```
##
# @package    Joomla
# @copyright  Copyright (C) 2005 - 2015 Open Source Matters. All rights reserved.
# @license    GNU General Public License version 2 or later; see LICENSE.txt
##

##
# READ THIS COMPLETELY IF YOU CHOOSE TO USE THIS FILE!
#
# The line just below this section: 'Options +FollowSymLinks' may cause problems
# with some server configurations.  It is required for use of mod_rewrite, but may already
# be set by your server administrator in a way that disallows changing it in
# your .htaccess file.  If using it causes your server to error out, comment it out (add #
to
# beginning of line), reload your site in your browser and test your sef url's.  If they
work,
# it has been set by your server administrator and you do not need it set here.
##

########## Begin - No directory listings
## Note: +FollowSymlinks may cause problems and you might have to remove it
IndexIgnore *
########## End - No directory listings

########## Begin - File execution order, by Komra.de
DirectoryIndex index.php index.html
########## End - File execution order

########## Begin - ETag Optimization
## This rule will create an ETag for files based only on the modification
## timestamp and their size. This works wonders if you are using rsync'ed
## servers, where the inode number of identical files differs.
## Note: It may cause problems on your server and you may need to remove it
FileETag MTime Size
########## End - ETag Optimization

########## Begin - Optimal default expiration time
## Note: this might cause problems and you might have to comment it out by
## placing a hash in front of this section's lines
## Note: Some people prefer using "now plus 1 month" instead of "now plus 1 year".
## Edit to taste.
## Suit to taste.
<IfModule mod_expires.c>
  # Enable expiration control
  ExpiresActive On

  # Default expiration: 1 hour after request
  ExpiresDefault "now plus 1 hour"

  # CSS and JS expiration: 1 week after request
  ExpiresByType text/css "now plus 1 week"
  ExpiresByType application/javascript "now plus 1 week"
  ExpiresByType application/x-javascript "now plus 1 week"

  # Image files expiration: 1 month after request
  ExpiresByType image/bmp "now plus 1 month"
  ExpiresByType image/gif "now plus 1 month"
  ExpiresByType image/jpeg "now plus 1 month"
  ExpiresByType image/jp2 "now plus 1 month"
  ExpiresByType image/pipeg "now plus 1 month"
  ExpiresByType image/png "now plus 1 month"
  ExpiresByType image/svg+xml "now plus 1 month"
  ExpiresByType image/tiff "now plus 1 month"
  ExpiresByType image/vnd.microsoft.icon "now plus 1 month"
  ExpiresByType image/x-icon "now plus 1 month"
  ExpiresByType image/ico "now plus 1 month"
  ExpiresByType image/icon "now plus 1 month"
  ExpiresByType text/ico "now plus 1 month"
  ExpiresByType application/ico "now plus 1 month"
  ExpiresByType image/vnd.wap.wbmp "now plus 1 month"
  ExpiresByType application/vnd.wap.wbxml "now plus 1 month"
  ExpiresByType application/smil "now plus 1 month"

  # Audio files expiration: 1 month after request
  ExpiresByType audio/basic "now plus 1 month"
  ExpiresByType audio/mid "now plus 1 month"
  ExpiresByType audio/midi "now plus 1 month"
  ExpiresByType audio/mpeg "now plus 1 month"
  ExpiresByType audio/x-aiff "now plus 1 month"
  ExpiresByType audio/x-mpegurl "now plus 1 month"
  ExpiresByType audio/x-pn-realaudio "now plus 1 month"
  ExpiresByType audio/x-wav "now plus 1 month"
  # Movie files expiration: 1 month after request
  ExpiresByType application/x-shockwave-flash "now plus 1 month"
  ExpiresByType x-world/x-vrml "now plus 1 month"
  ExpiresByType video/x-msvideo "now plus 1 month"
  ExpiresByType video/mpeg "now plus 1 month"
  ExpiresByType video/mp4 "now plus 1 month"
  ExpiresByType video/quicktime "now plus 1 month"
  ExpiresByType video/x-la-asf "now plus 1 month"
  ExpiresByType video/x-ms-asf "now plus 1 month"
</IfModule>
########## End - Optimal expiration time

