Website Sicherheits-Check: Sichere deine Webseite gegen Malware und Spam

Es ist keine große Überraschung, dass Sicherheit ein wichtiges Thema für Webentwickler und Betreiber von Webseiten geworden ist. Da das Internet immer beliebter wird und die neue Methode zur Kommunikation, Recherche und zum Einkaufen ist, sind Sicherheitschecks für Webseiten entscheidend, um die Verbreitung von Malware und Spam zu verhindern.

Egal ob du einen kleinen persönlichen Blog oder einen riesigen multinationalen Online-Shop betreibst, die Gefahr, gehackt zu werden, ist immer gegeben. Einige Leute werden deine Webseite verunstalten und Malware darin einbetten, versuchen, deine Daten oder die deiner Kunden zu stehlen und wichtige Inhalte auf deinem Server zu löschen. Du musst dich und deine sensiblen Informationen schützen.

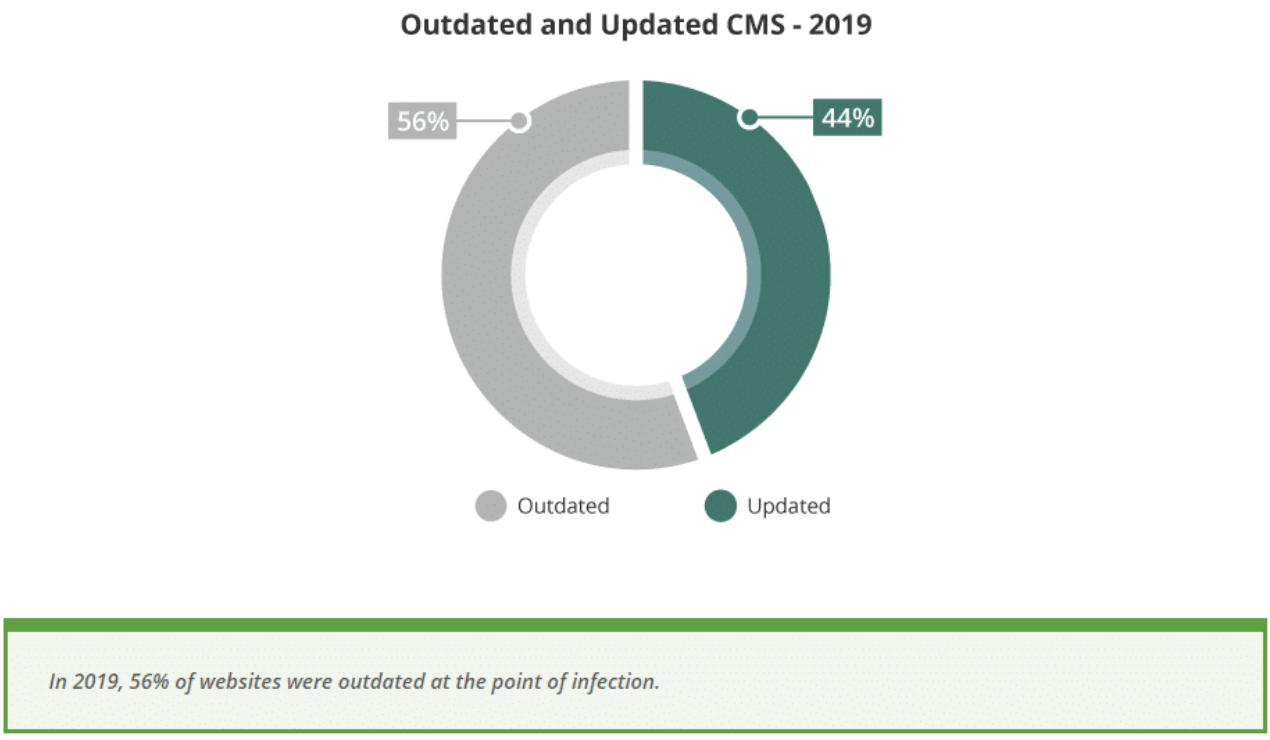
Lass uns genau herausfinden, wie sicher deine Webseite im Moment ist. Außerdem geben wir dir ein paar Tipps, wie du die niedrig hängenden Früchte entfernen kannst, die sich Malware-Autoren zunutze machen. WordPress ist von Haus aus sicher, aber es braucht ein wenig Arbeit, um es komplett zu reparieren.

Schau dir unseren Video-Leitfaden zur Überprüfung der Sicherheit deiner Webseite an

Webseiten Sicherheitscheck: Warum ist es wichtig?

Du denkst vielleicht, dass deine Webseite so klein und unwichtig ist, dass sich niemand die Mühe machen würde, sie ins Visier zu nehmen. Oder vielleicht hast du noch nie über Sicherheit nachgedacht und denkst, dass es nicht wichtig genug ist, um sich damit zu beschäftigen.

So zu denken ist der Grund, warum im Jahr 2013 mehr als 70% der WordPress Installationen anfällig für Angriffe waren. Viele dieser Angriffe waren auf veraltete Software zurückzuführen – weil die meisten Leute entweder nicht genug wissen oder sich nicht genug darum kümmern, ihre Webseiten zu sichern, was zu einer massiven Welle von Hackern führte, die es auf WordPress Installationen abgesehen hatten.



Veraltetes vs. aktualisiertes CMS im Jahr 2019.

Was könnte also passieren, wenn deine Webseite ein unerwünschtes Ereignis erlebt? Es ist nicht nur ein einfaches Ärgernis, das leicht durch das Ändern deines Passworts gelöst werden kann.

- In deine Webseite könnte Code eingeschleust sein, der Besucher dazu bringt, sich mit Malware zu infizieren, die extrem schwer zu finden und zu entfernen sein könnte.
- Deine kritischen Seiten können verunstaltet, ausgeblendet oder mit Links zu illegalen Webseiten gefüllt sein.
- Es kann zur Löschung von Inhalten wie Blogposts und Seiten führen.
- Sensible Daten wie Login- oder Kreditkarteninformationen, die dir, deinen Nutzern oder Kunden gehören, können gestohlen und online verkauft werden.
- Angriffe können sich auf andere Webseiten auf deinem Server ausbreiten.
- Wenn Google Malware auf deiner Webseite entdeckt, wird es den Zugang blockieren und sie aus den Suchergebnissen entfernen, was deine Bemühungen zur Suchmaschinenoptimierung (SEO) zunichte macht.
- Der Benutzername und das Passwort des Admin-Accounts könnten geändert werden, sodass du überhaupt keinen Zugriff mehr auf dein Backend hast.

