PHP absichern

Konfigurationsdatei

PHP hat für jede Verwendung eine eigene Konfigurationsdatei namens php.ini.
Ihr müsst also Erfahrung bringen, welche für euch relevant ist. Bei Apache2 liegt die php.ini unter /etc/php5/apache2/php.ini.
Die meisten Einstellungen lassen sich auch mit entsprechenden Funktionsaufrufen für jedes Projekt einzeln setzen.
Passt aber auf, dass ihr die globale Einstellung nicht durch schlecht konfiguriertes error_reporting() aushebelt.

Inhaltsverzeichnis

Keine Fehlermeldungen zeigen

Ihr solltet dem Benutzer keine Fehlermeldungen zeigen. Häufig bekommt er den Stacktrace geliefert mit Funktionsparametern zu sehen.
Fatal wäre hier zum Beispiel ein Konstruktor mit den Datenbankbankverbindungsdaten.

Ihr löst das Problem indem ihr Warnungen ausblendet und fatale Fehler mit einer leeren Seite quittiert.
Dazu sind folgende Einstellungen notwendig

Quellcode

```
1. log_errors = On
2. display_errors = Off
```

Version unterdrücken

Die Kenntnis der verwendeten PHP Version bietet eine potentielle Angriffsfläche für den Angreifer. Für zahlreiche alte PHP Versionen sind exploits bekannt, die dem Angreifer erweiterte Rechte geben.

Die PHP Version wird nicht einfach sichtbar mitgeliefert, erfährt man aber indem man die HTTP Abfrage direkt (z.B. über Telnet) durchführt.

Da die meisten Distributoren eigene PHP Versionen kompilieren, kann man im Beispiel sogar auf das verwendete Betriebssystem schließen.

Quellcode

```
1. HTTP/1.1 200 OK
2. Date: Thu, 12 Mar 2009 16:29:00 GMT
3. Server: Apache
4. X-Powered-By: PHP/5.2.0-8+etch4
5. Cache-control: max-age=3600, must-revalidate
6. Pragma: public
7. Content-Length: 0
8. Connection: close
9. Content-Type: text/html; charset=UTF-8
```

Folgende Einstellung verhindert das Senden von "X-Powered-By"

Quellcode

1. expose_php = Off

Keine phpinfo()

Entwickler tauschen häufig die Einstellungen ihrer PHP-Konfiguration aus. Solch eine Konfiguration ist das Herz von PHP und hat nichts im öffentlich erreichbaren Web zu suchen.
Ihr solltet also keine öffentlich erreichbaren phpinfo.php Dateien anlegen.

register_globals

register_globals ist eine Eigenschaft die auf modernen Umgebungen auf **off** zu setzen ist.
Ist die Funktion aktiviert sind die Variablen $_POST['foo'] und $foo gleichzusetzen. Es ist die Angriffsfläche für viele verbreitete Scripte.