

WORDPRESS SICHERHEITSBEREICHE

Funktionssicherheit

Datensicherheit

Rechtssicherheit

Zugriffssicherheit

Funktionssicherheit

- Ziel: Stabile Funktion der gesamten Website
- Maßnahmen:
 - WP Updates organisieren
 - Plugins immer updaten
 - Themes immer aktuell halten
 - Großvolumige Medien (Videos) extern hosten (Vimeo, Youtube)
 - Deaktivierte Plugins löschen

Datensicherheit

- Regelmäßiges Backup mit Updraft Plus
- Regelmäßiges Backup mit Duplicator
- Serverbackup mit Provider vereinbaren
- Upload-Ordner lokal oder auf Cloud speichern
- Datenbank mit Hilfe von ‚phpmyadmin‘ sichern (exportieren)

Rechtssicherheit

- Impressum mit Hilfe von e-Recht24.de generieren
- Datenschutzerklärung mit Hilfe von e-recht24.de generieren
- Plugin ‚Germanized‘ installieren und aktivieren
- Bei Shop-Betrieb (Woocommerce): Plugin German Market erwägen

German Market

Rechtssicher mit deiner E-Commerce Suite.

Mache deinen WooCommerce-Shop fit für den deutschsprachigen Markt und die gesamte EU. Inklusive rechtlich relevanter Inhalte, integrierter Rechnungserstellung, Anbindung an deine Buchhaltung und deine Warenwirtschaft, Bearbeitung von Stornos und vielem mehr. Verkaufe so einfach wie nie - mit German Market.

Ab 85,00 €

beinhaltet MwSt.

[JETZT KAUFEN!](#)[ALLE FUNKTIONEN](#)

Voraussetzungen: PHP 7.4+, PHP-Bibliothek cURL, WooCommerce 6.4+,

WordPress 5.8+



German Market

? Hilfe

Hackangriffe abwehren

(Zugriffssicherheit)

- Grundsätzlich: 100% Sicherheit ist praktisch nicht erreichbar. Dieser Extremwert würde die Funktion der wordpress-Website praktisch beenden. Auch die permanente, persönliche Überprüfung der Hackersicherheit würde den Betrieb der Webseite aus der praktischen Realität entfernen oder unwirtschaftlich machen. Ziel muss sein, dass sich ein Angriff auf die Website für den Angreifer nicht lohnt.

„Hintertüren“ verhindern

CANTON BECKER

Website Design ▾ Music ▾ Projects Contact

How to search for ‘backdoors’ in a hacked WordPress site

AUG 25, 2009 | ET CETERA

If your WordPress site has been hacked, then you've probably already been advised to:

1. Backup your WordPress database and **wp-content** directory
2. Reinstall WordPress from scratch (the latest version, of course)
3. Restore your database and **wp-content** directory

Next, you need to make sure there are no ‘backdoors’ installed in your wp-content directory. Here are a couple of tips. They all require that you have shell (SSH) access to your server, and at least a little familiarity with the command line.

If a backdoor has been installed on your site, it is almost certainly located in your wp-content directory. The reasoning behind this is that once you discover that your site has been hacked, you will most likely wipe out every single file on your server except for your wp-content directory, where your uploads, plugins, and themes are installed.

Begin your investigation by logging into your website via SSH and changing to your wp-content directory:

```
cd ~/public_html/wp-content
```

Here's what to do next:

1. SEARCH WP-CONTENT FOR EVERY INSTANCE OF AN ‘EVAL’ COMMAND

```
grep -R eval * | more
```

A number of plugins have legitimate uses of the **eval** command but if you see anything like this (especially at the very top of a .php file) OR if you see an eval anywhere in your uploads or themes directories, then you should be suspicious. And if the contents of the **eval** command are hidden inside of a **base64_decode** and/or **gzinflate** command like you see in the example below, then you're definitely looking at a backdoor.



MORE WORK

The Illustrated Gallery

North Shore Learning Clinic

Stillness Speaks

The Asia Foundation’s 2016 Redesign

Christ in the Desert Monastery

GCI General Contractors: Portfolio site with full-screen slideshows

Jim Rabby Gallery: Elegant & easy-to-edit artist website

Website redesign for Upaya Zen Center, Santa Fe NM

WORK PORTFOLIO >

ET CETERA

Russian Warship, Go F*** Yourself Fundraiser

Should I Copyright My Work?

Rare Audio Recording of Salvador Dali Talking About Logarithmic Patterns

Economist Frederick Hayek Anticipates Bitcoin in 1984

Facebook Live Techno DJ Set (COVID-19)

Wurde meine Seite gehackt?

