Hacking WordPress – Ein Blick hinter die Kulissen

Angreifen und Sichern von WordPress

Hacking WordPress – Ein Blick hinter die Kulissen

Wie Angreifer WordPress-Installationen hacken bzw. Schwachstellen in Plugins, Themes oder Konfigurationen ausnutzen.

1. Hilfe ich wurde gehackt!

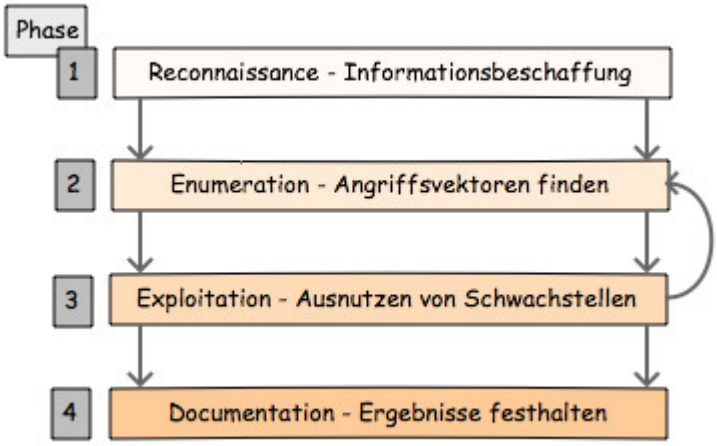
Allein in Deutschland ist der **Verbreitungsgrad** von WordPress enorm – Tendenz weiter steigend. Im weltweiten Vergleich mit anderen Content Management Systemen (CMS) hält WordPress einen Anteil von bis zu 51% (Top Million Sites). Beeindruckende Zahlen also, die WordPress immer stärker in den Fokus von **professionellen Angreifern** rückt. So attackierte ein Botnet im April diesen Jahres WordPress-Installationen weltweit.

Zum Schutz und Absicherung von Installationen wurden bereits zahlreiche Anleitungen veröffentlicht. Empfehlenswert sind »Hardnening WordPress« oder auch meine Artikelserie »WordPress absichern«.

In diesem Beitrag werden allerdings keine weiteren **Schutzmaßnahmen** vorgestellt, sondern wie Angreifer vorgehen, um WordPress-Installationen zu hacken. Es soll ein kleiner Einblick hinter die **Kulissen** sein – in der Realität existieren weitaus mehr Möglichkeiten und Varianten.

2. Hinweis zu »Hacking WordPress«

Der Angriff von WordPress-Installationen oder Systemen ohne Erlaubnis bzw. Einverständniserklärung stellt eine **strafbare Handlung** dar. Wer ohne vertragliche Grundlage fremde Systeme angreift begibt sich auf sehr dünnes Eis. Die nachfolgenden Informationen dienen der Aufklärung und sollten lediglich im Rahmen eines Penetrationstests Verwendung finden. Im Gegensatz zu illegalen Hacking-Angriffen stellt ein Penetrationstest ein **auftragsgesteuerter** Einbruch in ein oder mehrere Systeme dar. Das Vorgehen dient im Grunde der »Qualitätskontrolle« der aktuell umgesetzten IT-Sicherheit im Unternehmensumfeld.



Ein Angriff / Penetrationstest lässt sich in unterschiedlichen **Phasen** unterteilen, von denen ein Teil sequentiell wiederholt wird. Phase 1 dient zunächst der **Informationsgewinnung** über das Ziel. Während ein Penetrationstester in Phase 4 die Ergebnisse festhält, wird sich ein Angreifer diesen Schritt wohl eher sparen…

3. Informationsgewinnung – Phase 1

Im ersten Schritt wird ein Angreifer möglichst viele **Informationen** über sein Ziel sammeln, die für den weiteren Verlauf von Interesse sein können. Zu diesem Zweck werden verschiedene öffentlich verfügbare Informationsquellen durchsucht. Diese werden im Anschluss ausgewertet und sollen Aufschluss darüber geben, über welchen Weg ein Einbruch am **einfachsten** realisiert werden kann. Für diesen Zweck stehen unterschiedliche Tools zur Verfügung – die meisten davon befinden sich auf der Linux Distribution Kali. Die Distribution wird sowohl von **Hackern**, als auch von **Penetrationstestern** zur Auffindung von Schwachstellen / Sicherheitsanalysen eingesetzt.

Dabei helfen Tools die unter »Information Gathering« zusammengefasst sind. Letztendlich werden in der ersten Phase folgende Ziele verfolgt:

- Ziel identifizieren
- System / Anwendungsversion bestimmen
- Verfügbare Netzwerk-Ports
- Laufende Services
- Verteidigungsstrategien erkennen
- […]

Du kannst den Blog aktiv unterstützen!

No Tracking. No Paywall. No Bullshit.

Die Arbeit von kuketz-blog.de finanziert sich zu 100% aus den Spenden unserer Leserinnen und Leser. Werde Teil dieser Community und unterstütze auch du unsere Arbeit mit deiner Spende.

