```
# ☺
# Apache Server Configs for [Project name]
#

# ######################################################################
# CROSS-ORIGIN
# ######################################################################

# ----------------------------------------------------------------------
# Cross-origin requests
# ----------------------------------------------------------------------

# Allow cross-origin requests.
#
# https://developer.mozilla.org/en-US/docs/Web/HTTP/Access_control_CORS
# http://enable-cors.org/
# http://www.w3.org/TR/cors/

# <IfModule mod_headers.c>
#   Header set Access-Control-Allow-Origin "*"
# </IfModule>

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

<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
# ----------------------------------------------------------------------

<IfModule mod_headers.c>
    <FilesMatch "\.(eot|otf|tt[cf]|woff2?)$">
```

```
    <FilesMatch "\.(eot|ttf|otf|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>

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

# ----------------------------------------------------------------------
# Error prevention
# ----------------------------------------------------------------------

Options -MultiViews

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

# ----------------------------------------------------------------------
# Document modes
# ----------------------------------------------------------------------
```

```
<IfModule mod_headers.c>
    Header set X-UA-Compatible "IE=edge"
    <FilesMatch "\.
(appcache|atom|bbaw|bmp|crx|css|curl|eot|f4[abpv]|flv|geojson|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|topojson|tt[cf]|txt|vcard|vcf|vtt|webapp|web[mp]|woff2?|xloc|xml|xpi)$">
        Header unset X-UA-Compatible
    </FilesMatch>
</IfModule>

# ----------------------------------------------------------------------
# Iframes cookies
# ----------------------------------------------------------------------

# Allow cookies to be set from iframes in Internet Explorer.
#
# http://msdn.microsoft.com/en-us/library/ms537343.aspx
# http://www.w3.org/TR/2000/CR-P3P-20001215/

# <IfModule mod_headers.c>
#   Header set P3P "policyref=\"/w3c/p3p.xml\", CP=\"IDC DSP COR ADM DEVi TAIi PSA PSD
IVAi IVDi CONi HIS OUR IND CNT\""
# </IfModule>

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

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

<IfModule mod_mime.c>

    # Data interchange
    AddType application/json                    json map topojson
    AddType application/ld+json                 jsonld
    AddType application/vnd.geo+json            geojson
    AddType application/xml                     atom rdf rss xml
```

```
    # JavaScript
    AddType application/javascript                  js

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

    # Media files
    AddType audio/mp4                               f4a f4b m4a
    AddType audio/ogg                               oga ogg opus
    AddType image/bmp                               bmp
    AddType image/webp                              webp
    AddType video/mp4                               f4v f4p m4v mp4
    AddType video/ogg                               ogv
    AddType video/webm                              webm
    AddType video/x-flv                             flv
    AddType image/svg+xml                           svg svgz
    AddType image/x-icon                            cur ico

    # Web fonts
    AddType application/font-woff                   woff
    AddType application/font-woff2                  woff2
    AddType application/vnd.ms-fontobject           eot
    AddType application/x-font-ttf                  ttc ttf
    AddType font/opentype                           otf

    # Other
    AddType application/octet-stream                safariextz
    AddType application/x-bb-appworld               bbaw
    AddType application/x-chrome-extension          crx
    AddType application/x-opera-extension           oex
    AddType application/x-xpinstall                 xpi
    AddType text/vcard                              vcard vcf
    AddType text/vnd.rim.location.xloc              xloc
    AddType text/vtt                                vtt
    AddType text/x-component                        htc

</IfModule>

# ----------------------------------------------------------------------
# Character encodings
```

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

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

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

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

# If your web host doesn't allow the `FollowSymlinks` option,
# you need to comment it out or remove it, and then uncomment
# the `Options +SymLinksIfOwnerMatch` line, but be aware of
# the performance impact.
# http://httpd.apache.org/docs/current/misc/perf-tuning.html#symlinks
#
# Some cloud hosting services will require you set `RewriteBase`.
# http://www.rackspace.com/knowledge_center/frequently-asked-question/why-is-mod-rewrite-
not-working-on-my-site
#
# Depending on how your server is set up, you may also need to
# use the `RewriteOptions` directive to enable some options for
# the rewrite engine.
```

```
# https://httpd.apache.org/docs/current/mod/mod_rewrite.html#rewriteoptions

<IfModule mod_rewrite.c>
    RewriteEngine On
    Options +FollowSymlinks
    # Options +SymLinksIfOwnerMatch
    # RewriteBase /
    # RewriteOptions <options>
</IfModule>

# ----------------------------------------------------------------------
# Forcing `https://`
# ----------------------------------------------------------------------

# Redirect from the `http://` to the `https://` version of the URL.
# https://wiki.apache.org/httpd/RewriteHTTPToHTTPS

# <IfModule mod_rewrite.c>
#   RewriteEngine On
#   RewriteCond %{HTTPS} !=on
#   RewriteRule ^(.*)$ https://%{HTTP_HOST}/$1 [R=301,L]
# </IfModule>