Gehackte Webseiten können ein großes Problem darstellen, wenn du einen E-Commerce-Shop betreibst.

Und während du vielleicht sagst, dass deine Webseite nicht wichtig genug ist, sind nicht alle Angriffe gezielt. Viele WordPress Angriffe sind automatisiert – ein Bot sucht deine Webseite nach Schwachstellen ab und startet einen Angriff ohne menschliches Zutun.

Deshalb musst du Maßnahmen ergreifen, um deine Webseite zu sichern, egal was passiert.

Warum wird WordPress gehackt?

Hacking ist weit verbreitet, aber was sind die häufigsten Schwachstellen, die Hacker ausnutzen, um in deine Webseite einzubrechen?

Du stellst dir vielleicht vor, dass es ein schwieriger Prozess ist, in eine Webseite einzudringen, der Tage oder Wochen an Arbeit und ein enormes Wissen über Computer, Codierung und Server erfordert. Diese Situation könnte für gezielte Versuche zutreffen, die Verteidigungsanlagen einer großen, gut geschützten Webseite zu überwinden, aber die Geschichte sieht ganz anders aus, wenn es um kleine WordPress Domains geht.

Die überwiegende Mehrheit der Angriffe auf WordPress sind erfolgreich, weil die Leute leicht zu erratende Passwörter benutzen und ihre Themes und Plugins nicht aktualisieren. Hacker brechen in die meisten solcher Webseiten mit Hilfe von automatisierten Programmen ein.

Passwort-Cracking ist die einfachste Form des Hackens, die möglich ist, aber es ist so verbreitet, weil es funktioniert. Viele Leute belassen ihr WordPress Login auf dem Standard „admin“, was die Hälfte des Rätselraten ausschaltet, und benutzen dann ein einfaches, erratbares Passwort.

Wenn das nicht funktioniert, nutzen Hacker häufige Schwachstellen in beliebten Plugins oder veralteten Versionen von WordPress aus. Deshalb ist es so wichtig, alles auf dem neuesten Stand zu halten.

Es gibt viele kompliziertere, komplexere Wege, um in eine Webseite „einzubrechen“. Dennoch nutzen die meisten WordPress-Angriffe die niedrig hängenden Früchte eines unsicheren Passworts und veralteter Software, die es extrem einfach macht, auf deine Webseite zu gelangen.

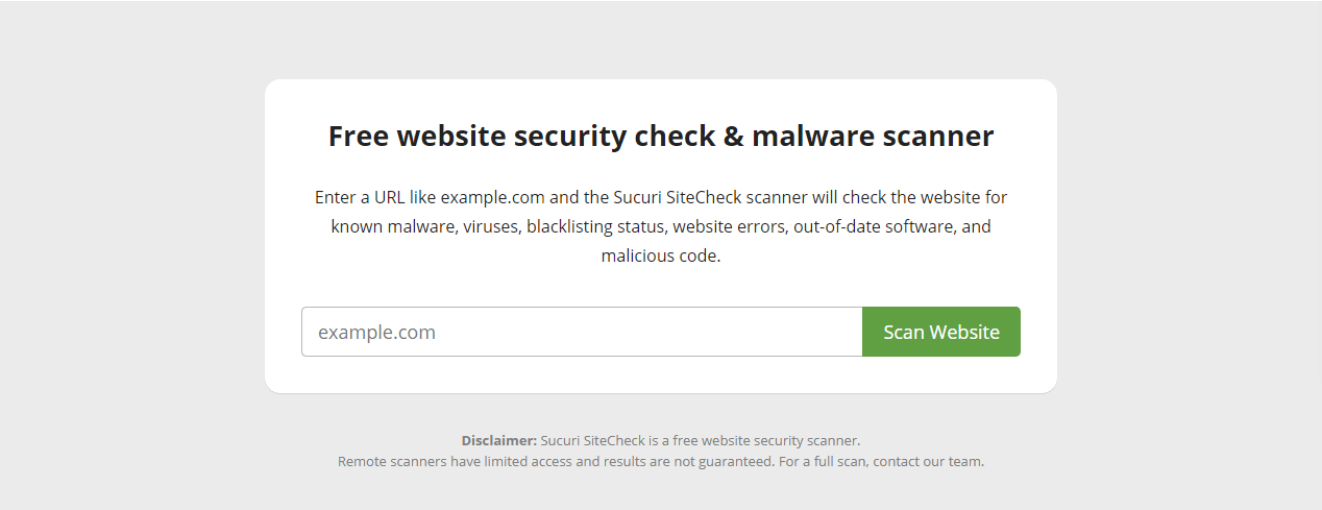
Wie man einen Sicherheitscheck der Webseite durchführt

Der erste Schritt zur Absicherung deiner Webseite: Feststellen, wie sicher deine Webseite bereits ist. Gibt es irgendwelche eklatanten Schwachstellen in deinem Backend, die du sofort flicken musst, oder irgendwelche einfachen Korrekturen, die du jetzt vornehmen kannst?

