

Inhaltsverzeichnis

Inhaltsverzeichnis.....	1
Einleitung.....	2
WordPress installieren.....	2
<i>Zugriff auf die WordPress Tabellen.....</i>	<i>2</i>
Ändern des WordPress Tabellen Präfix.....	3
<i>Vor der Installation.....</i>	<i>3</i>
<i>Manuelle Änderung.....</i>	<i>3</i>
<i>Verwendung des WP Prefix Table Changer.....</i>	<i>4</i>
Vorbereitung des Blog.....	5
<i>Ändern des Admin Benutzernamens.....</i>	<i>5</i>
<i>Erstellen eines neuen Benutzer mit limitierten Rechten.....</i>	<i>6</i>
<i>Absicherung der WP Installation⁵.....</i>	<i>7</i>
<i>Begrenzter Zugriff auf wp-content & wp-includes.....</i>	<i>7</i>
<i>Begrenzter Zugriff auf wp-admin.....</i>	<i>7</i>
<i>Blockieren alle von IP Adressen außer der eigenen.....</i>	<i>7</i>
<i>Passwort Schutz mit .htpasswd.....</i>	<i>7</i>
<i>Die .htaccess Datei.....</i>	<i>8</i>
<i>Die .htpasswd Datei.....</i>	<i>8</i>
MUSTHAVE Plugins.....	8
<i>WPIDS - Angriffe erkennen.....</i>	<i>8</i>
<i>WordPress Plugin Tracker – Bist Du auf dem neusten Stand?.....</i>	<i>9</i>
<i>WordPress Online Security Scanner.....</i>	<i>10</i>
Ende.....	10

Einleitung

Dieses Dokument soll Informationen bereit stellen, um die Sicherheit Deines Blogs zu erhöhen. Wir haben versucht die Schritte in einer verständlichen Sprache zu verfassen, so dass diese einfach nachvollziehbar sind und bei der Durchführung der Änderungen an Deinem Blog keine Probleme auftreten. Alle Informationen aus diesem Dokument findet Du auch auf BlogSecurity.net. Dieses Dokument soll eine Art Kurzreferenz darstellen, um Dein Blog sicher zu halten. Wir werden b deshalb versuchen dieses Dokument regelmäßig zu aktualisieren.

Wenn Du Fragen, Problem oder Verbesserungsvorschläge zu diesem Dokument hast, stehen wir Dir gerne [per E-Mail](#) zu Verfügung.

Wichtig: Bevor irgendwelche Änderungen, die in diesem Dokument beschrieben sind durchgeführt werden, solltest Du zunächst ein vollständiges Backup Deiner WP Dateien durchführen. Näheres dazu findest du unter "[5 failsafe steps to upgrade WordPress](#)"

WordPress installieren

Zugriff auf die WordPress Tabellen

Bevor du mit der Installation deines Blogs beginnst, ist es wichtig, dem Benutzer, der auf die Datenbank zugreift, die richtigen Rechte zu geben. Die Idee hinter diesem Schritt ist, dem Benutzer der auf die Datenbank zugreift, so wenig Rechte wie möglich zu geben. Den für den Fall, dass Dein Blog übernommen wird, wird der Angreifer versuchen seine Rechte auch außerhalb (z.B. auf dem Rest des Webservers oder Webspace) zu benutzen.

Anmerkung: Dies gilt auch für andere Anwendungen. Niemals sollte eine Web-Anwendung mit **root Rechten** auf die Datenbank zugreifen können (es sei den dies ist nötig).

Dein Datenbankbenutzer sollte keine globalen SQL Rechte haben und nur limitierten Zugriff auf die Datenbank haben auf der Deine WordPress Installation liegt. Für WordPress reicht es völlig aus, wenn die folgenden Rechte vergeben sind:

Für Daten-Manipulation: SELECT, INSERT, UPDATE, DELETE

Für Struktur-Manipulation: CREATE, ALTER, DROP

Wenn Du nur eine Datenbank bei Deinem Webhoster zur Verfügung hat, aber mehrere Benutzer anlagen kannst, erstelle einen Benutzer der mit folgenden Rechten auf die WordPress Tabellen zugreifen kann:

Für Daten-Manipulation: SELECT, INSERT, UPDATE, DELETE

Für Struktur-Manipulation: ALTER

Wieso machen wir das? Wenn ein Angreifer Zugriff auf dein Blog erlangt, und Datenbankabfragen durchführen kann, ist er limitiert auf die Berechtigungen, die für den Datenbankbenutzer Deiner WordPress Installation zur Verfügung stehen.

