

WARNING: For PHP 7 the module name in the line below need to be modified!

<IfModule mod_php5.c>

php_flag display_errors Off

php_flag log_errors On

php_value error_log logs/errors

php_value upload_max_filesize 5M

php_value post_max_size 6M

php_value memory_limit 64M

php_flag zlib.output_compression Off

php_flag suhosin.session.encrypt Off

#php_value session.cookie_path /

#php_value session.hash_function sha256

php_flag session.auto_start Off

php_value session.gc_maxlifetime 21600

php_value session.gc_divisor 500

php_value session.gc_probability 1

</IfModule>

<IfModule mod_rewrite.c>

Options +SymLinksIfOwnerMatch

RewriteEngine On

RewriteRule ^favicon\.ico\$ skins/larry/images/favicon.ico

security rules:

- deny access to files not containing a dot or starting with a dot

in all locations except installer directory

RewriteRule ^(!installer|\.well-known|/[a-zA-Z0-9]{16})(\.[^\.]+)\$ - [F]

- deny access to some locations

RewriteRule ^/?

(\.git|\.txt|SQL|bin|config|logs|templ|tests|program|<include|lib|localization|steps)) -

[F]

- deny access to some documentation files

RewriteRule /?(README\.md|composer\.json-dist|composer\.json|package\.xml|Dockerfile)\$ -

[F]

</IfModule>

<IfModule mod_deflate.c>

SetOutputFilter DEFLATE

```
SetOutputFilter DEFLATE
```

```
</IfModule>
```

```
<IfModule mod_expires.c>
```

```
ExpiresActive On
```

```
ExpiresDefault "access plus 1 month"
```

```
</IfModule>
```

```
FileETag MTime Size
```

```
<IfModule mod_autoindex.c>
```

```
Options -Indexes
```

```
</ifModule>
```

```
<IfModule mod_headers.c>
```

```
# Disable page indexing
```

```
Header set X-Robots-Tag "noindex, nofollow"
```

```
# replace 'append' with 'merge' for Apache version 2.2.9 and later
```

```
#Header append Cache-Control public env=!NO_CACHE
```

```
# Optional security header
```

```
# Only increased security if the browser support those features
```

```
# Be careful! Testing is required! They should be adusted to your intallation / user environment
```

```
# HSTS - HTTP Strict Transport Security
```

```
#Header always set Strict-Transport-Security "max-age=31536000; preload" env=HTTPS
```

```
# HPKP - HTTP Public Key Pinning
```

```
# Only template - fill with your values
```

```
#Header always set Public-Key-Pins "max-age=3600; report-uri=\"\"; pin-sha256=\"\"; pin-sha256=\"\"" env=HTTPS
```

```
# X-Xss-Protection
```

```
# This header is used to configure the built in reflective XSS protection found in Internet Explorer, Chrome and Safari (Webkit).
```

```
#Header set X-XSS-Protection "1; mode=block"
```

```
# X-Frame-Options
```

```
# The X-Frame-Options header (RFC), or XFO header, protects your visitors against
```

```
clickjacking attacks.
```

clickjacking attacks

Already set by php code! Do not activate both options

#Header set X-Frame-Options SAMEORIGIN

X-Content-Type-Options

It prevents Google Chrome and Internet Explorer from trying to mime-sniff the content-type of a response away from the one being declared by the server.

#Header set X-Content-Type-Options: "nosniff"

CSP - Content Security Policy

for better privacy/security ask browsers to not set the Referer

more flags for script, stylesheets and images available, read RFC for more information

#Header set Content-Security-Policy "referrer no-referrer"

</IfModule>