Verwende ein Online Tool

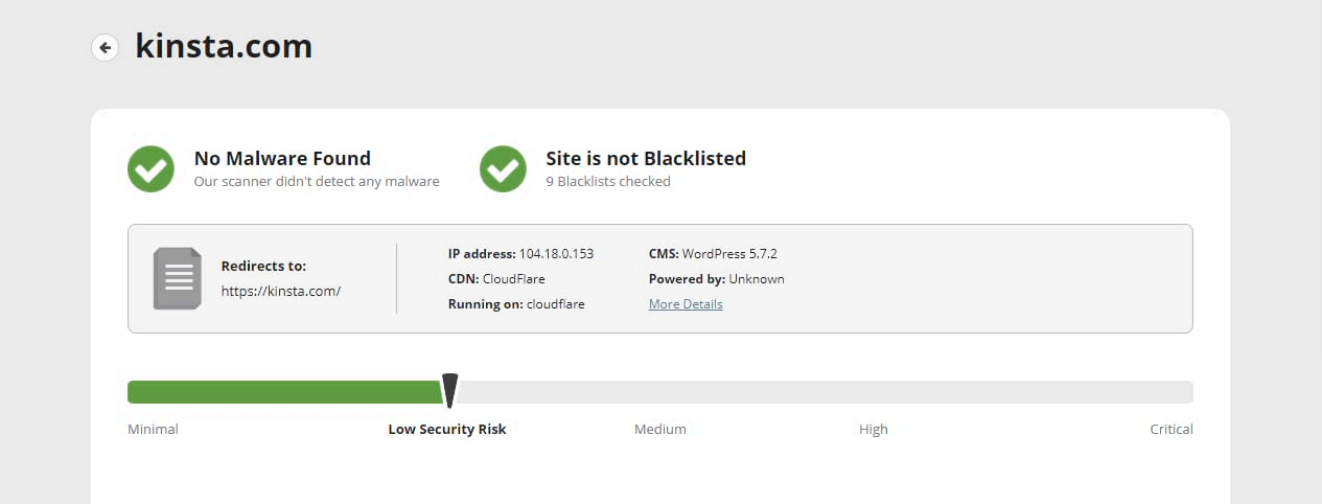
Eine schnelle und einfache Möglichkeit, deine Webseite auf Malware und Schwachstellen zu überprüfen, ist die Verwendung eines Online-Scanners. Diese scannen deine Webseite aus der Ferne und identifizieren häufige Probleme. Es ist super bequem, da es keine Software oder Plugins benötigt und nur ein paar Sekunden dauert.

Es gibt Dutzende von Online-Scannern zur Auswahl und wir werden ein paar weitere in unserem Tool-Bereich weiter unten auflisten, aber für den Moment nehmen wir einen beliebten, der einfach zu benutzen ist: Sucuri SiteCheck.



Sucuri SiteCheck.
Dieses Tool ist eine gute Wahl, denn du kannst das Sucuri Plugin installieren und dich direkt an die Behebung der Probleme machen, die es erkennt.

Sobald du deine Webseite gescannt hast, gleicht Sucuri sie mit Blocklisten ab, sucht nach offensichtlichen Problemen wie eingeschleustem Spam oder veralteter Software und scannt kurz jeden Code, auf den es zugreifen kann, auf Malware. Sucuri bietet auch einige Vorschläge, um deine Webseite gegen Angriffe zu schützen.



Scannen einer Webseite mit dem Sucuri Plugin.
Tools wie dieses sind ein hervorragender Ausgangspunkt für die Erkennung versteckter Malware und anderer Probleme.

Scanne deine Webseite mit einem WordPress Plugin

Während Online-Scanner gut genug funktionieren, ist es noch besser, ein Plugin zu installieren, das in der Lage ist, tief in die Wurzel deines Codes zu graben und Schwachstellen oder schwer zu entdeckende Malware herauszufischen.

Wir haben bereits Sucuri als eine Option erwähnt. Es gibt auch zwei noch populärere Sicherheits Plugins: All in One WP Security & Firewall und das meist heruntergeladene im Repository, Wordfence Security.

Sobald du das Plugin deiner Wahl installiert hast, wird es dich wahrscheinlich anweisen, sofort einen Scan durchzuführen. Der Vorteil dieser Plugins gegenüber Remote-Scannern ist, dass sie Malware entfernen und Änderungen automatisch vornehmen

können.

Suche nach seltsamen Änderungen

Wenn du den Verdacht hast oder weißt, dass deine Webseite mit Malware infiziert wurde, kann es manchmal schwierig sein, die Quelle zu lokalisieren. Hier sind ein paar unerklärliche Änderungen, die dir auffallen könnten, sowie die Dateien, auf die es Hacker typischerweise abgesehen haben:

- Plötzliche Links zu fremden Webseiten, die du nicht selbst hinzugefügt hast
- Neue Artikel und Seiten, die du nicht erstellt hast, oder der Inhalt bestehender Seiten ändert sich plötzlich
- Änderungen an Einstellungen, die du nicht vorgenommen hast
- Ein neuer Benutzer, besonders einer mit hohen Rechten, den du nicht hinzugefügt hast
- Plugins oder Themes, die du nicht installiert hast
- Malware kann oft bösartigen Code in deine Dateien einschleusen. Überprüfe Plugin- und Theme-Dateien, den Ordner **wp-content/uploads**, WordPress-Core-Dateien, die sich in einem falschen Verzeichnis befinden, **wp-config.php** und **.htaccess**. Du solltest ein Backup deiner Webseite machen und den Code verstehen, bevor du sensible Änderungen vornimmst.

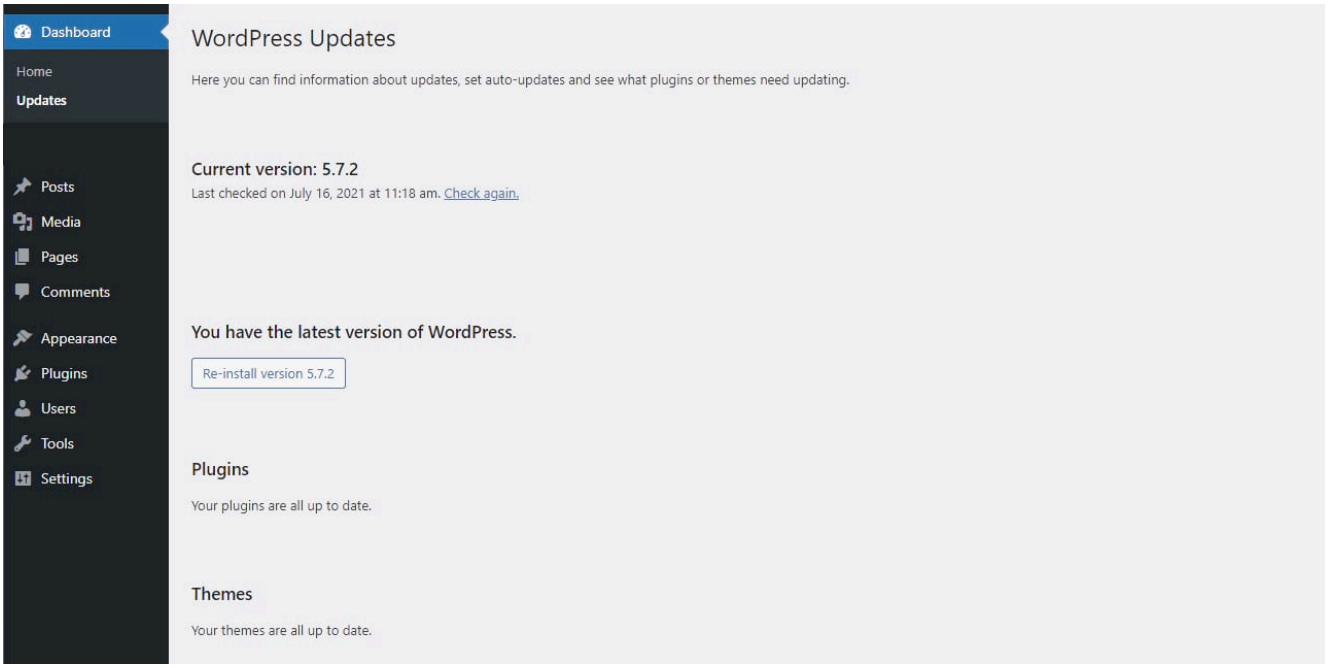
Wenn du dich mit FTP mit deiner Webseite verbindest, kannst du nach kürzlich geänderten Dateien sortieren, um Code zu finden, der dort nicht sein sollte.