Mitmachen →

3.1 Beispiel: WordPress Identifikation

Das Verstecken der **WordPress-Versionsnummer** oder sonstigen **Meta-Daten** wird bei Laien oftmals mit dem Schutz gegen Spambots oder Sicherheitslücken in Verbindung gebracht. In der Tat lassen sich damit die besonders »dämlichen« Bots an der Nase herumführen, aber bereits semi-professionelle Varianten lassen sich von den Security by Obscurity Maßnahmen nicht beirren. Sie benutzen ausgeklügelte Methoden zur Feststellung ob eine Seite mit WordPress betrieben wird.


```
[*] Num of checks set to: 100

------------------------------------------------------
[*] Input plugin list set to: wp_plugin_list_2013_feb.txt
[*] Num of threats set to: 10
------------------------------------------------------

==> Results for: http://[redacted] <==

[i] Wordpress version found:  3.5.2
[i] Wordpress last public version: 3.5.2


[*] Search for installed plugins


[i] Plugin found: google-sitemap-generator
    |_Latest version:  3.2.9
    |_ Installed version: 3.2.8

[i] Plugin found: jetpack
    |_Latest version:  2.1.2
    |_ Installed version: 2.3.1
    |_CVE list:
    |___CVE-2011-4673: (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4673)

[i] Plugin found: si-contact-form
    |_Latest version:  3.1.8.1
    |_ Installed version: trunk

[i] Plugin found: wp-pagenavi
    |_Latest version:  2.83
    |_ Installed version: 2.83
```

Wer selbst mal schauen möchte ob seine WordPress-Installation als solche erkannt wird kann folgende Webseite nutzen: [Is it WordPress?]

Mehr Informationen benötigt? Beispielsweise alle installierten Plugins? Auch gar kein Problem mit dem Tool [plecost]. Hier ein Fingerprint einer WordPress-Installation:

Mit Hilfe der gesammelten Informationen lässt sich WordPress bzw. eines der installierten Plugins gezielt angreifen. Details zu Schwachstellen für bestimmte Versionen stellt beispielsweise CVE-Details zur Verfügung.

3.2 Beispiel: System identifizieren

Nmap ist ein Werkzeug zum **Scannen** und **Auswerten** von Hosts in einem Netzwerk und fällt in die Kategorie der Portscanner. Der Name steht für Network Mapper. Nmap wird in erster Linie für Portscanning eingesetzt. Daneben verfügt es über weitere Techniken, wie beispielsweise die Erkennung des eingesetzten Betriebssystems (OS-Fingerprinting).

Letztendlich dienen solche Informationen wiederum als **Ausgangspunkt** für die weiteren Phasen, in denen Schwachstellen aktiv ausgenutzt werden.

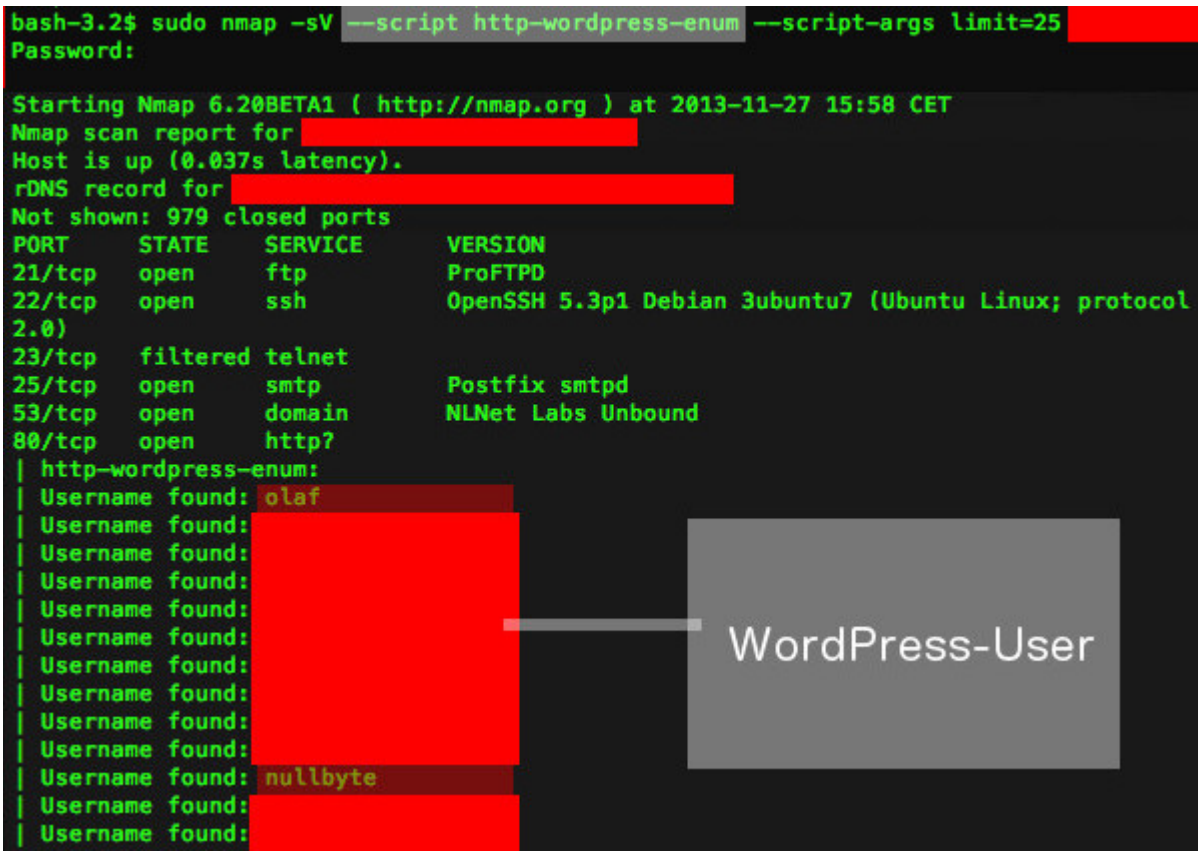
3.3 Beispiel: Erkennung von Benutzer-Accounts

Um sich in den **Administrationsbereich** von WordPress einzuloggen ist die Kombination aus einem Benutzernamen und Passwort erforderlich. Falls ein Angreifer im Vorfeld den Benutzernamen »erraten« kann, benötigt er im Anschluss lediglich das korrekte Passwort. Insgesamt erleichtert das ein erfolgreiches Eindringen in den sensiblen Administrationsbereich.

