Handleiding beveiligen van Joomla

Deze handleiding beschrijft de stappen die je dient te nemen om je Joomla 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 je aan nooit hetzelfde wachtwoord op meer dan één website of systeem te gebruiken.
Verander je wachtwoord regelmatig, een standaard advies luidt: elke drie maanden het wachtwoord aanpassen.
Ons advies is hoe vaker hoe beter.

Wijzig de 'Administrator' username

Zodra je Joomla hebt geïnstalleerd raden wij aan om het superadmin account Administrator aan te passen.
Bij het aanmaken van Joomla wordt "Administrator" als standaard username gebruikt.
Hackers weten dit en hebben met deze kennis al de helft van je gegevens te pakken.

Houdt Joomla en desbetreffende plugins up-to-date

De meest voorkomende beveiligingslekken ontstaan door out-of-date Joomla installaties en out-of-date plugins.
Helaas onderhoudt Joomla geen beveiligings-updates voor oudere versies.
Dit maakt het voor hackers erg gemakkelijk om via oude versies van Joomla alsnog op je website te kunnen inbreken.
Bekijk minimaal één keer per maand de Joomla administrator pagina of er nieuwe versies beschikbaar zijn voor Joomla en voor de plugins.

Aanpassen van het standaard database voorvoegsel

Als de database geïnstalleerd wordt verander dan het voorvoegsel jos_ in iets willekeurigs.
Dit zal een hoop SQL injecties voorkomen, omdat hackers vaak proberen de administrator login te achterhalen uit de user tabel.

Aanpassen van het .htaccess bestand voor IP toegang

Voeg onderstaande regels toe in je .htaccess bestand zodat alleen jij toegang hebt tot het Joomla administrator gedeelte.
Pas het IP-adres aan naar je eigen lokale IP-adres.

```
order deny,allow
deny from all
allow from 192.168.2.1
```

Gebruik zoekmachine vriendelijke URL's

Hackers gebruiken vaak een zoekmachine (bijv. Google) om te zoeken naar zwakke plekken. Door de URL's te aan te passen naar "zoekmachine vriendelijke URL's" wordt dit tegengegaan. Tevens helpt het om Google de URL's beter te laten indexeren.

Beperk het gebruik van "third party plugins"

Beperk het gebruik van "third party plugins" (welke niet door Joomla zijn ontwikkeld)
Controleer welke extra plugins er nodig zijn aangezien veel hackers via slecht geprogrammeerde plugins Joomla binnen kunnen komen.
Installeer daarom alleen plugins die je ook daadwerkelijk gebruikt en houdt deze te allen tijde up-to-date.
Verwijder de plugins die je niet gebruikt.

Gebruik de juiste bestand en map rechten

Als Joomla correct is geïnstalleerd door jezelf hoef je de onderstaande wijzigingen niet door te voeren, maar mocht dit door een derde partij zijn gedaan dan kun je dit ter controle het beste nalopen.
Alle maprechten dienen op 755 ingesteld te worden en alle bestanden dienen op 644 ingesteld te worden.
Bestanden die je wilt bewerken d.m.v. een Joomla editor moeten worden ingesteld op 666.
Gebruik nooit als rechten 777 omdat met deze rechten-instelling elke gebruiker aanpassingen kan verrichten op jouw Joomla 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 je maar 1 keer hoeft in te loggen.
Er wordt niet gevraagd of je deze wilt opslaan, dit wordt automatisch gedaan.
Als een hacker je computer heeft geïnfecteerd met bijvoorbeeld een "Trojan" kan hij gemakkelijk via de FTP client je FTP gebruikersnaam en wachtwoord achterhalen.
Om misbruik te voorkomen kun je onderstaande stappen volgen, wij raden aan dit elke keer te doen nadat je ingelogd bent.

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

- Klik eerst op "Snelverbindbalk leegmaken" en daarna op "Geschiedenis leegmaken".

- Als je dit elke keer nadat je ingelogd bent doorvoert krijgen hackers niet de kans om je gegevens uit te lezen.

Houdt de fora van Joomla in de gaten

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

http://forum.joomla.org
http://docs.joomla.org