```
# Apache Server Configs | MIT License
# https://github.com/h5bp/server-configs-apache

# ############################################################################
# # ERRORS                                                                   #
# ############################################################################

# ----------------------------------------------------------------------------
# | 404 error prevention                                                     |
# ----------------------------------------------------------------------------

# Disable the pattern matching based on filenames.

# This setting prevents Apache from returning a 404 error as the result
# of a rewrite when the directory with the same name does not exist.

# http://httpd.apache.org/docs/current/content-negotiation.html#multiviews
# http://www.webmasterworld.com/apache/3808792.htm

Options -MultiViews

# ----------------------------------------------------------------------------
# | Custom error messages / pages                                            |
# ----------------------------------------------------------------------------

# Customize what Apache returns to the client in case of an error.
# http://httpd.apache.org/docs/current/mod/core.html#errordocument

ErrorDocument 404 /404.html

# ############################################################################
# # INTERNET EXPLORER                                                        #
# ############################################################################

# ----------------------------------------------------------------------------
# | Better website experience                                                |
# ----------------------------------------------------------------------------

# Force Internet Explorer to render pages in the highest available
# mode in the various cases when it may not.
# https://hsivonen.fi/doctype/#ie8
# https://hsivonen.fi/doctype/#ie8

<IfModule mod_headers.c>
    Header set X-UA-Compatible "IE=edge"
    # `mod_headers` cannot match based on the content-type, however, this header
    # should be send only for HTML documents and not for the other resources
    <FilesMatch "\.(appcache|atom|crx|css|cur|eot|f4[abpv]|flv|gif|htc|ico|jpe?
g|js|json(ld)?
|m4[av]|manifest|map|mp4|oex|og[agv]|opus|otf|pdf|png|rdf|rss|safariextz|svgz?
|swf|tt[cf]|txt|vcf|vtt|webapp|web[mp]|woff|xml|xpi)$">
        Header unset X-UA-Compatible
    </FilesMatch>
</IfModule>

# ##############################################################################
# # MEDIA TYPES AND CHARACTER ENCODINGS                                        #
# ##############################################################################

# ------------------------------------------------------------------------------
# | Media types                                                                |
# ------------------------------------------------------------------------------

# Serve resources with the proper media types (formerly known as MIME types).
# http://www.iana.org/assignments/media-types/media-types.xhtml

<IfModule mod_mime.c>

  # Audio
    AddType audio/mp4                                   f4a f4b m4a
    AddType audio/ogg                                   oga ogg opus

  # Data interchange
    AddType application/json                            json map
    AddType application/ld+json                         jsonld

  # JavaScript
    # Normalize to standard type.
    # http://tools.ietf.org/html/rfc4329#section-7.2
    AddType application/javascript                      js

  # Manifest files
```

```
    # If you are providing a web application manifest file (see the
    # specification: http://w3c.github.io/manifest/), it is recommended
    # that you serve it with the `application/manifest+json` media type.
    #
    # Because the web application manifest file doesn't have its own
    # unique file extension, you can set its media type either by matching:
    #
    # 1) the exact location of the file (this can be done using a directive
    #    such as `<Location>`, but it will NOT work in the `.htaccess` file,
    #    so you will have to do it in the main server configuration file or
    #    inside of a `<VirtualHost>` container)
    #
    #    e.g.:
    #
    #       <Location "/.well-known/manifest.json">
    #           AddType application/manifest+json               json
    #       </Location>
    #
    # 2) the filename (this can be problematic as you will need to ensure
    #    that you don't have any other file with the same name as the one
    #    you gave to your web application manifest file)
    #
    #    e.g.:
    #
    #       <Files "manifest.json">
    #           AddType application/manifest+json               json
    #       </Files>

    AddType application/x-web-app-manifest+json         webapp
    AddType text/cache-manifest                         appcache manifest

  # Video
    AddType video/mp4                                   f4v f4p m4v mp4
    AddType video/ogg                                   ogv
    AddType video/webm                                  webm
    AddType video/x-flv                                 flv

  # Web fonts
    AddType application/font-woff                       woff
    AddType application/vnd.ms-fontobject               eot
    # Browsers usually ignore the font media types and simply sniff
