Domain-Check Plugin WordPress

WP24 Domain Check

Beschreibung

Mit WP24 Domain Check können Domains überprüft werden, ob sie frei zur Registrierung sind. Das responsive Formular kann einfach über einen Shortcode oder ein Widget integriert werden. Beschriftungen und Farben können über die Einstellungsseite angepasst werden.

Funktionen

- Einfache Integration über Shortcode oder Widget
- Ajax-basierte Suche (kein erneutes Laden der Seite erforderlich)
- Definition einer Liste testbarer TLDs
- Drop-Down Liste (TLD aus vordefinierter Liste auswählen)
- Freitext Eingabe (TLD in Feld für Domainnamen eingeben)
- Über 1.500 unterstützte TLDs
- Möglichkeit, jede TLD zu überprüfen
- Unterstützung für internationalisierte Domainnamen (IDN)
- Gleichzeitige Überprüfung aller TLDs (asynchron)
- Detaillierte Whois Informationen anzeigen (wenn die Domain registriert ist)
- Preis und Kauflink für jede TLD hinterlegen
- WooCommerce Integration
- Responsives Design
- Botschutz mit reCAPTCHA (Version 2 und 3)
- Anpassung von Beschriftungen und Farben
- WPML- und Polylang-kompatibel

Internetnutzer – Report – Deutschland

Downloads – OVK

Trendstudie 2022 – Werbung im Internet

Search One (SEO)

WordPress – SEARCH ONE

Hier findest Du alle Artikel zum Thema WordPress, die wir in den letzten Jahren geschrieben haben. Wenn Du auf der Suche nach einem WordPress-Hosting, WordPress-Plugins oder WordPress-Theme bist, wirst Du hier garantiert fündig!

WordPress – SICHERHEIT – So bereinigen Sie eine gehackte

WordPress

How to Clean a Hacked WordPress Site using Wordfence – Wordfence

If your site has been hacked, Don’t Panic. This article will describe how to clean your site if it has been hacked and infected with malicious code, backdoors, spam, malware, or other nastiness. This article was updated in December of 2021 with additional resources to help clean specific infection t… Wenn Ihre Website gehackt wurde, geraten Sie nicht in Panik.

In diesem Artikel wird beschrieben, wie Sie Ihre Website bereinigen, wenn sie gehackt und mit bösartigem Code, Hintertüren, Spam, Malware oder anderen schädlichen Inhalten infiziert wurde. Dieser Artikel wurde im Dezember 2021 mit zusätzlichen Ressourcen zur Beseitigung bestimmter

Infektionstypen aktualisiert. Dieser Artikel wurde von Mark Maunder, dem Gründer von Wordfence, geschrieben. Ich bin ein akkreditierter Sicherheitsforscher, ein CISSP, ein WordPress-Entwickler und der Geschäftsführer von Defiant Inc, dem Hersteller von Wordfence. Auch wenn Sie kein WordPress verwenden, enthält dieser Artikel mehrere Tools, mit denen Sie Ihre Website von einer Infektion befreien können.

Wenn Sie WordPress verwenden und gehackt wurden, können Sie Wordfence verwenden, um einen Großteil des Schadcodes von Ihrer Website zu entfernen. Mit Wordfence können Sie Ihre gehackten Dateien mit den ursprünglichen WordPress-Kerndateien und den Originalkopien von WordPress-Themes und -Plugins im Repository vergleichen. Mit Wordfence können Sie sehen, was sich geändert hat, und haben die Möglichkeit, Dateien mit einem Klick zu reparieren oder zu löschen.

Wenn Sie ein vielbeschäftigter Geschäftsinhaber sind und möchten, dass sich unser erfahrenes Team um das Problem kümmert, melden Sie sich jetzt bei Wordfence Care auf den Link „Hilfe anfordern“, an und klicken Sie dann auf der Lizenzseite um sofort eine Anfrage zur Website-Bereinigung zu stellen .

Wenn Sie eine geschäftskritische Website haben und diese sofort oder außerhalb der regulären Geschäftszeiten gereinigt werden muss, melden Sie sich jetzt bei Wordfence Response an und stellen Sie eine Website-Reinigungsanfrage. Unser 24-Stunden-Team zur Reaktion auf Vorfälle wird innerhalb einer Stunde mit der Arbeit beginnen. Sie reagieren unglaublich schnell und lösen das gesamte Problem innerhalb von 24 Stunden. Gehen Sie wie bei Wordfence Care nach der Anmeldung zur Seite „Lizenzen“ und klicken Sie bei Ihrer Lizenz auf „Hilfe anfordern“. Sie gelangen dann in die Prioritätswarteschlange für Response-Kunden.

Wenn Sie sich selbst um das Problem kümmern möchten oder Wordfence Care oder Response nicht in Ihrem Budget liegt, lesen Sie weiter. WIR KÖNNEN DAS SCHAFFEN!! Das Bereinigen

Ihrer gehackten Website ist einer der Gründe, warum ich Wordfence erstellt habe. Die kostenlose Version von Wordfence enthält leistungsstarke Tools, die Ihnen beim Bereinigen Ihrer Website helfen.

Wurden Sie wirklich gehackt?

Wenn Sie vermuten, dass Sie gehackt wurden, stellen Sie zunächst sicher, dass Sie tatsächlich gehackt wurden. Manchmal wenden sich Website-Administratoren in Panik an uns und denken, sie seien gehackt worden, obwohl sich ihre Website einfach nur schlecht verhält, ein Update fehlgeschlagen ist oder ein anderes Problem auftritt. Manchmal sehen Websitebesitzer Spam-Kommentare und können den Unterschied zwischen diesen und einem Hack nicht erkennen.

Ihre Website wurde gehackt, wenn:

- In der Kopf- oder Fußzeile Ihrer Website wird Spam angezeigt, der Werbung für Dinge wie Pornografie, Drogen, illegale Dienste usw. enthält. Oftmals wird dieser Spam in den Inhalt Ihrer Seite eingefügt, ohne dass an die Darstellung gedacht wurde, sodass er möglicherweise als dunkler Text auf einer Seite erscheint Der Hintergrund muss dunkel sein und für das menschliche Auge nicht gut sichtbar sein (die Suchmaschinen können ihn jedoch erkennen).
- Sie führen eine Site:example.com-Suche (ersetzen Sie example.com durch Ihre Website) bei Google durch und sehen Seiten oder Inhalte, die Sie nicht kennen und die bösartig aussehen.
- Sie erhalten Berichte von Ihren Benutzern, dass sie auf eine bösartige oder Spam-Website weitergeleitet werden. Achten Sie besonders darauf, da viele Hacks erkennen, dass Sie der Site-Administrator sind, und Ihnen keine Spam-Inhalte anzeigen, sondern Spam nur Ihren Besuchern oder den Suchmaschinen-Crawlern anzeigen. Versuchen Sie,

beim Besuch Ihrer Website ein Inkognito-Fenster zu verwenden oder Ihre Website über ein Suchergebnis zu besuchen, anstatt die URL direkt einzugeben.

- Sie erhalten von Ihrem Hosting-Anbieter eine Meldung, dass Ihre Website böswillige oder Spam-Aktivitäten ausführt. Wenn Ihr Host Ihnen beispielsweise mitteilt, dass er Berichte über Spam-E-Mails erhält, die einen Link zu Ihrer Website enthalten, kann dies bedeuten, dass Sie gehackt wurden. Was die Angreifer in diesem Fall tun, besteht darin, Spam von irgendwoher zu versenden und Ihre Website als Link zu verwenden, um Personen auf eine Website umzuleiten, die ihnen gehört. Sie tun dies, weil das Einfügen eines Links zu Ihrer Website Spamfilter umgeht, während das Einfügen eines Links zu ihrer eigenen Website von Spamfiltern erfasst wird.

Wordfence erkennt viele dieser Probleme sowie andere, die ich hier nicht erwähnt habe. Achten Sie daher auf unsere Warnungen und reagieren Sie entsprechend.

Sichern Sie jetzt Ihre Website. Hier ist der Grund:

Sobald Sie festgestellt haben, dass Sie gehackt wurden, sichern Sie sofort Ihre Website. Verwenden Sie FTP, das Backup-System Ihres Hosting-Anbieters oder ein Backup-Plugin, um eine Kopie Ihrer gesamten Website herunterzuladen. Sie müssen dies tun, da viele Hosting-Anbieter Ihre gesamte Website sofort löschen, wenn Sie melden, dass sie gehackt wurde, oder wenn sie schädliche Inhalte entdecken. Klingt verrückt, oder? In manchen Fällen ist dies jedoch ein Standardverfahren, um zu verhindern, dass andere Systeme in ihrem Netzwerk infiziert werden.

Stellen Sie sicher, dass Sie auch Ihre Website-Datenbank

sichern. Die Sicherung Ihrer Dateien und Datenbank sollte Ihre erste Priorität sein. Wenn Sie dies erledigen, können Sie sicher mit dem nächsten Schritt der Bereinigung Ihrer Website fortfahren und dabei beruhigt sein, dass Sie zumindest eine Kopie Ihrer gehackten Website haben und nicht alles verlieren.

Dinge, die Sie wissen sollten, bevor Sie eine gehackte WordPress-Site bereinigen:

Hier sind die Verkehrsregeln für die Reinigung Ihrer Website:

- Normalerweise können Sie alles im wp-content/plugins/-Verzeichnis löschen, ohne dass dabei Daten verloren gehen oder Ihre Website beschädigt wird. Dabei handelt es sich um Plugin-Dateien, die Sie neu installieren können, sodass Sie keine Daten löschen, die Sie nicht einfach ersetzen können. Wenn Sie diese Dateien löschen, erkennt WordPress automatisch, dass Sie ein Plugin gelöscht haben und deaktiviert es. Es wird also nicht zum Absturz Ihrer Website führen. **Stellen Sie einfach sicher, dass Sie in wp-content/plugins ganze Verzeichnisse löschen und nicht nur einzelne Dateien.** Wenn Sie beispielsweise das Wordfence-Plugin löschen möchten, müssen Sie wp-content/plugins/wordfence und alles in diesem Verzeichnis löschen, einschließlich des Verzeichnisses selbst. Wenn Sie nur ein paar Dateien aus einem Plugin löschen, kann Ihre Website möglicherweise nicht mehr funktionsfähig sein.
- Normalerweise haben Sie nur ein Theme-Verzeichnis, das für Ihre Site im Verzeichnis wp-content/themes verwendet wird. Wenn Sie wissen, welches das ist, können Sie alle anderen Theme-Verzeichnisse löschen. **Beachten Sie, dass Sie bei einem „untergeordneten Thema“ möglicherweise zwei Verzeichnisse in wp-content/themes verwenden** . Dies

ist keine übliche Konfiguration.
- Den Verzeichnissen wp-admin und wp-includes werden sehr selten neue Dateien hinzugefügt. Wenn Sie also in diesen Verzeichnissen etwas Neues finden, ist die Wahrscheinlichkeit hoch, dass es bösartig ist.

Achten Sie auf alte WordPress-Installationen und Backups. Wir sehen oft infizierte Websites, bei denen jemand sagt: „Aber ich habe meine Website auf dem neuesten Stand gehalten und ein Sicherheits-Plugin installiert, warum wurde ich also gehackt?“ Manchmal passiert es, dass Sie oder ein Entwickler eine Kopie aller Ihrer Site-Dateien in einem Unterverzeichnis wie /old/ sichern, auf das über das Internet zugegriffen werden kann. Dieses Backup wird nicht gepflegt und obwohl Ihre Hauptseite sicher ist, kann ein Angreifer auf die alte Seite zugreifen, sie infizieren und über die von ihm installierte Hintertür auf Ihre Hauptseite zugreifen. Lassen Sie also **niemals alte WordPress-Installationen herumliegen. Wenn Sie gehackt werden, überprüfen Sie diese zuerst, da sie wahrscheinlich voller Malware sind.**

Ein paar nützliche Tools:

Wenn Sie SSH-Zugriff auf Ihren Server haben, melden Sie sich an und führen Sie den folgenden Befehl aus, um alle Dateien anzuzeigen, die in den letzten 2 Tagen geändert wurden. Beachten Sie, dass der Punkt das aktuelle Verzeichnis angibt. Dadurch durchsucht der folgende Befehl das aktuelle Verzeichnis und alle Unterverzeichnisse nach kürzlich geänderten Dateien. Um herauszufinden, was Ihr aktuelles Verzeichnis ist, wenn Sie SSH verwenden, geben Sie „pwd“ ohne Anführungszeichen ein und drücken Sie die Eingabetaste.

```
find . -mtime -2 -ls
```

Oder Sie können ein bestimmtes Verzeichnis angeben:

```
find /home/yourdirectory/yoursite/ -mtime -2 -ls
```

Oder Sie können die Suche ändern, um Dateien anzuzeigen, die in den letzten 10 Tagen geändert wurden:

```
find /home/yourdirectory/yoursite/ -mtime -10 -ls
```

Wir empfehlen Ihnen, die obige Suche durchzuführen und die Anzahl der Tage schrittweise zu erhöhen, bis Sie geänderte Dateien sehen. Wenn Sie selbst nichts geändert haben, seit Sie gehackt wurden, ist es sehr wahrscheinlich, dass Sie die Dateien sehen, die der Angreifer geändert hat. Sie können sie dann selbst bearbeiten oder löschen, um den Hack zu bereinigen. Dies ist bei weitem die effektivste und einfachste Methode, um herauszufinden, welche Dateien infiziert wurden, und wird von jedem professionellen Website-Reinigungsdienst verwendet.

Ein weiteres nützliches Tool in SSH ist „grep“. Um beispielsweise nach Dateien zu suchen, die auf die Base64-Kodierung verweisen (häufig von Hackern verwendet), können Sie den folgenden Befehl ausführen:

```
grep -ril base64 *
```

Dadurch werden nur die Dateinamen aufgelistet. Sie können die Option „l“ weglassen, um den tatsächlichen Inhalt der Datei anzuzeigen, in der die Base64-Zeichenfolge vorkommt:

```
grep -ri base64 *
```

Bedenken Sie, dass „base64“ auch in legitimem Code vorkommen kann. Bevor Sie etwas löschen, sollten Sie sicherstellen, dass Sie keine Datei löschen, die von einem Theme oder Plugin auf Ihrer Website verwendet wird. Eine verfeinerte Suche könnte so aussehen:

```
grep --include=*.php -rn . -e "base64_decode"
```

Dieser Befehl durchsucht alle Verzeichnisse und

Unterverzeichnisse nach Dateien, die auf .php enden, durchsucht sie nach der Textzeichenfolge „base64_decode“ und gibt alle gefundenen Ergebnisse einschließlich der Zeilennummer aus, sodass Sie leicht finden können, wo sie in jeder Datei vorkommt .

Nachdem Sie nun wissen, wie man „grep“ verwendet, empfehlen wir Ihnen, grep in Kombination mit „find“ zu verwenden. Was Sie tun sollten, ist, Dateien zu finden, die kürzlich geändert wurden, zu sehen, was in der Datei geändert wurde, und wenn Sie eine häufige Textzeichenfolge wie „bad hacker was here“ finden, können Sie einfach alle Ihre Dateien wie folgt nach diesem Text durchsuchen:

grep -irl "bad hacker was here" *

und das zeigt Ihnen alle infizierten Dateien, die den Text „bad hacker was here“ enthalten. Vergessen Sie nicht das Sternchen (den Stern) am Ende des letzten Befehls.

Ich habe dir gesagt, dass wir das schaffen können! Ich bin mir sicher, dass Sie sich zu diesem Zeitpunkt wegen Ihrer gehackten Website viel weniger gestresst fühlen, da Sie jetzt über ein paar Tools zum Sortieren schädlicher Dateien aus Ihrer regulären WordPress-Installation verfügen.

Gehen wir noch tiefer! Wenn Sie viele infizierte Websites bereinigen, werden Sie Muster bemerken, an denen sich häufig bösartiger Code befindet. Ein solcher Ort ist das Upload-Verzeichnis in WordPress-Installationen. Der folgende Befehl zeigt Ihnen, wie Sie alle Dateien im Upload-Verzeichnis finden, die keine Bilddateien sind. Die Ausgabe wird in einer Protokolldatei namens „uploads-non-binary.log“ in Ihrem aktuellen Verzeichnis gespeichert.

find public_html/wp-content/uploads/ -type f -not -name "*.jpg" -not -name "*.png" -not -name "*.gif" -not -name "*.jpeg" -not -name “*.webp” >uploads-non-binary.log

Beachten Sie den Verzeichnispfad direkt nach dem Befehl „find“ oben. Wir gehen davon aus, dass Ihr aktuelles Verzeichnis Ihr Home-Verzeichnis auf Ihrem Webserver ist. Wir gehen außerdem davon aus, dass sich Ihre Website in public_html/ direkt neben diesem Home-Verzeichnispfad befindet. Denken Sie daran, dass Sie „pwd“ eingeben können, um herauszufinden, in welchem Verzeichnis Sie sich gerade befinden. Sie können auch „ls“ eingeben, um alle Dateien in Ihrem aktuellen Verzeichnis anzuzeigen, oder „ls -la“, um die Dateien in Ihrem aktuellen Verzeichnis mit weiteren Daten anzuzeigen jede Datei, wie Berechtigungen, Besitzer und wann die Datei zuletzt geändert wurde.

Mit den beiden einfachen Befehlszeilentools „grep“ und „find“ können Sie häufig eine ganze infizierte Website bereinigen. Wie einfach ist das! Ich wette, Sie sind jetzt bereit, Ihr eigenes Unternehmen für die Gebäudereinigung zu gründen.

So bereinigen Sie Ihre gehackte WordPress-Site mit Wordfence:

Nachdem Sie nun einige leistungsstarke Tools in Ihrem Arsenal haben und bereits einige Grundreinigungen durchgeführt haben, starten wir Wordfence und führen einen vollständigen Scan durch, um Ihre Website zu bereinigen. Dieser Schritt ist wichtig, da Wordfence eine sehr komplexe Suche nach Infektionen durchführt. Zum Beispiel:

- Wir wissen, wie alle WordPress-Kerndateien, Open-Source-Themes und Open-Source-Plugins aussehen sollten, sodass Wordfence erkennen kann, ob eine Ihrer Quelldateien infiziert ist, selbst wenn es sich um eine neue Infektion handelt, die noch niemand zuvor gesehen hat. **Dies erreichen wir, indem wir die öffentlich verfügbaren Originaldateien mit Ihren Daten vergleichen und alle Änderungen kennzeichnen.** Es ist tatsächlich eine der

coolsten Funktionen in Wordfence und völlig kostenlos!

- Wir suchen mithilfe komplexer regulärer Ausdrücke, die wir „Malware-Signaturen“ nennen, nach Anzeichen einer Kompromittierung. Unsere Malware-Signaturen werden basierend auf unserer Datenbank bekannter Infektionen kontinuierlich aktualisiert und unsere Premium-Kunden erhalten sofort die neuesten Signaturen. Mit einfachen Unix-Befehlszeilentools oder cPanel ist dies nicht möglich. Wir haben die besten Malware-Signaturen der Branche!
- Wir durchsuchen Ihre Dateien nach bekannten bösartigen Domänennamen, die häufig in Malware- und Spam-Dateien vorkommen.
- Wir verwenden SpamHaus, um festzustellen, ob die Domain oder IP-Adresse Ihrer Website zum Versenden von Spam verwendet wurde.
- Der Wordfence-Scan ist außerdem so konzipiert, dass er SEHR schnell läuft, wenn man bedenkt, wie viel Arbeit er macht, und sucht im Gegensatz zu generischen Scannern gezielt nach WordPress-Malware.

So bereinigen Sie Ihre gehackte Website mit Wordfence:

1. Aktualisieren Sie Ihre Website auf die neueste Version von WordPress. Dies ist wichtig, da ältere Versionen von WordPress ungepatchte Schwachstellen aufweisen können.
2. Aktualisieren Sie alle Ihre Themes und Plugins auf die neuesten Versionen. Das Gleiche gilt auch hier. Entwickler beheben ständig Schwachstellen und Sicherheitsprobleme in Themes und Plugins. Besorgen Sie sich daher die neueste Version jedes Themes oder Plugins, das Sie verwenden.
3. Ändern Sie alle Passwörter auf der Website, insbesondere Administratorpasswörter. Wenn ein Benutzer oder, schlimmer noch, ein Administrator ein Passwort wiederverwendet hat, ist der Angreifer möglicherweise

auf diese Weise überhaupt auf Ihre Website gelangt. Daher ist es wichtig, diese Änderung vorzunehmen.

4. Erstellen Sie ein weiteres Backup und speichern Sie es getrennt von dem oben empfohlenen Backup. Jetzt haben Sie eine infizierte Site, aber auf dieser Site wird die neueste Version von allem ausgeführt. Wenn beim Bereinigen Ihrer Website mit Wordfence etwas kaputt geht, können Sie zu dieser Sicherung zurückkehren und müssen nicht alle oben genannten Schritte erneut ausführen.
5. Stellen Sie sicher, dass Wordfence installiert ist. Die kostenlose Version reicht völlig aus, aber die Premium-Version bietet Ihnen die neuesten Malware-Signaturen und bösartigen Domänen.
6. Gehen Sie zum Wordfence-Menü „Scannen“ und klicken Sie einfach auf „Scan starten“. Dadurch wird ein erster Scan durchgeführt und Sie erhalten möglicherweise viele Ergebnisse, die Sie durcharbeiten müssen. Jedes Ergebnis erklärt, was Wordfence gefunden hat, und hilft Ihnen bei der Lösung des Problems.
7. Sobald der Scan abgeschlossen ist und Sie die von Wordfence gefundenen Probleme behoben haben, können Sie einen noch tieferen Scan durchführen. Gehen Sie links zum Menü „Alle Optionen“. Scrollen Sie etwa zwei Drittel nach unten zur Überschrift „Grundlegende Scantypoptionen“ und aktivieren Sie das Kontrollkästchen, um „Hohe Empfindlichkeit“ zu aktivieren. Dadurch wird ein viel tiefergehender Scan durchgeführt, der etwas länger dauert, aber dieser Scan findet wirklich hartnäckige Malware, die schwerer zu erkennen und zu entfernen ist.
8. Wenn Sie zusätzliche Scans durchführen möchten, können Sie Ihren Wordfence-Scan auf der Seite „Alle Optionen“ genau an Ihre Bedürfnisse anpassen. Führen Sie so viele Scans durch, wie Sie möchten. Es gibt keine Begrenzung für die Anzahl der Scans, auch für unsere kostenlosen Kunden.

9. Wenn die Ergebnisse angezeigt werden, wird möglicherweise eine sehr lange Liste infizierter Dateien angezeigt. Nehmen Sie sich Zeit und arbeiten Sie die Liste langsam durch.
10. Untersuchen Sie alle verdächtigen Dateien und bearbeiten Sie diese entweder manuell, um sie zu bereinigen, oder löschen Sie die Datei. Denken Sie daran, dass Sie Löschungen nicht rückgängig machen können. Aber solange Sie das oben empfohlene Backup erstellt haben, können Sie die Datei jederzeit wiederherstellen, wenn Sie das Falsche löschen.
11. Sehen Sie sich alle geänderten Kern-, Theme- und Plugin-Dateien an. Verwenden Sie die von Wordfence bereitgestellte Option, um zu sehen, was sich zwischen der Originaldatei und Ihrer Datei geändert hat. Wenn die Änderungen bösartig aussehen, verwenden Sie die Wordfence-Option, um die Datei zu reparieren.
12. Arbeiten Sie sich langsam durch die Liste, bis sie leer ist.
13. Führen Sie einen weiteren Scan durch und bestätigen Sie, dass Ihre Website sauber ist.

anmelden, Wenn Sie weiterhin Hilfe benötigen, können Sie sich bei Wordfence Care um während der regulären Geschäftszeiten Hilfe zu erhalten, oder bei Wordfence Response , wenn Sie einen 24-Stunden-Service mit einer Reaktionszeit von 1 Stunde wünschen.

Ich habe eine Datei, die verdächtig aussieht, bin mir aber nicht sicher, ob sie es ist. Wie kann ich sagen?

Schicken Sie es uns per E-Mail an Samples@wordfence.com und wir informieren Sie. Wenn Ihre WordPress-Konfigurationsdatei

wp-config.php infiziert ist, senden Sie keine Kopie dieser Datei an uns, ohne zuvor Ihre Datenbankanmeldeinformationen und die eindeutigen Authentifizierungsschlüssel und -salze zu entfernen.

Wenn Sie keine Antwort erhalten, hat entweder Ihr oder unseres E-Mail-System die Nachricht aufgrund Ihres Anhangs möglicherweise verworfen und geglaubt, sie sei bösartig. Senden Sie uns also bitte eine E-Mail ohne Anhang und teilen Sie uns damit mit, dass Sie uns etwas zusenden möchten. Wir werden dann mit Ihnen zusammenarbeiten, um die Probe zu erhalten.

Wo finde ich Hilfe bei der Beseitigung einer bestimmten Art von Infektion?

Das Wordfence Learning Center bietet eine Reihe hilfreicher Artikel. Hier ist eine Liste von Artikeln, die Ihnen bei bestimmten Infektionsarten helfen:

- Entfernen bösartiger Weiterleitungen von Ihrer Website
- Hintertüren finden und entfernen
- Entfernen von Spam-Seiten von WordPress-Sites
- Spam-Links finden und entfernen
- Entfernen von Phishing-Seiten von WordPress-Sites
- Entfernen bösartiger Mailer-Codes von Ihrer Website
- Schädliche Datei-Uploader finden und entfernen
- Entfernung von WordPress-Defacement-Seiten
- So entfernen Sie verdächtigen Code von WordPress-Sites

Ich habe meine gehackte WordPress-

Site bereinigt, aber Google Chrome zeigt mir immer noch die Malware-Warnung an. Was soll ich machen?