<https://sitecheck.sucuri.net/>

The screenshot shows the Sucuri SiteCheck interface for the website vhs-kurs-wp.beeverso.eu. The main summary card indicates a **Site Issue** (500 Internal Server Error) and that the **Site is not Blacklisted** (9 Blacklists checked). A yellow button for **Request Review** is visible. Below this, detailed server information is provided: **Redirects to:** <https://vhs-kurs-wp.beeverso.eu/>; **IP address:** 85.13.145.247; **Hosting:** All-Inkl.com/Neue Medien Münich; **Running on:** Apache. A security risk bar at the bottom is labeled from **Minimal** to **Critical**, with the current level being **Low Security Risk**. A yellow box highlights a **Site Issue Detected** at <http://vhs-kurs-wp.beeverso.eu/404testpage4525d2fdc>, with a note that it's [Unable to scan the page. 500 Internal Server Error](#). A message at the bottom states: "Our automated scan found an issue on some pages of your website. If you believe your website has been hacked, [sign up](#) for a complete scan and guaranteed malware removal." At the bottom, two sections are shown: **Website Malware & Security** (No malware detected by scan (Low Risk), No injected spam detected (Low Risk)) and **Website Blacklist Status** (Domain clean by Google Safe Browsing, Domain clean by McAfee).

Brute-Force Login-Versuche

- Erlauben Sie dem Angreifer nicht mehr als 3 Versuche, Ihr Passwort zu knacken.
- Voraussetzung: Ihr Passwort lautet nicht 123456 o.ä.
- Plugin ‚Limit login attempts‘

WPS hide Login

WPS Hide Login

Wenn du Hilfe benötigst, sieh im [Supportforum](#) nach. Dieses Plugin wurde dir freundlicherweise von [WPServeur](#) zur Verfügung gestellt (Auf WordPress spezialisiertes Hosting)
Entdecke auch unsere anderen Plugins: das Plugin [WPS Bidouille](#), das Plugin [WPS Cleaner](#) und [WPS Limit Login](#)

Anmelde-URL

/

Schütze deine Website, indem du die Login-URL änderst und verhindere den Zugriff auf die wp-login.php-Seite und das wp-admin-Verzeichnis für nicht angemeldete Personen.

Umleitungs-URL

/

Weiterleitungs-URL, wenn jemand nicht angemeldet ist und versucht, auf die wp-login.php-Seite oder das wp-admin-Verzeichnis zuzugreifen.

Änderungen speichern

Two Factor Authorization

- Mit dem Plugin 'Two Factor' (Beispiel)
- Hier sollte man daran denken, eine Authorization APP für den QR-Code auf dem Handy zu installieren

WP-Config-Daten verbergen

- WP-Config enthält zum Beispiel das Datenbank-Login
- Man kann den Code durch ein include-Statement verbergen:
- `<?php include('/home/yourname/wp-config.php');`

Alles in Wordfence:

- Installation des Plugins 'wordfence'

The screenshot shows the Wordfence Firewall dashboard for the website vhs9.bee35.de. The left sidebar includes links for Dashboard, Beiträge, Medien, Seiten, Kommentare, Astra, Design, Plugins (with 3 notifications), Benutzer, Werkzeuge, Einstellungen, WP Mail SMTP, Wordfence (selected), and Dashboard. The main content area is titled 'Firewall' and displays the following information:

- Learning Mode Until 25. September 2023**: A note explaining that Wordfence is in learning mode to understand the site and protect it. It includes a 'MANAGE FIREWALL' button and a 'LEARN MORE' link.
- Premium Protection Disabled**: A note about using the Community version of the Threat Defense Feed. It includes a 'UPGRADE TO PREMIUM' button and a 'LEARN MORE' link.
- Web Application Firewall**: Shows 35% completion. Status: Currently in Learning Mode. Actions: Manage WAF, Upgrade to Premium.
- Firewall Rules: Community**: Shows 70% completion. Status: Currently in Learning Mode. Actions: Upgrade to Premium.
- Real-Time IP Blocklist: Disabled**: Shows 0% completion. Status: Blocks requests from known malicious IPs. Actions: Upgrade to Premium.
- Brute Force Protection**: Shows 100% completion. Status: Stops Password Guessing Attacks. Actions: Manage Brute Force Protection.
- Rate Limiting**: Block crawlers that are using too many resources or stealing content.
- Blocking**: Block traffic by country, IP, IP range, user agent, referrer, or hostname.
- Help**: Find the documentation and help you need.
- All Firewall Options**: Manage global and advanced firewall options.
- Top IPs Blocked**: Shows a list of blocked IPs.
- Firewall Summary**: Attacks Blocked for vhs9.bee35.de.

Datenbanksicherheit

- Bei der Installation bitte keinen Datenbanknamen wie den Name der Webseite verwenden
- Und den Datenbanknamen nicht mit WP anfangen lassen

Dateiveränderungen im Backend sperren

- Dateien können im Themeeditor editiert werden. Natürlich auch von Eindringlingen durch die Hintertür!
- Abhilfe: in wp-config.php die Zeile einfügen:
`define('DISALLOW_FILE_EDIT', true);`