

Handleiding Beveiligen van Wordpress

Deze handleiding beschrijft de stappen die u dient te nemen om uw Wordpress website te beveiligen

Versie 1.0



Kies een sterk wachtwoord

Gebruik als wachtwoord een combinatie van minimaal 8 letters, cijfers en speciale karakters door elkaar.

Tevens raden wij u aan nooit hetzelfde wachtwoord op meer dan één website of systeem te gebruiken.

Verander uw wachtwoord regelmatig, een standaard advies luid elke drie maanden het wachtwoord aanpassen.

Ons advies is hoe vaker hoe beter.

Wijzig de admin username

Zodra u WordPress heeft geïnstalleerd raden wij aan om het standaard account admin aan te passen.

Bij het aanmaken van WordPress wordt namelijk admin als standaard username gebruikt. Hackers weten dit en hebben met deze kennis al de helft van uw gegevens te pakken.

- Maak een nieuw account aan met beheerder als rol.
- Log nu onder de admin user uit. Log vervolgens in met het account welke u heeft aangemaakt.
- Nu kunt u het admin account verwijderen. Tijdens het verwijderen van de gebruiker kunt u aangeven om alle berichten naar uw nieuwe gebruiker over te zetten.

Registraties nieuwe accounts uitzetten

WordPress wordt standaard ingesteld met de optie waarin het bezoekers van uw website mogelijk word gemaakt een gast-account aan te maken.

Dit is een voordeel voor community-sites maar helaas word deze optie erg vaak gebruikt door de meest recente exploits waardoor wij aanraden deze optie uit te zetten.

U kunt deze optie uitschakelen door onderstaande stappen te volgen.

- Log in met uw beheerders account
- Klik op instellingen en zet het vinkje uit bij iedereen kan registreren naast lidmaatschap

Reactie mogelijkheden uitschakelen

WordPress wordt standaard ingesteld met de optie waarin het bezoekers van uw website mogelijk word gemaakt reacties achter te laten op uw berichten.

Indien u dit niet wenst kunt u dit uitzetten.

Wij raden dit ook aan aangezien hackers de mogelijkheid gebruiken om code te uploaden naar uw website en deze bijvoorbeeld gebruiken om spam te versturen.

Zet deze optie uit door onderstaande stappen te volgen.

- Log in met uw beheerders account.
- Klik op instellingen en klik op reacties en zet vervolgens de instellingen zoals hieronder weergegeven



Houd uw WordPress plugins en thema versies up-to-date

Misschien wel de meest voorkomende reden van een hack is een out-of-date versie van het CMS, één van de plugins of thema versies.

Houd daarom altijd uw WordPress versie up-to-date.

Helaas onderhoud WordPress geen beveiliging updates voor oudere versies.

Dit maakt het voor hackers erg gemakkelijk om via oude versies van WordPress alsnog in uw website te kunnen inbreken.

Bekijk minimaal één keer per maand uw WordPress administrator pagina of er nieuwe versies beschikbaar zijn voor WordPress en voor de plugins.

U kunt zien of WordPress geüpgrade kan worden door onderstaande stappen te volgen.

- Log in met uw beheerders account.
- Indien u bovenaan het begin scherm de volgende tekst ziet: WordPress "x.x.x". is available kunt u een upgrade installeren.
- Voor plugins zal achter de knop Plugins een nummer verschijnen met hoeveel plugins geüpgrade kunnen worden.

- Voor het upgraden van het thema zal er in het dashboard een bericht verschijnen met een upgrade mogelijkheid.

Beperk het gebruik van third party plugins

Beperk het gebruik van “third party plugins” (welke niet door WordPress zijn ontwikkeld) Controleer welke extra plugins er nodig zijn aangezien veel hackers via slecht geprogrammeerde plugins Wordpress binnen kunnen komen.

Installeer daarom alleen plugins welke u ook daadwerkelijk gebruikt en houd deze te allen tijde up-to-date.

Verwijder de plugins die u niet gebruikt.

Voorkom browsen door mappen

Er is een probleem met het laten zien binnen WordPress van geïnstalleerde plugins en de versies van deze plugins. Hier kunnen hackers door een “hack exploit” makkelijk misbruik van maken. Door een regel aan uw .htaccess bestand toe te voegen kunt u dit voorkomen.

