Sehr geehrter Interessent,
bei diesem Dokument im PDF-Format handelt es sich um eine Leseprobe des E-Books. Das E-Book selbst umfasst 57 Seiten geballte Information zum Thema Sicherheit unter Joomla 5 und Joomla 6.

Sie finden in dieser Leseprobe:

- Die ersten 8 Seiten des Sicherheits- E-Books,
- das gesamte Inhaltsverzeichnis des E-Books.

Updates zu unseren Handbüchern:

Ein einmal gekauftes Handbuch im E-Book-Format können Sie 12 Monate lang in Ihrem Kundenkonto updaten. Dort finden Sie jeweils die aktuelle Version. Diesen Updatezeitraum können Sie jederzeit zum Sonderpreis verlängern. Wir informieren Sie regelmäßig über wichtige Aktualisierungen.

Der EBW Joomla Club:

Weitere wichtige E-Books und Tools finden Sie in unserem EBW Joomla 365er Club. Als Mitglied des Clubs sind Sie bei Joomla und Co. stets auf dem Laufenden und haben Zugriff auf ein reichhaltiges Angebot an Beiträgen und Tools. Dort finden Sie, neben weiteren Dokumentationen zu wichtigen Themen rund um Joomla, nützliche Erweiterungen zur Optimierung und Tools zur Absicherung gegen Schadsoftware. Als Clubmitglied genießen Sie bis zu 50% Rabatt bei weiteren Einkäufen.
Nun wünschen wir Ihnen viel Spaß mit dieser Leseprobe.
Ihr EasyBay-Web Team

Sie kommen selber nicht weiter und benötigen professionelle Hilfe. Egal ob Sie Ihre Joomla Installation effektiv absichern wollen. oder Unterstützung nach einem Angriff benötigen. Hier finden Sie unsere entsprechenden Serviceangebote zum Thema Sicherheit.

Nun wünschen wir Ihnen viel Spaß mit dieser Leseprobe.
Ihr EasyBay-Web Team


Joomla
Sicherheit unter
Joomla
E-Book
eBook

Vorwort zum Thema Sicherheit:

Sie kennen es von Ihrem eigenen Computer. Sobald man mit dem Rechner im Internet ist, gibt es ständig Angriffe auf Ihren Computer. Wenn Sie keine Sicherheitstools, wie Virenscanner und Firewall einsetzen, ist Ihr Computer in kürzester Zeit verseucht oder von extern übernommen.

Sehen Sie sich mal die Protokolle Ihres Virenscanners und Ihrer Firewall an, dann wissen Sie, was ich meine. Also, gute Sicherheitstools und Einstellungen sind zwingend erforderlich.

Genauso ist es auch mit Ihrem Internetauftritt. Sie müssen Ihre Dateien und Verzeichnisse in Ihrer Domain schützen. Dieses erfolgt mit Ordner- und Dateirechten und mit Zugriffseinstellungen, die in einer oder mehreren Dateien Namens ***.htaccess*** zusammengefasst werden.

Das Joomla Packet beinhaltet auch eine Datei mit dem Namen ***htaccess.txt***. Diese enthält aber nur einige wichtige Grundeinstellungen. Sie wird durch Umbenennung in ***.htaccess*** aktiviert. Dabei den führenden Punkt nicht übersehen. Die Einstellungen sind aber nur sehr allgemein gehalten und der Zugriffschutz ist absolut nicht ausreichend, er kann noch wesentlich verbessert werden

Die ***.htaccess*** kann quasi zu einer regelrechten Firewall ausgebaut werden. Außerdem ist es durch entsprechende Einträge möglich, die Geschwindigkeit einer Webseite sehr positiv zu beeinflussen.

Das ist besonders wichtig, da immer mehr Internetnutzer mit mobilen Endgeräten z.B. Smartphones in das Internet gehen. Alle Suchmaschinen beurteilen eine Webseite auch besonders nach der Geschwindigkeit des Aufbaus der Seiten. Es ist einer der wichtigsten Faktoren für die Platzierung bei Google und Co.

Alles Wissenswerte dazu finden Sie in diesem Handbuch. Außerdem liegt diesem Handbuch eine ***.htaccess*** Datei bei, in der die zuvor Beschriebenen Maßnahmen zur Sicherheit und Steigerung der Geschwindigkeit optimal umgesetzt sind.

