

DOCUMENT 3 OF 4 • VERSION 1.0 • 22 OCTOBER 2026

Understanding Your Result

SocialNow · What each result means and what you can do yourself

At the top of the check page you see the result for the PHP vulnerability php2shell. Below it are five points about your website as a whole. This document explains in plain language what you see and what you can do about it.

ISSUED BY	SocialNow, Amstelstraat 43G, 1017 DA Amsterdam, the Netherlands, Chamber of Commerce 77146301
VERSION	1.0, 22 October 2026
APPLIES TO	The free website check at socialnow.nl/check
CONTACT	secure@socialnow.nl

PART A

The PHP result

PHP is the programming language many websites run on, including WordPress. On 21 October 2026 a serious vulnerability in PHP became known, php2shell. The check reads which PHP version your server shows publicly and compares it with the versions in which the vulnerability has been fixed.

GREEN Fix seen

WHAT IT MEANS

The PHP version your server shows contains the fix. This does not mean your website is secure: an earlier intrusion, other PHP versions on the same server and whether all PHP processes have been restarted cannot be seen from the outside.

WHAT YOU CAN DO

Ask your host to confirm that PHP was restarted after the update. Also check your other websites and subdomains.

ORANGE Uncertain

WHAT IT MEANS

We see PHP, but from the outside it is not certain whether the fix is included. Many hosts fix the vulnerability without changing the version number. PHP 8.1 and older no longer receive an official fix; only your host can have updated that version.

WHAT YOU CAN DO

Ask your host in writing whether PHP has been updated for CVE-2026-109618 and CVE-2026-109619. If you run PHP 8.1 or older, ask about an upgrade to 8.3 or later. Or book the extended check.

RED Not patched

WHAT IT MEANS	Your server shows a version that is known to lack the fix. We give this result only when the evidence is in the version itself.
WHAT YOU CAN DO	Have PHP updated and restarted today, by your host or your web developer. Then have it checked whether anything unusual has happened since 17 October. We help free of charge.

GREY Your site shields this

WHAT IT MEANS	The PHP version could not be read. Your server hides it, a firewall blocks the check or the site did not respond. This is neither a good nor a bad sign.
WHAT YOU CAN DO	Book the extended check. After proof of ownership we read the exact version.

PART B

The five points

Each point gets a colour. **Green**: in order. **Orange**: needs attention. **Red**: action required. **Grey**: could not be measured, for example because the site did not respond. For each point the check shows exactly what it saw.

1 Mobile speed

WHAT WE MEASURE	How fast your homepage loads on a phone, measured by Google PageSpeed Insights.
WHY IT MATTERS	Slow pages cost visitors and search visibility.
WHAT YOU CAN DO	Reduce large images, remove plugins you do not use and ask your host whether caching is enabled.

2 Secure connection

WHAT WE MEASURE	Whether your site works over https, redirects http, has a valid certificate that is not about to expire, and uses modern encryption.
WHY IT MATTERS	Without proper https, what visitors enter can be read in transit, and browsers show a warning.
WHAT YOU CAN DO	Enable a free certificate with your host, often Let's Encrypt, and redirect all traffic to https.

3 Outdated software

WHAT WE MEASURE	Software your page mentions itself, such as your CMS, plugins or libraries, compared with public lists of known vulnerabilities.
WHY IT MATTERS	Outdated components are the most common way in for intrusions.
WHAT YOU CAN DO	Install the available updates and remove components you no longer use. The check only sees what is visible; there may be more.

4 Security headers

WHAT WE MEASURE	Instructions your server gives to browsers, for example that your site may not be embedded in another page, and whether your server reveals version numbers.
WHY IT MATTERS	These instructions make common attacks on your visitors harder.
WHAT YOU CAN DO	Ask your host or web developer to enable the missing headers. This usually takes a few lines of configuration.

5 E-mail security

WHAT WE MEASURE	Whether your domain specifies who may send e-mail on your behalf (SPF) and what recipients should do with forged e-mail (DMARC).
WHY IT MATTERS	Without these settings others can more easily send e-mail that appears to come from you.
WHAT YOU CAN DO	Ask your domain administrator to create an SPF record and a DMARC record, preferably with the policy quarantine or reject.

PART C

What a result is not

- C.1 A result is a snapshot of what is visible from the outside, for this one domain. Other subdomains or servers may differ.
- C.2 Green means that the version your server shows contains the fix. It is not a statement that your website is secure, not a guarantee and not a certification.
- C.3 If you are unsure about what you see, e-mail secure@socialnow.nl or book the extended check. The check and the updates are free of charge.