```
# ----------------------------------------------------------------------
# Better website experience for IE users
# ----------------------------------------------------------------------

# Force the latest IE version, in various cases when it may fall back to IE7 mode
#  github.com/rails/rails/commit/123eb25#commitcomment-118920
# Use ChromeFrame if it's installed for a better experience for the poor IE folk

<IfModule mod_headers.c>
  Header set X-UA-Compatible "IE=Edge,chrome=1"
  # mod_headers can't match by content-type, but we don't want to send this header on *every
  <FilesMatch "\.(js|css|gif|png|jpe?
g|pdf|xml|oga|ogg|m4a|ogv|mp4|m4v|webm|svg|svgz|eot|ttf|otf|woff|ico|webp|appcache|manifest|
>
    Header unset X-UA-Compatible
  </FilesMatch>
</IfModule>

# ----------------------------------------------------------------------
# Cross-domain AJAX requests
# ----------------------------------------------------------------------

# Serve cross-domain Ajax requests, disabled by default.
# enable-cors.org
# code.google.com/p/html5security/wiki/CrossOriginRequestSecurity

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

# ----------------------------------------------------------------------
# Disable content sniffing while no Content-Type header set
# We disable iframe "DENY" or "SAMEORIGIN"
# ----------------------------------------------------------------------

<IfModule mod_headers.c>
     Header set X-Content-Type-Options "nosniff"
     Header set X-Frame-Options "SAMEORIGIN"
     #Header set Content-Security-Policy: "default-src 'self'; frame-src 'self'; object-src
     Header set Strict-Transport-Security: "max-age=31536000; includeSubDomains"
</IfModule>
```

```
</IfModule>

# ----------------------------------------------------------------------
# CORS-enabled images (@crossorigin)
# ----------------------------------------------------------------------

# Send CORS headers if browsers request them; enabled by default for images.
# developer.mozilla.org/en/CORS_Enabled_Image
# blog.chromium.org/2011/07/using-cross-domain-images-in-webgl-and.html
# hacks.mozilla.org/2011/11/using-cors-to-load-webgl-textures-from-cross-domain-images/
# wiki.mozilla.org/Security/Reviews/crossoriginAttribute

<IfModule mod_setenvif.c>
  <IfModule mod_headers.c>
    # mod_headers, y u no match by Content-Type?!
    <FilesMatch "\.(gif|png|jpe?g|svg|svgz|ico|webp)$">
      SetEnvIf Origin ":" IS_CORS
      Header set Access-Control-Allow-Origin "*" env=IS_CORS
    </FilesMatch>
  </IfModule>
</IfModule>

# ----------------------------------------------------------------------
# Webfont access
# ----------------------------------------------------------------------

# Allow access from all domains for webfonts.
# Alternatively you could only whitelist your
# subdomains like "subdomain.example.com".

<IfModule mod_headers.c>
  <FilesMatch "\.(ttf|ttc|otf|eot|woff|font.css)$">
    Header set Access-Control-Allow-Origin "*"
  </FilesMatch>
</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
# 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|cur|eot|f4[abpv]|flv|geojson|gif|htc|ico
|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 always set Content-Security-Policy "script-src 'self' 'unsafe-inline' www.googl
'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|cur|eot|f4[abpv]|flv|geojson|gif|htc|ic
|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>

# ----------------------------------------------------------------------
# Proper MIME type for all files
# ----------------------------------------------------------------------
# JavaScript
#   Normalize to standard type (it's sniffed in IE anyways)
#   tools.ietf.org/html/rfc4329#section-7.2
AddType application/javascript         js
AddType application/json               json

# Audio
AddType audio/ogg                      oga ogg
AddType audio/mp4                      m4a

# Video
AddType video/ogg                      ogv
AddType video/mp4                      mp4 m4v
AddType video/webm                     webm

# SVG
#   Required for svg webfonts on iPad
#   twitter.com/FontSquirrel/status/14855840545
AddType     image/svg+xml              svg svgz
AddEncoding gzip                       svgz

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

# Assorted types
AddType image/x-icon                        ico
AddType image/webp                          webp
AddType text/cache-manifest                 appcache manifest
AddType text/x-component                    htc
AddType application/x-chrome-extension      crx
AddType application/x-opera-extension       oex
AddType application/x-xpinstall             xpi
AddType application/octet-stream            safariextz
AddType application/x-web-app-manifest+json webapp
AddType text/x-vcard                        vcf

