Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

Veiligheidsscan: websitenaam.nl

Datum 23 - 07 - 2021

noeste ijver

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

Inhoud

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

Legenda

✅ Ja (goed)

🟡 Nee (geen punt van zorgen, wel mogelijkheid tot verbetering)

🟠 Onvoldoende (moet verbeterd worden)

❌ Nee (punt van zorgen)

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

SSL

Is SSL geïnstalleerd?
✅

Uitleg:
Als een website een SSL-certificaat heeft, is er de mogelijkheid beschikbaar om een versleutelde verbinding op te zetten, waardoor het voor tussenliggende partijen nagenoeg onmogelijk is om communicatie te onderscheppen en lezen.

Is SSL op de front-end van WordPress geforceerd?
✅

Uitleg:
Als SSL op de front-end van WordPress is geforceerd, dan wordt de browser van de bezoeker gedwongen om alle verbindingen met versleuteling op te zetten. Als dit niet geforceerd wordt, is het afhankelijk van of de bezoeker de ‘http://’- of ‘https://’-versie van de website bezoekt.

Is SSL op de back-end van WordPress geforceerd?
✅

Uitleg:
Als SSL op de back-end van WordPress is geforceerd, dan wordt de browser van de bezoeker gedwongen om alle verbindingen met het beheer-gedeelte van WordPress met versleuteling op te zetten. Als dit niet geforceerd wordt, is het afhankelijk van of de bezoeker de ‘http://’- of ‘https://’-versie van de website bezoekt.

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

Is SSL op losse bestanden geforceerd?
🟡

Uitleg:
Wanneer SSL niet op losse bestanden wordt geforceerd, kunnen deze zowel met als zonder versleuteling bezocht worden. Afhankelijk van de inhoud van het bestand kan dit een veiligheidsrisico opleveren.

Toelichting:
Op websitenaam.nl is het mogelijk om losse bestanden -welke niet of niet direct door WordPress worden beheerd- zowel met als zonder versleutelde verbinding te bezoeken.

Geen mixed-content aanwezig?
✅

Uitleg:
Het kan voorkomen dat er in bijvoorbeeld artikelen verwezen wordt naar de niet-versleutelde locatie van een afbeelding. In dit geval geeft de browser een foutmelding en wordt de pagina als onveilig gemarkeerd.

Is de SSL-keten in orde?
✅

Uitleg:
Een SSL-keten bestaat normaliter uit drie certificaten: ‘root’, ‘intermediate’ en ‘end-user’. Als één of meerdere van deze certificaten niet in orde of verlopen zijn, kunnen er problemen ontstaan op gebied van functionaliteit en beveiliging van de website.

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

WordPress inlogformulier

Is het WordPress-inlogformulier verborgen?
🟡

Uitleg:
Als het inlogformulier verborgen is, dan wordt het niet getoond op de standaard-locaties die WordPress biedt, zoals in onderstaande lijst vermeld. Door het loginformulier te verbergen, wordt het voor hackers/bots lastiger om pogingen te doen om wachtwoorden te kraken.

- websitenaam.nl/wp-admin/
- websitenaam.nl/admin/
- websitenaam.nl/login/
- websitenaam.nl/wp-login.php

Toelichting:
Op websitenaam.nl is het inlogformulier op de reguliere plek te vinden. Mits er extra maatregelen zijn genomen is dit niet direct een punt van zorgen.

Is er extra beveiliging op het inlogformulier geplaatst?
🟡

Uitleg:
Standaard heeft WordPress geen adequate beveiliging op het loginformulier zitten. Kwaadwillenden kunnen oneindig veel pogingen doen om een wachtwoord te kraken en als website-eigenaar merk je daar niks van, totdat het ook werkelijk gebeurd is. Onderstaand een lijst van eventuele mogelijkheden.

- Een maximaal aantal pogingen instellen voordat een IP-adres (tijdelijk) wordt geblokkeerd;
- Alleen bepaalde IP-adressen toegang tot de back-end verlenen;
- Alleen IP-adressen uit bepaalde landen toegang tot de back-end verlenen;
- Tweestapsverificatie toevoegen;
- reCaptcha toevoegen.

Opmerkingen:
Op websitenaam.nl is middels de plugin ‘IP geo block’ ingesteld dat IP-adressen na 5 mislukte inlogpogingen definitief worden geblokkeerd. Dit is een goed uitgangspunt, al is de maatregel om IP-adressen direct definitief te blokkeren weinig subtiel. Aan de andere kant zijn er ook nog aanvullende mogelijkheden beschikbaar.

