Gerald Martin
Dipl.-Inf. (FH)

August-Bebel-Str. 10
D-08118 Hartenstein

Joomla! 1.5
Security Checklist + hidden secrets :)

Stand 2010-12-03

Hinweise
Diese Security Checklist stellt keine offizielle Anleitung für den Umgang mit Joomla! 1.5 dar.
Die Liste entstand durch die tägliche Arbeit mit dem System und den damit verbundenen Erfahrungen.
Diese Erfahrungswerte sind in dieser Liste zusammen gefasst und sind als Empfehlung gedacht.
Diese Security Checklist hat keinen Anspruch auf Vollständigkeit.

die HTACCESS-Datei

Mittels der Datei [***.htaccess***] lassen sich viele Webserverfunktionen modifizieren. Das machen wir uns zunutze. Ob die aufgeführten Änderungen wirklich umgesetzt werden können, hängt vom jeweiligen Provider ab.

a) Joomla! vom FTP-User im Fast-CGI-Modus ausführen lassen

An den Anfang der [.htaccess]-Datei muss folgender Code:

```
AddHandler php5-cgi .php
```

Mit diesem Steuerbefehl weißt man Apache (den Webserver) nicht nur an, alle PHP-dateien mit PHP5 zu interpretiern, es wird damit auch der Fast-CGI-Modus genutzt.
Die Syntax dieser Anweisung kann sich auch von Provider zu Provider unterscheiden.
Diese Anweisung wurde mit dem Provider *all-inkl.com* erfolgreich getestet.

b) Double Content vermeiden

Double Content ergibt sich zum Beispiel daraus, dass www.domain.de und domain.de (ohne www) auf das gleiche Docroot zeigen. UM DC zu vermeiden, sollte eine saubere 301-Weiterleitung

eingerichtet werden.

```
RewriteEngine On

RewriteCond %{HTTP_HOST} ^rs-systeme\.com$ [NC]
RewriteRule ^(.*)$ http://www.rs-systeme.com/$1 [R=301,L]
```

c) Die „Register Globals Emulation“ deaktivieren

```
php_flag register_globals off
```

Versionsinformationen von Joomla!-Core und Erweiterungen verstecken

XML-Dateien:

```
<Files ~ "\.xml$">
Order allow,deny
Deny from all
Satisfy All
</Files>
```

Administrator-Verzeichnis separat schützen

Kontrolle aller Verzeichnis- und Dateirechte und korrekte Rechte setzen

configuration.php auf ***nicht beschreibbar*** setzen

Generator-Tag Joomla! 1.5 entfernen/ändern

```
$this->setGenerator('MadeByWonderfulOpenSourceCMSCAlledDschummLa');
```

„Template-Positions“-Anzeige verhindern

```
JRequest::setVar('tp',0);
```

Joomla!-Seite für Google-Bildersuche öffnen

Aus robots.txt entfernen:

```
Disallow: /images/
```

Meta-Tags (Description/Keywords) ändern (ohne „Joomla“ im Kontext)

Gerald Martin
Dipl.-Inf. (FH)

August-Bebel-Str. 10
D-08118 Hartenstein

User-Account ***admin*** mit ID 62 löschen

Datenbank-Prefix jos_ ändern

configuration.php unbeschreibbar (444)

ungenutzte Dateien bzw. nicht verwendete Erweiterungen entfernen

Nicht verwendete Erweiterungen des Joomla!-Kerns deaktivieren
Beispiel: Suche (com_search)

Verwendete Erweiterungen auf Schwachstellen überprüfen
Anlaufpunkte:

http://docs.joomla.org/Vulnerable_Extensions_List
http://developer.joomla.org/security/news.html (Joomla! Core)

Quellen

Übersetzung und Ergänzung von:
http://docs.joomla.org/Category:Security_Checklist
http://brian.teeman.net/tips-and-tricks/joomla-hidden-secrets-the-movie.html