

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 3.28

[PRODUKTSEITE](#)[ALLE FUNKTIONEN](#)[CHANGELOG](#)[DOKUMENTATION](#)[FAQ](#)[SUPPORT](#)[DEMO ANFRAGEN](#)[KAUFEN](#)

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.

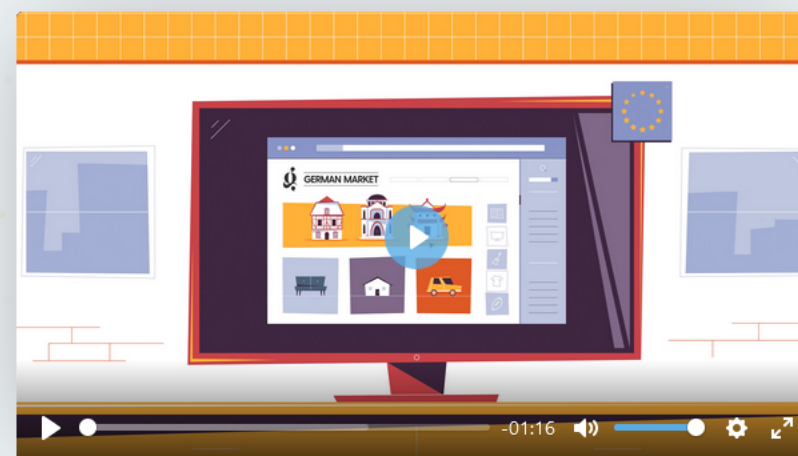
Ab 85,00 €

beinhaltet MwSt.

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

1

DEUTSCHLANDS NO. 1 WOOCOMMERCE
PREMIUM PLUGIN FÜR RECHTSSICHERHEIT



Voraussetzungen: PHP 7.4+, PHP-Bibliothek cURL, WooCommerce 6.4+,
WordPress 5.8+



German Market

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](#)

[CCI 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/>

 **SUCURI**


Website MonitoringWebsite FirewallMalware RemovalKnowledgebaseSupport

➔ vhs-kurs-wp.beeverso.eu

 **Site Issue**
500 Internal Server Error

 **Site is not Blacklisted**
9 Blacklists checked

Request Review

 **Redirects to:**
<https://vhs-kurs-wp.beeverso.eu/>

IP address: 85.13.145.247
Hosting: All-Inkl.com/Neue Medien Munnich
Running on: Apache

CMS: WordPress 6.3.1
Powered by: Unknown
[More Details](#)

Minimal

Low Security Risk

Medium

High

Critical


Site Issue Detected


<http://vhs-kurs-wp.beeverso.eu/404testpage4525d2fdc>

[Unable to scan the page. 500 Internal Server Error](#)


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.


Website Malware & Security

 No malware detected by scan (Low Risk)

 No injected spam detected (Low Risk)

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 [WPSServeur](#) 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

`http://vhs9.bee35.de/` `/`

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

`http://vhs9.bee35.de/` `/`

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 in a web browser. The browser's address bar displays 'vhs9.bee35.de'. The dashboard is titled 'Firewall' and includes a link to 'Learn more about the Firewall'. It features two main informational boxes at the top: 'Learning Mode Until 25. September 2023' and 'Premium Protection Disabled'. Below these are four status cards: 'Web Application Firewall' (35%), 'Firewall Rules: Community' (70%), 'Real-Time IP Blocklist: Disabled' (0%), and 'Brute Force Protection' (100%). The bottom section contains links for 'Rate Limiting', 'Blocking', 'Help', and 'All Firewall Options'. A sidebar on the left lists various WordPress dashboard items, with 'Wordfence' highlighted. The bottom of the dashboard shows 'Top IPs Blocked' and a 'Firewall Summary' for the domain 'vhs9.bee35.de'.

Firewall [Learn more about the Firewall](#)

Learning Mode Until 25. September 2023
When you first install the Wordfence Web Application Firewall, it will be in learning mode. This allows Wordfence to learn about your site so that we can understand how to protect it and how to allow normal visitors through the firewall. We recommend you let Wordfence learn for a week before you enable the firewall.
[MANAGE FIREWALL](#) [LEARN MORE](#)

Premium Protection Disabled
As a free Wordfence user, you are currently using the Community version of the Threat Defense Feed. Premium users are protected by additional firewall rules and malware signatures. Upgrade to Premium today to improve your protection.
[UPGRADE TO PREMIUM](#) [LEARN MORE](#)

Web Application Firewall	Firewall Rules: Community	Real-Time IP Blocklist: Disabled	Brute Force Protection
35%	70%	0%	100%
Currently in Learning Mode Manage WAF	Currently in Learning Mode Upgrade to Premium	Blocks requests from known malicious IPs Upgrade to Premium	Stops Password Guessing Attacks 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

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);`