# ----------------------------------------------------------------------
# Suppressing / Forcing the `www.` at the beginning of URLs
# ----------------------------------------------------------------------

# The same content should never be available under two different
# URLs, especially not with and without `www.` at the beginning.
# This can cause SEO problems (duplicate content), and therefore,
# you should choose one of the alternatives and redirect the other
# one.
#
# By default `Option 1` (no `www.`) is activated.
# http://no-www.org/faq.php?q=class_b
#
# If you would prefer to use `Option 2`, just comment out all the
# lines from `Option 1` and uncomment the ones from `Option 2`.
#
# (!) NEVER USE BOTH RULES AT THE SAME TIME!
```

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

# Option 1: 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>

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

# Option 2: rewrite example.com → www.example.com
#
# Be aware that the following might not be a good idea if you use "real"
# subdomains for certain parts of your website.

# <IfModule mod_rewrite.c>
#    RewriteCond %{HTTPS} !=on
#    RewriteCond %{HTTP_HOST} !^www\. [NC]
#    RewriteCond %{SERVER_ADDR} !=127.0.0.1
#    RewriteCond %{SERVER_ADDR} !=::1
#    RewriteRule ^ http://www.%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
# </IfModule>

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

# ----------------------------------------------------------------------
# Clickjacking
# ----------------------------------------------------------------------

# Protect website against clickjacking.
#
# The example below sends the `X-Frame-Options` response header with
# the value `DENY`, informing browsers not to display the content of
# the web page in any frame.
#
# This might not be the best setting for everyone. You should read
# about the other two possible values the `X-Frame-Options` header
```

```
# field can have: `SAMEORIGIN` and `ALLOW-FROM`.
# https://tools.ietf.org/html/rfc7034#section-2.1.
#
# Keep in mind that while you could send the `X-Frame-Options` header
# for all of your website's pages, this has the potential downside that
# it forbids even non-malicious framing of your content (e.g.: when
# users visit your website using a Google Image Search results page).
#
# Nonetheless, you should ensure that you send the `X-Frame-Options`
# header for all pages that allow a user to make a state changing
# operation (e.g: pages that contain one-click purchase links, checkout
# or bank-transfer confirmation pages, pages that make permanent
# configuration changes, etc.).
#
# Sending the `X-Frame-Options` header can also protect your website
# against more than just clickjacking attacks:
# 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-
frame-options.aspx
# https://www.owasp.org/index.php/Clickjacking

# <IfModule mod_headers.c>
#   Header set X-Frame-Options "DENY"
#   # `mod_headers` cannot match based on the content-type, however,
#   # the `X-Frame-Options` 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|ico|jpe?
g|js|json(ld)?
|m4[av]|manifest|map|mp4|oex|og[agv]|opus|otf|pdf|png|rdf|rss|safariextz|svgz?
|swf|topojson|tt[cf]|txt|vcard|vcf|vtt|webapp|web[mp]|woff2?|xloc|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.
#
# 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|ico|jpe?
g|js|json(ld)?
|m4[av]|manifest|map|mp4|oex|og[agv]|opus|otf|pdf|png|rdf|rss|safariextz|svgz?
|swf|topojson|tt[cf]|txt|vcard|vcf|vtt|webapp|web[mp]|woff2?|xloc|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 all hidden files and directories with the exception of
# the visible content from within the `/.well-known/` hidden directory
```

```
# the visible content from within the `/.well-known/` hidden directory.
#
# The `/.well-known/` directory represents the standard (RFC 5785) path
# prefix for "well-known locations" (e.g.: `/.well-known/manifest.json`,
# `/.well-known/keybase.txt`), and therefore, access to its visible
# content should not be blocked.
# https://www.mnot.net/blog/2010/04/07/well-known
# https://tools.ietf.org/html/rfc5785
<IfModule mod_rewrite.c>
    RewriteCond %{REQUEST_URI} "!(^|/)\.well-known/([^./]+./?)+$" [NC]
    RewriteCond %{SCRIPT_FILENAME} -d [OR]
    RewriteCond %{SCRIPT_FILENAME} -f
    RewriteRule "(^|/)\." - [F]
</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>

# ----------------------------------------------------------------------
# HTTP Strict Transport Security (HSTS)
# ----------------------------------------------------------------------

# Force client-side SSL redirection.
#
# If a user types `example.com` in their browser, even if the server
# redirects them to the secure version of the website, that still leaves
# a window of opportunity (the initial HTTP connection) for an attacker
# to downgrade or redirect the request.
```

```
# to downgrade or redirect the request.
#
# The following header ensures that browser will ONLY connect to your
# server via HTTPS, regardless of what the users type in the browser's
# address bar.
#
# (!) Remove the `includeSubDomains` optional directive if the website's
# subdomains are not using HTTPS.
#
# http://www.html5rocks.com/en/tutorials/security/transport-layer-security/
# https://tools.ietf.org/html/draft-ietf-websec-strict-transport-sec-14#section-6.1
# http://blogs.msdn.com/b/ieinternals/archive/2014/08/18/hsts-strict-transport-security-
attacks-mitigations-deployment-https.aspx

