

PHPCheck

EXAMPLE REPORT - Sample data; no real website was checked.

Your website. A clearer next step.

sample.example.org | 2026-10-23

Your results at a glance

This check found 1 PHP update warning, 2 recommended improvements. 7 checks found no issue in the responses reviewed; 1 could not be assessed or did not apply. 2 information-only observations are listed separately.

The PHP version shown by your website is listed as needing a PHP2Shell fix. Your host can confirm whether the fix is already installed.

Your next steps

1. Your PHP version may need an update

Website host | high priority

Ask your website host to confirm the fixes for both PHP2Shell issues in the PHP version running your website. If an update is needed, have the host back up the site, check compatibility, and confirm the update is running everywhere.

2. Keep visitors on a secure connection

Server team | low priority

Ask your host to review this setting after confirming secure connections work across your website. Changes that also affect other parts of your website need extra care.

3. Help browsers handle files safely

Server team | low priority

Ask your host or developer to check that files are labelled correctly and review adding this protection.

Your PHP version

PHP/8.4.26 | x-powered-by | HTTP 200

<https://sample.example.org/>

Listed as needing a PHP2Shell fix

PHP lists fixes in 8.2.35, 8.3.36, 8.4.27 and 8.5.12. Your host can confirm the installed package and any separately supplied fixes.

A message for your website host

Please review the website check for sample.example.org, dated 2026-10-23T16:00:11.349Z.

The PHP version shown by your website is listed as needing a PHP2Shell fix. Your host can confirm whether the fix is already installed.

PHP versions shown by the website:

8.4.26 in x-powered-by at <https://sample.example.org/>

Please confirm fixes for CVE-2026-109618 and CVE-2026-109619 in the PHP version running this website, including any

fixes supplied separately by the host.

Steps to review:

- Your PHP version may need an update: Ask your website host to confirm the fixes for both PHP2Shell issues in the PHP version running your website. If an update is needed, have the host back up the site, check compatibility, and confirm the update is running everywhere.
- Keep visitors on a secure connection: Ask your host to review this setting after confirming secure connections work across your website. Changes that also affect other parts of your website need extra care.
- Help browsers handle files safely: Ask your host or developer to check that files are labelled correctly and review adding this protection.

This check used a small set of public website responses. No attacks were attempted. Please confirm the updates and the results of your own checks.

Technical details

Website requested: <https://sample.example.org/>

Rules: phpcheck-2026-10-22.1 | Advisory review: 2026-10-22

Requests: 2 | Response body bytes: 57 | Elapsed: 0 ms (sample values)

PHP-001 - Your PHP version may need an update

Review suggested | potential exposure | medium confidence

x-powered-by: PHP/8.4.26

Source: <https://sample.example.org/>

Confirm CVE-2026-109618 and CVE-2026-109619 fixes, package provenance, vendor backports and all web-serving PHP workers.

The PHP version shown by your website is listed as needing a PHP2Shell fix. Your host can confirm whether the fix is already installed.

Check the fix: Ask your host to confirm both PHP2Shell fixes, including any fixes supplied separately by the host, in the PHP version running your website.

NET-001 - Secure connection

No issue seen in this check | observed issue | high confidence

Certificate chain and hostname validated.

Source: <https://sample.example.org/>

HTTPS helps keep information private as it travels between a visitor and your website.

NET-002 - Send visitors to the secure website

No issue seen in this check | observed issue | high confidence

HTTP response status 301.

Source: <https://sample.example.org/>

Visitors using an HTTP address should be sent to the secure HTTPS version.

TLS-001 - Security certificate expiry

No issue seen in this check | observed issue | high confidence

Observed leaf certificate expires 2027-10-22T00:00:00.000Z.

Source: <https://sample.example.org/>

A renewed security certificate helps your secure connection keep working. This check does not cover every certificate or encryption setting.

HDR-001 - Keep visitors on a secure connection

Review suggested | configuration recommendation | high confidence

No effective HSTS header observed.

Source: <https://sample.example.org/>

Review Strict-Transport-Security only after validating HTTPS coverage. Do not enable includeSubDomains or preload without checking every affected host.

This setting tells a visitor's browser to keep using a secure connection after a trusted visit. Adding it can improve protection; a missing setting does not show that an attack happened.

Check the fix: Ask the team making the change to check the website response and confirm the setting is working.

HDR-002 - Control which scripts can run

No issue seen in this check | configuration recommendation | high confidence

An enforcing policy contains a bounded restrictive script-source signal.

Source: <https://sample.example.org/>

This setting can limit which scripts a page runs. We check a few rules, so your developer still needs to review and test the full policy.

HDR-003 - Control where your page can appear

No issue seen in this check | configuration recommendation | high confidence

Applicable CSP frame-ancestors protection observed.

Source: <https://sample.example.org/>

This setting helps stop other websites from displaying your page inside their own page. Some websites allow this on purpose. We check the two common ways to control it together.

HDR-004 - Help browsers handle files safely

Review suggested | configuration recommendation | high confidence

No nosniff response header observed.

Source: <https://sample.example.org/>

Review correct MIME types and X-Content-Type-Options: nosniff.

This setting helps browsers treat files as the type your website says they are. Adding it is a recommended security improvement.

Check the fix: Ask the team making the change to check the website response and confirm the setting is working.

COOKIE-001 - Login cookie protection

Does not apply | observation | high confidence

No Set-Cookie header observed.

Source: <https://sample.example.org/>

We did not find a cookie we could clearly identify as a login cookie. This does not tell us whether all cookies are protected.

HTML-001 - Secure page resources

No issue seen in this check | observed issue | high confidence

0 explicit HTTP resource reference(s); CSP upgrade-insecure-requests not observed.

Source: <https://sample.example.org/>

We looked for files and images using an HTTP address in the page code. Browsers may block them or switch them to HTTPS. We do not run the page or check every link created by scripts or styles.

HTML-002 - Secure form submissions

No issue seen in this check | observed issue | high confidence

0 explicit HTTP form destination(s) on the HTTPS page.

Source: <https://sample.example.org/>

A form that sends information to an HTTP address may expose what a visitor enters. We only read the form's address; we never submit it.

INFO-001 - Software information shared by your website

Review suggested | observation | high confidence

PHP software banners were publicly advertised.

Source: <https://sample.example.org/>

A website may show which software it uses. This can help with maintenance, but does not prove there is a security issue. This information alone does not create a report to buy.

About this check

We checked a small set of pages and responses. A service in front of your website may hide or change what the server shows.

We use information the website shares. Your host can confirm installed fixes. This check cannot tell whether the website has been hacked.

We do not log in, run page scripts, crawl every page, try attacks, inspect malware or check every Content Security Policy setting.

Cookie values and downloaded page code are discarded. If the PHP updates cannot be confirmed, no paid report is offered.

A version shown by a website does not prove which fixes are installed. We did not try an attack. A command-line PHP version can differ from the PHP version running the website.

Sources

<https://www.php.net/archive/2026.php#2026-10-21-5>

<https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w>

<https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp>

Keep your report

Online access and email recovery are available for 90 days from payment. Save this PDF for your records. To recover a purchased PDF, enter your checkout email on the Recover my report page.

Need help? Open your online report to see whether a consultation can be booked. Calls are separate from the report.