Sie müssen Ihre Website aus der Google Safe Browsing-Liste entfernen lassen. Dazu müssen Sie eine Bewertung bei Google anfordern. finden Sie auf dieser Seite in der Google-Dokumentation . Detaillierte Schritte dazu.

Besucher meiner Website erhalten Warnungen von anderen Sicherheitsprodukten und Antivirensystemen. Was soll ich machen?

Der Verzicht auf die Google Safe Browsing-Liste ist ein großer Schritt, aber möglicherweise liegt noch einiges an Arbeit vor Ihnen. Sie müssen eine Liste aller Antivirenprodukte führen, die melden, dass Ihre Website infiziert ist. Dazu können Produkte wie ESET Antivirus, McAfee's Web Advisor und andere gehören.

Besuchen Sie die Website jedes Antiviren-Herstellers und finden Sie dort Anweisungen zum Entfernen Ihrer Website aus der Liste gefährlicher Websites. Dies wird von Antiviren-Herstellern oft als „Whitelisting" bezeichnet. Wenn Sie also nach Begriffen wie „Whitelisting", „Website-Entfernung", „False Positive" und dem Produktnamen googeln, gelangen Sie normalerweise zu der Stelle, an der Sie Ihre Website entfernen lassen können.

Wie kann ich manuell überprüfen, ob meine Website in der Safe Browsing-Liste von Google aufgeführt ist?

Besuchen Sie die folgende URL und ersetzen Sie example.com durch Ihre eigene Site-Adresse.

https://transparencyreport.google.com/safe-browsing/search?url=https://example.com/

Sie können ein Unterverzeichnis hinzufügen, wenn Ihre Site über eines verfügt. Die angezeigte Seite ist sehr einfach, enthält jedoch detaillierte Informationen zum aktuellen Status Ihrer Website, warum sie in der Liste der sicheren Browser von Google aufgeführt ist und was als Nächstes zu tun ist.

Was tun, wenn Ihre Website sauber ist:

Glückwunsch!! Öffnen Sie auf jeden Fall Ihr Lieblingsgetränk und nehmen Sie einen großen Schluck! Jetzt müssen Sie sicherstellen, dass Ihre Website nicht erneut gehackt wird. Hier ist wie:

- Installieren Sie Wordfence und führen Sie regelmäßige Scans auf Ihrer WordPress-Site durch.
- Stellen Sie sicher, dass WordPress und alle Plugins und Themes auf dem neuesten Stand sind. Dies ist das Wichtigste, was Sie tun können, um Ihre Website zu sichern.
- Stellen Sie sicher, dass Sie sichere Passwörter

verwenden, die schwer zu erraten sind.

- Aktivieren Sie die Zwei-Faktor-Authentifizierung. Wordfence bietet dies, sogar in unserer kostenlosen Version!
- Befreien Sie sich von allen alten WordPress-Installationen, die auf Ihrem Server herumliegen.
- Melden Sie sich für unsere WordPress-Sicherheitsmailingliste an , um über wichtige Sicherheitsupdates im Zusammenhang mit WordPress benachrichtigt zu werden. Dies ist eine E-Mail-Liste mit geringem Datenverkehr und hohem Signal-Rausch-Verhältnis, die sich auf die WordPress-Sicherheit konzentriert.
- Verbinden Sie Ihre Site mit Wordfence Central, um die Verwaltung der Sicherheit Ihrer Site erheblich zu vereinfachen. Mit Central können Sie mit einem Klick einen Scan auf allen Ihren WordPress-Sites auslösen und die Sicherheitskonfiguration auf allen Ihren WordPress-Sites einfach verwalten. Ein effektives Konfigurationsmanagement ist eine äußerst effektive Möglichkeit, eine gehackte Website zu verhindern.

Vielen Dank, dass Sie dies gelesen haben, und ich hoffe, es hat Ihnen geholfen. auf Twitter markieren Wenn nicht, können Sie @wordfence oder mich direkt mit @mmaunder markieren .

Bleiben Sie gesund und munter!!

Mark Maunder – Gründer von Wordfence und CEO von Defiant Inc.

WordPress – SICHERHEIT – Experten Tipps

WordPress absichern wie ein Profi – Der komplette Guide

Wie Du WordPress absichern kannst wie ein Profi | Experten Tipps

WordPress absichern 2022 ✔ Professionelle Tipps zur echten WordPress Sicherheit vom Experten ✔ Schritt für Schritt Aktualisiert: 17.05.2023

Es kursieren sehr viele gut gemeinte Tipps im Netz, wie man WordPress absichern kann. Viele von ihnen taugen leider nicht viel. Denn echte WordPress Sicherheit gibt es nicht mit der einfachen Installation eines Plugins. Es ist ein Konzept von Maßnahmen, die aufeinander aufbauen. In diesem Beitrag zeige

ich Dir, wie Du Dein WordPress bombensicher machst.

Inhaltsverzeichnis Anzeigen

Wenn Dir wirklich etwas an der WordPress Sicherheit liegt, dann solltest Du alle existierenden Sicherheitslücken schließen. Das kannst Du jedoch nur, wenn Dir bewusst ist, über welche Wege Dein WordPress angegriffen werden kann.

Erst dann leuchten die Maßnahmen ein und erst dann wird Dir bewusst, dass es keine Sicherheit mittels Plugin-Installation geben kann. Als **langjährige Experten** in der WordPress Sicherheit geben wir Dir heute Hintergrundwissen und eine Anleitung zur Absicherung Deines WordPress. Übrigens: Bis heute wurde keine Website gehackt, die wir abgesichert haben.

Dieses Tutorial ist nur für fortgeschrittene Anwender gedacht und **nicht für Anfänger**. Du musst Dich auskennen mit FTP und der functions.php.

Auch interessant:

Cloud Sicherheit – Wie Du Dropbox und Co absichern kannst

WordPress Sicherheitslücken

Klären wir doch mal die wichtige Frage, über welche Wege WordPress überwiegend gehackt wird (und gehackt werden kann).

1. **Sehr leicht zu merkende und viel zu kurze Passwörter** (!)
2. **Veraltete WordPress-Versionen** – Mit jeder neuen Version werden die Sicherheitslücken der alten bekannt
3. **Veraltete Plugin-Versionen** – Auch Plugins haben eklatante Sicherheitslücken.
4. **Brute-Force Angriffe** gegen den Admin-Zugang
5. **Brute-Force Angriffe** gegen die xmlrpc.php Datei
6. **SQL-Injektionen** über Formulare
7. **Von außen zugängliche** WordPress-Dateien

8. Sicherheitslücke **WordPress REST-API (Update 26.05.2022)**

Zu 1: – WordPress Sicherheit fängt mit Deinem Passwort an

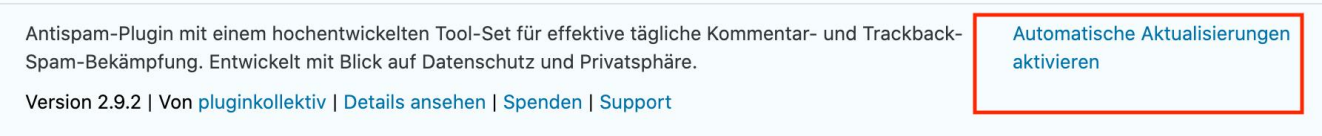
WordPress absichern ohne ein richtig gutes und wirklich sicheres Passwort hat leider überhaupt keinen Zweck. Alles, was leicht zu merken ist, ist auch leicht zu knacken. Und das wäre fatal. Deshalb sorge für ein anständiges Passwort aus Buchstaben, Zahlen, Sonderzeichen und Groß- und Kleinschreibung.

Ein gutes Passwort sollte schon 30stellig sein. Merken kann man sich das nicht mehr, aber es gibt ja Passwortmanager oder die entsprechenden Funktionen im Webbrowser.

Passwort-Generator aufrufen (externer Link)

Zu 2 + 3: – Die Updates

Das Du **WordPress und die Plugins aktuell halten** solltest und die Updates so schnell wie möglich ausführen solltest, hast Du bestimmt schon gelesen. Aber lesen bringt nichts. **Du musst es tun!** Ansonsten bettelst Du darum, gehackt zu werden. Zudem werden gern Plugins eingesetzt, die als beständig unsicher gelten – zum Beispiel der Revolution Slider. Übrigens kannst Du ab WordPress 5.5 Deine Plugins automatisch aktualisieren lassen.



Zu 4 + 5: – Brute-Force Angriffe

Hier versucht man mit der Brechstange Deine Zugangsdaten zu bekommen. Es werden zum Teil Tausende Variationen von Benutzernamen und Passwort ausprobiert. Diese Angriffe haben

immer wieder Erfolg, weil der Benutzername meistens Admin ist und das Passwort kurz und gut zu merken ist.

Gern wird auch ein Angriff gegen die xmlrpc.php Datei ausgeführt, die zum Beispiel dazu dient, Beiträge per E-Mail veröffentlichen zu können. Auch über diese Datei kann man einen Vollzugriff auf die Website bekommen.

Was ist ein Brute-Force Angriff? (externer Link)

Zu 6: – SQL-Injektionen über Formulare

In ungeschützte Formulare (und auch direkt in der Adresszeile des Browsers) wird gern versucht Schadcode einzubringen. Hat das Erfolg, werden die Besucher Deiner Seite bereits durch einen einfachen Aufruf der Website mit Viren und Trojanern verseucht. Du wirst es erst merken, wenn Dein Webhoster die Website abschaltet oder Google die Seite aus dem Index nimmt.

Was ist eine SQL-Injektion? (externer Link)

Zu 7: – Von außen zugängliche WordPress-Dateien

Nicht jeder Webhoster hat eine sichere Konfiguration seiner Hosting-Pakete oder Server. Manchmal sind WordPress-Dateien von außen zugänglich. Beliebte Angriffsziele sind hier zum Beispiel die install.php und die wp-config.php

Zu 8: – Die WordPress REST-API

Die REST-API bietet viele Möglichkeiten Inhalte auszulesen und diese können dann an externe Apps oder Websites übergeben werden. Dazu stellt die API strukturierte Daten (JSON) öffentlich zur Verfügung. Dazu gehören jedoch auch Daten, die man nicht gern für jedermann öffentlich abrufbar sehen möchte. Dazu solltet Ihr den vollständigen Artikel lesen, es gibt erstens noch viel mehr Informationen dazu und zweitens ein

umfangreicheres Code-Beispiel.

Als kleines Goodie habe ich Dir noch ein Plugin geschrieben, das Du im Artikel herunterladen kannst.

WordPress REST-API Sicherheitslücke deaktivieren

Ein Code-Beispiel, das die REST-API für externe Besucher abschaltet

```
<?php
/* Ab hier kopieren */
/**
 * REST-API fuer extere User abschalten
 */
add_filter('rest_authentication_errors', function($result) {
if ( ! is_user_logged_in() ) {
return new WP_Error( 'rest_API_cannot_access', array( 'status'
=> rest_authorization_required_code() ) );
}
return $result;
});
```

PHP

Copy

WordPress absichern. Echte WordPress Sicherheit!

Du solltest die folgenden Arbeiten immer mit einem **FTP-Zugang** erledigen, niemals in den Editoren von WordPress. Diese gehören abgeschaltet, weil sie ein extremes Sicherheitsrisiko darstellen.

Wie das geht, erfährst Du weiter unten.

Die Snippets sind geeignet für:

- **WordPress-Version:** Ab 4.5 – inklusive 5.5.xx

- **PHP-Version:** inkl. PHP 7.4.xx

Am Ende dieses Artikels hast Du alle Sicherheitslücken geschlossen und kannst dich an einer sicheren Website erfreuen. Als spezialisierte SEO Agentur wissen wir, wovon wir sprechen. Wir führen Dich Schritt für Schritt durch die einzelnen Punkte.

Die Basis der Sicherheit. Eine perfekte .htaccess Datei

Seit mittlerweile 9 Jahren entwickle ich eine .htaccess Datei und habe sie jedes Jahr stets verbessert und überarbeitet. Sie ist die Grundlage einer guten Sicherheitsstrategie und sorgt zudem noch für einen enormen Performance-Schub für Dein WordPress.

Folgendes wird abgesichert:

- Alle wichtigen WordPress-Dateien und Ordner gegen Zugriff von außen
- Dank ausgeklügelter Firewall Schutz vor SQL-Injektionen
- Schutz gegen die Ausnutzung von eventuellen Sicherheitslücken in Plugins
- Schutz gegen die Einschleusung von Schadsoftware jeder Art
- Schutz gegen Brute-Force Angriffe auf Uploads-Ziele
- Setzt HTTP-Response Header für Browser-Sicherheit
- Sperrt die xmlrpc.php Datei gegen jeden Zugriff

Den Adminbereich von WordPress absichern

Der Adminbereich ist das Herz Deiner Website und sollte so sicher wie nur möglich sein. Das erreichen wir durch drei wichtige Schritte. Alle drei Maßnahmen sorgen dafür, dass sich Hacker die Zähne ausbeissen und keine Chance mehr haben, über

diesen Weg in Deine Website einzudringen.

1

Teil 1: Eine zusätzliche Passwortabfrage – HTTP Authentifikation

Eine HTTP Authentifikation ist eine sehr wirkungsvolle Sache. Bevor man nicht die korrekten Zugangsdaten eingegeben hat, kommt man nicht an den Adminbereich von WordPress und kann sich demzufolge auch nicht einloggen. Diese zusätzliche Passwortabfrage ist schnell eingerichtet.

Du benötigst dafür **einen FTP-Zugang** zu Deinem Webhosting und ein **FTP-Programm** wie zum Beispiel FileZilla.

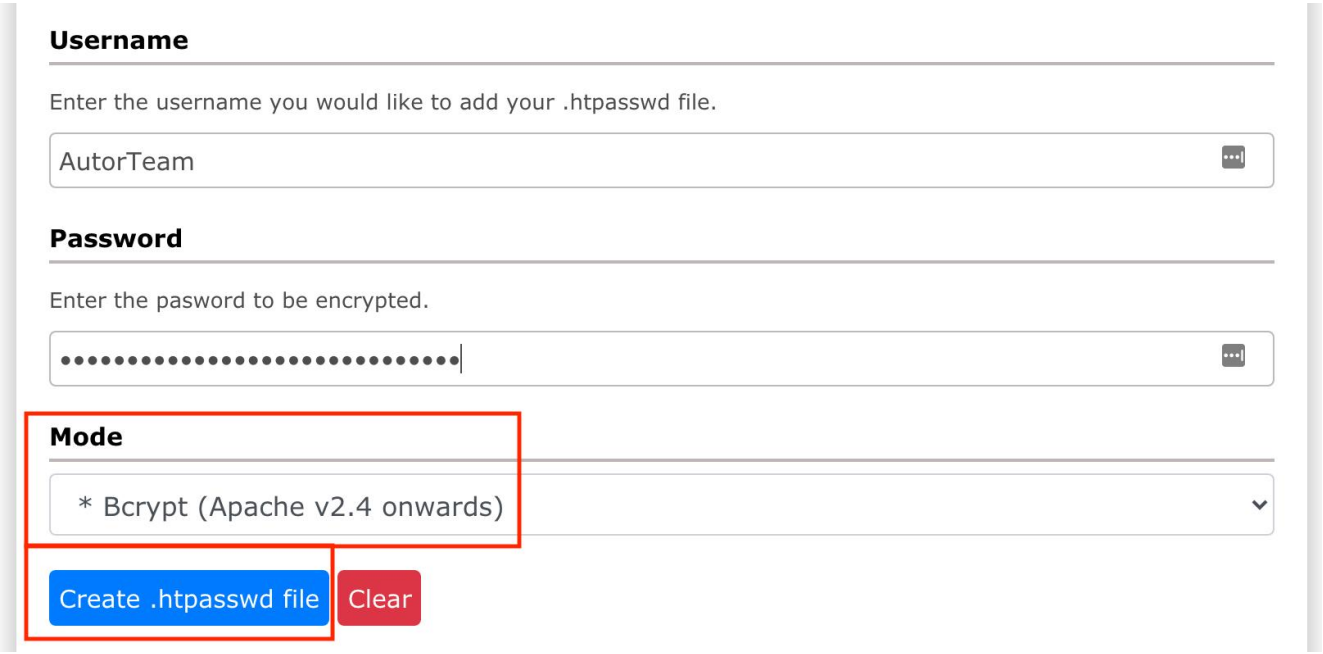
.htpasswd erstellen

Um diese Abfrage einzurichten benötigst Du erstens die obige .htaccess Datei und eine Datei namens .htpasswd, die Du erstellen musst. Beide Dateien sind versteckte – oder Systemdateien – die normalerweise nicht angezeigt werden. Du musst die Anzeige von versteckten Dateien also aktivieren.

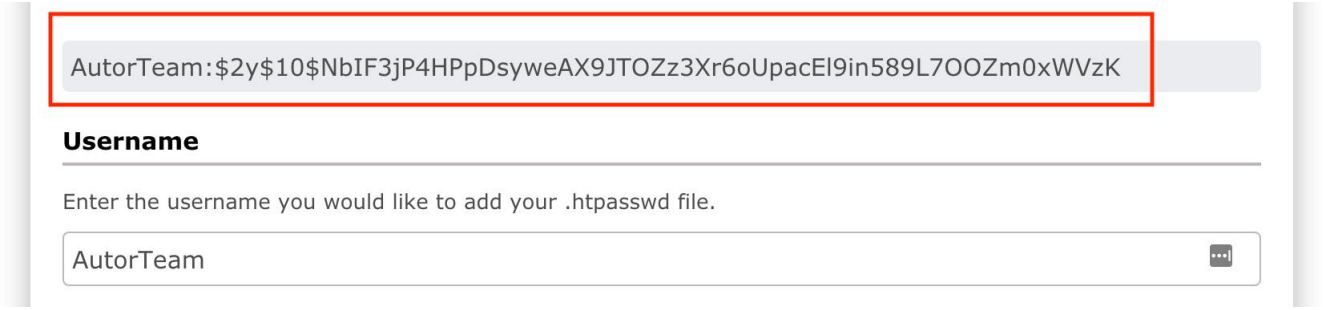
Lege nun mit dem Editor von Windows oder TextEdit von macOS eine reine Textdatei mit dem Namen .htpasswd an.

Erzeuge jetzt mit dem Passwort-Generator ein sicheres Passwort. Es sollte mindestens 25stellig sein. Notiere Dir das Passwort und rufe jetzt den .htpasswd Generator auf. Gib einen Benutzernamen Deiner Wahl ein und das soeben generierte Passwort.

Stelle bei »Mode« **Bcrypt** ein. Siehe Screenshot. Das sorgt für eine ziemlich gute Verschlüsselung des Passworts. Danach klicke auf den blauen Button.



Die dadurch erstellten Zugangsdaten findest Du oberhalb von Username.



Kopiere diese Zeile und füge sie in Deine .htpasswd Datei ein. Speichere die Datei ab und lade sie mit dem FTP-Programm in das Hauptverzeichnis von WordPress.

Jetzt muss der korrekte und vollständige Server-Pfad zur .htpasswd ermittelt werden.

Server-Pfad ermitteln

Um den vollständigen Server-Pfad zur Datei zu ermitteln, nutzen wir eine kleine PHP-Datei. Erstelle mit einem Text-Editor eine Datei namens dir.php und kopiere folgendes hinein:

```
<?php
$dir = dirname(__FILE__);
echo "<p>Der vollständige Pfad zur .htpasswd Datei in diesem Verzeichnis: " . $dir . "/.htpasswd" . "</p>";
```

PHP

Copy

Lade diese Datei nun in das Hauptverzeichnis von WordPress und rufe die Datei im Browser auf:

https://deine-website.de/dir.php

HTTP

Copy

Kopiere den angezeigten Pfad und notiere Ihn. Er sieht so aus:

/usr/local/www/apache24/noexec/deinewebseite/.htpasswd

HTTP

Copy

Dieser Pfad muss nun in die .htaccess eingetragen werden. Wenn Du meine Datei nutzt, ist der betreffende Block relativ weit unten zu finden. Du musst vor dem Code die Rauten # entfernen, um ihn nutzen zu können.

So muss es nachher aussehen:

```
# ----------------------------------------------------------
----------
#   Protect your WordPress Login with HTTP Authentification
# ----------------------------------------------------------
----------

# If you want to use it, comment it out and set your path to
.htpasswd
<Files wp-login.php>
 AuthName "Admin-Bereich"
 AuthType Basic
                                                AuthUserFile
/usr/local/www/apache24/noexec/deinewebseite/.htpasswd
 require valid-user
</Files>
```

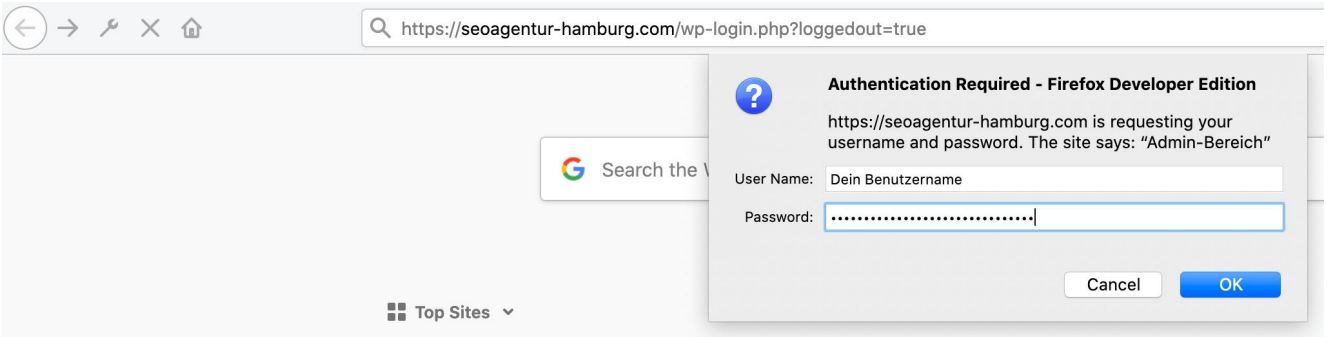
Apache Configuration

Copy

WICHTIG: Lösche jetzt die dir.php wieder vom Server. Sie stellt ein Sicherheitsrisiko dar.

Lade jetzt die .htaccess Datei wieder auf Deinen Server hoch. Jetzt sollten sich beide Dateien (.htaccess und .htpasswd) im Hauptverzeichnis von WordPress befinden.

Wenn Du jetzt Deinen Adminbereich aufrufst – egal ob mit wp-login.php oder wp-admin – kommt die folgende Passwortabfrage:



Übrigens musst Du die Zugangsdaten nur einmal eingeben, danach befindet sich die Abfrage im Browser-Cache. Erst wenn dieser gelöscht wird, kommt die Abfrage erneut.

2

Teil 2: WordPress absichern: Zugang nur noch mit E-Mail-Adresse

Ein kleines Code-Snippet mit großer Wirkung. Hacker probieren allen möglichen und unmöglichen Benutzernamen aus, bevorzugt natürlich »Admin«, weil er so weit verbreitet ist. Hat ein Hacker Deinen Benutzernamen, braucht er nur noch Dein Passwort.

Daher sorgen wir dafür, dass er garantiert nicht Deinen Benutzernamen bekommt. Weil es ihn nicht mehr gibt. Denn statt dem Benutzernamen kannst Du Dich nur noch mit Deiner E-Mail-

Adresse und dem Passwort einloggen.

Kopiere den folgenden Code in die functions.php Deines (Child-) Themes. Du kannst für die Snippets auch ein eigenes Plugin anlegen.

```
<?php

// Ab hier kopieren

/**
 * Sicherheit: Anmeldung nur noch mit E-Mail-Adresse, anstatt Benutzernamen
 *
 * @author Andreas Hecht
 */

//WordPress Authentifikation löschen
remove_filter('authenticate', 'wp_authenticate_username_password', 20);

// Neue Authentifikation setzen - Anmelden nur mit E-Mail und Passwort
add_filter('authenticate', function($user, $email, $password){

    //Check for empty fields
        if(empty($email) || empty ($password)){
            //create new error object and add errors to it.
            $error = new WP_Error();

            if(empty($email)){ //No email
                        $error->add('empty_username', __('<strong>FEHLER</strong>: Das E-Mail Feld ist leer.'));
            }
                        else  if(!filter_var($email, FILTER_VALIDATE_EMAIL)){ //Invalid Email
                    $error->add('invalid_username', __('<strong>FEHLER</strong>:  Die  E-Mail-Adresse  ist ungültig'));
            }
```

```
            if(empty($password)){ //No password
                        $error->add('empty_password',
__('<strong>FEHLER</strong>: Das Passwort-Feld ist leer.'));
            }

            return $error;
        }

        //Check if user exists in WordPress database
        $user = get_user_by('email', $email);

        //bad email
        if(!$user){
            $error = new WP_Error();
                                $error->add('invalid',
__('<strong>FEHLER</strong>: Deine Eingaben sind ungültig.'));
            return $error;
        }
        else{ //check password
            if(!wp_check_password($password, $user->user_pass,
$user->ID)){ //bad password
                $error = new WP_Error();
                                $error->add('invalid',
__('<strong>FEHLER</strong>: Deine Eingaben sind ungültig.'));
                return $error;
            }else{
                return $user; //passed
            }
        }
}, 20, 3);
```

PHP

Copy

3

Teil 3: Redirect auf Google nach

falscher Eingabe der Zugangsdaten

Mit diesem Code-Snippet wirst Du garantiert jeden Hacker verblüffen, der es doch bis zum Adminbereich geschafft hat. Einmal die Zugangsdaten falsch eingegeben, und schon ist Google Dein bester Freund.

```
<?php

// Ab hier kopieren
if ( ! function_exists( 'ah_redirect_after_login_errors' ) ) :
/**
 * Redirect auf Google nach falscher Eingabe der WP-Zugangsdaten
 */
function ah_redirect_after_login_errors() {
  wp_redirect( 'https://www.google.de' );
  exit;
}
add_filter( 'login_errors', 'ah_redirect_after_login_errors' );
endif;
```

PHP

Copy

WordPress absichern mit den richtigen Einstellungen für die wp-config.php

Die wp-config.php Datei an sich haben wir ja schon mit der .htaccess abgesichert. Jetzt kommen noch wichtige Einstellungen in diese WordPress-Steuerungsdatei hinein.

