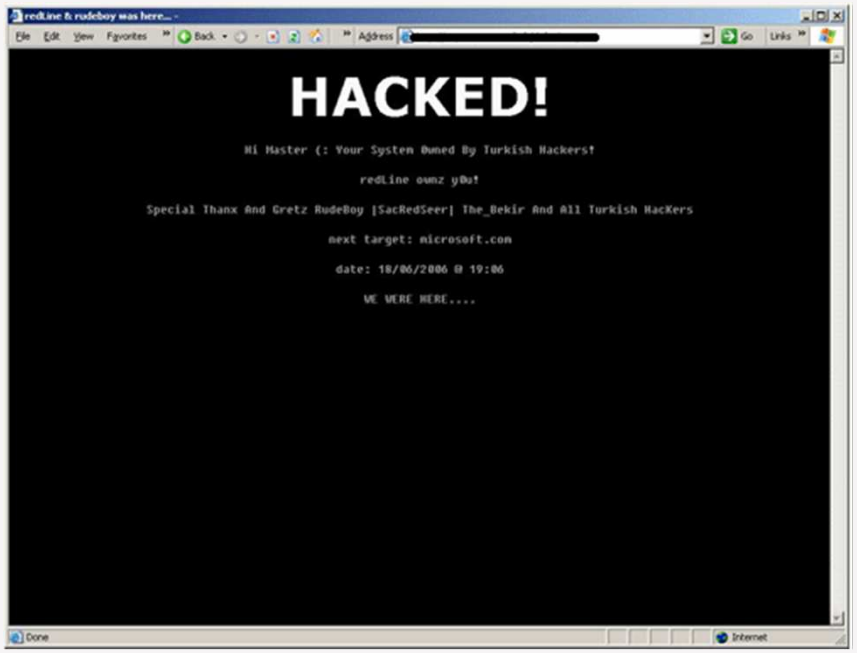
Es gibt keine 100 % ige Sicherheit, man kann sie nur anstreben.

Joomla!-Sicherheit

von Joomla-Security.de

Jan Erik Zassenhaus & Christian Schmidt

Wollen Sie sowas?



Allgemeines

PC

- Anti-Viren-Software
- Firewall
- Updates des Systems und von der eingesetzten Software

Passwörter

NICHT: „passwort“, „admin“, „sysadmin“, „operator“, „manager“, „gott“, „123456“
Besser: *?(ttmAJw3SNcN?E$,{MZ5n)+E%dEbKT8X}q/$!z3b$+&n

Allgemeines

Joomla!

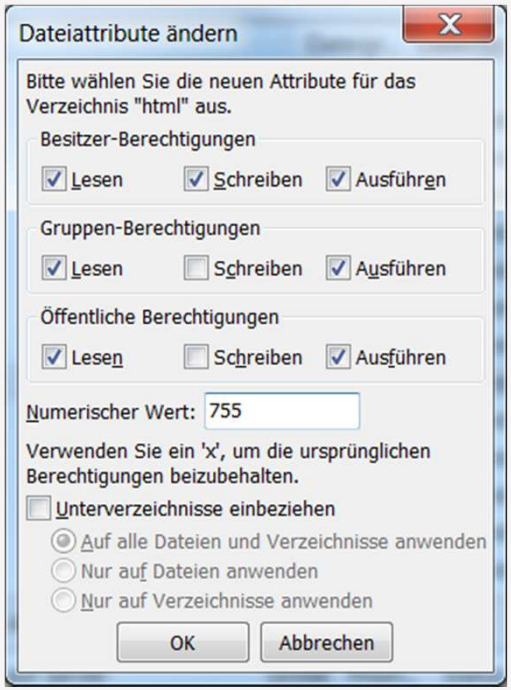
- Updates vom Core (Ab 1.6.5 Updates über den Administrationsbereich aktualisierbar)
- Updates der eingesetzten Erweiterungen
- Keine unsicheren Erweiterungen einsetzen -> Sicherheitsmeldungen auf www.joomla-security.de

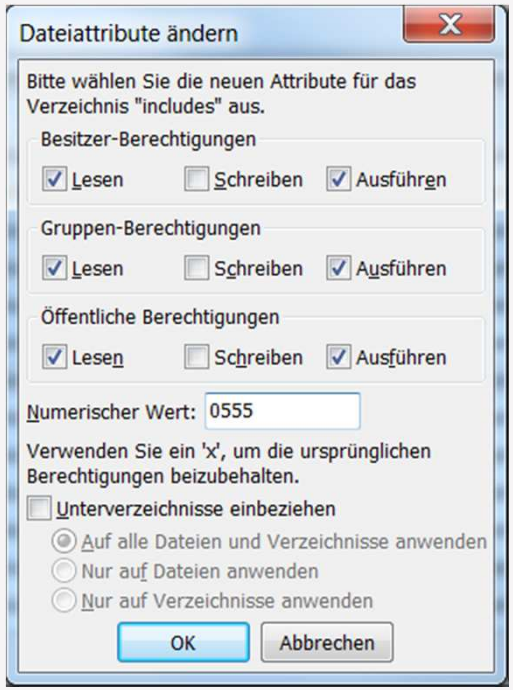
Allgemeines

Verzeichnisse & Dateien

- Rechte für Ordner : 0755 (besser 0555)
- Rechte für Dateien: 0644 (besser 0444)
- Die configuration.php immer 0444

