WordPress: 10 tips om je website te beveiligen

Houd hackers buiten 's werelds populairste content management systeem

Willem L. Middelkoop
31 mrt. 2019

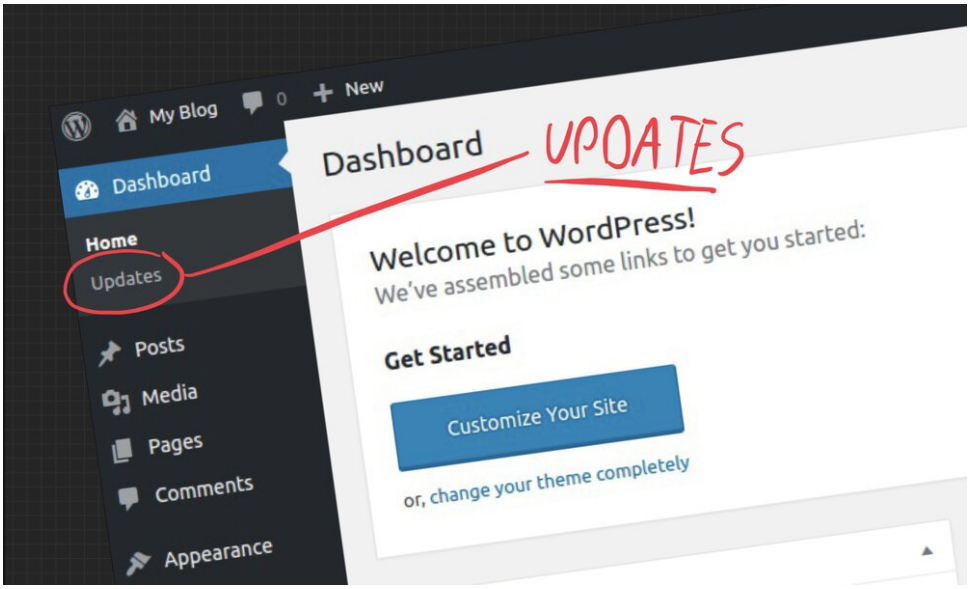
Veel mensen gebruiken WordPress om hun website te beheren, daarom is het geen verrassing dat mensen me vragen om naar de beveiliging van hun site te kijken. Als ethisch hacker kom ik WordPress in verschillende vormen, maten en staten tegen. Sommige zijn echt slecht beschermd tegen hacks. Voorkom dat jouw site gehackt wordt met deze 10 praktische tips.

1) WordPress bijwerken (en plugins + thema's)

De meerderheid van WordPress hacks is het gevolg van een gebrekkig updatebeleid. Hackers gebruiken geautomatiseerde bots om verouderde softwareversies te vinden die bekende

beveiligingsproblemen bevatten. Zodra ze hebben ontdekt dat jouw website kwetsbaar is, is het hacken ervan vaak een fluitje van een cent.

Tegenwoordig kan het updaten van WordPress automatisch worden gedaan, dus je hoeft het niet zelf te doen. Bekijk de instructies over hoe je WordPress bijwerkt.