Der korrekte Platz für unsere Eintragungen ist **oberhalb** der define('WP_DEBUG', false); Konstante.

Nutze die Sicherheitsschlüssel!

Die Sicherheitsschlüssel sorgen für eine Verschlüsselung Deiner Zugangsdaten während des Logins. Nutzt Du keine, werden die Zugangsdaten unverschlüsselt übertragen.

```
<?php


/**#@+
 * Sicherheitsschlüssel
 *
 * Ändere jeden untenstehenden Platzhaltertext in eine beliebige,
 * möglichst einmalig genutzte Zeichenkette.
 * Auf der Seite {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * kannst du dir alle Schlüssel generieren lassen.
 * Du kannst die Schlüssel jederzeit wieder ändern, alle angemeldeten
 * Benutzer müssen sich danach erneut anmelden.
 *
 * @since 2.6.0
 */
define('AUTH_KEY',                                ')tr/o>x!>CD+@VV4EH}TAmm+i[!]f4|r.>K@MCo/,wDkBq^`c_0t9>fkgPnO?;g');
define('SECURE_AUTH_KEY',
'Zw!x0qEni%?OdHHs*s[kRF3ULD~xw*iCWO9F6oyzdL}}8%e2>+{Cd@a~`2>wQ-S|');
define('LOGGED_IN_KEY',
'W<De;xTff~PE?^xXlE{vkN{O$mOlSIz`4za`cYk/;-<<&/hC>a.Q1!k`mK>HE6bQ');
define('NONCE_KEY',                        'qH_9<.w&fC6$YON~WK`zge#iuc3~<WPLD5nF;Bdl8:+G)2+s_vzk&bVC79C2>?b');
define('AUTH_SALT',
'X*2OOu?q)JhQ3=NUumf[(I^u?|sH|>vY?r^:XPJLW+w7JCYeakqAjtjnI{_h~1a');
define('SECURE_AUTH_SALT',
'0wyeDI|N[]8}U<m[>g{]MhVA@WA|*<h}=j9i2vM)3m%`a/gtVSoH7>mb|cN2VL/');
```

```
define('LOGGED_IN_SALT',                'U]y/VEz<pP$-
+r0Iv^.CGBSh$.zI;~HSp:p0xtb9YMN%46${^F>?Bd!xrm$y}^bq');
define('NONCE_SALT',                '-|~?0 Hs%`,Ce$d+Oo#.mw
D5MW<7aI`Of]:gkp`r6S}tJfumjn2jvQsJqz-vgvM');
```

PHP

Copy

Die folgende Website generiert Dir die Schlüssel:

https://api.wordpress.org/secret-key/1.1/salt/

2

Schalte die Editoren für Theme und Plugins ab

> *In jeder WordPress-Installation kann man Theme- und Plugin-Dateien direkt im Adminbereich bearbeiten. Unter den Menüpunkten »Design« und »Plugins« findet man auch jeweils den Editor für die betreffenden Dateien. Dieser Editor ist sehr gefährlich, wenn er in die Hände eines Hackers gerät.*

```
<?php


/**
 *
 * Files Editoren abschalten
 *
 */
define('DISALLOW_FILE_EDIT', true);
```

PHP

Copy

3

Login in den Adminbereich nur über HTTPS

Sollte selbsterklärend sein. Wenn Deine Website HTTPS nutzt, sollte auch kein HTTP-Login in den Adminbereich möglich sein.

```
<?php

// Forciere das Anmelden mit SSL
define('FORCE_SSL_LOGIN', true);

// Adminbereich nur Nutzbar mit SSL
define('FORCE_SSL_ADMIN', true);
```

PHP

Copy

4

Datenübertragung nur mit FTPS

Die Datenübertragung von Deinem Rechner zum FTP-Zugang Deiner Website sollte ausschliesslich mit FTPS erfolgen. Tut es das nicht, werden Deine Zugangsdaten unverschlüsselt an den Server übertragen. Das wäre ein enormes Sicherheitsrisiko.

```
<?php

//FTP nur über SSL
define('FTP_SSL', true);
```

PHP

Copy

Extra: Du hast einen Blog mit mehreren

Autoren?

Dann solltest du Deine Autoren daran hindern, einfache Passwörter zu verwenden. Hier kommt ein Code-Snippet, dass Deine Autoren daran hindert, ihre Passwörter zu ändern.

```
<?php

//Ab hier kopieren
/**
 * Sicherheit: User davon abhalten, ihre Passwörter zu ändern
 *
 * @author Andreas Hecht
 */
class Password_Reset_Removed
{

  function __construct()
  {
      add_filter( 'show_password_fields', array( $this, 'disable' ) );
      add_filter( 'allow_password_reset', array( $this, 'disable' ) );
  }

  function disable()
  {
    if ( is_admin() ) {
      $userdata = wp_get_current_user();
      $user = new WP_User($userdata->ID);
      if ( !empty( $user->roles ) && is_array( $user->roles ) && $user->roles[0] == 'administrator' )
        return true;
    }
    return false;
  }

}

$pass_reset_removed = new Password_Reset_Removed();
```

PHP

Copy

Entfernen der XML-RPC Schnittstelle aus dem HTML-Header der Website

Die gefährliche Datei xmlrpc.php haben wir ja bereits mit der .htaccess Datei gesperrt, jetzt entfernen wir diese Schnittstelle noch aus dem HTTP-Response Header. Der Code kommt in die functions.php.

```
<?php

//Ab hier kopieren
if ( ! function_exists( 'AH_remove_x_pingback' ) ) :
/**
 * Entfernen der XML-RPC Schnittstelle aus dem HTML-Header der Website
 */

 function AH_remove_x_pingback( $headers )
 {
 unset( $headers['X-Pingback'] );
 return $headers;
 }
add_filter( 'wp_headers', 'AH_remove_x_pingback' );
endif;
```

PHP

Copy

Kleines FAQ zur WordPress

Sicherheit

Bringt es was, wenn ich die wp-config.php verschiebe?

Nein. Außer das Du Deine Website fehleranfälliger gemacht hast nicht. Hacker finden die Datei, auch wenn Du sie verschiebst. Das bringt absolut nichts.

Was bringen Sicherheitsplugins wie WordFence, Sucuri etc.

Absolut nichts. Sie gaukeln Dir eine Sicherheit vor, die sie nicht erfüllen können. Diese Plugins versprechen Sicherheit, weil sie Deine WP-, Theme- und Plugin-Dateien auf Schadsoftware scannen. Wenn Du gehackt wurdest, manipuliert der Hacker zuerst diese Plugins. Denn er will ja, dass der Hack möglichst lange unentdeckt bleibt. Zudem sorgen diese Plugins noch dafür, dass Deine Website deutlich langsamer wird. Wenn Du Sicherheit willst, dieser Artikel ist die Anleitung dazu.

Ich brauche keine WordPress Absicherung. Ich habe Limit Login Attemps!

Klasse. Ehrlich. Einen Hacker im ersten Lehrjahr kannst Du damit erschrecken. Profis werden vor Lachen auf dem Fußboden liegen. Warum? Das Plugin limitiert die Loginversuche von EINER bestimmten IP-Adresse. Profis hingegen greifen Dich mit einem Botnetz an. Da prasseln dann Tausende von Anfragen an Deinen Adminbereich von Tausenden von IP-Adressen ein. Wenn von jeder IP nur ein Hackversuch kommt, kann das Plugin nichts stoppen. Im Grunde ist es vollkommen wirkungslos.

Soll ich explizite Dateiberechtigungen auf dem Server setzen?

Hmm, kannst Du schon machen. Aber ob das wirklich praktikabel ist, ist die zweite Sache. Ab und an brauchen Plugins bestimmte Berechtigungen, um zu funktionieren. Auch Updates müssen ohne Probleme laufen. Natürlich kann man sagen, dass man durch Dateiberechtigungen die Manipulation der Dateien von Außen unterbindet.

Im Prinzip wäre das nützlich. Aber Du hast durch meine .htaccess ja schon den Zugriff auf die wichtigsten Dateien gesperrt. Wenn ich auf die Dateien nicht zugreifen kann, kann ich sie auch nicht manipulieren.

WordPress absichern durch das Abändern des Benutzernamens?

Auch erfahrene WordPress Webworker wie Perun empfehlen Dir, den Standard »Administrator« oder »Admin« in einen anderen Benutzernamen abzuändern. Manche gehen einen Schritt weiter und empfehlen Dir, den ersten Admin zu löschen und vorher einen weiteren Admin mit eigenem Benutzernamen anzulegen, um die #ID 1 gegen eine #ID 2 auszutauschen.

Kann dieser Tipp meine Website sicherer machen?

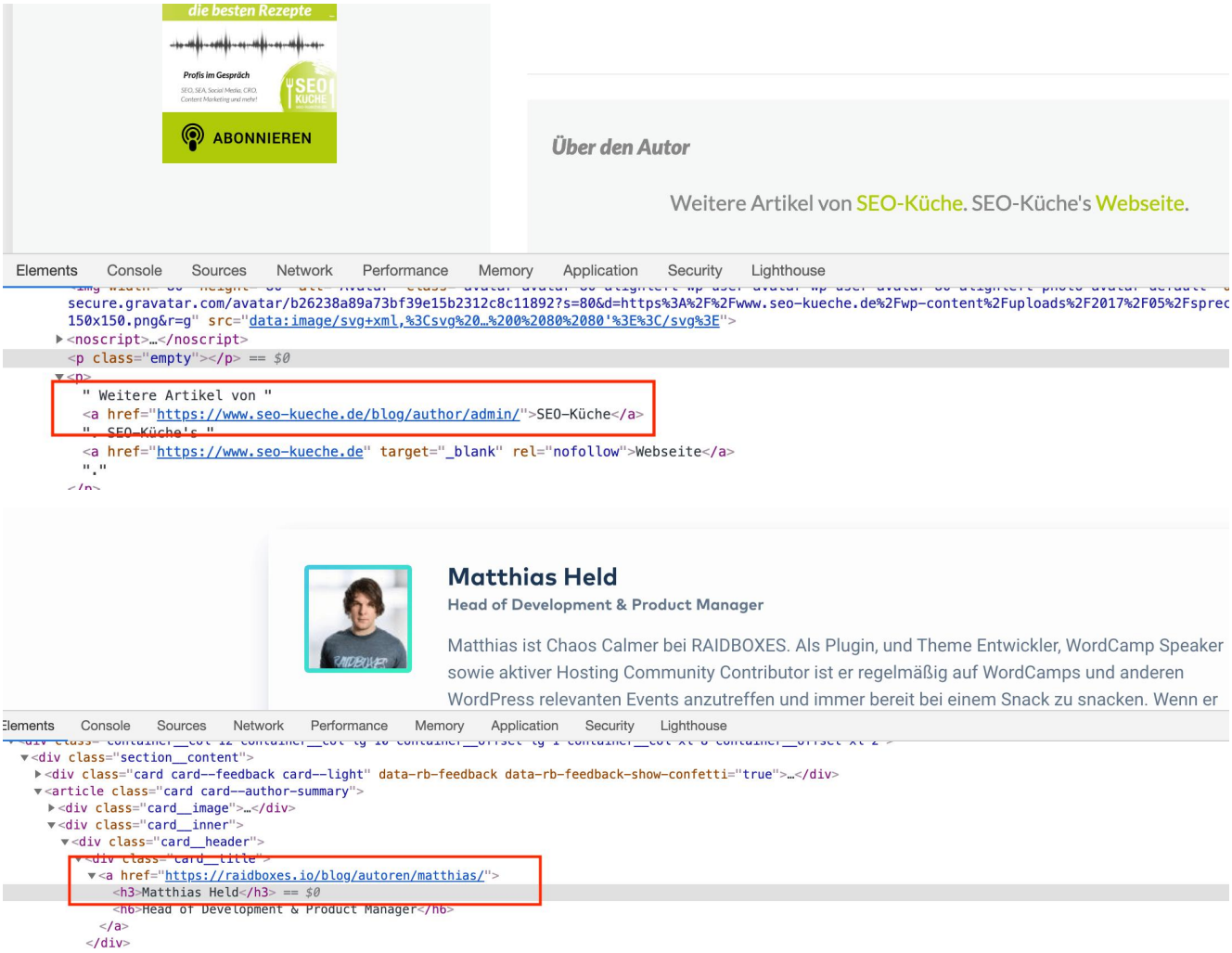
Nein. Der Tipp zeugt von absolut fehlender Sachkenntnis oder von nicht durchdachter Problemstellung. Der Benutzername des Administrators kann innerhalb von Sekunden herausgefunden werden.

Denn jede Autor-Box unter den Beiträgen und jedes Autoren-Archiv in WordPress gibt den Benutzernamen preis. Solltest Du also mit einem Admin-Account Beiträge schreiben, geben alle zwei Möglichkeiten Deinen Admin-Benutzernamen preis.

Wenn alles nichts bringt, kann der Benutzername auch im

Quelltext der Kommentare gefunden werden. Ups…

Zwei Beispiele:



https://gist.github.com/seoagentur-hamburg/c96bc796764baaa64d43b70731013f8a#file-htaccess

eine automatische Aktualisierung durchführen

„wp-config-php“ lässt sich durch den Eintrag

```
define( ‚WP_AUTO_UPDATE_CORE‘, true );
```

Plugins automatisch aktualisieren

```
add_filter( 'auto_update_plugin', '__return_true' );
```

Themes automatisch aktualisieren

```
add_filter( 'auto_update_theme', '__return_true' );
```

Du bist auf der Suche nach einer seriösen SEO Agentur?

Dir hat unser Artikel gefallen und Du möchtest unsere Hilfe in Anspruch nehmen? Dann melde dich bei unverbindlich bei uns. Wir freuen uns auf Deine Anfrage!

+49 40 – 209 659 47info@seoagentur-hamburg.com

Jetzt weitere interessante Beiträge lesen

WordPress

Google Fonts Download: Den Google Font lokal laden

vor 1 Jahr

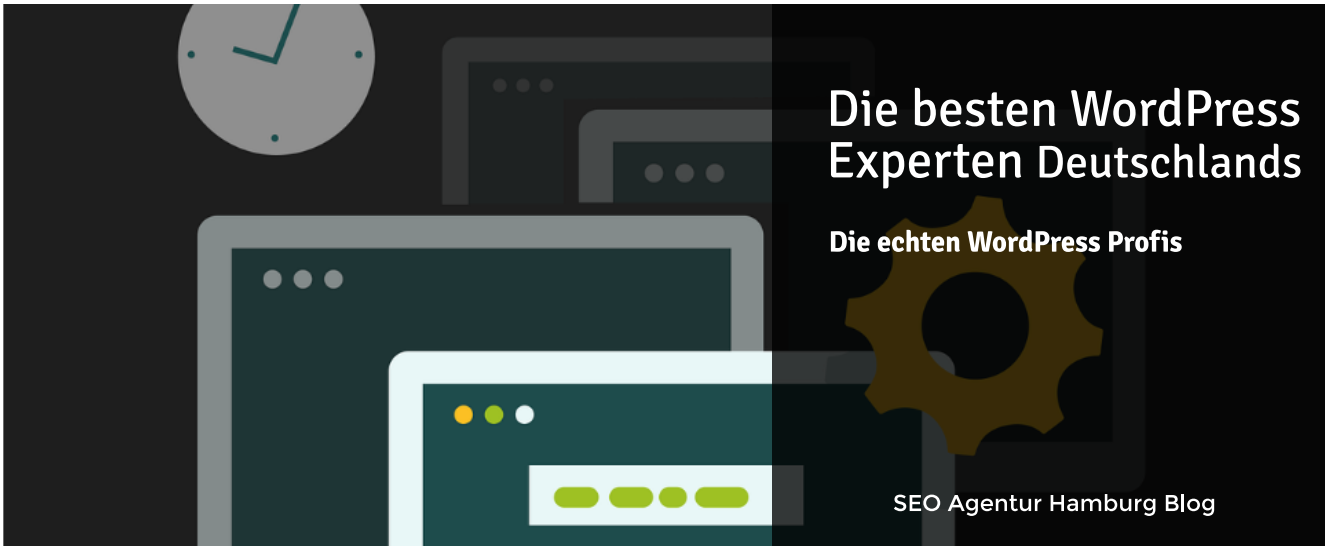
Google Schriften zu verwenden ist sehr beliebt. Doch ein Google Font verursacht erhebliche DSGVO Probleme, da Daten in die USA…

WordPress

Wie Du ein WordPress Child Theme erstellen kannst für Anfänger

vor 3 Jahren

Um zu vermeiden, dass ein Theme-Update eigene Änderungen überschreibt, lohnt es sich, ein WordPress-Child-Theme zu erstellen. Denn ein Child Theme…



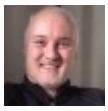
WordPress

Die 10 besten WordPress Spezialisten Deutschlands?

vor 4 Jahren

Ich wurde vor einiger Zeit im Rahmen einer Spezialistenempfehlung als einer der zehn besten WordPress Spezialisten Deutschlands von der Website…

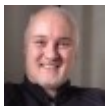
39 Kommentare. Hinterlasse eine Antwort

- Markus16. Februar 2023 10:34 Hallo Andreas, nochmals herzlichen Dank für diese vielen Infos hier.
  Ich habe festgestellt, dass nach Entfernen der XML-RPC Schnittstelle aus dem HTML-Header der Website die Seite nicht mehr erreichbar ist. Als ich den Eintrag aus der wp-config entfernt hatte, lief es wieder. Kennst du das Phänomen bzw. hast du eine Idee, woran es liegen könnte?
  Antworten
  -  Andreas Hecht16. Februar 2023 14:32 Hi Markus,ich habe im Artikel nichts davon geschrieben, dass der Code zum Entfernen der XML-RPC Schnittstelle in die wp-config.php hinein soll. Lesen hilft in solchen Fällen ungemein.
    Antworten

- Isa1. Februar 2023 19:39 Hallo Andreas,
  Danke für diese Anleitung. Ich habe diese umgesetzt und alles Funktioniert bis auf eine Kleinigkeit: Ich benutze deine htaccess Datei und habe anschließend die zusätzliche Passwortabfrage (HTTP Authentifikation) mit reingenommen. Sobald ich mich anmelde komme ich rein,

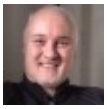
allerdings sobald ich den Browser neustarte muss ich die Daten erneut eingeben (die Login Daten speichern sich anscheinend nicht im Cache ab. Kann es sein das es was mit der htaccess Datei zu tun hat, da diese ja den Cache komprimiert? Den Cache vom Browser löschen hat nichts gebracht. Übrigens nutze ich All-Inkl als Hoster. Ich finde den Fehler nicht. Hast du da einen Tipp? Antworten

-  Andreas Hecht1. Februar 2023 20:43 Hi Isa,das hört sich für mich an, als ob der Cache des Browsers beim beenden geleert wird. Antworten
  -  Isa4. Februar 2023 9:40 Danke für die Schnelle Antwort. Allerdings ist es nicht nur auf einem Gerät und Browser so sondern bei allen die ich jetzt ausprobiert habe. Eine Lösung habe ich dazu noch nicht gefunden. Antworten

-  Frank19. September 2022 1:09 Toller Artikel! Funktionieren die Snippets auch mit WordPress 6.0.2. ? Antworten
  -  Andreas Hecht25. September 2022 15:11 Hallo Frank,ja, das tun sie. Antworten

-  Frank16. September 2022 1:28 I’m Snippet „REST-API fuer extere User abschalten“ hat sich eine fehlerhafte Klammersetzung eingeschlichen.
„return $result;“ wird nie ausgeführt und der Filter

liefert demzufolge nichts zurück, wenn die Bedingung nicht zutrifft. Antworten

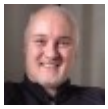
-  Andreas Hecht16. September 2022 14:27 Hi Frank,bei meinem Test wird genau das gewünschte Ergebnis erreicht. Was genau sollte da nicht funktionieren? Antworten

  -  Frank19. September 2022 23:54 Hallo Andreas,also wenn du zweimal hintereinander ein „return“ laufen lassen willst wie in deinem Beispiel oben, dann kann das 2. return doch nie erreicht werden, weil das erste return die gesamte Funktion verlässt und alles danach schlicht nicht mehr ausgeführt wird.Die Funktion macht formal in folgender Form weitaus mehr Sinn:

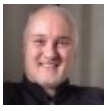
    ```
    add_filter('rest_authentication_errors', function($result) {
    if ( ! is_user_logged_in() ) {
    return new WP_Error( 'rest_API_cannot_access', array( 'status' => rest_authorization_required_code() ) );
    }
    return $result;
    });
    ```

    … und zwar darum, weil add_filter() sich von add_action() in WP dadurch unterscheidet, dass add_filter einen Wert entgegennimmt, ihn modifiziert (oder auch nicht) und dann wieder zurückgibt. Deine Funktion oben gibt aber praktisch immer dann gar nichts zurück, wenn die Bedingung nicht greift, also im konkreten Fall: wenn du eingeloggt bist. Ein

eingeloggter Benutzer wird daher NIE eine REST-Error zu sehen bekommen, auch dann nicht, wenn es einen gibt. Mag schon sein, dass dann alles funktional erscheint, aber wenn Fehler, die auftreten, nicht rückgemeldet werden, muss noch lange nicht alles in Ordnung sein …
Ich hoffe, das hilft. Die Klammer ist einfach verrutscht – keine große Sache. Antworten

-  Andreas Hecht25. September 2022 15:12 Hi Frank,okay, das hatte ich nicht bedacht. Danke für Deine Mühe, ich ändere das Snippet ab. Antworten

-  Joachim2. September 2022 10:21 Hallo Andreas, ich hoffe, du kannst mir helfen: Es geht um Teil 1, eine zusätzliche Passwortabfrage. Die Schritte habe ich alle ausgeführt und die Eingabemaske erscheint auch bei mir. Allerdings geht es nach der Eingabe der Zugangsdaten nicht weiter, sondern die Maske erscheint einfach erneut und es geht nicht weiter. Verhindert eventuell die Ninja-Firewall die Ausführung? Ich würde mich freuen, wenn du helfen kannst. Mein Hoster ist All-Inkl. Antworten

  -  Andreas Hecht2. September 2022 14:14 Hi Joachim,schalte mal diese Firewall komplett ab. Diesen Mist brauchst Du nicht mehr. Wenn es dann noch nicht funktioniert, stimmt etwas mit dem Pfad

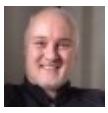
zur .htpasswd nicht. Antworten

-  Heiko26. Mai 2022 10:04 Hallo Andreas, diese Seite wurde am 25.05.2022 aktualisiert, hat sich inhaltlich was geändert? Bei der Gelegenheit möchte ich mal DANKE sagen für das Know-How, das du hier kostenlos mit uns teilst. Antworten
  -  Andreas Hecht26. Mai 2022 15:11 Hallo Heiko,ja, da ist die Absicherung der WordPress REST-API dazugekommen. Ich habe das heute noch einmal deutlicher herausgestellt. Antworten
    -  Heiko7. Juni 2022 15:09 Hallo Andreas, ich habe die Absicherung der REST-API ausprobiert, sowohl per Code als auch mit deinem Plugin. In beiden Fällen kann ich keine Beiträge mehr bearbeiten – es erscheint nur eine weiße Seite… Theme TwentyTwenty mit Twentig… Antworten
      -  Andreas Hecht7. Juni 2022 15:19 Hi Heiko,dann ist eines Deiner Plugins schlecht programmiert und benötigt die (komplette) Schnittstelle. Da kann man am Code nichts ändern. Antworten
        -  Frank21. September 2022 13:36 Doch, kann man. Man könnte den Fehler im Snippet beseitigen, so: https://www.kuketz-blog.de/wordpress-rest-api-unter-

wordpress-4-7-deaktivieren/ (https://www.kuketz-blog.de/wordpress-rest-api-unter-wordpress-4-7-deaktivieren/)Das Snippet kursiert in unzählige Male in falsch abgeschriebener Fassung im Netz, sogar beim Kulturbanausen. Auf dieser Seite einmal mehr.