Ändern des WordPress Tabellen Präfix

Um SQL-Injections zu vermeiden solltest Du den Standard WordPress Präfix der Datenbank von `wp_` in einen **zufälligen Wert**, wie z.B. `4i32a_`, ändern. Oft benutzten Angreifer öffentlich gemachte Exploits aus dem Internet. Diese Exploits basieren i.d.R. darauf, dass der Standard Präfix von WordPress „wp_“ benutzt wird. Ist dieser geändert, ist es für einen Angreifer schwieriger diesen Exploit auszunutzen.

Um nachträglich heraus zu finden welcher Präfix für welche Web-Anwendung steht, kann ein Teil des Namens (also z.B. das „wp“) weiterbenutzt werden. Es ist nur wichtig, dass der Präfix durch etwas Zufälliges erweitert wird, so dass ein Angreifer den neuen Präfix nicht einfach erraten kann.

Vor der Installation

Wenn Du WordPress noch nicht installiert hast, ist dieser Schritt sehr einfach durchzuführen. Alles was Du dafür tun musst, ist die folgende Zeile in der Datei **WP-CONFIG.PHP** zu ändern:

```
$table_prefix = 'wp_';
```

Der neue Präfix könnte z.B. so aussehen:

```
$table_prefix = '4i32a_';
```

Nach der Änderung kannst Du Deine WordPress Installation starten und alle Tabellen werden mit dem von Dir **geänderten** Präfix angelegt.

Manuelle Änderung

Wenn der Präfix bei einer bereits bestehenden Installation geändert werden soll, sind einige Schritte mehr nötig. Dies ist ein eher aufwendiger Prozess, wenn Du einen einfachen Weg bevorzugst, empfehlen wir die den nächsten Abschnitt. Für die manuelle Änderung gehe wie folgt vor.

Öffne die Datei **WP-CONFIG.PHP** und suche die folgende Zeile:

```
$table_prefix = 'wp_';
```

Wir benutzen das Beispiel von gerade `4i32a_` und ändern die Zeile wie folgt:

```
$table_prefix = '4i32a_';
```

Nun weiß zwar die WordPress Installation mit welchem Präfix sie von nun an arbeiten soll, aber wir müssen noch die Tabellen der Datenbank entsprechend anpassen. Hierfür müssen wir einige SQL Kommandos¹ z.B. mit PhpMyAdmin, oder einem ähnlichen Programm, ausführen. Mit Wordpress steht kein Zugriff direkter Zugriff auf den Präfix der Tabellen zur Verfügung.

¹ Beispiel: `RENAME TABLE wp_categories TO 4i32a_categories`

Folgende Tabellen müssen geändert werden:

wp_categories, wp_comments, wp_link2cat, wp_links, wp_options, wp_post2cat, wp_postmeta, wp_posts, wp_usermeta, wp_users

So sollen sie nach der Änderung aussehen:

4i32a_categories, 4i32a_comments, 4i32a_link2cat, 4i32a_links, 4i32a_options, 4i32a_post2cat, 4i32a_postmeta, 4i32a_posts, 4i32a_usermeta, 4i32a_users

Leider sind damit noch nicht mit alle Änderung abgeschlossen. WordPress beinhaltet auch innerhalb der Tabellen einige Informationen, die das Präfix verwenden. Damit Dein Blog einwandfrei funktioniert, müssen wir auch diese anpassen.

Innerhalb der Tabelle `wp_options`² müssen wir den Eintrag unter `option_name` mit dem Feld `wp_user_roles` zu `4i32a_user_roles`³ ändern.

Nun müssen noch zwei weitere Werte⁴ in der Tabelle `wp_usermeta` geändert werden.

Die Werte `wp_autosave_draft_ids` und `wp_user_level` für das Feld Meta-Key müssen mit dem neuen Präfix ausgestattet werden: `4i32a_autosave_draft_ids` und `4i32a_user_level`.

Das ist alles! **Aber BlogSecurity macht es Dir mit dem [WP Prefix Table Changer](#) noch einfacher!**

Verwendung des WP Prefix Table Changer

Wir haben das Plugin [WP Prefix Table Changer](#) erstellt, mit dem Du automatisch den Präfix Deiner WordPress Tabellen ändern kannst.

