Content Management System - Joomla! - PHP

== Beschreibung ==
Joomla ist das CMS, das sich in den letzten Jahren immer weiter an Typo3 (Light) heranpirschen konnte. Dies liegt nicht allein daran, dass es eine große Community besitzt.
Doch dieses CMS fällt nicht nur durch Positives auf, es müssen immer selbst Bugfixes nachgelegt werden, da man dessen Auftreten nicht leugnen kann.
Durch Joomla API gibt es eine große Menge an Erweiterungen von privaten Programmierern.
Allerdings gibt es dadurch eine Vielzahl von Patches, die nicht wirklich zur Sicherheit beitragen.
Es gibt grundlegende Sicherheitseinstellungen, die auch auf andere CMS's übertragbar sind.

Absicherung auf Dateisystemebene
Absicherung auf HTTP – Ebene
Absicherung auf Datenbankebene

Ein sehr gutes Tool zur automatisierten Überprüfung des gesamten Webservers ist das „Joomla Tool Suite“. ?
joomlacode.org/gf/project/jts/fr
Bei der Installation ist darauf zu achten, dass setup.exe Joomla 1.5 im Legacy-Modus ausgeführt wird.
Dazu muss das Legacy – Plugin von Joomla aktiviert werden. Nach dieser Installation und dem Testen von JTS sollte man allerdings die Software wieder deinstallieren und das Plugin deaktivieren.
(Das Assessment – Rating in der Ratgeber – Funktion, sollte auf 100% kommen.)

== PHP - Security ==
Zur PHP – Sicherheit, sollte eine Datei erstellt werden „phpinfo.php“ hier muss folgender Content eingetragen werden: „phpinfo();“ (natürlich ohne „“). Diese Datei wird dann in das Root – Verzeichnis eingefügt.
Nun kann man die Datei im Browser aufrufen ? meinedomain.de/phpinfo.php
Hier kann man dann die Ausgabe von dem Skript überprüfen. „magic_quotes“ sollte aktiviert sein, „register_globals“ hingegen nicht.
Die Überprüfung ist an der Stelle kein Muss, das Skript kann auch später im Backend unter Hilfe ? Systeminfo kontrolliert werden.
Falls die beiden Erweiterungen in PHP einen anderen Wert als den, der empfohlen wurde, aufweisen, erstellt man im Root – Verzeichnis eine „.htaccess – Datei“ mit nur zwei Zeilen:

php_flag register_globals off
php_ flag magic_quotes_gpc on

Falls diese beiden nicht funktionieren sollten, gibt es noch eine weitere Schreibweise:

php_flag register_globals 0
php_flag magic_quotes-gpc 1

== Verbergen von htaccess.txt ==
Im Allgemeinen sollte man mitgeführte „htaccess.txt“ - Datei in „.htaccess“ umbenennen und um die entsprechenden Zeilen erweitern.
Der Vorteil besteht darin, dass in der Joomla – Config mittels „mod_rewrite“ das 'Umschreiben' aktiviert werden kann.

== Die aktuelle Version von Joomla! vertuschen ==
Des Weiteren ist es wichtig die aktuelle Version von Joomla zu vertuschen, oder auch das Joomla benutzt wird, dies gibt einem Hacker weniger Informationen über mögliche Sicherheitslücken.
Zwar kann man mit Hilfe der Bilder in Joomla (images ? stories) das vorliegende CMS identifizieren, aber es ist besser so viele Informationsquellen wie möglich auszuschalten.
Darum sollte auch das „favicon“ der eigenen URL geändert werden, dies kann der Einfachheit halber mit einem favicon – Generator aus dem WwW gemacht werden. (Meine Empfehlung: favicon-generator.org/) oder einfach mal bei Google suchen.
Nach der Installation wird standardmäßig der Benutzer „admin“ angelegt, dieser sollte in einen beliebigen Namen verändert werden.

Weiter muss die „guration.php“ gesichert werden. Man muss ein Verzeichnis auf dem Webserver erstellen und hier die

„configuratation.php“ einfügen. Die Datei umbenennen in „.htcinf.php“.
(der Punkt vor dem Dateinamen verstekt die Datei auf dem Web – Server bei normaler Config des Servers.)
Nach diesem Schritt muss eine Datei im Root – Verzeichnis erstellt werden mit Namen „configuration.php“ hier muss folgendes eingefügt werden:

Quellcode

```
1. <?php include("{Verzeichnisname}/.htconf.php"); ?>
```

(Diese Zeile -Verzeichnisname- wird ohne die geschweiften Klammern geschrieben.)
Dieser Befehl macht, dass die configuration – Datei in die ihr entsprechenden configuration – Datei im Root eingefügt wird. Zum Schluss müssen die Rechte dieser Datei verändert werden (? Zahl auf 640 setzen).