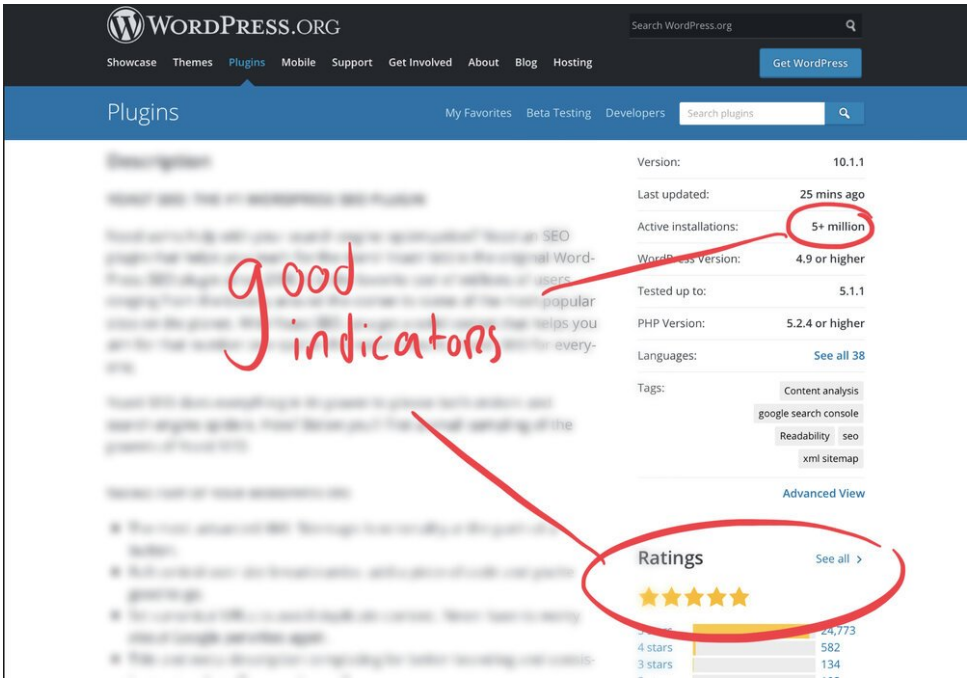


WordPress updaten vanuit het wp-admin dashboard

2) Plugins en Thema's

De slechte beveiligingsreputatie die WordPress heeft verdiend, is voornamelijk te wijten aan de uitbreidbare onderdelen van het platform, met name plugins en thema's. Dit zijn de primaire aanvalsvectoren die door cybercriminelen worden gebruikt om jouw WordPress-website te hacken en misbruiken. Hun beveiligingsproblemen zijn meestal het gevolg van fouten en vergissingen tijdens de ontwikkeling.

Wees zeer terughoudend en voorzichtig met het installeren van plugins op jouw WordPress-website. Je moet controleren wie de ontwikkelaar van de plugin of het thema is en bepalen of ze een goede reputatie hebben als het gaat om het schrijven van veilige code. Plugins en thema's met veel downloads worden vaak actief onderhouden, een goede indicator voor beveiliging. Werk alle plugins en thema's bij en houd het beveiligingsoverzicht in de gaten met behulp van een website zoals wpvulndb.com.

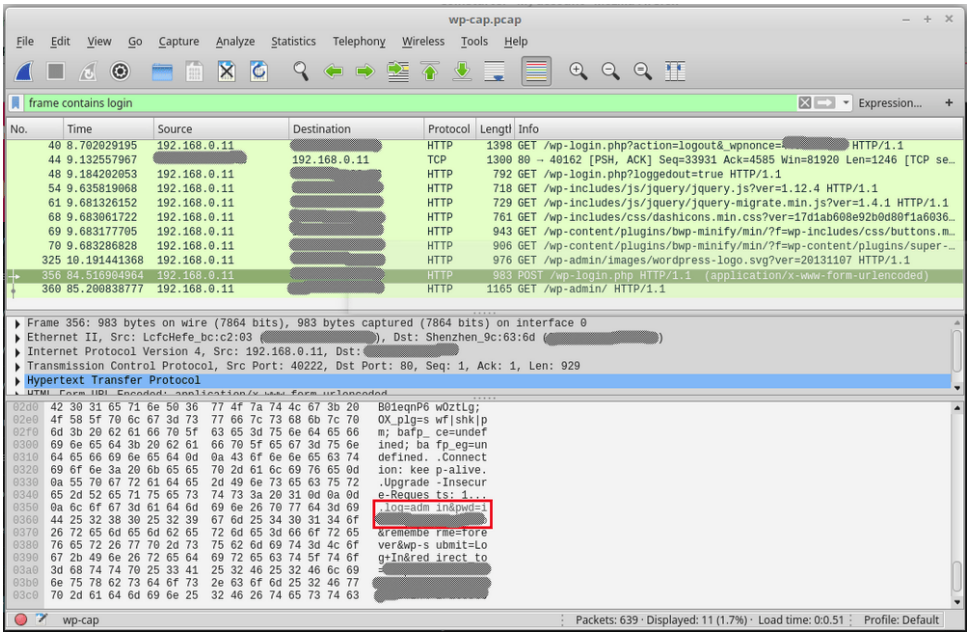


Controleer de reputatie van een WordPress plugin door te kijken naar het aantal downloads en de beoordeling

