Wordpress? Aber sicher!

– Schutz gegen Angriffe und Datenverlust

Werkstattgespräch

TT-Workshop-Wochenende auf der Ebernburg am 30. Mai 2014

Schutzmöglichkeiten

- Vor der Installation
  - Sicheres Passwort für die Datenbank
  - Einträge in der Konfigurationsdatei „*config.php*“
  - Ggf. SSL-Zertifikat kaufen zur Verschlüsselung des Backend-Zugangs
- Während der Installation
  - Unterordner auf dem Server anlegen
  - Standardverzeichnis „Wordpress“ umbenennen
- Bei einem bereits installierten System
  - Sicherheits-Plugins nutzen
  - Dateirechte (Schreiben/Lesen) ändern -> FTP
  - Schutzmaßnahmen über .htaccess und functions.php
  - Datenbank bearbeiten

Vor der Installation

- **Sicheres Passwort für die Datenbank**
  - Mind. 12 Zeichen mit Zahlen und Sonderzeichen
- **Einträge in der Konfigurationsdatei wp-config.php**
  - Standard „wp_“ umbenennen z.B. in „weg951_“
  - Unbedingt die Sicherheitsschlüssel eintragen -> Zufallsgenerator unter https://api.wordpress.org/secret-key/1.1/salt/
  - Meine Empfehlung: automatisches Update abschalten (s. Anhang Codeschnipsel)
- **Verschlüsselung des Backends per SSL**
  - Login-Zugang wird per https:// aufgerufen
  - Per Browser gesendete Daten werden verschlüsselt

Willkommen

Willkommen bei der berühmten 5-Minuten-Installation von WordPress! Vielleicht möchtest du zunächst einen Blick in die liesmich-Datei (ReadMe) werfen, bevor wir fortfahren. Du kannst auch einfach unten die benötigten Informationen eingeben, um das mächtigste und flexibelste Weblog-System der Welt benutzen zu können.

Benötigte Informationen

Bitte trage die folgenden Informationen ein. Keine Sorge, du kannst all diese Einstellungen später auch wieder ändern.

Blogtitel

Textinen auf der Burg

Benutzername

Redaktion

Benutzernamen dürfen nur alphanumerische Zeichen, Leerzeichen, Unterstriche, Bindestriche, Punkte und das @-Symbol enthalten.

Passwort, doppelt

Wenn du nichts angibst, wird dir automatisch ein Passwort erstellt.

••••••••••••••

••••••••••••••

Stark

Hinweis: Dein Passwort sollte mind. 7 Zeichen lang sein. Um es sicherer zu machen, nutze die Groß- und Kleinschreibung, Ziffern und Symbole wie ! " ? $ % ^ &).

Deine E-Mail-Adresse

renate@css-manufaktur.de

Bitte die E-Mail-Adresse ganz genau überprüfen, bevor wir fortfahren.

Privatsphäre

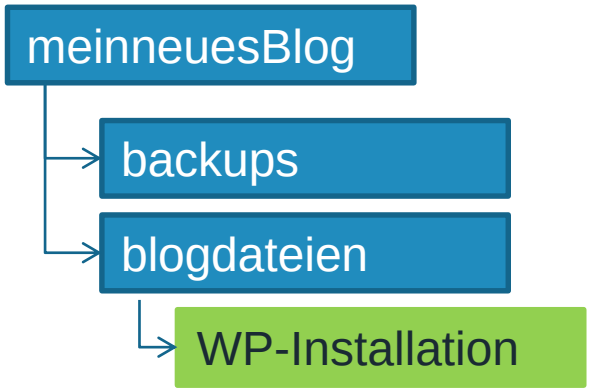
☐ Suchmaschinen dürfen diese Webseite indexieren.

