```
# 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

#Protect wpconfig file
<Files wp-config.php>
  order allow,deny
  deny from all
</Files>

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

# Disable xmlrpc.php access except for Automattic
# https://wordpress.org/support/topic/htaccess-configure-to-allow-jetpack-only

<Files xmlrpc.php>
  Order Deny,Allow
  Deny from all
  Allow from 76.74.254.*
  Allow from 216.151.209.*
  Allow from 69.174.248.*
  Allow from 66.135.48.*
  Allow from 76.74.255.*
  Allow from 216.151.209.*
  Allow from 216.151.210.*
  Allow from 76.74.248.*
  Allow from 207.198.*
  Allow from 207.198.101.*
  Allow from 198.181.*
```

Allow from 198.101.*
Allow from 207.198.101.*
Allow from 192.0.64.*
Allow from 192.0.65.*
Allow from 192.0.66.*
Allow from 192.0.67.*
Allow from 192.0.68.*
Allow from 192.0.69.*
Allow from 192.0.70.*
Allow from 192.0.71.*
Allow from 192.0.72.*
Allow from 192.0.73.*
Allow from 192.0.74.*
Allow from 192.0.75.*
Allow from 192.0.76.*
Allow from 192.0.77.*
Allow from 192.0.78.*
Allow from 192.0.79.*
Allow from 192.0.80.*
Allow from 192.0.81.*
Allow from 192.0.82.*
Allow from 192.0.83.*
Allow from 192.0.84.*
Allow from 192.0.85.*
Allow from 192.0.86.*
Allow from 192.0.87.*
Allow from 192.0.88.*
Allow from 192.0.89.*
Allow from 192.0.90.*
Allow from 192.0.91.*
Allow from 192.0.92.*
Allow from 192.0.93.*
Allow from 192.0.94.*
Allow from 192.0.95.*
Allow from 192.0.96.*
Allow from 192.0.97.*
Allow from 192.0.98.*
Allow from 192.0.99.*
Allow from 192.0.100.*
Allow from 192.0.101.*
Allow from 192.0.102.*

```
  Allow from 192.0.103.*
  Allow from 192.0.104.*
  Allow from 192.0.105.*
  Allow from 192.0.106.*
  Allow from 192.0.107.*
  Allow from 192.0.108.*
  Allow from 192.0.109.*
  Allow from 192.0.110.*
  Allow from 192.0.111.*
  Allow from 192.0.112.*
  Allow from 192.0.113.*
  Allow from 192.0.114.*
  Allow from 192.0.115.*
  Allow from 192.0.116.*
  Allow from 192.0.117.*
  Allow from 192.0.118.*
  Allow from 192.0.119.*
  Allow from 192.0.120.*
  Allow from 192.0.121.*
  Allow from 192.0.122.*
  Allow from 192.0.123.*
  Allow from 192.0.124.*
  Allow from 192.0.125.*
  Allow from 192.0.126.*
  Allow from 192.0.127.*
  Satisfy All
  ErrorDocument 403 http://127.0.0.1/
</Files>

<IfModule mod_rewrite.c>
  RewriteEngine On
  RewriteBase /

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

  #------------ Redirect from the `http://` to the `https://` version of the URL.
```

```
  #------------ https://wiki.apache.org/httpd/RewriteHTTPToHTTPS

  RewriteCond %{HTTPS} !=on
  RewriteRule ^(.*)$ https://%{HTTP_HOST}/$1 [R=301,L]

  #------------ rewrite www.example.com → example.com
  # RewriteCond %{HTTP_HOST} ^www\.(.+)$ [NC]
  # RewriteRule ^ %{ENV:PROTO}://%1%{REQUEST_URI} [R=301,L]

  #------------ Block access to all hidden files and directories with the exception of
  #------------ the visible content from within the `/.well-known/` hidden directory.

  RewriteEngine On
  RewriteCond %{REQUEST_URI} "!(^|/)\.well-known/([^./]+./?)+$" [NC]
  RewriteCond %{SCRIPT_FILENAME} -d [OR]
  RewriteCond %{SCRIPT_FILENAME} -f
  RewriteRule "(^|/)\." - [F]
</IfModule>

# ----------------------------------------------------------------------
# | Cross-origin images                                                |
# ----------------------------------------------------------------------

# Send the CORS header for images when browsers request it.
# https://developer.mozilla.org/en-US/docs/Web/HTML/CORS_enabled_image
# https://blog.chromium.org/2011/07/using-cross-domain-images-in-webgl-and.html

<IfModule mod_setenvif.c>
    <IfModule mod_headers.c>
        <FilesMatch "\.(bmp|cur|gif|ico|jpe?g|png|svgz?|webp)$">
            SetEnvIf Origin ":" IS_CORS
            Header set Access-Control-Allow-Origin "*" env=IS_CORS
        </FilesMatch>
    </IfModule>
</IfModule>

# ----------------------------------------------------------------------
# | Cross-origin web fonts                                             |
# ----------------------------------------------------------------------

# Allow cross-origin access to web fonts.
```

```
<IfModule mod_headers.c>
    <FilesMatch "\.(eot|otf|tt[cf]|woff2?)$">
        Header set Access-Control-Allow-Origin "*"
    </FilesMatch>
</IfModule>

# ----------------------------------------------------------------------
# | Cross-origin resource timing                                       |
# ----------------------------------------------------------------------

# Allow cross-origin access to the timing information for all resources.
#
# If a resource isn't served with a `Timing-Allow-Origin` header that
# would allow its timing information to be shared with the document,
# some of the attributes of the `PerformanceResourceTiming` object will
# be set to zero.
#
# http://www.w3.org/TR/resource-timing/
# http://www.stevesouders.com/blog/2014/08/21/resource-timing-practical-tips/

<IfModule mod_headers.c>
  Header set Timing-Allow-Origin: "*"
</IfModule>

Options -MultiViews

