

```
# BEGIN WordPress
```

```
<IfModule mod_rewrite.c>  
RewriteEngine On  
RewriteBase /  
RewriteRule ^index\.php$ - [L]  
RewriteCond %{REQUEST_FILENAME} !-f  
RewriteCond %{REQUEST_FILENAME} !-d  
RewriteRule . /index.php [L]  
</IfModule>
```

```
# END WordPress
```

```
#Charset
```

```
AddCharset utf-8 .html .css .php  
AddType application/rss+xml; charset=utf-8 .rss
```

```
#DIR index
```

```
DirectoryIndex index.php
```

```
# Redirect www urls to non-www
```

```
RewriteEngine on  
RewriteCond %{HTTP_HOST} !^YOURDOMAIN\.COM  
RewriteRule (.*) http://YOURDOMAIN.COM/$1 [R=301,L]
```

```
# Block the include-only files.
```

```
<IfModule mod_rewrite.c>  
RewriteEngine On  
RewriteBase /  
RewriteRule ^wp-admin/includes/ - [F,L]  
RewriteRule !^wp-includes/ - [S=3]  
RewriteRule ^wp-includes/[^/]+\.(php)$ - [F,L]  
RewriteRule ^wp-includes/js/tinymce/langs/.+\.php - [F,L]  
RewriteRule ^wp-includes/theme-compat/ - [F,L]  
</IfModule>
```

```
##To protect against script injections and attempts to modify PHP's global and request vari.
```

```
<IfModule mod_rewrite.c>  
RewriteCond %{QUERY_STRING} (\<| %3C). *script. *(\>| %3E) [NC,OR]  
RewriteCond %{QUERY_STRING} GLOBALS(=| \[| \)| %0-9A-Z){0,2} [OR]  
RewriteCond %{QUERY_STRING} _REQUEST(=| \[| \)| %0-9A-Z){0,2}  
RewriteRule .* index.php [F,L]
```

```
</IfModule>
```

```
</ITModule>
```

```
# Securing any HTACCESS file
```

```
<files ~ "^.*\.(.Hh|.Tt|.Aa)">
```

```
order allow,deny
```

```
deny from all
```

```
satisfy all
```

```
</files>
```

```
# Deny Access to WPconfig
```

```
<files wp-config.php>
```

```
order allow,deny
```

```
deny from all
```

```
</files>
```

```
# Deny Access to XMLRPC
```

```
<Files xmlrpc.php>
```

```
Order Allow,Deny
```

```
Deny from all
```

```
</Files>
```

```
## deny directory browsing
```

```
Options All -Indexes
```

```
## deny folder listing
```

```
IndexIgnore *
```

```
## prevent mime based attacks
```

```
Header set X-Content-Type-Options "nosniff"
```

```
## Don't allow any pages to be framed - Defends against CSRF - CLICKJACKING
```

```
Header set X-Frame-Options DENY
```

```
RewriteBase /
```

```
# Against Narsty site rippers/bots/etc
```

```
# useragents starting with
```

```
RewriteCond %{HTTP_USER_AGENT} ^atraxbot [NC,OR]
```

```
RewriteCond %{HTTP_USER_AGENT} ^Azureus [NC,OR]
```

```
RewriteCond %{HTTP_USER_AGENT} ^geohasher [NC,OR]
```

```
RewriteCond %{HTTP_USER_AGENT} ^PycURL [NC,OR]
```

```
RewriteCond %{HTTP_USER_AGENT} ^Python-urllib [NC,OR]
```

```
RewriteCond %{HTTP_USER_AGENT} ^research-scan-bot [NC,OR]
```

```
RewriteCond %{HTTP_USER_AGENT} ^[a-zA-Z0-9-]*bot [NC,OR]
```

