De ultieme gids voor het beveiligen van sites van klanten

KINSTA

Scan de QR code voor de laatste versie
van dit e-book, of ga naar:
https://kinsta.com/nl/ebooks/

Gepubliceerd door KINSTA

De ultieme gids voor het beveiligen van sites van klanten

Inhoud

De ultieme gids voor het beveiligen van sites van klanten

Volgens internet live stats worden elke dag meer dan 100.000 websites gehackt. 😲 Daarom is het zo belangrijk om de tijd te nemen en onderstaande aanbevelingen door te nemen over hoe je je WordPress beveiliging kunt verbeteren.

Als het gaat om de beveiliging van WordPress, is er veel meer dan alleen het beschermen van je site, in deze gids geven we je de beste aanbevelingen over hoe je dat kunt doen.

Investeer in veilige WordPress hosting

Laten we beginnen met de beveiliging op webserver niveau waarvoor je WordPress host verantwoordelijk is. Het is erg belangrijk dat je een host kiest die je als bedrijf kunt vertrouwen als je de sites van je klanten naar hen verplaatst.

Als je WordPress op je eigen VPS host, dan moet je de technische kennis hebben om veel dingen zelf te doen. Maar om eerlijk te zijn, proberen een sysadmin te zijn om €20/maand te besparen is geen effectieve manier om een bedrijf te runnen.

Server hardening is de sleutel tot het onderhouden van een goed beveiligde WordPress omgeving. Er zijn meerdere lagen hardware- en softwarematige beveiligingsmaatregelen nodig om ervoor te zorgen dat de IT-infrastructuur waarin WordPress sites worden gehost, in staat is zich te verdedigen tegen geavanceerde bedreigingen, zowel fysiek als virtueel.

Om deze reden moeten servers die WordPress hosten worden geüpdatet met het nieuwste besturingssysteem en (beveiligings) software, en moeten ze grondig worden getest en gescand op kwetsbaarheden en malware.

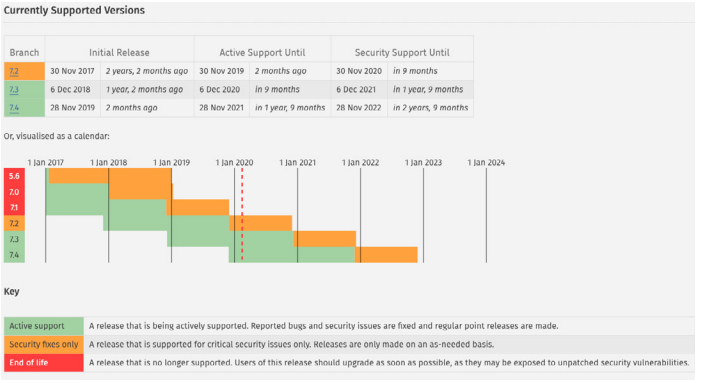
Firewalls en inbraakdetectiesystemen moeten ook aanwezig zijn om de sites van je klanten goed te beschermen, zelfs tijdens de WordPress installatie- en realisatiefase. Alle software die op de machine is geïnstalleerd en bedoeld is om de inhoud van WordPress te beschermen, moet compatibel zijn met de nieuwste databasebeheersystemen om optimale prestaties te behouden. De server moet ook worden geconfigureerd om veilige netwerk- en bestandsoverdracht protocollen (zoals SFTP in plaats van FTP) te gebruiken om gevoelige inhoud te verbergen voor kwaadwillige indringers.

Bij Kinsta gebruiken we Google Cloud Platform voor al onze WordPress klanten om een veilige WordPress hosting te garanderen. Beveiliging is vanaf het begin in onze architectuur ingebouwd en het is een veel veiligere methode dan andere die vandaag de dag beschikbaar zijn.

Gebruik de nieuwste PHP-versie

PHP is de ruggengraat van elke WordPress site, dus het is erg belangrijk om ervoor te zorgen dat de sites van je klanten de laatste versie op je server gebruiken. Elke grote release van PHP wordt doorgaans twee jaar na de release volledig ondersteund.

Gedurende die tijd worden bugs en beveiligingsproblemen regelmatig verholpen en gepatcht. Op dit moment heeft iedereen die op versie PHP 7.1 of lager draait geen ondersteuning meer voor beveiligingsupdates en staan ze mogelijk bloot aan diverse beveiligingsproblemen.



Currently Supported Versions

Branch	Initial Release		Active Support Until		Security Support Until	
7.2	30 Nov 2017	*2 years, 2 months ago*	30 Nov 2019	*2 months ago*	30 Nov 2020	*in 9 months*
7.3	6 Dec 2018	*1 year, 2 months ago*	6 Dec 2020	*in 9 months*	6 Dec 2021	*in 1 year, 9 months*
7.4	28 Nov 2019	*2 months ago*	28 Nov 2021	*in 1 year, 9 months*	28 Nov 2022	*in 2 years, 9 months*

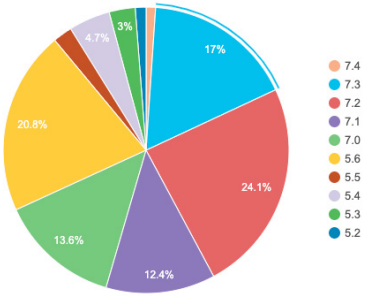
Or, visualised as a calendar:

Key

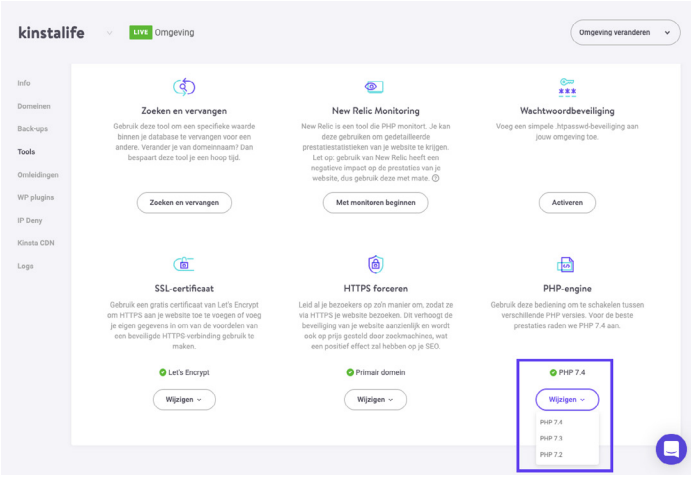
Active support	A release that is being actively supported. Reported bugs and security issues are fixed and regular point releases are made.
Security fixes only	A release that is supported for critical security issues only. Releases are only made on an as-needed basis.
End of life	A release that is no longer supported. Users of this release should upgrade as soon as possible, as they may be exposed to unpatched security vulnerabilities.

En raad eens? Volgens de officiële WordPress Statistics pagina draait ongeveer 34% van de WordPress websites nog steeds op PHP 5.6 of lager, wat betekent dat meer dan een derde van de websites op dit moment PHP versies gebruikt die niet langer worden ondersteund. Dat is eng!

PHP-versies



Bij Kinsta adviseren wij alleen stabiele en ondersteunde versies van PHP te gebruiken, waaronder 7.2, 7.3 en 7.4. PHP 5.6, 7.0 en 7.1 zijn uitgefaseerd. Je kunt zelfs vanuit het MyKinsta dashboard met één druk op de knop schakelen tussen de PHP-versies.



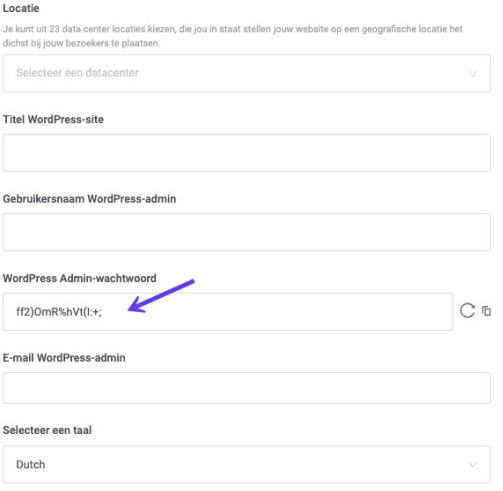
Als je het zelf wilt proberen, ga dan naar demo.kinsta.com en probeer het eens!

Gebruik slimme gebruikersnamen en wachtwoorden

Verrassend genoeg is één van de beste manieren om je WordPress beveiliging te verbeteren het gebruik van slimme gebruikersnamen en wachtwoorden. Klinkt vrij eenvoudig, toch? Nou, bekijk SplashData's jaarlijkse lijst van 2019 met de meest populaire wachtwoorden die het hele jaar door zijn gestolen (gesorteerd op volgorde van populariteit).

- 123456
- 123456789
- qwerty
- password
- 1234567
- 12345678
- 12345
- iloveyou
- 111111
- 123123

Het meest populaire wachtwoord is "123456". Dat is een van de redenen waarom we bij Kinsta op nieuwe WordPress installaties een complex wachtwoord afdwingen om te worden gebruikt voor de wp-admin login (zoals hieronder te zien bij ons één-klik installatieproces). Dit is verplicht.



Bekijk deze functie met de MyKinsta demo. 

De WordPress functie wp_hash_password maakt gebruik van het phpass password hashing framework en achtvoudige MD5 gebaseerde hashing. Voor je WordPress installatie moet je nooit de standaard “admin” gebruikersnaam gebruiken, maar unieke WordPress gebruikersnamen maken voor beheerdersaccounts.

Het is ook belangrijk om verschillende wachtwoorden te gebruiken voor elke klantensite. De beste manier om ze op te slaan is lokaal in een versleutelde database op je computer.

Een goede gratis tool hiervoor is KeePass. Als je deze niet wilt gebruiken zijn er ook online wachtwoordmanagers zoals 1Password of LastPass.

Gebruik altijd de nieuwste versie van WordPress, plugins en thema’s

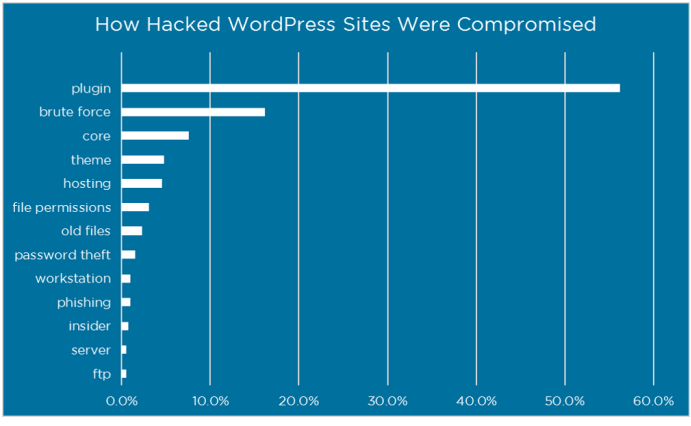
Een andere zeer belangrijke manier om de beveiliging van de sites van je klanten te verbeteren is om ze altijd up-to-date te houden. Dit omvat WordPress core, plugins en thema’s. Deze worden niet voor niets geüpdatet, en vaak zijn er ook beveiligingsverbeteringen en bugfixes.