3) Gebruik encryptie (TLS/SSL)

WordPress-websites zonder TLS/SSL-encryptie vormen een beveiligingsrisico, omdat wanneer je inlogt om de website te beheren, je wachtwoord in leesbare tekst wordt verzonden. Dit betekent dat iedereen die jouw netwerkverkeer afluistert, gemakkelijk jouw wachtwoord kan bemachtigen. Met een geldig wachtwoord kunnen hackers gewoon inloggen, je wilt het ze toch niet zo gemakkelijk maken, toch?

Gebruik TLS/SSL om alle communicatie tussen de webserver en jouw browser te versleutelen. Dat betekent dat niemand kan ontcijferen wat je in het wachtwoordveld typt door naar het netwerkverkeer te kijken. TLS/SSL-certificaten die je nodig hebt om HTTPS-encryptie in te schakelen, zijn tegenwoordig erg goedkoop. Vraag jouw hostingprovider om er een op jouw site te installeren.

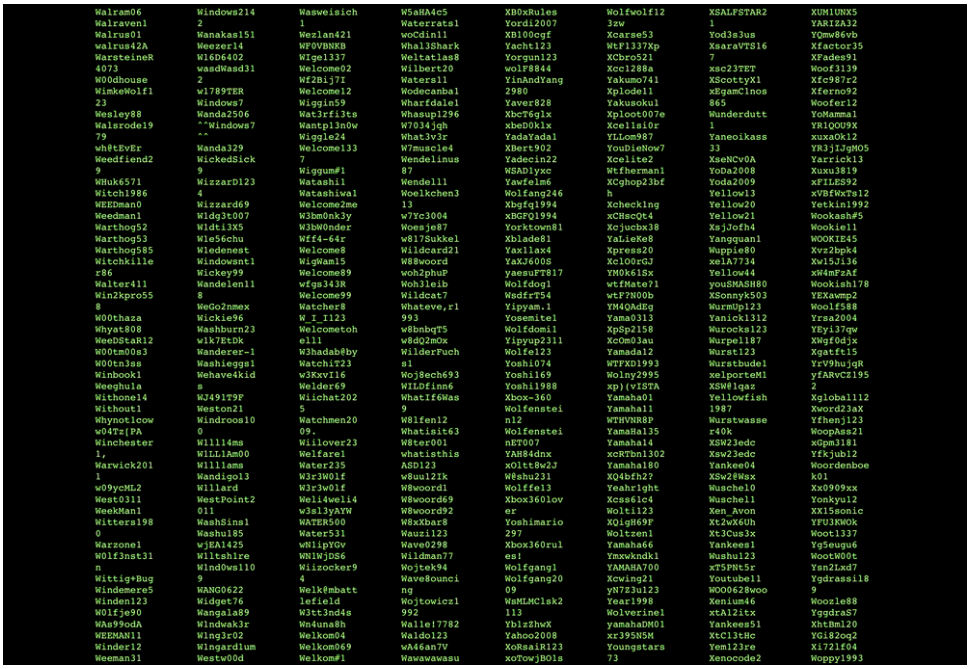


Snuffelen naar WordPress wachtwoorden met WireShark packet capturing (via blog.wpscans.com)

4) Gebruik sterke wachtwoorden

Ongeacht of je alle andere tips volgt om jouw website te beveiligen, zwakke wachtwoorden zijn een andere veelvoorkomende oorzaak van WordPress-beveiligingsinbreuken. Omdat de meeste WordPress-installaties een ”admin”-gebruiker hebben, kunnen hackers wachtwoord woordenboeken gebruiken om automatisch jouw wachtwoord te raden.