== Das SEO - Patch ==
Mit Hilfe des Patches „SEO“ kann man, wenn man möchte, noch den Meta – Tag "generator" entfernen. Durch den Patch kann man im normalen Quelltext von der Website nicht mehr erkennen, dass es sich dabei um eine Joomla – Seite handelt. Eine andere Möglichkeit wäre es den Generator – Text manuell zu ändern. Wenn man es so machen will, muss man in die Datei 'libraries/joomla/document/document.php'.
Nun muss in der Zeile 85 nur der Inhalt des Generators geändert werden. Der Nachteil ist, dass wenn ein Update durchgeführt wird diese Datei wieder überschrieben wird. (ist aber noch nicht bei jedem Update der Fall gewesen)
Auch das Backend kann verschleiert werden. Dazu muss man sich das Plugin „JSecure“ downloaden. „JSecure“ ermöglicht es, die Backend – URL, um einen gewünschten Parameter erweitern zu können. Dadurch gelangt man nicht mehr über: meinedomain.de/administrator in das Backend, sondern man fügt einen Parameter ein, der wie folgt lautet: meinedaomain.de/administrator/?parameter
Daraus folgt eine Fehlermeldung von Joomla,wenn eine URL eingegeben wird, die nicht existiert, weil sie ja geändert wurde. Hierzu erstellt man einfach eine Datei im Template – Ordner namens „error.php“. In diese Datei muss der „Errorcode“ von Norbert Bayer eingefügt werden. Dadurch wird statt Standard – Fehlermeldung von Joomla nun auf Sucher weitergeleitet. (Die Information stammt von redim.de/downloads/joomla-1.5/keine-fehlerseiten.html und kann auch dort gedownloaded werden.)

== Die error.php ==

Quellcode

```
1. <?php
2. # error.php for Joomla 1.5.x
3. # reDim - Norbert Bayer (www.redim.de)
4. # 07.04.2009 - V1.1
5. // no direct access
6. defined( '_JEXEC' ) or die( 'Restricted access' );
7. $link=strtolower($_SERVER['REQUEST_URI']);
8. if($ar = @parse_url($link)){
9. $link=$ar['path'];
10. $link=strrchr($link,DS);
11. $link=str_replace(DS," ",$link);
12. $link=str_replace("-"," ",$link);
13. $ch=strrchr(strtolower($link),".html");
14. if ($ch){
15. $link=substr($link,0,-5);
16. }
17. $link=trim(htmlspecialchars($link));
18. $link="index.php?option=com_search&view=search&searchword=".$link;
19. $component =& JComponentHelper::getComponent('com_search');
20. $menus= &JApplication::getMenu('site', array());
21. $items= $menus->getItems('componentid', $component->id);
22. if ($items){
```

```
29. if ($items[0]->id>0){
30. $link.="&Itemid=".$items[0]->id;
31. }
32. }
33. $link=JRoute::_($link);
34. global $mainframe;
35. $mainframe->redirect( $link, "" );
36. }else{
37. #### Hier können Sie Ihre Funktionen einbauen um Hackangriffe besser zu erkennen und zu protokollieren.
38. echo JText::_("Hack Verdacht, Ihre IP wurde gespeichert!");
39. die();
40. }
41. ?>
```

Alles anzeigen

== Tipp ==
Ein weiterer Tipp ist es immer die aktuellen Updates zu installieren und die Erweiterungen auf auftretende Sicherheitslücken zu prüfen.
Man kann aber sagen, dass man lieber Erweiterungen weglassen kann und nicht installiert, wenn diese Sicherheitslücken aufweisen. Auf den folgenden Seiten, kann man nach gucken, ob die eigenen Erweiterungen aufgelistet sind. Falls ja, sollte man sofort handeln und Erweiterungen entfernen.

joomlaos.de/Security.html
joomla-downloads.de/sicherheit…en/unsichere-komponenten/
joomla-grundlagen.de/das-web-c…system/erweiterungen.html

Auch nach der Installation erhält man schon Hinweise auf Erweiterungen. Direkt nach dem Login, in das Backend, bekommt man auf der rechten Seite ein Pfeil, ob man ein „Update nötig?“ hat.
Dort wird angezeigt, ob Erweiterungen oder Aktualisierungen allgemein zur Verfügung stehen.
Auch hier gibt es schon Hinweise zu den Updates.
[Blockierte Grafik: http://img607.imageshack.us/img607/7827/joomlabackendupdatentig.jpg]
Diese beschriebenen Methoden kann man teilweise ohne weiteres auf andere CMS's übertragen.
Wenn man in der Joomla Einrichtung der Joomla – Config nach allen diesen oben beschriebenen Kriterien vorgeht, hat man nichts mehr zu befürchten.
Aber wie es halt immer so ist in der IT – Security, nichts ist zu 100% sicher, immer gibt es Jemanden oder ein System, dass all diese Vorkehrungen umgehen kann. Allerdings macht man es durch alle beschriebenen Verfahren für einen möglichen Angreifer schwerer, Sicherheitslücken zu finden und diese zu auszunutzen.

Ich hoffe ich kann dem Einen oder Anderen mit dieser Antwort zu dem Thema „Content Management System – Joomla“ weiter helfen.
Bei weiteren Fragen zu einzelnen Themen oder Anregungen, möglicher Fehler, die ich in dem Text gemacht haben könnte, bitte ich darum sich bei mir per email zu melden. Ich werde dann im schlimmsten Fall xDD alles neu schreiben müssen ;-).

Ich von mir aus kann sagen, dass Joomla knapp unter Typo3 eines der erfolgreichsten CMS ist.
Es gibt keine Endlösung für das Bedienproblem, welches bei allen CMS's auftritt. Ich habe mich am meisten mit Joomla! befasst, also kann ich leider nur für Joomla sprechen und keine anderen Argumente für oder gegen konkurrierende Systeme auflisten.
Für mich glänzt die große Community von Joomla!

== Quellen: ==
joomla.org/
joomlaos.de/
gn-webdesign.de/joomla-tutorials/joomla-sicherheit.html
redim.de/

MfG der >>>spacehero<<<