WordPress installieren

Während der Installation

- Ordnerstruktur auf dem Server einrichten
  - Unterordner für Gesamtinstallation anlegen, darin einen weiteren für das „Wordpress“-Verzeichnis
  - Standardverzeichnis „wordpress“ umbenennen
  - Backup-Verzeichnis im 1. Unterordner anlegen
  - Die Domain zeigt (pointet) dann auf den 2. Unterordner

Beispiel:



Alternative

- Wenn der Server nicht zulässt, die Domain auf ein Unterverzeichnis zu pointen, dann den Eintrag in den WP-Einstellungen vornehmen:

Quelle: http://playground.ebiene.de/adminbereich-in-wordpress-schuetzen/

Im bestehenden System

- Plugins
- Weitere Einstellungen ändern
- Anpassungen in der .htaccess-Datei
- Ergänzungen in der functions.php
  (über ein Child-Theme => Master-Themes werden bei jedem Update überschrieben)

Plugins

- Login-Bereich schützen
  - http://wordpress.org/plugins/login-lockdown/ (aktueller gepflegt)
  - und http://wordpress.org/plugins/limit-login-attempts/
- Security-Suiten
  - https://wordpress.org/plugins/better-wp-security
  - https://wordpress.org/plugins/all-in-one-wp-security-and-firewall/
  - http://wordpress.org/plugins/wp-security-scan/

Einstellungen

- Dateiberechtigen per FTP reduzieren, wp-admin + wp-includes 710
- Editor abschalten -> wp-config
- wp-content verschieben/umbenennen
  Probleme bei Plugins, die auf Unterordner zugreifen müssen.
- Jedes Verzeichnis mit einer leeren index.php versehen, damit die enthaltenen Ordner und Dateien nicht einfach ausgelesen werden könnnen. In neueren WPs standardmäßig vorhanden.
- Backup-Ordner außerhalb des Root-Verzeichnisses anlegen.

.htaccess-Datei

- Mit .htaccess + .htpasswd für die wp-login.php ein zusätzliches PW erzwingen.
  => Schränkt den Komfort stark ein, da der User 2 PWs benötigt. Für Foren oder erlaubte Nutzeranmeldung ungeeignet.
- wp-config.php sichern

Alle Codeschnipsel als Textdateien im Zip-Format unter:
http://workshop.css-manufaktur.de/_Snippets.zip

.htaccess Codeschnipsel

```
// config.php per htaccess sichern
# protect wpconfig.php
<files wp-config.php>
Order deny,allow
deny from all
</files>

# protect wp-login.php
<files wp-login.php>
AuthName "Admin-Bereich"
AuthType Basic
AuthUserFile /lokaler-pfad-zu/.htpasswd
require valid-user
</files>
```

