```
# (!) Using `.htaccess` files slows down Apache, therefore, if you have
# access to the main server configuration file (which is usually called
# `httpd.conf`), you should add this logic there.
#
# https://httpd.apache.org/docs/current/howto/htaccess.html.

RewriteEngine On

# Change this to production when go live
SetEnv APPLICATION_ENV "development"

# The following rule tells Apache that if the requested filename
# exists, simply serve it.
RewriteCond %{REQUEST_FILENAME} -s [OR]
RewriteCond %{REQUEST_FILENAME} -l [OR]
RewriteCond %{REQUEST_FILENAME} -d
RewriteRule ^.*$ - [NC,L]
# The following rewrites all other queries to index.php. The
# condition ensures that if you are using Apache aliases to do
# mass virtual hosting, the base path will be prepended to
# allow proper resolution of the index.php file; it will work
# in non-aliased environments as well, providing a safe, one-size
# fits all solution.
RewriteCond %{REQUEST_URI}::$1 ^(/.+)(.+)::\2$
RewriteRule ^(.*) - [E=BASE:%1]
# CGI does not support apache_response_headers, but we need this header in order to do basi
RewriteRule ^(.*)$ %{ENV:BASE}index.php [E=HTTP_AUTHORIZATION:%{HTTP:Authorization},L,NC]

# Rules to block foreign characters in URLs
RewriteCond %{QUERY_STRING} ^.*(%0|%A|%B|%C|%D|%E|%F).* [NC]
RewriteRule ^(.*)$ - [F]

<IfModule mod_rewrite.c>

# Rules to block unneeded HTTP methods
RewriteCond %{REQUEST_METHOD} ^(TRACE|DELETE|TRACK) [NC]
RewriteRule ^(.*)$ - [F]

# Rules to block suspicious URIs
RewriteCond %{QUERY_STRING} \.\.\/ [NC,OR]
RewriteCond %{QUERY_STRING} ^.*\.(bash|git|hg|log|svn|swp|cvs) [NC,OR]
RewriteCond %{QUERY_STRING} .*\.(bash|git|hg|log|svn|swp|cvs) [NC,OR]
RewriteCond %{QUERY_STRING} etc/passwd [NC,OR]
RewriteCond %{QUERY_STRING} boot\.ini [NC,OR]
RewriteCond %{QUERY_STRING} ftp\:  [NC,OR]
RewriteCond %{QUERY_STRING} http\:  [NC,OR]
RewriteCond %{QUERY_STRING} https\:  [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(\[|\]|\(|\)|<|>|ê|"|;|\?|\*|=$).* [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(&#x22;|&#x27;|&#x3C;|&#x3E;|&#x5C;|&#x7B;|&#x7C;).* [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(%24&x).* [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(127\.0).* [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(globals|encode|localhost|loopback).* [NC,OR]
RewriteCond %{QUERY_STRING} ^.*(request|concat|insert|union|declare).* [NC,OR]
# proc/self/environ? no way!
RewriteCond %{QUERY_STRING} proc/self/environ [NC,OR]
# Block out any script trying to set a mosConfig value through the URL
RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z_]{1,21}(=|\%3D) [NC,OR]
# Block out any script trying to base64_encode crap to send via URL
RewriteCond %{QUERY_STRING} base64_encode.*\(.*\) [NC,OR]
# Block out any script that includes a <script> tag in URL
RewriteCond %{QUERY_STRING} (\<|%3C).*script.*(\>|%3E) [NC,OR]
# Block out any script trying to set a PHP GLOBALS variable via URL
RewriteCond %{QUERY_STRING} GLOBALS(=|\[|\%[0-9A-Z]{0,2}) [NC,OR]
# Block out any script trying to modify a _REQUEST variable via URL
RewriteCond %{QUERY_STRING} _REQUEST(=|\[|\%[0-9A-Z]{0,2})
# Send all blocked request to homepage with 403 Forbidden error!
RewriteRule ^(.*)$ index.php [F,L]

</IfModule>

# Block access to "hidden" directories whose names begin with a period. This
RewriteRule "(^|/)\." - [F]

#Specify Vary: Accept-Encoding
<IfModule mod_headers.c>
  <FilesMatch "\.(js|css|xml|gz|html|phtml|php|shtml|jpg|jpeg|gif|png|bmp|rar)$">
    Header append Vary: Accept-Encoding
  </FilesMatch>
</IfModule>

#The following lines prevent .htaccess and .htpasswd files from being viewed by Web clients.
