you find these in any HTACCESS file in your site and the domain that they are redirecting to has nothing to do with a WordPress plugin or just doesn't seem right, then you potentially have a problem. They also might be using trickery just to direct a USER\_AGENT or a search engine robot to another domain but not your visitors.