

```
# -----
# UTF-8 encoding
# -----

# use utf-8 encoding for anything served text/plain or text/html
AddDefaultCharset utf-8

# force utf-8 for a number of file formats
AddCharset utf-8 .html .css .js .xml .json .rss

# "-Indexes" will have Apache block users from browsing folders without a default document
# Usually you should leave this activated, because you shouldn't allow everybody to surf
# through
# every folder on your server (which includes rather private places like CMS system
# folders).
Options -Indexes

# If your server is not already configured as such, the following directive
# should be uncommented in order to set PHP's register_globals option to OFF.
# This closes a major security hole that is abused by most XSS (cross-site
# scripting) attacks. For more information: http://php.net/register\_globals
#
# IF REGISTER_GLOBALS DIRECTIVE CAUSES 500 INTERNAL SERVER ERRORS :
#
# Your server does not allow PHP directives to be set via .htaccess. In that
# case you must make this change in your php.ini file instead. If you are
# using a commercial web host, contact the administrators for assistance in
# doing this. Not all servers allow local php.ini files, and they should
# include all PHP configurations (not just this one), or you will effectively
# reset everything to PHP defaults. Consult www.php.net for more detailed
# information about setting PHP directives.

php_flag register_globals Off

# -----
# Start rewrite engine
# -----

# Turning on the rewrite engine is necessary for the following rules and features.
#
# If you are using a commercial web host, contact the administrators for assistance in
# doing this. Not all servers allow local .htaccess files, and they should
# include all Apache configurations (not just this one), or you will effectively
# reset everything to Apache defaults. Consult www.apache.org for more detailed
# information about setting Apache directives.
```

```
<!DOCTYPE mod_rewrite.c>
```

```
RewriteEngine On
```

```
# Block access to "hidden" directories whose names begin with a period. This  
# includes directories used by version control systems such as Subversion or Git.
```

```
RewriteRule "(^/)\." - [F,L]
```

```
#####
```

```
#          GENERAL REWRITES          #
```

```
#####
```

```
#-----#
```

```
#          GENERAL NOTES          #
```

```
#-----#
```

```
# We use [S=X] to skip the next X RewriteRules when a condition is met so #  
# if you add or edit anything, take this into account.                    #
```

```
#-----#
```

```
# All environmental variables we might want to use in the engine have the #  
# prefix REWRITE_, so we can easily scoop them out of $_SERVER in PHP     #
```

```
#-----#
```

```
# If you think this is groovy, check this out:                            #
```

```
#          http://www.webmasterworld.com/apache/3208525.htm #
```

```
#-----#
```

```
#-----#
```

```
#          Flag certain IPs as Trusted          #
```

```
#-----#
```

```
# Always flag local IPs as trusted          #
```

```
#-----#
```

```
SetEnvIf Remote_Addr ^192\.168\.1\. REWRITE_TRUSTED_IP=true
```

```
SetEnvIf Remote_Addr ^127\.0\.0\.[1-7]$ REWRITE_TRUSTED_IP=true
```

```
#-----#
```

```
#-----#
```

```
# Redirected everything that is an existing file and part of the public #  
# dir is directed straight to the existing file.                        #
```

```
#-----#
```

```
RewriteCond %{REQUEST_URI} !^/$ [OR]
```

```
RewriteCond %{REQUEST_URI} !^/_/(.*)
```

```
RewriteCond %{DOCUMENT_ROOT}%{REQUEST_URI} -f
```

```
RewriteRule .? - [QSA,L,E=REWRITE_SOURCE:REAL_FILE,E=_REDIRECT:yes]
```

```
#-----#
```

```

#-----#
#           Get the client-requested full URI and full query string           #
#-----#
RewriteCond %{THE_REQUEST} ^[A-Z]{3,9}\ (/(?:^?)*)(\?(?:\ |)*)?\ HTTP/
RewriteRule .? - [E=REWRITE_URI:%1,E=REWRITE_QUERYSTRING:%2]
#-----#

#-----#
# Make sure pages that have already been rewritten are not rewritten again. #
#-----#
RewriteCond %{ENV:_REDIRECT} ^yes$ [OR]
RewriteCond %{ENV:REDIRECT_STATUS} 200
RewriteRule .? - [L]
#-----#

#-----#
# Redirected everything that is an existing file and part of the public #
# directory to the engine. This alternative to passing straight through #
# gives us the possibility to do things in PHP, like authentication for #
# sensitive JS files, minification, cache control, newer versions etc. #
#
#-----#
RewriteCond %{REQUEST_URI} !^/$
RewriteCond %{REQUEST_URI} !^/backoffice/(.*)
RewriteCond %{DOCUMENT_ROOT}%{ENV:REWRITE_URI} -f
RewriteRule .? - [E=REWRITE_SOURCE:REAL_FILE,E=_REDIRECT:yes,S=4]
#-----#

#-----#
#           redirect calls to the homepage           #
#-----#
RewriteCond %{REQUEST_URI} ^(/)$
RewriteRule .* - [E=REWRITE_SOURCE:FRONT_PAGE,E=_REDIRECT:yes,S=3]
#-----#

#-----#
# Images that are to be resized are also redirected to the enige, #
# which calls a resize script #
#-----#
RewriteCond %{REQUEST_FILENAME} ^/resize/. *(.jpg|.gif|.png)

```

```
    RewriteRule .? - [E=REWRITE_SOURCE: IMAGE_RESIZE, E=_REDIRECT: yes, S=1]
#-----#

#-----#
#           Set the source if not already set           #
#-----#
    RewriteCond %(ENV: REWRITE_SOURCE) ^$
    RewriteRule .? - [E=REWRITE_SOURCE: EVERYTHING_ELSE, E=_REDIRECT: yes]
#-----#

#-----#
#           Redirected everything to the engine           #
#-----#
# this includes any URL pointing to a non-existing file. This is based on #
# the assumption that the engine checks file extensions and reports an #
# useful 404!                                           #
#-----#
    RewriteRule ^(.*)$ index.php [L, QSA]
#-----#
```

</IfModule>

#EOF