```
# Security
#ServerSignature Off
#ServerTokens Prod
#expose_php Off
#Header unset Server

# Deny access to certain filetypes
<FilesMatch "\.(htaccess|htpasswd|lang|log|sql|cache|ini)$">
Order Allow,Deny
Deny from all
</FilesMatch>

# Disable Directory Listings
#Options -Indexes

# Options +FollowSymLinks
RewriteEngine on
RewriteBase /

# Rewrite rules to block out some common exploits.
# 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]

# Redirect petitions to the index.php, unless the request adresses an actual file or
directory.
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule ^(.*)$ index.php?$1 [L,QSA]
```