

```

# Set some environment variables depending on host
SetEnv APPLICATION_ENV=default
SetEnvIfNoCase Host domain\.dev APPLICATION_ENV=dev
SetEnvIfNoCase Host domain.devdomain\.com APPLICATION_ENV=dev
SetEnvIfNoCase Host domain.qadomain\.com APPLICATION_ENV=qa
SetEnvIfNoCase Host domain\.com APPLICATION_ENV=live
SetEnvIfNoCase Host www\.domain\.com APPLICATION_ENV=live

<IfModule mod_rewrite.c>
    RewriteEngine On
    RewriteBase /

    ##### Redirect non www to www #####
    # RewriteCond %{ENV:APPLICATION_ENV} live
    # RewriteCond %{HTTP_HOST} ^domain.com [NC]
    # RewriteRule ^(.*)$ http://www.domain.com/$1 [L,R=301]

    # RewriteCond %{HTTP_HOST} ^domain\.co.uk$ [OR]
    # RewriteCond %{HTTP_HOST} ^www\.domain\.co.uk$
    # RewriteRule (.*)$ http://www.domain.com/$1 [R=301,L]

    # Remove trailing slash
    RewriteRule ^(.*)/$ $1 [R=301,L]

    ##### Prevent hotlinking #####
    # RewriteCond %{HTTP_REFERER} !^$
    # RewriteCond %{HTTP_REFERER} !^http://(www.)?domain.com/.*$ [NC]
    # RewriteRule .(gif|jpg|swf|flv|png)$ / [R=302,L]

    ##### Force https for certain pages #####
    # RewriteCond %{REQUEST_METHOD} !^POST$
    # RewriteCond %{HTTPS} !=on
    # RewriteCond %{HTTP_HOST} domain.com [NC]
    # RewriteCond %{REQUEST_URI} contact-us
    # RewriteRule ^(.*)$ https://www.domain.com/$1 [L,R=301]

    ErrorDocument 404 /404.html
    ErrorDocument 500 /500.html

    ##### Security restrictions #####
    # deny from all

```

```
# proc/self/environ? no way!
RewriteCond %{QUERY_STRING} proc/self/environ [OR]
# Block out any script trying to set a mosConfig value through the URL
RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z]{1,21}(=|\%3D) [OR]
# Block out any script trying to base64_encode crap to send via URL
RewriteCond %{QUERY_STRING} base64_encode.*(?:*) [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(=| [ ]\%[\d-9A-Z]{0,2}) [OR]
# Block out any script trying to modify a _REQUEST variable via URL
RewriteCond %{QUERY_STRING} _REQUEST(=| [ ]\%[\d-9A-Z]{0,2})
# Send all blocked request to homepage with 403 Forbidden error!
RewriteRule ^(?:.*)$ /403.html [QSA,L]
```