Passwort-Generator: http://www.homepage-kosten.de/htaccess/

functions.php

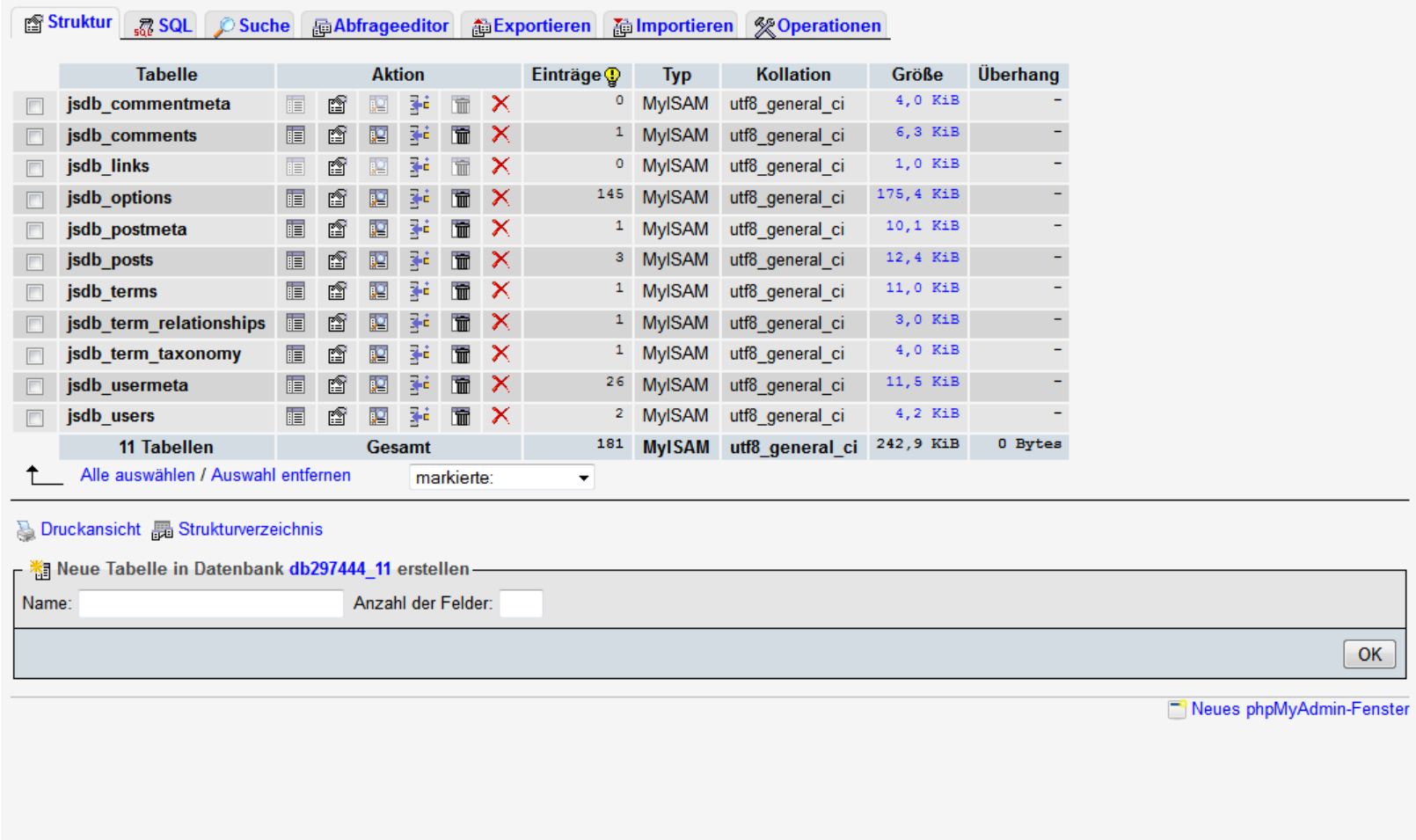
- Login-Fehlermeldungen unterdrücken
- Versionsnummern abschalten
  für Wordpress und alle Skriptdateien