########## Begin - Common hacking tools and bandwidth hoggers block
## By SigSiu.net and @nikosdion.
# This line also disables Akeeba Remote Control 2.5 and earlier
SetEnvIf user-agent "Indy Library" stayout=1
# WARNING: Disabling wget will also block the most common method for
# running CRON jobs. Remove if you have issues with CRON jobs.
SetEnvIf user-agent "Wget" stayout=1
# The following rules are for bandwidth-hogging download tools
SetEnvIf user-agent "libwww-perl" stayout=1
SetEnvIf user-agent "Download Demon" stayout=1
SetEnvIf user-agent "GetRight" stayout=1
SetEnvIf user-agent "GetWeb!" stayout=1
SetEnvIf user-agent "Go!Zilla" stayout=1
SetEnvIf user-agent "Go-Ahead-Got-It" stayout=1
SetEnvIf user-agent "GrabNet" stayout=1
SetEnvIf user-agent "TurnitinBot" stayout=1
# This line denies access to all of the above tools
deny from env=stayout
########## End - Common hacking tools and bandwidth hoggers block

## Can be commented out if causes errors, see notes above.
Options +FollowSymlinks
Options -Indexes

## Mod_rewrite in use.

RewriteEngine On
```

```
## Begin - Rewrite rules to block out some common exploits.
# If you experience problems on your site block out the operations listed below
# This attempts to block the most common type of exploit `attempts` to Joomla!
#
# Block out any script trying to base64_encode data within the URL.
RewriteCond %{QUERY_STRING} base64_encode[^(]*\([^)]*\) [OR]
# Block out any script that includes a <script> tag in URL.
RewriteCond %{QUERY_STRING} (<|%3C)([^s]*s)+cript.*(>|%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}) [OR]
# Block out any script trying to modify a _REQUEST variable via URL.
RewriteCond %{QUERY_STRING} _REQUEST(=|\[|\%[0-9A-Z]{0,2})
# Return 403 Forbidden header and show the content of the root homepage
RewriteRule .* index.php [F]
#
## End - Rewrite rules to block out some common exploits.

## Begin - Custom redirects
#
# If you need to redirect some pages, or set a canonical non-www to
# www redirect (or vice versa), place that code here. Ensure those
# redirects use the correct RewriteRule syntax and the [R=301,L] flags.
#
## End - Custom redirects

##
# Uncomment following line if your webserver's URL
# is not directly related to physical file paths.
# Update Your Joomla! Directory (just / for root).
##

# RewriteBase /

## Begin - Joomla! core SEF Section.
#
RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
#
# If the requested path and file is not /index.php and the request
# has not already been internally rewritten to the index.php script
RewriteCond %{REQUEST_URI} !^/index\.php
# and the requested path and file doesn't directly match a physical file
```

```
RewriteCond %{REQUEST_FILENAME} !-f
# and the requested path and file doesn't directly match a physical folder
RewriteCond %{REQUEST_FILENAME} !-d
# internally rewrite the request to the index.php script
RewriteRule .* index.php [L]
#

########## Begin - File execution order, by Komra.de
DirectoryIndex index.php index.html
########## End - File execution order
## End - Joomla! core SEF Section.

########## Begin - Rewrite rules to block out some common exploits
## If you experience problems on your site block out the operations listed below
## This attempts to block the most common type of exploit `attempts` to Joomla!
#
# If the request query string contains /proc/self/environ (by SigSiu.net)
RewriteCond %{QUERY_STRING} proc/self/environ [OR]
# Legacy variable injection (these attacks wouldn't work w/out Joomla! 1.5's Legacy Mode plugin)
RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z_]{1,21}(=|\%3D) [OR]
# Block out any script trying to base64_encode/base64_decode data to send via URL
RewriteCond %{QUERY_STRING} base64_(en|de)code\(.*\) [OR]
## IMPORTANT: If the above line throws an HTTP 500 error, replace it with these 2 lines:
# RewriteCond %{QUERY_STRING} base64_encode\(.*\) [OR]
# RewriteCond %{QUERY_STRING} base64_decode\(.*\) [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}) [OR]
# Block out any script trying to modify a _REQUEST variable via URL
RewriteCond %{QUERY_STRING} _REQUEST(=|\[|\%[0-9A-Z]{0,2})
# Return a 403 Forbidden header and show the content of the root homepage
RewriteRule .* index.php [F]
#
########## End - Rewrite rules to block out some common exploits

########## Begin - File injection protection, by SigSiu.net
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]
########## End - File injection protection