</IfModule>

*#### Disable server signature*

ServerSignature Off

*#### disable directory browsing*

Options All -Indexes

*#### Set the timezone*

*# SetEnv TZ Europe/London*

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

AddDefaultCharset utf-8

*#### Sample Redirects*

*#### Redirect 301 http://www.domain.com/home http://www.domain.com/*

*#### Always download attachments*

AddType application/octet-stream .pdf

AddType application/octet-stream .zip

*#### Always treat those extensions as file types*

AddType application/xml xml

AddType text/xsl xsl

*### END OF FILE ###*

```

# Allow the user to see the pdf in the browser
# <Files *.pdf>
#     ForceType application/pdf
#     Header set Content-Disposition inline
# </Files>

# -----
# | Caching and performance |
# -----

#### Gzip Files ####
<ifModule mod_deflate.c>
    AddOutputFilterByType DEFLATE text/html text/xml text/css text/plain
    AddOutputFilterByType DEFLATE image/svg+xml application/xhtml+xml application/xml
    AddOutputFilterByType DEFLATE application/rdf+xml application/rss+xml application/atom+xml
    AddOutputFilterByType DEFLATE text/javascript application/javascript application/x-javascr
application/json
    AddOutputFilterByType DEFLATE application/x-font-ttf application/x-font-otf
    AddOutputFilterByType DEFLATE font/truetype font/opentype
</ifModule>

#### Cache-Control Headers ####
<ifModule mod_headers.c>
    #### HTTP ETag header ####
    FileETag None
    Header unset ETag

    <filesMatch "\.(ico|jpe?g|png|gif|swf)$">
        Header set Cache-Control "public"
    </filesMatch>
    <filesMatch "\.(css)$">
        Header set Cache-Control "public"
    </filesMatch>
    <filesMatch "\.(js)$">
        Header set Cache-Control "public"
    </filesMatch>
    <filesMatch "\.(x?html?|php)$">
        Header set Cache-Control "public, must-revalidate"
    </filesMatch>
</ifModule>

```

### #### *Expire Headers* ####

```
<IfModule mod_expires.c>
```

```
<IfModule mod_expires.c>
```

```
ExpiresActive On
```

```
ExpiresDefault A3600
```

```
ExpiresByType image/x-icon A2592000
```

```
ExpiresByType application/x-javascript A604800
```

```
ExpiresByType application/javascript A604800
```

```
ExpiresByType text/css A604800
```

```
ExpiresByType image/gif A2592000
```

```
ExpiresByType image/png A2592000
```

```
ExpiresByType image/jpeg A2592000
```

```
ExpiresByType text/plain A86400
```

```
ExpiresByType application/x-shockwave-flash A2592000
```

```
ExpiresByType application/shockwave-flash A2592000
```

```
ExpiresByType video/x-flv A2592000
```

```
ExpiresByType video/flv A2592000
```

```
ExpiresByType application/pdf A2592000
```

```
ExpiresByType text/html A3600
```

```
</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 /css/style.12345.css to /css/style.css.
```

```
# To understand why this is important and a better idea than *.css?v231, read:  
# http://www.stevesouders.com/blog/2008/08/23/revving-filenames-dont-use-querystring/
```

```
# <IfModule mod_rewrite.c>
```

```
# RewriteCond %{REQUEST_FILENAME} !-f
```

```
# RewriteRule ^(\.+)\/(\d+)\. (css|curl|gif|ico|jpe?|j|js|png|svgz?!|webp)$ $1. $3 [L]
```

```
# </IfModule>
```

```
# -----  
# | Security and Extra Headers |  
# -----
```

```

<ifModule mod_headers.c>

    # Set HTTPOnly Secure cookies
    Header always edit Set-Cookie (.*) "$1; HTTPOnly"
    Header always edit Set-Cookie (.*) "$1; Secure"

    ##### IE
    Header set X-UA-Compatible "IE=Edge,chrome=1"
    <FilesMatch "\.(appcache|crx|css|eot|gif|htc|ico|jpe?
gl|js|m4a|m4v|manifest|mp4|oex|og|ogg|ogv|otf|pdf|png|safariextz|svg|svgz|ttf|vcf|webm|webp|
    Header unset X-UA-Compatible
</FilesMatch>

    ##### P3P Header of IE issues with 3rd party cookies
    Header set P3P "policyref=\"/w3c/p3p.xml\", CP=\"IDC DSP COR ADM DEVI TAIi PSA PSD IVAi
OUR IND CNT\""

    ##### Security Hardening
    # Vivid Matter - Bulletproof Header Security
    # Don't allow pages to be framed externally - Defends against CSRF
    # `SAMEORIGIN` & `ALLOW-FROM`
    Header set X-FRAME-OPTIONS "SAMEORIGIN"
    <FilesMatch "\.(appcache|atom|crx|css|curl|eot|f4[abpv]|flv|geojson|gif|htc|ico|jpe?gl|js|
|m4[av]|manifest|map|mp4|oex|og[agv]|opus|otf|pdf|png|rdp|rss|safariextz|svgz?
|swf|topojson|ttf|txt|vcf|vtt|webapp|web[mp]|woff2?|xml|xpi)$">
        Header unset X-Frame-Options
    </FilesMatch>

    # Tell the browser to attempt the HTTPS version first
    #Header add Strict-Transport-Security "max-age=157680000"

    # Turn on IE8-IE9 XSS prevention tools
    #<IfModule mod_headers.c>
    #     Header set X-XSS-Protection "1; mode=block"
    #
    #     <FilesMatch "\.(appcache|atom|crx|css|curl|eot|f4[abpv]|flv|geojson|gif|htc|ico|jpe:
|m4[av]|manifest|map|mp4|oex|og[agv]|opus|otf|pdf|png|rdp|rss|safariextz|svgz?
|m4[av]|manifest|map|mp4|oex|og[agv]|opus|otf|pdf|png|rdp|rss|safariextz|svgz?
|swf|topojson|ttf|txt|vcf|vtt|webapp|web[mp]|woff2?|xml|xpi)$">
        #         Header unset X-XSS-Protection
    #     </FilesMatch>
    #</IfModule>

