

```
#####
# WP htaccess Boilerplate #
#####

### https://github.com/Creare/WP-htaccess/

#####
# Security #
#####

### Recognise SSL when set at a load balancer/proxy level (for CloudFlare)
SetEnvIf X-Forwarded-Proto https HTTPS=on

### Prevent wp-config.php from being loaded:
<files wp-config.php>
    order allow,deny
    deny from all
</files>

### Prevent sftp-config.json from being loaded:
<files sftp-config.json>
    order allow,deny
    deny from all
</files>

### Protect .htaccess
<Files ~ "^.*\.([Hh][Tt][Aa])">
    order allow,deny
    deny from all
    satisfy all
</Files>

### Secure wp-includes
<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-support/ - [F,L]
```

```
RewriteRule wp-includes/theme-compat/ - [F,L]

# block user enumeration
RewriteCond %{QUERY_STRING} (^|&)author=
RewriteRule . http://%(SERVER_NAME)/? [L]

RewriteRule ^wp-login.php?loginkey=TmV3dG9u&redirect_to=http://%(SERVER_NAME)/wp-admin/index.php [L]
RewriteRule ^recover-password wp-login.php?loginkey=TmV3dG9u&action=lostpassword

RewriteCond %{HTTP_REFERER} !^http://%(SERVER_NAME)/wp-admin
RewriteCond %{HTTP_REFERER} !^http://%(SERVER_NAME)/wp-login\.php

RewriteCond %{QUERY_STRING} !^loginkey=TmV3dG9u
RewriteCond %{QUERY_STRING} !^action=logout
RewriteCond %{QUERY_STRING} !^action=lostpassword
RewriteCond %{REQUEST_METHOD} !POST
RewriteRule ^wp-login\.php http://%(SERVER_NAME)/? [R,L]

RewriteCond %{QUERY_STRING} ^loggedout=true
RewriteRule . http://%(SERVER_NAME)/? [L]

</IfModule>

### Prevent directory browsing
<IfModule mod_autoindex.c>
    Options -Indexes
</IfModule>

### Prevent this .htaccess from being accessed:
<files .htaccess>
    order allow,deny
    deny from all
</files>

### Prevent WordPress' readme.html from being accessed (as it contains the version number)
<files readme.html>
Deny from all
</files>

### Disable HTTP Trace
```

```

RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^TRACE
RewriteRule .* - [F]

### Block access to hidden files & directories
<IfModule mod_rewrite.c>
    RewriteCond %{SCRIPT_FILENAME} -d [OR]
    RewriteCond %{SCRIPT_FILENAME} -f
    RewriteRule "(^|/)\." - [F]
</IfModule>

### Block access to source files
<FilesMatch "(^#.#|\. (bak|config|dist|fla|incl|ini|log|psd|sh|sql|sw[op])| (^)$">
    Order allow,deny
    Deny from all
    Satisfy All
</FilesMatch>

#####
# Default Wordpress Settings #
#####

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

# END WordPress

<ifModule mod_deflate.c>
    AddOutputFilterByType DEFLATE text/html text/xml text/css text/plain
    AddOutputFilterByType DEFLATE image/svg+xml application/xhtml+xml application/xml
    AddOutputFilterByType DEFLATE application/rdf+xml application/rss+xml
application/atom+xml
    AddOutputFilterByType DEFLATE text/javascript application/javascript application/x-
javascript application/json

```

```
AddOutputFilterByType DEFLATE application/x-font-ttf application/x-font-otf
AddOutputFilterByType DEFLATE font/truetype font/opentype
</ifModule>
```

*# 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 10 seconds"
  ExpiresByType application/xhtml+xml "access plus 10 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*

*# BEGIN Turn ETags Off*

```
FileETag None
```

```
# END Turn ETags Off
```

```
# no follow robots
```

```
Header set X-Robots-Tag "noindex, nofollow"
```

```
#####
```

```
# File Format Support #
```

```
#####
```

```
### Add support for SVG and HTC
```

```
AddType image/svg+xml svg svgz
```

```
AddEncoding gzip svgz
```

```
AddType text/x-component .htc
```