Helaas zijn er miljoenen bedrijven die verouderde versies van WordPress software en plugins draaien en nog steeds geloven dat ze op het juiste pad van zakelijk succes zitten. Ze noemen diverse redenen om niet bij te

werken, zoals “onze site zal stuk gaan” of “aanpassingen aan WordPress core zullen overschreven worden” of “plugin X zal niet meer werken” of “we hebben de nieuwe functionaliteit gewoon niet nodig”.

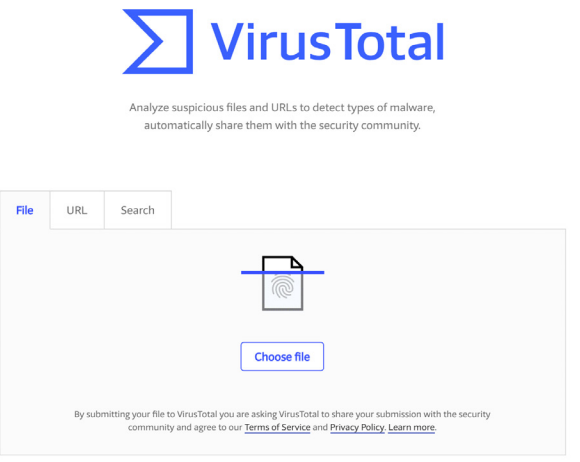
In feite breken websites vooral door bugs in oudere WordPress versies. Aanpassingen in WordPress core worden afgeraden door het WordPress team en deskundige ontwikkelaars die de risico’s ervan begrijpen. En WordPress updates bevatten meestal must-have beveiligingspatches, samen met de toegevoegde functionaliteit die nodig is om de nieuwste plugins uit te voeren.

Wist je dat melding is gemaakt van plugin-kwetsbaarheden die 55,9% van de bekende ingangen voor hackers vertegenwoordigen? Dat is wat WordFence vond in een onderzoek waar ze meer dan 1.000 WordPress site-eigenaren interviewden die het slachtoffer waren van aanvallen. Door je plugins te updaten kun je er voor zorgen dat je niet één van deze slachtoffers wordt.



Het is ook aan te raden om alleen vertrouwde plugins te installeren voor je klanten. De “uitgelichte” en “populaire” categorieën in de WordPress plugin repository kunnen een goede plek zijn om te beginnen. Of download ze direct van de website van de ontwikkelaar. Wij raden je sterk af om gebruik te maken van nulled WordPress plugins en -thema’s.

Je kunt een online hulpmiddel zoals VirusTotal gebruiken om een plugin of de bestanden van een thema te scannen om te zien of het malware bevat.



Er zijn ook veel middelen beschikbaar om je te helpen op de hoogte te blijven van de nieuwste WordPress beveiligingsupdates en -kwetsbaarheden. Zie een aantal daarvan hieronder:

- WP Security Bloggers: Een geweldige geaggregeerde bron van 20+ beveiligingsfeeds.

- WPScan Vulnerability Database: Catalogiseert meer dan 10.000 WordPress Core, Plugin en Thema kwetsbaarheden.
- ThreatPress: Dagelijks bijgewerkte database van WordPress plugins, thema's en kwetsbaarheden van WordPress core.
- Officieel WordPress veiligheidsarchief

Vergrendel je WordPress admin

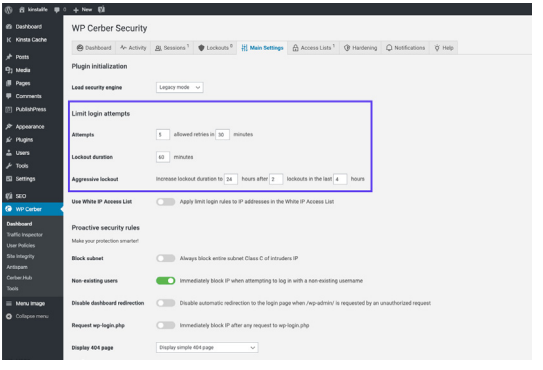
Soms is de populaire strategie van WordPress beveiliging door middel van obscuriteit effectief voor een gemiddeld online bedrijf en WordPress site. Als je het moeilijker maakt voor hackers om bepaalde backdoors te vinden dan heb je minder kans om aangevallen te worden. Het vergrendelen van de WordPress admin van je klanten en het inloggen is een goede manier om je beveiliging te verbeteren. Twee geweldige manieren om dit te doen is ten eerste door het wijzigen van je standaard wp-admin login URL en ook het beperken van aanmeldingspogingen.

Hoe je je WordPress login URL kunt wijzigen
Standaard is de login URL van je WordPress site domein.nl/wp-admin. Eén van de problemen hiermee is dat alle bots, hackers en scripts die er zijn dit ook weten. Door het veranderen van de URL kun je je site een minder makkelijk doelwit maken en beter beschermen tegen brute kracht aanvallen.
Dit is geen oplossing voor alle problemen, het is gewoon een kleine truc die je zeker kan helpen om je site te beschermen.

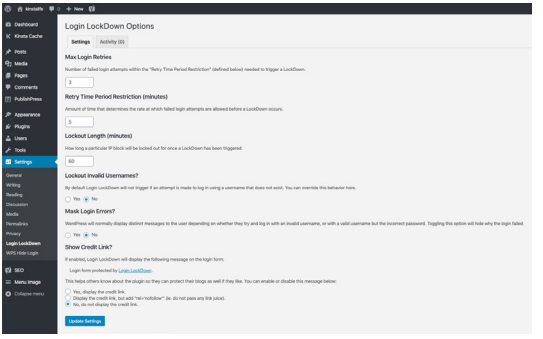
Om je WordPress login URL te wijzigen raden wij je aan de gratis WPS Hide login plugin te gebruiken. Vergeet niet om een unieke naam te kiezen die niet al op een lijst staat die een bot of script zou kunnen proberen te scannen.