Oft genügt dazu die Eingabe von

wordpress-blog-adress.de/?author=1

in die Browser-Zeile. In der Standard-Installation bekommt ein Administrator / Nutzer eine eindeutige **Identifikationsnummer** zugewiesen. Meist endet diese auf **author=1** bzw. kann durch den Austausch der 1 am Ende leicht durchprobiert werden.



Falls der WordPress-Betreiber dies manuell geändert hat hilft ein Skript für nmap – wer probiert schon gerne alle

Kombinationen durch:

4. Angriffsvektoren finden – Phase 2

Ausgehend von den in Schritt eins gesammelten Informationen werden anschließend mögliche **Einstiegspunkte** in das System identifiziert. Mit Hilfe von Tools und manuellen Abfragen wird konkrekt nach Schwachstellen und Lücken gesucht, die einen Einbruch ermöglichen. Unter »Vulnerability Analysis« sind die benötigten Tools zusammengefasst und dienen folgenden Zielen:

- Schwachstellen identifizieren
- Identifizieren und priorisieren von System Zugangspunkten
- Risiken einschätzen
- […]

WordPress auf Schwachstellen und Konfigurationsfehler prüfen

Für Deine WordPress-Installation habe ich ein **spezielles** Leistungspaket im Angebot:

- Scan Deiner WordPress-Installation auf Schwachstellen
- Auswertung und Beurteilung der gefundenen Schwachstellen
- Auf Basis der Ergebnisse erhälst Du von mir individuelle Maßnahmenempfehlungen zur Behebung und Absicherung

Wenn du Deine WordPress-Installation **nachhaltig** absichern möchtest, kannst Du mich gerne kontaktieren.

Gut zu wissen: Sicherheit erlangst Du nicht durch die Installation unzähliger Security-Plugins, sondern durch eine saubere Konfiguration, stetige Updates und proaktive Maßnahmen