-  Frank21. September 2022 13:28 Hi Heiko, ich würde das REST-Snippet einmal auf die folgende (richtige) Variante abändern und schauen, ob es damit geht (dennwenn du als authentifizierter Benutzer REST-Fehler hast, produziert das Snippet selbst Fehler, weil es keinen Rückgabewert hat):
https://www.kuketz-blog.de/wordpress-rest-api-unter-wordpress-4-7-deaktivieren/ (https://www.kuketz-blog.de/wordpress-rest-api-unter-wordpress-4-7-deaktivieren/)
Schöne Grüße! Antworten

-  Leon17. Mai 2021 8:29 Kann man die Einträge in der functions.php des Child-Themens nicht auch in ein gesondertes Plugin schieben? Antworten

- die schreibmaus22. April 2021 13:04 hallo andreas,auf der suche nach weiteren sicherheits-features für wordpress im netz bin ich auf eine andere seite gestoßen: „https://kinsta.com/de/blog/wordpress-url-loggst/“. dort empfehlen sie unter anderem, mithilfe des wps hide plugins die normale url, unter der üblicherweise der login stattfindet, umzubiegen auf eine beliebig selbstgewählte url, die der angreifer nicht kennen kann. das plugin funktioniert soweit, allerdings natürlich nicht in kombination mit der zusätzlichen Passwortabfrage (HTTP Authentifikation), die du am anfang deines artikels beschreibst. frage an dich als experten: würde es sich lohnen, die login-url zusätzlich zu „verbiegen“, um hackerangriffe weiter zu erschweren? könnte man das mit deiner zusätzlichen passwortabfrage kombinieren? vermutlich müsste man deine .htaccess-datei noch mal anpassen, aber dafür bin ich nicht profi genug. es wäre toll, wenn du das machen könntest, sofern du es für sinnvoll hältst.liebe grüße,die schreibmaus Antworten
  -  Andreas Hecht22. April 2021 13:12 Das verstecken der Login-URL hilft nicht, das können Hacker schnell herausfinden. Antworten
    - die schreibmaus28. April 2021 13:53 vielen dank für deine einschätzung! Antworten
- schreibmaus21. April 2021 19:53 hallo

andreas,vielen dank für dein tolles tutorial! die beschriebenen dinge haben gut funktioniert, bis auf eines: der redirect auf die google-startseite bei eingabe eines falschen logins funktioniert bei mir so nicht. jedenfalls bekomme ich da genauso eine weiße seite mit wordpress-logo angezeigt, wir der andere andreas, der die schrieb. dabei bin ich kein anfänger und habe das gesamte tutorial bestimmt 5 mal gelesen. hast du eine idee, was ich eventuell doch falsch mache?danke dir für eine rückmeldung,
die schreibmaus Antworten

-  schreibmaus19. April 2021 20:59 hallo andreas,herzlichen dank auch von mir für diesen tollen beitrag. was die weiterleitung zu google angeht, geht es mir allerdings wie dem anderen andreas hier, zitat:„Das mit dem Redirect beim falscher Eingabe der Zugangsdaten passt bei mir leider auch noch nicht. Statt Redirect bekomme ich eine leere Seite mit dem WP-Logo (befinde mich da noch immer auf meiner Domain).“das geht mir leider auch so. habe das snippet direkt nach dem „Anmeldung nur noch mit E-Mail-Adresse“-snippet am beginn der functions.php-datei des child-themes eingefügt. ich bin zwar kein anfänger, aber trotzdem unsicher, ob ich das entsprechend richtig gemacht habe, weil es – wie gesagt – nicht funktioniert.vielleicht hast du eine idee, was ich falsch mache.die schreibmaus Antworten

-  Konstantin3. März 2021 15:33 Moin Moin,
kann sein das: Teil 3: Redirect auf Google nach falscher Eingabe der Zugangsdaten
mit dem aktuellen WordPress nicht mehr funktioniert? Antworten

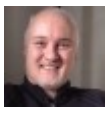
-  Frank15. Dezember 2020 17:25 Hallo Andreas,
einfach mal ein herzliches Dankeschön für deine tolle Arbeit, die unglaublich viel Zeit spart und WP deutlich sicherer macht. Bleib gesund und herzliche Grüße
Frank Antworten
-  Tilo10. Dezember 2020 16:37 Hallo,1.000 Dank für die hervorragende Anleitung.Ich habe ein paar Fragen und Probleme, die evtl. beantwortet und gelöst werden könnten.Zu Punkt Teil 2: WordPress absichern: Zugang nur noch mit E-Mail-Adresse:
Mit der Benutzeranmeldung (normale Kundenanmeldung) hinter einem woocommerceshop, können sich die Kunden nun auch alle nur noch mit der E-Mail anmelden? Oder gilt dies nur für den Admin?…lese ich am Code zumindest nicht heraus. Das würde evtl. für Probleme sorgen, da nicht alle Kunden so firm drinnen sind.Zu Punkt htaccess und Firewall:
ich habe seit der Umstellung auf die/Ihre htaccess auf experten-kredite.de Probleme mit dem PlugIn CalculateFiledsForm (Button „Direkt anfragen“). Da ich dort Daten abfrage und via Clickevent weitergebe denke ich das dies an einer Firewallregel liegt, da er mir im Anschluss einen 403 ausgibt.Gibt es dafür evtl. eine Lösung?Vielen Dank
Tilo Antworten
  -  Andreas Hecht10. Dezember 2020 17:58 Hallo Tilo,Punkt 2: Ja, das dürfte sich auch auf die WooCommerce-User auswirken. Zur .htaccess: Der 403 sollte durch die 7G-Firewall ausgelöst werden. Da bitte die 7G-Firewall in der Datei gegen die 6G-Firewall austauschen. Siehe: https://seoagentur-hamburg.com/die-perfekte-htacce

ss-fuer-wordpress/ (https://seoagentur-hamburg.com/die-perfekte-htaccess-fuer-wordpress/) Antworten

-  Tilo11. Dezember 2020 7:05 Hallo Andreas,Vielen Dank für deine schnelle Antwort…Mit der Anmeldung mit einem woocommerceshop gibt es da sicher einige Probleme mit Kunden, da ja da auch steht „Benutzername oder E-Mail-Adresse“ (hier mal am Kundenbeispiel https://viewegerback.de/mein-konto/ (https://viewegerback.de/mein-konto/)). Gibt der Nutzer nicht die/seine E-Mail ein, wird er auf Google weitergeleitet. Hier ist die Frage, an dich als Profi, ob es dafür einen anderen Weg gibt. Einfachster Weg, die Zeile ändern in nur „E-Mail-Adresse“. Hier wäre die Frage, wo ich dies ändern muss?Mit der Firewall hatte ich die 6G getestet, aber da war gar nichts zu machen, sondern gleich alles dicht. Ich habe jetzt bei den Filtereinstellungen den einen Wert (null) rausgenommen…und es geht. Ich denke, das wird nicht gleich die Sicherheit auf den Kopf stellen. ;opDanke dir
  Tilo Antworten

  -  Tilo11. Dezember 2020 8:30 …wichtig für alle die WordPress 5.6 und die .htaccess https://gist.github.com/seoagentur-hamburg/c96bc796764baaa64d43b70731013f8a#file-htaccess (https://gist.github.com/seoagentur-hamburg/c96bc796764baaa64d43b70731013f8a

#file-htaccess)
verwenden, sei noch mitgeteilt, dass die Permalinkstruktur evtl. neu gesetzt (wegen der Authorization) werden muss
https://de.wordpress.org/support/topic/nach-update-auf-5-6-keine-bearbeitung-moeglich/
(https://de.wordpress.org/support/topic/nach-update-auf-5-6-keine-bearbeitung-moeglich/) Antworten

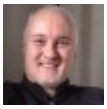
-  Iva29. Oktober 2020 15:21 Hallo Andreas,
vielen Dank für deinen hilfreichen Beitrag. Ich habe eine Frage noch: was würdest du empfehlen für die Absicherung der functions.php-Datei. Besonders sensibel sind z.B. die Zugangsdaten zu dem SMTP-Server, da Username und Passwort im Klartext stehen? Kann man sie verschlüsseln?
Besten Dank! Antworten
  -  Andreas Hecht13. November 2020 14:55 Sorry für die späte Antwort. Seit Corona habe ich mehr Arbeit als ich bewältigen kann. Warum willst Du einen E-Mail-Server (SMTP) in die functions.php eintragen? Antworten

-  Matthias28. Oktober 2020 3:06 Hey Andreas … interessanter Beitrag! Ich hab 2 Fragen.
1. Wenn ich das alles so umsetze, brauch ich dann noch

Wordfence?
2. Das mit Child Theme hab ich nicht ganz verstanden .. Ich nutze kein Child Theme, kann ich dann das trotzdem anwenden? Danke Antworten

-  Andi3. November 2020 0:20 Wenn du die 7G Firewall in deiner htaccess implementiert hast, ein 32 Zeichen langes Passwort und eine 2 Faktor-Authentifizierung, sowie zusätzlichen htacces-Schutz für wp-admin verwendest, dann brauchst du das Plugin „Wordfence“ nicht. Nutze am besten die htaccess-Datei, welche Adresse hier im Beitrag zur Verfügung stellt.Du könntest die von Andreas aufgeführten Anpassungen auch direkt in der functions.php einfügen. Problem: Nach einem WordPress Update werden all deine Einträge überschrieben. Daher ist ein Child-Theme zu empfehlen.Andreas Hecht hat hier in seinem Blog eine Anleitung dazu. Antworten

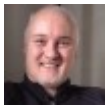
-  Andreas2. September 2020 12:24 Hi Andreas,
toller Beitrag – aber gleich zwei Fragen.1) Umleitung auf Google nach falscher Eingabe der Zugangsdaten funktioniert bei mir nicht.
2) Login via E-Mails ist möglich, aber auch weiterhin mit dem Standard-Benutzernamen.Deinen Code habe ich in die funtions.php unter /wp-includes eingefügt. Ist das evtl. der Fehler? Oder muss ich deine Code Snippets direkt am Anfang oder am Ende der php-Datei einfügen? Antworten

-  Andreas Hecht2. September 2020 12:31 Hi Andreas,genau deshalb schrieb ich, dass die Maßnahmen des Artikels nicht für Anfänger geeignet

sind. Du kannst nicht einfach **irgendwo** etwas hinein kopieren und dann sagen, dass es nicht funktioniert. Der Code gehört in die functions.php **des verwendeten Themes!** Und da solltest Du vorher ein Child-Theme erstellt und aktiviert haben, ansonsten sind die Änderungen nach dem nächsten Theme-Update weg. Das steht da auch ganz deutlich, wo das hin muss. Man muss nur **LESEN**. Ich zitiere mich mal:Kopiere den folgenden Code in die functions.php Deines (Child-) Themes: Antworten

-  Andreas2. September 2020 17:30
  Trotzdem danke Andreas. Den Hinweis hatte ich auch gelesen, dachte mir aber, weil du Child in Klammern gesetzt hast, dass es auch in die Haupt-Functions.php eingefügt werden kann. Sorry, Anfängerfehler.Aber wenn man als Anfänger keine Fragen stellt, kann sich an dem Status auch nichts ändern.
  Und ich habe nicht behauptet, dass dein Code nicht funktioniert. Ich habe lediglich als Anfänger einen Fehler gemacht und hatte keine Erklärung dafür. Ich möchte ja den gesamten Code verstehen, bevor ich einfach nur ‚Copy and Paste' mache.Leider bin ich kein gelernter Informatiker und muss mir die Materie hier selbst erarbeiten und beibringen – nicht immer einfach.
  Bevor ich Dir also weitere unnötige Fragen stelle, kannst du mir evtl. einen Tipp geben, welche Quellen ich für das Verstehen des Codes nutzen kann?Das mit dem Redirect beim falscher Eingabe der Zugangsdaten passt bei mir leider auch noch nicht. Statt Redirect bekomme ich eine leere Seite mit dem WP-Logo (befinde mich da noch immer auf

meiner Domain). Entweder habe ich den Snippet an der falschen Stelle eingefügt (‚functions.php' im Hauptverzeichnis, da du hier ja nicht auf die functions.php des Child-Themes verwiesen hast oder?) oder es fehlt noch eine andere Voraussetzung, die ich übersehen habe.Deine Arbeit und Ratschläge weiß ich sehr wohl zu schätzen. Nochmals vielen Dank. Antworten

-  Andreas Hecht2. September 2020 17:55 Andreas,selbst wenn Du das (Child-) einfach mal streichst, bleibt noch »**in die functions.php Deines Themes**« über. Dort, und nur dort kommt Code hinein. Und wenn Du willst, dass sich der Code auch noch nach einem Theme-Update dort befindet, dann erstellst Du von Deinem aktiven Theme ein Child-Theme, dass Du dann aktivierst. In dieses Child-Theme kommt ebenfalls eine functions.php hinein, in die dann jeder Code-Schnipsel hineinkommt. Übrigens muss man dafür kein Informatiker sein. Aber erstens sehr genau lesen und zweitens **VORHER fragen**, bevor man einfach irgendetwas macht, was man nicht versteht.

https://gist.github.com/seoagentur-hamburg/c96bc796764baaa64d43b70731013f8a#file-htaccess

3CX – Telefonie und Chat

https://portal.3cx.com/customer/keys

Schritt 1: Installieren der 3CX-Apps

iOS: Download die iOS VoIP App aus dem App Store und QR-Code scannen **Android**: Download die Android VoIP App von Google Play und QR-Code scannen **Windows**: 3CX Desktop-App Melden Sie sich bei Ihrem Web Client an und klicken Sie auf das Windows-Symbol, um die App zu installieren und bereitzustellen

Schritt 2: Anrufe verwalten – Der Webclient

URL: https://web-werkstatt.3cx.at/webclient/ **Benutzername:** 10**Passwort:** 30dDHUSC6g Installieren Sie die 3CX-Browsererweiterung für Chrome or Edge und lesen Sie die Benutzerhandbuch.

Schritt 3: Hinzufügen von Benutzern und SIP-Trunks – Die Verwaltungskonsole

URL: https://web-werkstatt.3cx.at/ Fügen Sie Nebenstellen und SIP-Trunks hinzu und konfigurieren Sie IP-Telefone. Erfahren Sie, wie Sie konfigurieren IP-Telefone, SIP-Trunks und lesen Sie unsere Administratorhandbuch. **Benutzername:** admin**Passwort:** zkZ3YfOZA0CtN7bX

Schritt 4: Installieren Sie den Live-Chat-Code auf Ihrer Website

- Installieren Sie das WordPress-Plugin hier oder generieren Sie Live-Chat zur Verwendung mit jedem CMS. Konfigurieren Sie, welche Agenten Live-Chats und Anrufe annehmen sollen. Konfigurationshandbuch
  Integrieren Sie Ihre Facebook-Nachrichten mit 3CX. Einrichtungsanleitung

Login zum Web Client

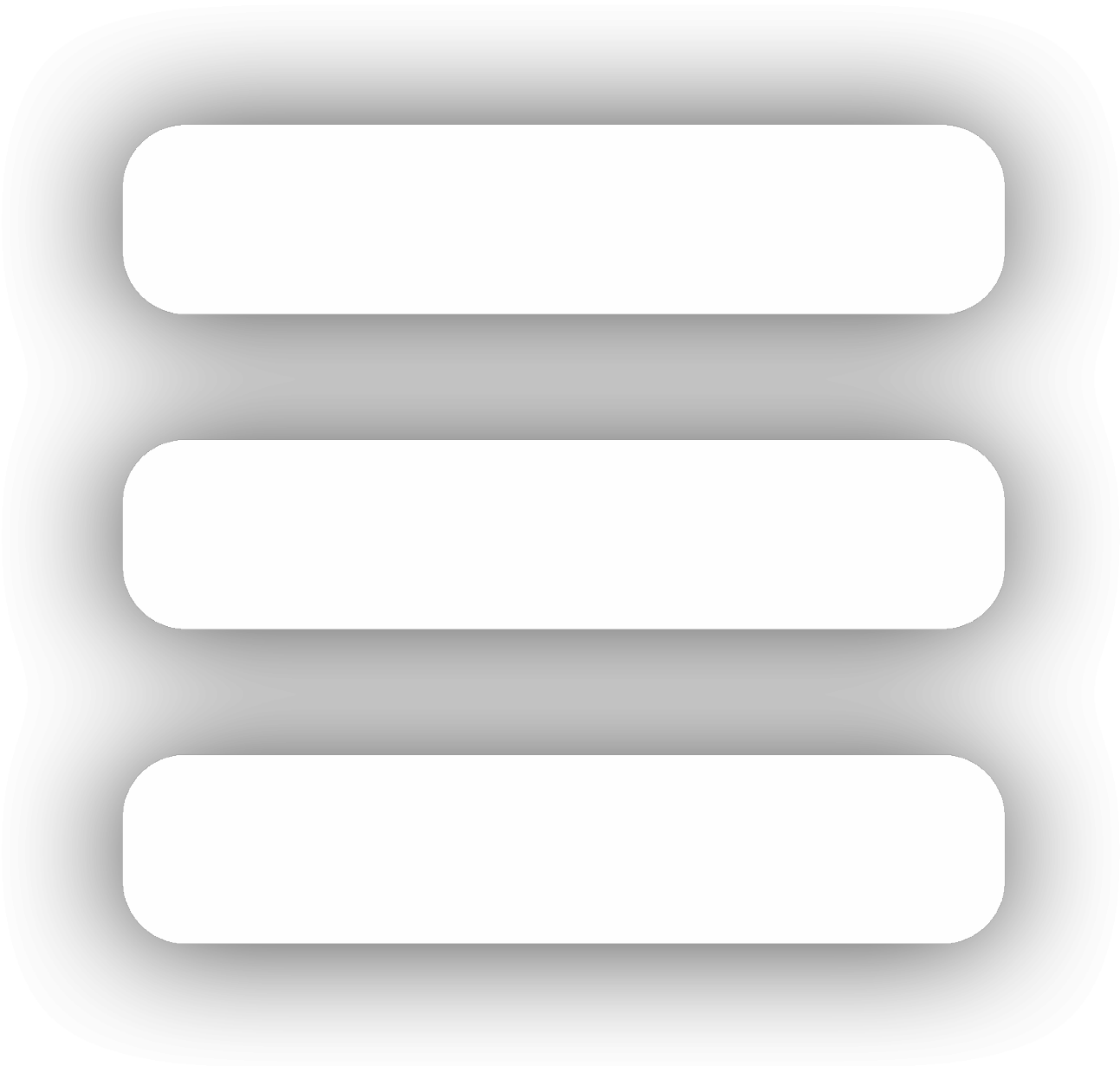
https://web-werkstatt.3cx.at/webclient/

Login zur Console

https://web-werkstatt.3cx.at/

3CX Free Live Chat, Calls & WhatsApp

WordPress – geschützten Mitgliederbereich erstellen – how to



TravelAgency – Schema.org Type

Schema.org Type: TravelAgency – A travel agency.

Einen geschützten Kundenbereich in WordPress einrichten

20. Dezember 2017Kim SalewskiFunktion

Haben Sie schon einmal überlegt, einen geschützten Kunden- oder Mitgliederbereich für Ihre Website einzurichten? Es gibt unzählige Membership-Plug-ins im großen, weiten Internet, genau so wie es unzählige Anforderungen an Mitgliederbereiche gibt. Kein Wunder, dass man dafür oftmals eine Menge Zeit und Energie investieren muss, um eine geeignete Lösung zu finden.

Inhalt

Worum geht es?

Manche Mitgliedschaften sollen z.B. gekauft werden können, andere wiederum sollen nach einer gewissen Zeit ablaufen, wieder andere sollen komplett kostenlos sein und lediglich Inhalte für Kunden oder Kursmitglieder zur Verfügung stellen. In diesem Beitrag gehen wir auf einen Mitgliederbereich ein, in welchem sie Dateien zum Download in einem geschützten Kunden- oder Mitgliedsbereich bereitstellen können.

Was ist der Plan?

In dem beschriebenen Beispiel gehen wir davon aus, dass Sie einen oder mehrere Kurse/Schulungen anbieten. Ihren Kursteilnehmern möchten Sie Download-Dateien wie Infohefte, Aufgabenzettel oder ähnliches auf Ihrer Website in einem geschützten Bereich zum Herunterladen bereitstellen. *(Natürlich könnte es sich auch um einen geschützten Bereich handeln, bei denen Sie Ihren **Kunden zum Beispiel Preislisten zum Download anbieten**. Das Vorgehen ist das gleiche.)*
In einem ersten Schritt richten wir einen Mitgliederbereich ein, in dem Kursteilnehmer sich mittels eines spezifischen Benutzernamen und Passwortes einloggen können. Diese Daten erhalten die Kursteilnehmer von Ihnen zum Beispiel per E-Mail oder per Post. Durch eine Log-in-Seite auf Ihrer Website melden sich die Kursteilnehmer an und werden daraufhin direkt auf die entsprechende Kursseite weitergeleitet, auf die Sie Zugriff haben. Hier können sie die gewünschten Dateien herunterladen.

Was wir benötigen

- Eine Log-in-Seite
- Eine Mitgliedschaft sowie ausgewählte Benutzerdaten pro Kurs, mit dem sich Kursteilnehmer zukünftig zum Herunterladen Ihrer Dateien anmelden können
- Die Möglichkeit, nach Log-in direkt zur entsprechenden Downloadseite weitergeleitet zu werden
- Geschütze Downloads, die nur von angemeldeten Benutzern heruntergeladen werden können

Das alles werden wir mit Hilfe von nur drei Plug-ins umsetzen. Das erste Plug-in Simple Membership dient der Erstellung eines Mitgliederbereiches. Mit dem zweiten Plug-in, der Erweiterung After Login Redirection, erstellen wir die Umleitung nach dem Log-in. Das dritte Plug-in, genannt Download Monitor, sorgt dafür, dass auf bestimmte Dateien nur zugegriffen werden kann,

wenn der Besucher eingeloggt ist. Dies verhindert den Zugriff von nicht angemeldeten Besuchern auf die Dateien, die sonst durch einen Permalink für alle aufrufbar wären.

Installation des Plug-ins Simple Membership

Die Installation der Plug-ins läuft wie gewohnt ab. Unter Plug-ins im Backend suchen Sie unter Installieren nach dem Plug-in **Simple Membership**. Dieses installieren und aktivieren Sie.

Bei der Aktivierung werden automatisch die folgenden Seiten angelegt:

Diese Seiten regeln über die in ihnen automatisch angelegten Shortcodes, welche Funktion jeweils durchgeführt werden. Die **Join Us** Seite ist eine Beispiel-Seite, die zeigt wie Sie Ihre Mitgliedschaften präsentieren können, sofern es für Besucher möglich sein soll, sich selbst zu registrieren. Die **Registration-**Seite ist die Seite, auf der Besucher sich für eine Mitgliedschaft registrieren können. Beim **Membership Login** melden sich Mitglieder mit Ihrem Benutzernamen und Passwort an, um Zugriff auf Ihre Mitgliedsseiten zu erhalten. Unter **Passwort Reset** werden Passwörter zurückgesetzt und das **Profile** zeigt dem Besucher die Daten an, die bei dem Benutzer hinterlegt sind (hier kann er diese ggf. auch ändern).

Anpassen der Log-in Seite

Soviel zu der Erklärung der einzelnen Seiten. Für unser oben genanntes Beispiel löschen Sie bitte die folgenden Seiten:

Wir benötigen lediglich den **Membership Login**, über welchen Ihre Nutzer sich anmelden können. Es sollen sich keine neuen Benutzer registrieren können, auch das Passwort und die restlichen Benutzerdaten sollen lediglich von Ihnen selbst im

Backend geändert werden können, weshalb die restlichen Seiten wegfallen. Genau so wie die **Join Us** Seite, die somit überflüssig wird.
Während Sie dabei sind, die Seitenanzahl zu reduzieren, benennen Sie gleich die **Membership Login** Seite in **Login** um, damit es hier später nicht zu Verwirrungen kommt. Vergessen Sie dabei nicht, auch den Permalink anzupassen.

Wenn Sie diese Anpassungen vorgenommen haben, wird es nun Zeit, Einstellungen in **Simple Membership** an sich vorzunehmen. Hierzu suchen Sie in der Seitenleiste den Punkt **WP Mitgliedschaften** und wählen in dem Untermenü **Einstellungen** aus.
Im Allgemeinen lassen Sich hier allerlei Einstellungen vornehmen, die interessant für Sie sind, wenn Sie z.B. Mitgliedschaften anbieten wollen, zu denen sich Ihre Besucher registrieren sollen. Für unseren Fall sind aber bereits alle Einstellungen ausreichend eingestellt. Lediglich die URLs unter **Seiteneinstellungen** müssen gemäß unserer Änderungen an den Seiten angepasst werden.

Wir benötigen nämlich **nur** die URL der Login Seite in **jedem** Feld. Das verhindert zum einen, dass später Fehlermeldungen erscheinen. Zum anderen werden erreichen die Kursteilnehmer nie Seiten wie **Passwort zurücksetzen** und können so keinen Unsinn treiben.

Eine Mitgliedschaftsstufe einrichten

Nun ist es soweit, es wird Zeit, die **Mitgliedschaft** oder auch **Mitgliedschaftsstufe** für Ihre Benutzer einzurichten. Diese regelt, welcher Benutzer was sehen darf. Ein kleines Beispiel:
Sie richten eine Mitgliedschaftsstufe mit dem Namen **Kurs A** und eine mit dem Namen **Kurs B** an.
Auf der Download-Seite für den Kurs A, die wir später erstellen, stellen Sie dann ein, dass nur Benutzer, die zu der

Mitgliedschaft **Kurs A** gehören, diese Seite sehen/aufrufen können. Das verhindert sowohl, dass **Kurs B-Teilnehmer**, als auch dass **unangemeldete Besucher** die Seite sehen können.

Um eine Mitgliedschaftsstufe anzulegen, gehen Sie unter **WP Mitgliedschaften** auf den Unterpunkt **Mitgliedschaftsstufen**. Über den Button **Neu hinzufügen** erstellen Sie neue Mitgliedschaften.
Die geforderten Einstellungen in den **Mitgliedschaftsstufen** ist für unseren Mitgliederbereich nicht besonders umständlich. Was festgelegt sein muss ist der **Name**, sowie die **Benutzerrolle** und ein **Ablaufdatum**.

Als Name nehmen wir beispielsweise **Kurs A**, alternativen wären aber auch **Grundkurs** oder z.B. **Einsteiger**. Die WordPress-Benutzerrolle stellen wir auf **Abonnent**, um den Benutzern so wenig Befugnisse wie nur möglich zu geben. Als Ablaufdatum stellen wir **keinen Ablauf** ein, da in unserem Fall die Benutzer eigenhändig angelegt und zugeordnet werden. Es liegt also an uns, **wann** der Benutzer Zugriff hat und **wann nicht**.

