Sicherheit für WordPress

Walter Ebert
walterebert.de

WP FRA

https://wpmeetup-frankfurt.de

Webhosting

- Aktuelle PHP-Version: 7.2/3/4
- SSL-Zertifikat für HTTPS
- FTPS

Optional:

- SSH-Zugang
- DDoS-Schutz/Firewall
- Virenscanner

Login

- Benutzername: ~~admin~~
- Passwort: Mindestens 12 Zeichen

Login

- Benutzername: ~~admin~~
- Passwort: Mindestens 12 Zeichen
- ~~Passwort~~ vs. Passphrase

Login

- Benutzername: ~~admin~~
- Passwort: Mindestens 12 Zeichen
- ~~Passwort~~ vs. ~~Passphrase~~ vs. Hole Phrase

1 Hoch auf die §-enreiter!

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

Passwörter

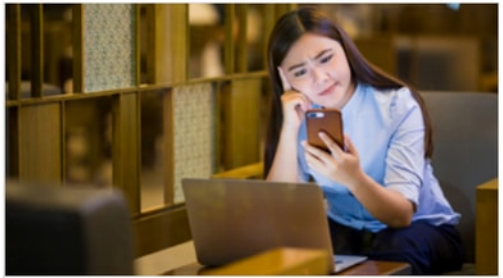
Passwörter

Wer die Wahl hat, hat die Qual – heißt es. Besonders bei der **Wahl der richtigen Passwörter** tun sich viele Internetnutzer schwer. Wen wundert's da, dass schlecht gewählte Passwörter wie 123456 oder qwert auf der Hitliste besonders häufiger IT-Sicherheitsdefizite ganz weit oben stehen? Bei denen, die sich stattdessen die Mühe machen, ein etwas komplizierteres Passwort zu nutzen, kommt es nicht selten vor, dass ein und dasselbe Passwort für viele verschiedene Programme beziehungsweise Zugänge genutzt wird. Hacker freut das alles natürlich. Sie haben Werkzeuge, die vollautomatisch alle möglichen Zeichenkombinationen ausprobieren, ganze Wörterbücher einschließlich gängiger Kombinationen aus Worten und angefügten Zahlen testen oder einmal im Internet veröffentlichte Zugangsdaten bei allen möglichen Diensten durchprobieren. Um das zu verhindern, sollte ein Passwort bestimmte Qualitätsanforderungen erfüllen und immer nur für einen Zugang genutzt werden.

Hinzu kommt, dass Passwörter nicht nur zum Schutz von vertraulichen Daten dienen. Ein Beispiel: Inzwischen ist es üblich, dass man sich bei unterschiedlichsten Anbietern im Internet ein Konto oder einen Zugang (Account) anlegen kann. Die Anmeldung an diesem Account wird mit einem Passwort geschützt. Was könnte passieren, wenn sich jemand unter Ihrem Namen dort anmeldet? Wer möchte

Inhaltsverzeichnis

Verwandte Themen



Passwort-Manager

- Vom Browser
- KeePass (Windows) https://keepass.info/
- KeePassXC https://keepassxc.org/
- Bitwarden https://bitwarden.com/
- 1Password https://1password.com/

https://de.wordpress.org/plugins/limit-login-attempts-reloaded/

Einstellungen für „Limit Login Attempts“

Einstellungen | Debug

Statistiken

Aussperrungen insgesamt — Den Zähler zurücksetzen — 10739 Aussperrungen seit dem letzten Zurücksetzen

Optionen

DSGVO-Konformität — ☑ dies macht das Plugin DSGVO-konform

Aussperrung

2 erlaubte Versuche
90 Minuten Aussperrung
2 Aussperrungen erhöhen die Aussperrzeit auf 24 Stunden
48 Stunden bis zum Zurücksetzen der Loginversuche

Benachrichtigung über Aussperrung

☑ Aussperrungsprotokoll
☐ Per E-Mail an hallo@wpmeetup-frankfurt.de nach 2 Aussperrungen

Whitelist

Eine IP-Adresse oder ein IP-Bereich (1.2.3.4-5.6.7.8) pro Zeile

https://de.wordpress.org/plugins/two-factor/

Dashboard
Beiträge
Medien
Seiten
Kommentare
Design
Plugins
Benutzer
Alle Benutzer
Neu hinzufügen
Dein Profil
Werkzeuge
Einstellungen
SEO
Menü einklappen

Dies kann öffentlich angezeigt werden.

