```
#AuthUserFile /etc/apache2/.htpasswd
#AuthGroupFile /dev/null
#AuthName "SWG new site demo"
#AuthType Basic
#require user swg


# API Redirects from stable URLs to actual Joomla pages
RewriteRule ^api/eventlisting /index.php?
option=com_swg_events&view=eventlisting&includeWalks=1&includeSocials=1&includeWeekends=1&st
RewriteRule ^api/walkdetails /index.php?option=com_swg_walklibrary&view=walkdetails [L,QSA]
RewriteRule ^api/route /index.php?option=com_swg_walklibrary&view=route [L,QSA]
RewriteRule ^api/nominatim /index.php?option=com_swg_walklibrary&view=nominatimwrapper [L,QS


##
# @package     Joomla
# @copyright   Copyright (C) 2005 - 2012 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 dissallows changing it in
# your .htaccess file.  If using it causes your server to error out, comment it out (add # :
# beginning of line), reload your site in your browser and test your sef url's.  If they wor
# it has been set by your server administrator and you do not need it set here.
##


## Can be commented out if causes errors, see notes above.
Options +FollowSymLinks


## 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 request is for something within the component folder,
# or 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|vcf|raw))$ [NC]
```

```
# 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]
#
## End - Joomla! core SEF Section.
```