Hoe kan ik de aanmeldingspogingen beperken?

Hoewel de bovenstaande oplossing van het veranderen van je admin login URL kan helpen het merendeel van de kwaadaardige loginpogingen te verminderen, kan het instellen van een limiet ook zeer effectief zijn. De gratis Cerber Limit Login Attempts plugin is een geweldige oplossing om eenvoudig limieten voor aanmeldingspogingen en IP whitelists en blacklists in te stellen.



Als je op zoek bent naar een meer eenvoudige WordPress beveiligingsoplossing, is een ander goed alternatief: de gratis Login Lockdown plugin.

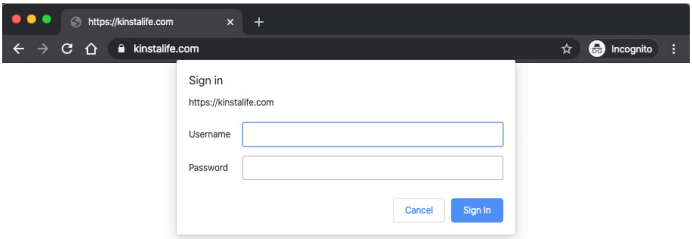


Login LockDown registreert het IP-adres en de tijdstempel van elke mislukte aanmeldingspoging. Als er meer dan een bepaald aantal pogingen worden gedetecteerd binnen een korte periode van hetzelfde IP-bereik, dan is het inloggen niet meer mogelijk vanaf dat IP-bereik. En het is volledig compatibel met de WPS Hide login plugin die we hierboven hebben genoemd.

Als je de sites van je klanten verplaatst naar Kinsta, hoeft je geen extra plugin te installeren omdat ons platform deze automatisch beperkt en blokkeert.

Hoe kan ik basis HTTP-authenticatie toevoegen (.htpasswd bescherming)?

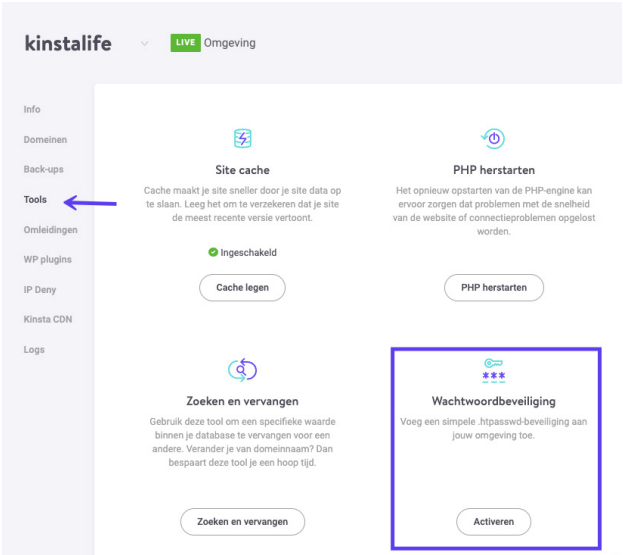
Een andere manier om je admin te vergrendelen is het toevoegen van HTTP-authenticatie. Hiervoor is een gebruikersnaam en wachtwoord nodig voordat je zelfs maar toegang kunt krijgen tot de WordPress inlogpagina.



Bekijk deze functie met de MyKinsta demo.

Belangrijk: Dit moet over het algemeen niet worden gebruikt op e-commerce sites of lidmaatschap sites, aangezien gebruikers daar ook moeten kunnen inloggen. Maar het kan een zeer effectieve manier zijn om te voorkomen dat bots je site proberen te benaderen.

Als je de sites van je klanten bij Kinsta host, kunt je gebruik maken van onze eenvoudige wachtwoordbeveiliging (htpasswd) in het MyKinsta-dashboard (bekijk hoe op de gratis MyKinsta demoaccount). Je kunt het vinden onder de “Tools” sectie op je site. Klik op “Inschakelen”, kies een gebruikersnaam en wachtwoord en het is geregeld!



Bekijk deze functie met de MyKinsta demo.

Nadat wachtwoordbeveiliging is ingeschakeld, heeft de WordPress site extra authenticatie nodig om toegang te krijgen tot de site. Je kunt de gegevens op elk moment wijzigen of uitschakelen wanneer je ze niet meer nodig hebt.

Profiteer van Two-Factor Authenticatie (2FA)

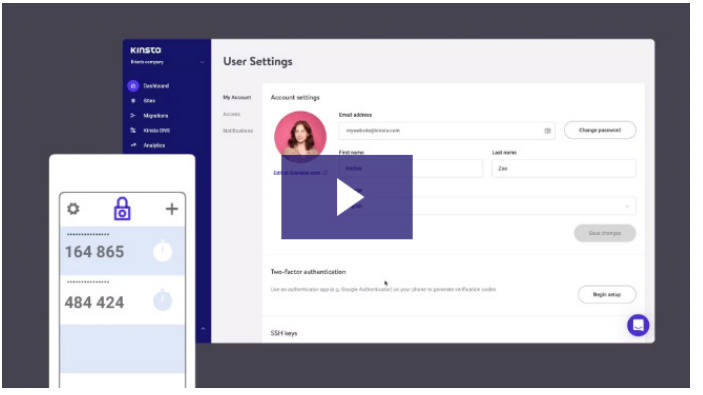
Twee-factor authenticatie is een proces in twee stappen waarbij je niet alleen je wachtwoord nodig hebt om in te loggen, maar ook een tweede methode om in te loggen. In de meeste gevallen is dit 100% effectief in het voorkomen van brute kracht aanvallen op de WordPress sites van je klanten.