Two-Factor-Einstellungen

Aktiviert	Primär	Name
☑	○	E-Mail. Authentifizierungs-Codes werden an wordpress@walterebert.de gesendet.
☐	○	Zeitlich limitiertes Einmalpasswort (Google Authenticator) Secret Key wurde konfiguriert und registriert. Key zurücksetzen *Du musst den QR-Code auf allen Geräten erneut scannen, da die vorherigen Codes nicht mehr funktionieren werden.*
☑	◉	FIDO Universal 2nd Factor (U2F) Erfordert eine HTTPS-Verbindung. Konfiguriere deine Security-Keys im Abschnitt "Security-Keys" unten.
☐	○	Backup-Verifizierungs-Codes (einmalige Nutzung) Verifizierungs-Codes generieren 0 unbenutzte Codes verbleibend.
☐	○	Testmethode

Security-Keys

Neuen Key registrieren

Hier findest du Verkaufsstellen für FIDO U2F Security-Key-Devices.

Name	Hinzugefügt	Kürzlich verwendet

wp-config.php

```
define( 'WP_AUTO_UPDATE_CORE', true );
define( 'WP_DEBUG', false );
define( 'DISALLOW_FILE_EDIT', true );
```

https://wordpress.org/support/article/editing-wp-config-php/

WordPress-Updates

- Händisch über WordPress-Admin
- Automatisch, Minor/Major-Version
- Automatisch, inkl. Plugins & Themes
- Händisch über WP-CLI (auch Remote)

Auto-Updates Plugins/Themes

wp-content/mu-plugins/hooks.php

```
<?php
add_filter( 'auto_update_plugin', '__return_true' );
add_filter( 'auto_update_theme', '__return_true' );
```

wp-cli

```
wp core update

wp @prod core update
```

wp-cli.yml

```
path: document_root

@prod:
  ssh: user@example.com
  path: path/to/document_root
```

https://sitecheck.sucuri.net/

Free website security check & malware scanner

Enter a URL (ex. sucuri.net) and the Sucuri SiteCheck scanner will check the website for known malware, viruses, blacklisting status, website errors, out-of-date software, and malicious code.

Scan Website | Scan Website

Disclaimer: Sucuri SiteCheck is a free website security scanner.
Remote scanners have limited access and results are not guaranteed. For a full scan, contact our team.

Keep your site clean, fast, and protected

https://siwecos.de/

SIWECOS
Auf der sicheren Seite

IT-Sicherheit
IN DER WIRTSCHAFT

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

SIWECOS Schnell-Check

Hinweis: Nur registrierte Webseiten können auf zusätzliche kritische Schwachstellen hin geprüft werden.

Die Registrierung und Nutzung von **SIWECOS ist kostenlos!**
Bitte registrieren Sie Ihre Webseite um weitere Funktionen wie den **täglichen Sicherheitscheck**, **automatische Benachrichtigungen** beim Fund einer kritischen Schwachstelle und den **ausführlichen Sicherheitsbericht** für Ihre Webseite nutzen zu können.

Domain, bspw. https://www.example.org

Scan starten

SIWECOS in 2 Minuten

https://de.wordpress.org/plugins/wpscan/

WPScan

WPScan

Von WPScan Team

Herunterladen

Details | Rezensionen | Installation | Support | Entwicklung

Beschreibung

Dieses Plugin überprüft täglich dein System auf mögliche Sicherheitslücken aus der WPScan-Sicherheitslücken-Datenbank. Mit einem Symbol in

Version:	1.4
Zuletzt aktualisiert:	vor 2 Monaten
Aktive Installationen:	3.000+

Dashboard
Media
Pages
Products
Forms
Appearance
OptionTree
Plugins 12
Installed Plugins
Add New
Plugin Report
Users
Tools
Settings
Custom Fields
Collapse menu

WordPress 5.3.2 is available! Please update now.

