# 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>

# but now allow just *certain* necessary files:
<FilesMatch "(^/favicon.ico$|.*\.(php|js|css|jpg|gif|png)$)"
  Order Allow,Deny
  Allow from all
</FilesMatch>

IndexIgnore /*/

# The following makes adjustments to the SSL protocol for Internet Explorer browsers
<IfModule mod_setenvif.c>
  #ifdef SSL
IfDefine SSL
    SetEnvIf User-Agent ".*MSIE.*" \
        nokeepalive ssl-unclean-shutdown \
        downgrade-1.0 force-response-1.0
</IfDefine>
</IfModule>

# Fix certain PHP values

#<IfModule mod_php4.c>
#  php_value session.use_trans_sid 0
#  php_value register_globals 1
#</IfModule>

# to turn off register_globals
# php_value register_globals 0

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