# <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>

# ----------------------------------------------------------------------
# Reflected Cross-Site Scripting (XSS) attacks
# ----------------------------------------------------------------------

<IfModule mod_headers.c>
    Header set X-XSS-Protection "1; mode=block"
    <FilesMatch "\.
(appcache|atom|bbaw|bmp|crx|css|curl|eot|f4[abpv]|flv|geojson|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|topojson|tt[cf]|txt|vcard|vcf|vtt|webapp|web[mp]|woff2?|xloc|xml|xpi)$">
        Header unset X-XSS-Protection
    </FilesMatch>
</IfModule>

"
```

```
# ----------------------------------------------------------------------
# Increase session cookie security
# ----------------------------------------------------------------------

<IfModule php5_module>
    php_value session.cookie_httponly true
</IfModule>

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

# ----------------------------------------------------------------------
# Compression
# ----------------------------------------------------------------------

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

# ----------------------------------------------------------------------
# Content transformations
# ----------------------------------------------------------------------

# (!) If you are using `mod_pagespeed`, please note that setting
# the `Cache-Control: no-transform` response header will prevent
# `PageSpeed` from rewriting `HTML` files, and, if the
# `ModPagespeedDisableRewriteOnNoTransform` directive isn't set
# to `off`, also from rewriting other resources.
#
# https://developers.google.com/speed/pagespeed/module/configuration#notransform

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

# ----------------------------------------------------------------------
# ETag removal
# ----------------------------------------------------------------------
```

```
<IfModule mod_headers.c>
    Header unset ETag
</IfModule>
FileETag None

# ----------------------------------------------------------------------
# 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 month"

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

    # 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 year"
    ExpiresByType application/x-javascript              "access plus 1 year"
    ExpiresByType text/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 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 month"
    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
    ExpiresByType application/vnd.ms-fontobject         "access plus 1 month"
    ExpiresByType font/eot                              "access plus 1 month"
    ExpiresByType font/opentype                         "access plus 1 month"
    ExpiresByType application/x-font-ttf                "access plus 1 month"
    ExpiresByType application/font-woff                 "access plus 1 month"
    ExpiresByType application/x-font-woff               "access plus 1 month"
    ExpiresByType font/woff                             "access plus 1 month"
    ExpiresByType application/font-woff2                "access plus 1 month"

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

</IfModule>

# ----------------------------------------------------------------------
# File concatenation
# ----------------------------------------------------------------------
```

```
# Allow concatenation from within specific files.
#
# e.g.:
#
#   If you have the following lines in a file called, for
#   example, `main.combined.js`:
#
#       <!--#include file="js/jquery.js" -->
#       <!--#include file="js/jquery.timer.js" -->
#
#   Apache will replace those lines with the content of the
#   specified files.

# <IfModule mod_include.c>
#   <FilesMatch "\.combined\.js$">
#       Options +Includes
#       AddOutputFilterByType INCLUDES application/javascript \
#                                      application/x-javascript \
#                                      text/javascript
#       SetOutputFilter INCLUDES
#   </FilesMatch>
#   <FilesMatch "\.combined\.css$">
#       Options +Includes
#       AddOutputFilterByType INCLUDES text/css
#       SetOutputFilter INCLUDES
#   </FilesMatch>
# </IfModule>

# ----------------------------------------------------------------------
# Filename-based cache busting
# ----------------------------------------------------------------------

# If you're not using a build process to manage your filename version
# revving, you might want to consider enabling the following directives
# to route all requests such as `/style.12345.css` to `/style.css`.
#
# To understand why this is important and even a better solution than
# using something like `*.css?v231`, please see:
# http://www.stevesouders.com/blog/2008/08/23/revving-filenames-dont-use-querystring/

# <IfModule mod_rewrite.c>
```

```
#   RewriteCond %{REQUEST_FILENAME} !-f
#   RewriteRule ^(.+)\.(\d+)\.(bmp|css|curl|gif|ico|jpe?g|js|png|svgz?|webp)$ $1.$3 [L]
# </IfModule>

# ----------------------------------------------------------------------
# Persistent connections
# ----------------------------------------------------------------------

# Allow multiple requests to be sent over the same TCP connection:
# http://httpd.apache.org/docs/current/en/mod/core.html#keepalive.

# Enable if you serve a lot of static content but, be aware of the
# possible disadvantages!

# <IfModule mod_headers.c>
#   Header set Connection Keep-Alive
# </IfModule>
```