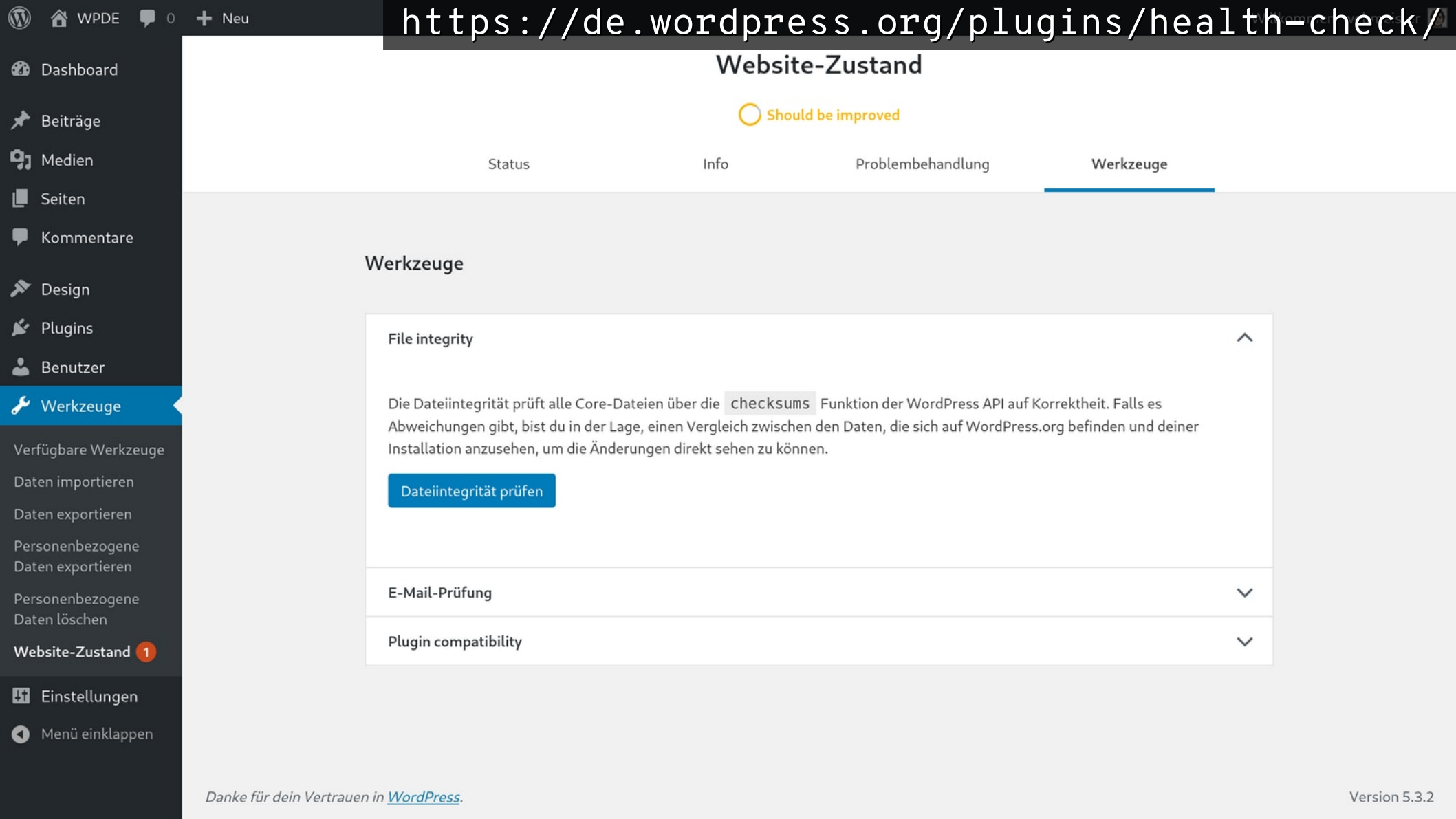
Plugin Report

Currently running WordPress version: 4.8.1. (An upgrade to 5.3.2 is available)