Ein Mitglied einrichten und einer Mitgliedschaftsstufe zuordnen

Da wir nun die passende Mitgliedschaftsstufe haben, müssen wir als nächstes einen Benutzer anlegen, dem wir diese zuordnen. Das geht in der Regel auch ganz leicht, alles, was benötigt wird, ist eine E-Mail-Adresse pro Benutzer. Hierbei ist **pro** das ausschlaggebende Wort, da nicht mehrere Benutzer mit der selben E-Mail-Adresse angelegt werden können. Sie müssen also **pro** Kurs einen Benutzer mit einer eigenen E-Mail-Adresse angeben.
Um einen Benutzer **mit einer bestimmten Mitgliedschaftsstufe** anzulegen, suchen Sie in der Seitenleiste **WP Mitgliedschaften** und wählen Sie den Unterpunkt Mitglieder aus. Hier finden Sie, wie bei den Mitgliedschaftsstufe auch, einen Butten mit dem Namen Neu hinzufügen, über welchen neue Mitglieder angelegt

werden können.
Neben den benötigten Angaben wie **Benutzername**, **E-Mail-Adresse** und **Passwort**, können Sie weitere Angaben machen, wie zum Beispiel den Kontostatus, welcher standardmäßig auf **Aktiv** steht. Sollte einmal ein Benutzer zeitweise deaktiviert werden müssen, beispielsweise wenn Sie geschützte Seiten anpassen wollen, ohne dass ein Mitglied diese Anpassungen sieht, stellen Sie den Benutzer einfach auf **Inaktiv**.

Essenziell für unsere Voraussetzungen ist aber die **Mitgliedschaftsstufe**, die für den Benutzer ausgewählt werden kann. Ist ein Benutzer einer Stufe zugeordnet, hat er Zugriff auf alle Seiten, die für diese Mitgliedschaftsstufe freigeben wurden.

Das sind auch schon alle Einstellungen, die für unseren Mitgliederbereich notwendig sind. Was nun folgt, ist das Erstellen der Seiten, auf den das jeweilige Kursmitglied zugreifen können soll.

Eine Kurs-Seite einrichten und schützen

Als nächstes legen Sie eine neue Seite an, die rein für den Kurs A-Teilnehmer zu sehen sein soll.
Sobald Sie eine neue Seite angelegt haben, finden Sie unterhalb des Editors die Einstellungen zum Schutz der Seite.

Sie haben unter „Möchten Sie diesen Inhalt schützen?“ zum einen die Wahl, den Inhalt zu schützen oder den Schutz aufzuheben. Zum anderen können Sie unter „Wählen Sie die Mitgliedschaftsstufe aus, die auf diesen Inhalt zugreifen kann“ entscheiden, welche Mitgliedschaftsstufe diese Seite sehen kann. Für unser Beispiel wählen wir Kurs A aus, was dafür sorgt, dass sowohl Kurs B als auch alle anderen Benutzer/Besucher die Seite nicht aufrufen können.

URL der Seite als Redirect einstellen

Wie bereits oben beschrieben wäre es wünschenswert, dass Kurs-Teilnehmer, die Sich mit einem Benutzer von Kurs A anmelden, auch direkt bei der Download-Seite von Kurs A landen. Glücklicherweise gibt es hier ein Add-on für das **Simple Membership** Plug-in. Sie rufen einfach unter **WP Mitgliedschaft** im Backend den Menüpunkt Add-ons auf. Hier finden die, für gewöhnlich gleich an erster Stelle, das Add-on After Login Redirection, alternativ können Sie unter Plug-ins gleich nach **Simple Membership After Login Redirection** suchen und dieses installieren und aktivieren.
Was nun passiert ist, dass automatisch bei Ihren Mitgliedschaftsstufen eine zusätzliche Spalte auftut, in welche Sie die URL der Seite eintragen, auf die Benutzer weitergeleitet werden, die dieser Mitgliedschaftsstufen angehören.

In unserem Fall leiten wir in der Kurs A Mitgliedschaftsstufe auf die Download-Seite von Kurs A weiter. Somit werden Benutzer, die für Kurs A eingetragen sind, nach erfolgreichem Einloggen automatisch auf diese Seite weitergeleitet und müssen nicht erst mühselig zu ihr finden.

Die Downloadseite des Kurses befüllen

Nun geht es darum, die Downloads zu schützen, die auf den einzelnen Download-Seiten angeboten werden. Der Sinn hierbei ist, dass selbst wenn jemand den Link zum Download weitergibt, nur angemeldete Benutzer diese herunterladen können. Hier hilft das Plug-in Download Monitor weiter.
Nach der Installation finden Sie in der Seitenleiste im Backend den Menüpunkt **Downloads**. Hier können Sie Downloads anlegen, Ihnen Titel geben und sie lediglich für angemeldete

Benutzer zugreifbar machen.

Ein Download kann dabei aus mehreren Dateien bestehen. Sie klicken unter **Dateien/Versionen** einfach auf **Download hinzufügen**, um eine neue Datei zum Download hinzuzufügen.

Sie können neben der Download-Anzahl auch eine Versionsnummer angeben, falls Sie die Datei zu einem späteren Zeitpunkt aktualisieren möchten.
Wichtig: Sollte sich Ihre Website noch auf einer Entwicklungsumgebung befinden, so sollten Sie relative Links als Datei-URLs angeben.
Also
/wp-content/uploads/2015/07/Rakete.png
statt
https://ihredomain.de/wp-content/uploads/2015/07/Rakete.png

Nachdem Sie alle Dateien eingefügt haben, kopieren Sie den Shortcode und veröffentlichen Sie den Download. Nun können Sie diesen Shortcode in jede mögliche Seite eintragen, in der die Dateien herunterladbar sein sollen. Am sinnvollsten ist es in unserem Fall, diesen Download direkt auf der Kurs-Download-Seite einzufügen, zur der Kursteilnehmer automatisch weitergeleitet werden. So haben diese sofort Zugriff auf die wichtigsten Dateien.
Zu guter Letzt müssen Sie die Kurs-Download-Seite mit Inhalten füllen, wie beispielsweise mit einem netten Willkommens-Text, ein Paar Bilder oder sonstigen Handlungsanweisungen.

Übersetzung und CSS anpassen

Zwei letzte, wichtige Anpassungen, die Sie vornehmen müssen, finden in der Übersetzungsdatei sowie über CSS statt.

Die Herausforderung:

Ruft man als gewöhnlicher, nicht angemeldeter Besucher eine geschützte Seite wie die Kurs-Download-Seite auf, so erhält

man die oben gezeigte Benachrichtigung. In unserem Beispiel sollen sich Besucher aber gar nicht **registrieren** können.

Das selbe gilt für das Log-in Formular auf der Log-in-Seite an sich. Hier sind sowohl der **Passwort-Vergessen-Link** als auch der **Registrieren-Link** überflüssig, da niemand diese Funktionen nutzen soll.
Mittels CSS können wir die jeweils grün markierten Links entfernen. Dazu müssen Sie den folgenden Code in Ihr **Zusätzliches CSS** unter den **Customizer** bei dem Menüpunkt **Design** oder in der **Administrationsleiste** einfügen.

```
div.swpm-forgot-pass-link,
div.swpm-join-us-link,
.swpm-post-not-logged-in-msg a:not(.swpm-login-link) {display: none;}
```

Nun, da die Links weg sind, müssen wir uns nur noch um einen kleinen Textteil kümmern, der fehl am Platz ist:

Leider lässt sich dieser Textteil nicht durch CSS allein entfernen. Wir müssen uns also mit der Übersetzungsdatei des Plug-ins weiterhelfen. Eine grundsätzliche Erklärung, wie Sie Themes und Plug-ins Übersetzen, finden Sie in unserem Beitrag „WordPress Themes und Plug-ins übersetzen: Ein Vergleich“.
Wir gehen trotzdem Schritt für Schritt durch, was genau Sie tun müssen. Zunächst installieren Sie das Programm Poedit, mit welchem Sie Übersetzungsdateien bearbeiten können.
Danach loggen Sie sich über FTP auf Ihrem Server ein und navigieren zu **/wp-content/plugins/simple-membership/languages/**. Hier suchen Sie sich die **simple-membership-de_DE.po** Datei heraus und laden Sie auf Ihren Desktop herunter. Als nächstes öffnen Sie diese in Poedit, bzw. durch einen Doppelklick.

Als nächstes drücken Sie die **Befehlstaste + F** (Windows Strg + F), um in dem Programm nach einem Bestimmten Text zu suchen.

Sobald Sie auf **Weiter** klicken, zeigt ihnen Poedit sofort die Stelle in der Übersetzungsdatei an, an der Sie den Text

anpassen können. Es bleibt Ihnen überlassen, ob Sie lediglich ein Leerzeichen anstelle des eigentlichen Textes eintragen, oder einen anderen Text angeben wie z.B. „**Halten Sie Ihre Zugangsdaten parat.**“ In unserem Fall tragen wir ein einfaches Leerzeichen anstelle des eigentlichen Textes ein, was dafür sorgt, dass das Feld nicht komplett leer steht und die englische Übersetzung verwendet wird.

Danach Speichern Sie. Lassen Sie sich nicht durch die Fehlermeldung beunruhigen, diese besagt lediglich, dass der Englische Text auf einem Fragezeichen endet, wo hingegen Ihre dies nicht tut. Dies ist in diesem Falle aber so gewollt.

Wenn Sie die Datei Speichern, wird automatisch eine .mo Datei erstellt, die ebenfalls auf dem Desktop erscheinen sollte. Ist dem nicht der Fall, klicken Sie bitte in der Menü-Leiste unter **Datei** auf die Option **MO-Datei erstellen**. Sie benötigen beide Dateien, für den nächsten Schritt.
Nun laden Sie die beiden Dateien in den folgenden Ordner hoch:
/wp-content/languages/plugins/
Sobald dies getan ist, wird der fehlerhafte Text entweder verschwunden, oder durch Ihren eingegebenen Text ersetzt worden sein.

Den Benutzer abhalten, seine Daten anzupassen

In unserem Fall möchten wir die volle Kontrolle über die Log-in-Daten behalten. Die Kursteilnehmer sollen nicht die Möglichkeit erhalten, Ihr Passwort zurückzusetzen, das Profil in irgendeiner Weise zu bearbeiten oder ins Backend zu gelangen. Um dies zu verhindern, müssen unter **WP Mitgliedschaft** –> **Einstellungen** die folgenden Häkchen gesetzt sein:

Nun muss ein letzter Feinschliff vorgenommen werden. Auf der Log-in Seite erhält der Kursteilnehmer Informationen und

Handlungsmöglichkeiten wie **„Profil bearbeiten“** und **„Ausloggen„**.

Da er sein Profil **nicht bearbeiten** soll, muss dieser Link mittels CSS ausgeblendet werden.
.swpm-edit-profile-link {display:none;}
Um die Übrigen, für den Kunden unwichtigen, Infos auszublenden, wie zum Beispiel den **Kontostatus** etc., fügen Sie außerdem den folgenden Code ein:
.swpm-logged-status, .swpm-logged-membership, .swpm-logged-expiry

Die Log-in Seite verlinken

Damit Ihre Mitglieder nun zukünftig auch eine Seite haben, auf der Sie sich anmelden können, verlinken Sie die oben erstellte Log-in Seite am besten im **Haupt- oder Footermenü**. Ihre Kursmitglieder finden so schnell den Zugang zu Ihrer Seite und somit zu Ihren Download-Dateien.

Fazit

Selbst für einen einfachen, kostenlosen Mitgliederbereich ist der Aufwand, den Sie betreiben, um alles am Laufen zu halten, sehr groß. Daher müssen Sie auch bei diesem Mitgliedschaftsbereich, aber vor allen bei größeren, kostenpflichtigen Mitgliedschafts-Projekten genau Planen und Testen.*turned_in_not*Benutzerfreundlichkeit, PluginsKim Salewskihttps://kim-salewski.de/Ich bin seit August 2015 Teil der Elbnetz-Crew und ein großer WordPress-Fan. Ich habe eine Ausbildung zur Assistentin für Screen Design absolviert und programmiere/zeichne in meiner Freizeit rund um die Uhr.

126 Kommentare. Wir freuen uns über Ihren Kommentar

- Stef 26. September 2021 20:33 Hallo, vielen herzlichen

Dank für diese tolle Anleitung. Ich habe allerdings ein Problem: Ich habe eine Newsseite (Beitragsseite) im geschützten Bereich angelegt. In dieser befinden sich etliche Beiträge (also keine weiteren Seiten, sondern Beiträge). Leider kann man sich nun über die Goggle Suche diese Beiträge ansehen. Was habe ich falsch gemacht? Bzw. wie kann ich den allgemeinen Zugriff auf diese Beiträge verhindern und wie kann ich schnellstmöglich die Beiträge aus der Google-Suche entfernen? Vielen Dank für Eure Hilfe!!! Antworten

- Thorsten Faltings 27. September 2021 9:21 Moin Stef, um den allgemeinen Zugriff auf die Beiträge zu verhindern, musst Du auch diese jeweils – wie oben beschrieben – analog der Seiten vor dem Zugriff schützen. Du kannst versuchen, über die Google Search Console die Beiträge möglichst schnell aus dem Suchindex zu löschen. Ahoi!
  Thorsten Antworten

- Kersbers 16. September 2021 9:47 Hey,
  tolles Plugin.
  Eine Frage habe ich noch: Gehe ich auf den Link einer Mitgliederseite für die ich nicht freigegeben bin, erscheint ja „Sie müssen sich anmelden, um diesen Inhalt zu sehen. Bitte Anmelden. Kein Mitglied?“. Kann ich hier auch direkt zur Login Seite verlinken? Wenn ja, wie geht das? Vielen Dank schonmal Antworten
  - Dirk 9. Oktober 2021 14:40 Hey, genau das selbe Problem habe ich jetzt auch. Bzw. ich würde nicht gerne direkt auf die Loginseite verlinken, sondern auf eine eigene Seite, die einen Text anzeigt und danach Links für die Login- oder die Startseite bereitstellt.
    Ich hab dazu jetzt schon extra ein Child-Theme erstellt, damit ich evlt. Änderungen nicht nach jedem Update machen muss. Wäre toll, wenn es hierzu eine kleine Antwort/Anleitung geben würde.
    Antworten

- Nuray Kirch 22. August 2021 12:50 Hallo! Diese Anleitung hat mir sehr geholfen.
  Ich habe aber die gleiche Frage, die Jessie Fröde am 14. Januar 2021 gestellt hat und deren Beantwortung ich hier nicht gefunden habe:
  Da ich den Login Bereich auch für eine englische Seite erstelle, möchte ich den Text „Not a member?“ ebenfalls entfernen. Wo muss bzw. kann ich den englischen Quelltext entfernen?
  Ich würde auch gerne den Text „Username“ auf der Login Seite verändern. Welche Dateien nutze ich dazu? Antworten
- Hans-Georg Hauser 30. April 2021 23:12 Hallo! Ich habe eben einen geschützten Mitgliederbereich eingerichtet. Leider lassen sich keine Mitglieder hinzufügen. Zwei habe ich geschafft, das wars! Es kommt keine Fehlermeldung, nur die Mitglieder werden nicht angelegt. Woran könnte das liegen? Für Hilfe bin ich sehr dankbar. Antworten
  - red-loop 25. Juli 2021 9:52 Wenn Mitglieder bereits unter „Benutzer“ angegeben sind, können diese nicht erneut im Mitgliederbereich angelegt werden. Eine Fehlermeldung bleibt in diesem Fall aus. Antworten
- Malko 17. März 2021 15:36 Erst einmal vielen Dank für Mühe diese Anleitung zu schreiben.
  Ich habe aber jetzt folgendes Problem. Wenn man nach dem Login auf die weitergeleitete Seite kommt, wo der Download Bereich ist, dann kommt diese Meldung „Sie müssen sich anmelden, um diesen Inhalt zu sehen. Bitte Anmelden. Kein Mitglied?“
  Wenn ich auf der Download Seite ganz unten bei „Möchten Sie diese Inhalte schützen?“ den Haken bei „Nein, diesen Inhalt nicht schützen“ setzte funktioniert es, aber dann ist die Seite natürlich nicht geschützt.
  Mache ich den Haken „Ja, diesen Inhalt schützen“. Bekomme ich bei der Weiterleitung den Fehler. „Sie

müssen sich anmelden, um diesen Inhalt zu sehen. Bitte Anmelden. Kein Mitglied?“
Jemand hier, hatte das selbe Problem, hatte dazu aber leider keine Antwort bekommen.
LG
Malko Antworten

- Sebastian 5. Juli 2021 22:01 Die verlinkte Seite muss natürlich noch der entsprechenden Mitgliedsschaftstufe zugeordnet werden, sonst ist derjenige der sich eingeloggt hat trotzdem fremd für die Seite. Dort wo du den Haken setzt, kannst du auch direkt die Mitgliedsschaftstufe auswählen, sofern sie vorher auch angelegt wurde. Antworten

- Frank 3. März 2021 16:26 Hallo.
  Toll erklärt! Ein Problem habe ich aber doch.Gibt es eine Möglichkeit das ausloggen zu erzwingen? Das Problem ist, selbst bei gesetzem Haken “ beim Schließen des Browsers abmelden“ bleibt der Zugang offen wenn nur der Tab geschlossen wird.Man muß zum Abmelden den Browser komplett schließen.Das macht aber in der Praxis ja keiner.
  Ich wäre für eine Idee dankbar.
  Gruß Frank Antworten
  - Thorsten Faltings 4. März 2021 11:20 Moin Frank, schön, dass wir Dir weiterhelfen konnten. Es scheint so, als sei folgendes Plug-in die Lösung für Dein Problem: Idle User Logout. Bitte nutze das Plug-in auf ‚eigene Gefahr‘, wir haben es nicht getestet. Ahoi!
    Thorsten Antworten
- Andreas 22. Februar 2021 22:12 Hallo zusammen, erstmal vielen Dank für die tolle Anleitung. Gibt es auch die Möglichkeit, mehrere Unterseiten zu schützen? Die z.B. erst im Memberbereich sichtbar werden oder so? Antworten
- Robert Werhahn 12. Februar 2021 13:37 Eine wirklich umfassende Beschreibung, vielen Dank dafür. Habe jetzt eine Mitgliedschaftsstufe angelegt (LC Mitglied) und

versuche dazu neue Mitglieder mit Benutzer-Name (zB LCMitgl_2021), eMail & PW (enthält Sonderzeichen, Zahlen, Großbuchstaben) anzulegen: funktioniert nicht. Beim Anlegen erscheint am Oberrand des Dashboardfensters unter der obersten Menüleiste verdeckt und nur zum Teil sichtbar ein rotes und grünes Feld, welches ich aber nicht entziffern kann. Hab ich hier irgend etwas vergessen? Kann mir da jemand weiter helfen? Antworten

- Klara 25. März 2021 11:21 Hat sich das Problem beheben lassen? Ich hänge nämlich auch schon genau hier. Antworten
- Pia wolf 12. Juli 2021 11:06 Ich habe das gleiche Problem :-/ Antworten

- Emma 26. Januar 2021 12:44 Hallo Thorsten, toller Beitrag! Sind die Plug-ins noch aktuell, oder gibt es da mittlerweile Alternativen? Außerdem: Ist es möglich, die Download Dateien in Ordnern zu strukturieren und/oder eine Suchfunktion hinzuzufügen? Vielen Dank vorab! Antworten
  - Thorsten Faltings 26. Januar 2021 13:14 Moin Emma, es freut uns, dass Dir der Beitrag gefällt. Wir überprüfen es nicht jeden Monat, aber die Plug-ins sollten noch aktuell sein. Im Backend werden die ‚Downloads' ähnlich aller Dateien in einem speziellen Unterverzeichnis abgelegt. Wenn Du aber das Frontend meinst, dann hast Du alle Freiheiten, die Links in eine Struktur zu bringen. Mit dem richtigen Plug-in kannst Du auch nach ihnen suchen. Ahoi!
    Thorsten Antworten
- Jessie Fröde 14. Januar 2021 18:05 Tolle & hilreiche Anleitung! Die Seite, die ich gestalte, soll allerdings in zwei Sprachen aufgesetzt werden.
  Gibt es hier auch eine Möglichkeit die Login Seite in DE und EN anzulegen?
  Dafür habe ich bisher leider noch keine Lösung gefunden. Zudem kommt damit das Problem, dass das bearbeiten der

.po Datei dann trotzdem der englische Text „Not a member?“ angezeigt wird … Lieben Dank schon mal für die Antwort. Antworten

- Eckhard Kujawa 9. Januar 2021 14:50 Wie schon von den Vorkommentatoren häufig geschrieben. Die Anleitung ist sehr verständlich.
  Bei mir funktioniert der Download via „Medien“ einwandfrei und der Pfad zum Dokument wird auch richtig angezeigt.
  Wenn ich den Short-Code in die Download-Seite einfüge werden die Links auch für den angemeldeten Kunden angezeigt, führen aber zur Startseite der Website.
  Füge ich in die Download-Seite den Link zum Dokument händisch ein, wird das Dokument wie gewünscht geöffnet.
  Ich kann es mir nicht erklären. Vieleicht hat ja jemand eine Idee.? Antworten
    - E. Kujawa 11. Januar 2021 12:01 Editiere meinen Kommentar vom 09.Januar 2021
      Das geschilderte Problem hat sich erledigt. Kann nur nicht berichten wo der Fehler lag.
      Funktioniert einwandfrei.
      Danke noch mal für die ganz einzigartig gute Anleitung. Antworten
- Herwig 1. Dezember 2020 15:54 Nochmal Hallo,
  das Problem hat mir keine Ruhe gelassen. Auf der Seite des Plugin-Entwicklers findet man eine sehr ausführliche englischsprachige Dokumentation. Im Zuge der Weiterentwicklung des Plugins haben sich wohl die entsprechenden Befehle geändert.
  Wer den Paswortvergessen-Link loswerden will gibt jetzt folgendes ein:
  .swpm-login-widget-form #forgot_pass {display:none;}
  den join us Link so:
  .swpm-login-form-register-link {display:none;}
  und die remember me checkbox so:
  .swmp-remember-me {display:none;}
  Ich habe jedem dieser Befehle eine eigene Zeile in der

Rubrik ‚Zusätzliches CSS', welche man unter dem Customizer findet, den man aus der Administrationszeile erreicht, spendiert und es hat funktioniert.
Die Seite des Entwicklers des SimpleMembership PlugIns ist eine wahre Fundgrube. Man findet die Seite leicht.
Antworten

- Herwig 1. Dezember 2020 14:36 Hallo,
das ist wirklich eine gute Anleitung und ich habe sie bestimmt schon ein paar Mal gelesen. Leider scheitere ich schon hier:
„Das selbe gilt für das Log-in Formular auf der Log-in-Seite an sich. Hier sind sowohl der Passwort-Vergessen-Link als auch der Registrieren-Link überflüssig, da niemand diese Funktionen nutzen soll.
Mittels CSS können wir die jeweils grün markierten Links entfernen. Dazu müssen Sie den folgenden Code in Ihr Zusätzliches CSS unter den Customizer bei dem Menüpunkt Design oder in der Administrationsleiste einfügen."
Wo ist ‚mein zusätzliches CSS'? Dann soll der Code ‚unter den customizer bei dem Menüpunkt Design'. In der Administrationsleiste kann ich nur was auswählen(z.B. Customizer, Neu, Seite bearbeiten) aber nichts eintragen. Wenn ich dort ‚Customizer' wähle erscheint ganz unten als letzte Auswahl ‚Zusätzliches CSS' und dahinter eine Eingabemöglichkeit für code. Wenn ich dort den Code eingebe (gehört er in eine Zeile oder mehrere?) passiert nichts, die Links verschwinden nicht. Ich benutze das kommerzielle Theme ‚Head Blog' für meine Website und bin kein Informatiker, leider. Ich war schon etwas älter, als ich mich mit 6502 Assembler in meinem Commodore 64 beschäftigt habe, Mnemonics und so.
Meine Frage(und Bitte): wo genau muss ich diesen code eintragen. Kann mir jemand den Weg dorthin bitte step by step aufzeigen? Antworten
- Eric 23. November 2020 11:36 Wirklich guter Beitrag! Ich hätte nur ein kleines Problem. Die Seiten die z.B. Kunde A sehen soll aber Kunde B nicht, kann Kunde B trotzdem

sehen. Die Meldung „Dieser Inhalt ist für Ihre Mitgliedschaftsstufe nicht freigegeben.“ erschein zwar aber der Inhalt der Seite auch. Downloads werden blockiert. Jedoch sollte der Inhalt auch blockiert werden. Ich habe diese Methode schon früher einmal genutzt und dort war dies auch so der Fall. Kann dies an meinem Theme liegen? Oder hat jemand eine Idee? Antworten

- Florian 18. August 2020 11:15 Interessanter Atrikel! dennoch mal einen Frage zu wordpress und Persönliche Downloads.
  Gibt es ein Plungin, dass :
  Persönlicher Login
  Persönliche Seite, wo nur die Daten hinterlegt sind (Abrechnung) die für die Person zusehen ist die den Zugang dazu hat. (Beispiel: Peter logt sich ein und sieht seine Abrechnung, Ingo logt sich ein und sieht nur seine Abrechnung und nicht die von Peter)
  Gibt es da ein plugin für auch kerne kostenpflichtig Antworten
  - Thorsten Faltings 18. August 2020 11:31 Moin Florian,
    da Peter und Ingo ja am Ende die gleichen Seiten aufrufen (mit unterschiedlichen Inhalten), sollte das Plug-in Redirect After Login weiterhelfen können.
    Ahoi!
    Thorsten Antworten
  - Thomas 25. November 2020 13:11 Das wäre über die Build-In Funktion von WordPress, den Standardschutz per Passwort, sehr gut lösbar. Antworten
    - Peter 25. Januar 2021 17:44 Hallo Thomas, wie genau wäre das lösbar? Ich habe die gleiche Anforderung, aber so etwas richtig „schönes und einfaches“ kann ich nicht finden. @Florian, wie hast du denn gelöst?