Wenn deine Webseite regelmäßig mit Malware infiziert wird und du keine Ursache in den Dateien finden kannst, kann das Problem bei deinem Server oder einer anderen Webseite auf deinem Server liegen.

Stelle sicher, dass alles auf dem neuesten Stand ist

Wie wir bereits erwähnt haben, ist veraltete Software der mit Abstand häufigste Infektionsvektor in WordPress. Wenn es nur eine Sache gibt, die du tun kannst, um deine Webseite sicher zu halten, dann sollte es sein, WordPress auf dem neuesten Stand zu halten.

Der einfachste Weg, den Status aller Software auf deiner Webseite zu überprüfen, ist das **Dashboard > Updates**, welches dich darauf hinweist, wenn dein Core, Theme oder Plugins veraltet sind.



WordPress Updates

Da WordPress nun seit Version 5.5 automatische Updates durchführt, sollte nichts veraltet sein, es sei denn, du hast eine veraltete Version von WordPress. Wenn das nicht der Fall ist, kannst du alles von diesem Bildschirm aus aktualisieren.

Wenn du weißt, dass es eine neue Version von WordPress gibt, sie aber nicht angezeigt wird, klicke auf den Button **Erneut** prüfen unter **Aktuelle Version**.

Du kannst auch auf den Seiten **Plugins** > **Installierte Plugins**

oder **Erscheinungsbild** > **Themes** nach Updates suchen.

Important

Es ist wichtig, PHP auf dem neuesten Stand zu halten, besonders wenn du eine Version älter als 7.3 verwendest, da es erhebliche Sicherheitslücken aufweisen kann.

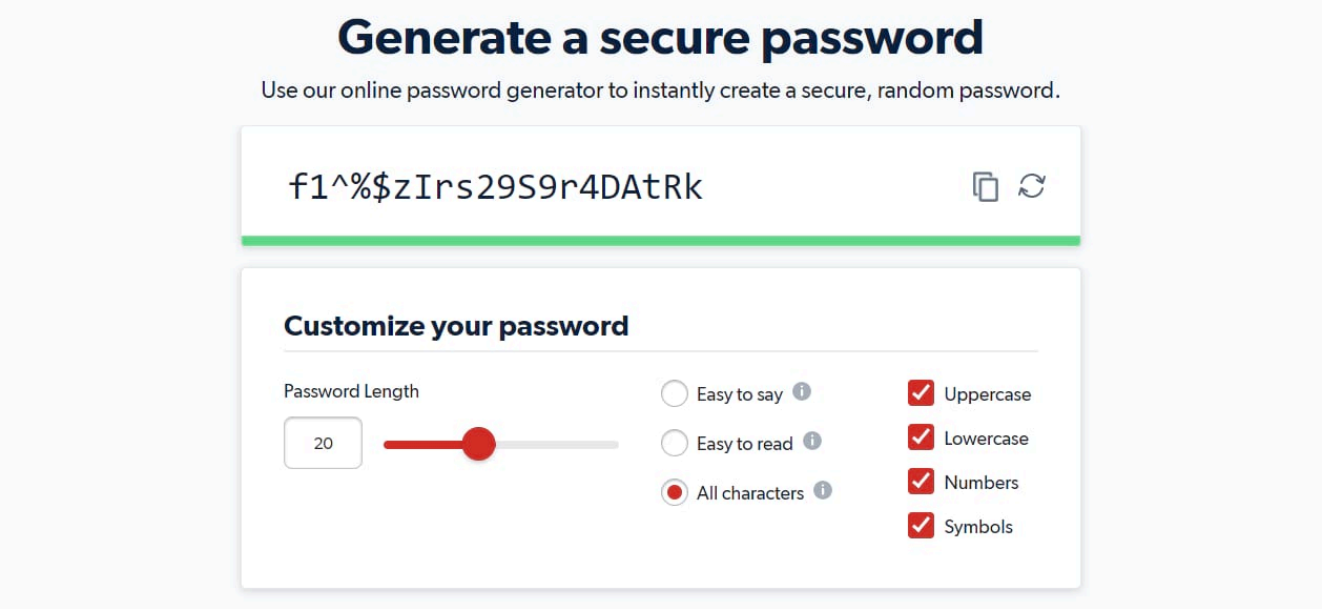
Sichere Konten und Passwörter

Ein schwaches Passwort für deinen Hauptaccount macht es jedem leicht, mit Brute-Force-Programmen in deine Webseite einzubrechen, ihnen Administrator-Zugang zu geben und die Möglichkeit, alles zu ändern.

Während ein kompliziertes Passwort mühsam zu merken ist und das Einloggen weniger bequem macht, ist es noch unangenehmer, wenn du deine Webseite nach einem Hack wiederherstellen musst. Es lohnt sich auf jeden Fall, ein sichereres Passwort zu verwenden, selbst wenn du es aufschreiben musst.