<Files ".ht*">
```

```
  Require all denied
</Files>

# ######################################################################
# # 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>

# ------------------------------------------------------------------------------
# | CORS-enabled 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>

# 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>

# ----------------------------------------------------------------------
# | 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.
#
# https://httpd.apache.org/docs/current/content-negotiation.html#multiviews

Options -MultiViews

# ######################################################################
# # INTERNET EXPLORER                                                  #
# ######################################################################
# ----------------------------------------------------------------------
# | Document modes                                                     |
# ----------------------------------------------------------------------

# Force Internet Explorer 8/9/10 to render pages in the highest mode
# available in the various cases when it may not.
#
# https://hsivonen.fi/doctype/#ie8
#
# (!) Starting with Internet Explorer 11, document modes are deprecated.
# If your business still relies on older web apps and services that were
# designed for older versions of Internet Explorer, you might want to
# consider enabling `Enterprise Mode` throughout your company.
#
# http://msdn.microsoft.com/en-us/library/ie/bg182625.aspx#docmode
# http://blogs.msdn.com/b/ie/archive/2014/04/02/stay-up-to-date-with-enterprise-mode-for-in

<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>

# ----------------------------------------------------------------------
# | 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 IV
# </IfModule>

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

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

# Serve resources with the proper media types (f.k.a. MIME types).
#
# https://www.iana.org/assignments/media-types/media-types.xhtml
# https://httpd.apache.org/docs/current/mod/mod_mime.html#addtype

<IfModule mod_mime.c>

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

  # JavaScript
    # Normalize to standard type (it's sniffed in IE anyways):
    # http://tools.ietf.org/html/rfc4329#section-7.2
    AddType application/javascript                      js
    AddType application/json                            json map topojson
    AddType application/vnd.geo+json                    geojson
    AddType application/ld+json                         jsonld
    AddType application/xml                             atom rdf rss xml

  # Video
    AddType video/mp4                                   mp4 m4v f4v f4p
    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
    AddType application/font-woff2                      woff2

    # Browsers usually ignore the font MIME types and sniff the content,
    # however, Chrome shows a warning if other MIME types are used for the
    # following fonts.
    AddType application/x-font-ttf                      ttc ttf
    AddType font/opentype                               otf

    # Make SVGZ fonts work on iPad:
    # https://twitter.com/FontSquirrel/status/14855840545
    AddType     image/svg+xml                           svg svgz

  # 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-shockwave-flash               swf
    AddType application/x-web-app-manifest+json         webapp
    AddType application/x-xpinstall                     xpi
    AddType application/x-compress                      Z
    AddType application/x-gzip                          gz tgz
    AddType image/webp                                  webp
    AddType text/cache-manifest                         appcache manifest
    AddType text/vtt                                    vtt
    AddType text/x-component                            htc
    AddType text/x-vcard                                vcf

    # Serving `.ico` image files with a different media type
    # prevents Internet Explorer from displaying then as images:
    # https://github.com/h5bp/html5-boilerplate/commit/37b5fec090d00f38de64b591bcddcb205aad

    AddType image/x-icon                                cur ico
</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 \
                     .xml \
                     .php \
                     .xloc \
                     .html \
                     .htm \
                     .phtml \
                     .shtml
</IfModule>

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

# Block access to hidden files and directories.
# This includes directories used by version control systems such as Git and SVN.

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

# - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
# Block access to backup and source files.
# These files may be left by some text editors and can pose a great security
# danger when anyone has access to them.

<FilesMatch "(^#.*#|\.(info|install|make|module|engine|git|bak|conf[ig]|dist|fla|in[ci]|log|
    # 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>

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

# Block access to directories without a default document.
#
# You should leave the following uncommented, as you shouldn't allow
# anyone to surf through every directory on your server (which may
# includes rather private places such as the CMS's directories).

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

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

# Prevent some browsers from MIME-sniffing the response.
#
# This reduces exposure to drive-by download attacks and cross-origin
# data leaks, and should be left uncommented, especially if the server
# data leaks, and should be left uncommented, especially if the server
# is serving user-uploaded content or content that could potentially be
# treated as executable by the browser.
#
# http://www.slideshare.net/hasegawayosuke/owasp-hasegawa
# http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-v-comprehensive-protectio
# http://msdn.microsoft.com/en-us/library/ie/gg622941.aspx
# https://mimesniff.spec.whatwg.org/

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

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

# Prevent intermediate caches or proxies (e.g.: such as the ones
# used by mobile network providers) from modifying the website's
# content.
#
# https://tools.ietf.org/html/rfc2616#section-14.9.5
#
# (!) 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 merge Cache-Control "no-transform"
</IfModule>

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

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

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