Vielen Dank schon einmal
Peter Antworten

- Pascal 9. August 2020 18:32 Top Beitrag
  Habe eine Frage und vielleicht wird mir diese ja auch noch 2020 beantwortet
  Ich habe auf meiner Seite jetzt ein Kundensystem eingerichtet und das auch mit verschiedenen Kursen. Nach dem Login werden die jeweiligen Kursmitglieder zu der für sie angepassten Seite weitergeleitet. Mein Problem/Frage: Kann man es im Menü so einrichten, dass Wenn sich Kursmitglied A anmeldet Kursliste A im Menü erscheint und bei Kursmitglied B Kursliste B und so weiter? Abgesehen von dem einmaligem Weiterleiten haben die Kunden danach keinen zugriff mehr darauf. Möchte das man diesen MenüPunkt nur sieht wenn man auch mit dem jeweiligem Kurs angemeldet ist. Habe mir dazu erst das Plugin Nav Menu Roles geholt, aber das Arbeit meines Wissens nur mit WordPressRollen wie Admin, Abonnent etc und nicht mit meinen erstellten Kurs-Rollen.
  Vielleicht kann mir ja jemand helfen. Danke schonmal im Voraus!
  Lg Antworten
  - Thorsten Faltings 10. August 2020 9:32 Moin Pascal,
    vielen Dank für Deine Nachricht. Wenn ich Dich richtig verstehe, hat jeder User seine eigenen Kurse, gelistet auf einer individuellen Seite. Du würdest als eine Erweiterung benötigen, die tatsächlich einen Menü-Eintrag ermöglicht, der für jeden angemeldeten User individuell ist. Ein passendes Plug-in haben wir bei einer schnellen Recherche nicht gefunden. Mit einer individuellen Entwicklung würde man das Problem aber sicher lösen können.
    Ahoi!
    Thorsten Antworten
    - Pascal 10. August 2020 20:27 Danke für die

schnelle Antwort!
Habe das Problem jetzt über einen kleinen Umweg gelöst!
Geholfen haben mir dabei die Plugins: Nav Menu Roles und User Role Editor.
habe für die jeweiligen Kurse eigene WP-Rollen erstellt und dann den erst über das Nav Menu gelöst.
Dennoch vielen Dank für die Hilfe! Antworten

- Thorsten Faltings 11. August 2020 8:46
  Sehr guter Lösungsansatz!
  Ahoi!
  Thorsten Antworten

- mpr_92 2. Mai 2020 4:40 Guten Tag, ich habe eine Frage zu den Plugins und der Vorgehensweise.
  Und zwar möchte ich jetzt nicht nur eine Datei zum Download freigeben, sondern ich würde gerne eine URL bzw. nur einen bestimmten Inhalt mit Zugriffen verwaltet. Kann ich in dem Download auch eine URL angeben? Ist das auch möglich?
  Und zweite Frage: In dem Donwload-Post kann man ja auch Inhalt im Textfeld eingeben (dort wo bei Ihnen aktuell Lorem Ipsum drin steht). Wie kann ich denn zusätzlich diesen Inhalt ausgeben? Gibt es da einen anderen Shortcode für?
  Herzlichen Dank für eine hoffentlich zeitige Rückmeldung. Antworten
- Lara-Maria Nestyak 24. März 2020 0:23 Erstmals vielen herzlichen Dank für diese ausführliche und wirklich sehr hilfreiche Anleitung!
  Eine Frage habe ich noch: Gehe ich auf den Link einer Kursseite für die ich nicht freigegeben bin, erscheint ja „Sie müssen sich anmelden, um diesen Inhalt zu sehen. Bitte Anmelden. Kein Mitglied?“ Dabei ist das Wort „Anmelden“ mit einem Hyperlink hinterlegt. Ich würde gerne statt „Kein Mitglied?“ etwas wie „Hier zur Kursbuchung klicken!“ eingeben – den Text kann ich ja

ganz einfach mit Poedit editieren, aber woher kommt der Link? Antworten

- Maximilian Pfützner 11. März 2020 16:02 Hallo,
  zunächst einmal vielen Dank für die super Anleitung! Soweit funktioniert auch alles, aber leider komme ich an einem Punkt nicht so richtig weiter:
  Wenn ich mich auf der Login-Seite befinde und mich als Nutzer einlogge gelange ich mit Hilfe der Login Redirection auch auf die jeweils richtig zugewiesene Seite. Das funktioniert allerdings leider nur, wenn den Passwortschutz der Seite deaktiviert habe. Sobald dieser allerdings aktiv ist, kommt nach dem Einloggen die Meldung „Sie müssen sich anmelden, um diesen Inhalt ansehen zu können. Bitte Einloggen. Noch kein Mitglied?“ daraufhin muss ich mich nochmal einloggen und komme nicht auf die voreingestellte Seite.
  Ich hoffe es ist soweit verständlich was ich damit sagen wollte und bin über jeden Hinweis sehr dankbar.
  Liebe Grüße,
  Max Antworten
- Stefan Paulus 21. Februar 2020 21:39 Hallo,
  ja das klingt sehr interessant. Was mich jedoch interessiert, ob es eine Möglichkeit gibt, registrierten Nutzern individuelle Inhalte, wie PDF Dokumente individualisiert in den jeweiligen Nutzerkonten zur Verfügung zu stellen. Wissen Sie hierzu eine Lösung oder Plugins die diese Möglichkeiten bieten?
  Viele Grüße
  Stefan Antworten
    - Stephanie Ta 4. Dezember 2020 10:29 Hallo Stefan,
      bist du schon damit weitergekommen? Wir haben ein Plugin, welches diesen Use Case abdeckt. Du brauchst eine fein-granulare Rollen-/Rechtevergabe. Melde dich gerne bei mir: an „Stephanie Ta“ unter https://login-master.com/kontakt/
      Liebe Grüße, Stephanie Antworten

- Franziska 3. November 2019 18:21 Hallo,
  die Anleitung war sehr hilfreich und gut erläutert.
  Leider komme ich an einer Stelle nicht weiter:
  >Um die Übrigen, für den Kunden unwichtigen, Infos auszublenden, wie zum Beispiel den Kontostatus etc., fügen Sie außerdem den folgenden Code ein:
  .swpm-logged-status, .swpm-logged-membership, .swpm-logged-expiry
  Der Code funktioniert bei mir leider nicht. Es kommt eine Fehlermeldung. Habe an dieser Stelle schon einiges probiert. Kann mir jemand weiterhelfen?
  Liebe Grüße Antworten
    - SDdorf 28. November 2019 14:54 Hallo Franziska,
      das gehört noch zu darüberliegenden Satz:
      Soll so – komplett – im css eingefügt werden:
      .swpm-edit-profile-link, .swpm-logged-status, .swpm-logged-membership, .swpm-logged-expiry {display:none;}
      Gruß SDdorf Antworten
- Julian 13. Oktober 2019 22:44 Guten Abend liebes Team!
  Erstmal vielen herzlichen Dank für die ausführliche Anleitung.
  Nun scheint erstmal alles sehr praktisch und simpel.
  Mein Anwendungsbereich scheint aber etwas von der beschriebenen Situation abzuweichen. Ich möchte insggesamt 140 Benutzer anlegen, die in verschiedene Gremien aufgeteilt sind (Kommissionen und Departemente)
  Muss ich jetzt für jeden einzelnen Benutzer ein Passwort anlegen und es ihm später per Mail zukommen lassen, damit er sich überhaupt einloggen kann?
  Ich habe schon die Variante mit der E-Mail Aktivierung getestet. Praktisch! Nur leider muss sich jeder Benutzer, noch bevor er einen Aktivierungslink erhält das erste Mal einloggen. Sprich: Er braucht die Login Daten. Gibt es eine Möglichkeit, dass der Benutzer das Passwort selbst anlegen kann? Ist es möglich dem Benutzer den Aktivierungslink samt Login Daten

automatisch zu versenden?
Euer Rat wäre sehr hilfreich. Ansonsten bin ich wohl gezwungen, sämtlichen 140 angelegten Benutzern ein Passwort zu versenden :/
Ich wünsche euch einen erholsamen Abend und schon jetzt danke für das Feedback!
Julian Antworten

- Andreas 27. März 2019 12:17 Hi, super Anleitung und sehr schöne PlugIns.
  Als work around für das Log Out Problem geht mit der neuesten WordPress Version (5.1.1) folgender Weg:
  1. Role der Mitglieder unter dem Punkt Menüpunkt Benutzer als – Keine Benutzerrolle für diese Website – festlegen
  2. Die Adminbar unter WP Mitgliedschaft Einstellungen auf anzeigen setzen (default Einstellung).
  Die Bar beinhaltet nun nur ein Bild, Name und AUSLOGGEN Feld. Die Bar kann natürlich per css nach Stylewünschen angepasst werden. Antworten
- Manu 25. März 2019 17:40 Ich habe in einem Anfall geistiger Umnachtung aus Versehen die Login-Seite gelöscht, dabei hatte ich alles schon schön eingestellt und funktionierte prima. Ich habe das Plugin „Simple-Membership“ gelöscht und wieder installiert. Aber das generieren der Login-Seite bleibt aus. Was kann ich jetzt machen? Hoffentlich kannst Du mir helfen. Antworten
  - Thorsten Faltings 26. März 2019 11:40 Moin Manu,
    liegt die Seite vielleicht noch im „Papierkorb“ und wird deswegen nicht neu angelegt?
    Ahoi!
    Thorsten Antworten
- Sabrina Tausch 15. März 2019 10:35 Hallo, wirklich toller Beitrag!
  Ich hoffe ihr könnt mir bei meinem Problem weiterhelfen. Wenn ich die Loginseite aufrufe, steht bei mir im Feld „Benutzer“ immer der Benutzer drinnen mit dem ich die

WordPress Seite erstellt habe, es ist mir nicht möglich diesen raus zu löschen und mich mit einem anderen Benutzer anzumelden. Das Feld reagiert einfach nicht. Antworten

- Thorsten Faltings 15. März 2019 15:43 Moin Sabrina,
  kann es sein, dass Du in WordPress eingeloggt bist?
  Melde Dich ab und teste dann das Login.
  Ahoi!
  Thorsten Antworten

- Stefanie S. 14. März 2019 17:17 Hallo Kim, Hallo Thorsten,
  SUPER geschrieben! Ich habe nur noch eine Frage: Ich würde gerne eine E-Mail Benachrichtigung erhalten, wenn einer unserer Kunden ein Dokument herunterlädt. Wie kann ich das am besten machen?
  DANKE und liebe Grüße,
  Steffi Antworten
  - Thorsten Faltings 14. März 2019 17:20 Moin Steffi,
    das ist keine schlechte Idee. Leider gibt es in dem Plug-in keine entsprechende Funktionalität.
    Vielleicht schlägst Du dem Entwickler Deine Idee mal vor?
    Ahoi!
    Thorsten Antworten

- Micha 11. März 2019 11:01 Hallihallo Thorsten,
  ich bin ja begeistert von eurer sehr gut erklärten Lösung zum Thema geschützter Kundebereich.
  Nun habe ich als Admin, noch einige Mitarbeiter im RedakteurStatus welche dann auf einmal nicht mehr regulär über den WP Login auf ihr Dashboard Bereich kommen. In den „allgemeinen Einstellungen“ der WP Mitgliedschaft habe ich dann das Häkchen im Bereich „Deaktivieren Sie den Zugriff auf das WP Dashboard“ entfernt, sodass meine Mitarbeiter wieder über den WP Login regulär ihren Zugang erhalten.

Leider kann dann das reguläre Kursmitglied, sofern sie den WP Login URL (aus Sicherheitsgründen wurde die URL um geändert) kennen würden, auf ihr abgespecktes Dashboard Profil zugreifen, was ja eigentlich nicht sooo sein soll.
Ich hatte auch den Weg über die „Erweiterte Einstellung“ bei der WP Mitgliedschaft versucht, wo ich unter „Admin-Dashboard Zugriffsberechtigung“ den Zugriff meiner Redakteure zu ermöglichen versuchte. Vorher hatte ich das Häkchen im „Deaktivieren Sie den Zugriff auf das WP Dashboard“ wieder aktiviert. Irgendwie klappt erstaunlicherweise die Option auch nicht. Eine weitere Idee bzw. Kombination mit dem PlugIn „User Role Editor“ war vergebene Müh.
Habe ich irgendwas in den WP Mitgliedschafts-Einstellungen übersehen, sodass meine Mitarbeiter „Redakteuren“ weiter ungehindert sich über das reguläre WP Login einloggen können, wiederum das „gemeine“ Kursmitglied nur das zu sehen bekommt, was es soll und keine weiteren Möglichkeiten im BackEnd bzw im Dashboard rumzuwuseln?
Danke vor ab.
Herzliche Grüße vom Niederrhein
Micha Antworten

- Thorsten Faltings 15. März 2019 15:48 Moin Micha,
  Hmm, hast Du mal das Plug-in „Remove Dashboard Access“ probiert? Solltest Du Dich mit Anpassungen in der functions.php auskennen gibt es hier sonst noch einen alternativen Lösungsvorschlag: Disable WordPress dashboard for subscribers.
  Ahoi!
  Thorsten Antworten
  - Micha 18. März 2019 10:27 Moin Thorsten,
    Danke für die beiden Tipps. Et funktioniert. Hervorragend. Ick freu mir.
    Danke nochmals
    Herzlichen Gruß

Micha Antworten

- Daniel von bo:mi:well® 8. März 2019 13:59 Hallo Kim,
  hallo Thorsten,
  jetzt habe ich auch endlich meine Downloads geschützt. Das Einrichten hat gut funktioniert, nur hätte ich gerne, dass die Downloads wie bisher in einem neuen Tab geöffnet werden. Es handelt sich nämlich bei den Downloads um PDF- und MP3-Datein, die der Browser automatisch öffnet. Bisher hatte ich einfach den target="_blank"-Zusatz in meinem Link drin stehen gehabt. Dieser funktioniert aber in dem shortcode nicht. Und leider konnte ich weder in den Einstellungen des Download-Plugins noch auf den Seiten der einzelnen Downloads die Option finden.
  Natürlich kann man einfach wieder auf „Die vorherige Seite anzeigen" klicken, nachdem sich die Datei im Browser geöffnet hat. Nur kann es eben auch gut sein, dass jemand den Tab dann schließt, nachdem er festgestellt hat, dass sich die Datei „nur geöffnet hat" und sie nicht heruntergeladen wurde. Und dann hat er eben auch ungewollt meine Seite geschlossen.
  Liebe Grüße
  Daniel Antworten
    - Thorsten Faltings 8. März 2019 16:51 Moin Daniel,
      ich habe es soeben getestet und bei mir hat nicht der Browser (Safari) die Datei angezeigt, sondern einen Download initiiert.
      Hast Du mal den Link (URL) über dem Shortcode kopiert und ausprobiert? Hat bei mir funktioniert.
      Ahoi!
      Thorsten Antworten
- ungoliant 8. März 2019 12:34 Hallo,
  toller Beitrag! Genau das was ich suche!
  Gibt es auch eine Möglichkeit einen Mitglied mehrere Mitgliedsstufen zuzuweisen?
  cheers ungoliant Antworten
    - Thorsten Faltings 8. März 2019 16:52 Moin,

meines Wissens ist das nicht möglich. Am besten die Mitgliedsstufen so planen, dass sie die Möglichkeiten der anderen Stufen beinhalten und noch jeweils weiter Optionen bieten. So nach dem Motto Bronze, Silber, Gold.
Ahoi!
Thorsten Antworten

- Gaby 4. März 2019 11:32 Moin Thorsten,
vielen Dank, für die schnelle Reaktion!
Es geht darum, dass für einen Lehrgang, der in Blockwochen stattfindet, für die jeweilige Woche alle Skripte heuntergeladen werden sollen.
Ich würde also gerne alle betreffenden Dateien z.B. unter dem Download Titel „Skripte Woche 1“ hochladen und den Shotcode, unter dem ja jetzt evtl. 5 Dateien gespeichert sind, in die Download Seite für die Teilnehmer einfügen.
Oder muss ich für jedes einzelne Skript einen eigenen Shortcode einfügen?
Ich würde dann aber nicht den Sinn verstehen, dass unter einem Download Titel mehrere Dateien hochgeladen werden können, wenn tatsächlich nur eine downgeloadet werden kann.
Schon jetzt vielen Dank für Deine Geduld mit mir ….
Beste Grüße
Gaby Antworten
    - Thorsten Faltings 4. März 2019 11:43 Moin Gaby,
    alles gut
    Dann würde ich die Unterlagen in eine ZIP-Datei zusammenfassen.
    Ahoi!
    Thorsten Antworten
- Gaby 3. März 2019 20:12 Hallo Kim,
es ist zwar schon oft gesagt, aber trotzdem nochmal:
Vielen Dank für die super Anleitung!
Leider komme ich mit einem Problem nicht weiter.
Ich habe über den Download Monitor mehrere Dateien

hochgeladen und den Shortcode auf die Download Seite kopiert. Aber nur die erste Datei kann heruntergeladen werden. Alle anderen erscheinen erst gar nicht.
Im Dashboard erscheint unter Downloads bei „Datei“ auch nur eine Datei.
Muss ich bei der Bereitstellung von mehreren Dateien denn vielleicht noch weitere Einstellungen im Download Monitor vornehmen? Antworten

- Thorsten Faltings 4. März 2019 9:00 Moin Gabi,
  erstmal vielen Dank für Dein Lob!
  Wir sind nicht sicher, ob wir Dein Problem richtig verstehen, haben aber eine Vermutung:
  Kann es sein, dass Du alle Dateien zu einem „Download“ zusammengefasst hast? Versuche mal für jede Datei einen eigenen „Download“ anzulegen und entsprechend die jeweiligen Shortcodes einzufügen.
  Ahoi!
  Thorsten Antworten

- Peter Lehmann 20. Februar 2019 14:51 Hallo, ich wollte ein Mitglied manuell über das Plugin anlegen. Das funktioniert nicht. Es wird aber jedesmal eine admin.php Datei heruntergeladen. Was mache ich falsch?
  Hintergrund ist der, dass ich die Kunden manuell anlegen will. Nicht jeder bekommt einen Zugriff auf eine Seite.
  Kann man auch jedem Benutzer eine spezielle Seite anzeigen? Antworten
- Maja 17. Januar 2019 17:47 Hallo Kim,
  vielen Dank für den tollen Beitrag. Ist total hilfreich!
  Bei mir hakt es nur noch an einer Stelle…
  Wenn ein Besucher ohne einggeloggt zu sein die Download-Seite aufruft erscheint da der Satz: „Sie müssen sich anmelden …“. Und sonst nichts. Gibt es eine Möglichkeit in diesem Fall direkt auf die Login Seite umzulenken?
  Gruß Maja Antworten

  - Thorsten Faltings 18. Januar 2019 14:50 Moin Maja,
    Du kannst beim Download-Plug-in unter *Einstellungen > Zugriff* den Text anpassen und eine

entsprechende Verlinkung zur gewünschten Login-Seite einfügen.
Ahoi!
Thorsten Antworten

- Ronny Meyer 27. Dezember 2018 20:05 Hallo Kim. Vielen Dank für Deine Anleitung. Sehr gute Sache.
  Leider habe ich ein Problem: wenn ich den Shortcode in der Seite einfüge, und danach darauf klicke passiert nichts… was habe ich falsch gemacht?
  Gruss Ronny Antworten
- Konstantin 1. Dezember 2018 3:25 Hallo,
  toller Artikel! Sehr ausführlich und gut beschrieben.
  Eine Frage hätte ich dennoch. Mit welchem Plugin kann ich die automatische Registrierung ermöglichen?
  Es steht zwar eine Seite namens Registration zur Verfügung, nur enthält diese kein Formular. Antworten
- Daniel von bo:mi:well® 16. November 2018 18:17 Liebe Kim, ich danke dir vielmals für diesen tollen Artikel!
  Ich hatte mich vor einigen Monaten schon mal damit beschäftigt und es dann verzweifelt aufgegeben. Heute morgen bin ich dann auf diese absolut perfekte Anleitung gestoßen und konnte die Einrichtung dann auf meiner Seite zur vollsten Zufriedenheit durchführen. Wirklich toll erklärt – sowas findet man leider zu selten.
  Einen Spenden-Button für eine „Tasse Kaffe“ gibts nicht auf der Seite, oder?
  Würde mich gerne erkenntlich zeigen. Habe fast ein schlechtes Gewissen, dass ich diese tolle Anleitung einfach kostenlos erhalten habe.
  Liebe Grüße
  Daniel von bo:mi:well® Antworten
    - Kim Salewski 19. November 2018 9:22 Moin Daniel,
      Es freut mich sehr zu hören, dass die Anleitung eine Hilfe und verständlich ist! Deine Hilfestellung für Ben ist reicht uns vollkommen als Entlohnung Wir freuen uns, wenn durch unseren Beitrag und die vielen hilfreichen

Kommentare offene Fragen geklärt werden können.
Viele liebe Grüße,
Kim Antworten

- Olaf 12. November 2018 18:21 Hallo, super Beitrag… Ich habe das nun auf meiner Seite auch hinbekommen, danke dafür.
  Eine Frage hab ich noch dazu, wie bekomme ich es hin das sich ein User mehr als einmal anmeldet? Sozusagen ein User für eine Gruppe… geht das? Antworten
- Alexander Mäding 8. November 2018 12:30 Hallo,
  kann ich auch eine Seite erst nach 7 Tagen nach der ersten Anmeldung freischalten?
  LG Alexander Antworten
  - Thorsten Faltings 12. November 2018 11:20 Moin Alexander,
    ja, oben rechts im Kasten „Veröffentlichung“ kannst Du ein Veröffentlichungsdatum festlegen.
    Ahoi!
    Thorsten Antworten
- Der Waldi 7. November 2018 12:18 Vielen vielen Dank für diesen Beitrag. Du hast mir sehr geholfen.
  Ich habe nur noch eine Frage.
  Kann ein Mitglied mehreren Mitgliedsstufen angehören?
  Ich möchte auf der Seite mehrere Kurse anbieten, die alle Separat bestellt werden können. Was passiert, wenn ein Mitglied einen zweiten Kurs bestellen möchte. Muss ich das Mitglied neu anlegen mit einer anderen Mailadresse, oder gibt es die Möglichkeit das man ihm einfach den zweiten Kurs zuweist?
  Danke nochmal Antworten
  - Daniel von bo:mi:well® 7. März 2019 11:11 Hallo Waldi,
    genau vor diesem Problem stand ich auch. In dem Plugin lässt sich ja immer nur eine Mitgliedschaftsstufe auswählen. Man kann leider nicht mehrere anklicken.
    Meine Idee war dann einfach eine weitere

Mitgliedschaftsstufe anzulegen. Und alle Seiten, die den beiden anderen Mitgliedschaftsstufen jeweils zugeordnet sind, auch der neuen zuzuordnen.
Im meinem Fall sah das so aus:
1. Mitgliedschaftsstufe: Tagesworkshop Rückenschule (Seiten A, B, C)
2. Mitgliedschaftsstufe: Faszientraining Workshop (Seiten 1, 2, 3)
3. Mitgliedschaftsstufe: Tagesworkshop Rückenschule und Faszientraining (Seiten A, B, C und Seiten 1, 2, 3)
Ich habe dann eine Auswahl-Seite erstellt, auf der ich die Links zu beiden Workshops eingefügt habe. Diese Seite wurde dann zu der Redirection-Page der Mitgliedschaftsstufe. Und damit man von einem Workshop zum anderen wechseln kann, habe ich diese Auswahlseite in meiner Seitenleiste verlinkt.
So funktioniert es jetzt eigentlich ganz gut.
Ich weiß zwar nicht, ob ich einen solchen Kommentarbereich nutzen darf, um Werbung zu machen – falls es nicht erwünscht sein sollte, dann entschuldige ich mich dafür und dann darf der Kommentar natürlich gelöscht werden – aber vielleicht gibt es hier ja jemanden, der gerne seine Rückenschmerzen loswerden möchte.
bomiwell.de/ruecken
Liebe Grüße
Daniel von bo:mi:well® Antworten

- Thorsten Faltings 7. März 2019 11:16 Moin Daniel,
  es ist tatsächlich so, dass wir hier normalerweise keine Werbung zulassen.
  Da uns aber Dein Lösungsweg gefallen hat, drücken wir mal ein Bullauge zu
  Ahoi!
  Thorsten Antworten

- Sandra Oelschläger 5. November 2018 8:51 Einfach nur ein riesiges Danke für den Beitrag! Sehr übersichtlich und leicht nachzumachen. Danke!
  Liebe Grüße
  Sandra Antworten
- Akinom 11. September 2018 13:25 Tolle Anleitung.
  Gibt es auch die Möglichkeit, Berechtigungen (Veröffentlicht, Privat) nachträglich außerhalb des Dashboards zu ändern? Möchte einem eingeloggten Nutzer die Möglichkeit geben, seine privaten Elemente der Seite zu veröffentlichen. Antworten
    - Thorsten Faltings 11. September 2018 14:27 Moin Akinom,
      grundsätzlich ist das möglich, bedarf aber der Programmierung.
      Ahoi!
      Thorsten Antworten
- Herbert 6. September 2018 20:52 Diese Anleitung ist wirklich Spitze. Die stimmt wirklich bis ins Detail. Herzlichen Dank dafür. Ich habe über dem Problem einige Tage gebrütet und diverse Member Plugins inkl. Anleitungen ausprobiert. Nur diese Weg war erfolgreich, und dann sogar noch ohne Kosten. Ich kann auch kaum glauben, dass ein solches tolles Plugin kostenfrei ist. Obwohl mein Kunde plötzlich andere Anforderungen stellt, die wahrscheinlich so nicht realisierbar sind, werde ich diese Lösungen mit Sicherheit bei anderen Projekten umsetzen. Antworten
- Lennart 20. August 2018 19:27 Super Erklärung, danke dafür!
  Mein Problem ist nur gerade, dass ich selbst wenn ich eingeloggt bin, die Dateien nicht Downloaden kann. Es erscheint die Meldung: „Du besitzt nicht die nötige Berechtigung, um auf diese Download-Datei zuzugreifen. Gehe zur Startseite“.
  Ich bin der Meinung, ich hätte alles richtig eingestellt… :/ Antworten