1 So sichern Sie Ihre Joomla Webseite effektiv gegen Angriffe ab

Mit der Umsetzung der folgenden Maßnahmen sichern Sie Ihre Joomla Installation ab:

- sichere Zugangsdaten zum Backend,
- Schützen Sie den Administrator- Zugang mit einer vorgeschalteten Sicherheitsabfrage,
- Dateiberechtigungen der Joomla Installation richtig setzen,
- regelmäßige Datensicherung,
- optimierte .htaccess als Firewall nutzen,
- Sicherheitstool installieren, das die Datenbank schützt und Angriffsversuche dokumentiert,
- Halten Sie eine aktuelle lokale Kopie des Joomla Template vor.
- Halten Sie eine aktuelle lokale Kopie der Joomla Datenbank vor.
- Lassen Sie Ihre Joomla Installation in regelmäßigen Zeitabständen automatisch von entsprechenden Scannern überwachen.

1.1 Die Ordner- und Dateirechte richtig setzen:

Einen ersten und effektiven Schutz erreichen Sie, wenn Sie die Ordner und Dateien mit den minimalen möglichen Rechten versehen. Nachfolgend die Werte für die einzelnen Ordner und Dateien.

Diese Dateien brauchen nur Leserechte („0444“):

- index.php
- configuration.php
- /administrator/index.php
- /templates/*Ihr Template*/index.php
- Alle „.htaccess“-Dateien
- Alle Dateien mit der Endung „.css“

Alle anderen Dateien erhalten die ***Rechte („0644“).***

Alle anderen Ordner erhalten die ***Rechte („0755“).***

1.2 Allgemeine Informationen zu .htaccess:

.htaccess (engl. hypertext access „Hypertext-Zugriff“) ist eine Konfigurationsdatei, in der verzeichnisspezifische Einstellungen auf Webservern (z. B. Apache) vorgenommen werden können.

Beispielsweise lässt sich dort ein Zugriffsschutz durch HTTP-Authentifizierung (auch ein zusätzlicher Passwortschutz ist möglich) für ein Verzeichnis oder einzelne Dateien einrichten. Aber auch Fehlerseiten oder interne Verknüpfungen (siehe Rewrite-Engine) lassen sich hierüber einstellen, ohne den Server neu starten zu müssen.

Änderungen in der .htaccess-Datei treten immer sofort in Kraft, da diese bei jeder Anfrage an den Webserver ausgewertet werden. In diesen Dateien vorgenommene Einstellungen wirken wie <Directory>-Abschnitte in zentralen Konfigurationsdateien (z. B. httpd.conf). Sie gelten für das Verzeichnis, in dem sie gespeichert sind, sowie allen Unterverzeichnissen. Das heißt, die Einstellungen in einer ***.htaccess*** Datei im ***root*** Verzeichnis einer Joomla Installation gilt auch in allen Unterordnern. Jedoch können die Einstellungen in den Unterverzeichnissen wieder überschrieben werden, indem man dort eine weitere ***.htaccess*** platziert.

1.2.1 Sicherheit durch optimierte .htaccess- Dateieinträge:

In Joomla werden alle Aufrufe zentral über eine Datei gesteuert. Alle abgerufenen Webseiten werden erst mit den in der Datenbank vorhandenen Daten temporär gebildet. Diese Daten und zusätzlich benötigte Dateien werden nur in diese zentrale Datei hinein geladen. Diese Logik kann man sich bei der Absicherung von Joomla zu Nutze machen, da außer auf diese zentrale Datei kein weiterer Zugriff auf andere Dateien nötig ist.

Die nachfolgend aufgeführten Konfigurationen und Anpassungen können sehr aufwändig sein. Für eine sichere Webseite sind sie aber zwingend erforderlich. Man kann sich das ganze erheblich erleichtern, wenn man die mit diesem Handbuch gelieferte ***.htaccess*** Datei benutzt.

Wir werden in diesem Kapitel auf die grundsätzlichen Möglichkeiten einer manuellen Absicherung eingehen.

1.2.2 Ordnerschutz durch .htaccess Dateien:

Die nachfolgend aufgeführten Ordner sollten zusätzlich durch eine .htaccess Datei geschützt werden. Das ist allerdings nur dann notwendig, wenn Sie die von uns mitgelieferte ***.htaccess Firewall*** nicht einsetzen. Diese schützt zuverlässig auch alle Unterverzeichnisse.

- /administrator/cache
- /administrator/includes
- /administrator/language
- /administrator/manifests
- /cache
- /cli
- /includes
- /language
- /libraries
- /logs
- /tmp

Der Dateiinhalt der .htaccess in diesen Ordner sollte so aus aussehen:

```
<Files "*.*">
Deny from all
</Files>
```

Durch den Befehl „***Deny from all***“ wird der direkte Zugriff auf alle Dateien, Unterverzeichnisse und das Verzeichnis, in dem diese ***.htaccess***- Datei abgelegt ist, verweigert.