Denk aan een sterk wachtwoord als iets dat nog nooit eerder is gebruikt. Dit betekent meestal langer, met meer verschillende tekens, zonder bekende woorden of zinnen. Je kunt een wachtwoordgenerator gebruiken om iets te krijgen dat echt moeilijk te raden is (en gemakkelijk te vergeten...). Voorkom het gebruik van hetzelfde wachtwoord op meerdere sites en overweeg het inschakelen van tweestapsverificatie voor maximale toegangscontrole.



Wachtwoord dictionary attacks gebruiken lijsten met bekende (gelekte) wachtwoorden, je kunt ze vinden op schimmige delen van het internet

5) Gebruik een vertrouwde computer en netwerk

Net zoals je jouw geld en gadgets niet moet laten zien in louche straten, moet je voorzichtig zijn waar (en wanneer) je inlogt op jouw website. Een computer met spyware, malware of een virus kan toetsaanslagen (en jouw wachtwoord) registreren en naar criminelen sturen. Of zelfs op een niet-digitale manier: een tegenstander kan letterlijk over je schouder meekijken (in de bus, trein of koffiebar) terwijl je jouw wachtwoord invoert.

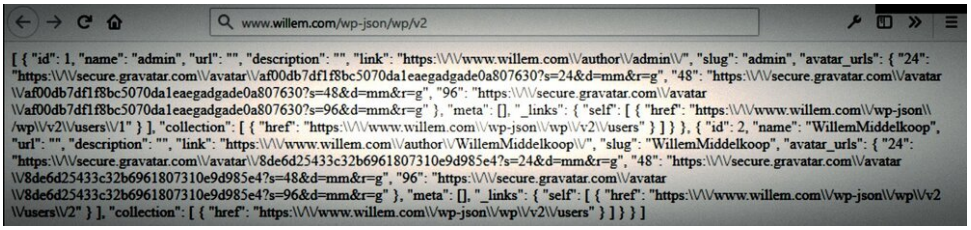
Wees voorzichtig waar en wanneer je aan jouw website werkt. Werk niet op een gedeelde of openbare computer als dat niet nodig is. Als je werkt via een openbare wifi-hotspot, moet je encryptie gebruiken om te voorkomen dat iemand meekijkt. Je kunt dit doen met TLS/SSL of door een VPN te gebruiken (zoals buffered.com). Zorg ervoor dat jouw computer, tablet of smartphone is bijgewerkt.

Vertrouw je de gratis wifi die je gebruikt? (Image via buffered.com)

6) Schakel de WordPress REST API uit

De WordPress REST API biedt toegang tot alle gegevens die beschikbaar zijn op jouw website in machineleesbaar JSON-formaat. Berichten, pagina's, categorieën, tags, reacties, media, gebruikers, instellingen en meer kunnen gemakkelijk worden geopend. Voeg bijvoorbeeld dit deel toe aan jouw websiteadres: **/wp-json/wp/v2/users** om een lijst te krijgen van alle geldige gebruikersnamen van jouw website. *Wil* je dat delen met hackers?

Schakel de REST-API uit om content scraping (plagiaat) en het lekken van gebruikersgegevens te voorkomen. Gebruikersgegevens zijn persoonlijk en mogen niet openbaar worden gedeeld als je privacy en beveiliging belangrijk vindt - denk aan de AVG. Je kunt de REST API uitschakelen met behulp van plugins zoals Disable REST API of REST API Toolbox. Bekijk de gedetailleerde blog post van Jeff Star voor meer informatie over het beveiligen van de WP REST API.



Lekken van persoonlijke gebruikersinformatie vanuit de WordPress REST API

7) Schakel XML-RPC-toegang uit

De XML-RPC is een functie van WordPress die bediening op afstand van jouw website mogelijk maakt met behulp van XML (RPC staat voor "remote procedure call"). Dit mechanisme stelt je in staat om jouw website te beheren zonder in te loggen op WP-Admin, bijvoorbeeld met behulp van externe services of apps. Helaas is de XML-RPC-functie een beveiligingsprobleem, omdat het in feite een achterdeur is die hackers kunnen proberen te kraken met brute force of speciale commando's.