- Christian 20. Juli 2018 17:17 Hallo,
  können bei Simple Membership auch Einstellungen vorgenommen werden, dass die angelegten Mitglieder automatisch per Email darüber informiert werden dass sie angelegt wurden und ihnen auch der Benutzername und das Passwort mitgeschickt wird?
  VG
  Christian Antworten
- Dia 20. Juli 2018 8:49 Vielen Dank für die ausführliche und sehr gut verständliche Anleitung!
  Ich habe nun alles so eingerichtet, jedoch haben sich zwei Probleme aufgetan:
  1.) Nachdem der Abonnent eingeloggt ist kommt er nochmals auf eine Seite, wo das Passwort wieder abgefragt wird. „Dieser Inhalt ist passwortgeschützt. Um ihn anzuschauen, gib …..“… und wie gesagt, er muss nochmals das vorher bereits eingegebene PW eingeben.
  2.) es gibt keine Möglichkeit sich auszuloggen. Erst wenn der Abon. wieder auf die Login-Seite zurückkehrt kann er sich ausloggen. Gibt es da eine einfache Lösung mit einem Button oder Link, den ich einfügen kann? (Bitte Dummie-Version …)
  Vielen Dank und sonnige Grüße,
  Dia Antworten
    - Kim Salewski 20. Juli 2018 8:59 Moin Dia,
      Zu 1) kann ich leider nicht viel sagen. Die oben beschriebene Methode mit dem Redirect und dem aktivieren der Zugriffseinstellungen für eine bestimmte Mitgliedschaft haben dieses Problem bei uns bisher nicht hervorgerufen.
      Zu 2) gibt es lediglich diese Möglchkeit. Du kannst es deinen Besuchern etwas erleichtern, indem du die Menüführung anpasst. Hierzu einer meiner früheren Kommentare:
      „Es ist wahr, das Ausloggen findet bei diesem Plug-in/bei dieser Methode auf der Log-in Seite statt. Wenn man auf diese klickt, findet man dort

den “Ausloggen” Link.
Eine Möglichkeit, das Ausloggen für Benutzer logischer zu gestalten wäre:
1. Du benennst die Seite “Log-in” in “Konto” um.
oder
2. Du nutzt das Plug-in “Nav Menu Roles”, mit dem du angeben kannst, welcher Menüpunkt angemeldeten und welcher Menüpunkt abgemeldeten Besuchern angezeigt wird. Hier kannst du zwei mal den Link “Log-in” zu deinem Menü hinzufügen, den ersten shaltest du für abgemeldete Besucher sichtbar. Den zweiten benennst du um in “Log-out” um und schaltest ihn für angemeldete Benutzer sichtbar. So sehen abgemeldete Besucher “Log-in”, und angemeldete Besucher “Log-out” im Menü stehen.“
Ich hoffe, das konnte dir etwas weiterhelfen.
Viele liebe Grüße,
Kim Antworten

- Josef S. 12. September 2018 12:01 Hallo zusammen,
  was ich gemacht habe, um sich bequem auszuloggen:
  Den „Ausloggen“-Link von der Profilseite kopiert und auf der gesicherten Seite in einen „Ausloggen“-Button eingefügt. Funktioniert einwandfrei und ist sehr übersichtlich
  LG Josef Antworten

- Ben 19. Juli 2018 9:51 Salut,
  Danke erstmal für die hammer Erklärung, war sehr leicht alles umzusetzten.
  Jetzt habe ich die Herrausforderung das ich, User habe die recht alt sind, und mit dem PC oft nicht klarkommen. Heißt Sie Loggen sich ein, machen dann aber irgendwas anderes, und gehen nach einer gewissen Zeit wieder auf dem LINK… den wir ihnen geschickt haben. Jetzt kommen sie aber auf dem Benutzerprofil raus, und nicht mehr auf

der Redirekt-Seite. Manche sind nicht in der Lage den Logout button zu finden, egal wie groß man den macht -_- …
meine Idee wäre eine Art: Autologout! Nach einer gewissen Zeit oder wenn mann den Tab oder das Fenster schließt oder so-….. !
Hat jemand das schonmal gemacht, und hat dazu tips oder ideen? Danke schonmal…
mit freundlichen Grüßen
Ben Antworten

- Daniel 16. November 2018 18:07 Hi Ben,
  deine Frage ist zwar schon ein paar Monate alt, ich wollte an dieser Stelle aber dennoch eine Antwort darauf geben, da ich selbst auch eine solche Funktion haben wollte. Und vielleicht möchte es der eine oder andere, der in der Zukunft einen solchen Mitgliederbereich erstellen möchte, ebenfalls. Ich habe ihn selbst erst heute morgen eingerichtet, nachdem ich auf diese TOLLE Anleitung stieß.
  Nun endlich zur Antwort:
  Unter Einstellungen/Erweiterte Einstellungen hat man die Möglichkeit „Logout Member on Browser Close“ zu aktivieren.
  Viele Grüße
  Daniel von bo:mi:well® Antworten

- Dennis 5. Juli 2018 14:58 Hallo Kim und vielen Dank für die tolle Anleitung.
  Ich suche aktuell noch nach einer Möglichkeit auszulesen welcher membership der angemeldete User angehört um damit zu steuern welche Bereiche ihm angezeigt werden, bzw. ob der dynamisch generierte Content für ihn angezeigt werden soll.
  Also sowas wie aktuellerUser.get_membership();
  Um quasi abzufragen:
  $args = array(
  ‚post_parent‘ => $post->ID,

```
,post_type‘ => ,page‘,
,orderby‘ => ,menu_order‘
);
$child_query = new WP_Query( $args );
while ( $child_query->have_posts() )
{
if (get_membership() == „1“)
{
echo “ . get_the_excerpt() . “;
echo ,mehr erfahren,;
}
}
```

Hast Du da eine Idee?
Danke,
Dennis Antworten

- Kim Salewski 5. Juli 2018 15:16 Moin Dennis,
  So weit haben wir uns mit diesem Thema in Hinblick auf Simple Membership nicht auseinandergesetzt. Unser Beispiel war deutlich simpler und hat diese Funktion nicht benötigt.
  In diesem Falle lege ich dir eher nahe, dir ein umfangreicheres Plug-in zu suchen, was diese Funktion bereits mit sich bringt.
  Alternativ stelle deine Frage lieber in dem entsprechenden Plug-in Support-Forum: https://wordpress.org/support/plugin/simple-membership
  Viele liebe Grüße,
  Kim Antworten
  - Dennis 5. Juli 2018 17:04 Moin Kim,
    ich habe es inzwischen lösen können. In der Klasse SwpmMemberUtils gibt es eine Methode dazu. Damit bekommt man die gewünschte ID.
    Musste mich halt durch die Klassen lesen, da sind so einige Methoden, die man gut nutzen oder ändern und nutzen kann.
    Die Lösung ist dann z.B. so:

$member_id = SwpmMemberUtils::get_logged_in_members_id();
Dann kann ich mit der Varible weiterarbeiten.
Danke und viele Grüße,
Dennis Antworten

- Carsten 12. Juni 2018 18:08 Hallo, wunderbar erklärt und verständlich.
  Ich möchte allerdings, dass bestimmte eingeloggte Klienten nur den für sie bestimmten Inhalt sehen können … nicht in Gruppen – aber in Klienten unterteilt. Müsste ich dazu eigene Mitgliedschaftsstufen für jeden Klienten einrichten? Und dann die Startseite nach dem einloggen für jeden Klienten individuell einrichtenß
  GLG, Carsten Antworten
    - Kim Salewski 13. Juni 2018 8:53 Moin Carsten,
      Für einen einzelnen Klienten müsstest du ebenfalls ein eigenes Mitglied und eine eingene Mitgliedschaft anlegen, nach dem Prinzip oben, und dann lediglich diesem Klienten den Zugang zukommen lassen. Je nach dem, wie viele Klienten du hast, könnte das vielleicht unübersichtlich werden. Daher müsstest du hier wahrscheinlich eine andere Lösung in betracht ziehen.
      Viele liebe Grüße,
      Kim Antworten
        - Carsten 13. Juni 2018 11:24 Hallo Kim,
          vielen Dank für die schnelle Antwort. Da ich nur einem recht kleinen Kreis Zugang gewähren werde, nutze ich erst einmal SimpleMembership. Ich habe nach anderen Tools geschaut – diese sind dann zu umfangreich. So viel Aufhebens brauche ich am Ende nicht.
          Hugs, Carsten Antworten
- oliver 2. Juni 2018 1:41 Hallo Ihr Lieben,
  ihr habt mir mit dieser Anleitung sehr weitereholfen!

Vielen Dank dafür. 2 Fragen hätte ich noch dazu:
a) ich wollte ebenfalls den Text „Erinneren Sie mich…“ + dem Würfel unter dem Login rausnehmen.Das mit dem Text hatauch mit der mo. Datei funktioniert. Habt ihr eine Idee, wie ich den Würfel weg bekomme?
b) wenn ich die Seite nun durch den Login geschützt habe und ebenfalls den Seitenschutz aktiviert habe, können Inhalte wohl trotzdem gesehen werden? Inhalte auf der Seite wie Produkte, Inhalte etc.?
Vielen Dank schon mal für die Antwort(en) und liebe Grüße OG Antworten

    - Lukas 19. November 2019 11:58 Hallo Oliver,
      ich habe das selbe Problem wie in deiner Frage a). Hast du mittlerweile eine Lösung gefunden? Bzw. welche mo. Datei meinst du?
      Vielen Dank vorab und liebe Grüße
      Lukas Antworten

- Daniel 29. Mai 2018 18:37 Hallo,
  sehr hilfreicher Beitrag. Ich nutze nun auch einen WordPress Mitgliederbereich, da ich nun einen Online-Kurs erstellt habe und diesen nur ausgewählte Leute sehen sollen. Also ich finde das Plugin klasse. Eigentlich war WordPress ja früher eher für Blogger gedacht und durch ein Membership Plugin wie Digimember kann man gleich viel mehr daraus machen.
  Beste Grüße
  Daniel Antworten
- Vanessa 16. Mai 2018 10:49 Halli hallo,
  vielen Dank für die wunderbare und ausführliche Anleitung. In meinem Fall möchte ich keine Downloads anbieten, sondern nur eine Seite für verschiedene (von mir vorgegebene Nutzer) zugänglich machen.
  Ich möchte allerdings gerne verfolgen können wer sich wann eingeloggt hat. Gibt’s dafür eine Möglichkeit?
  Vielen Dank schon mal Antworten

    - Thorsten Faltings 16. Mai 2018 13:51 Moin Vanessa,
      das ist mit diesem Plug-in Simple Membership

unseres Wissens nicht möglich.
Außerdem solltest Du über diese Idee im Zuge von DSGVO noch einmal nachdenken.
Ahoi!
Thorsten Antworten

- Vanessa 16. Mai 2018 14:29 Vielen Dank für die schnelle Antwort.
  Gibt es ein Plugin mit dem eine solche Auswertung möglich wäre? Antworten
  - Thorsten Faltings 16. Mai 2018 14:32
    Wir kennen so ein Plug-in nicht.
    Antworten

- Marcel 9. Mai 2018 11:51 Hallo Kim,
  Danke für die tolle Anleitung. Kann man beim Download Monitor auch festlegen, welcher Benutzer welche Downloads abrufen kann? Ich habe 2 verschiedene Benutzer, die jeweils nur bestimmte Downloads abrufen können sollen. Das sie nur die gewünschten Seiten sehen funktionioniert ja über Simple Membership gut. Aber falls jetzt jemand über den Permalink zum Download verfügt, kann er die Datei runterladen egal als welcher Nutzer er eingeloggt ist. Gibt es eine Lösung, dass man die Datei nur runterladen kann, wenn man als der richtige User eingeloggt ist? Danke. Antworten
  - Thorsten Faltings 14. Mai 2018 12:53 Moin Marcel,
    wie im Beitrag beschrieben, können den beiden Benutzern unterschiedliche Seiten zugewiesen werden. Allerdings: kennt Benutzerin A von Benutzer B die Download-Links und ist eingeloggt, dann hätte sie auch Zugriff auf die Dateien. Soll auch diese Situation verhindert werden, müsste man sich eine alternative Strategie ausdenken.
    Ahoi!
    Thorsten Antworten
    - Marcel 14. Mai 2018 20:20 Moin Torsten,
      ok danke für die Bestätigung des Sachverhalts. Dann habe ich erst mal nix

falsch eingestellt. Antworten

- Thomas 2. Mai 2018 20:36 Sehr schöne Lösung, genau was ich gesucht habe. Vielen Dank! Antworten
- Uwe 11. April 2018 5:27 Klasse Script was ich schon lange gesucht habe, alles eingebaut und es funktioniert… Was aber nicht funktioniert ist der Logout über die „Kontoseite“, klicke ich auf Logout leitet dieses mich um auf eine Seite meines Webhosters https://meinedomain.de/?swpm-logout=true ist der Link der dahinter liegt und weitergeleitet werde ich zu: http://s79.goserver.host/neutral/
  Hab ich da einen Denkfehler oder ist es etwas anderes?
  Danke schon mal Antworten
    - Uwe 11. April 2018 6:17 Hab den Fehler selber gefunden, lag am httpS… habs im Script selber rausgenommen Antworten
- Stefan 23. März 2018 18:34 Ein wirklich toller Beitrag, vielen Dank! Ich habe ihn soweit umgesetzt und angepasst, und es funktioniert auch alles, bis auf ein Problem: Wenn ich mich über meinen Desktop-PC einlogge, oder über verschiedene Apple-Tablets oder ein Samsung-Smartphone, werde ich zur angegebenen Seite weitergeleitet und bin eingeloggt, aber es funktioniert nicht über ein iPhone, dort wird mir immer der Hinweis ausgegeben, dass ich mich anmelden müsste, und ich kann mir das nicht erklären. Hat jemand dieses Problem auch, oder kann mir dazu Hilfestellungen geben? Vielen Dank im Voraus! Antworten
- Klaus 22. März 2018 17:17 Ich habe einfach auf der Download-Seite den Logout-Buttom eingefügt, einmal am Anfang und einmal am Ende. Antworten
- Nicole 22. März 2018 15:45 Hallo Kim, das ist ein super Beitrag – es steht alles drin, einfach und sehr nachvollziehbar erklärt TOP.
  Nur eine Frage habe ich: Ich bin 1 zu 1 den Schritten gefolgt und es funktioniert super und ist genau das, was ich benötige. Wenn ich mich als Tester einlogge, wird

mir aber leider kein Logout Button angezeigt.
Wo steckt der denn? Muss ich den extra ausweisen oder programmieren?
Danke für eine Rückmeldung.
Grüße Nicole Antworten

- Kim Salewski 22. März 2018 16:57 Liebe Nicole,
  das ist wahr, das Ausloggen findet bei diesem Plug-in/bei dieser Methode auf der Log-in Seite statt. Wenn man auf diese klickt, findet man dort den „Ausloggen“ Link.
  Eine Möglichkeit, das Ausloggen für Benutzer logischer zu gestalten wäre:
  1. Du benennst die Seite „Log-in“ in „Konto“ um.
  oder
  2. Du nutzt das Plug-in „Nav Menu Roles“, mit dem du angeben kannst, welcher Menüpunkt angemeldeten und welcher Menüpunkt abgemeldeten Besuchern angezeigt wird. Hier kannst du zwei mal den Link „Log-in“ zu deinem Menü hinzufügen, den ersten shaltest du für abgemeldete Besucher sichtbar. Den zweiten benennst du um in „Log-out“ um und schaltest ihn für angemeldete Benutzer sichtbar. So sehen abgemeldete Besucher „Log-in“, und angemeldete Besucher „Log-out“ im Menü stehen.
  Ich hoffe, das konnte dir etwas weiterhelfen.
  Viele liebe Grüße,
  Kim Antworten
  - Nicole 28. März 2018 12:00 Hallo Kim,
    danke für die Rückmeldung. Sorry, ich konnte noch nicht an der Website weiterarbeiten – aber am Wochenende setze ich mich wieder ran. Gerne sag ich Bescheid, ob und wie ich es geschafft habe
    Danke nochmals für deine Zeit und die Tips.
    Grüße,
    Nicole
    @Klaus: Das klingt auch wie eine gute simple

Lösung. Antworten

- Constanze Straub 23. Februar 2018 11:00 Hallo Kim,
  ganz genau weiß ich nicht, was du meinst: Wenn ich mich als Mitglied ausloggen möchte, klicke ich im Menü oben auf „Logout“. Dann erscheint, wie auch vor Installation des Plugins, die Seite mit dem Befehl „Abmelden“. Hatte ich vor Installation des Plugins darauf geklickt, wurde ich tatsächlich auf die Startseite geführt. Jetzt wie gesagt werde ich auf die WP-Anmeldeseite geführt. Da ist also irgendwo ein Fehler, ich weiß nur nicht wo…
  Liebe Grüße,
  Constanze Antworten
  - Kim Salewski 23. Februar 2018 11:09 Hallo Constanze,
    Leider kann ich dir da nicht weiter helfen.
    Das Plug-in Nav Menu Roles hat lediglich die Funktion freigeschaltet, dass Menüpunkte für angemeldete/abgemeldete Besucher angezeigt werden. An dem Abmelden-Link auf der Log-in Seite von Simple Membership hat es (bei uns) nichts geändert.
    Leider kann ich hier nur sagen „Probieren geht über Studieren“. Teste, ob der Link wieder funktioniert, wenn das Plug-in Nav Menu Roles deaktiviert ist. Wenn ja, suche nach einem anderen in dieser Richtung.
    Viele Liebe Grüße,
    Kim Antworten
    - Constanze Straub 23. Februar 2018 11:18 Hallo Kim,
      ist schon okay, Support kann ich ja nicht erwarten. Du hast mir so schon sehr weitergeholfen, danke nochmals. Ich habe gerade das Plugin deaktiviert und das Problem existiert trotzdem noch. Muss also noch probieren und den Fehler suchen.
      Danke und liebe Grüße,

Constanze Antworten

- Constanze Straub 23. Februar 2018 8:28 Hallo Kim.
  Ein grandioser Beitrag! Sehr gut und sehr detailliert erklärt. Mein Kompliment. Ich stehe gerade vor genau dieser Herausforderung: ein Mitgliederbereich. Noch dazu auf einer dreisprachigen Seite. Ich habe dieses Plugin ausprobiert und es scheint zu funktionieren. Meine Aufgabe: Ein Teil der Website soll nur Mitgliedern zugänglich sein. Wie im obereren Beispiel brauche ich kein Passwort etc., das macht der Admin.
  Mein Problem ist: Wie ändere ich das Menü im Mitgliederbereich, damit dort zum Ausloggen nicht „Login“ steht, sondern eben „Logout“. Momentan komme ich auf die Seite zum Ausloggen, indem ich auf „Login“ klicke. Dort ist der korrekte Link zur Weiterleitung auf die Abmelden-Seite enthalten. Nur: Wie kann ich auf den Mitgliederseiten den Link „Login“ umbenennen in „Logout“? Ist das möglich? Oder geht es in einer WordPressinstallation nicht?
  Liebe Grüße,
  Constanze Antworten
  - Kim Salewski 23. Februar 2018 8:49 Moin Constanze,
    Ich würde folgendes Plug-in nutzen: Nav Menu Roles
    Dieses Plug-in erlaubt es dir, in deinem Menü bei einzelnen Menüpunkten anzugeben, ob diese nur von angemeldeten Benutzern, abgemeldeten Besuchern oder Benutzern mit speziellen Benutzerrollen gesehen werden können.
    Du könntest in dein Menü die Seite „Log-in“ zwei Mal einfügen. Den zweiten Menüpunkt „Log-in“ benennst du dann um in „Log-out“ und schaltest ihn durch das Plug-in nur für angemeldete Besucher sichtbar (so sehen abgemeldete Besucher diesen nicht). Genau so kannst du „Log-in“ nur für abgemeldete Besucher sichtbar machen, dann wirkt es, als würde aus **Log-in** nach dem Anmelden **Log-out** werden.

Ich hoffe, das hat dir etwas geholfen, auf der Plug-in Seite findest du Screenshots, die sicherlich etwas Klarheit bringen.
Viele Liebe Grüße,
Kim Antworten

- Constanze 23. Februar 2018 10:03 Moin Kim,
  Danke sehr! Super Tipp, und dann noch so schnell. Ich bin begeistert!
  Ich probiere das Plugin aus. Theoretisch wären für dieses Problem ja verschiedene Möglichkeiten denkbar: Von vornherein für jede Seite ein eigenes, vom Theme unabhängiges Menü erstellen und entsprechend auf der Mitgliederseite ändern. Oder den ganzen Mitgliederbereich von vornherein auslagern auf eine Subdomain (mit neuem WordPress). Aber wie es aussieht, scheint die Plugin-Lösung eine wenig aufwendige Lösung. Danke sehr!
  Liebe Grüße
  Constanze Antworten
  - Constanze 23. Februar 2018 10:37 Hallo Kim,
    es funktioniert leider nicht wie erhofft.
    Zwar klappt es mit der Sichtbarkeit der Links, also als eingeloggt Mitglied wird nur der Link Logout gezeigt (und umgekehrt, Nichtmitglieder sehen nur das Login).
    Doch wenn ich mich als Mitglied wieder auslogge, werde ich zur WP-Abmeldung geführt. Mache ich da gerade einen Denkfehler? Welche Einstellungen könnten Verkehr sein?
    Liebe Grüße
    Constanze Antworten

- Kim Salewski 23. Februar 2018 10:44 Hallo Constanze,
  Hast du auf den Link „Logout“ und dann auf „Abmelden“ unten auf der Seite geklickt?
  Das sollte einen ganz normal ausgeloggt auf die Startseite zurückleiten.
  Liebe Grüße,
  Kim

- Ute Bender 21. Februar 2018 16:43 Vielen Dank für den tollen Beitrag. Genau das habe ich gesucht und es klappt auch wunderbar. Eine kleine Frage bleibt:
  Unsere Mitglieder gehören Gruppen an (das sind meine Level), die unterschiedlich Zugriff auf unsere Kursinhalte haben sollen. Der Kurs umfasst fast 130 Seiten. Füge ich nun eine neue Gruppe (Level) hinzu, die auf alle 130 Seiten zugreifen soll, muss ich dann jede Seite wieder aufrufen und per Klick die Zuweisung bestätigen, oder gibt es hier ein Addon oder Trick, wie ich schnell Mitglieder eines Levels alle Seiten zugänglich machen kann.
  Es wäre toll, wenn ihr einen Hinweis hättet.
  Besten Dank im voraus.
  Ute Antworten
  - Kim Salewski 22. Februar 2018 8:41 Moin Ute,
    Das ist eine sehr gute Frage. Ich habe mich einmal erkundigt und es gibt tatsächlich die Möglichkeit, mehrere Seiten (oder Beiträge) auf einmal zu schützen.
    Du begibst dich in dem Bereich **„WP Mitgliedschaft“** zu dem Menüpunkt **„Mitgliedschaftsstufen“**. Dort findest du oben fünf Reiter, bei denen der letzte **„Schutz von Beiträgen uns Seiten“** heißt. Hier erscheinen nun drei weitere Reiter, bei denen du Beiträge, Seiten, oder Benutzerdefinierte Beiträge (Custom Post Type) anhaken und mittels des

DropDownMenüs oben allen samt die gewünschte Mitgliedschaftsstufe zuteilen kannst.
Hier einmal ein Link, mit der Erklärung des Plug-in Autors, inklusive Screenshots (Englisch).
Mehrere Seiten auf einmal schützen
Viele liebe Grüße,
Kim Antworten