    # the bytes to figure out the font type.
    # http://mimesniff.spec.whatwg.org/#matching-a-font-type-pattern

    # Chrome however, shows a warning if any other media types are used
    # for the following two font types.

    AddType application/x-font-ttf                      ttc ttf
    AddType font/opentype                               otf

    AddType image/svg+xml                               svg svgz

  # Other
    AddType application/octet-stream                    safariextz
    AddType application/x-chrome-extension              crx
    AddType application/x-opera-extension               oex
    AddType application/x-xpinstall                     xpi
    AddType application/xml                             atom rdf rss xml
    AddType image/webp                                  webp
    AddType image/x-icon                                cur ico
    AddType text/vtt                                    vtt
    AddType text/x-component                            htc
    AddType text/x-vcard                                vcf

</IfModule>

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

# Set `UTF-8` as the character encoding for all resources served with
# the media type of `text/html` or `text/plain`.
AddDefaultCharset utf-8

# Set `UTF-8` as the character encoding for other certain resources.
<IfModule mod_mime.c>
    AddCharset utf-8 .atom .css .js .json .jsonld .rss .vtt .webapp .xml
</IfModule>

# ##############################################################################
# # URL REWRITES                                                               #
# ##############################################################################

# ------------------------------------------------------------------------------
# | Rewrite engine                                                             |
# ------------------------------------------------------------------------------

# Turn on the rewrite engine and enable the `FollowSymLinks` option
# (this is necessary in order for the following directives to work).

<IfModule mod_rewrite.c>
    Options +FollowSymlinks
    RewriteEngine On
</IfModule>

# ------------------------------------------------------------------------------
# | Suppressing the `www.` at the beginning of URLs                            |
# ------------------------------------------------------------------------------

# Rewrite www.example.com → example.com

<IfModule mod_rewrite.c>
    RewriteCond %{HTTPS} !=on
    RewriteCond %{HTTP_HOST} ^www\.(.+)$ [NC]
    RewriteRule ^ http://%1%{REQUEST_URI} [R=301,L]
</IfModule>

# ##############################################################################
# # SECURITY                                                                   #
# ##############################################################################

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

# Protect website against clickjacking and other types of attacks by
# informing browsers not to display the web page content in any frame.

# https://cure53.de/xfo-clickjacking.pdf
# http://tools.ietf.org/html/rfc7034
# http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-
```

```
frame-options.aspx
# https://www.owasp.org/index.php/Clickjacking

<IfModule mod_headers.c>
    Header set X-Frame-Options "DENY"
    <FilesMatch "\.(appcache|atom|crx|css|cur|eot|f4[abpv]|flv|gif|htc|ico|jpe?
g|js|json(ld)?
|m4[av]|manifest|map|mp4|oex|og[agv]|opus|otf|pdf|png|rdf|rss|safariextz|svgz?
|swf|tt[cf]|vcf|vtt|webapp|web[mp]|woff|xml|xpi)$">
        Header unset X-Frame-Options
    </FilesMatch>
</IfModule>

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

# Mitigate the risk of cross-site scripting and other content-injection attacks.

# http://html5rocks.com/en/tutorials/security/content-security-policy
# http://w3.org/TR/CSP

<IfModule mod_headers.c>

    # All HTML pages
    Header set Content-Security-Policy "\
default-src 'none';\
font-src http://themes.googleusercontent.com;\
frame-src http://platform.twitter.com;\
img-src 'self' http://i.ytimg.com www.google-analytics.com;\
script-src 'self' 'unsafe-inline' www.google-analytics.com http://ajax.googleapis.com
http://platform.twitter.com;\
style-src 'self' http://fonts.googleapis.com"

    # The 404 page
    <FilesMatch "404.html">
        # Replace previous set header
        Header set Content-Security-Policy "\
default-src 'none';\
style-src 'unsafe-inline'"
    </FilesMatch>
    <FilesMatch "\.(appcache|atom|crx|css|cur|eot|f4[abpv]|flv|gif|htc|ico|jpe?
g|js|json(ld)?
|m4[av]|manifest|map|mp4|oex|og[agv]|opus|otf|pdf|png|rdf|rss|safariextz|svgz?
|swf|tt[cf]|vcf|vtt|webapp|web[mp]|woff|xml|xpi)$">
        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 hidden files and directories.

<IfModule mod_rewrite.c>
    RewriteCond %{SCRIPT_FILENAME} -d [OR]
    RewriteCond %{SCRIPT_FILENAME} -f
    RewriteRule "(^|/)\." - [F]
</IfModule>

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

# Block access to files that can expose sensitive information.

# IMPORTANT: Update the `<FilesMatch>` regular expression from below to include
# any files that might end up on the production server and can expose sensitive
# information about the website. These files may include: configuration files,
# files that contain metadata about the project (e.g.: project dependencies),
# build scripts, etc..

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