########## Begin - Advanced server protection rules exceptions ####
##
## These are sample exceptions to the Advanced Server Protection 3.0
## rule set further down this file.
##
## Allow UddeIM CAPTCHA
RewriteRule ^components/com_uddeim/captcha15\.php$ - [L]
## Allow Phil Taylor's Turbo Gears
RewriteRule ^plugins/system/GoogleGears/gears-manifest\.php$ - [L]
## Allow JoomlaWorks AllVideos
RewriteRule ^plugins/content/jw_allvideos/includes/jw_allvideos_scripts\.php$ - [L]
## Allow Admin Tools Joomla! updater to run
RewriteRule ^administrator/components/com_admintools/restore\.php$ - [L]
## Allow Akeeba Backup Professional's integrated restoration script to run
RewriteRule ^administrator/components/com_akeeba/restore\.php$ - [L]
## Allow Akeeba Kickstart
RewriteRule ^kickstart\.php$ - [L]

# Add more rules to single PHP files here

## Allow Agora attachments, but not PHP files in that directory!
RewriteCond %{REQUEST_FILENAME} !(\.php)$
RewriteCond %{REQUEST_FILENAME} -f
RewriteRule ^components/com_agora/img/members/ - [L]

# Add more rules for allowing full access (except PHP files) on more directories here

## Uncomment to allow full access to the cache directory (strongly not recommended!)
#RewriteRule ^cache/ - [L]
## Uncomment to allow full access to the tmp directory (strongly not recommended!)
#RewriteRule ^tmp/ - [L]
# Add more full access rules here

########## End - Advanced server protection rules exceptions ####

########## Begin - Advanced server protection
# Advanced server protection, version 2.0 - August 2010
# by Nicholas K. Dionysopoulos

## Referrer filtering for common media files. Replace with your own domain.
## This blocks most common fingerprinting attacks ;)
## Note: Change www\.example\.com with your own domain name, substituting the
## dots with \., i.e.: www\.example\.com for www.example.com
RewriteRule ^images/stories/.*\.(jp(e?g|2)?|png|gif|bmp|css|js|swf|ico)$ - [L]
RewriteCond %{HTTP_REFERER} .
RewriteCond %{HTTP_REFERER} !^https?://(www\.)?pharmec\.local [NC]
RewriteCond %{REQUEST_FILENAME} -f
RewriteRule \.(jp(e?g|2)?|png|gif|bmp|css|js|swf|ico)$ - [F]

## Disallow visual fingerprinting of Joomla! sites (module position dump)
## Initial idea by Brian Teeman and Ken Crowder, see:
## http://www.slideshare.net/brianteeman/hidden-joomla-secrets
## Improved by @nikosdion to work more efficiently and handle template
## and tmpl query parameters
RewriteCond %{QUERY_STRING} (^|&)tmpl=(component|system) [NC]
RewriteRule .* - [L]
RewriteCond %{QUERY_STRING} (^|&)t(p|emplate)= [NC]
RewriteRule .* - [F]

## Disallow PHP Easter Eggs (can be used in fingerprinting attacks to determine
## your PHP version). See http://www.0php.com/php_easter_egg.php and
## http://osvdb.org/12184 for more information
RewriteCond %{QUERY_STRING} \=PHP[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]
{12} [NC]
RewriteRule .* - [F]

## Back-end protection
## This also blocks fingerprinting attacks browsing for XML and INI files
RewriteRule ^administrator/?$ - [L]
RewriteRule ^administrator/index\.(php|html?)$ - [L]
RewriteRule ^administrator/index[23]\.php$ - [L]
RewriteRule ^administrator/(components|modules|templates|images|plugins)/.*\.(jp(e?g|2)?
|png|gif|bmp|css|js|swf|html?|mp(eg?|[34])|avi|wav|og[gv]|xlsx?|docx?|pptx?