# ----------------------------------------------------------------------
# Allow concatenation from within specific js and css files
# ------------------------------------------------------------------------

# e.g. Inside of script.combined.js you could have
#   <!--#include file="libs/jquery-1.5.0.min.js" -->
#   <!--#include file="plugins/jquery.idletimer.js" -->
# and they would be included into this single file.

# This is not in use in the boilerplate as it stands. You may
# choose to name your files in this way for this advantage or
# concatenate and minify them manually.
# Disabled by default.

#<FilesMatch "\.combined\.js$">
#  Options +Includes
#  AddOutputFilterByType INCLUDES application/javascript application/json
#  SetOutputFilter INCLUDES
#</FilesMatch>
#<FilesMatch "\.combined\.css$">
#  Options +Includes
#  AddOutputFilterByType INCLUDES text/css
#  SetOutputFilter INCLUDES
#</FilesMatch>

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

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

<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|de
HAVE_Accept-Encoding
            RequestHeader append Accept-Encoding "gzip,deflate" env=HAVE_Accept-Encoding
    </IfModule>
</IfModule>

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

# 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>

# ----------------------------------------------------------------------
# Expires headers (for better cache control)
# ----------------------------------------------------------------------

# These are pretty far-future expires headers.
# They assume you control versioning with cachebusting query params like
#   <script src="application.js?20100608">
# Additionally, consider that outdated proxies may miscache
#   www.stevesouders.com/blog/2008/08/23/revving-filenames-dont-use-querystring/

# If you don't use filenames to version, lower the CSS  and JS to something like
# If you don't use filenames to version, lower the css  and js to something like
#   "access plus 1 week" or so.

<IfModule mod_expires.c>
  ExpiresActive on

# Perhaps better to whitelist expires rules? Perhaps.
  ExpiresDefault                          "access plus 1 month"

# cache.appcache needs re-requests in FF 3.6 (thanks Remy ~Introducing HTML5)
  ExpiresByType text/cache-manifest       "access plus 0 seconds"

# Your document html
  ExpiresByType text/html                 "access plus 0 seconds"

# Data
  ExpiresByType text/xml                  "access plus 0 seconds"
  ExpiresByType application/xml           "access plus 0 seconds"
  ExpiresByType application/json          "access plus 0 seconds"

# Feed
  ExpiresByType application/rss+xml       "access plus 1 hour"
  ExpiresByType application/atom+xml      "access plus 1 hour"

# Favicon (cannot be renamed)
  ExpiresByType image/x-icon              "access plus 1 week"

# Media: images, video, audio
  ExpiresByType image/gif                 "access plus 1 month"
  ExpiresByType image/png                 "access plus 1 month"
  ExpiresByType image/jpg                 "access plus 1 month"
  ExpiresByType image/jpeg                "access plus 1 month"
  ExpiresByType video/ogg                 "access plus 1 month"
  ExpiresByType audio/ogg                 "access plus 1 month"
  ExpiresByType video/mp4                 "access plus 1 month"
  ExpiresByType video/webm                "access plus 1 month"

# HTC files  (css3pie)
  ExpiresByType text/x-component          "access plus 1 month"

# Webfonts
  ExpiresByType application/x-font-ttf    "access plus 1 month"
  ExpiresByType application/x-font-ttf    "access plus 1 month"
  ExpiresByType font/opentype             "access plus 1 month"
  ExpiresByType application/x-font-woff   "access plus 1 month"
  ExpiresByType image/svg+xml             "access plus 1 month"
  ExpiresByType application/vnd.ms-fontobject "access plus 1 month"

# CSS and JavaScript
  ExpiresByType text/css                  "access plus 1 year"
  ExpiresByType application/javascript    "access plus 1 year"

</IfModule>

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

# FileETag None is not enough for every server.
<IfModule mod_headers.c>
  Header unset ETag
</IfModule>

# Since we're sending far-future expires, we don't need ETags for
# static content.
#   developer.yahoo.com/performance/rules.html#etags
FileETag None

# ----------------------------------------------------------------------
# Stop screen flicker in IE on CSS rollovers
# ----------------------------------------------------------------------

# The following directives stop screen flicker in IE on CSS rollovers - in
# combination with the "ExpiresByType" rules for images (see above). If
# needed, un-comment the following rules.

# BrowserMatch "MSIE" brokenvary=1
# BrowserMatch "Mozilla/4.[0-9]{2}" brokenvary=1
# BrowserMatch "Opera" !brokenvary
# SetEnvIf brokenvary 1 force-no-vary

# ----------------------------------------------------------------------
# Cookie setting from iframes
#
```