RewriteCond %{HTTP_USER_AGENT} ^Sospider [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Wget [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^xenu [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^.*casper [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^.*goblox [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^.*sun4u [NC]
RewriteCond %{HTTP_USER_AGENT} BlackWidow [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Bot\ mailto:craftbot@yahoo.com [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ChinaClaw [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Custo [NC,OR]
RewriteCond %{HTTP_USER_AGENT} DISCo [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Download\ Demon [NC,OR]
RewriteCond %{HTTP_USER_AGENT} EirGrabber [NC,OR]
RewriteCond %{HTTP_USER_AGENT} EmailSiphon [NC,OR]
RewriteCond %{HTTP_USER_AGENT} EmailWolf [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Express\ WebPictures [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ExtractorPro [NC,OR]
RewriteCond %{HTTP_USER_AGENT} EyeNetIE [NC,OR]
RewriteCond %{HTTP_USER_AGENT} FlashGet [NC,OR]
RewriteCond %{HTTP_USER_AGENT} GetRight [NC,OR]
RewriteCond %{HTTP_USER_AGENT} GetWeb! [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Go! Zilla [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Go-Ahead-Got-It [NC,OR]
RewriteCond %{HTTP_USER_AGENT} GrabNet [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Grafula [NC,OR]
RewriteCond %{HTTP_USER_AGENT} HMView [NC,OR]
RewriteCond %{HTTP_USER_AGENT} HTTrack [NC,OR]
RewriteCond %{HTTP_USER_AGENT} HTTrack [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Image\ Stripper [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Image\ Sucker [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Indy\ Library [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Indy\ Library [NC,OR]
RewriteCond %{HTTP_USER_AGENT} InterGET [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Internet\ Ninja [NC,OR]
RewriteCond %{HTTP_USER_AGENT} JOC\ Web\ Spider [NC,OR]
RewriteCond %{HTTP_USER_AGENT} JetCar [NC,OR]
RewriteCond %{HTTP_USER_AGENT} LeechFTP [NC,OR]
RewriteCond %{HTTP_USER_AGENT} MIDown\ tool [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Mass\ Downloader [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Mister\ PiX [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Navroad [NC,OR]

RewriteCond %{HTTP_USER_AGENT} NearSite [NC, OR]
RewriteCond %{HTTP_USER_AGENT} NetAnts [NC, OR]
RewriteCond %{HTTP_USER_AGENT} NetSpider [NC, OR]
RewriteCond %{HTTP_USER_AGENT} NetZIP [NC, OR]
RewriteCond %{HTTP_USER_AGENT} Net\ Vampire [NC, OR]
RewriteCond %{HTTP_USER_AGENT} Octopus [NC, OR]
RewriteCond %{HTTP_USER_AGENT} Offline\ Explorer [NC, OR]
RewriteCond %{HTTP_USER_AGENT} Offline\ Navigator [NC, OR]
RewriteCond %{HTTP_USER_AGENT} PageGrabber [NC, OR]
RewriteCond %{HTTP_USER_AGENT} Papa\ Foto [NC, OR]
RewriteCond %{HTTP_USER_AGENT} ReGet [NC, OR]