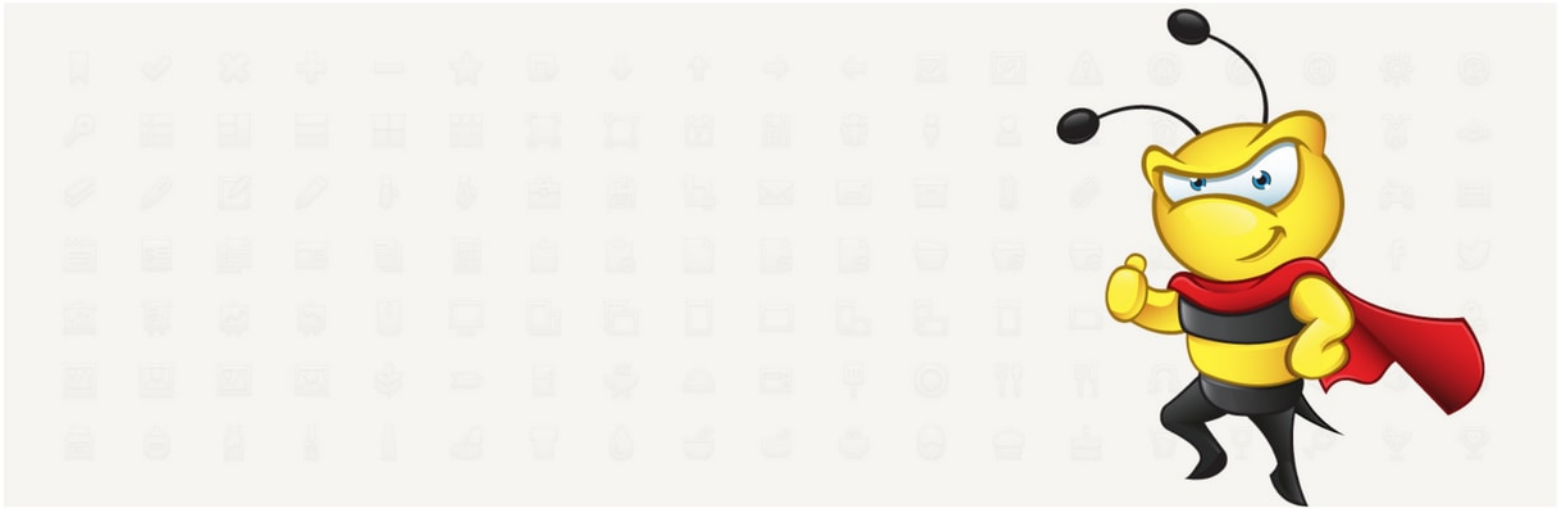
Clear cached plugin data and reload

Currently installed plugins

Name	Author	Activated	Installed version	Last update	Tested up to WP version	Rating
Advanced Custom Fields PRO	Elliot Condon	Yes	5.6.2	No data available	No data available	No data available
Disable Comments	Samir Shah	Yes	1.7 (1.10.2 available)	6 months	5.3.2	98%
EWWW Image Optimizer	Shane Bishop	Yes	3.6.1 (5.1.4 available)	2 weeks	5.3.2	92%
Imsanity	Shane Bishop	Yes	2.3.9 (2.5.0 available)	2 months	5.3.2	98%
Limit Login Attempts	Johan Eenfeldt	Yes	1.7.1	8 years	3.3.2	92%
Ninja Forms	The WP Ninjas	Yes	3.1.9 (3.4.22 available)	2 months	5.3.2	88%
Ninja Forms - Conditional Logic	The WP Ninjas	Yes	1.4.0	No data available	No data available	No data available
Normalizer	Torsten Landsiedel	Yes	1.0.0	4 years	4.2.26	No data available
OptionTree	Derek Herman	Yes	2.6.0 (2.7.3 available)	8 months	5.2.5	94%
Plugin Report	Roy Tanck	Yes	1.4	7 days	5.3.2	100%


WPDE
0
Neu
https://de.wordpress.org/plugins/health-check/
Dashboard
Beiträge
Medien
Seiten
Kommentare
Design
Plugins
Benutzer
Werkzeuge
Verfügbare Werkzeuge
Daten importieren
Daten exportieren
Personenbezogene Daten exportieren
Personenbezogene Daten löschen
Website-Zustand 1
Einstellungen
Menü einklappen
Website-Zustand
Should be improved
Status
Info
Problembehandlung
Werkzeuge
Werkzeuge
File integrity
Die Dateiintegrität prüft alle Core-Dateien über die checksums Funktion der WordPress API auf Korrektheit. Falls es Abweichungen gibt, bist du in der Lage, einen Vergleich zwischen den Daten, die sich auf WordPress.org befinden und deiner Installation anzusehen, um die Änderungen direkt sehen zu können.
Dateiintegrität prüfen
E-Mail-Prüfung
Plugin compatibility
Danke für dein Vertrauen in WordPress.
Version 5.3.2

https://de.wordpress.org/plugins/antispam-bee/



Antispam Bee

Von pluginkollektiv

Herunterladen

Details | Rezensionen | Installation | Support | Entwicklung

Beschreibung

Sag „Auf Wiedersehen“ zu Kommentar-Spam auf deiner WordPress-Installation. *Antispam Bee* blockiert Spam-Kommentare und -Trackbacks

Version:	2.9.1
Zuletzt aktualisiert:	vor 4 Monaten
Aktive Installationen:	500.000+

Dashboard
Beiträge
Medien
Seiten
Kommentare 3
Design
Plugins
Benutzer
Werkzeuge
Einstellungen
Allgemein
Schreiben
Lesen
Diskussion
Medien
Permalinks

Einstellungen › Diskussion

Standardeinstellungen für Beiträge

- [ ] Versuchen, jedes in Beiträgen verlinkte Weblog zu benachrichtigen (verlangsamt das Veröffentlichen)
- [ ] Link-Benachrichtigungen von anderen Blogs (Pingbacks und Trackbacks) zu neuen Beiträgen erlauben
- [ ] Besuchern erlauben, neue Beiträge zu kommentieren