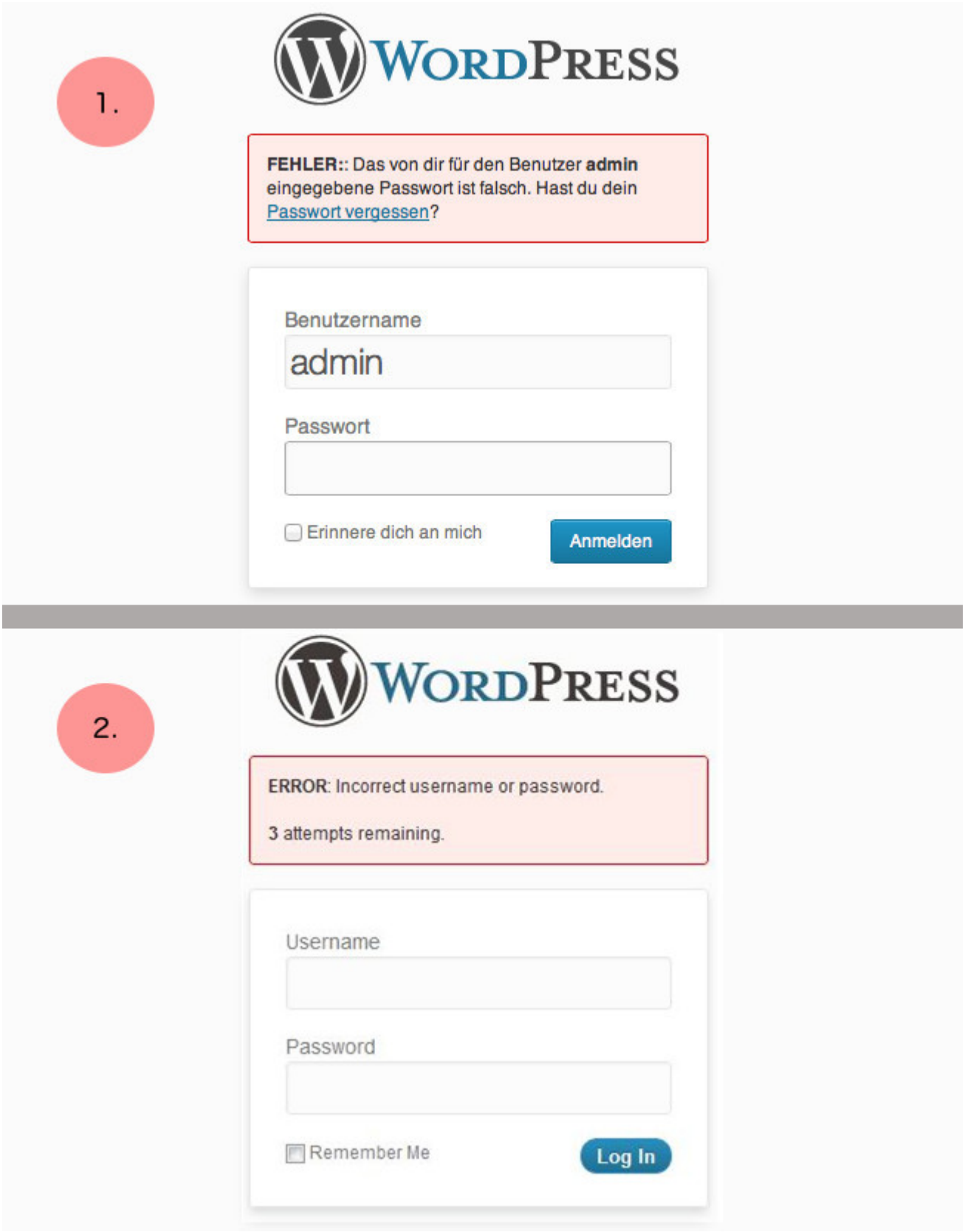
zur Absicherung. Kontakt aufnehmen

4.1 Administrationsbereich

Äußert beliebt als Einstiegspunkt ist der Login zum **Administrationsbereich** von WordPress – nicht zuletzt deswegen, weil sich ein Angriff bei vielen Installationen mit einfachen Mitteln bewerkstelligen lässt.

Über den Browser lässt sich prüfen, ob der Administrationsbereich generell für jeden erreichbar ist:

wordpress-blog-adress.de/wp-admin



Nach der Eingabe eines Benutzernamens und Passwort kann zunächst die Reaktion von WordPress erkundet werden.

Im ersten Beispiel wird der Account »**admin**« bestätigt. Dieser ist also vorhanden und dient vermutlich der Administration der

WordPress-Installation.

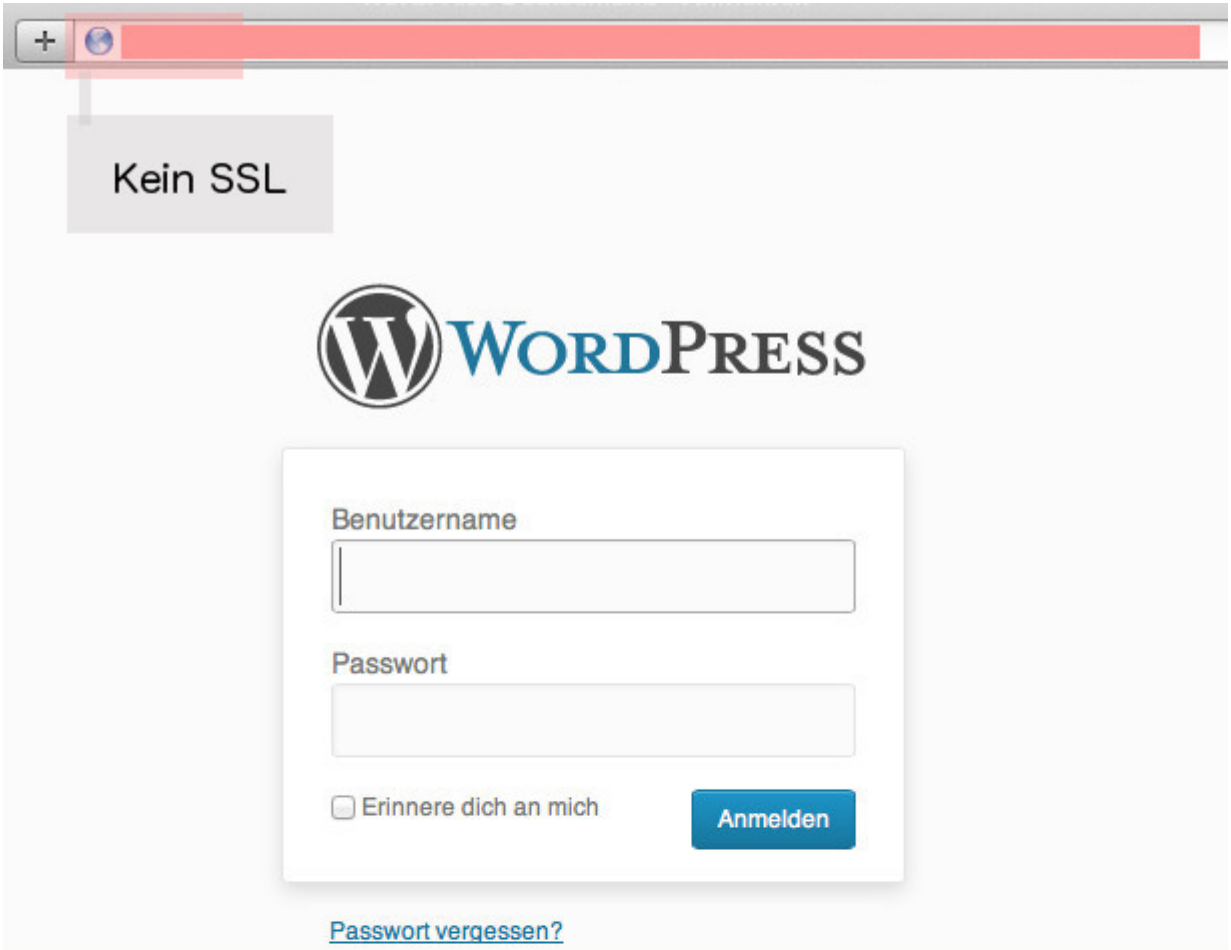
Aus Beispiel zwei lässt sich die Verwendung eines Security-Plugins ableiten. Vermutlich kommt hier Login LockDown / Limit Login Attempts oder ein ähnliches Plugin zum Einsatz. Diese protokollieren fehlgeschlagene **Login-Versuche**. Falls ein Anmeldeversuch innerhalb von 5 Minuten dreimal hintereinander fehlschlägt blockiert das Plugin die anfragende IP-Adresse beispielsweise für eine Stunde. Script-Kiddies und dämliche Bots lassen sich von solchen Maßnahmen abschrecken – professionelle Angreifer hingegen weniger.