# (1) Turn on the rewrite engine (this is necessary in order for
#     the `RewriteRule` directives to work).
#
#     https://httpd.apache.org/docs/current/mod/mod_rewrite.html#RewriteEngine
#
# (2) Enable the `FollowSymLinks` option if it isn't already.
#
#     https://httpd.apache.org/docs/current/mod/core.html#options
#
# (3) 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 (4), but be aware
#     of the performance impact.
#
#     https://httpd.apache.org/docs/current/misc/perf-tuning.html#symlinks
#
# (4) Some cloud hosting services will require you set `RewriteBase`.
#
#     http://www.rackspace.com/knowledge_center/frequently-asked-question/why-is-modrewrite-
#     https://httpd.apache.org/docs/current/mod/mod_rewrite.html#rewritebase
#
# (5) 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>

    # (1)
    RewriteEngine On

    # (2)
    Options +FollowSymlinks

    # (3)
    # Options +SymLinksIfOwnerMatch

    # (4)
    # RewriteBase /

    # (5)
    # 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>
    RewriteEngine On
    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>
#     RewriteEngine On
#     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>

# ----------------------------------------------------------------------
# | Server software information                                        |
# ----------------------------------------------------------------------

# Prevent Apache from sending in the `Server` response header its
# exact version number, the description of the generic OS-type or
# information about its compiled-in modules.
#
# (!) The `ServerTokens` directive will only work in the main server
# configuration file, so don't try to enable it in the `.htaccess` file!
#
# https://httpd.apache.org/docs/current/mod/core.html#servertokens
# ServerTokens Prod
ServerSignature Off

# ----------------------------------------------------------------------
# Set Keep-Alive Header
# ----------------------------------------------------------------------
# Keep-Alive allows the server to send multiple requests through one
# TCP-connection. Be aware of possible disadvantages of this setting. Turn on
# if you serve a lot of static content.

<IfModule mod_headers.c>
  Header unset X-Powered-By
  Header set Connection Keep-Alive
</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

# MUST BE MONITORED

# 2013 UA BLACKLIST [1/3]
<IfModule mod_rewrite.c>
  RewriteCond %{HTTP_HOST} !^(127\.0\.0\.0|localhost) [NC]
  RewriteCond %{HTTP_USER_AGENT} (\<|\>|\'|\$x0E|\%0A|\%0D|\%27|\%3C|\%3E|\%00|\@\$x|\!susie
fetch|avsearch|axod|axon|baboom|baby|back|baid|bali|bandit|barry|basichttp|batch|bdfetch|bea
cz|cshttp|cuill|CURI|curl|curry|custo|cute|cyber|cz3|czx|daily|dalvik|daobot|dark|darwin|dat
cra|gsearch|gt\:\:www|guidebot|guruji|gyps|haha|hailo|harv|hash|hatena|hax|head|helm|herit|
evv|iccra|ichiro|icopy|ics\)|ida|ie\/5\.0|ieauto|iempt|iexplore\.exe|ilium|ilse|iltrov|inde
[NC]
  RewriteRule .* - [G]
</IfModule>

# 2013 UA BLACKLIST [2/3]
```

```
<IfModule mod_rewrite.c>
  RewriteCond %{HTTP_USER_AGENT} (mozilla\/0|mozilla\/1|mozilla\/4\.61\ \[en\]|mozilla\/fire
com|poirot|pomp|post|postrank|powerset|preload|press|privoxy|probe|program\_shareware|protec
http|rsscache|ruby|ruff|rufus|rv\:0\.9\.7\)|salt|sample|sauger|savvy|sbcyds|sbider|sblog|sbp
5\.7|sunrise|superbot|superbro|supervi|surf4me|surfbot|survey|susi|suza|suzu|sweep|swish|sy
agent\:|useragent|usyd|vagabo|valet|vamp|vci|veri\~li|verif|versus|via|vikspider|virtual|vis
  RewriteRule .* - [G]
</IfModule>

# 2013 UA BLACKLIST [3/3] (pentag0)
<IfModule mod_rewrite.c>
  RewriteCond %{HTTP_USER_AGENT} (black\ hole|titan|webstripper|netmechanic|cherrypicker|ema
hari|lexibot|web\ image\ collector|the\ intraformant|true_robot/1\.0|true_robot|blowfish/1\.
  RewriteRule .* - [G]
</IfModule>

##############################################################################
# MOBILE SPECIFIC                                                            #
##############################################################################

# Proper MIME types

<IfModule mod_mime.c>

  # Blackberry
    # http://docs.blackberry.com/en/developers/deliverables/18169/
    AddType application/x-bb-appworld                  bbaw
    AddType text/vnd.rim.location.xloc                 xloc

  # Nokia
    # http://www.developer.nokia.com/Community/Wiki/Apache_configuration_for_mobile_applica
    # http://wiki.forum.nokia.com/index.php/How_to_enable_OTA_(Over_The_Air)_SIS_install_fr
    AddType application/octet-stream                   sisx
    AddType application/vnd.symbian.install            sis

</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, thi!s 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-fram
# 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|
        Header unset X-Frame-Options
    </FilesMatch>
</IfModule>

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