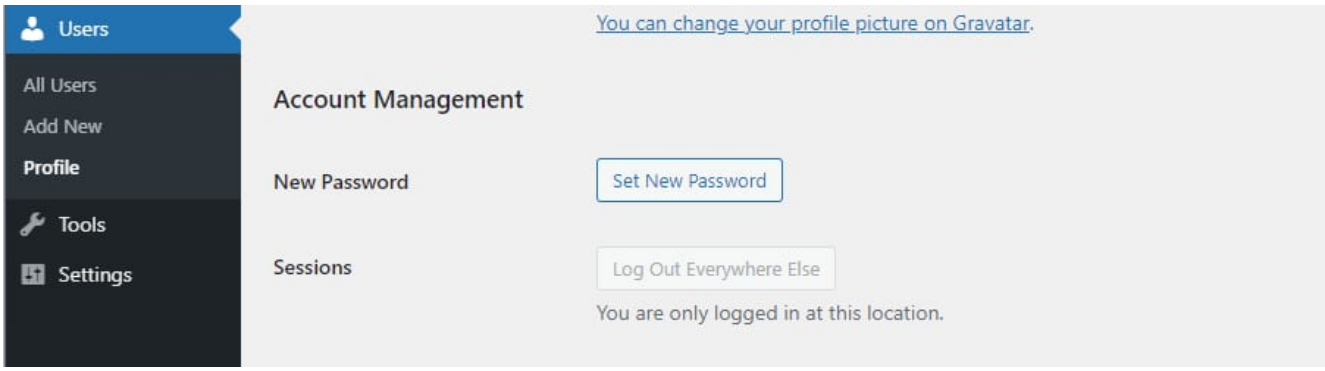
Dein Passwort sollte eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Symbolen verwenden. Am besten wäre es, wenn du es nicht auf Wörterbuchwörtern oder persönlichen, erratbaren Informationen wie deiner Adresse oder dem Namen eines Familienmitglieds basieren würdest.

Im besten Fall ist dein Passwort eine lange, verworrene Kette aus zufälligen Zeichen. Wir empfehlen dir dringend, einen Passwort-Manager zu verwenden. Verwende eine Webseite wie 1Password oder LastPass, um ein sicheres, nicht zu erratendes Passwort zu generieren.



Generiere ein sicheres Passwort mit LastPass.

Du kannst dein Passwort und deine E-Mail in WordPress aktualisieren, indem du zu **Benutzer** > **Alle Benutzer** oder direkt zu **Benutzer** > **Profil** gehst. Scrolle nach unten und finde **E-Mail** unter **Kontaktinformationen** und **Neues Passwort** unter **Kontoverwaltung**.



Ein neues Passwort in WordPress setzen

Wenn du auf der **Benutzerseite** bist, schaue dir alle deine Benutzer an und stelle sicher, dass niemand dabei ist, den du nicht kennst oder der unangemessene Berechtigungen hat. Du solltest jeden nicht identifizierten Benutzer mit Admin-Rechten sofort entfernen.

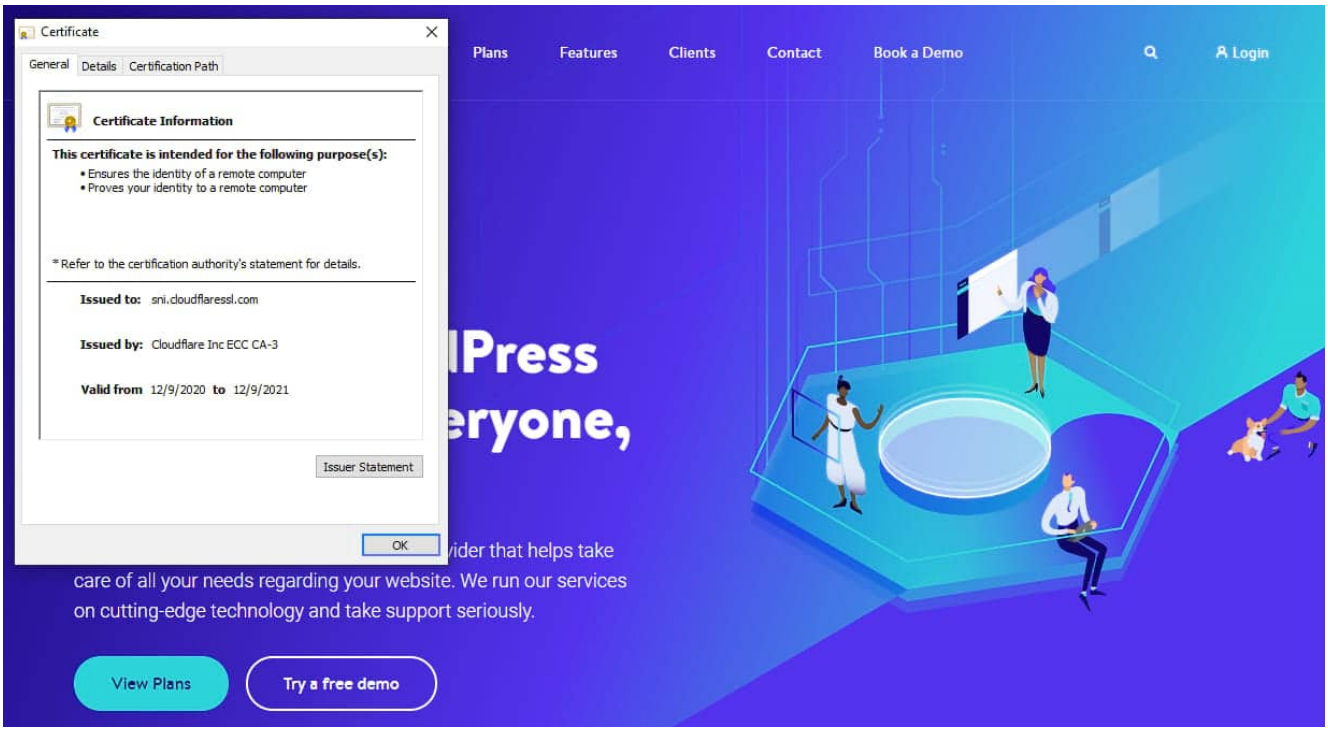
Wir empfehlen dir auch diesen Leitfaden zur Einschränkung von Benutzerrechten, damit nur dein Konto sensible Dateien auf deiner Webseite ändern kann.