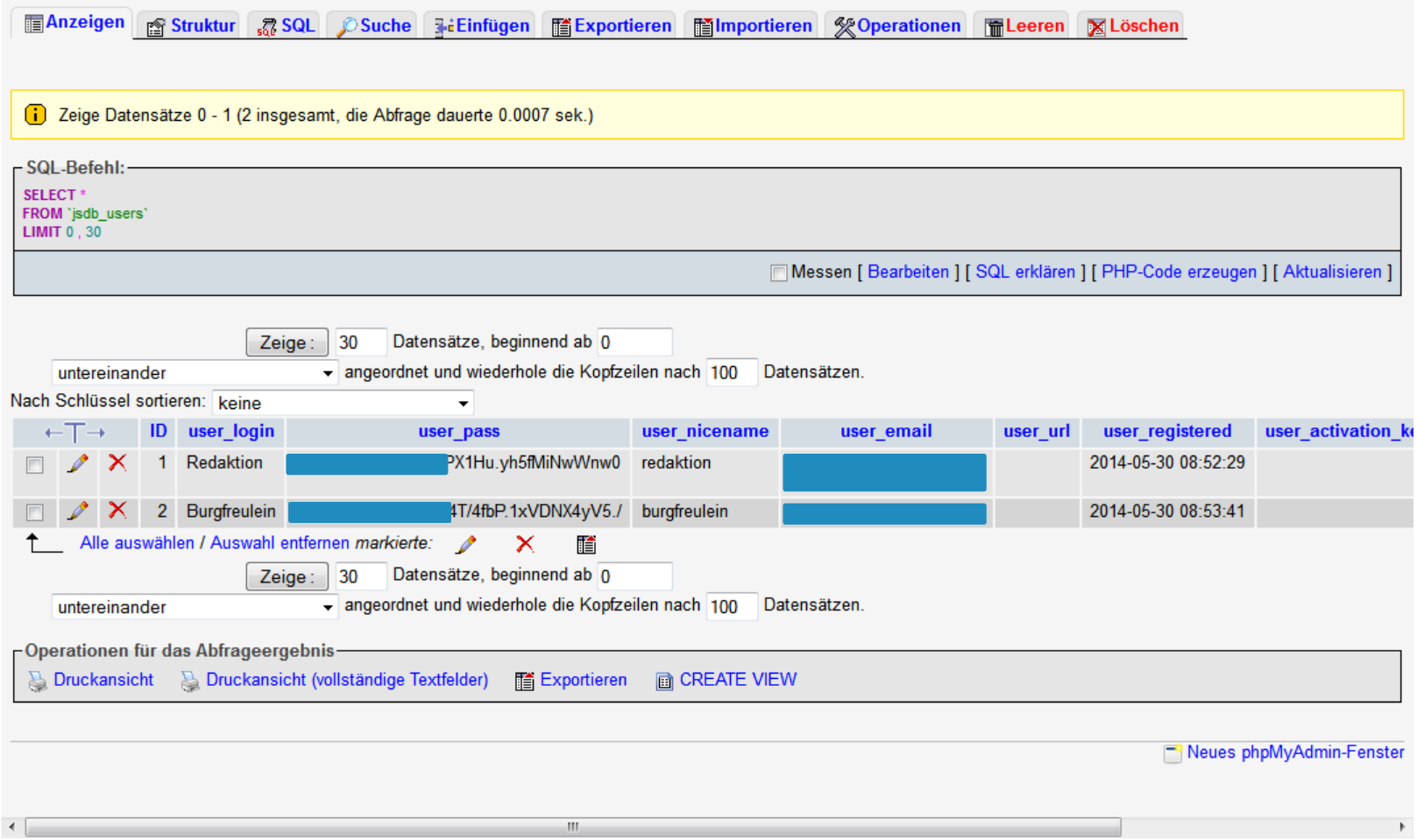
functions.php Codeschnipsel

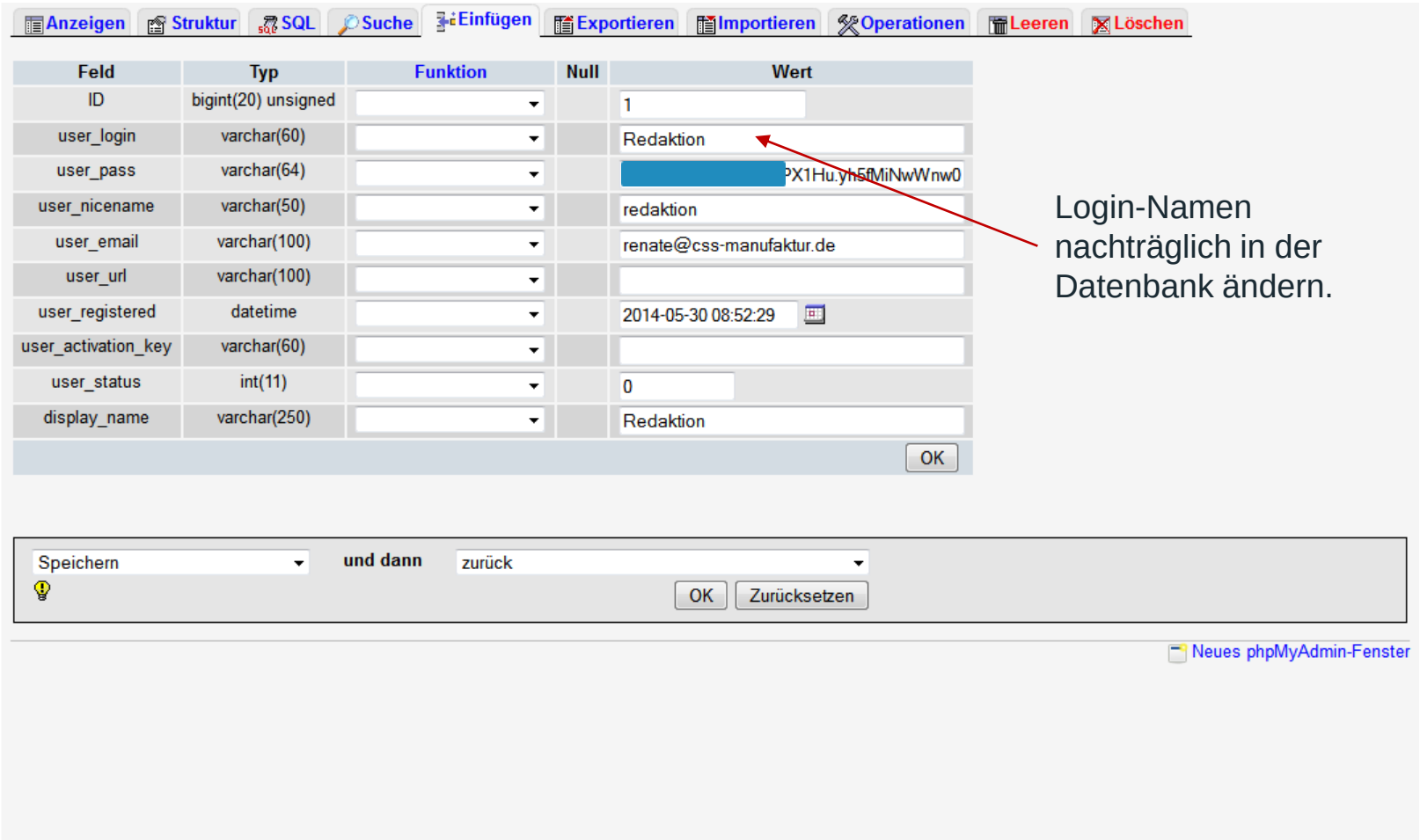
```
// Fehlermeldungen beim Login unterdruecken - functions.php
add_filter('login_errors',create_function('$a', "return null;"));


// Wordpress-Versionsnummern ausblenden - functions.php
// Remove the WordPress Generator Meta Tag
function remove_generator_filter() { return ''; }

if (function_exists('add_filter')) {
 $types = array('html', 'xhtml', 'atom', 'rss2', /*'rdf',*/ 'comment', 'export');

 foreach ($types as $type)
 add_filter('get_the_generator_'.$type, 'remove_generator_filter');
}
// remove wp version param from any enqueued scripts
function vc_remove_wp_ver_css_js( $src ) {
    if ( strpos( $src, 'ver=' . get_bloginfo( 'version' ) ) )
        $src = remove_query_arg( 'ver', $src );
    return $src;
}
add_filter( 'style_loader_src', 'vc_remove_wp_ver_css_js', 9999 );
add_filter( 'script_loader_src', 'vc_remove_wp_ver_css_js', 9999 );
```

Datenbank

- In den Nutzerkonten (Tabelle „xxx_users“) Login-Namen ändern:
  Dazu im Feld „user_login“ einen anderen Namen setzen als im im Feld „user_nicename“.
- Login-Name ist der Eintrag aus Feld „user_login“, Anzeigename im Frontend ist der Eintrag im Feld „user_nicename“.
- Alternative:
  Plugin: http://wordpress.org/plugins/user-name-security/