```
    <IfModule !mod_authz_core.c>
        Order allow,deny
        Deny from all
        Satisfy All
    </IfModule>
</FilesMatch>

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

# Prevent some browsers from MIME-sniffing the response.

# http://www.slideshare.net/hasegawayosuke/owasp-hasegawa
# http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-
protection.aspx
# http://msdn.microsoft.com/en-us/library/ie/gg622941.aspx
# http://mimesniff.spec.whatwg.org/

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

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

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

<IfModule mod_deflate.c>

    # Force compression for mangled 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|deflate)\s*,?\s*)+|[X~-]{4,13}$ HAVE_Accept-Encoding
            RequestHeader append Accept-Encoding "gzip,deflate" env=HAVE_Accept-Encoding
        RequestHeader append Accept-Encoding "gzip,deflate" env=HAVE_Accept-Encoding
    </IfModule>
</IfModule>

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

# Mark certain resources as been compressed in order to:
#
#  1) prevent Apache from recompressing them
#  2) ensure that they are served with the
#     `Content-Encoding: gzip` HTTP response header

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

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

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

AddOutputFilterByType DEFLATE application/atom+xml \
                              application/javascript \
                              application/json \
                              application/ld+json \
                              application/manifest+json \
                              application/rss+xml \
                              application/vnd.ms-fontobject \
                              application/x-font-ttf \
                              application/x-web-app-manifest+json \
                              application/xhtml+xml \
                              application/xml \
                              font/opentype \
                              image/svg+xml \
                              image/x-icon \
                              text/cache-manifest \
                              text/css \
                              text/html \
                              text/plain \
                              text/vtt \
                              text/x-component \
                              text/xml
```

```
</IfModule>

# ------------------------------------------------------------------------------
# | Content transformation                                                     |
# ------------------------------------------------------------------------------

# Prevent mobile network providers from modifying the website's content.
# http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html#sec14.9.5.

# <IfModule mod_headers.c>
#     Header merge Cache-Control "no-transform"
# </IfModule>

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

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

# `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.

<IfModule mod_expires.c>

    ExpiresActive on
    ExpiresDefault                                      "access plus 1 year"

  # CSS
    ExpiresByType text/css                              "access plus 1 year"
```

```
# Data interchange
  ExpiresByType application/json                      "access plus 0 seconds"
  ExpiresByType application/ld+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/x-icon                          "access plus 1 week"

# HTML components (HTCs)
  ExpiresByType text/x-component                      "access plus 1 month"

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

# JavaScript
  ExpiresByType application/javascript                "access plus 1 year"

# Manifest files
  ExpiresByType application/manifest+json             "access plus 1 year"
  ExpiresByType application/x-web-app-manifest+json   "access plus 0 seconds"
  ExpiresByType text/cache-manifest                   "access plus 0 seconds"

# Media
  ExpiresByType audio/ogg                             "access plus 1 month"
  ExpiresByType image/gif                             "access plus 1 month"
  ExpiresByType image/jpeg                            "access plus 1 month"
  ExpiresByType image/png                             "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 feeds
  ExpiresByType application/atom+xml                  "access plus 1 hour"
  ExpiresByType application/rss+xml                   "access plus 1 hour"

# Web fonts
  ExpiresByType application/font-woff                 "access plus 1 month"
  ExpiresByType application/vnd.ms-fontobject         "access plus 1 month"
  ExpiresByType application/x-font-ttf                "access plus 1 month"
```

```
    ExpiresByType font/opentype                      "access plus 1 month"
    ExpiresByType image/svg+xml                      "access plus 1 month"

</IfModule>
```