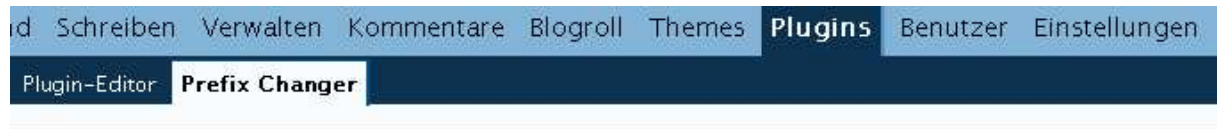
Nachdem Du das Plugin von BlogSecurity.net heruntergeladen hast, musst Du die extrahierten Dateien in Deinen Plugin-Ordner kopieren, der unter **WORDPRESS/WP-CONTENT/PLUGINS** zu finden sein sollte. Anschließend musst Du in Deinem WP-Admin Bereich das WP Prefix Table Changer Plugin aktivieren. Nach der Aktivierung ist ein neues Untermenü namens Prefix Changer innerhalb der Plugin Seite verfügbar.

² Hier wird der Standard Präfix verwendet, um Verwechslungen mit dem neuen Präfix zu vermeiden

³ `UPDATE 4i32a_options SET option_name='4i32a_user_roles' WHERE option_name='wp_user_roles' LIMIT 1`

⁴ **Anmerkung:** es kann vorkommen, dass diese Werte noch nicht existieren, da sie erst erstellt werden wenn sie benötigt werden

Auf dieser Seite sollte folgendes erscheinen:



WP Prefix Changer

This plugin will change your database table prefix to mitigate zero-day SQL Injection attacks.

Please Change the current: prefix to something different (i.e. 619fa1).

Wie man sehen kann, benutzt dieses Blog den WordPress Standard Präfix. Dieser soll nun in einen **zufälligen Wert**, ohne weitere Bedeutung, wie z.B. *4i32a_* geändert werden. Nachdem Du die Änderungen vorgenommen hast klicke auf 'Start Renaming' und das Plugin wird alle entsprechenden Einträge in den neuen Präfix umbenennen. Dabei werden auch Tabellen von anderen Plugins, welche eine Tabelle benötigen, entsprechend umbenannt.

Der letzte Schritt ist die Änderung der **WP-CONFIG.PHP** Datei.

Du erhältst eine Meldung ob der Prozess erfolgreich war oder fehlgeschlagen ist. Wenn der Prozess erfolgreich war, wird die Datei **WP-CONFIG.PHP** aus Sicherheitsgründen auf Nur-Lesen (**644**) gesetzt. Wenn der Prozess fehlschlägt, liegt dies i.d.R. daran, dass die Datei nicht beschreibbar war. Sollte dies der Fall sein, must Du den Eintrag für den Präfix in der Datei **WP-CONFIG.PHP** von Hand in den neuen Wert ändern.

Vorbereitung des Blog

Das betriebsbereite Blog hat nun einige gute Grundsicherheit! Im nächsten Schritt werden wir einige Änderungen an den WP-Benutzern vornehmen, um die Sicherheit weiter zu erhöhen.

Ändern des Admin Benutzernamens

Da alle derzeit verfügbaren WordPress Versionen anfällig gegen [User Enumeration](#) sind, solltest Du das Standard Administrator Konto von **admin** in einen Wert ändern, der schwieriger zu erraten ist. Durch die Änderung machen wir es einem Angreifer schwieriger mit einer Brute-Force-Attacke das Passwort zu erraten.

Anmerkung: Du must davon ausgehen, dass ein Angreifer deinen Benutzernamen kennt. Stelle also sicher, dass Du ein starkes Passwort benutzt.

Melde Dich mit Deinen Administrator Konto an und erstelle einen neuen Administrator Benutzer. Wähle dabei einen Benutzername der sehr schwierig zu erraten ist. Gib ihm ein starkes Passwort. Du kannst ihm die E-Mail Adresse von deinem jetzigen Konto geben, da wir dieses gleich löschen werden.

Nachdem das Konto erstellt wurde, müssen wir nun in dieses wechseln. Melde Dich wieder ab und anschließend mit dem Benutzer Deines neu erstellten Kontos an. Nun können wir Dein altes Administrator Konto löschen.