Voorkom xml-rpc.php-problemen door deze WordPress-functie volledig uit te schakelen. Je kunt dit doen met de Disable XML-RPC plugin of door de webserver handmatig te configureren met behulp van een htaccess bestand.

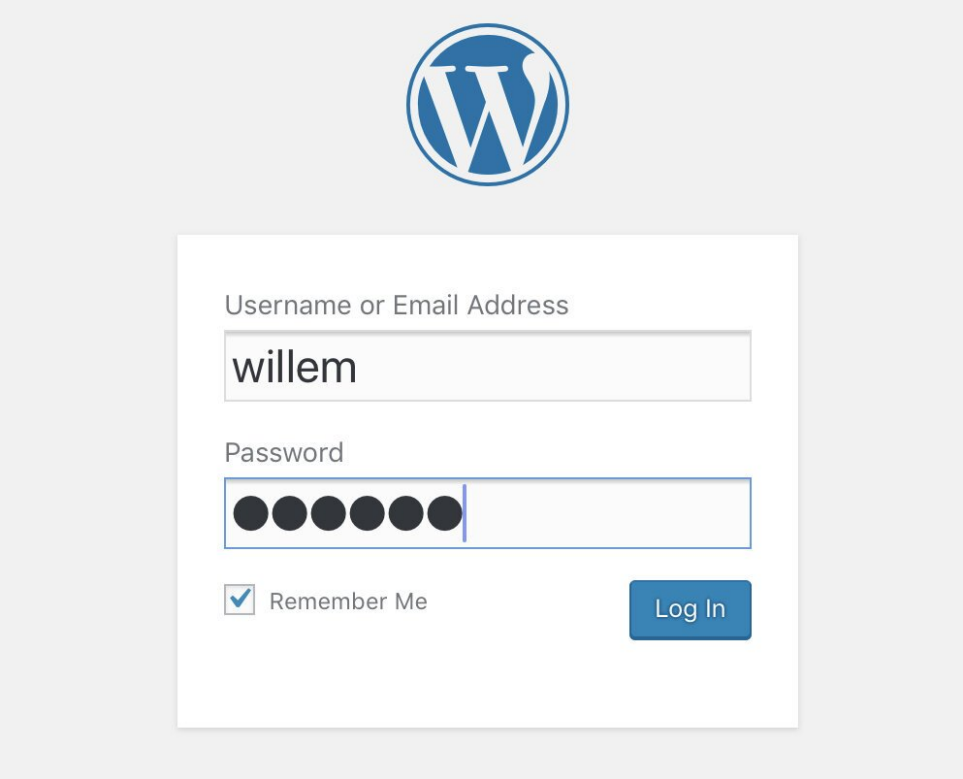
```
# Block WordPress xmlrpc.php requests
<Files xmlrpc.php>
order deny,allow
deny from all
allow from [IP]
</Files>
```

Beperk toegang op basis van IP-adres tot XML-RPC met behulp van een .htaccess bestand

8) Verberg of bescherm de inlogpagina (wp-admin)

Iedereen weet dat je om in te loggen op WordPress eenvoudig '/wp-admin' toevoegt aan jouw websiteadres. Elke hacker kan hierdoor gemakkelijk beginnen met het bruteforcen van jouw website. Het is veel moeilijker om een slot te kraken als je het niet kunt vinden.

Overweeg om de wp-admin-pagina te verbergen of te vervangen. Experts noemen dit "beveiliging door onduidelijkheid", waarbij men vertrouwt op geheimhouding voor beveiliging. Je kunt hiervoor een plugin gebruiken of de webserver configureren om de toegang tot wp-admin te beperken door middel van IP-adresfiltering. Bekijk deze blog post voor manieren om de wp-admin pagina te verbergen en te beschermen. Wees echter gewaarschuwd, alleen vertrouwen op geheimhouding is niet voldoende - je moet ook de andere tips implementeren.