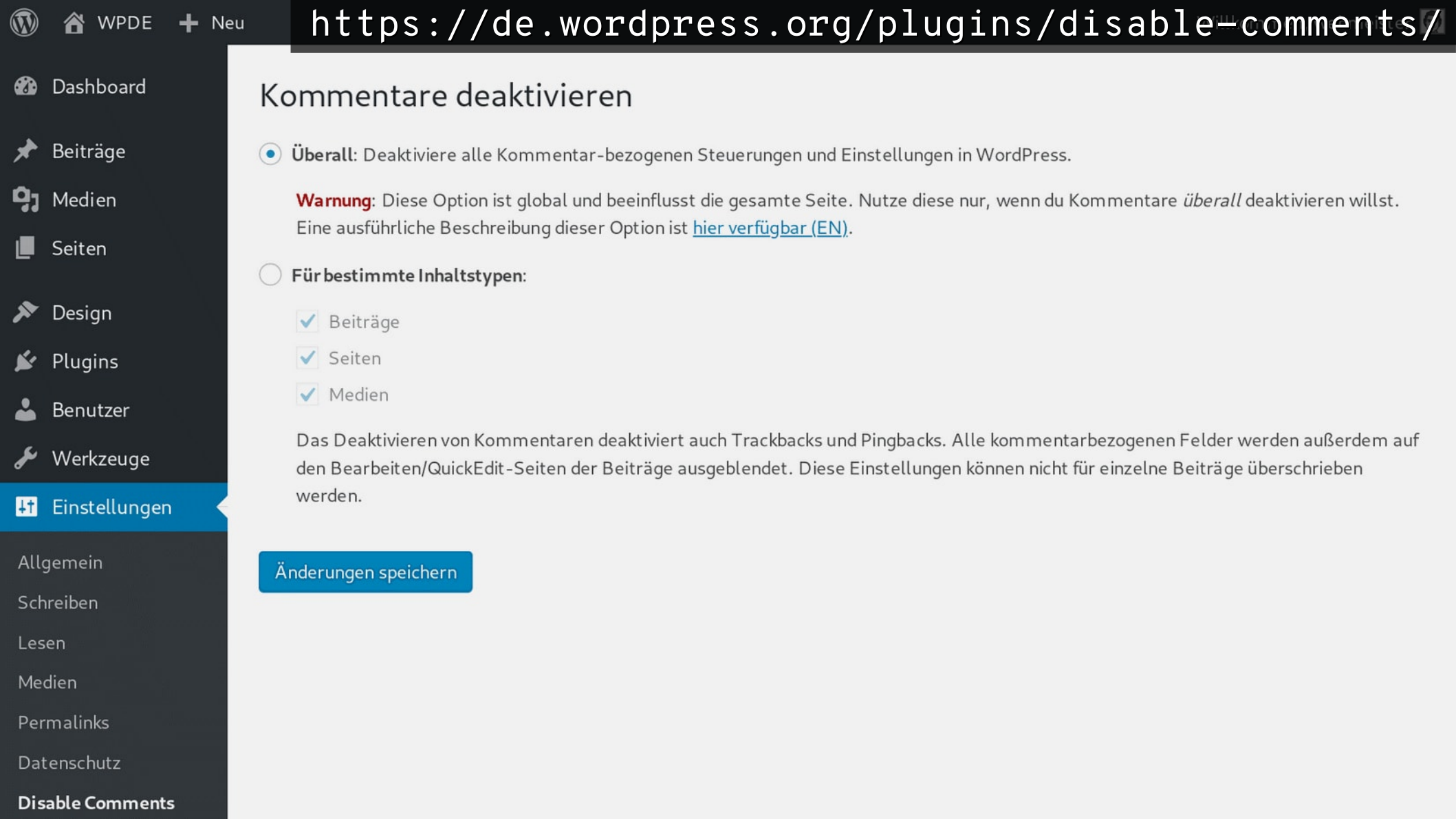
(Diese Einstellungen können für jeden Beitrag individuell geändert werden.)

Weitere Kommentareinstellungen

- [x] Benutzer müssen zum Kommentieren Name und E-Mail-Adresse angeben
- [ ] Benutzer müssen zum Kommentieren registriert und angemeldet sein
- [ ] Kommentare zu Beiträgen, die älter als 14 Tage sind, automatisch schließen
- [x] Das Opt-in-Kontrollkästchen für Kommentar-Cookies anzeigen, damit die Cookies des Kommentar-Autors gesetzt werden können.
- [x] Verschachtelte Kommentare in 5 Ebenen organisieren
- [ ] Kommentare in Seiten umbrechen, mit

50 Top-Level-Kommentaren pro Seite und die

letzte -Seite standardmäßig anzeigen.


