

```
<IfModule mod_rewrite.c>
    RewriteEngine On
    RewriteBase /

    # set some environment variables depending on host
    RewriteRule .* - [E=ENVIRONMENT:prod]
    RewriteCond %{HTTP_HOST} ^bardiscms.prod [NC]
    RewriteRule .* - [E=ENVIRONMENT:prod]
    RewriteCond %{HTTP_HOST} ^bardiscms.dev [NC]
    RewriteRule .* - [E=ENVIRONMENT:dev]
    RewriteCond %{HTTP_HOST} ^bardiscms.test [NC]
    RewriteRule .* - [E=ENVIRONMENT:test]

    # Use authorization headers for user context
    RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]

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

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

    ##### Sample Redirects
    ##### Redirect 301 http://www.domain.com/home http://www.domain.com/

    ##### 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 ####
# 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} (<|%)script.*(?:|%) [NC,OR]
# Block out any script trying to set a PHP GLOBALS variable via URL
RewriteCond %{QUERY_STRING} GLOBALS(=| [| \|[0-9A-Z]{0,2}) [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 ^(?:.*)$ app.php [QSA,L]

RewriteCond %{REQUEST_URI} ^/admin(?:/.*|$) [NC]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule ^(?:.*)$ app_admin.php [QSA,L]

RewriteCond %{REQUEST_URI} !^/admin(?:/.*|$) [NC]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{ENV:ENVIRONMENT} test
RewriteRule ^(?:.*)$ app_test.php [QSA,L]

RewriteCond %{REQUEST_URI} !^/admin(?:/.*|$) [NC]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{ENV:ENVIRONMENT} dev
RewriteRule ^(?:.*)$ app_dev.php [QSA,L]

RewriteCond %{REQUEST_URI} !^/admin(?:/.*|$) [NC]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{ENV:ENVIRONMENT} prod
RewriteRule ^(?:.*)$ app.php [QSA,L]

```

```
</IfModule>
```

```
<IfModule !mod_rewrite.c>
```

```
<IfModule mod_alias.c>
```

```

# When mod_rewrite is not available, we instruct a temporary redirect of
# all requests to the homepage.

```

```
    # the start page to the front controller explicitly so that the website
    # and the generated links can still be used.
    RedirectMatch 302 ^/$ /app.php/
    # RedirectTemp cannot be used instead
</IfModule>
</IfModule>

# Use the front controller as index file. It serves as a fallback solution when
# every other rewrite/redirect fails (e.g. in an aliased environment without
# mod_rewrite). Additionally, this reduces the matching process for the
# start page (path "/") because otherwise Apache will apply the rewriting rules
# to each configured DirectoryIndex file (e.g. index.php, index.html, index.pl).
# DirectoryIndex app.php

#### Disable server signature
ServerSignature Off

#### disable directory browsing
Options All -Indexes

#### Set the timezone
# SetEnv TZ Europe/London

#### Always download attachments
AddType application/octet-stream .pdf
AddType application/octet-stream .zip

#
#### Optimize ####
#

#### 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+
    AddOutputFilterByType DEFLATE text/javascript application/javascript application/x-javas
    AddOutputFilterByType DEFLATE application/x-font-ttf application/x-font-otf
    AddOutputFilterByType DEFLATE font/truetype font/opentype
</ifModule>
```

```
#### Set headers
<ifModule mod_headers.c>
  #### IE
  Header append X-UA-Compatible "IE=Edge,chrome=1"

  #### P3P Header of IE issues with 3rd party cookies
  Header append P3P: "cp=BardisCMS"

  #### Security Hardening
  # Vivid Matter - Bulletproof Header Security
  # Don't allow pages to be framed externally - Defends against CSRF
  # Prevent Clickjacking
  Header append X-Frame-Options "deny"

  # Turn on IE8-IE9 XSS prevention tools
  Header append X-XSS-Protection "1; mode=block"

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

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

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

  #### Set the Creator
  Header append X-Created-By "George Bardis - george@bardis.info"

  #### Set the Version
  Header append X-Version "0.0.1"

  Header always unset link
  Header always unset Server
  Header always unset X-Pingback

  # 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';"
```

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

# Tell the browser to attempt the HTTPS version first
#Header always set Strict-Transport-Security "max-age=157680000"
</ifModule>

# By default allow cross-origin access to web fonts.
<IfModule mod_headers.c>
    <FilesMatch "\.(eot|otfl tt[cf]|woff2?)$">
        Header always set Access-Control-Allow-Origin "*"
    </FilesMatch>
</IfModule>

#### Cache-Control Headers ####
<ifModule mod_headers.c>
    <filesMatch "\.(ico|jpe?g|png|gif|swf|eot|otfl tt[cf]|woff2?)$">
        Header always set Cache-Control "public"
    </filesMatch>
    <filesMatch "\.(css)$">
        Header always set Cache-Control "public"
    </filesMatch>
    <filesMatch "\.(js)$">
        Header always set Cache-Control "public"
    </filesMatch>
    #### Disable Cache for generated pages ####
    <filesMatch "\.(x?html?|php)$">
        # Header set Cache-Control "private, no-cache, no-store, must-revalidate"
        # Header set Pragma "no-cache"
        # Header set Expires "-1"
    </filesMatch>
</ifModule>

#### HTTP ETag header ####
# FileETag None

#### Expire Headers ####
<IfModule mod_expires.c>

    <FilesMatch "\.(appcache|crx|css|eot|gif|htcl|ico|jpe?
gl|jsl|m4a|m4v|manifest|mp4|oex|ogal|ogg|ogv|otfl|pdf|png|safariextz|svg|svgz|tfl|vcfl|webml|webpl
```

```

    Header always unset X-UA-Compatible
</FilesMatch>

ExpiresActive On
#ExpiresDefault A3600
ExpiresByType image/x-icon A2592000
ExpiresByType application/x-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 video/x-flv A2592000
ExpiresByType application/pdf A2592000
#ExpiresByType text/html A3600
</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 always 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]
```

```
</IfModule>
```

```
#### 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|http|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).*(libww  
perl|python|nikto|curl|scan|java|winhttp|HTTrack|clsh|http|archiver|loader|email|harvest|extr:  
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>