```
<IfModule mod_rewrite.c>
    <IfModule mod_negotiation.c>
        Options -MultiViews
    </IfModule>

    RewriteEngine On

## 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

## Begin - Security
# Block all direct access for these folders
RewriteRule ^(.git|cache|bin|logs|backup)/(.*) error [L]
# Block access to specific file types for these folders
RewriteRule ^(system|user|vendor)/(.*)\.(txt|md|html|yaml|php|twig|sh|bat)$ error [L]
# Block all direct access to .md files:
RewriteRule \.md$ error [L]
# 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|composer.lock|composer.json|nginx.conf|web.config)$ error [F]
## End - Security

    # Redirect Trailing Slashes...
    RewriteRule ^(.*)/$ /$1 [L,R=301]

    # Handle Front Controller
```

```
    # Handle Front Controller...
    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteRule ^ index.php [L]
</IfModule>
```