WPDE
Neu
https://de.wordpress.org/plugins/disable-comments/
Dashboard
Beiträge
Medien
Seiten
Design
Plugins
Benutzer
Werkzeuge
Einstellungen
Allgemein
Schreiben
Lesen
Medien
Permalinks
Datenschutz
Disable Comments
Kommentare deaktivieren
Überall: Deaktiviere alle Kommentar-bezogenen Steuerungen und Einstellungen in WordPress.
Warnung: Diese Option ist global und beeinflusst die gesamte Seite. Nutze diese nur, wenn du Kommentare überall deaktivieren willst.
Eine ausführliche Beschreibung dieser Option ist hier verfügbar (EN).
Für bestimmte Inhaltstypen:
Beiträge
Seiten
Medien
Das Deaktivieren von Kommentaren deaktiviert auch Trackbacks und Pingbacks. Alle kommentarbezogenen Felder werden außerdem auf den Bearbeiten/QuickEdit-Seiten der Beiträge ausgeblendet. Diese Einstellungen können nicht für einzelne Beiträge überschrieben werden.
Änderungen speichern

https://de.wordpress.org/plugins/disable-json-api/

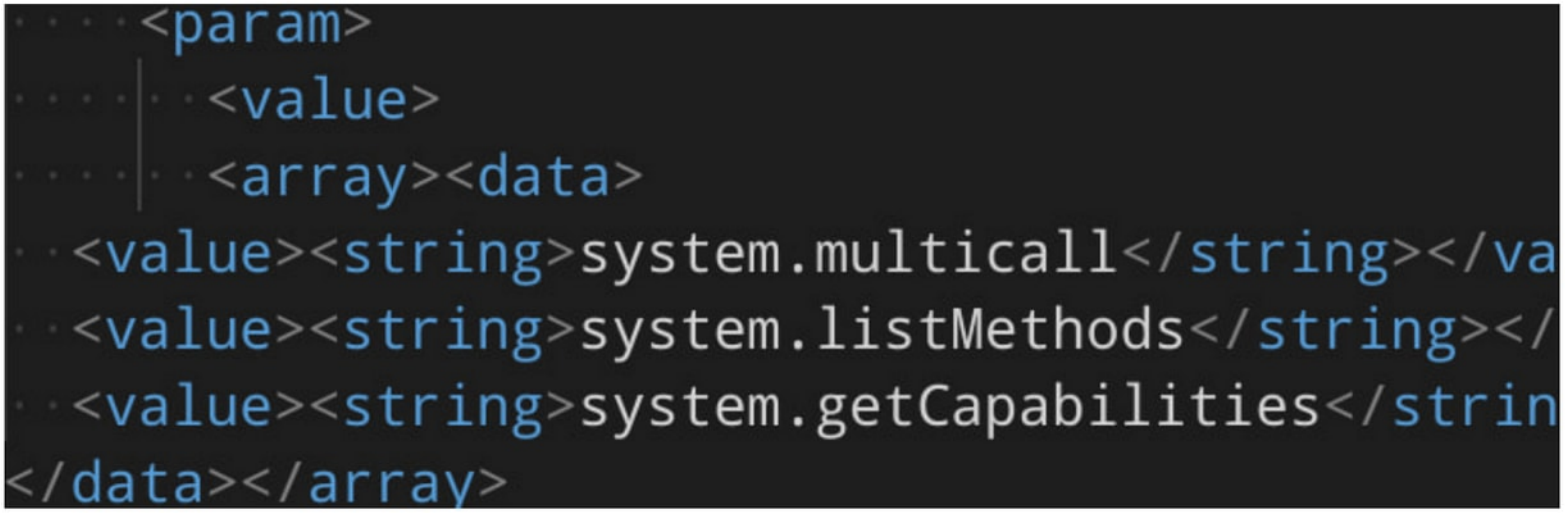
Kommentare 3
Formulare
Design
Plugins
Benutzer
Werkzeuge
Einstellungen
Allgemein
Schreiben
Lesen
Diskussion
Medien
Permalinks
Datenschutz
Disable REST API
Menü einklappen

- [ ] / *REST API ROOT*

Das Stammverzeichnis der REST API auf dieser Website ist **http://wpde.localhost/wp-json/**

- [ ] **/oembed/1.0**
  - [ ] /oembed/1.0/embed
  - [ ] /oembed/1.0/proxy
- [x] **/contact-form-7/v1**
  - [x] /contact-form-7/v1/contact-forms
  - [x] /contact-form-7/v1/contact-forms/(?P<id>\d+)
  - [x] /contact-form-7/v1/contact-forms/(?P<id>\d+)/feedback
  - [x] /contact-form-7/v1/contact-forms/(?P<id>\d+)/refill
- [ ] **/wp/v2**
  - [ ] /wp/v2/posts
  - [ ] /wp/v2/posts/(?P<id>[\d]+)
  - [ ] /wp/v2/posts/(?P<parent>[\d]+)/revisions
  - [ ] /wp/v2/posts/(?P<parent>[\d]+)/revisions/(?P<id>[\d]+)
  - [ ] /wp/v2/posts/(?P<id>[\d]+)/autosaves
  - [ ] /wp/v2/posts/(?P<parent>[\d]+)/autosaves/(?P<id>[\d]+)
  - [ ] /wp/v2/pages

https://de.wordpress.org/plugins/wee-remove-xmlrpc-methods/



Remove XML-RPC Methods

Von Walter Ebert

Herunterladen

Dieses Plugin wurde noch nicht auf Deutsch übersetzt. Hilf mit, es zu übersetzen!

