PHP Secure Configuration Checker
Version 0.1-dev5

SektionEins

[*] This script is rather old. Please check for updates: https://github.com/sektioneins/pcc

critical: 0	high: 4	medium: 1	low: 1	maybe: 7	comment: 2

Risk	Name / Description	Reason	Recommendation
high	php.ini / extension_dir	path is writable or chmod-able.	An attacker may try to leave a PHP extension in the extensions directory. This directory should not be writable and the web user must not be able to change file permissions
high	Writable document root Checks if the current document root is writable	document root is writable.	Making the document root writable may give an attacker the advantage of persisting an exploit. It is probably best to restrict write access to the document root and its subdirectories. Temporary files your application may need to write can be safely stored outside the document root.
high	Writable include_path Checks if at least one directory listed in the include_path is writable	The directory '.' is writable.	An attacker may try to place a file here.
high	Writable include_path Checks if at least one directory listed in the include_path is writable	The directory '/Applications/MAMP/bin/php/php5.6.10/lib/php' is writable.	An attacker may try to place a file here.
medium	php.ini / session.use_strict_mode	strict mode not activated.	If activated, PHP will regenerate unknown session IDs. This effectively counteracts session fixation attacks.
low	php.ini / open_basedir	open_basedir not set.	Usually it is a good idea to restrict file system access to directories related to the application, e.g. the document root.
maybe	php.ini / intl.error_level	ICU functions fail with error.	An error induced by an attacker can change the program's control flow and may lead to unexpected side-effects.
maybe	php.ini / ldap.max_links	Number of LDAP connections not limited.	In order to prevent denial-of-service attacks this options should be set to the lowest number possible. If LDAP is not needed at all, the LDAP extension should not be loaded in the first place.
maybe	php.ini / memory_limit	Memory limit is 128M or more.	A high memory limit may easily lead to resource exhaustion and thus make your application vulnerable to denial-of-service attacks. This value should be set approximately 20% above an empirically gathered maximum memory requirement.
maybe	php.ini / session.cookie_httponly	no implicit httpOnly-flag for session cookie.	This option controls if cookies are tagged with httpOnly which makes them accessible by HTTP only and not by the JavaScript. httpOnly cookies are supported by all major browser vendors and therefore can be instrumental in minimising the danger of session hijacking. It should either be activated here or in your application with session_set_cookie_params().
maybe	php.ini / session.cookie_lifetime	no implicit lifetime for session cookie.	Not limiting the cookie lifetime increases the chance for an attacker to be able to steal the session cookie. Depending on your application, this should be set to a reasonable value here or with session_set_cookie_params().
maybe	php.ini / session.cookie_secure	no implicit secure-flag for session cookie.	This options controls if cookies are tagged as secure and should therefore be sent over

			SSL encrypted connections only. It should either be activated here or in your application with session_set_cookie_params().
maybe	Suhosin Checks whether the Suhosin-Extension is loaded	Suhosin extension is not loaded	Suhosin is an advanced protection system for PHP. It is designed to protect servers and users from known and unknown flaws in PHP applications and the PHP core. For more information see http://suhosin.org/
comment	php.ini / intl.default_locale	ICU default locale not set.	The ICU default locale is not set explicitly, which forces the usage of ICU's default locale.
comment	php.ini / session.name	default session name.	Your session name is boring. Why not change it to something more suitable for your application?