# ----------------------------------------------------------------------
# | Document modes                                                     |
# ----------------------------------------------------------------------

# Force Internet Explorer 8/9/10 to render pages in the highest mode
# available in the various cases when it may not.

<IfModule mod_headers.c>
    Header set X-UA-Compatible "IE=edge"
    # `mod_headers` cannot match based on the content-type, however,
    # the `X-UA-Compatible` response header should be send only for
    # HTML documents and not for the other resources.
    <FilesMatch "\.(appcache|atom|bbaw|bmp|crx|css|cur|eot|f4[abpv]|flv|geojson|gif|htc|ico|
        Header unset X-UA-Compatible
```

```
    </FilesMatch>
</IfModule>

# ----------------------------------------------------------------------
# | Character encodings                                                |
# ----------------------------------------------------------------------

# Serve all resources labeled as `text/html` or `text/plain`
# with the media type `charset` parameter set to `UTF-8`.
#
# https://httpd.apache.org/docs/current/mod/core.html#adddefaultcharset

AddDefaultCharset utf-8

# - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

# Serve the following file types with the media type `charset`
# parameter set to `UTF-8`.
#
# https://httpd.apache.org/docs/current/mod/mod_mime.html#addcharset

<IfModule mod_mime.c>
    AddCharset utf-8 .atom \
                     .bbaw \
                     .css \
                     .geojson \
                     .js \
                     .json \
                     .jsonld \
                     .rdf \
                     .rss \
                     .topojson \
                     .vtt \
                     .webapp \
                     .xloc \
                     .xml
</IfModule>

# ######################################################################
# # SECURITY                                                           #
# ######################################################################
```

```
# ----------------------------------------------------------------------
# | Clickjacking                                                       |
# ----------------------------------------------------------------------

# Protect website against clickjacking.
# https://cure53.de/xfo-clickjacking.pdf.
#
# https://tools.ietf.org/html/rfc7034
# http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-fram
# https://www.owasp.org/index.php/Clickjacking

<IfModule mod_headers.c>
     Header set X-Frame-Options "DENY"
    <FilesMatch "\.(appcache|atom|bbaw|bmp|crx|css|curl eot|f4[abpv]|flv|geojson|gif|htc|ico|
        Header unset X-Frame-Options
   </FilesMatch>
</IfModule>

# ----------------------------------------------------------------------
# | Content Security Policy (CSP)                                      |
# ----------------------------------------------------------------------

# Mitigate the risk of cross-site scripting and other content-injection
# attacks.
#
# This can be done by setting a `Content Security Policy` which
# whitelists trusted sources of content for your website.
#
# The example header below allows ONLY scripts that are loaded from the
# current website's origin (no inline scripts, no CDN, etc). That almost
# certainly won't work as-is for your website!
#
# For more details on how to craft a reasonable policy for your website,
# read: http://www.html5rocks.com/en/tutorials/security/content-security-policy/
# (or the specification: http://www.w3.org/TR/CSP11/). Also, to make
# things easier, you can use an online CSP header generator such as:
# http://cspisawesome.com/.

# <IfModule mod_headers.c>
#     Header set Content-Security-Policy "script-src 'self'; object-src 'self'"
```

```
#     # `mod_headers` cannot match based on the content-type, however,
#     # the `Content-Security-Policy` response header should be send
#     # only for HTML documents and not for the other resources.
#     <FilesMatch "\.(appcache|atom|bbaw|bmp|crx|css|curl|eot|f4[abpv]|flv|geojson|gif|htc|i
#         Header unset Content-Security-Policy
#     </FilesMatch>
# </IfModule>

# ----------------------------------------------------------------------
# | File access                                                        |
# ----------------------------------------------------------------------

# Block access to directories without a default document.

<IfModule mod_autoindex.c>
    Options -Indexes
</IfModule>

# Block access to files that can expose sensitive information.

<FilesMatch "(^#.*#|\.(bak|conf|dist|fla|in[ci]|log|psd|sh|sql|sw[op])|~)$">

    # Apache < 2.3
    <IfModule !mod_authz_core.c>
        Order allow,deny
        Deny from all
        Satisfy All
    </IfModule>

    # Apache ≥ 2.3
    <IfModule mod_authz_core.c>
        Require all denied
    </IfModule>

</FilesMatch>

<IfModule mod_headers.c>
    Header set Strict-Transport-Security "max-age=16070400; includeSubDomains"
</IfModule>

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