```

```
# Only allow JavaScript from the same domain to be run.
# Don't allow inline JavaScript to run.
#Header set X-Content-Security-Policy "allow 'self';"

# Prevent mime based attacks
Header set X-Content-Type-Options "nosniff"

Header unset link
Header unset Server
Header unset X-Pingback

# Disable server signature
Header set ServerSignature "Off"
Header set ServerTokens "Prod"

# Control Cross-Domain Policies
#Header set X-Permitted-Cross-Domain-Policies "master-only"

#### Set the content language header
Header set Content-Language en

#### Set the Creator
Header set Created-By "George Bardis - george@bardis.info"
Header set Bardis-Version "1.0.0"
</ifModule>

#### IE
<FilesMatch "\.(html|html|php)$">
  <IfModule mod_headers.c>
    BrowserMatch MSIE ie
    Header set X-UA-Compatible "IE=Edge,chrome=1" env=ie
  </IfModule>
</FilesMatch>

# -----
# | 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>

# -----
# | Cross-domain requests |
# -----

# Allow cross-origin requests.

# http://enable-cors.org/
# http://www.w3.org/TR/cors/
# https://code.google.com/p/html5security/wiki/CrossOriginRequestSecurity

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

# -----

# By default 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>

# Send the CORS header for images when browsers request it.
<IfModule mod_setenvif.c>
    <IfModule mod_headers.c>
        <FilesMatch "\.(curl|gif|ico|jpe?g|png|svgz?|webp)$">
            SetEnvIf Origin ":" IS_CORS
            Header set Access-Control-Allow-Origin "*" env=IS_CORS
        </FilesMatch>
    </IfModule>
</IfModule>

# -----
# | Spam bots blocking |
# -----
```