Details | Rezensionen | Installation | Support | Entwicklung

Beschreibung

Version: 1.1.0

https://de.wordpress.org/plugins/better-wp-security/

iThemes Security (formerly Better WP Security)

Von iThemes

Herunterladen

Details | Rezensionen | Installation | Support | Entwicklung

Beschreibung

ITHEMES SECURITY IST FÜR WORDPRESS DAS SICHERHEITS-PLUGIN NUMMER 1

iThemes Security (formerly Better WP Security) bietet dir mehr als 30

Version:	7.6.1
Zuletzt aktualisiert:	vor 1 Monat
Aktive Installationen:	900.000+

https://de.wordpress.org/plugins/wordfence/

Wordfence Security – Firewall & Malware Scan

Von Wordfence

Herunterladen

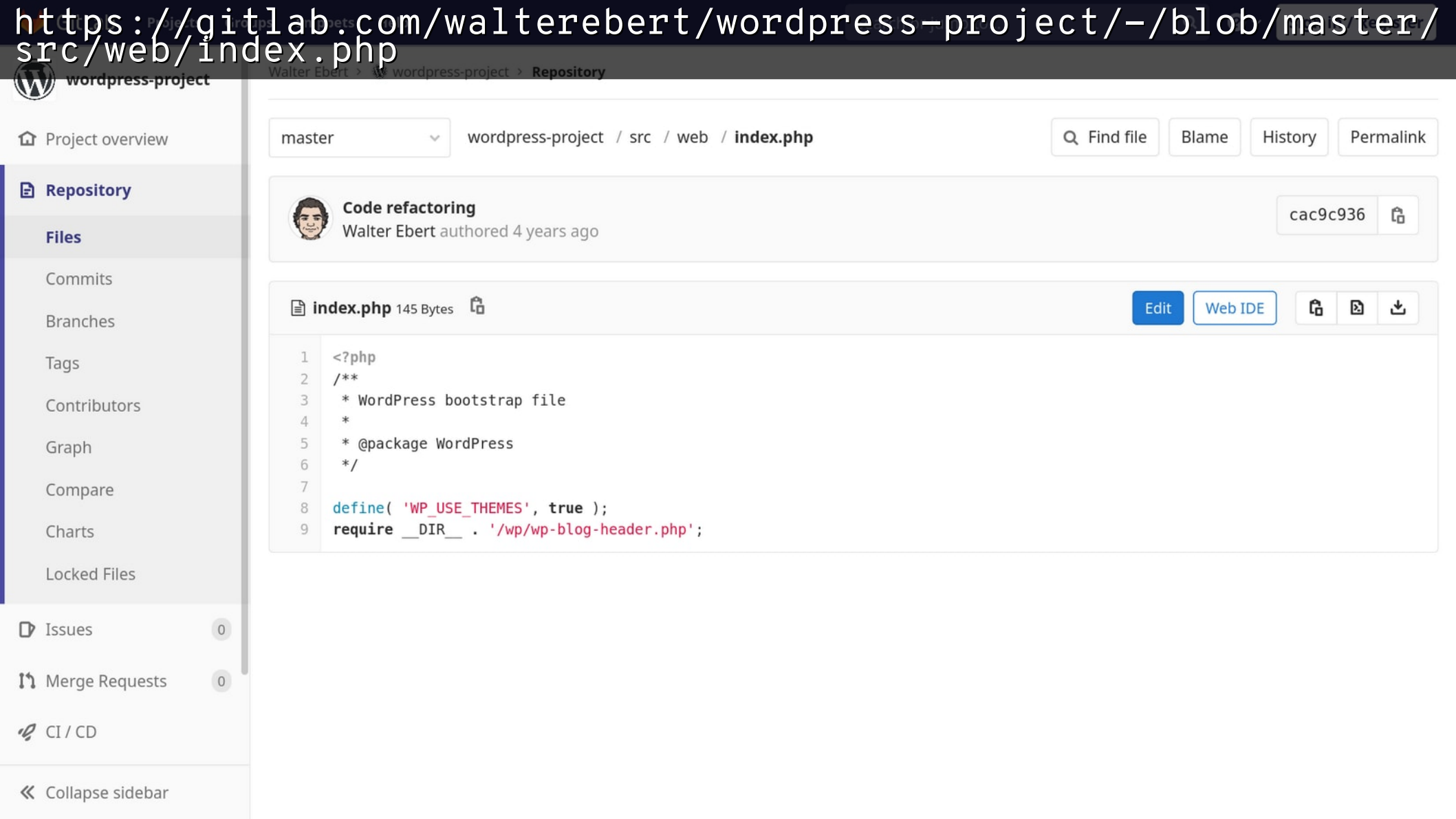
Dieses Plugin wurde noch nicht auf Deutsch übersetzt. Hilf mit, es zu übersetzen!

