Find the owner. Confirm the fix.

Your website is part of your livelihood. Use this checklist to get a documented answer about PHP2Shell from the people responsible for your hosting and website.

1. Know who owns the work

- ☐ Website address: _____
- ☐ Hosting provider: _____
- ☐ Hosting security owner: _____
- ☐ Website / extension maintainer: _____

2. Send the message on page 2

- ☐ Use your provider's established support channel.
- ☐ Include subdomains, test sites, old installations and separately hosted tools.
- ☐ Save the response and support-ticket reference.

3. Look for a specific answer

- ☐ The provider identifies the systems covered and any exclusions.
- ☐ The response names the fixed package or relevant official protection notice.
- ☐ The fixed software is running and required restarts are complete.
- ☐ Any remaining work has a named owner and completion time.
- ☐ Temporary firewall protection is identified as temporary.

Keep asking if the answer is vague. "We updated WordPress," "you have a security plugin," and "the site looks fine" do not establish that the underlying PHP issue is fixed. A version number alone may miss a documented vendor backport.

Copy. Paste. Get confirmation.

Send this message to your hosting provider and website team.

Subject: Please confirm our website's PHP2Shell protection

> **"Have you addressed both PHP2Shell vulnerabilities on the systems running my website? What fix is in place, when was it applied, and what action remains?"**

Please cover CVE-2026-109618 and CVE-2026-109619, and answer these questions in plain language:

1. Does any part of our setup use affected PHP? If we're unaffected, what is that conclusion based on?

2. What fixed PHP package or documented vendor security update is installed? Please provide package details or your official protection notice.

3. When was it applied? Are required restarts complete, and is the protected software actually serving our website?

4. Does this cover our main site, subdomains, staging / test sites, old installations and separate tools? What is excluded?

5. Have you reviewed PHP's October 23 follow-up advisory? Does our setup need additional action?

6. Is any protection temporary? What remains to be patched, who owns it, and when will it be completed?

7. Have you found signs of compromise? What checks were performed, and what investigation remains?

8. Who will test our forms, bookings, checkout and confirmation emails after the work?

Please identify any action we need to take and who will confirm completion. Thank you.

Verify. Record. Follow through.

4. Test what customers need

- ☐ Submit a contact form and confirm delivery to the right inbox.
- ☐ Test bookings and checkout using an appropriate test procedure.
- ☐ Confirm customer notifications and internal alerts arrive.
- ☐ Record tester / date: _____

These checks verify business functions. They do not prove that a site has never been compromised. Suspicious accounts, redirects or changes need qualified investigation; patching and recovery are separate jobs.

5. Record the status supported by the evidence

- ☐ Confirmed protected against these two flaws for the listed systems.
- ☐ Confirmed unaffected, with a documented explanation.
- ☐ Temporary measures only - permanent work remains.
- ☐ Unconfirmed - waiting for a specific answer.
- ☐ Possible compromise - qualified investigation needed.

Confirmed by / date: _____
Ticket / evidence reference: _____
Remaining action / owner / completion: _____

A quick platform distinction

WordPress, Drupal and Joomla: contact the host and maintainer. Application updates alone do not establish that PHP is patched.
WordPress.com: consult its specific protection notice; it does not apply to all WordPress hosts.
Shopify: hosting is included for standard stores. Check separately hosted blogs, apps and integrations individually.

Need a straight answer? Contact Falls+Partners.

We're declaring war on PHP2Shell on behalf of small businesses. Bring your website address, your host's response and this checklist. Tell us: "I need a straight answer about my website."

fallspartners.com/contact/ | jason@fallspartners.com
Do not send passwords or access codes with your inquiry.

Scope: PHP2Shell verification, not a guarantee of overall website security. Review current provider guidance. Sources: PHP advisories; WordPress.com notice; Shopify hosting.