De regel welke u toe dient te voegen is:

```
# BEGIN Prevents directory listing  
Options -Indexes
```

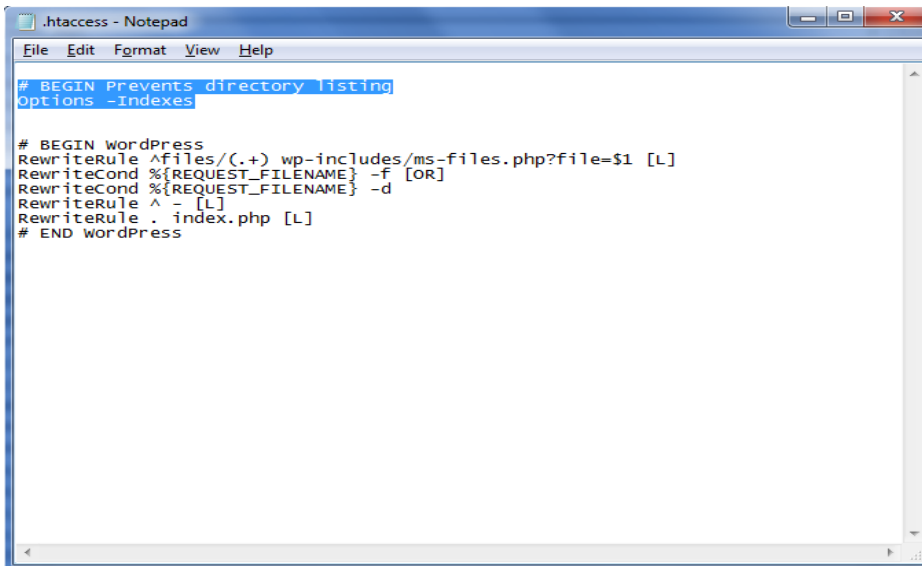
Om het .htaccess te bewerken gebruikt u een FTP client, bijvoorbeeld FileZilla.

Wanneer FileZilla geïnstalleerd is schakelt u de zichtbaarheid van de verborgen bestanden in. Dit kan worden aangezet onder Server > Tonen van verborgen bestanden forceren in de menu balk van FileZilla.

U logt nu in met uw FTP gegevens welke u van uw hosting provider heeft gekregen.

U kunt nu het .htaccess bestand bewerken door onderstaande stappen te volgen.

- U gaat naar de root van uw WordPress installatie. Klik met de rechtermuisknop op het .htaccess bestand en klik op bekijken/bewerken
- Voeg vervolgens de gemarkeerde regels tekst toe aan het bestand zoals hieronder aangegeven



```
# BEGIN Prevents directory listing
Options -Indexes

# BEGIN WordPress
RewriteRule ^files/(.+) wp-includes/ms-files.php?file=$1 [L]
RewriteCond %{REQUEST_FILENAME} -f [OR]
RewriteCond %{REQUEST_FILENAME} -d
RewriteRule ^ - [L]
RewriteRule . index.php [L]
# END WordPress
```

Gebruik de juiste bestand en map rechten

Indien WordPress correct is geïnstalleerd door uzelf hoeft u de onderstaande wijzigingen niet door te voeren, maar mocht dit door een derde partij zijn gedaan dan kunt u dit ter controle het beste nalopen.

Alle maprechten dienen op 755 ingesteld te worden en alle bestanden dienen op 644 ingesteld te worden.

Bestanden welke u wilt bewerken d.m.v. een WordPress editor moeten worden ingesteld op 666.

Gebruik nooit als rechten 777 omdat met deze rechten-instelling elke gebruiker aanpassingen kan verrichten op uw WordPress website.

FileZilla FTP Client

Het gebruik van een FTP client brengt ook een gevaar met zich mee.

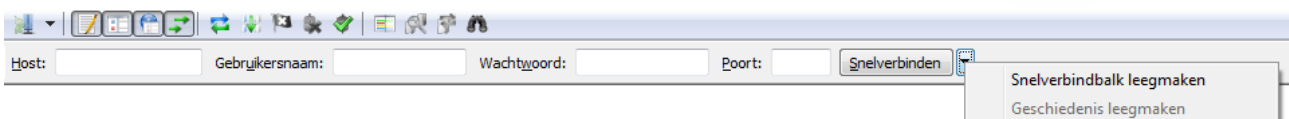
Er worden namelijk in de meeste gevallen binnen de FTP clients gebruikersnamen en wachtwoorden opgeslagen zodat u maar 1 keer hoeft in te loggen.

Er wordt niet gevraagd of u deze wilt opslaan, echter dit wordt automatisch gedaan.

Als een hacker uw computer heeft geïnfected met bijvoorbeeld een "Trojan" kan hij gemakkelijk via de FTP client uw FTP gebruikersnaam en wachtwoord achterhalen.

Om misbruik te voorkomen kunt u onderstaande stappen volgen, wij raden aan dit elke keer te doen nadat u ingelogd bent geweest.

- Log in met uw FTP gegevens en voer de gewenste werkzaamheden uit aan uw website.
- Nadat u klaar bent klikt u eerst op "Server" > "Verbinding verbreken".
- Klik daarna (zoals hieronder aangegeven) op het dropdown menu naast de knop "snelverbinden".



Houd de fora van WordPress in de gaten

Kijk regelmatig op de fora van Wordpress of er nieuws is.
Hier wordt melding gemaakt van beveiligings issues, nieuwe features etc.

<http://wordpress.org/support>

[http://codex.wordpress.org/Main Page](http://codex.wordpress.org/Main_Page)