# The following expires headers are set pretty far in the future. If you don't
# control versioning with filename-based cache busting, consider lowering the
# cache time for resources like CSS and JS to something like 1 week.

<IfModule mod_expires.c>

    ExpiresActive on
    # Cache all files for 2 weeks after access (A).
    ExpiresDefault A1209600

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

  # 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 year"

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

  # HTML
    ExpiresByType text/html                             "access plus 0 week"
  ExpiresByType text/html                               "access plus 1 week"

# JavaScript
  ExpiresByType application/javascript                  "access plus 1 week"
  ExpiresByType application/x-javascript                "access plus 1 week"
  ExpiresByType text/javascript                         "access plus 1 week"

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

# Media
  ExpiresByType image/bmp                               "access plus 1 month"
  ExpiresByType image/gif                               "access plus 1 month"
  ExpiresByType image/jpeg                              "access plus 1 month"
  ExpiresByType image/jpg                               "access plus 1 month"
  ExpiresByType image/png                               "access plus 1 month"
  ExpiresByType image/svg+xml                           "access plus 1 month"
  ExpiresByType audio/ogg                               "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/font-woff                  "access plus 1 week"
  ExpiresByType application/vnd.ms-fontobject          "access plus 1 week"
  ExpiresByType application/x-font-ttf                  "access plus 1 week"
  ExpiresByType font/truetype                           "access plus 1 week"
  ExpiresByType font/opentype                           "access plus 1 week"
  ExpiresByType image/svg+xml                           "access plus 1 week"
  ExpiresByType font/eot                                "access plus 1 week"
  ExpiresByType application/x-font-woff                 "access plus 1 week"
  ExpiresByType application/font-woff2                  "access plus 1 week"

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

<IfModule mod_headers.c>
  Header append Cache-Control "public"
</IfModule>
```

```
</IfModule>

# ######################################################################
# # 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|def
            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/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/png" \
                                  "image/gif" \
                                  "image/jpeg" \
                                  "image/jpg" \
                                  "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>

# ----------------------------------------------------------------------
# | 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>
  #script-src https://apis.google.com https://platform.twitter.com; child-src https://youtu

    Header set X-Content-Security-Policy "object-src 'self'; connect-src 'self'; font-src '

    Header set Content-Security-Policy: "object-src 'self'; connect-src 'self'; font-src 'se

    Header set X-WebKit-CSP: "object-src 'self'; connect-src 'self'; font-src 'self';"
    Header set X-Permitted-Cross-Domain-Policies: "master-only"

    # `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|ico|
        Header unset Content-Security-Policy
    </FilesMatch>
</IfModule>

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

# (1) Try to re-enable the cross-site scripting (XSS) filter built
#     into most web browsers.
#
#     The filter is usually enabled by default, but in some cases it
#     may be disabled by the user. However, in Internet Explorer for
#     example, it can be re-enabled just by sending the
#     `X-XSS-Protection` header with the value of `1`.
#
# (2) Prevent web browsers from rendering the web page if a potential
#     reflected (a.k.a non-persistent) XSS attack is detected by the
#     filter.
#
#     By default, if the filter is enabled and browsers detect a
#     reflected XSS attack, they will attempt to block the attack
#     by making the smallest possible modifications to the returned
#     web page.
#
#     Unfortunately, in some browsers (e.g.: Internet Explorer),
#     this default behavior may allow the XSS filter to be exploited,
#     thereby, it's better to inform browsers to prevent the rendering
#     of the page altogether, instead of attempting to modify it.
#
#     http://hackademix.net/2009/11/21/ies-xss-filter-creates-xss-vulnerabilities
#
# (!) Do not rely on the XSS filter to prevent XSS attacks! Ensure that
#     you are taking all possible measures to prevent XSS attacks, the
#     most obvious being: validating and sanitizing your website's inputs.
#
# http://blogs.msdn.com/b/ie/archive/2008/07/02/ie8-security-part-iv-the-xss-filter.aspx
# http://blogs.msdn.com/b/ieinternals/archive/2011/01/31/controlling-the-internet-explorer->
# https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

<IfModule mod_headers.c>
    #                           (1)    (2)
    Header set X-XSS-Protection "1; mode=block"
    # `mod_headers` cannot match based on the content-type, however,
    # the `X-XSS-Protection` 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-XSS-Protection
    </FilesMatch>
</IfModule>

# prevent access to PHP error log
<Files phplog.log>
 Order allow,deny
 Deny from all
 Satisfy All
</Files>

<IfModule mod_php5.c>
    php_flag  log_errors on
    php_value error_log  phplog.log
    # Block cookie access via js. This might be already set via php.ini
    php_flag session.cookie_httponly on
    php_flag session.use_only_cookies on
    php_flag session.use_strict_mode on
    php_flag session.hash_function 1
    php_value default_charset utf-8
    php_flag cgi.fix_pathinfo off
</IfModule>
```