Er zijn twee onderdelen als het gaat om twee-factor authenticatie voor sites van klanten.

De eerste is je account en of dashboard dat je bij je hosting provider hebt. Als iemand hier toegang toe krijgt, kan hij de wachtwoorden van al je klanten wijzigen, hun websites verwijderen, DNS-records wijzigen en allerlei vreselijke dingen doen. Bij Kinsta gebruiken we Authenticator-gebaseerde 2FA voor je MyKinsta-dashboard omdat:

- Authenticator-gebaseerde 2FA is veiliger dan SMS-gebaseerde 2FA omdat het niet gebonden is aan je mobiele telefoonnummer en niet afhankelijk is van legacy SMS-technologie. Dit maakt Authenticator-gebaseerde 2FA bestand tegen SIM-swapping technieken.
- Authenticator-gebaseerde 2FA kan worden gebruikt met apps voor wachtwoordmanagers zoals 1Password voor extra gemak. Door je 2FA-gegevens toe te voegen aan een wachtwoordmanager, hoeft je niet te vertrouwen op een extern apparaat om in te loggen op MyKinsta.

Hier zie je hoe gemakkelijk het is om in te stellen:



Het tweede deel van de twee-factor authenticatie heeft betrekking op de eigenlijke WordPress installaties van je klanten. Hiervoor zijn er een aantal plugins die je misschien wilt testen en aanbevelen:

- Duo Two-Factor Authentication
- Google Authenticator
- Two Factor Authentication

Na het installeren en configureren van één van de bovenstaande plugins op een site, zal je meestal een extra veld op de WordPress login pagina krijgen om de beveiligingscode in te voeren.
Of, met de Duo-plugin, log je eerst in met je inloggegevens en moet je vervolgens een authenticatiemethode kiezen, zoals Duo Push, call of passcode.

Gebruik HTTPS voor versleutelde verbindingen - SSL-certificaat

Eén van de meest over het hoofd geziene manieren om de beveiliging van WordPress te verbeteren is het installeren van een SSL-certificaat en sites te laten werken met HTTPS. HTTPS (Hypertext Transfer Protocol Secure) is een mechanisme waarmee elke browser of webapplicatie veilig verbinding kan maken met een website. Een groot misverstand is dat als de sites van je klanten geen creditcards accepteren, ze geen SSL nodig hebben.

Laten we een paar redenen bekijken waarom HTTPS niet alleen voor e-commerce belangrijk is. Veel hosts, waaronder Kinsta, bieden gratis SSL-certificaten aan met Let's Encrypt.

6 Belangrijke redenen waarom HTTPS niet alleen belangrijk is voor e-commerce

1. Toegevoegde veiligheid
Hoe belangrijk is de login informatie van je klanten? Je moet weten dat elke keer als een gebruiker inlogt, die informatie in platte tekst aan de server wordt doorgegeven. HTTPS is absoluut noodzakelijk voor het onderhouden van een veilige verbinding tussen een website en een browser. Zo kun je beter voorkomen dat hackers en/of een tussenpersoon toegang krijgen tot de sites van je klant.

2. SEO
Google heeft officieel gezegd dat HTTPS als factor gebruikt wordt bij het bepalen van de zoekresultaten. Aangezien de meeste van je klanten waarschijnlijk elk mogelijk voordeel van SEO en SERP's

zouden willen hebben om hun concurrenten te verslaan, is dit een no-brainer.

3. Vertrouwen en geloofwaardigheid
Volgens een onderzoek van GlobalSign zoekt 28,9% van de bezoekers naar het (groene) hangslot in de adresbalk in hun browser. En 77% van hen maakt zich zorgen over het feit dat hun gegevens online worden onderschept of misbruikt. Door dat (groene) hangslot, hebben klanten direct meer vertrouwen in de wetenschap dat hun gegevens veiliger zijn.

4. Verwijzingsgegevens
Veel mensen realiseren zich niet dat HTTPS naar HTTP-verwijzingsgegevens geblokkeerd zijn in Google Analytics.
Wat gebeurt er dan met de gegevens? Nou, het grootste deel ervan wordt gewoon op één hoop gegooid met het "directe verkeer" gedeelte. Als iemand van HTTP naar HTTPS gaat, wordt de referrer nog steeds doorgegeven.

5. Chrome waarschuwingen
Vanaf 24 juli 2018 zijn versies van Chrome 68 en hoger begonnen met het markeren van alle niet-HTTPS-sites als "Niet veilig" en vanaf 2020 begon de populaire browser de ondersteuning voor oudere TLS-versies af te bouwen. Google maakt het voor bezoekers veel duidelijker dat een WordPress website misschien niet op een beveiligde verbinding draait. Daarom is HTTPS belangrijker dan ooit!

6. Prestaties
Door een protocol dat HTTP/2 heet, kunnen degenen die correct geoptimaliseerde sites over HTTPS draaien zelfs snelheidsverbeteringen zien. HTTP/2 vereist HTTPS vanwege

de ondersteuning van de browser. De verbetering van de prestaties is te danken aan verschillende redenen, zoals HTTP/2 die betere multiplexing, parallellisme, HPACK-compressie met Huffman-versleuteling, de ALPN-extensie en serverpush kan ondersteunen. En met TLS 1.3 zijn HTTPS-verbindingen nog sneller.

Kinsta ondersteunt TLS 1.3 op al onze servers en Kinsta CDN.

Bekijk onze uitgebreide WordPress HTTPS-migratiegids om je op weg te helpen en leer meer in onze TLS vs SSL-vergelijking.