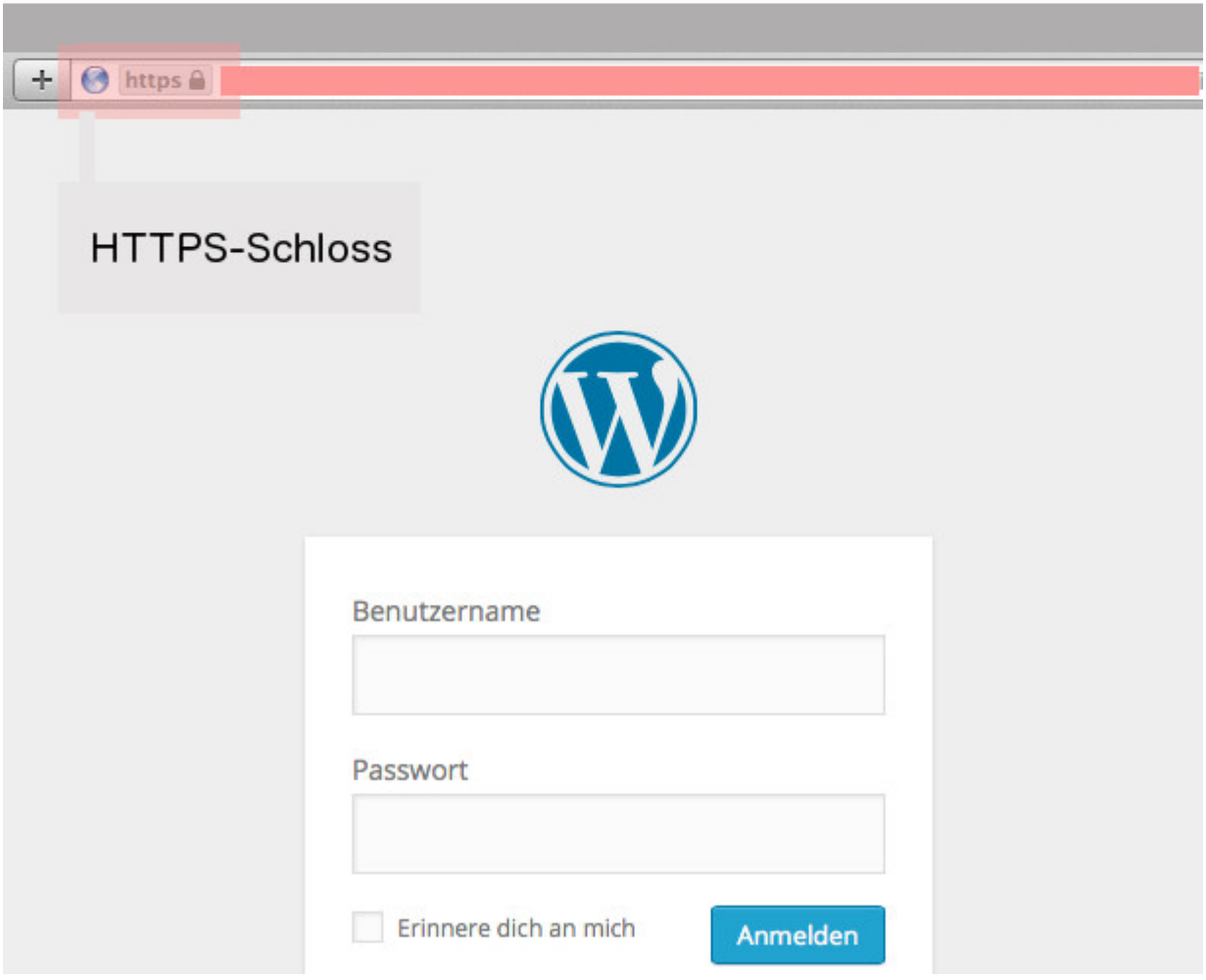
4.2 Fehlende SSL-Verschlüsselung

Hauptsächlich wird SSL für die **Absicherung** zwischen Webbrowser und Webserver eingesetzt – also immer dann, wenn sensible Informationen über das **unsichere** Internet ausgetauscht werden sollen.

Über den Browser wird abermals der Login zum Administrationsbereich aufgerufen:

wordpress-blog-adress.de/wp-admin


Kein SSL
WordPress
Benutzername
Passwort
Erinnere dich an mich
Anmelden
Passwort vergessen?


https
HTTPS-Schloss
Benutzername
Passwort
Erinnere dich an mich
Anmelden

Falls zwischen Browser und Server keine verschlüsselte SSL-Verbindung ausgehandelt wird, können die **Anmeldedaten** mitgeschnitten werden. Ganz konkret: Ein WordPress-Blogger nutzt das kostenlose **WLAN** in seinem Lieblingskaffee und loggt sich in den Administrationsbereich ein. Da die Verbindung nicht über SSL abgesichert wird, kann einer Angreifer die Anmeldedaten im Klartext bzw. unverschlüsselt mitlesen. Solch ein Angriff ist mit einfachen Mitteln bereits von Anfängern durchführbar.