|zip|rar|pdf|xps|txt|7z|svg|od[tsp]|flv|mov)$ - [L]
RewriteRule ^administrator/ - [F]

## Explicitly allow access only to XML-RPC's xmlrpc/index.php or plain xmlrpc/ directory
RewriteRule ^xmlrpc/(index\.php)?$ - [L]
RewriteRule ^xmlrpc/ - [F]

## Disallow front-end access for certain Joomla! system directories
RewriteRule ^includes/js/ - [L]
RewriteRule ^(cache|includes|language|libraries|logs|tmp)/ - [F]

## Allow limited access for certain Joomla! system directories with client-accessible content
RewriteRule ^(components|modules|plugins|templates)/.*\.(jp(e?g|2)?|png|gif|bmp|css|js|swf|html?|mp(eg?|[34])|avi|wav|og[gv]|xlsx?|docx?|pptx?|zip|rar|pdf|xps|txt|7z|svg|od[tsp]|flv|mov)$ - [L]
## Uncomment this line if you have extensions which require direct access to their own
## custom index.php files. Note that this is UNSAFE and the developer should be ashamed
## for being so lame, lazy and security unconscious.
# RewriteRule ^(components|modules|plugins|templates)/.*(index\.php)?$ - [L]
## Uncomment the following line if your template requires direct access to PHP files
## inside its directory, e.g. GZip compressed copies of its CSS files
# RewriteRule ^templates/.*\.php$ - [L]
RewriteRule ^(components|modules|plugins|templates)/ - [F]

## Disallow access to rogue PHP files throughout the site, unless they are explicitly allowed
RewriteCond %{REQUEST_FILENAME} (\.php)$
RewriteCond %{REQUEST_FILENAME} !(/index[23]?\.php)$
RewriteCond %{REQUEST_FILENAME} -f
RewriteRule (.*\.php)$ - [F]

## Disallow access to htaccess.txt and configuration.php-dist
RewriteRule ^(htaccess\.txt|configuration\.php-dist|php\.ini)$ - [F]

## SQLi first line of defense, thanks to Radek Suski (SigSiu.net) @
## http://www.sigsiu.net/presentations/fortifying_your_joomla_website.html
## May cause problems on legitimate requests
RewriteCond %{QUERY_STRING} concat.*\( [NC,OR]
RewriteCond %{QUERY_STRING} union.*select.*\( [NC,OR]
RewriteCond %{QUERY_STRING} union.*all.*select.* [NC]
RewriteRule .* - [F]

########## End - Advanced server protection

########## Begin - Basic antispam Filter, by SigSiu.net
```

```
########## Begin - Basic antispam Filter, by SigSiu.net
## I removed some common words, tweak to your liking
## This code uses PCRE and works only with Apache 2.x.
## This code will NOT work with Apache 1.x servers.
RewriteCond %{QUERY_STRING} \b(ambien|blue\spill|cialis|cocaine|ejaculation|erectile)\b
[NC,OR]
RewriteCond %{QUERY_STRING}
\b(erections|hoodia|huronriveracres|impotence|levitra|libido)\b [NC,OR]
RewriteCond %{QUERY_STRING}
\b(lipitor|phentermin|pro[sz]ac|sandyauer|tramadol|troyhamby)\b [NC,OR]
## Note: The final RewriteCond must NOT use the [OR] flag.
RewriteCond %{QUERY_STRING} \b(ultram|unicauca|valium|viagra|vicodin|xanax|ypxaieo)\b [NC]
RewriteRule .* - [F]
## Note: The previous lines are a "compressed" version
## of the filters. You can add your own filters as:
## RewriteCond %{QUERY_STRING} \bbadword\b [NC,OR]
## where "badword" is the word you want to exclude
########## End - Basic antispam Filter, by SigSiu.net

########## Begin - Joomla! core SEF Section
#
RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
# If the requested path and file is not /index.php and the request
# has not already been internally rewritten to the index.php script
RewriteCond %{REQUEST_URI} !^/index\.php
# and the request is for the site root, or for an extensionless URL,
# or the requested URL ends with one of the listed extensions
RewriteCond %{REQUEST_URI} /component/|(/[^.]*|\.(php|html?
|feed|pdf|raw|ini|zip|json|file|vcf))$ [NC]
# and the requested path and file doesn't directly match a physical file
RewriteCond %{REQUEST_FILENAME} !-f
# and the requested path doesn't match a physical folder
RewriteCond %{REQUEST_FILENAME} !-d
# internally rewrite the request to the index.php script
RewriteRule .* index.php [L]
#
########## End - Joomla! core SEF Section

##### Rewrite index.php to /
RewriteEngine On
RewriteCond %{REQUEST_URI} ^/index\.php/
RewriteRule ^index.php/(.*) /$1 [R,L]
RewriteRule ^index.php/(.*)$ /$1 [R,L]
```