RewriteCond %{HTTP_USER_AGENT} RealDownload [NC, OR]
RewriteCond %{HTTP_USER_AGENT} SiteSnagger [NC, OR]
RewriteCond %{HTTP_USER_AGENT} SmartDownload [NC, OR]
RewriteCond %{HTTP_USER_AGENT} SuperBot [NC, OR]
RewriteCond %{HTTP_USER_AGENT} SuperHTTP [NC, OR]
RewriteCond %{HTTP_USER_AGENT} Surfbot [NC, OR]
RewriteCond %{HTTP_USER_AGENT} Teleport\ Pro [NC, OR]
RewriteCond %{HTTP_USER_AGENT} TurnitinBot [NC, OR]
RewriteCond %{HTTP_USER_AGENT} VoidEYE [NC, OR]
RewriteCond %{HTTP_USER_AGENT} WWWOFFLE [NC, OR]
RewriteCond %{HTTP_USER_AGENT} WebAuto [NC, OR]
RewriteCond %{HTTP_USER_AGENT} WebCopier [NC, OR]
RewriteCond %{HTTP_USER_AGENT} WebFetch [NC, OR]
RewriteCond %{HTTP_USER_AGENT} WebGo\ IS [NC, OR]
RewriteCond %{HTTP_USER_AGENT} WebLeacher [NC, OR]
RewriteCond %{HTTP_USER_AGENT} WebReaper [NC, OR]
RewriteCond %{HTTP_USER_AGENT} WebSauger [NC, OR]
RewriteCond %{HTTP_USER_AGENT} WebStripper [NC, OR]
RewriteCond %{HTTP_USER_AGENT} WebWhacker [NC, OR]
RewriteCond %{HTTP_USER_AGENT} WebZIP [NC, OR]
RewriteCond %{HTTP_USER_AGENT} Web\ Image\ Collector [NC, OR]
RewriteCond %{HTTP_USER_AGENT} Web\ Sucker [NC, OR]
RewriteCond %{HTTP_USER_AGENT} Website\ Quester [NC, OR]
RewriteCond %{HTTP_USER_AGENT} Website\ extractor [NC, OR]
RewriteCond %{HTTP_USER_AGENT} Widow [NC, OR]
RewriteCond %{HTTP_USER_AGENT} Xaldon\ WebSpider [NC, OR]
RewriteCond %{HTTP_USER_AGENT} Zeus [NC, OR]
RewriteCond %{HTTP_USER_AGENT} archiverloader [NC, OR]
RewriteCond %{HTTP_USER_AGENT} casper [NC, OR]
RewriteCond %{HTTP_USER_AGENT} clshhttp [NC, OR]

```
RewriteCond %{HTTP_USER_AGENT} cmsworldmap [NC,OR]
RewriteCond %{HTTP_USER_AGENT} curl [NC,OR]
RewriteCond %{HTTP_USER_AGENT} diavol [NC,OR]
RewriteCond %{HTTP_USER_AGENT} dotbot [NC,OR]
RewriteCond %{HTTP_USER_AGENT} eCatch [NC,OR]
RewriteCond %{HTTP_USER_AGENT} email [NC,OR]
RewriteCond %{HTTP_USER_AGENT} extract [NC,OR]
RewriteCond %{HTTP_USER_AGENT} flicky [NC,OR]
RewriteCond %{HTTP_USER_AGENT} grab [NC,OR]
RewriteCond %{HTTP_USER_AGENT} harvest [NC,OR]
RewriteCond %{HTTP_USER_AGENT} jakarta [NC,OR]
RewriteCond %{HTTP_USER_AGENT} java [NC,OR]
RewriteCond %{HTTP_USER_AGENT} kmccrew [NC,OR]
RewriteCond %{HTTP_USER_AGENT} larbin [NC,OR]
RewriteCond %{HTTP_USER_AGENT} libwww [NC,OR]
RewriteCond %{HTTP_USER_AGENT} miner [NC,OR]
RewriteCond %{HTTP_USER_AGENT} nikto [NC,OR]
RewriteCond %{HTTP_USER_AGENT} pavuk [NC,OR]
RewriteCond %{HTTP_USER_AGENT} pcBrowser [NC,OR]
RewriteCond %{HTTP_USER_AGENT} planetwork [NC,OR]
RewriteCond %{HTTP_USER_AGENT} pycurl [NC,OR]
RewriteCond %{HTTP_USER_AGENT} python [NC,OR]
RewriteCond %{HTTP_USER_AGENT} scan [NC,OR]
RewriteCond %{HTTP_USER_AGENT} skygrid [NC,OR]
RewriteCond %{HTTP_USER_AGENT} takeOut [NC,OR]
RewriteCond %{HTTP_USER_AGENT} wget [NC,OR]
RewriteCond %{HTTP_USER_AGENT} winhttp [NC]