Schakel XML-RPC uit

In de afgelopen jaren is XML-RPC een steeds groter doelwit geworden voor brute kracht aanvallen. Er zijn een paar WordPress plugins zoals Jetpack die afhankelijk zijn van XML-RPC, maar een meerderheid van de mensen zal dit niet nodig hebben en dan het kan slim zijn om de toegang tot XML-RPC eenvoudigweg uit te schakelen.

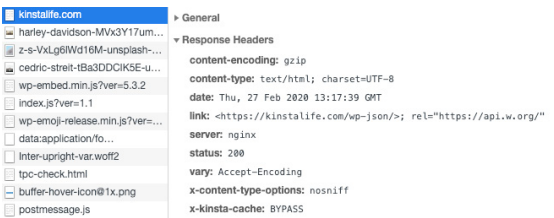
Als je klant bij Kinsta bent, hoef je je daar geen zorgen over te maken, want wij hebben actieve en passieve maatregelen genomen om aanvallen en kwaadwillige bedoelingen tegen te gaan. Om precies te zijn, wanneer een aanval via XML-RPC wordt gedetecteerd, wordt er een klein stukje code toegevoegd aan het Nginx-configuratiebestand om te voorkomen dat ze een 403-fout produceren.

Toevoegen van de nieuwste HTTP security headers

Een andere stap die je kunt nemen om de beveiliging van je WordPress site te verbeteren, is om te profiteren van HTTP security headers. Deze zijn meestal geconfigureerd op webserver niveau en vertellen de browser hoe hij zich moet gedragen bij het omgaan met de inhoud van je sites. Er zijn veel verschillende HTTP security headers, hieronder staan de meest belangrijkste.

- Content-Security Policy
- X-XSS-Protection
- Strict-Transport-Security
- X-Frame-Options
- Public-Key-Pins
- X-Content-Type

Je kunt controleren welke headers worden gebruikt op je WordPress installatie, door Chrome devtools te lanceren en te kijken naar de headers van de response van je site.



Hier is een voorbeeld van kinstalife.com (een demosite). Je kunt zien dat we gebruik maken van de x-content-type-options header.

Als het gaat om sites van klanten, zoals in het getoonde voorbeeld, worden standaard altijd x-content-type-options toegevoegd, terwijl x-frame-options en strict-transport-security alleen worden ingesteld als dat nodig is.

Als je de sites van je klanten moet scannen, kunt je dat doen met de gratis securityheaders.io-tool van Scott Helme.

Het is ook belangrijk om te onthouden dat wanneer je HTTP security headers implementeert, dit invloed kan hebben op je WordPress subdomeinen. Als je bijvoorbeeld de Content Security Policy header toevoegt en de toegang tot domeinen beperkt, dan moet je ook je eigen subdomeinen toevoegen. Als je niet zeker weet hoe je ze moet implementeren, kunt je altijd je host om hulp vragen.

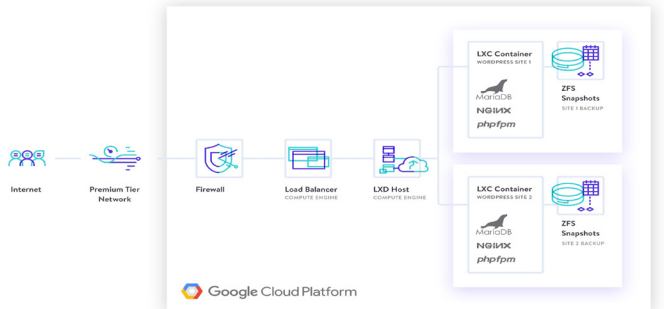
Gebruik WordPress beveiligingsplugins

Er zijn een heleboel geweldige ontwikkelaars en bedrijven die geweldige oplossingen bieden om je WordPress site beter te beschermen. Hier is een kleine selectie:

- Sucuri Security
- iThemes Security
- Wordfence Security
- WP Security Audit Log
- WP fail2ban
- All In One WP Security & Firewall
- SecuPress
- BulletProof Security
- VaultPress
- Google Authenticator – Two Factor Authentication

- Security Ninja
- Defender
- Astra Web Security
- Shield Security
- Hide my WP
- WebARX

Kinsta heeft hardware firewalls, actieve en passieve beveiliging, uptime controles per minuut en diverse andere geavanceerde functies om te voorkomen dat aanvallers toegang krijgen tot je gegevens. Als je site, ondanks onze inspanningen, wordt gehacked, repareren we deze gratis.

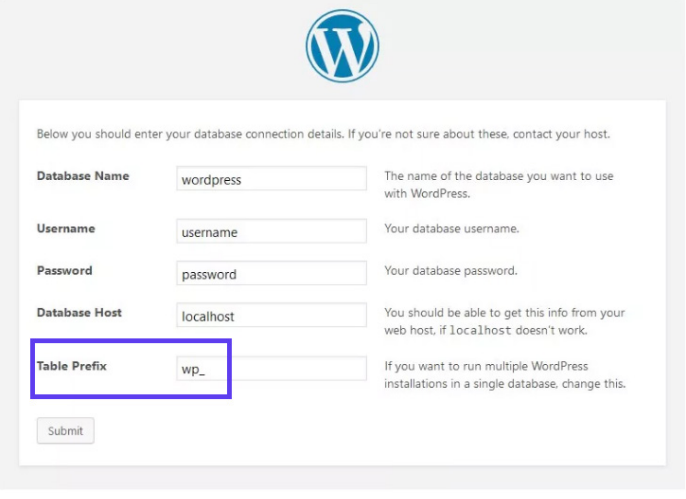


Een zeer belangrijke functie die veel veiligheidsplugins bevatten is een checksum controle. Dit betekent dat ze elk van de WordPress installaties van je klant inspecteren en zoeken naar wijzigingen aan de hoofdbestanden zoals die door WordPress.org worden geleverd (via de API). Eventuele wijzigingen of aanpassingen aan deze bestanden kunnen duiden op een hack.