Struktur
SQL
Suche
Abfrageeditor
Exportieren
Importieren
Operationen
Tabelle
Aktion
Einträge
Typ
Kollation
Größe
Überhang
jsdb_commentmeta 0 MyISAM utf8_general_ci 4,0 KiB -
jsdb_comments 1 MyISAM utf8_general_ci 6,3 KiB -
jsdb_links 0 MyISAM utf8_general_ci 1,0 KiB -
jsdb_options 145 MyISAM utf8_general_ci 175,4 KiB -
jsdb_postmeta 1 MyISAM utf8_general_ci 10,1 KiB -
jsdb_posts 3 MyISAM utf8_general_ci 12,4 KiB -
jsdb_terms 1 MyISAM utf8_general_ci 11,0 KiB -
jsdb_term_relationships 1 MyISAM utf8_general_ci 3,0 KiB -
jsdb_term_taxonomy 1 MyISAM utf8_general_ci 4,0 KiB -
jsdb_usermeta 26 MyISAM utf8_general_ci 11,5 KiB -
jsdb_users 2 MyISAM utf8_general_ci 4,2 KiB -
11 Tabellen Gesamt 181 MyISAM utf8_general_ci 242,9 KiB 0 Bytes
Alle auswählen / Auswahl entfernen
markierte:
Druckansicht
Strukturverzeichnis
Neue Tabelle in Datenbank db297444_11 erstellen
Name:
Anzahl der Felder:
OK
Neues phpMyAdmin-Fenster


Anzeigen
Struktur
SQL
Suche
Einfügen
Exportieren
Importieren
Operationen
Leeren
Löschen
Zeige Datensätze 0 - 1 (2 insgesamt, die Abfrage dauerte 0.0007 sek.)
SQL-Befehl:
SELECT *
FROM `jsdb_users`
LIMIT 0 , 30
Messen [Bearbeiten] [SQL erklären] [PHP-Code erzeugen] [Aktualisieren]
Zeige : 30 Datensätze, beginnend ab 0
untereinander angeordnet und wiederhole die Kopfzeilen nach 100 Datensätzen.
Nach Schlüssel sortieren: keine
ID user_login user_pass user_nicename user_email user_url user_registered user_activation_k
1 Redaktion PX1Hu.yh5fMiNwWnw0 redaktion 2014-05-30 08:52:29
2 Burgfreulein 4T/4fbP.1xVDNX4yV5./ burgfreulein 2014-05-30 08:53:41
Alle auswählen / Auswahl entfernen markierte:
Zeige : 30 Datensätze, beginnend ab 0
untereinander angeordnet und wiederhole die Kopfzeilen nach 100 Datensätzen.
Operationen für das Abfrageergebnis
Druckansicht
Druckansicht (vollständige Textfelder)
Exportieren
CREATE VIEW
Neues phpMyAdmin-Fenster



Login-Namen nachträglich in der Datenbank ändern.

Backups und Updates

- Plugins, z.B. BackWPup
  - Datenplanung für manuelle und zeitgesteuerte Backups
  - Tutorial: http://michaelsonntag.net/wordpressblog-komplett-mit-datenbank-und-dateien-sichern/
- Updates von Wordpress, Themes und Plugins
  - Regelmäßig Updates prüfen
  - Kleiner Helfer => Plugin für Benachrichtung: http://wordpress.org/plugins/wp-updates-notifier/

SuperGau -> Erste-Hilfe

- Blankostartseite und kein Backend mehr erreichbar
- Zugriff über FTP -> wie geht das?
- Blick in die Datenbank für alle, die sich trauen ;-)

Plugins

- Backup
  - https://wordpress.org/plugins/backwpup/
- Diverse
  - http://wordpress.org/plugins/user-name-security/

Weiterführende Links

- Wordpress absichern
  - http://playground.ebiene.de/adminbereich-in-wordpress-schuetzen/
  - http://www.wpbuch.de/2010/01/wordpress-installieren-und-sicherer-machen/
  - http://t3n.de/news/wordpress-anfaengerfehler-514335/
  - http://ralph-segert.de/zur-sicherheit-leitfaden-fuer-wordpress-kunden/
  - http://wp.smashingmagazine.com/2010/07/01/10-useful-wordpress-security-tweaks/
  - http://codex.wordpress.org/Hardening_WordPress