```
..
# | Reducing MIME type security risks                                  |
# ----------------------------------------------------------------------

<IfModule mod_headers.c>
    Header set X-Content-Type-Options "nosniff"
</IfModule>

# ######################################################################
# # WEB PERFORMANCE                                                    #
# ######################################################################

# ----------------------------------------------------------------------
# | Compression                                                        |
# ----------------------------------------------------------------------

<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>

<IfModule mod_deflate.c>

    # Force compression for mangled `Accept-Encoding` request headers
    # https://developer.yahoo.com/blogs/ydn/pushing-beyond-gzipping-25601.html

    <IfModule mod_setenvif.c>
        <IfModule mod_headers.c>
            SetEnvIfNoCase ^(Accept-EncodXng|X-cept-Encoding|X{15}|~{15}|-{15})$ ^((gzip|def
            RequestHeader append Accept-Encoding "gzip,deflate" env=HAVE_Accept-Encoding
        </IfModule>
    </IfModule>

    # - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

    # Compress all output labeled with one of the following media types
```

```
# Compress all output labeled with one of the following media types.
#
# (!) For Apache versions below version 2.3.7 you don't need to
# enable `mod_filter` and can remove the `<IfModule mod_filter.c>`
# and `</IfModule>` lines as `AddOutputFilterByType` is still in
# the core directives.
#
# https://httpd.apache.org/docs/current/mod/mod_filter.html#addoutputfilterbytype

<IfModule mod_filter.c>
    AddOutputFilterByType DEFLATE "application/atom+xml" \
                                  "application/javascript" \
                                  "application/json" \
                                  "application/ld+json" \
                                  "application/manifest+json" \
                                  "application/rdf+xml" \
                                  "application/rss+xml" \
                                  "application/schema+json" \
                                  "application/vnd.geo+json" \
                                  "application/vnd.ms-fontobject" \
                                  "application/x-font-ttf" \
                                  "application/x-javascript" \
                                  "application/x-web-app-manifest+json" \
                                  "application/xhtml+xml" \
                                  "application/xml" \
                                  "font/eot" \
                                  "font/opentype" \
                                  "image/bmp" \
                                  "image/svg+xml" \
                                  "image/vnd.microsoft.icon" \
                                  "image/x-icon" \
                                  "text/cache-manifest" \
                                  "text/css" \
                                  "text/html" \
                                  "text/javascript" \
                                  "text/plain" \
                                  "text/vcard" \
                                  "text/vnd.rim.location.xloc" \
                                  "text/vtt" \
                                  "text/x-component" \
                                  "text/x-cross-domain-policy" \
                                  "text/xml"
```

```
    </IfModule>

    # - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

    # Map the following filename extensions to the specified
    # encoding type in order to make Apache serve the file types
    # with the appropriate `Content-Encoding` response header
    # (do note that this will NOT make Apache compress them!).
    #
    # If these files types would be served without an appropriate
    # `Content-Enable` response header, client applications (e.g.:
    # browsers) wouldn't know that they first need to uncompress
    # the response, and thus, wouldn't be able to understand the
    # content.
    #
    # https://httpd.apache.org/docs/current/mod/mod_mime.html#addencoding