5. Ausnutzen von Schwachstellen – Phase 3

Gefundene Schwachstellen gilt es in Phase 3 gezielt auszunutzen. Dafür werden vorhandene Exploits verwendet oder neue entwickelt, die es ermöglichen Systeme zu **kompromittieren**. Falls in ein System eingerungen werden kann, ergeben sich aus dem Zugriff oftmals weitere mögliche **Angriffsziele**, die vorher nicht erreichbar waren. Mit der Toolkiste aus »Exploitation Tools« oder »Privilige Escalation« stehen in Kali genügend Mittel zur Verfügung. Verfolgt wird damit:

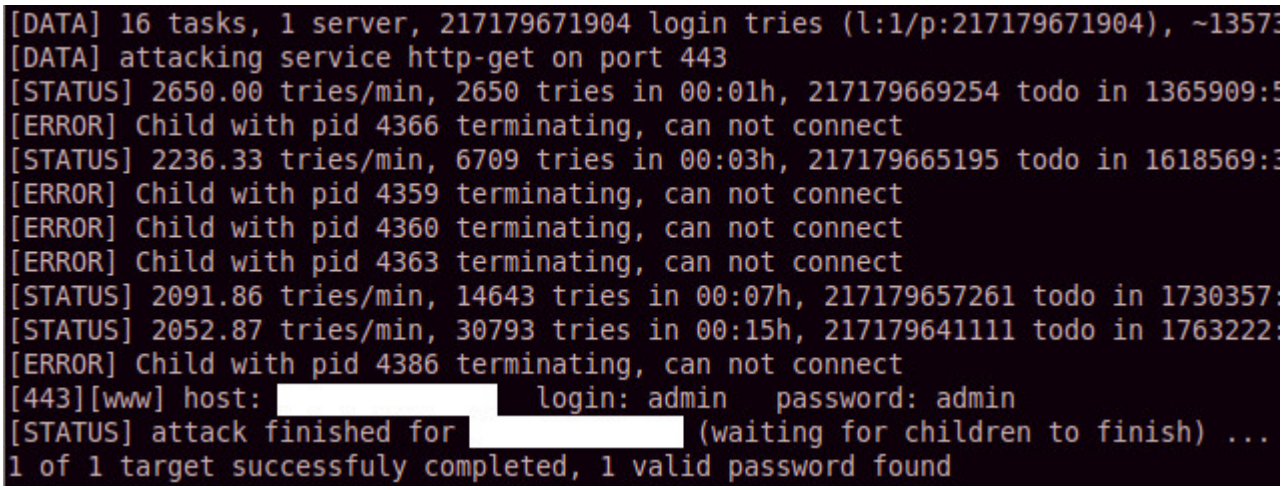
- Schwachstellen in Systemen / Anwendungen ausnutzen
- Systemzugriff erhalten
- Zugang zu geschützten Web-Bereichen
- Erfassen von sensiblen Daten
- […]

5.1 Brute-Force WP-Login

Da Administratoren über die weitreichendsten **Berechtigungen** verfügen, stellen sie ein beliebtes Ziel für Angreifer dar. Einmal eingeloggt erlauben Sie beispielsweise das Hinzufügen von schädlichen PHP- oder Javascript-Befehlen direkt über das

Dashboard. In der Informationsphase wurden bereits Anmeldeinformationen gesammelt, die gezielt für den Einbruch in das Backend genutzt werden können.