Je kan ook WP-CLI gebruiken om je eigen checksum controle uit te voeren. Bekijk deze extra WordPress beveiligingsplugins die de slechteriken kunnen helpen uitsluiten.

Verbeteren van de beveiliging van de database

Er zijn een aantal manieren om de veiligheid van je WordPress database te verbeteren. De eerste is het gebruik van een slimme database naam. Door de naam van je database te veranderen in een meer obscure naam helpt het je site te beschermen door het moeilijker te maken voor hackers om je database gegevens te raden en te benaderen.

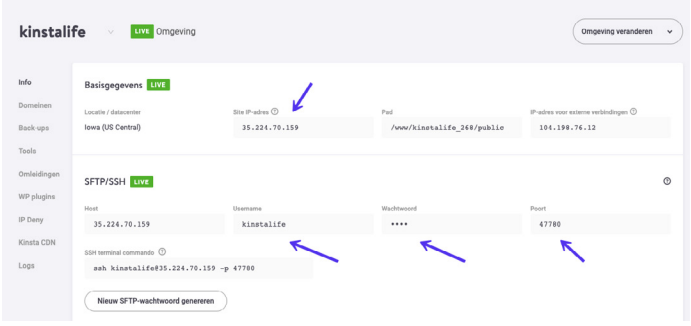


Een tweede aanbeveling is het gebruik van een andere table prefix. Wanneer je WordPress installeert, vraagt het om een table prefix. Standaard gebruikt WordPress `wp_`. Dit veranderen naar iets als `39xw_` kan veel veiliger zijn.

Als je klant bij Kinsta bent en alle sites van je klanten bij ons host, is dit niet nodig. We hebben de site en de database al voor je beveiligd!

Gebruik altijd veilige verbindingen

We kunnen niet genoeg benadrukken hoe belangrijk het is om veilige verbindingen te gebruiken! Zorg ervoor dat je WordPress host voorzorgsmaatregelen neemt zoals het aanbieden van SFTP of SSH. SFTP of Secure File Transfer Protocol (ook bekend als SSH file transfer protocol), is een netwerkprotocol dat wordt gebruikt voor de overdracht van bestanden. Het is een veel veiligere methode dan standaard FTP.



Bekijk deze functie met de MyKinsta demo.

Wij ondersteunen bij Kinsta alleen SFTP-verbindingen om ervoor te zorgen dat je gegevens veilig en versleuteld blijven. De meeste WordPress hosts gebruiken doorgaans ook poort 22 voor SFTP. Wij gaan hier bij Kinsta nog een stap verder, elke site heeft een willekeurige poort die te vinden is in je MyKinsta-dashboard.

Bestands- en serverrechten controleren

Bestandsrechten op zowel de installaties van je klanten als de webservers zijn cruciaal om de veiligheid van deze omgevingen te versterken. Als de rechten te losjes zijn, kan iemand gemakkelijk toegang krijgen tot een site en een ravage aanrichten. Aan de andere kant, als je permissies te strikt zijn, kan dit de functionaliteit op je site verstoren. Het is dus belangrijk om de juiste rechten over de hele linie in te stellen.

Je kunt een gratis plugin als iThemes Security gebruiken om de rechten op de WordPress sites van je klanten te scannen.

File Permissions

Reload File Permissions Details

Relative Path	Suggestion	Value	Result	Status
/	755	755	OK	
wp-includes	755	755	OK	
wp-admin	755	755	OK	
wp-admin/js	755	755	OK	
wp-content	755	755	OK	
wp-content/themes	755	755	OK	
wp-content/plugins	755	755	OK	
wp-content/uploads	755	755	OK	
wp-config.php	444	644	WARNING	
nginx.conf	444	644	WARNING	
Relative Path	Suggestion	Value	Result	Status

Hier zijn enkele typische aanbevelingen voor permissies als het gaat om bestands- en mapmachtigingen in WordPress:

- Alle bestanden moeten 644 of 640 zijn. Uitzondering: wp-config.php moet 440 of 400 zijn om te voorkomen dat andere gebruikers op de server het kunnen lezen.
- Alle mappen moeten 755 of 750 zijn.
- Geen enkele map mag ooit 777 worden gegeven, zelfs de upload directory niet.

Zie het WordPress Codex-artikel over het wijzigen van bestandsrechten voor een meer uitgebreide uitleg.

DDoS-bescherming

DDoS is een type DOS-aanval waarbij meerdere systemen worden gebruikt om een enkel systeem aan te vallen, waardoor een Denial of Service (DoS)-aanval wordt veroorzaakt. DDoS-aanvallen zijn niets nieuws - volgens Britannica dateert het eerste gedocumenteerde geval uit begin 2000. In tegenstelling tot iemand die je site hackt, brengen dit soort aanvallen normaal gesproken geen schade toe aan je site, maar halen ze je site gewoon een paar uur of dagen naar beneden.

Wat kun je doen om jezelf te beschermen? Eén van de beste aanbevelingen is om gebruik te maken van een gerenommeerde veiligheidsdienst zoals Cloudflare of Sucuri.

Hun geavanceerde DDoS-bescherming kan worden gebruikt om DDoS-aanvallen in alle vormen en maten te beperken, inclusief die welke gericht zijn op de UDP- en ICMP-protocollen, evenals SYN/ACK-, DNS-amplification en Layer 7-aanvallen. Andere voordelen zijn dat je je achter een proxy bevindt die helpt om je oorspronkelijke IP-adres te verbergen, hoewel het niet compleet waterdicht is.

