```
### ================================================================================
### Security Enhanced & Highly Optimized .htaccess File for Joomla!
### automatically generated by Admin Tools 3.6.1 on 2015-09-29 19:50:08 GMT
### Auto-detected Apache version: 2.2 (best guess)
### ================================================================================
###
### The contents of this file are based on the same author's work "Master
### .htaccess", published on http://snipt.net/nikosdion/the-master-htaccess
###
### Admin Tools is Free Software, distributed under the terms of the GNU
### General Public License version 3 or, at your option, any later version
### published by the Free Software Foundation.
###
### !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! IMPORTANT !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
### !!                                                                        !!
### !!  If you get an Internal Server Error 500 or a blank page when trying  !!
### !!  to access your site, remove this file and try tweaking its settings  !!
### !!  in the back-end of the Admin Tools component.                         !!
### !!                                                                        !!
### !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
###

##### RewriteEngine enabled - BEGIN
RewriteEngine On
##### RewriteEngine enabled - END

##### RewriteBase set - BEGIN
RewriteBase /portals/decopatio
##### RewriteBase set - END

##### File execution order -- BEGIN
DirectoryIndex index.php index.html
##### File execution order -- END

##### No directory listings -- BEGIN
IndexIgnore *
Options -Indexes
##### No directory listings -- END

##### Redirect index.php to / -- BEGIN
RewriteCond %{THE_REQUEST} ^POST
```

```
RewriteCond %{THE_REQUEST} !^POST
RewriteCond %{THE_REQUEST} ^[A-Z]{3,9}\ /index\.php\ HTTP/
RewriteCond %{SERVER_PORT}>s ^(443>(s)|[0-9]+>s)$
RewriteRule ^index\.php$ http%2://www.jaffili.com/portals/decopatio/ [R=301,L]
##### Redirect index.php to / -- END
##### Rewrite rules to block out some common exploits -- BEGIN
RewriteCond %{QUERY_STRING} proc/self/environ [OR]
RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z_]{1,21}(=|\%3D) [OR]
RewriteCond %{QUERY_STRING} base64_(en|de)code\(.*\) [OR]
RewriteCond %{QUERY_STRING} (<|%3C).*script.*(>|%3E) [NC,OR]
RewriteCond %{QUERY_STRING} GLOBALS(=|\[|\%[0-9A-Z]{0,2}) [OR]
RewriteCond %{QUERY_STRING} _REQUEST(=|\[|\%[0-9A-Z]{0,2})
RewriteRule .* index.php [F]
##### Rewrite rules to block out some common exploits -- END
##### File injection protection -- BEGIN
RewriteCond %{REQUEST_METHOD} GET
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=http:// [OR]
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=(\.\.//?)+ [OR]
RewriteCond %{QUERY_STRING} [a-zA-Z0-9_]=/([a-z0-9_.]//?)+ [NC]
RewriteRule .* - [F]
##### File injection protection -- END

##### Advanced server protection rules exceptions -- BEGIN
RewriteRule ^administrator\/components\/com_akeeba\/restore\.php$ - [L]
RewriteRule ^administrator\/components\/com_admintools\/restore\.php$ - [L]
RewriteRule ^administrator\/components\/com_joomlaupdate\/restore\.php$ - [L]
RewriteRule ^administrator\/components\/com_extplorer\/fetchscript\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !(\.php)$
RewriteCond %{REQUEST_FILENAME} -f
RewriteRule ^cache/ - [L]
RewriteRule ^templates\/your_template_name_here/ - [L]
##### Advanced server protection rules exceptions -- END

##### Advanced server protection -- BEGIN

RewriteCond %{QUERY_STRING} \=PHP[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12
RewriteRule .* - [F]
## Back-end protection
RewriteRule ^administrator/?$ - [L]
RewriteRule ^administrator/index\.(php|html?)$ - [L]
RewriteRule ^administrator/index[23]\.php$ - [L]
```

```
RewriteRule ^administrator/(components|modules|templates|images|plugins)/.*\.(jpe|jpg|jpeg|
RewriteRule ^administrator/ - [F]
## Allow limited access for certain Joomla! system directories with client-accessible conte
RewriteRule ^(components|modules|templates|images|plugins|media|libraries|media/jui/fonts)/.
(jpe|jpg|jpeg|jp2|jpe2|png|gif|bmp|css|js|swf|html|mpg|mp3|mpeg|mp4|avi|wav|ogg|ogv|xls|xls>
RewriteRule ^(components|modules|templates|images|plugins|media|libraries|media/jui/fonts)/
## Disallow front-end access for certain Joomla! system directories (unless access to their
RewriteRule ^includes/js/ - [L]
RewriteRule ^(cache|includes|language|logs|log|tmp)/ - [F]
RewriteRule ^(configuration\.php|CONTRIBUTING\.md|htaccess\.txt|joomla\.xml|LICENSE\.txt|php

## Disallow access to rogue PHP files throughout the site, unless they are explicitly allow
RewriteCond %{REQUEST_FILENAME} (\.php)$
RewriteCond %{REQUEST_FILENAME} !(/index[23]?\.php)$
RewriteCond %{REQUEST_FILENAME} -f
RewriteRule (.*\.php)$ - [F]
## Disallow access to htaccess.txt, php.ini and configuration.php-dist
RewriteRule ^(htaccess\.txt|configuration\.php-dist|php\.ini)$ - [F]
## Protect against clickjacking
<IfModule mod_headers.c>

  Header always append X-Frame-Options SAMEORIGIN

  # 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|jp
    Header unset X-Frame-Options
  </FilesMatch>

</IfModule>
## Reduce MIME type security risks
<IfModule mod_headers.c>
  Header set X-Content-Type-Options "nosniff"
</IfModule>
## Reflected XSS prevention
<IfModule mod_headers.c>
Header set X-XSS-Protection "1; mode=block"
</IfModule>

# 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.

<IfModule mod_headers.c>
  <FilesMatch "\.(appcache|atom|bbaw|bmp|crx|css|curl|eot|f4[abpv]|flv|geojson|gif|htc|ico|jp
    Header unset X-XSS-Protection
  </FilesMatch>
</IfModule>
## Remove Apache and PHP version signature
<IfModule mod_headers.c>
    Header unset X-Powered-By
</IfModule>

ServerSignature Off
## Prevent content transformation
<IfModule mod_headers.c>
    Header merge Cache-Control "no-transform"
</IfModule>
##### Advanced server protection -- END

## Set the UTF-8 character set as the default
#  Serve all resources labeled as `text/html` or `text/plain`
#  with the media type `charset` parameter set to `UTF-8`.

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 \
                    .xloc \
                    .xml
</IfModule>
##### Joomla! core SEF Section -- BEGIN
RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
RewriteCond %{REQUEST_URI} !^/index\.php
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule .* index.php [L]
##### Joomla! core SEF Section -- END
```