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

Is er geen account met de gebruikersnaam ‘admin’ aanwezig?
✅

Uitleg:
Standaard krijgt de eerste WordPress-gebruiker de gebruikersnaam ‘admin’. Als dit het geval is, dan zijn kwaadwillenden al op de helft als ze toegang willen verkrijgen tot het beheer-gedeelte. Het is daarom aangeraden om geen gebruiker met de gebruikersnaam ‘admin’ te hebben.

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

Beveiliging navigatie FTP-mappen

Is navigatie voor FTP-mappen uitgeschakeld?
✅

Uitleg:
Als het mogelijk is om de mappen op de server in te zien, is het voor kwaadwillenden eenvoudiger om vast te stellen welke versie van WordPress, plugins en thema's gebruikt worden. Vervolgens zal bekeken worden of er bekende kwetsbaarheden voor de aanwezige zaken zijn, welke uitgebuit kunnen worden.

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

Server

Is de gebruikte PHP-versie nog ondersteund?
❌

Uitleg:
Het wordt momenteel aangeraden om minimaal PHP 7.4 te gebruiken, kwetsbaarheden in oudere versies van PHP worden niet meer opgelost en daarmee ontstaan dus veiligheidsrisico's. Het upgraden van de PHP-versie kan doorgaans via een beheer-paneel van de hostingpartij en levert niet alleen voordelen qua beveiliging op, maar ook qua snelheid van de site.

Toelichting:
websitenaam.nl draait momenteel op PHP-versie 7.0.33.

Is communicatie met wordpress.org mogelijk?
✅

Uitleg:
Indien er geen communicatie met wordpress.org mogelijk is, kan er niet gecontroleerd worden of er nieuwe beveiligingsupdates voor WordPress zijn.

Werken achtergrond-updates?
✅

Uitleg:
Met achtergrond-updates worden 'minor' releases van WordPress automatisch geïnstalleerd. Deze releases zijn bedoeld om bugs en kwetsbaarheden op te lossen.

Werkt de autorisatie-header zoals verwacht?
✅

Uitleg:
De autorisatie-header wordt gebruikt om applicaties van derden goed te keuren. Zonder deze header kunnen diensten van derden geen verbinding met je site opzetten.

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

Security Headers

Is de x-frame-options header toegepast?

🟡

Uitleg:
Middels de x-frame-options header kan worden bepaald of een pagina van de website in een ‘iframe’-element kan worden geplaatst. Op deze manier kan een website proberen om de identiteit van een andere website te repliceren ten behoeve van ‘clickjacking’ of om gebruikersinvoer te onderscheppen.

Toelichting:
Op websitenaam.nl is de x-frame-options header niet gespecificeerd.

Is de x-xss-protection header toegepast?

🟡

Uitleg:
Middels de x-xss-protection header zullen pagina’s niet ingeladen worden als de browser bemerkt dat er sprake is van een cross-site scripting (XSS)-aanval. Deze header is tegenwoordig vooral voor oudere browsers nog relevant.

Toelichting:
Op websitenaam.nl is de x-xss-protection header niet gespecificeerd.

Is de x-content-type-options header toegepast?

🟡

Uitleg:
De header x-content-type-options is bedoeld om bij uploads te verifiëren of bestands-extensie van een bestand overeenkomt met de inhoud van het bestand, zonder het al werkelijk te openen of uit te voeren. Zo wordt bijvoorbeeld voorkomen dat een gebruiker een uitvoerbaar bestand (code-instructies) vermomd als video kan uploaden.

Toelichting:
Op websitenaam.nl is de x-content-type-options header niet actief.

Is de Strict Transport header toegepast?

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

❌

Uitleg:
Met de Strict Transport header wordt een browser geïnstrueerd om een website direct met een versleutelde verbinding op te zetten. Dit is zeer belangrijk voor websites die gevoelige informatie overdragen, zoals webwinkels.

Toelichting:
Op websitenaam.nl is de Strict Transport header niet actief.

Is de Referrer Policy header toegepast?

🟡

Uitleg:
De Referrer-Policy HTTP header is bedoeld om browsers te instrueren welke informatie ze mogen meesturen wanneer de gebruiker doorklikt naar een externe website. Als alle informatie wordt meegestuurd, kunnen website-eigenaars via diensten als Google Analytics vaststellen via welke pagina van een website een bezoeker is doorgeklikt naar hun eigen site.

Toelichting:
Op websitenaam.nl is de Referred Policy header niet actief.

Is de Feature-Policy header toegepast?

🟡

Uitleg:
De Feature-Policy header is een mechanisme om te bepalen welke browser-functies gebruikt mogen worden wanneer een site via een iframe op een andere site wordt getoond. Zo kan bijvoorbeeld toegang tot de camera of schermopname worden beperkt of juist toegestaan.

Toelichting:
Op websitenaam.nl is de Feature-Policy header niet actief.