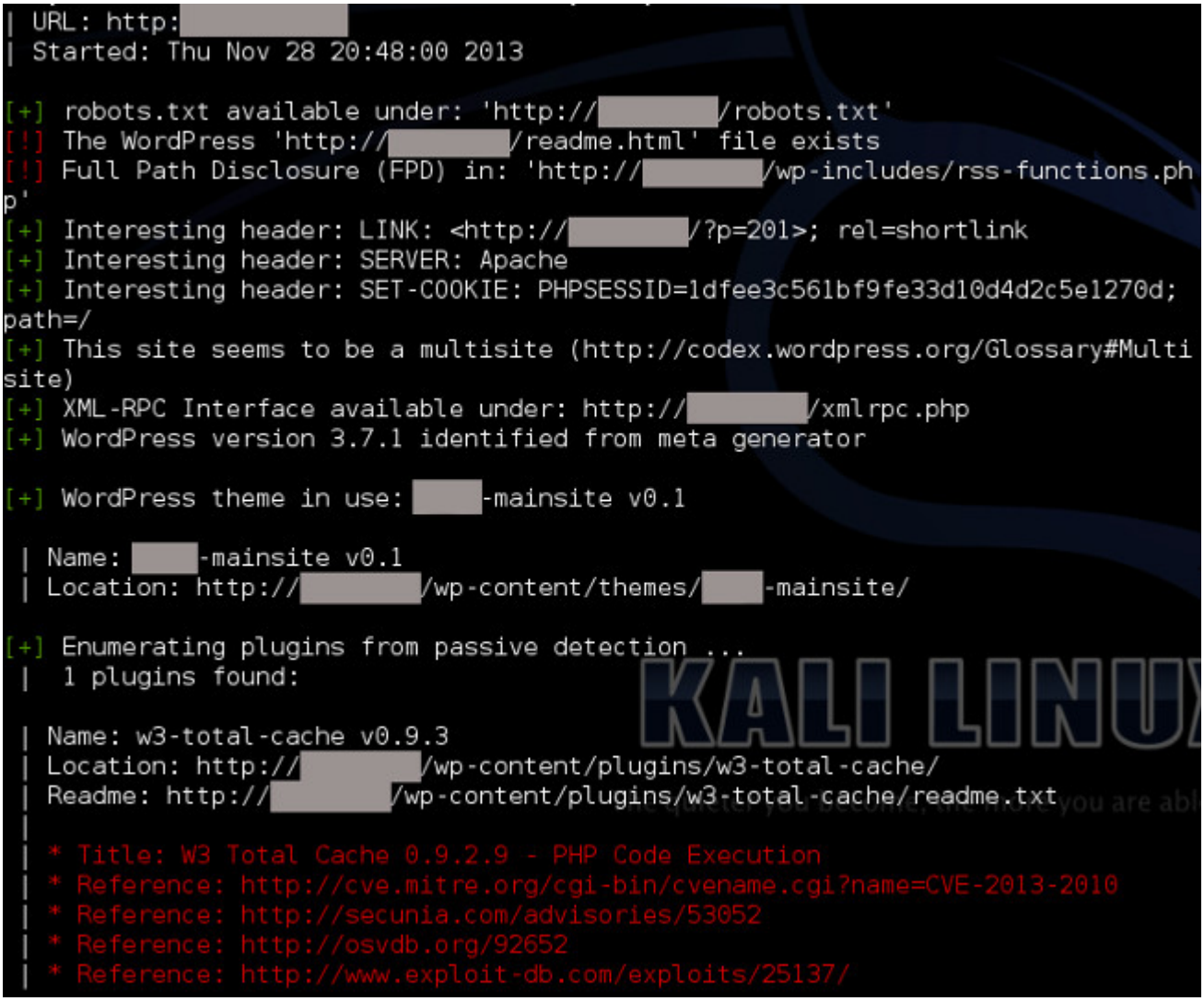
Geschützt wird der Administrationsbereich aus einer **Kombination** von Benutzername und Passwort. Falls ein Angreifer bereits über den Benutzernamen verfügt, so muss er im nächsten Schritt das Passwort »erraten«. Mittels einem Brute-Force-Angriff wird durch Ausprobieren das passende Passwort ermittelt. In freier Wildbahn führt dieser Angriff oft zum Erfolg, da viele Anwender noch immer unsichere Passwörter verwenden.



Speziell für diesen Zweck steht Hydra zur Verfügung. Neben WordPress-Installationen kann damit eine breite Palette von Systemen und Anwendungen angegriffen werden.

5.2 Das Tool WPScan

WPScan ist speziell auf WordPress zugeschnitten. Es bietet zahlreiche Funktionen, wie beispielsweise die **Erkennung** der installierten Plugins, Themes und WordPress-Versionen. Des Weiteren ist es in der Lage Benutzer-Accounts für Brute-Force-Angriffe zu »erraten« und verweist direkt auf **Schwachstellen-Datenbanken**, falls während des Scans auffällige Plugins gefunden werden. Im Beispiel wird eine Lücke im Plugin W3 Total Cache (Version 0.9.3) detektiert.



5.3 Metasploit

Metasploit ist eine Art **Allzweckwaffe** bzw. große Toolbox für Penetrationstests und Sicherheitsanalysen. Es besteht aus unterschiedlichen Teilbereichen, Teilprojekten und Modulen – der Umfang erlaubt den Einsatz in allen **Phasen** eines Penetrationstests. Auch Angreifer machen sich Metasploit zu Nutze, um in fremde Systeme einzudringen. Hier lediglich ein kurzer Einblick in das Metasploit Universum.