## Note: The final RewriteCond must NOT use the [OR] flag.
## Return 403 Forbidden error.
RewriteRule .* - [F]

## Disallow PHP Easter Eggs (can be used in fingerprinting attacks to determine
## your PHP version). See http://www.0php.com/php_easter_egg.php and
## http://osvdb.org/12184 for more information
RewriteCond %{QUERY_STRING} \=PHPI[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}
RewriteRule .* - [F,L]

## Deny POST requests sent through proxies
RewriteCond %{REQUEST_URI} !^(search/|site-search/|wp-login.php|wp-admin/|wp-access/plugins
RewriteCond %{REQUEST_METHOD} =POST
RewriteCond %{HTTP:VIA}%{HTTP:FORWARDED}%{HTTP:USERAGENT_VIA}%{HTTP:X_FORWARDED_FOR}%{HTTP:F
```

```

RewriteCond %{HTTP: XPROXY_CONNECTION} %{HTTP: HTTP_PC_REMOTE_ADDR} %{HTTP: HTTP_CLIENT_IP} !^$
RewriteRule .* - [F,NS,L]

## Deny bogus graphic exploits
RewriteCond %{HTTP: Content-Disposition} \.php [NC]
RewriteCond %{HTTP: Content-Type} image/.+ [NC]
RewriteRule .* - [F,NS,L]

# Anti SQL injections, RFI, base64 etc etc
RewriteCond %{QUERY_STRING} [a-zA-Z0-9]=http:// [OR]
RewriteCond %{QUERY_STRING} [a-zA-Z0-9]=(\.\.//?)+ [OR]
RewriteCond %{QUERY_STRING} [a-zA-Z0-9]=/([a-z0-9_ ]//?)+ [NC,OR]
RewriteCond %{QUERY_STRING} \=PHPI[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12} [NC,OR]
RewriteCond %{QUERY_STRING} (\.\.//|\.\.\/) [OR]
RewriteCond %{QUERY_STRING} ftp\: [NC,OR]
RewriteCond %{QUERY_STRING} http\: [NC,OR]
RewriteCond %{QUERY_STRING} https\: [NC,OR]
RewriteCond %{QUERY_STRING} \=| |w| [NC,OR]
RewriteCond %{QUERY_STRING} ^(.*)/self/(.*)$ [NC,OR]
RewriteCond %{QUERY_STRING} ^(.*)cPath=http://(.*)$ [NC,OR]
RewriteCond %{QUERY_STRING} (<| %3C) .*script.*(>| %3E) [NC,OR]
RewriteCond %{QUERY_STRING} (<| %3C)([^\s]*)+cript.*(>| %3E) [NC,OR]
RewriteCond %{QUERY_STRING} (<| %3C) .*iframe.*(>| %3E) [NC,OR]
RewriteCond %{QUERY_STRING} (<| %3C)([^\i]*)+frame.*(>| %3E) [NC,OR]
RewriteCond %{QUERY_STRING} base64_encode.*\(.*) [NC,OR]
RewriteCond %{QUERY_STRING} base64_(en|de)code[^\(\)[^\(\^)]*\ [NC,OR]
RewriteCond %{QUERY_STRING} GLOBALS(=| \[| \| %)[0-9A-Z]{0,2} [OR]
RewriteCond %{QUERY_STRING} _REQUEST(=| \[| \| %)[0-9A-Z]{0,2} [OR]
RewriteCond %{QUERY_STRING} ^.*(\\|\/| |<|>).* [NC,OR]
RewriteCond %{QUERY_STRING} (NULL|OUTFILE|LOAD_FILE) [OR]
RewriteCond %{QUERY_STRING} (\.\.//|\.\.\/|\.\.\/)+(\.motd|etc|bin) [NC,OR]
RewriteCond %{QUERY_STRING} (localhost|loopback|127\.\.0\.\.1) [NC,OR]
RewriteCond %{QUERY_STRING} (<|>|'| %0A| %0D| %27| %3C| %3E| %00) [NC,OR]
RewriteCond %{QUERY_STRING} concat\([^\)]*\ [NC,OR]
RewriteCond %{QUERY_STRING} union\([^\s]*)+select [NC,OR]
RewriteCond %{QUERY_STRING} union\([^\a]*a)+1\([^\s]*)+select [NC,OR]
RewriteCond %{QUERY_STRING} (;|<|>|'| | \)| %0A| %0D| %22| %27| %3C| %3E| %00).*
(&| \*| union| select| insert| drop| delete| update| cast| create| char| convert| alter| declare| order| scr
[NC,OR]
RewriteCond %{QUERY_STRING} (sp_executesql) [NC]
RewriteRule ^(.*)$ - [F,L]

```

```
# BEGIN Expire headers
```

```
<ifModule mod_expires.c>