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

WordPress-installatie

Is WordPress geheel up-to-date?
🟡

Uitleg:
Wij raden aan om WordPress altijd geheel up-to-date te hebben, maar dit levert voornamelijk op functioneel vlak voordelen op.

Toelichting;
Op websitenaam.nl draait momenteel WordPress 5.7.2, de nieuwste versie is WordPress 5.8.

Is de nieuwste beveiligingsupdate van WordPress geïnstalleerd?
✅

Uitleg:
WordPress brengt met grote regelmaat kleine updates uit, waarmee bugs en kwetsbaarheden worden opgelost. Deze updates worden normaliter automatisch geïnstalleerd.

Toelichting;
Op websitenaam.nl draait momenteel WordPress 5.7.2, van de 5.7.x-tak is dit de nieuwste versie.

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

Malware

Zijn alle WordPress-bestanden gelijk aan het origineel?
✅

Uitleg:
Als niet alle bestanden van de WordPress-installatie gelijk zijn aan de bestanden die WordPress heeft uitgegeven, kan dit erop wijzen dat er (waarschijnlijk via een kwetsbaarheid) geknoeid is met de WordPress-installatie.

Zijn alle plugin-bestanden gelijk aan het origineel?
✅

Uitleg:
Als niet alle bestanden van plugins gelijk zijn aan de bestanden die door hun ontwikkelaar zijn uitgegeven, kan dit erop wijzen dat er (waarschijnlijk via een kwetsbaarheid) mee geknoeid is, of dat de plugin zichzelf vermomt als een plugin van een vertrouwde ontwikkelaar.

Zijn er geen plugins met bekende kwetsbaarheden?
✅

Uitleg:
Als plugins niet voldoende up-to-date worden gehouden, kan het zijn dat er ontdekte kwetsbaarheden onopgelost blijven. Net als WordPress zelf, brengen ook ontwikkelaars regelmatig kleine updates met oplossingen voor bugs en kwetsbaarheden uit. Deze worden in de regel echter niet automatisch geïnstalleerd.

Zijn er geen plugins met verdachte code?
✅

Uitleg:
Het is mogelijk om niet-geverifieerde plugins in WordPress te installeren. Deze plugins worden niet gemonitord door WordPress en/of de community. We checken de aanwezige plugins tot op zekere hoogte op verdachte code.

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

Zijn er geen WordPress-vreemde bestanden in de installatie aanwezig?
🟡

Uitleg:
De WordPress-installatie bestaat uit een aantal mappen en bestanden. Het is het best om de installatie zo schoon mogelijk te houden, maar er kunnen redenen zijn waarom er andere bestanden aan de installatie worden toegevoegd.

Toelichting:
Op websitenaam.nl zijn een aantal WordPress-vreemde bestanden te vinden. Het gaat hier om de map ‘header1’ in de hoofdmap van de installatie. Op het eerste oog gaat het hier om eigen en niet-kwetsbare bestanden.

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

Diverse

Is xml-rpc uitgeschakeld?

❌

Uitleg:
xml-rpc is een systeem om blog-berichten te plaatsen via andere tools zoals Windows Live Writer. Tegenwoordig wordt dit systeem echter veel misbruikt door hackers, om WordPress ongewenste handelingen uit te laten voeren.

Toelichting:
Op websitenaam.nl is xml-rpc niet uitgeschakeld.

Zijn trackbacks en pingbacks uitgeschakeld?

❌

Uitleg:
Met trackbacks en pingbacks worden eigenaars van WordPress-websites er (middels een reactie onder een eigen blog) van op de hoogte gesteld als een link naar diens site op een andere WordPress-site wordt geplaatst. In de basis is dit een leuke functionaliteit, maar dit systeem is makkelijk te misbruiken om in enkele seconden een succesvolle DDoS-aanval op een website uit te voeren.

Toelichting:
Op websitenaam.nl zijn trackbacks en pingbacks niet uitgeschakeld.

Worden namen van gebruikersaccounts afgeschermd?

✅

Uitleg:
Als een kwaadwillende weet wat de gebruikersnaam van een account met admin-rechten is, dan beschikt diegene al over 50% van de benodigde gegevens om binnen te geraken. Standaard stuurt WordPress bezoek aan bijvoorbeeld websitenaam.nl/?author=1 door naar websitenaam.nl/author/loginnaam en zo weet een kwaadwillende dat de gebruikersnaam ‘loginnaam’ is.

Toelichting:
Op websitenaam.nl is het achterhalen van gebuikersnamen afgeschermd.