Het is behoorlijk moeilijk om mijn WP-Admin pagina te hacken omdat je hem niet kunt vinden (hint: hij staat niet op /wp-admin)

9) Betrouwbare hosting

Zelfs als je al deze beveiligingstips implementeert om jouw WordPress-website te beveiligen, is het mogelijk niet voldoende als jouw hosting onveilig is. Hosting is de service waarmee jouw website beschikbaar wordt gesteld op internet. Dit gebeurt met behulp van speciale computers, servers genaamd. Net als de website zelf, moet ook de webserver die deze publiceert, beveiligd zijn. Denk aan een hosting als een schip, als het zinkt, neemt het alle passagiers (websites) mee...

Investeer in betrouwbare hosting door een hostingbedrijf met een goede reputatie te kiezen. Kies er een die goed bij jouw bedrijf past, overweeg hosting met een dedicated (managed) VPS. Houd er rekening mee dat goedkope hostingopties vaak goedkoop zijn

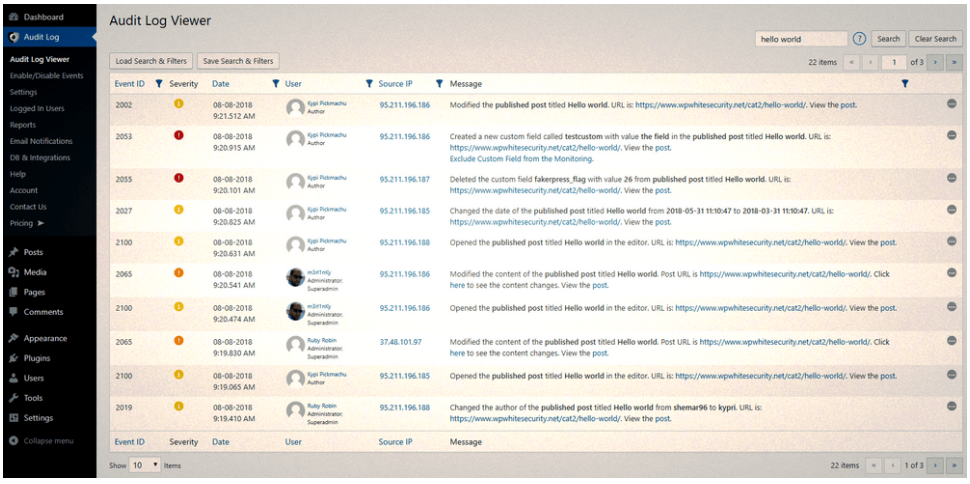
omdat de server wordt gedeeld met (veel) andere (mogelijk onveilige) websites. Lees verder om de beveiligingsproblemen bij gedeelde hosting te begrijpen.

Ergens in een datacenter staat een machine zoals deze die jouw website host

10) Backup en controle

Hoewel jouw website nu soepel draait, kunnen de dingen in de toekomst verslechteren. Beveiliging is nooit een absoluut gegeven, het is altijd mogelijk dat je slecht weer tegenkomt. Bereid je voor op problemen en laat beveiligingsproblemen niet onopgemerkt blijven.

Controleer jouw eigen website regelmatig - of huur iemand in om dit voor je te doen. Met een plugin zoals WP Security Audit Log kun je aanvallen en verdacht gedrag vroegtijdig opsporen. Maak back-ups van jouw website, zodat je klaar bent om te herstellen van een cyberramp. Ongelukken gebeuren bij de besten, maak een back-up van jouw website om te voorkomen dat je jouw werk volledig kwijtraakt. Bekijk deze blog post om meer te leren over verschillende manieren om een back-up van jouw WordPress website te maken.



Gebruik WP Security Audit Log om in de gaten te houden wat er gebeurt met je WordPress website (wpsecurityauditlog.com)

Conclusie

De beveiliging van jouw website is net als de beveiliging van jouw kantoor of huis. Als je weggaat, sluit je de ramen en doe je de deuren op slot, toch? Verwaarloos de beveiliging van jouw website niet, het is net zo belangrijk als het ontwerp en de inhoud.

Als je deze beveiligingstips implementeert, wordt jouw website veel moeilijker te hacken door cybercriminelen. Doe het zelf of vraag iemand om je te helpen.