```

```
ExpiresActive On
```

```
ExpiresDefault "access plus 5 seconds"
```

```
ExpiresByType image/x-icon "access plus 2592000 seconds"
```

```
ExpiresByType image/jpeg "access plus 2592000 seconds"
```

```
ExpiresByType image/png "access plus 2592000 seconds"
```

```
ExpiresByType image/gif "access plus 2592000 seconds"
```

```
ExpiresByType application/x-shockwave-flash "access plus 2592000 seconds"
```

```
ExpiresByType text/css "access plus 604800 seconds"
```

```
ExpiresByType text/javascript "access plus 216000 seconds"
```

```
ExpiresByType application/javascript "access plus 216000 seconds"
```

```
ExpiresByType application/x-javascript "access plus 216000 seconds"
```

```
ExpiresByType text/html "access plus 600 seconds"
```

```
ExpiresByType application/xhtml+xml "access plus 600 seconds"
```

```
</ifModule>
```

```
# END Expire headers
```

```
# BEGIN Cache-Control Headers
```

```
<ifModule mod_headers.c>
```

```
<filesMatch "\.(ico|jpe?g|png|gif|swf)$">
```

```
Header set Cache-Control "public"
```

```
</filesMatch>
```

```
<filesMatch "\.(css)$">
```

```
Header set Cache-Control "public"
```

```
</filesMatch>
```

```
<filesMatch "\.(js)$">
```

```
Header set Cache-Control "private"
```

```
</filesMatch>
```

```
<filesMatch "\.(x?html?|php)$">
```

```
Header set Cache-Control "private, must-revalidate"
```

```
</filesMatch>
```

```
</ifModule>
```

```
# END Cache-Control Headers
```

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

```
AddOutputFilterByType DEFLATE application/javascript
```

```
AddOutputFilterByType DEFLATE application/rss+xml
```

```
AddOutputFilterByType DEFLATE application/vnd.ms-fontobject
```

```
AddOutputFilterByType DEFLATE application/x-font
```

```
AddOutputFilterByType DEFLATE application/x-font-opentype
AddOutputFilterByType DEFLATE application/x-font-otf
AddOutputFilterByType DEFLATE application/x-font-truetype
AddOutputFilterByType DEFLATE application/x-font-ttf
AddOutputFilterByType DEFLATE application/x-javascript
AddOutputFilterByType DEFLATE application/xhtml+xml
AddOutputFilterByType DEFLATE application/xml
AddOutputFilterByType DEFLATE font/opentype
AddOutputFilterByType DEFLATE font/otf
AddOutputFilterByType DEFLATE font/ttf
AddOutputFilterByType DEFLATE image/svg+xml
AddOutputFilterByType DEFLATE image/x-icon
AddOutputFilterByType DEFLATE text/css
AddOutputFilterByType DEFLATE text/html
AddOutputFilterByType DEFLATE text/javascript
AddOutputFilterByType DEFLATE text/plain
```

```
</IfModule>
```

```
# GZIP ENABLED
```

```
<ifModule mod_gzip.c>
```

```
mod_gzip_on Yes
```

```
mod_gzip_dechunk Yes
```

```
mod_gzip_item_include file \.(html?|txt|css|js|php|pl)$
```

```
mod_gzip_item_include handler ^cgi-script$
```

```
mod_gzip_item_include mime ^text/.*
```

```
mod_gzip_item_include mime ^application/x-javascript.*
```

```
mod_gzip_item_exclude mime ^image/.*
```

```
mod_gzip_item_exclude rspheader ^Content-Encoding:.*gzip.*
```

```
</ifModule>
```