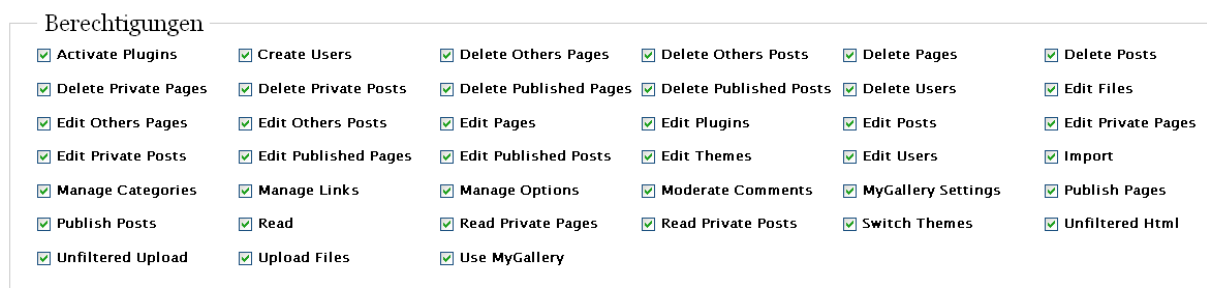
Erstellen eines neuen Benutzer mit limitierten Rechten

Bevor wir fortfahren, solltest Du die das [Role Manager](#) Plugin von [Thomas Schneider \(im-web-gefunden.de\)](#) installieren. Mit diesem Plugin kannst du die Rechte eines jeden Benutzer sehr fein einstellen. Nachdem Du das Plugin aktiviert hast, erstelle einen Benutzer mit den von Dir gewünschten Benutzerrechten.

Desto weniger Rechte dein Benutzerkonto hat, desto besser wird die Sicherheit; dein neuer Benutzer sollte nicht mehr Rechte haben als ein Contributor.

Die Rolle eines Contributors hat allerdings in der Standard Einstellung nicht genügend Rechte. Genau für diesen Fall haben wir das Role Manager Plugin installiert. Das Plugin erlaubt Dir zusätzliche Rechte für jeden Benutzer individuell zu vergeben. Du kannst die bestehenden Rechte ändern oder auch neue Rollen mit entsprechenden Rechten anlegen.

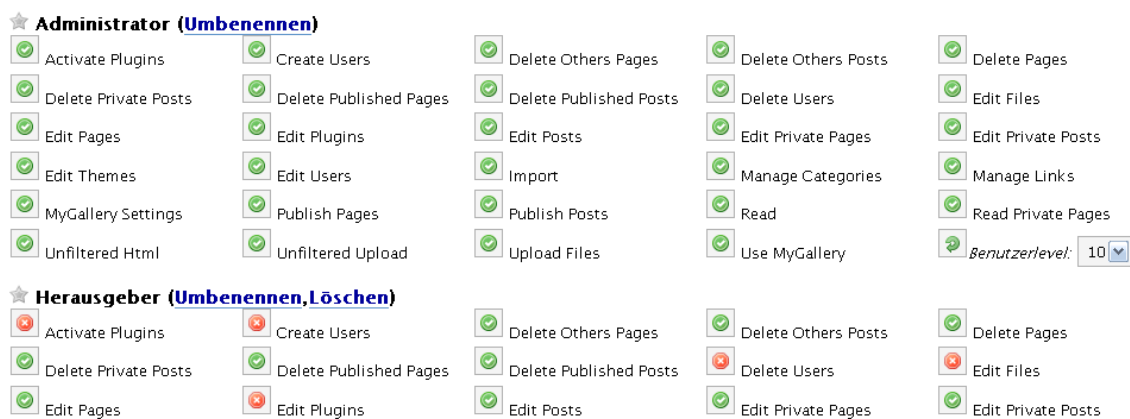
Wie bereits erwähnt sollte der neue Benutzer nicht mehr Rechte als ein Contributor haben. Mit dem Role Manager Plugin bekommen wir aber zusätzliche Flexibilität in die Rechte Manipulation, wie das folgende Bild zeigt.



Siehe: [Role Manager](#) für weitere Information.

Wenn Du mehrere Benutzer in Deinem Blog verwaltest, ist es das Beste die Rechte einer bereits bestehenden Rolle zu ändern. Du kannst natürlich auch eine neue Rolle mit den gewünschten Rechten anlegen.

Wenn Du einen neuen Benutzer anlegst, solltest du mit den Rechten "upload files", "general plugin access", "edit files/pages/posts", "import" und "unfiltered html", sehr behutsam umgehen, da sie dem Benutzer sehr viele Möglichkeiten geben.