<IfModule mod\_rewrite.c>

```
RewriteCond %{HTTP_USER_AGENT} ^BlackWidow [OR]
RewriteCond %{HTTP_USER_AGENT} ^Bot\ mailto:craftbot@yahoo.com [OR]
RewriteCond %{HTTP_USER_AGENT} ^ChinaClaw [OR]
RewriteCond %{HTTP_USER_AGENT} ^Custo [OR]
RewriteCond %{HTTP_USER_AGENT} ^DISCo [OR]
RewriteCond %{HTTP_USER_AGENT} ^Download\ Demon [OR]
RewriteCond %{HTTP_USER_AGENT} ^eCatch [OR]
RewriteCond %{HTTP_USER_AGENT} ^EirGrabber [OR]
RewriteCond %{HTTP_USER_AGENT} ^EmailSiphon [OR]
RewriteCond %{HTTP_USER_AGENT} ^EmailWolf [OR]
RewriteCond %{HTTP_USER_AGENT} ^Express\ WebPictures [OR]
RewriteCond %{HTTP_USER_AGENT} ^ExtractorPro [OR]
RewriteCond %{HTTP_USER_AGENT} ^EyeNetIE [OR]
RewriteCond %{HTTP_USER_AGENT} ^FlashGet [OR]
RewriteCond %{HTTP_USER_AGENT} ^GetRight [OR]
RewriteCond %{HTTP_USER_AGENT} ^GetWeb! [OR]
RewriteCond %{HTTP_USER_AGENT} ^Go! Zilla [OR]
RewriteCond %{HTTP_USER_AGENT} ^Go-Ahead-Got-It [OR]
RewriteCond %{HTTP_USER_AGENT} ^GrabNet [OR]
RewriteCond %{HTTP_USER_AGENT} ^Grafula [OR]
RewriteCond %{HTTP_USER_AGENT} ^HMView [OR]
RewriteCond %{HTTP_USER_AGENT} HTTrack [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Image\ Stripper [OR]
RewriteCond %{HTTP_USER_AGENT} ^Image\ Sucker [OR]
RewriteCond %{HTTP_USER_AGENT} Indy\ Library [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^InterGET [OR]
RewriteCond %{HTTP_USER_AGENT} ^Internet\ Ninja [OR]
RewriteCond %{HTTP_USER_AGENT} ^JetCar [OR]
RewriteCond %{HTTP_USER_AGENT} ^JOC\ Web\ Spider [OR]
RewriteCond %{HTTP_USER_AGENT} ^larbin [OR]
RewriteCond %{HTTP_USER_AGENT} ^LeechFTP [OR]
RewriteCond %{HTTP_USER_AGENT} ^Mass\ Downloader [OR]
RewriteCond %{HTTP_USER_AGENT} ^MIDown\ tool [OR]
RewriteCond %{HTTP_USER_AGENT} ^Mister\ PiX [OR]
RewriteCond %{HTTP_USER_AGENT} ^Navroad [OR]
RewriteCond %{HTTP_USER_AGENT} ^NearSite [OR]
RewriteCond %{HTTP_USER_AGENT} ^NetAnts [OR]
RewriteCond %{HTTP_USER_AGENT} ^NetSpider [OR]
RewriteCond %{HTTP_USER_AGENT} ^Net\ Vampire [OR]
```

```

RewriteCond %{HTTP_USER_AGENT} ^NetZIP [OR]
RewriteCond %{HTTP_USER_AGENT} ^Octopus [OR]
RewriteCond %{HTTP_USER_AGENT} ^Offline\ Explorer [OR]
RewriteCond %{HTTP_USER_AGENT} ^Offline\ Navigator [OR]
RewriteCond %{HTTP_USER_AGENT} ^PageGrabber [OR]
RewriteCond %{HTTP_USER_AGENT} ^Papa\ Foto [OR]
RewriteCond %{HTTP_USER_AGENT} ^pavuk [OR]
RewriteCond %{HTTP_USER_AGENT} ^pcBrowser [OR]
RewriteCond %{HTTP_USER_AGENT} ^RealDownload [OR]
RewriteCond %{HTTP_USER_AGENT} ^ReGet [OR]
RewriteCond %{HTTP_USER_AGENT} ^SiteSnagger [OR]
RewriteCond %{HTTP_USER_AGENT} ^SmartDownload [OR]
RewriteCond %{HTTP_USER_AGENT} ^SuperBot [OR]
RewriteCond %{HTTP_USER_AGENT} ^SuperHTTP [OR]
RewriteCond %{HTTP_USER_AGENT} ^Surfbot [OR]
RewriteCond %{HTTP_USER_AGENT} ^tAkeOut [OR]
RewriteCond %{HTTP_USER_AGENT} ^WWW-Mechanize [OR]
RewriteCond %{HTTP_USER_AGENT} ^Teleport\ Pro [OR]
RewriteCond %{HTTP_USER_AGENT} ^VoidEYE [OR]
RewriteCond %{HTTP_USER_AGENT} ^Web\ Image\ Collector [OR]
RewriteCond %{HTTP_USER_AGENT} ^Web\ Sucker [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebAuto [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebCopier [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebFetch [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebGo\ IS [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebLeacher [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebReaper [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebSauger [OR]
RewriteCond %{HTTP_USER_AGENT} ^Website\ eXtractor [OR]
RewriteCond %{HTTP_USER_AGENT} ^Website\ Quester [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebStripper [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebWhacker [OR]
RewriteCond %{HTTP_USER_AGENT} ^WebZIP [OR]
RewriteCond %{HTTP_USER_AGENT} ^Widow [OR]
RewriteCond %{HTTP_USER_AGENT} ^WWWOFFLE [OR]
RewriteCond %{HTTP_USER_AGENT} ^Xaldon\ WebSpider [OR]
RewriteCond %{HTTP_USER_AGENT} ^Toata\ dragostea\ mea\ pentru\ diavola [OR]
RewriteCond %{HTTP_USER_AGENT} ^Mozilla/5.0\ SF [OR]
RewriteCond %{HTTP_USER_AGENT} ^Zeus
RewriteRule ^.* - [F,L]