Überprüfe dein SSL Zertifikat

Wenn dein SSL-Zertifikat veraltet ist, merkst du das in der Regel sofort; Browser wie Google Chrome blockieren den Zugriff auf deine Webseite mit einer großen Warnung über das abgelaufene Zertifikat. Wenn du dir nicht sicher bist oder bereits diesen Fehler bekommst, überprüfe dein SSL Zertifikat, um zu sehen, ob es auf dem neuesten Stand ist und ob du die neueste Version von SSL/TLS verwendest.

Wenn du eine Webseite besuchst, siehst du in den meisten Browsern ein Schloss-Symbol in der Adressleiste. Wenn dein Zertifikat abgelaufen ist, kann dieses Schloss rot sein oder einen Schrägstrich haben.

Klicke auf das Schlosssymbol und dann erneut, um Informationen zum Zertifikat zu erhalten, einschließlich des Ablaufdatums.



Überprüfe das SSL Zertifikat einer Webseite.

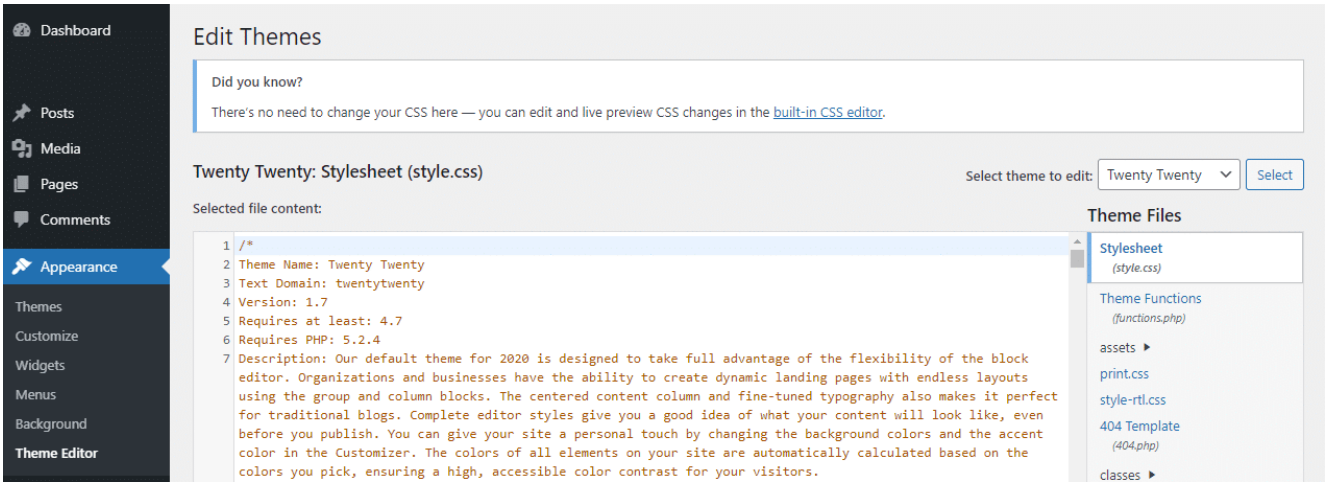
Du kannst auch einen SSL-Zertifikatschecker verwenden, um deine Webseite zu scannen und sicherzustellen, dass dein Zertifikat nicht abgelaufen ist und keine Schwachstellen in deinem SSL-Protokoll vorhanden sind.

Häufige Schwachstellen

Viele WordPress Seiten sind voll von winzigen Angriffsvektoren, die zwar harmlos erscheinen, aber mehr Informationen liefern können, als du teilen willst.

Eine sichtbare WordPress-Version in deinem Frontend verrät Hackern genau, welche Schwachstellen auf deiner Webseite vorhanden sind. Besonders, wenn du eine veraltete Version von WordPress verwendest, solltest du diese Informationen verstecken.

In deinem Backend findest du Dateieditoren unter **Appearance** > **Theme Editor** und **Plugins** > **Plugin Editor**.



Hinzufügen von Code zum Theme Editor

Diese Tools sind zwar sehr praktisch, aber es macht sie auch für jeden geeignet, der deine Webseite hackt, um etwas zu kaputt zu machen, also solltest du sie vielleicht abschalten. Du kannst dies tun, indem du diese Funktion in die **wp-config.php** einfügst:

```
define( 'DISALLOW_FILE_EDIT', true );
```

SQL-Injektionen sind eine gängige Methode, um in eine Webseite einzubrechen. Wenn du Formulare oder andere Benutzereingaben hast, schränke die Verwendung von Sonderzeichen ein und erlaube nur sichere, gebräuchliche Dateitypen, die hochgeladen werden können.

Für einen zusätzlichen Schutz kannst du Dateiverzeichnisse mit einem Passwort schützen.

Wie du deine Webseite sicher machst: Tipps und Tools

Wenn deine Webseite mit Malware infiziert ist, sollte ein gutes Sicherheits-Plugin ausreichen, um es zu entfernen. Und wir haben oben ein paar Sicherheitslücken beschrieben, auf die du achten solltest.

Schau dir unseren Video-Leitfaden zur Absicherung deiner Webseite an

Wir haben noch ein paar andere schnelle Tipps, um deine Webseite zu sichern und eine Infektion zu verhindern, bevor sie passieren kann. Die meisten dieser Tipps kannst du in wenigen Minuten umsetzen, so dass sie auch dann einfach einzurichten sind, wenn du dich mit WordPress und Websicherheit nicht auskennst.

Wähle einen sicheren Host

Wenn Hacker nach einem Weg auf deine Webseite suchen, wenden sie sich oft an den Server, um nach Exploits zu suchen. Es gibt viele billige Hosts, aber sie investieren nicht immer in die sichersten Server.

Shared Hosting kann ein Vektor für Infektionen sein. Wenn eine Webseite mit Malware infiziert ist, kann es sich potenziell auf alle Webseiten auf dem Server ausbreiten. Du könntest also mit einer Webseite voller Viren und SEO-Spam enden, und es wäre nicht einmal deine Schuld.