Ändern der Rechte mit dem [Role Manager](#)

Absicherung der WP Installation⁵

Dieser Abschnitt erklärt, wie man den Administrationsbereich vor unberechtigtem Zugriff schützen kann. Dieser Schritt ist einfacher wenn man ein Blog lediglich mit einem Benutzer betreibt. Bei einem Blog mit mehreren Benutzern ist der Aufwand recht hoch, so dass man hier eine Abwägung zwischen Aufwand und Sicherheit treffen muss.

Begrenzter Zugriff auf wp-content & wp-includes

In diesem Schritt schränken wir den Zugriff für bestimmte Verzeichnisse ein. Im Prinzip verweigern wir den kompletten Zugriff, bis auf Bilder, CSS und einige JavaScript Dateien.

Der folgende Code muss in einer **.HTACCESS** Datei in den Verzeichnissen **WP-CONTENT** & **WP-INCLUDES** abgelegt werden:

```
Order Allow,Deny
Deny from all
<Files ~ ".(css|jpe?g|png|gif|js)$">
Allow from all
</Files>
```

Anmerkung: In manchem Fälle kann es nötig sein" bestimmten" PHP Datei (en) Zugriff für Templates oder Plugins zu geben.

Begrenzter Zugriff auf wp-admin

Blockieren alle von IP Adressen außer der eigenen

Wenn Du Dein Blog nur mit einem Benutzer betreibst, kannst Du den Zugriff auf den **WP-ADMIN** Ordner auf eine IP Adresse beschränken. Dies setzt voraus, dass Du mit einer statischen (sich nicht wechselnden) IP-Adresse ins Internet gehst. Die **.HTACCESS** Datei innerhalb des **WP-ADMIN** Ordners sollte so aussehen:

```
Order deny,allow
Allow from a.b.c.d #Hier steht deine Statische IP
Deny from all
```

Speicher die Datei im wp-admin Ordner ab und versuche mit einer anderen IP Adresse (z.B. über einen Proxy) auf den wp-admin Ordner zuzugreifen. Wenn alles einwandfrei funktioniert, sollte der Zugriff geblockt werden. Versuche anschließend mit Deiner statischen IP Adresse zuzugreifen, um zu testen, ob jetzt der Zugriff funktioniert.

Wenn alles einwandfrei funktioniert ist der Zugriff auf den **WP-ADMIN** Ordner nur auf die IP Adresse Deiner Wahl beschränkt.

Passwort Schutz mit .htpasswd

Die einfacherer Variante ist die Verwendung eines Passwortschutzes. Damit kann man zwar von jeder IP Adresse zugreifen, aber es wird eine zusätzliche Sicherheitsbarriere eingebaut.

Die .htaccess Datei

Die **.HTACCESS** Datei im **WP-ADMIN** Ordner sollte so aussehen:

```
AuthUserFile /srv/www/user1/.htpasswd #Diese Datei sollte ausserhalb vom webroot liegen
AuthType Basic
AuthName "Blog"
require user youruser #Der Benutzername sollte nicht leicht zu erraten sein.
```

Die .htpasswd Datei

Wie bereits erwähnt, sollte die Datei⁵ außerhalb Deines Web-Verzeichnisses liegen. Im Idealfall genau einen Ordner darüber. Um ein verschlüsseltes Passwort zu erstellen kannst du die folgende Seite benutzen: <http://www.euronet.nl/~arnow/htpasswd/>. Hierfür gibt es natürlich auch andere Seiten. Gib Deinen gewünschten Benutzername und Dein gewünschtes Passwort im Klartext in das Formular ein und es wird automatisch der Code für Deine **.HTPASSWORD** Datei erstellt. Diese könnte z.B. so aussehen:

```
Yourusr:§a983seJ/a25.Aa
```

Sollte nicht alles einwandfrei funktionieren, generiere dir einen neuen Code und überschreibe die Datei.

MUSTHAVE Plugins

Nicht jedes Plugin ist ein potentielles Sicherheitsrisiko. Die folgende Liste von Plugins erhöht die Sicherheit Deines Blogs.