- Ute Bender 22. Februar 2018 12:43 Vielen Dank für die 1a Hilfe Kim! Antworten

- Klaus 16. Februar 2018 10:32 Danke für die schnelle und unkomplizierte Unterstützung.
  Schöne Grüße von der Isar an die Elbe. Antworten
- Klaus 15. Februar 2018 19:06 Ich habe diese interessante Funktion jetzt ausprobiert. Soweit läuft auch alles, aber bei Aufruf der Login-Seite werden Zugangsinformationen zur Seite sichtbar. Wie beim Backend von WP erscheint links " Meine Websites" und rechts das Profil und Logout-Möglichkeit für den angemeldeten Besucher. Ist das korrekt? Oder kann der Besucher sich somit Zugang zum kompletten Backend verschaffen? Antworten
  - Thorsten Faltings 15. Februar 2018 19:16 Moin Klaus,
    wir sind nicht sicher, ob wir dich richtig verstehen. Du siehst die Informationen nur, wenn Du eingeloggt, nicht aber, wenn du ausgeloggt bist?
    Indem Fall verstehen wir das Problem nicht.
    Ahoi!
    Thorsten Antworten
  - Thorsten Faltings 16. Februar 2018 9:04 Moin Klaus,
    um zu verhindern, dass Mitglieder ins Backend kommen, kannst Du ein Plug-in wie WP Admin No Show verwenden. Oder Du blendest unter den Benutzer-Einstellungen jeweils die Werkzeugleiste aus. Grundsätzlich können die Mitglieder aber nichts

anrichten, wenn Sie die Benutzerrolle „Abonnent“ haben.
Ahoi!
Thorsten Antworten

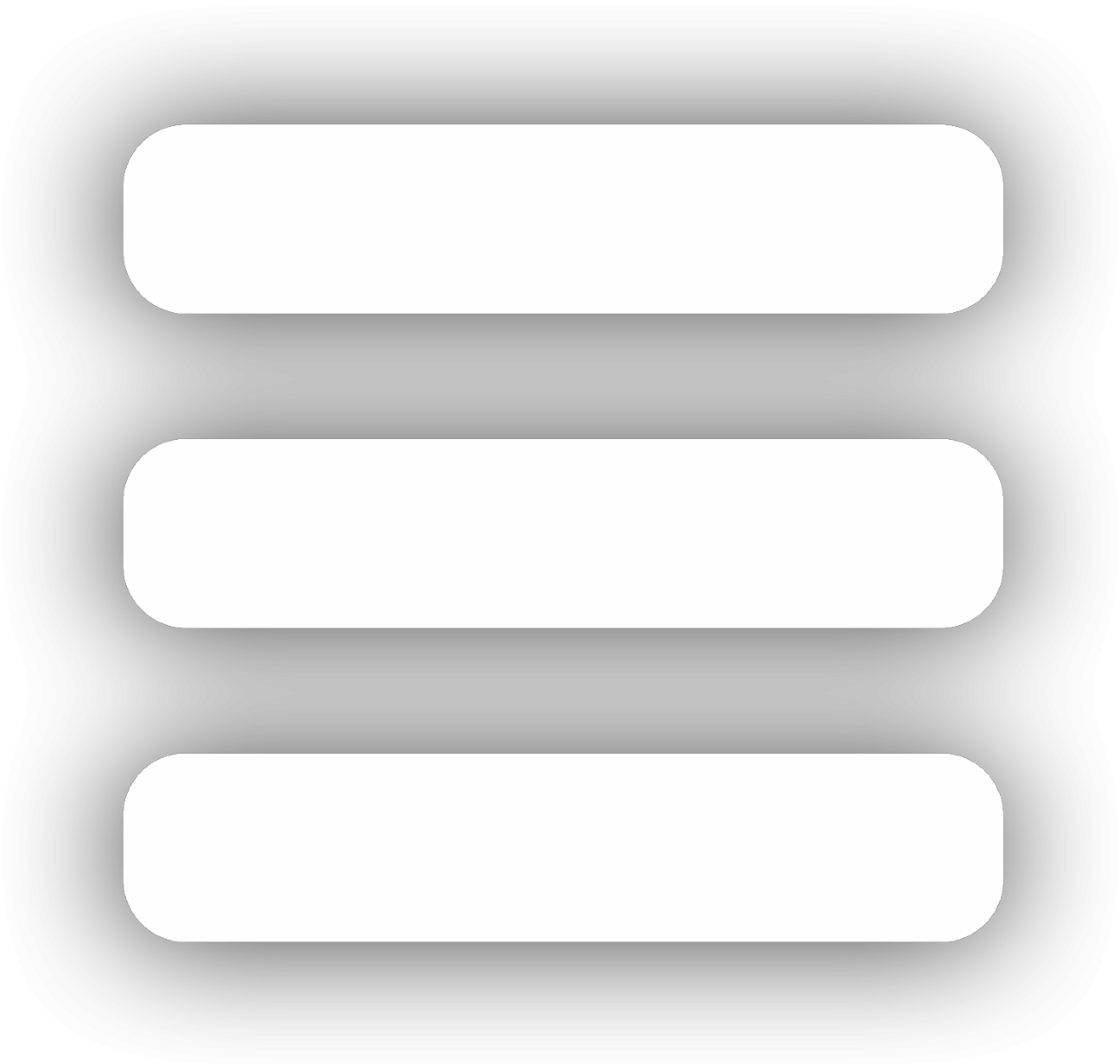
- Kim Salewski 16. Februar 2018 9:20 Moin Klaus,
  Ich habe den Beitrag um eine weitere Methode erweitert, die das Plug-in liefert. Generell erhalten Mitglieder die Rolle „Abonnent“ und können nichts an der Seite anpassen. Wenn man allerdings sicher gehen will, dass Sie nichts an dem Benutzer an sich ändern können, befolge die Schritte, die ich unter „Den Benutzer abhalten, seine Daten anzupassen“ hinzugefügt habe (ziemlich weit am Ende des Beitrags).
  Viele liebe Grüße,
  Kim Antworten

- Hendrik Wiedermann 14. Januar 2018 15:24 Hallo, wie ermögliche ich einem User, das manuelle ausloggen am besten?
  Ich habe in den Einstellungen von simple Membership ausgewählt, dass keine Werkzeugleiste angezeigt wird. Antworten
  - Hendrik Wiedermann 14. Januar 2018 16:04 habe es schon heraus gefunden. Einfach den Link des Logout der beim erneuten Klick auf den Mnüpunkt zum Login, erscheint, kopieren und als Link auf der Seite einbinden, auf die mal den User oder die Stufe durch das PlugIn weiterleiten lässt.
    Allerdings wäre es nun noch gut zu wissen, wie ich den einzelnen Mitgliedern und deren Stufe, den Zugriff auf eine Galerie ermöglichen kann bzw. nichtangemeldeten dies eben nicht. Antworten
    - Thorsten Faltings 15. Januar 2018 10:05 Moin Hendrik,
      eine Galerie lässt sich grundsätzlich in den geschützten Seiten anlegen. Allerdings ist das Problem, dass die Bilder standardmäßig

in einem öffentlichen Verzeichnis landen und grundsätzlich ungeschützt verteilt werden können.
Eine Lösung für dieses Problem bietet das Plug-in Media Vault.
Ahoi!
Thorsten Antworten

- Klaus 9. Januar 2018 18:40 Toller Beitrag! Gibt es auch die Möglichkeit, jeden Download zu protokollieren? Z.B. wer, wann,was? Antworten
  - Thorsten Faltings 10. Januar 2018 8:25 Moin Klaus, ja, die Downloads werden protokolliert.
    Ahoi!
    Thorsten Antworten

Schema.org Travel Agency



TravelAgency – Schema.org Type

Schema.org Type: TravelAgency – A travel agency.

TravelAgency

A Schema.org Type

Thing > Organization > LocalBusiness > TravelAgency

Thing > Place > LocalBusiness > TravelAgency

[more…] A travel agency.

Property	Expected Type	Description
Properties from LocalBusiness		

Property	Expected Type	Description
currenciesAccepted	Text	The currency accepted. Use standard formats: ISO 4217 currency format e.g. „USD“; Ticker symbol for cryptocurrencies e.g. „BTC“; well known names for Local Exchange Tradings Systems (LETS) and other currency types e.g. „Ithaca HOUR“.
openingHours	Text	The general opening hours for a business. Opening hours can be specified as a weekly time range, starting with days, then times per day. Multiple days can be listed with commas ‚,‘ separating each day. Day or time ranges are specified using a hyphen ‚-‚. Days are specified using the following two-letter combinations: Mo, Tu, We, Th, Fr, Sa, Su. Times are specified using 24:00 format. For example, 3pm is specified as 15:00, 10am as 10:00. Here is an example: <time itemprop="openingHours" datetime="Tu,Th 16:00-20:00">Tuesdays and Thursdays 4-8pm</time>. If a business is open 7 days a week, then it can be specified as <time itemprop="openingHours" datetime="Mo-Su">Monday through Sunday, all day</time>.
paymentAccepted	Text	Cash, Credit Card, Cryptocurrency, Local Exchange Tradings System, etc.
priceRange	Text	The price range of the business, for example $$$.
Properties from Organization		
actionableFeedbackPolicy	CreativeWork or URL	For a NewsMediaOrganization or other news-related Organization, a statement about public engagement activities (for news media, the newsroom’s), including involving the public – digitally or otherwise – in coverage decisions, reporting and activities after publication.
address	PostalAddress or Text	Physical address of the item.
aggregateRating	AggregateRating	The overall rating, based on a collection of reviews or ratings, of the item.
alumni	Person	Alumni of an organization. Inverse property: alumniOf
areaServed	AdministrativeArea or GeoShape or Place or Text	The geographic area where a service or offered item is provided. Supersedes serviceArea.
award	Text	An award won by or for this item. Supersedes awards.
brand	Brand or Organization	The brand(s) associated with a product or service, or the brand(s) maintained by an organization or business person.
contactPoint	ContactPoint	A contact point for a person or organization. Supersedes contactPoints.
correctionsPolicy	CreativeWork or URL	For an Organization (e.g. NewsMediaOrganization), a statement describing (in news media, the newsroom’s) disclosure and correction policy for errors.
department	Organization	A relationship between an organization and a department of that organization, also described as an organization (allowing different urls, logos, opening hours). For example: a store with a pharmacy, or a bakery with a cafe.
dissolutionDate	Date	The date that this organization was dissolved.
diversityPolicy	CreativeWork or URL	Statement on diversity policy by an Organization e.g. a NewsMediaOrganization. For a NewsMediaOrganization, a statement describing the newsroom’s diversity policy on both staffing and sources, typically providing staffing data.
diversityStaffingReport	Article or URL	For an Organization (often but not necessarily a NewsMediaOrganization), a report on staffing diversity issues. In a news context this might be for example ASNE or RTDNA (US) reports, or self-reported.
duns	Text	The Dun & Bradstreet DUNS number for identifying an organization or business person.
email	Text	Email address.

Property	Expected Type	Description
employee	Person	Someone working for this organization. Supersedes employees.
ethicsPolicy	CreativeWork or URL	Statement about ethics policy, e.g. of a NewsMediaOrganization regarding journalistic and publishing practices, or of a Restaurant, a page describing food source policies. In the case of a NewsMediaOrganization, an ethicsPolicy is typically a statement describing the personal, organizational, and corporate standards of behavior expected by the organization.
event	Event	Upcoming or past event associated with this place, organization, or action. Supersedes events.
faxNumber	Text	The fax number.
founder	Person	A person who founded this organization. Supersedes founders.
foundingDate	Date	The date that this organization was founded.
foundingLocation	Place	The place where the Organization was founded.
funder	Organization or Person	A person or organization that supports (sponsors) something through some kind of financial contribution.
globalLocationNumber	Text	The Global Location Number (GLN, sometimes also referred to as International Location Number or ILN) of the respective organization, person, or place. The GLN is a 13-digit number used to identify parties and physical locations.
hasCredential	EducationalOccupationalCredential	A credential awarded to the Person or Organization.
hasMerchantReturnPolicy	MerchantReturnPolicy	Specifies a MerchantReturnPolicy that may be applicable. Supersedes hasProductReturnPolicy.
hasOfferCatalog	OfferCatalog	Indicates an OfferCatalog listing for this Organization, Person, or Service.
hasPOS	Place	Points-of-Sales operated by the organization or person.
interactionStatistic	InteractionCounter	The number of interactions for the CreativeWork using the WebSite or SoftwareApplication. The most specific child type of InteractionCounter should be used. Supersedes interactionCount.
isicV4	Text	The International Standard of Industrial Classification of All Economic Activities (ISIC), Revision 4 code for a particular organization, business person, or place.
knowsAbout	Text or Thing or URL	Of a Person, and less typically of an Organization, to indicate a topic that is known about – suggesting possible expertise but not implying it. We do not distinguish skill levels here, or relate this to educational content, events, objectives or JobPosting descriptions.
knowsLanguage	Language or Text	Of a Person, and less typically of an Organization, to indicate a known language. We do not distinguish skill levels or reading/writing/speaking/signing here. Use language codes from the IETF BCP 47 standard.
legalName	Text	The official name of the organization, e.g. the registered company name.
leiCode	Text	An organization identifier that uniquely identifies a legal entity as defined in ISO 17442.
location	Place or PostalAddress or Text or VirtualLocation	The location of, for example, where an event is happening, where an organization is located, or where an action takes place.
logo	ImageObject or URL	An associated logo.
makesOffer	Offer	A pointer to products or services offered by the organization or person. Inverse property: offeredBy
member	Organization or Person	A member of an Organization or a ProgramMembership. Organizations can be members of organizations; ProgramMembership is typically for individuals. Supersedes musicGroupMember, members. Inverse property: memberOf

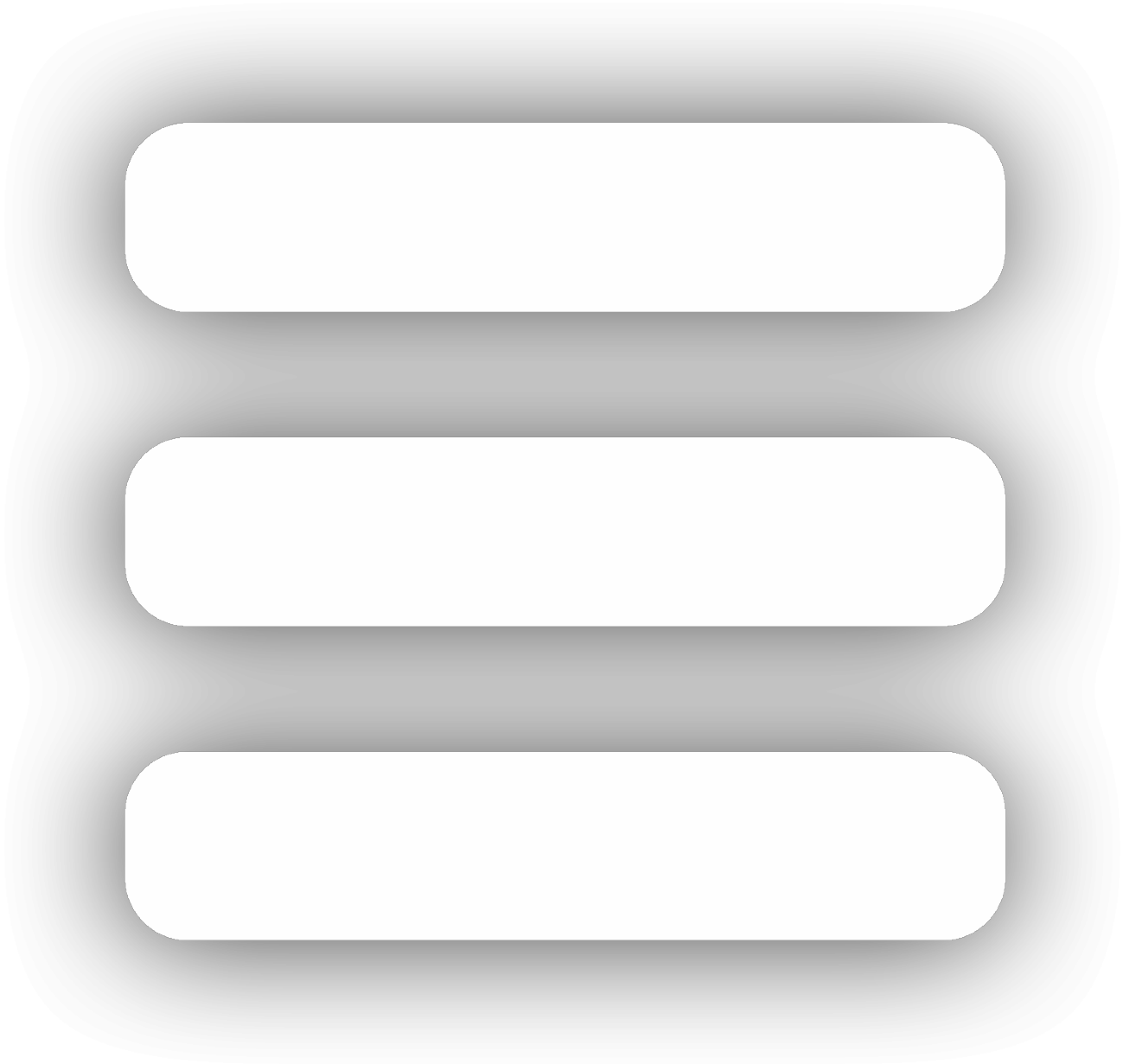
Property	Expected Type	Description
memberOf	Organization or ProgramMembership	An Organization (or ProgramMembership) to which this Person or Organization belongs. Inverse property: member
naics	Text	The North American Industry Classification System (NAICS) code for a particular organization or business person.
nonprofitStatus	NonprofitType	nonprofit Status indicates the legal status of a non-profit organization in its primary place of business.
numberOfEmployees	QuantitativeValue	The number of employees in an organization e.g. business.
ownershipFundingInfo	AboutPage or CreativeWork or Text or URL	For an Organization (often but not necessarily a NewsMediaOrganization), a description of organizational ownership structure; funding and grants. In a news/media setting, this is with particular reference to editorial independence. Note that the funder is also available and can be used to make basic funder information machine-readable.
owns	OwnershipInfo or Product	Products owned by the organization or person.
parentOrganization	Organization	The larger organization that this organization is a subOrganization of, if any. Supersedes branchOf. Inverse property: subOrganization
publishingPrinciples	CreativeWork or URL	The publishingPrinciples property indicates (typically via URL) a document describing the editorial principles of an Organization (or individual e.g. a Person writing a blog) that relate to their activities as a publisher, e.g. ethics or diversity policies. When applied to a CreativeWork (e.g. NewsArticle) the principles are those of the party primarily responsible for the creation of the CreativeWork. While such policies are most typically expressed in natural language, sometimes related information (e.g. indicating a funder) can be expressed using schema.org terminology.
review	Review	A review of the item. Supersedes reviews.
seeks	Demand	A pointer to products or services sought by the organization or person (demand).
slogan	Text	A slogan or motto associated with the item.
sponsor	Organization or Person	A person or organization that supports a thing through a pledge, promise, or financial contribution. e.g. a sponsor of a Medical Study or a corporate sponsor of an event.
subOrganization	Organization	A relationship between two organizations where the first includes the second, e.g., as a subsidiary. See also: the more specific ‚department' property. Inverse property: parentOrganization
taxID	Text	The Tax / Fiscal ID of the organization or person, e.g. the TIN in the US or the CIF/NIF in Spain.
telephone	Text	The telephone number.
unnamedSourcesPolicy	CreativeWork or URL	For an Organization (typically a NewsMediaOrganization), a statement about policy on use of unnamed sources and the decision process required.
vatID	Text	The Value-added Tax ID of the organization or person.
Properties from Place		
additionalProperty	PropertyValue	A property-value pair representing an additional characteristics of the entitity, e.g. a product feature or another characteristic for which there is no matching property in schema.org. Note: Publishers should be aware that applications designed to use specific schema.org properties (e.g. https://schema.org/width, https://schema.org/color, https://schema.org/gtin13, …) will typically expect such data to be provided using those properties, rather than using the generic property/value mechanism.
address	PostalAddress or Text	Physical address of the item.

Property	Expected Type	Description
aggregateRating	AggregateRating	The overall rating, based on a collection of reviews or ratings, of the item.
amenityFeature	LocationFeatureSpecification	An amenity feature (e.g. a characteristic or service) of the Accommodation. This generic property does not make a statement about whether the feature is included in an offer for the main accommodation or available at extra costs.
branchCode	Text	A short textual code (also called „store code“) that uniquely identifies a place of business. The code is typically assigned by the parentOrganization and used in structured URLs. For example, in the URL http://www.starbucks.co.uk/store-locator/etc/detail/3047 the code „3047“ is a branchCode for a particular branch.
containedInPlace	Place	The basic containment relation between a place and one that contains it. Supersedes containedIn. Inverse property: containsPlace
containsPlace	Place	The basic containment relation between a place and another that it contains. Inverse property: containedInPlace
event	Event	Upcoming or past event associated with this place, organization, or action. Supersedes events.
faxNumber	Text	The fax number.
geo	GeoCoordinates or GeoShape	The geo coordinates of the place.
geoContains	GeospatialGeometry or Place	Represents a relationship between two geometries (or the places they represent), relating a containing geometry to a contained geometry. „a contains b iff no points of b lie in the exterior of a, and at least one point of the interior of b lies in the interior of a“. As defined in DE-9IM.
geoCoveredBy	GeospatialGeometry or Place	Represents a relationship between two geometries (or the places they represent), relating a geometry to another that covers it. As defined in DE-9IM.
geoCovers	GeospatialGeometry or Place	Represents a relationship between two geometries (or the places they represent), relating a covering geometry to a covered geometry. „Every point of b is a point of (the interior or boundary of) a“. As defined in DE-9IM.
geoCrosses	GeospatialGeometry or Place	Represents a relationship between two geometries (or the places they represent), relating a geometry to another that crosses it: „a crosses b: they have some but not all interior points in common, and the dimension of the intersection is less than that of at least one of them“. As defined in DE-9IM.
geoDisjoint	GeospatialGeometry or Place	Represents spatial relations in which two geometries (or the places they represent) are topologically disjoint: they have no point in common. They form a set of disconnected geometries.“ (a symmetric relationship, as defined in DE-9IM)
geoEquals	GeospatialGeometry or Place	Represents spatial relations in which two geometries (or the places they represent) are topologically equal, as defined in DE-9IM. „Two geometries are topologically equal if their interiors intersect and no part of the interior or boundary of one geometry intersects the exterior of the other“ (a symmetric relationship)
geoIntersects	GeospatialGeometry or Place	Represents spatial relations in which two geometries (or the places they represent) have at least one point in common. As defined in DE-9IM.
geoOverlaps	GeospatialGeometry or Place	Represents a relationship between two geometries (or the places they represent), relating a geometry to another that geospatially overlaps it, i.e. they have some but not all points in common. As defined in DE-9IM.
geoTouches	GeospatialGeometry or Place	Represents spatial relations in which two geometries (or the places they represent) touch: they have at least one boundary point in common, but no interior points.“ (a symmetric relationship, as defined in DE-9IM)

Property	Expected Type	Description
geoWithin	GeospatialGeometry or Place	Represents a relationship between two geometries (or the places they represent), relating a geometry to one that contains it, i.e. it is inside (i.e. within) its interior. As defined in DE-9IM.
globalLocationNumber	Text	The Global Location Number (GLN, sometimes also referred to as International Location Number or ILN) of the respective organization, person, or place. The GLN is a 13-digit number used to identify parties and physical locations.
hasDriveThroughService	Boolean	Indicates whether some facility (e.g. FoodEstablishment, CovidTestingFacility) offers a service that can be used by driving through in a car. In the case of CovidTestingFacility such facilities could potentially help with social distancing from other potentially-infected users.
hasMap	Map or URL	A URL to a map of the place. Supersedes map, maps.
isAccessibleForFree	Boolean	A flag to signal that the item, event, or place is accessible for free. Supersedes free.
isicV4	Text	The International Standard of Industrial Classification of All Economic Activities (ISIC), Revision 4 code for a particular organization, business person, or place.
latitude	Number or Text	The latitude of a location. For example 37.42242 (WGS 84).
logo	ImageObject or URL	An associated logo.
longitude	Number or Text	The longitude of a location. For example -122.08585 (WGS 84).
maximumAttendeeCapacity	Integer	The total number of individuals that may attend an event or venue.
openingHoursSpecification	OpeningHoursSpecification	The opening hours of a certain place.
photo	ImageObject or Photograph	A photograph of this place. Supersedes photos.
publicAccess	Boolean	A flag to signal that the Place is open to public visitors. If this property is omitted there is no assumed default boolean value
review	Review	A review of the item. Supersedes reviews.
slogan	Text	A slogan or motto associated with the item.
smokingAllowed	Boolean	Indicates whether it is allowed to smoke in the place, e.g. in the restaurant, hotel or hotel room.
specialOpeningHoursSpecification	OpeningHoursSpecification	The special opening hours of a certain place. Use this to explicitly override general opening hours brought in scope by openingHoursSpecification or openingHours.
telephone	Text	The telephone number.
tourBookingPage	URL	A page providing information on how to book a tour of some Place, such as an Accommodation or ApartmentComplex in a real estate setting, as well as other kinds of tours as appropriate.
Properties from Thing		
additionalType	URL	An additional type for the item, typically used for adding more specific types from external vocabularies in microdata syntax. This is a relationship between something and a class that the thing is in. In RDFa syntax, it is better to use the native RDFa syntax – the ‚typeof' attribute – for multiple types. Schema.org tools may have only weaker understanding of extra types, in particular those defined externally.
alternateName	Text	An alias for the item.
description	Text	A description of the item.
disambiguatingDescription	Text	A sub property of description. A short description of the item used to disambiguate from other, similar items. Information from other properties (in particular, name) may be necessary for the description to be useful for disambiguation.

Property	Expected Type	Description
identifier	PropertyValue or Text or URL	The identifier property represents any kind of identifier for any kind of Thing, such as ISBNs, GTIN codes, UUIDs etc. Schema.org provides dedicated properties for representing many of these, either as textual strings or as URL (URI) links. See background notes for more details.
image	ImageObject or URL	An image of the item. This can be a URL or a fully described ImageObject.
mainEntityOfPage	CreativeWork or URL	Indicates a page (or other CreativeWork) for which this thing is the main entity being described. See background notes for details. Inverse property: mainEntity
name	Text	The name of the item.
potentialAction	Action	Indicates a potential Action, which describes an idealized action in which this thing would play an ‚object' role.
sameAs	URL	URL of a reference Web page that unambiguously indicates the item's identity. E.g. the URL of the item's Wikipedia page, Wikidata entry, or official website.
subjectOf	CreativeWork or Event	A CreativeWork or Event about this Thing. Inverse property: about
url	URL	URL of the item.

Schema.org Validator



Schema Markup Validator

Test your structured data

Schema.org Markup Generator

(JSON-LD)

Schema Markup Generator (JSON-LD) | TechnicalSEO.com

A Schema.org structured data generator that supports the creation of JSON-LD markups. Including all of the required item properties and more.