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

# Allow cookies to be set from iframes (for IE only)
# If needed, uncomment and specify a path or regex in the Location directive

# <IfModule mod_headers.c>
#   <Location />
#     Header set P3P "policyref=\"/w3c/p3p.xml\", CP=\"IDC DSP COR ADM DEVi TAIi PSA PSD IV
#   </Location>
# </IfModule>

# ----------------------------------------------------------------------
# Start rewrite engine
# ----------------------------------------------------------------------

# Turning on the rewrite engine is necessary for the following rules and features.
# FollowSymLinks must be enabled for this to work.

<IfModule mod_rewrite.c>
  Options +FollowSymlinks
  RewriteEngine On
#  RewriteCond %{HTTPS} off
#  RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</IfModule>

# ----------------------------------------------------------------------
# Built-in filename-based cache busting
# ----------------------------------------------------------------------

# If you're not using the build script to manage your filename version revving,
# you might want to consider enabling this, which will route requests for
# /css/style.20110203.css to /css/style.css

# To understand why this is important and a better idea than all.css?v1231,
# read: github.com/h5bp/html5-boilerplate/wiki/Version-Control-with-Cachebusting

#Uncomment to enable.
<IfModule mod_rewrite.c>
   RewriteCond %{REQUEST_FILENAME} !-f
   RewriteCond %{REQUEST_FILENAME} !-d
   RewriteRule ^(.+)\.(\d+)\.(js|css|png|jpg|gif)$ $1.$3 [L]
</IfModule>
```

```
</IfModule>

# ----------------------------------------------------------------------
# Prevent 404 errors for non-existing redirected folders
# ----------------------------------------------------------------------

# without -MultiViews, Apache will give a 404 for a rewrite if a folder of the same name do
#   e.g. /blog/hello : webmasterworld.com/apache/3808792.htm

Options -MultiViews

# ----------------------------------------------------------------------
# Custom 404 page
# ----------------------------------------------------------------------

# You can add custom pages to handle 500 or 403 pretty easily, if you like.
# If you are hosting your site in subdirectory, adjust this accordingly
#    e.g. ErrorDocument 404 /subdir/404.html
ErrorDocument 404 404.html
ErrorDocument 400 400.html

# ----------------------------------------------------------------------
# UTF-8 encoding
# ----------------------------------------------------------------------

# Use UTF-8  encoding for anything served text/plain or text/html
AddDefaultCharset UTF-8

# Force UTF-8  for a number of file formats
AddCharset UTF-8 .css .js .xml .json .rss .atom *

# ----------------------------------------------------------------------
# A little more security
# ----------------------------------------------------------------------

# Do we want to advertise the exact version number of Apache we're running?
# Probably not.
## This can only be enabled if used in httpd.conf - It will not work in .htaccess
# ServerTokens Prod

# "-Indexes" will have Apache block users from browsing folders without a default document
# Usually you should leave this activated, because you shouldn't allow everybody to surf th
# every folder on your server (which includes rather private places like CMS system folders.
<IfModule mod_autoindex.c>
  Options -Indexes
</IfModule>

# Block access to "hidden" directories whose names begin with a period. This
# includes directories used by version control systems such as Subversion or Git.
<IfModule mod_rewrite.c>
    # Don't rewrite files or directories
    RewriteCond %{REQUEST_FILENAME} -f [OR]
    RewriteCond %{REQUEST_FILENAME} -d
    RewriteRule ^ - [L]

    # Rewrite everything else to index.html to allow html5 state links
    RewriteRule ^ index.html [L]
</IfModule>

# Block access to backup and source files
# This files may be left by some text/html editors and
# pose a great security danger, when someone can access them
<FilesMatch "(\.(bak|config|sql|fla|psd|ini|log|sh|inc|swp|dist)|~)$">
  Order allow,deny
  Deny from all
  Satisfy All
</FilesMatch>
```