

DOCUMENT 3 VAN 4 • VERSIE 1.0 • 22 OKTOBER 2026

Zo lees je je uitslag

SocialNow · Wat elke uitslag betekent en wat je zelf kunt doen

Bovenaan de checkpagina staat de uitslag voor het PHP-lek php2shell. Daaronder volgen vijf punten over je website als geheel. Dit document legt in gewone taal uit wat je ziet en wat je er zelf mee kunt doen.

UITGEVER	SocialNow, Amstelstraat 43G, 1017 DA Amsterdam, KvK 77146301
VERSIE	1.0, 22 oktober 2026
GELDT VOOR	De gratis websitecheck op socialnow.nl/check
CONTACT	secure@socialnow.nl

DEEL A

De PHP-uitslag

PHP is de programmeertaal waarop veel websites draaien, waaronder WordPress. Op 21 oktober 2026 werd een ernstig lek in PHP bekend, php2shell. De check leest welke PHP-versie je server openbaar laat zien en vergelijkt die met de versies waarin het lek is gedicht.

GROEN Fix gezien

WAT HET BETEKENT

De PHP-versie die je server laat zien, bevat de fix. Dat betekent niet dat je website veilig is: een eerdere inbraak, andere PHP-versies op dezelfde server en of alle PHP-processen opnieuw zijn gestart, zijn van buitenaf niet te zien.

WAT JE ZELF KUNT DOEN

Vraag je host te bevestigen dat PHP na de update opnieuw is gestart. Check ook je andere websites en subdomeinen.

ORANJE Twijfel

WAT HET BETEKENT

We zien PHP, maar van buitenaf is niet zeker of de fix erin zit. Veel hosts dichten het lek zonder het versienummer te veranderen. Voor PHP 8.1 en ouder is er geen officiële fix meer; alleen je host kan die versie hebben bijgewerkt.

WAT JE ZELF KUNT DOEN

Vraag je host schriftelijk of PHP is bijgewerkt voor CVE-2026-109618 en CVE-2026-109619. Draai je PHP 8.1 of ouder, vraag dan naar een upgrade naar 8.3 of nieuwer. Of plan de uitgebreide check.

ROOD Niet gepatcht

WAT HET BETEKENT	Je server laat een versie zien waarvan vaststaat dat de fix ontbreekt. Deze uitslag geven wij alleen als het bewijs in de versie zelf staat.
WAT JE ZELF KUNT DOEN	Laat PHP vandaag bijwerken en opnieuw starten, door je host of je webbouwer. Laat daarna controleren of er sinds 17 oktober iets ongewoons is gebeurd. Wij helpen kosteloos.

GRIJS Je site schermt dit af

WAT HET BETEKENT	De PHP-versie was niet te lezen. Je server verbergt haar, een firewall houdt de check tegen of de site gaf geen antwoord. Dit is geen goed en geen slecht teken.
WAT JE ZELF KUNT DOEN	Plan de uitgebreide check. Na eigendomsbewijs lezen wij de exacte versie uit.

DEEL B

De vijf punten

Elk punt krijgt een kleur. **Groen:** in orde. **Oranje:** verdient aandacht. **Rood:** actie nodig. **Grijs:** niet te meten, bijvoorbeeld omdat de site niet antwoordde. Bij elk punt toont de check wat hij letterlijk zag.

1 Snelheid op mobiel

WAT WE METEN	Hoe snel je homepage laadt op een telefoon, gemeten door Google PageSpeed Insights.
WAAROM HET TELT	Trage pagina's kosten bezoekers en vindbaarheid.
WAT JE ZELF KUNT DOEN	Verklein grote afbeeldingen, verwijder plugins die je niet gebruikt en vraag je host of caching aanstaat.

2 Beveiligde verbinding

WAT WE METEN	Of je site via https werkt, http doorstuurt, het certificaat geldig is en niet bijna verloopt, en of de verbinding modern is beveiligd.
WAAROM HET TELT	Zonder goede https kan wat bezoekers invullen onderweg worden meegelezen, en tonen browsers een waarschuwing.
WAT JE ZELF KUNT DOEN	Zet bij je host een gratis certificaat aan, vaak Let's Encrypt, en laat al het verkeer naar https doorsturen.

3 Verouderde software

WAT WE METEN	Software die je pagina zelf noemt, zoals je CMS, plugins of bibliotheken, vergeleken met openbare lijsten van bekende lekken.
WAAROM HET TELT	Verouderde onderdelen zijn de meest gebruikte ingang bij inbraken.
WAT JE ZELF KUNT DOEN	Installeer de beschikbare updates en verwijder onderdelen die je niet meer gebruikt. De check ziet alleen wat zichtbaar is; er kan meer zijn.

4 Beveiligingsheaders

WAT WE METEN	Instructies die je server aan browsers meegeeft, bijvoorbeeld dat je site niet in een vreemde pagina mag worden ingesloten, en of je server versienummers prijsgeeft.
WAAROM HET TELT	Deze instructies maken veelvoorkomende aanvallen op je bezoekers moeilijker.
WAT JE ZELF KUNT DOEN	Vraag je host of webbouwer de ontbrekende headers aan te zetten. Meestal zijn dat een paar regels configuratie.

5 E-mailbeveiliging

WAT WE METEN	Of je domein vastlegt wie namens jou mag mailen (SPF) en wat ontvangers met valse mail moeten doen (DMARC).
WAAROM HET TELT	Zonder deze instellingen kunnen anderen makkelijker mail versturen die van jou lijkt te komen.
WAT JE ZELF KUNT DOEN	Laat bij je domeinbeheerder een SPF-record en een DMARC-record aanmaken, bij voorkeur met het beleid quarantine of reject.

DEEL C

Wat een uitslag niet is

- C.1 Een uitslag is een momentopname van wat van buitenaf zichtbaar is, voor dit ene domein. Andere subdomeinen of servers kunnen anders zijn.
- C.2 Groen betekent dat de versie die je server laat zien de fix bevat. Het is geen verklaring dat je website veilig is, geen garantie en geen certificering.
- C.3 Twijfel je over wat je ziet, mail dan secure@socialnow.nl of plan de uitgebreide check. De check en de updates zijn kosteloos.