    <IfModule mod_mime.c>
        AddEncoding gzip              svgz
    </IfModule>

</IfModule>

# ----------------------------------------------------------------------
# | ETags                                                              |
# ----------------------------------------------------------------------

# Remove `ETags` as resources are sent with far-future expires headers.
#
# https://developer.yahoo.com/performance/rules.html#etags
# https://tools.ietf.org/html/rfc7232#section-2.3

# `FileETag None` doesn't work in all cases.
<IfModule mod_headers.c>
    Header unset ETag
</IfModule>

FileETag None

# 
```

```
# ----------------------------------------------------------------------
# | Expires headers                                                    |
# ----------------------------------------------------------------------

# Serve resources with far-future expires headers.
#
# (!) If you don't control versioning with filename-based
# cache busting, you should consider lowering the cache times
# to something like one week.
#
# https://httpd.apache.org/docs/current/mod/mod_expires.html

<IfModule mod_expires.c>

    ExpiresActive on
    ExpiresDefault                                "access plus 1 week"

  # CSS
    ExpiresByType text/css                        "access plus 1 month"

  # Data interchange
    ExpiresByType application/atom+xml            "access plus 1 hour"
    ExpiresByType application/rdf+xml             "access plus 1 hour"
    ExpiresByType application/rss+xml             "access plus 1 hour"

    ExpiresByType application/json                "access plus 0 seconds"
    ExpiresByType application/ld+json             "access plus 0 seconds"
    ExpiresByType application/schema+json         "access plus 0 seconds"
    ExpiresByType application/vnd.geo+json        "access plus 0 seconds"
    ExpiresByType application/xml                 "access plus 0 seconds"
    ExpiresByType text/xml                        "access plus 0 seconds"

  # Favicon (cannot be renamed!) and cursor images
    ExpiresByType image/vnd.microsoft.icon        "access plus 1 week"
    ExpiresByType image/x-icon                    "access plus 1 week"

  # HTML
    ExpiresByType text/html                       "access plus 0 seconds"

  # JavaScript
    ExpiresByType application/javascript          "access plus 1 month"
```

```
  ExpiresByType application/x-javascript                "access plus 1 month"
  ExpiresByType text/javascript                         "access plus 1 month"

# Manifest files
  ExpiresByType application/manifest+json               "access plus 1 week"

  ExpiresByType application/x-web-app-manifest+json     "access plus 0 seconds"
  ExpiresByType text/cache-manifest                     "access plus 0 seconds"

# Media files
  ExpiresByType audio/ogg                               "access plus 1 month"
  ExpiresByType image/bmp                               "access plus 1 month"
  ExpiresByType image/gif                               "access plus 1 month"
  ExpiresByType image/jpeg                              "access plus 1 week"
  ExpiresByType image/png                               "access plus 1 month"
  ExpiresByType image/svg+xml                           "access plus 1 month"
  ExpiresByType video/mp4                               "access plus 1 month"
  ExpiresByType video/ogg                               "access plus 1 month"
  ExpiresByType video/webm                              "access plus 1 month"

# Web fonts

  # Embedded OpenType (EOT)
  ExpiresByType application/vnd.ms-fontobject           "access plus 1 month"
  ExpiresByType font/eot                                "access plus 1 month"

  # OpenType
  ExpiresByType font/opentype                           "access plus 1 month"

  # TrueType
  ExpiresByType application/x-font-ttf                  "access plus 1 month"

  # Web Open Font Format (WOFF) 1.0
  ExpiresByType application/font-woff                   "access plus 1 month"
  ExpiresByType application/x-font-woff                 "access plus 1 month"
  ExpiresByType font/woff                               "access plus 1 month"

  # Web Open Font Format (WOFF) 2.0
  ExpiresByType application/font-woff2                  "access plus 1 month"

# Other
```

```
    ExpiresByType text/x-cross-domain-policy                "access plus 1 week"