Vergeet niet de provider die je webhost gebruikt toe te voegen, want dat is ook vrij belangrijk.

Hardware firewalls, zoals de Google Cloud Platform Firewall die we bij Kinsta gebruiken, zijn aanwezig en hebben zeer strikte softwarematige beperkingen om de sites van je klanten te beschermen en hebben ook software om DDoS-aanvallen te detecteren als ze gebeuren.

Dit betekent dat jij en je klanten het voordeel krijgen van een beveiligingsmodel dat in de loop van 15 jaar is opgebouwd en dat momenteel producten en diensten zoals Gmail, Google Search, enz. beveiligt. Google heeft momenteel meer dan 500 fulltime beveiligingsprofessionals in dienst.

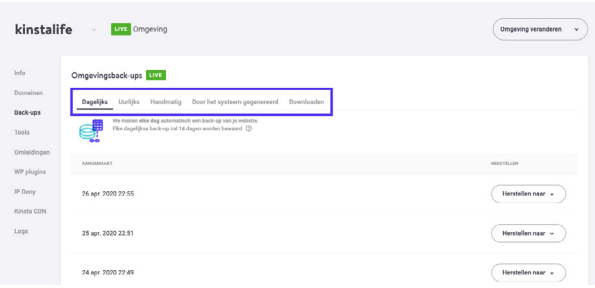
Naast het Google Cloud Platform gebruiken we ook Linux-containers (LXC en LXD) om ze te orkestreren, waardoor we niet alleen elk account, maar ook elke afzonderlijke WordPress site volledig kunnen isoleren.

Gaat het toch mis? Kinsta biedt gratis hackreparatie en malwareverwijdering. Als één van de sites van je klanten is geïnfecteerd, zal ons supportteam alles doen wat nodig is om het op te ruimen.

Lees meer over hoe serieus we de beveiliging van Kinsta nemen! 

Maak altijd back-ups

Hoe veilig je site ook is, het zal nooit 100% veilig zijn. Daarom wil je back-ups voor het geval dat het ergste gebeurt. Back-ups zijn het enige wat iedereen weet dat ze nodig hebben, maar niet altijd hebben. De meeste van de hier beschreven aanbevelingen zijn veiligheidsmaatregelen die je kunt nemen om de sites van je klanten en je bedrijf beter te beschermen.



Bekijk deze functie met de MyKinsta demo.

De meeste managed WordPress hostingproviders bieden nu back-ups aan. Kinsta heeft vijf verschillende soorten back-ups:

- Dagelijks: Kinsta maakt elke 24 uur geautomatiseerde back-ups van de sites van al je klanten, zodat je ‘s nachts gemakkelijk kunt uitrusten.
- Uurlijks: Als je een frequenter back-upschema nodig hebt, kun je 6-uurs- of uurlijkse automatische back-ups activeren voor elke doelsite die dat nodig heeft (dit komt bovenop je maandplan).
- Handmatig: als geautomatiseerde back-ups niet genoeg zijn, kun je handmatige back-ups maken voor elke site die je beheert en deze extra kopie beschikbaar houden voor 14 dagen of meer, op basis van je huidige plan.
- Systeem-gegenereerd: voor kritieke taken zoals het gebruik van de zoekvervangstool in MyKinsta, het live zetten van een testomgeving en het herstellen van een back-up naar

je live-omgeving, zal Kinsta systeem-gegenereerde back-ups triggeren.
- Downloadbaar archief: als dit alles niet genoeg is, kunt je één keer per week een zip-bestand downloaden van elke klantensite met website-bestanden en een SQL-bestand met de inhoud van de database van de site.

Back-up opties komen bij Kinsta samen met de mogelijkheid om elke site met één klik eenvoudig herstellen. Handig toch?

Test gratis hoe eenvoudig het maken van back-ups met MyKinsta is! 

Als je host geen back-ups aanbiedt, zijn er enkele populaire WordPress plugins die je kunt gebruiken om het proces te automatiseren.

WordPress back-up plugins

Met WordPress back-up plugins kunt je je back-ups via FTP ophalen of integreren met een externe opslagbron zoals Amazon S3, Google Cloud Storage, Google Drive of Dropbox. We raden je ten zeerste aan om met een incrementele oplossing te werken zodat het minder opslagruimte gebruikt:

- Duplicator
- WP Time Capsule
- BackupBuddy
- UpdraftPlus
- BackUpWordPress

- BackWPup
- WP BackItUp

Kinsta staat alleen incrementele back-up plugins toe vanwege prestatieproblemen: we behandelen dit alles voor je op serverniveau zodat het de sites van je klanten niet vertraagt.

Samenvatting

Beveiliging speelt zich af op diverse lagen. Hoe meer je erin slaagt om nieuwe beveiligingslagen op elkaar te stapelen, hoe veiliger de sites van je klanten zullen zijn. Het begint allemaal met het gebruik van slimme wachtwoorden, het up-to-date houden van WordPress core en plugins en het volgen van diverse best-practices op het gebied van beveiliging die we hier hebben behandeld.

Maar dat is niet alles wat je moet doen om de kans te verkleinen dat je te maken krijgt met gehackte sites. Door te kiezen voor een managed WordPress host zoals Kinsta, worden de meeste beveiligingsmaatregelen voor je verzorgd, zodat je een solide, veilige en schaalbare basis kunt opbouwen om de toekomst van de sites van je klanten veilig te stellen. En die van je bedrijf.

Wil je proberen hoe gemakkelijk het is om sites op Kinsta te beheren?

Bekijk dan demo.mykinsta.com!


KINSTA