Da es einige Ordner gibt, aus denen Bilder und Dateien geladen werden müssen, ist für diese Ordner eine Variante der ***.htaccess*** Datei erforderlich:

Inhalt dieser .htaccess Datei:

```
<Files "*.*">

Deny from all

</Files>

<FilesMatch "\.(js|css|png|jpg|jpeg|gif|ico|flv|swf|pdf)$">

Allow from all

</FilesMatch>
```

Diese angepasste .htaccess Datei sollte in die folgenden Ordner eingebracht werden:

- /administrator/components
- /administrator/help
- /administrator/modules
- /administrator/templates
- /components
- /images
- /media
- /modules
- /plugins
- /templates

Ausnahmen für bestimmte Erweiterungen:

Es kann durchaus vorkommen, dass bestimmte Erweiterungen einen Direktaufruf von PHP- oder HTML- Dateien benötigen.

In einer entsprechenden Anweisung, für einen Dateidirektaufruf, kann zum Beispiel eingetragen sein:

```
<Files dateiname.php>

Allow from all

</Files>
```

Dabei müssen natürlich Eintrag ***dateiname.php*** durch den realen Dateinamen ersetzen.

Ausnahme für den Editor TinyMCE:

Bei diesem vielfach eingesetzten Editor in Joomla ist eine spezielle Variante erforderlich, die im Ordner ***/media/editors/tinymce*** abgelegt werden muss.

```
<FilesMatch "\.(htm|html)$">

Allow from all

</FilesMatch>
```

1.2.3 Joomla Sicherheit durch unsere .htaccess Firewall:

Machen Sie die ***.htaccess*** zu einer Firewall. Wir bieten Ihnen eine auf Sicherheit optimierte ***.htaccess***. Diese htaccess Datei mit vielen Sicherheitseinstellungen ist durchaus als Firewall zu betrachten.

Außerdem befinden sich in ihr auch Parameter die den Cache der Seite und des Browsers aktivieren und somit für eine erhebliche Geschwindigkeitssteigerung sorgen. Die ***.htaccess Datei*** ist Bestandteil dieses Handbuchs.

Sie müssen die Datei ***htaccess.txt*** einfach in das Root Verzeichnis Ihrer Joomla Webseite auf den Webserver hochladen. Anschließend müssen Sie die ***htaccess.txt*** in ***.htaccess*** umbenennen. Dann das Ganze testen.

Sollte es danach zu einem Serverfehler 500 kommen, sind meist Einstellungen für die RewriteEngine schuld. Diese können in seltenen Fällen von Provider zu Provider voneinander abweichen.

Die RewriteEngine ist für Weiterleitungen (Redirects) verantwortlich, dieses wird mit dem Parameter ***RewriteEngine On*** aktiviert. Sie können es ganz leicht testen, indem Sie den Parameter auf Off setzen, oder die Zeilen in der ***.htaccess*** mit # auskommentieren. In diesem Fall muss allerdings in der Joomla Konfiguration (Suchmaschinenoptimierung SEO) der Parameter ***URL-Rewrite nutzen*** ausgeschaltet sein.

Tritt nach diesen Maßnahmen der Fehler nicht mehr auf, dann befragen Sie ihren Provider nach den notwendigen Einstellungen für die ***RewriteEngine.***

Wenn der Fehler trotzdem noch auftritt, ist es mit der Kompatibilität des Webservers nicht zum Besten bestellt. Mein Rat dazu; wechseln Sie den Provider. Unsere Empfehlung für einen günstigen und zuverlässigen Provider lautet HostEurope.

13 Inhaltsverzeichnis:

14 Zu den Autoren und Copyright ©:

Karl-Heinz Derhake:

Der Autor Karl-Heinz Derhake hat mehr als zwanzig Jahre Erfahrung im Projekt Management in den Bereichen Hardware- Computer- Softwareentwicklung, und staatliche Sicherheitstechnologien. Seit mehr als acht Jahren setzt er seine Projekterfahrungen mit Content Management Systemen in praktische Handbücher um. Er berät Firmen und Staaten in der Umsetzung von Internet- und Sicherheitsprojekten.

Jan Derhake:

Er ist verantwortlich für Layout und Gestaltung.

Caren Pott:

Lektorat

Bei Fragen stehen wir Ihnen gerne mit Rat und Tat zur Verfügung.

Ihr EasyBay-Web Team