```

### scanner bots as well as malicious input blocker

<IfModule mod\_rewrite.c>

RewriteCond %{HTTP\_USER\_AGENT} ^w3af.sourceforge.net [NC,OR]

RewriteCond %{HTTP\_USER\_AGENT} dirbuster [NC,OR]

RewriteCond %{HTTP\_USER\_AGENT} nikto [NC,OR]

RewriteCond %{HTTP\_USER\_AGENT} sqlmap [NC,OR]

RewriteCond %{HTTP\_USER\_AGENT} fimap [NC,OR]

RewriteCond %{HTTP\_USER\_AGENT} nessus [NC,OR]

RewriteCond %{HTTP\_USER\_AGENT} whatweb [NC,OR]

RewriteCond %{HTTP\_USER\_AGENT} Openvas [NC,OR]

RewriteCond %{HTTP\_USER\_AGENT} jbrofuzz [NC,OR]

RewriteCond %{HTTP\_USER\_AGENT} libwhisker [NC,OR]

RewriteCond %{HTTP\_USER\_AGENT} webshag [NC,OR]

RewriteCond %{HTTP\_USER\_AGENT} (havi|Netsparker|libwww-perl|python|nikto|curl|scan|java|winhttp|clsh|loader) [NC,OR]

RewriteCond %{HTTP\_USER\_AGENT} (%0A%0D%27%3C%3E%00) [NC,OR]

RewriteCond %{HTTP\_USER\_AGENT} (;|<|>|'|"|\)|\(|%0A%0D%22%27%28%3C%3E%00).\*(libwww-perl|python|nikto|curl|scan|java|winhttp|HTTrack|clsh|archiver|loader|email|harvest|extra) [NC,OR]

RewriteCond %{HTTP:Acunetix-Product} ^WVS

RewriteCond %{REQUEST\_URI} (<| %3C)([^\s]\*s)+cript.\*(>| %3E) [NC,OR]

RewriteCond %{REQUEST\_URI} (<| %3C)([^\e]\*e)+mbed.\*(>| %3E) [NC,OR]

RewriteCond %{REQUEST\_URI} (<| %3C)([^\o]\*o)+bject.\*(>| %3E) [NC,OR]

RewriteCond %{REQUEST\_URI} (<| %3C)([^\i]\*i)+frame.\*(>| %3E) [NC,OR]

RewriteCond %{REQUEST\_URI} base64\_(en|de)code[^\[]\*\([^\)]\*\) [NC,OR]

RewriteCond %{REQUEST\_URI} (%0A%0D\\r\\n) [NC,OR]

RewriteCond %{REQUEST\_URI} union([^\a]\*a)+11([^\s]\*s)+elect [NC]

RewriteRule ^(.\*)\$ http://127.0.0.1 [R=301,L]

</IfModule>