PHP Configuration Cheat Sheet

Introduction

This page is meant to help those configuring PHP and the web server it is running on to be very secure.

Below you will find information on the proper settings for the `php.ini` file and instructions on configuring Apache, Nginx, and Caddy web servers.

For general PHP codebase security please refer to the two following great guides:

- Paragonie's 2018 PHP Security Guide
- Awesome PHP Security

PHP Configuration and Deployment

php.ini

Some of following settings need to be adapted to your system, in particular `session.save_path`, `session.cookie_path` (e.g. `/var/www/mysite`), and `session.cookie_domain` (e.g. `ExampleSite.com`).

You should also be running PHP 7.2 or later. If running PHP 7.0 and 7.1, you will use slightly different values in a couple of places below (see inline comments). Finally look through the PHP Manual for a complete reference on every value in the php.ini configuration file.

You can find a copy of the following values in a ready-to-go php.ini file here.

PHP error handling

```
expose_php              = Off
error_reporting         = E_ALL
display_errors          = Off
display_startup_errors  = Off
log_errors              = On
error_log               = /valid_path/PHP-logs/php_error.log
ignore_repeated_errors  = Off
```

Keep in mind that you need to have `display_errors` to `Off` on a production server and it's a good idea to frequently notice the logs.

PHP general settings

```
doc_root                = /path/DocumentRoot/PHP-scripts/
open_basedir            = /path/DocumentRoot/PHP-scripts/
include_path            = /path/PHP-pear/
extension_dir           = /path/PHP-extensions/
mime_magic.magicfile    = /path/PHP-magic.mime
allow_url_fopen         = Off
allow_url_include       = Off
variables_order         = "GPCS"
allow_webdav_methods    = Off
session.gc_maxlifetime  = 600
```

`allow_url_*` prevents LFIs to be easily escalated to RFIs.

PHP file upload handling

```
file_uploads            = On
upload_tmp_dir          = /path/PHP-uploads/
upload_max_filesize     = 2M
max_file_uploads        = 2
```

If your application is not using file uploads, and say the only data the user will enter / upload is forms that do not require any document attachments, `file_uploads` should be turned `Off`.

PHP executable handling

```
enable_dl               = Off
disable_functions       = system, exec, shell_exec, passthru, phpinfo, show_sourc
 popen, proc_open,
fopen_with_path, dbmopen, dbase_open, putenv, move_uploaded_file,
chdir, mkdir, rmdir, chmod, rename,
filepro, filepro_rowcount, filepro_retrieve, posix_mkfifo
# see also: http://ir.php.net/features.safe-mode
disable_classes         =
```

These are dangerous PHP functions. You should disable all that you don't use.

PHP session handling

Session settings are some of the MOST important values to concentrate on in configuring. It is a good practice to change `session.name` to something new.

```
 session.save_path               = /path/PHP-session/
 session.name                    = myPHPSESSID
 session.auto_start              = Off
 session.use_trans_sid           = 0
 session.cookie_domain           = full.qualified.domain.name
 #session.cookie_path            = /application/path/
 session.use_strict_mode         = 1
 session.use_cookies             = 1
 session.use_only_cookies        = 1
 session.cookie_lifetime         = 14400 # 4 hours
 session.cookie_secure           = 1
```

```
session.cookie_httponly          = 1
session.cookie_samesite          = Strict
session.cache_expire             = 30
session.sid_length               = 256
session.sid_bits_per_character   = 6 # PHP 7.2+
session.hash_function            = 1 # PHP 7.0-7.1
session.hash_bits_per_character  = 6 # PHP 7.0-7.1
```

Some more security paranoid checks

```
session.referer_check   = /application/path
memory_limit            = 50M
post_max_size           = 20M
max_execution_time      = 60
report_memleaks         = On
track_errors            = Off
html_errors             = Off
```

Suhosin

Suhosin is a patch to PHP which provides a number of hardening and security features that are not available in the default PHP build. However, Suhosin only works with PHP 5, which is **unsupported** and **should not be used**.

For PHP 7, there is Suhosin-ng, but it's in a prerelease stage, and as such **should not be used in production**.

Snuffleupagus

Snuffleupagus is the spiritual descendent of Suhosin for PHP 7 and onwards, with modern features. It's considered stable, and is usable in production.