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

Is bestandsbewerking uitgeschakeld?
❌

Uitleg:
WordPress biedt standaard de mogelijkheid om bestanden van thema's en plugins te bewerken vanuit het beheer-gedeelte. Als een kwaadwillende toegang heeft tot het beheergedeelte, is dit een goede manier om een site in functioneel opzicht om zeep te helpen of om malafide code toe te voegen.

Toelichting:
Op websitenaam.nl is het bewerken van bestanden niet uitgeschakeld.

Wordt PHP-uitvoering voorkomen?
❌

Uitleg:
In het geval van een kwetsbaarheid is het in theorie mogelijk om een PHP-bestand te uploaden in de mappen van de WordPress-installatie. Als dit bestand vervolgens ook 'uitgevoerd' kan worden door het te bezoeken, kan dit allerlei gevolgen hebben. Het is echter mogelijk om te voorkomen dat PHP-bestanden uitgevoerd kunnen worden door ze te bezoeken.

Toelichting:
Op websitenaam.nl is het bewerken van bestanden niet uitgeschakeld.

Is het tonen van foutmeldingen uitgeschakeld?
✅

Uitleg:
Tijdens het bouwen van websites schakelen ontwikkelaars vaak de functionaliteit om foutmeldingen te tonen in. Als bij het 'live' plaatsen van de website wordt vergeten om deze functionaliteit uit te schakelen, kan dit voor kwaadwillenden een goed aanknopingspunt zijn om kwetsbaarheden in de code te vinden.

Toelichting:
Op websitenaam.nl is het tonen van foutmeldingen uitgeschakeld.

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

Zijn de SALT-keys minder dan één jaar oud?
✅

Uitleg:
SALT-keys zijn cryptografische elementen die worden gebruikt om gegevens te ‘hashen’ en op die manier te beveiligen. Zo wordt ‘gebruikersnaam’ bijvoorbeeld in de database opgeslagen als ‘8a5ccbe4900f4b9efaecbd6b72284131a8a782ff96f751c8781439cf0d61ed84’.

Dit systeem wordt door vrijwel alle platformen gebruikt om gevoelige gegevens zoals wachtwoorden te beschermen. Het is raadzaam om de SALT-keys minimaal jaarlijks te verversen

Toelichting:
Op websitenaam.nl zijn de SALT-keys minder dan een jaar oud.

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

Is de website niet aanwezig op de Google-blacklist?
✅

Uitleg:
Als een website op de Google-blacklist staat, betekent het dat Google deze site als ‘malafide’ heeft gemarkeerd. Dit kan om allerlei redenen gebeuren, bijvoorbeeld vanwege malware en phishing. Als een website op de blacklist staat, zullen browsers weigeren de site te bezoeken en een paginagrote melding tonen, totdat je expliciet aangeeft de pagina te willen bekijken.

Ringbaan Oost 116F / 5013CD Tilburg
mail@noesteijver.nl / www.noesteijver.nl
KvK 66330696 / BTW 856497757
IBAN NL28 KNAB 0255 3775 09 / BIC KNABNL2H

Overige opmerkingen

Geen 301-redirect in het .htaccess-bestand
Op websitenaam.nl wordt middels de plugin 'Really Simple SSL' voor WordPress verkeer via een versleutelde verbinding geforceerd. Dit is echter niet waterdicht. Het is beter om een versleutelde verbinding via het .htaccess-bestand af te dwingen. Het scheelt ook een plugin.

Module 'imagick' niet op de server geïnstalleerd
Het valt op dat de imagick-module niet is geïnstalleerd. Dit kan een keuze vanuit de hostingpartij zijn, maar voor verscheidene WordPress-functionaliteiten en -plugins kan het problematisch zijn. Imagick wordt door WordPress zelf bijvoorbeeld gebruikt om thumbnails van PDF-bestanden te genereren. Of dit echter mogelijk is, moet nagevraagd worden bij de hostingpartij.

max_execution_time bedraagt slechts 30 seconden
De server-variabele max_execution_time van websitenaam.nl is vanuit de hostingpartij ingesteld op 30 seconden. Dit is voor veel handelingen voldoende, maar bijvoorbeeld een malware-scan kan veel langer duren dan 30 seconden. Wij raden daarom aan om max_execution_time minstens op 150 in te stellen. Deze waarde is in te stellen via het wp-config.php bestand.

WP_MEMORY_LIMIT bedraagt slechts 40MB
Standaard beperkt WordPress zichzelf tot het gebruik van 40MB werkgeheugen van de server. Het hostingpakket van websitenaam.nl heeft echter 256MB tot de beschikking, wat aanzienlijk meer is. Dit kan net als de max_execution_time problemen opleveren bij langdurige processen. We raden aan om het werkgeheugen minimaal te verhogen tot 128MB, aangezien het toch beschikbaar is. Deze waarde is in te stellen via het wp-config.php bestand.