```
<IfModule mod_rewrite.c>

RewriteEngine On

RewriteCond %{HTTPS} off
# First rewrite to HTTPS:
# Don't put www. here. If it is already there it will be included, if not
# the subsequent rule will catch it.
RewriteRule .* https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
# Now, rewrite any request to the wrong domain to use www.
RewriteCond %{HTTP_HOST} !^www\.
RewriteRule .* https://www.%{HTTP_HOST}%{REQUEST_URI} [L,R=301]

## Begin RewriteBase
# If you are getting 404 errors on subpages, you may have to uncomment the RewriteBase
entry
# You should change the '/' to your appropriate subfolder. For example if you have
# your Grav install at the root of your site '/' should work, else it might be something
# along the lines of: RewriteBase /<your_sub_folder>
##

# RewriteBase /

## End - RewriteBase

## Begin - 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 Grav
#
# 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 - Exploits
```

```
## End - Exploits

## Begin - Index
# 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]
## End - Index

## Begin - Security
# Block all direct access for these folders
RewriteRule ^(.git|cache|bin|logs|backup)/(.*) error [F]
# Block access to specific file types for these system folders
RewriteRule ^(system|vendor)/(.*)\.(txt|xml|md|html|yaml|php|pl|py|cgi|twig|sh|bat)$ error
[F]
# Block access to specific file types for these user folders
RewriteRule ^(user)/(.*)\.(txt|md|yaml|php|pl|py|cgi|twig|sh|bat)$ error [F]
# Block all direct access to .md files:
RewriteRule \.md$ error [F]
# Block all direct access to files and folders beginning with a dot
RewriteRule (^\.|/\.) - [F]
# Block access to specific files in the root folder
RewriteRule
^(LICENSE.txt|composer.lock|composer.json|nginx.conf|web.config|htaccess.txt|\.htaccess)$
error [F]
## End - Security

</IfModule>

# Begin - Prevent Browsing and Set Default Resources
Options -Indexes
DirectoryIndex index.php index.html index.htm
# End - Prevent Browsing and Set Default Resources

#AuthType Basic
#AuthName "website"
```

```
#AuthUserFile .htpasswd
#Require valid-user
```