Deshalb ist es wichtig, dass du einen Hoster wählst, der sich um die Sicherheit kümmert und in sichere Server investiert. Du wirst immer noch Arbeit investieren müssen, um deine Webseite zu sichern, aber auf Server-Ebene sind deine Daten sicher.

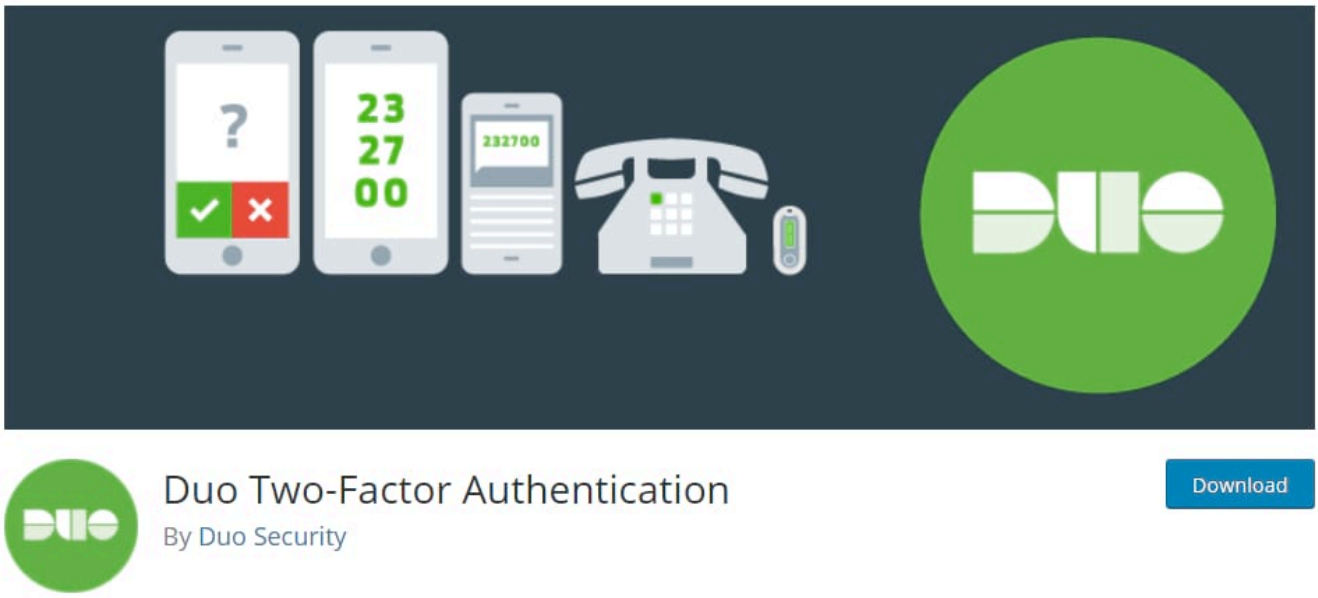
Aktiviere die Zwei-Schritt-Authentifizierung (2FA)

Die zweistufige Authentifizierung (auch bekannt als Zwei-Faktor-Authentifizierung oder 2FA) fügt einen weiteren Anmeldeschritt hinzu. Neben Benutzername und Passwort brauchst du oder jemand, der sich für dich ausgibt, noch eine weitere Information: einen einzigartigen Zusatzcode.

Es könnte ein Zahlencode sein, der an dein Telefon geschickt wird, was deinen WordPress-Account durch Brute-Force nahezu unknackbar machen kann. Alternativ kann es auch eine E-Mail-Verifizierung oder eine Information sein, die nur du kennst.

Während es keine eingebaute Möglichkeit gibt, die Zwei-Faktor-Authentifizierung zu aktivieren, fügen viele Plugins die Funktionalität zu WordPress hinzu.

Kinsta bietet die Zwei-Faktor-Authentifizierung für alle Kunden an. Wenn du kein Kinsta-Kunde bist, kannst du auch das bereits erwähnte Wordfence Plugin mit integrierter 2FA nutzen. Du kannst auch andere Tools für die Sicherheit deiner Webseite ausprobieren, wie z.B. das Two-Factor Plugin für E-Mail-Codes oder Duo, um eine Zwei-Faktor-Authentifizierung per Telefon über eine App einzurichten.



Duo Zwei-Faktor-Authentifizierung Plugin

Mache jeden Tag Backups

Ein Backup deiner Webseite kann sie nicht vor Hackern schützen, aber falls doch einmal etwas passiert, ist ein Backup von unschätzbarem Wert. Es kann den Unterschied ausmachen, ob du Wochen oder sogar Jahre an Arbeit verlierst oder ob du einfach ein Backup von vor dem Hack wiederherstellst.

Wenn du bei Kinsta bist, sichern wir dich mit täglichen automatischen Backups ab, die zwei Wochen lang gespeichert werden (30 Tage für diejenigen mit Kinstas Agenturpartnerprogramm). Zusätzlich kannst du fünf manuelle

Backups und ein herunterladbares Backup pro Woche erstellen und es gibt optionale Add-Ons, um stündlich Backups zu erstellen oder in die Cloud zu exportieren.

Plugins wie UpdraftPlus können ebenfalls helfen. Am besten ist es, einen Dienst zu wählen, der mindestens täglich ein Backup erstellt, um den Datenverlust zu minimieren.

Verwende eine Web Application Firewall

Eine Web Application Firewall (WAF) filtert mit strengen Regeln den eingehenden Traffic und blockiert IPs, die bekanntermaßen mit Hacker- oder DDoS-Angriffen in Verbindung gebracht werden. Es verhindert, dass viele Angriffe deinen Server überhaupt erreichen.

Obwohl du WAFs auf Serverebene einsetzen kannst, ist es am einfachsten, einen Cloud-basierten Service zu kaufen, wie zum Beispiel von Cloudflare oder Sucuri.

Verbindung über SSH oder SFTP

Manchmal musst du dich per FTP mit deiner Webseite verbinden, um dort Dateien hinzuzufügen oder zu ändern. Es ist immer besser, SFTP gegenüber FTP zu verwenden; der Unterschied ist einfach: SFTP ist sicher und FTP ist es nicht.