Das Metasploit Modul »**wordpress_login_enum**« dient zur Feststellung von gültigen Benutzer-Accounts und kann im Anschluss einen Passwort-Rate-Angriff durchführen.

```
msf > use auxiliary/scanner/http/wordpress_login_enum
msf auxiliary(wordpress_login_enum) > show options

Module options (auxiliary/scanner/http/wordpress_login_enum):

   Name               Current Setting  Required  Description
   ----               ---------------  --------  -----------
   BLANK_PASSWORDS    true             yes       Try blank passwords for all users
   BRUTEFORCE         true             yes       Perform brute force authentication
   BRUTEFORCE_SPEED   5                yes       How fast to bruteforce, from 0 to 5
   PASSWORD                            no        A specific password to authenticate
   PASS_FILE                           no        File containing passwords, one per
   Proxies                             no        Use a proxy chain
   RHOSTS                              yes       The target address range or CIDR id
   RPORT              80               yes       The target port
   STOP_ON_SUCCESS    false            yes       Stop guessing when a credential wor
   THREADS            1                yes       The number of concurrent threads
   URI                /wp-login.php    no        Define the path to the wp-login.php
   USERNAME                            no        A specific username to authenticate
   USERPASS_FILE                       no        File containing users and passwords
   USER_FILE                           no        File containing usernames, one per
   VALIDATE_USERS     true             yes       Enumerate usernames
   VERBOSE            true             yes       Whether to print output for all att
   VHOST                               no        HTTP server virtual host
```

```
msf auxiliary(wordpress_login_enum) > set URI /wordpress/wp-login.php
URI => /wordpress/wp-login.php
msf auxiliary(wordpress_login_enum) > set PASS_FILE /tmp/passes.txt
PASS_FILE => /tmp/passes.txt
msf auxiliary(wordpress_login_enum) > set USER_FILE /tmp/users.txt
USER_FILE => /tmp/users.txt
msf auxiliary(wordpress_login_enum) > set RHOSTS 192.168.1.201
RHOSTS => 192.168.1.201
msf auxiliary(wordpress_login_enum) > run

[*] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Enumeration - Runnin
[*] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Enumeration - Checki
[-] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Enumeration - Invali
[*] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Enumeration - Checki
[+] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Enumeration- Usernam
[*] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Enumeration - Checki
[-] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Enumeration - Invali
[*] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Enumeration - Checki
[-] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Enumeration - Invali
[+] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Enumeration - Found
[*] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Brute Force - Runnin
[*] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Brute Force - Skippi
[*] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Brute Force - Trying
[-] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Brute Force - Failed
[*] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Brute Force - Trying
[-] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Brute Force - Failed
[*] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Brute Force - Trying
[-] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Brute Force - Failed
[*] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Brute Force - Trying
[-] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Brute Force - Failed
[*] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Brute Force - Trying
[+] http://192.168.1.201:80/wordpress/wp-login.php - WordPress Brute Force - SUCCES
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(wordpress_login_enum) >
```

6. Weitere Möglichkeiten

Die oben dargestellten Tools und Möglichkeiten stellen lediglich eine Mini-Auswahl dar. In der **Praxis** existieren unzählige Tools und Varianten, Webanwendungen und deren Host-Systeme zu hacken. Allein in den Datenbanken von Metasploit und exploit-db.com sind hunderte von **Schwachstellen** erfasst und beschrieben. Immer wieder Ziel sind Plugins, Themes und der WordPress-Kern selbst.

Hinweis

Auch von deaktivierten Plugins oder Themes geht eine Gefahr aus. Selbst wenn sie nicht aktiv verwendet werden, so sind sie im Normalfall dennoch erreichbar. Beispielsweise erlaubt das Plugin Asset-Manager (Version <= 2.0) einen Datei-Upload in ein temporäres Verzeichnis – anschließend kann darüber Schadcode ausgeführt werden. Für diesen Einbruch muss das Plugin nicht aktiv sein, sondern lediglich auf dem Webspace vorhanden.**Lücke**: WordPress Asset-Manager PHP File Upload Vulnerability.

6.1 Angriffe auf Systemebene

Allein für Phase 1 (**Informationsbeschaffung**) wird ein Angreifer viel Zeit aufwenden, um an Daten / Informationen zu gelangen, die ihm später nützlich sein können. Immerhin hängt davon indirekt der Erfolg für den späteren Einbruch ab. Bereits einfache Wege wie, Google-Hacking (Dorks), DNS-Informationen und soziale Netzwerke stellen wichtige Informationsquellen dar. Daraus lassen sich oftmals Informationen ableiten, die entscheidende Hinweise für einen erfolgreichen Angriff bieten. Womöglich bietet eine WordPress-Installation selbst keinen **Angriffspunkt**, was den Fokus auf das Host-System richtet. Als Beispiel:

- MySQL-Datenbank

- FTP / SSH Service
- CPanel oder andere Tools für die web-basierte Administration
- phpMyAdmin Zugänge
- […]

Für die Sicherheit von WordPress müssen alle **Zahnräder** ineinandergreifen – letztendlich hat ein Angreifer immer das Ziel das schwächste Zahnrad auszumachen.

7. Fazit

Der Artikel WordPress-Hacking soll einen **Eindruck** über den Ablauf eines Angriffs vermitteln – auch wenn die Phasen leicht vermischt sind. Angreifer verfolgen damit meist unterschiedliche Ziele. Oftmals dienen infizierte WordPress-Installationen als **Ausgangspunkt** für weitere Angriffe oder zum Versenden von Spam-Mails. Neben Vandalismus und Rachegelüste sind praktisch unzählige Absichten denkbar.

Wenn eure WordPress-Installation selbst schon gehackt wurde oder ihr die Sicherheit im Vorfeld verbessern wollt, dann empfehle ich nochmals folgende Anleitungen: »Hardnening WordPress« und meine Artikelserie »WordPress absichern«.

Bildquellen:

Skull: „#9358035“, https://de.fotolia.com/id/9358035

Über den Autor | Kuketz

In meiner freiberuflichen Tätigkeit als Pentester / Sicherheitsforscher (Kuketz IT-Security) schlüpfe ich in die Rolle eines »Hackers« und suche Schwachstellen in IT-Systemen, Webanwendungen und Apps (Android, iOS). Des Weiteren bin ich **Lehrbeauftragter** für IT-Sicherheit an der dualen Hochschule Karlsruhe, schärfe durch Workshops und Schulungen das

Sicherheits- und **Datenschutzbewusstsein** von Personen und bin unter anderem auch als Autor für die Computerzeitschrift c’t tätig.

Der Kuketz-Blog bzw. meine Person ist regelmäßig in den Medien (heise online, Spiegel Online, Süddeutsche Zeitung etc.) vertreten.

Mehr Erfahren →

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.