</IfModule>

# 6G BLACKLIST/FIREWALL (beta)
# @ https://perishablepress.com/6g-beta/

# 6G:[REQUEST STRINGS]
<ifModule mod_alias.c>
  RedirectMatch 403 /(\$|\*)/?$
  RedirectMatch 403 (?i)(<|>|:|;|\'|\s)
  RedirectMatch 403 (?i)([a-zA-Z0-9]{18})
  RedirectMatch 403 (?i)(https?|ftp|php)\:/
  RedirectMatch 403 (?i)(\"|\.|\_|\&|\&amp)$
  RedirectMatch 403 (?i)(\=\\\'|\=\\%27|/\\\'/?)\.
  # RedirectMatch 403 (?i)/(author\-panel|submit\-articles)/?$
  RedirectMatch 403 (?i)/(([0-9]{5})|([0-9]{6}))\-([0-9]{10})\.(gif|jpg|png)
  RedirectMatch 403 (?i)(\,|//|\)\+|/\,/|\{0\}|\(/\(|\.\.|\+\+\+|\||\\\"\\\")
  RedirectMatch 403 (?i)/uploads/([0-9]+)/([0-9]+)/(cache|cached|wp-opt|wp-supercache)\.php
  RedirectMatch 403 (?i)\.(asp|bash|cfg|cgi|dll|exe|git|hg|ini|jsp|log|mdb|out|sql|svn|swp|t
  RedirectMatch 403 (?i)/(^$|1|addlink|btn_hover|contact?|dkscsearch|dompdf|easyboard|ezooms
scraper|mapcms|mobiquo|phpinfo|phpspy|pingserver|playing|postgres|product|register|scraper|s
  RedirectMatch 403 (?i)/(\=|\$\&|\_mm|administrator|auth|bytest|cachedyou|cgi\-|cvs|config\
  RedirectMatch 403 (?i)(\$\(this\)\.attr|\&pws\=0|\&t\=|\&title\=|\%7BshopURL\%7Dimages|\_\
(\)|gifamp|hilton.ch|index.php\&amp\;quot|jfbswww|monstermmorpg|msnbot\.html|netdefender/hui|
</ifModule>

# 6G:[QUERY STRINGS]
# (note: be sure to test extensively, as some might break your site)
<IfModule mod_rewrite.c>
  RewriteCond %{REQUEST_URI} !^/$ [NC]
  RewriteCond %{QUERY_STRING} (mod|path|tag)= [NC,OR]
  RewriteCond %{QUERY_STRING} ([a-zA-Z0-9]{32}) [NC,OR]
  RewriteCond %{QUERY_STRING} (localhost|loopback|127\.0\.0\.1) [NC,OR]
  RewriteCond %{QUERY_STRING} (\?|\.\./|\.|\*|:|;|<|>|'|"|\)|\[|\]|=\\\'$|%0A|%0D|%22|%27|%
  RewriteCond %{QUERY_STRING} (benchmark|boot.ini|cast|declare|drop|echo.*kael|environ|etc/pa
  RewriteRule .* - [F,L]
</IfModule>

# 6G:[USER AGENTS]
<ifModule mod_setenvif.c>
```

```
  #SetEnvIfNoCase User-Agent ^$ keep_out
  SetEnvIfNoCase User-Agent (<|>|'|<|%0A|%0D|%27|%3C|%3E|%00|href\s) keep_out
  SetEnvIfNoCase User-Agent
(archiver|binlar|casper|checkprivacy|clshttp|cmsworldmap|comodo|curl|diavol|dotbot|email|ext
keep_out
  <limit GET POST PUT>
    Order Allow,Deny
    Allow from all
    Deny from env=keep_out
  </limit>
</ifModule>

# 6G:[REFERRERS]
<IfModule mod_rewrite.c>
  RewriteCond %{HTTP_REFERER} (<|>|'|%0A|%0D|%27|%3C|%3E|%00) [NC,OR]
  RewriteCond %{HTTP_REFERER} ([a-zA-Z0-9]{32}) [NC]
  RewriteRule .* - [F,L]
</IfModule>

# 6G:[BAD IPS]
<Limit GET POST PUT>
  Order Allow,Deny
  Allow from all
  # uncomment/edit/repeat next line to block IPs
  Deny from 123.151.39.
  Deny from 77.172.210.
  Deny from 174.94.131.
  Deny from 89.238.137.59
  Deny from 212.90.148.101
  Deny from 91.207.61.129
  Deny from 202.46.52.120
  Deny from 128.73.60.194
  Deny from 68.108.17.141
  Deny from 27.54.93.178
  Deny from 194.9.94.213
  Deny from 122.166.169.127
  Deny from 96.9.163.49
  Deny from 54.229.73.40
  Deny from 203.109.158.201
  Deny from 46.105.113.8
  Deny from 183.60.244.
```

```
    Deny from 54.232.102.193
    Deny from 195.157.124.186
    Deny from 118.39.113.219
    Deny from 27.255.56.87
    Deny from 69.161.138.1
    Deny from 192.96.204.42
    Deny from 178.63.52.200
    Deny from 27.252.92.103
    Deny from 37.59.65.58
    Deny from 186.202.126.94
    Deny from 186.213.72.146
    Deny from 186.219.44.6
</Limit>
```