Bei FTP sind deine Daten nicht verschlüsselt. Wenn es jemandem gelingt, die Verbindung zwischen dir und deinem Server abzufangen, kann er alles sehen, von deinen FTP-Zugangsdaten bis zu den Dateien, die du hochlädst. Verbinde dich immer mit SFTP.

Du könntest auch einen SSH-Zugang in Betracht ziehen, der es dir erlaubt, dich mit einer Aufforderung zu verbinden und deine Webseite direkter zu verwalten. Es ist sicher und kann einfache Aufgaben aus der Ferne erledigen. Unser Guide zu SSH kann dir helfen, wenn du nicht weiterkommst.

Verhindere DDoS-Attacken

DDoS-Attacken verlangsamen deine Webseite zu einem Kriechgang, indem sie deinen Server mit tausenden von gefälschten Anfragen überschwemmen und so verhindern, dass potenzielle Leser oder Kunden auf sie zugreifen können. Hier sind ein paar Tipps, um sie zu stoppen, bevor sie passieren:

- Habe einen Plan für den Fall, dass ein DDoS-Angriff zuschlägt. Du willst nicht in Panik geraten, wenn du deinen Host alarmieren und die Attacke stoppen musst.
- Verwende eine Web Application Firewall, die möglicherweise gefälschten Traffic erkennen kann.
- Verwende speziell zugeschnittene Anti-DDoS-Software.
- Deaktiviere xmlrpc.php, um zu verhindern, dass Apps von Drittanbietern deinen Server nutzen.
- Deaktiviere die REST API für allgemeine Benutzer.

Brute-Force-Attacken verhindern

Brute-Force-Angriffe können ähnlich wie DDoS-Attacken sein, aber das Ziel ist es, dein Admin-Passwort zu erraten und in deine Webseite einzubrechen, anstatt deinen Server zum Absturz zu bringen. Trotzdem können sie auch deine Webseite ausbremsen.

- Auch hier kann eine WAF Bot-Traffic und krasse Brute-Force-Versuche herausfiltern.
- Verwende eine zweistufige Authentifizierung für deinen Admin-Account.
- Richte ein Aktivitätsprotokoll ein und behalte unautorisierte Login-Versuche im Auge.
- Ändere die URL der Login-Seite und begrenze die Anzahl der Login-Versuche.
- Schütze deine Anmeldeseite mit einem Passwort.
- Verwende ein langes, zufällig generiertes Passwort und

ändere es etwa alle Jahre.

Webseiten Security Tools, die du kennen solltest

Neben den bereits erwähnten Tools gibt es noch ein paar weitere Online-Sicherheitstools, die dir dabei helfen werden, deine Webseite abzusichern:

- Intruder.io: Scanne nach den neuesten Sicherheitslücken.
- SSL Server Test: Entwickler-Tool, das dein SSL Zertifikat analysiert und Schwachstellen identifiziert.
- HTML Purifier: Filtert bösartigen Code/XSS heraus, toll, wenn du infizierten Code hast, den du bereinigen musst.
- Mozilla Observatory: Umsetzbare Ratschläge, um deinen Code von häufigen Schwachstellen zu bereinigen.
- sqlmap: Ein Penetrationstest Tool, um Exploits in deinem SQL Code zu identifizieren.
- Detectify: Scanne deine Web-Apps mit der Hilfe von ethischen Hackern.
- WPScan: Ein CLI-basierter WordPress-Scanner.
- SonarQube: Schreibe standardkonformen Code frei von Sicherheitslücken.

Webseiten Sicherheit Checkliste

Ist deine Webseite sicher vor Angriffen? Stelle sicher, dass du fast alles auf dieser Checkliste angekreuzt hast:

- Nutzt du eine sichere, qualitativ hochwertige Hosting Umgebung?
- Hast du deine Webseite mit einem Plugin oder Online-Scanner auf Viren überprüft?
- Hast du ein Aktivitätsprotokoll installiert und

überwachst du es auf ungewöhnliche Änderungen?
- Verwenden du und alle Benutzer mit hohen Privilegien sichere Passwörter und Zwei-Faktor-Authentifizierung? Sind alle Emails korrekt?
- Sind WordPress, seine Themes und Plugins sowie die zugrunde liegenden Systeme wie PHP auf dem neuesten Stand?
- Ist dein SSL Zertifikat sicher und auf dem neuesten Stand?
- Hast du deine Webseiten, Einstellungen und Dateien auf unerklärliche Änderungen, das Löschen oder Hinzufügen von Inhalten oder Links, die du nicht hinzugefügt hast, überprüft?
- Ist deine Login-Seite durch ein Passwort und begrenzte Login-Versuche geschützt?
- Hast du nach neuen Benutzern gesucht, die du nicht hinzugefügt hast?
- Sind Formulare, Kommentarboxen und andere Quellen für Benutzereingaben gesichert? (Verbiete Sonderzeichen und beschränke Datei-Uploads auf bekannte Dateitypen).
- Hast du **xmlrpc.php** und die REST API deaktiviert, um DDoS-Angriffe zu verhindern?
- Hast du die Bearbeitung von Themes und Plugins im Dashboard deaktiviert?
- Hast du einen täglichen Backup-Service eingerichtet?
- Hast du eine Web Application Firewall eingerichtet?

Zusammenfassung

Die Sicherheit einer Webseite ist keine Nebensache. Wenn du dich also noch nicht darum kümmerst, ist es jetzt an der Zeit, es zu einer Priorität zu machen. Wenn du gehackt wirst, ist das nicht nur ärgerlich – es kann in beschädigter SEO, verheerendem Datenverlust, verlorenem Vertrauen der Nutzer und Malware enden, die immer wieder zurückkommt.

Du musst kein erfahrener Entwickler sein, um ein paar zusätzliche Schritte zu unternehmen, um deine Webseite zu sichern. Und das beginnt mit einem ordentlichen Sicherheitscheck der Webseite. Selbst etwas so Einfaches wie die Wahl eines besseren Passworts oder der Wechsel zu einem sichereren Host kann den Unterschied ausmachen.

Brauchst du mehr Sicherheitstipps? Erfahre mehr über 19 weitere Möglichkeiten, deine Webseite zu sichern. Und teile deine Vorschläge gerne in den Kommentaren unten!