WPIDS - Angriffe erkennen

BlogSecurity hat PHPIDS (Intrusion Detection System) in WordPress portiert. Mit PHPIDS ist es möglich, eine Vielzahl von Einbruchversuchen zu identifizieren. Wir benutzen diese Möglichkeit um gefährliche Angriffe zu blockieren. Jeder Angriffsversuch wird in der Datenbank gespeichert, so dass man anschließend mit passenden Mitteln darauf reagieren kann. Es besteht die Möglichkeit, dass System so zu konfigurieren, dass, wenn die Angriffe eine gewissen Anzahl erreichen, automatisch eine E-Mail generiert wird. Des Weiteren, kann die IP Adresse eines Angreifers für einen bestimmten Zeitraum blockiert werden. In jeden Fall wird WPIDS aber schlechten Input bereinigen. PHPIDS kannst Du Dir auf der offizielle [Webseite](#) herunterladen. Anmerkung: Für die einwandfreie funktionsweise dieses Plugins benötigst Du mind. PHP 5.1.6 oder höher. In Kürze wird eine neue Version von WPIDS mit der BlogSec's Erweiterung, WP-Lockdown, erscheinen.

⁵ Mehr Informationen über den Aufbau gibt es hier: http://httpd.apache.org/docs/1.3/mod/mod_auth.html

WordPress Plugin Tracker – Bist Du auf dem neusten Stand?

Wenn Du Dein Blog gerade inkl. der aktuellen Version der Plugins installiert hast, solltest Du auf dem neuste Stand sein. Du solltest dennoch das [WordPress Plugin Tracker](#) Plugin installieren um regelmäßig zu prüfen, ob Du die neusten Plugin Versionen benutzt. Nach der Installation und Aktivierung solltest Du folgende Übersicht sehen:

Plugin Release Tracker

Track the releases of the plugins you have installed in your website

Move WP Plugins Tracker to Plugins SubMenu

Plugin	Your Version	WPPDB Version	Status
Another Wordpress Meta Plugin	2.0.3	2.0.3	Versions are matching, You have latest v
Akismet	2.0.2	2.0.2	Versions are matching, You have latest v
Bad Behavior	2.0.10	2.0.10	Versions are matching, You have latest v
http:BL WordPress Plugin	1.4	1.4	Versions are matching, You have latest v

So sieht die Beispielseite des Plugin Release Tracker aus

Wenn ein Plugin nicht mehr auf dem neusten Stand sein sollte, erscheint eine entsprechende Meldung. Mit einem Klick auf das Plugin gelangst Du direkt auf die Seite des Entwicklers um Dir das neuste Update herunterzuladen. So kannst Du die Plugins in deinem Blog immer auf dem neusten Stand halten.

WordPress Online Security Scanner

BlogSecurity kann Dir dabei helfen, Schwachstellen in Deinem Blog zu identifizieren. Hierfür haben wir den WordPress Online Security Scanner entwickelt. Er prüft Dein Blog auf fehlerhafte Plugins, Cross-Site Scripting und andere Schwachstellen.

WordPress Version Leak

Test	Result
wp-links-opml.php	Version Leak: WordPress 2.2.1
wp-rss.php	Version Leak: WordPress 2.2.1
wp-commentsrss2.php	Version Leak: WordPress 2.2.1
wp-rdf.php	Version Leak: WordPress 2.2.1
wp-rss2.php	Version Leak: WordPress 2.2.1

According to wp-scanner this blog is running the latest version of WordPress.

WordPress Template XSS Checks

Test	Result
wp-xss-3	WordPress Template Vulnerable to XSS: /?

This blog uses a template that is vulnerable to Cross-Site Scripting Attacks. See [Vulnerable WP Themes](#) for more information.

WordPress Plugins Found

Test	Result
wp-plugins[1]	wp-backup
wp-plugins[2]	subscribe-to-comments.php
wp-plugins[4]	wp-contact-form
wp-plugins[0]	wp-cache2
wp-plugins[5]	sitemap
wp-plugins[3]	Akismet

Please check out [WordPress BlogWatch](#) for the latest vulnerabilities in WordPress plugins. More work will be done in this area for future releases.

EXCEPT WHERE OTHERWISE NOTED, CONTENT AND TOOLS ON THIS SITE ARE LICENSED UNDER THE ATTRIBUTION-NONCOMMERCIAL-NO DERIVS LICENSE

Der WP-Scanner ist ein kostenloser online Service, der bereits mehr als 5000 Blogs geprüft hat. Mehr Informationen findest Du [hier](#).

Ende

Wir haben das Ende unseres Dokumentes erreicht. Wir hoffen, dass es Dir gefallen hat und das Du bei der Implementierung unserer Vorschläge erfolgreich warst. Wir würden uns sehr über Feedback und Erfahrungsberichte freuen.