Details | Rezensionen | Installation | Support | Entwicklung

Beschreibung

Version: 7.4.5

https://gitlab.com/walterebert/wordpress-project/-/blob/master/src/web/index.php



wp-config.php

```
define( 'WP_SITEURL', 'https://de.wp.org/wp' );
define( 'WP_HOME', 'https://de.wp.org' );
define( 'WP_CONTENT_URL', 'https://de.wp.org/content' );
define( 'WP_CONTENT_DIR', '/path/to/content' );
```

https://wordpress.org/support/article/editing-wp-config-php/

https://gitlab.com/walterebert/wordpress-project/-/blob/master/src/web/.htaccess

Project overview

Repository

Files

Commits

Branches

Tags

Contributors

Graph

Compare

Charts

Locked Files

Issues 0

Merge Requests 0

CI / CD

Collapse sidebar

master wordpress-project / src / web / .htaccess

Find file | Blame | History | Permalink

Update dependencies; Require PHP 7.2 or later; Various improvements;
Walter Ebert authored 5 minutes ago

59a3360b

.htaccess 9.34 KB

Edit | Web IDE

```
# PHP
#php_flag display_errors off
#php_flag log_errors on
#php_value error_reporting "E_ALL & ~E_NOTICE & ~E_STRICT & ~E_DEPRECATED"
#php_flag session.cookie_httponly on
#php_value upload_max_filesize 10M
#php_value post_max_size 10M

# Redirect from the `http://` to the `https://` version of the URL.
# https://wiki.apache.org/httpd/RewriteHTTPToHTTPS
#<IfModule mod_rewrite.c>
#  RewriteEngine On
#  RewriteCond %{HTTPS} !=on
#  RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
#</IfModule>

<IfModule mod_headers.c>
  # More security: https://www.owasp.org/index.php/List_of_useful_HTTP_headers
  Header set X-XSS-Protection "1; mode=block"

  # Tell browser to always connect over HTTPS
  <If "%{HTTPS} == 'on'">
```

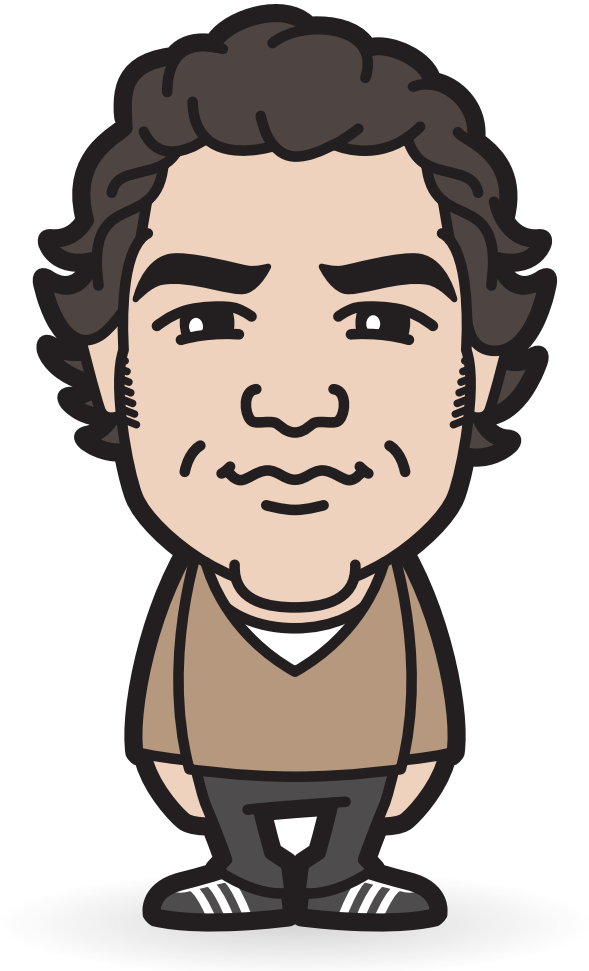
https://www.wp-wartung24.de/newsletter/

wpwartung24

Sicherheit und Wartung für Ihr WordPress.

Newsletter

WordPress-Sicherheit – zweiwöchentlicher Newsletter



@wltrd
walterebert.de
slideshare.net/walterebert
mastodon.social/@walterebert