Achtung: Für einige Ordner müssen min. 0755 Rechte vorliegen, wie z.B. für den Cache





Allgemeines

Richtiger Hoster

- Mittwald ☺
- Schwarzkünstler
- FC Hosting
- Hosteurope
- InternetX
- DM Solutions
- Joomla100
- usw.

Backup

Backups, Backups und noch mal Backups!

- Es sollten immer mehre Backups vorgehalten werden
- Backups an unterschiedlichen Orten lagern
- Backuperweiterung AkeebaBackup
- Zeitgesteuerte Backups (Cron)

Templates

Security by Obscurity - Sicherheit durch Verschleierung

- Nicht benutzte Templates
- Die Option „&tp=1“
- Die Option „?template=beez“
- Generator-Tag
- Fußzeilen-Informationen
- Die error.php (Fehlerseite)“

Sichere Joomla!-Einstellungen

Durch Kleinigkeiten Großes bewirken

- Benutzerregistrierung deaktivieren
- Aktivierung neuer Konten durch Administrator
- Ab 1.6 generell keine Berechtigungen („Nicht erlaubt“) setzen
- Super Administrator nicht auf ID 62 (42) und Benutzernamen „admin“ belassen

Sichere Joomla!-Einstellungen

Durch Kleinigkeiten Großes bewirken

- Tabellenpräfix ändern : „jos_“ nicht belassen
- Administrationsbereich mit Passwort (Htaccess) zusätzlich sichern
- Keine FTP- und SMTP-Daten im Administrationsbereich hinterlegen
- Verlegen Sie den Pfad des „tmp“- und „logs“-Verzeichnisses außerhalb des „Document Roots“

Sichere Joomla!-Einstellungen

Durch Kleinigkeiten Großes bewirken

- Systemkomponenten deaktivieren
  (Banner, Kontakte, Weblinks, Newsfeeds und Umfragen)
- Funktion „System debuggen“ nicht aktivieren
- Deaktivieren von Plugins, die nicht benötigt werden (LDAP, usw.)

Php.ini-Einstellungen

Security - General

safe_mode = Off

expose_php = Off

magic_quotes_gpc = Off

allow_url_fopen = Off

allow_url_include = Off

open_basedir = /Absoluter Pfad zu Joomla!/htdocs/joomla/

Php.ini-Einstellungen

Security - Hide Errors

error_reporting = (E_ALL & ~E_NOTICE & ~E_WARNING)

display_errors = Off

Php.ini-Einstellungen

Security - Session

session.use_trans_sid = 0

session.hash_function = 1

session.save_path = /Absoluter Pfad zu Joomla!/htdocs/joomla/tmp

session.entropy_file = /dev/urandom

Php.ini-Einstellungen

Security - Upload / Memory
file_uploads = Off
upload_tmp_dir = /Absoluter Pfad zu Joomla!/htdocs/joomla/tmp
upload_max_filesize = 3M
memory_limit = 40M
post_max_size = 4M
max_execution_time = 30
max_input_time = 30

Php.ini-Einstellungen

Security - Disabled functions

disable_functions = apache_child_terminate, apache_get_modules, apache_get_version, apache_getenv, apache_note, apache_setenv, disk_free_space, diskfreespace, dl, escapeshellcmd, exec, ini_alter, ini_get_all, ini_restore, ini_set, passthru, php_uname, phpinfo, popen, proc_nice, proc_open, shell_exec, show_source, symlink, system

Monitoring

Bei Problemen benachrichtigt werden

Sind die Dienste alle online?

- Apache
- MySQL
- Inhalt der Website
- Wurde die Website gehackt
- Mailserver

.htaccess, Bash und Cron

All dieses lässt sich mit einander verbinden

- Automatisches Blockieren von IP-Adressen
- Verzeichnissrechte regelmäßig prüfen und ggf. neu setzen
- Blockieren von verschiedenen Anfragen („Requests“)
- Blockieren einiger klassischer Methoden um fremden Inhalt in die Website einzuschleusen (sog. „Exploits“)

Server

Joomla! ist nur so sicher, wie das System worauf es läuft

- SSH absichern
- Firewall aktivieren und konfigurieren
- Updates des Systems
- Zusätzliche Software wie z.B. „Fail2ban“
- Ports unter Umständen abändern

Fragen?

Viel Dank für Ihre Aufmerksamkeit