mySites.guru

Six more J2Store flaws fixed in 3.3.23, 4.0.23 and 4.1.8

J2Store 3.3.23, 4.0.23 and 4.1.8 fix six flaws mySites.guru reported, including an anonymous blind SQL injection that reads a Joomla shop's whole database.

Phil E. Taylor | 15 September 2026

J2Store is one of the most widely installed e-commerce extensions for Joomla, turning ordinary Joomla articles into shop products. In August 2026 J2Commerce fixed five vulnerabilities we reported, across all three supported branches, and published them as CVEs crediting mySites.guru. This post is the second round. Reviewing that fix release turned up six more issues, all reported privately to J2Commerce, all assigned CVE identifiers by the Joomla CNA, and all fixed this morning in **J2Store 3.3.23, 4.0.23 and 4.1.8**.

The one that matters most needs no login at all: a **blind SQL injection in the public product list that reads the shop's entire database**. Every supported branch is affected, so whichever version of Joomla your shop runs, it needs updating today. If you manage more than a handful of shops, read on for how to find every affected one at once.

TL;DR

- mySites.guru found six more security issues in J2Store and reported them privately to J2Commerce. All six are fixed in **3.3.23 (Joomla 3), 4.0.23 (Joomla 4) and 4.1.8 (Joomla 5 and 6)**
- **Unauthenticated blind SQL injection, scored 8.7 High.** The storefront product list reads a filter value from the request without quoting it and concatenates it into a database query. No login, no CSRF token: an anonymous visitor reads the whole database one character at a time, the Super User password hash included
- **Arbitrary file read through the download handler**, also 8.7 High, returning files from outside the shop's folders including `configuration.php`
- An anonymous request that can **mark any order as Failed**, 8.7 High, plus **incomplete CSRF protection** across the checkout and profile controllers at 7.1 High, a **forgeable order access token** at 5.1 Medium, and **unescaped request data in the PayPal notify redirect** at 4.5 Medium

- **Check your checkout overrides before updating.** The fix adds an anti-CSRF token to the cart, checkout and profile forms, so custom overrides and add-ons that ship their own copies of those templates need the same token or they return an Invalid Token error
- J2Commerce reports no evidence that any of the six were exploited on a live store
- mySites.guru already flags every connected Joomla shop still running a vulnerable version

> **We fix first and publish second**
>
> mySites.guru discovered these issues and reported them to J2Commerce before publishing any detail. We are holding back the exact requests and the proof-of-concept payloads until enough sites have updated. This is how we handle every vulnerability we find.

Which version you need

Every supported branch is affected, and each has its own fix. The branch you are on follows from your Joomla version rather than from anything you chose:

Your Joomla version	Update J2Store to	Affected builds
Joomla 3	**3.3.23**	3.3.22 and earlier
Joomla 4	**4.0.23**	4.0.22 and earlier
Joomla 5 or Joomla 6	**4.1.8**	4.1.7 and earlier

One thing to check before you update a live shop. The CSRF fix adds an anti-CSRF token to the cart, checkout and my-profile forms, which means any custom template override, or any third-party add-on shipping its own copies of those templates, needs the same token adding to its own forms. J2Commerce names Easy Checkout specifically. Until those are updated to match, the affected actions produce an Invalid

Token error for real shoppers, so a shop with heavily customised checkout templates wants a staging run rather than a Tuesday-afternoon click on Update.

A note from J2Commerce for mySites.guru users

J2Commerce sent this through ahead of the release, and asked us to pass it on.
“Thanks to the responsible disclosure by Phil Taylor of mySites.guru, we’ve fixed six security vulnerabilities in J2Store, ranging from Medium to High severity. We have no evidence any of these were exploited on a live store. Even so, we recommend updating right away rather than waiting for your next maintenance window: Joomla 3 to J2Store 3.3.23, Joomla 4 to J2Store 4.0.23, Joomla 5 and Joomla 6 to J2Store 4.1.8.
Backup your site, then update through Joomla’s Components, Update screen, or download first from your account at J2Commerce.com. Full technical details are in the security advisory. Comprehensive update information is provided on install and in the J2Store dashboard. Contact us at support@j2commerce.com or j2commerce.com/support to request help.
Thank you to mySites.guru for the ongoing responsible disclosure that helps keep J2Store stores secure.”

The worst one: an anonymous visitor reads your whole database

Start with the one that needs no account, because it is the one an attacker can reach on any J2Store shop today. The storefront product list and the product-tags list both accept a `product_types` array filter, which the framework populates straight from the request into model state. Both models then built the `product_type IN (...)` fragment by wrapping each supplied value in literal quotes and joining them together, with no escaping and no check that the values were valid product-type keys at all. A value containing a single quote closes the string early, and an anonymous request controls part of the SQL.

We proved it against a running shop. The injection is blind, so nothing is echoed back on the page, but the query can be made to pause for a chosen number of seconds when a guess is right and stay instant when it is wrong. Used as a timing oracle, that

reads the database out one character at a time: every user record, every session, and the Super User's stored password hash. No login, no token, nothing but a crafted request to a public page.

8.7
CVSS 4.0

HIGH

J2Commerce security advisory, 15 September 2026 · CVE-2026-81567

An anonymous visitor reads the entire database through a blind time-based injection in the public product and product-tags lists: every user record, every session, and the Super User password hash. No account and no CSRF token are needed. Reachable on any public storefront that exposes the standard product listing filter.

`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N`

No login needed | Blind SQL injection | Full database read | Password hashes exposed

The download handler that reads any file

The second serious one is an arbitrary file read. `getFilePath()` built the on-disk path to a purchased digital download by concatenating the configured attachment folder with the product file's stored save name, normalising the separators but never resolving or rejecting a `../` segment, and never confirming the result stayed inside the attachment folder. A path that climbs out of the web root is served like any ordinary download. We retrieved the site's `configuration.php`, which holds the database password and the site secret, and `/etc/passwd`, to a request holding only an order token.

Reaching it is a chain rather than a single anonymous request, because the traversing path has to be stored first, most plausibly through the admin product-file save actions

that the CSRF gap below leaves forgeable. It compounds badly, though, because J2Store's order access tokens were predictable, which is the next finding.

8.7
CVSS 4.0

HIGH

J2Commerce security advisory, 15 September 2026 · CVE-2026-81568

The download handler serves files from outside the attachment folder when fed a stored traversing path, returning configuration.php with the database credentials and the site secret. Token-gated rather than fully anonymous, and chainable with the admin CSRF gap to plant the path without ever compromising an admin account.

`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N`

Arbitrary file read | Leaks site secret | CSRF-to-read chain

The other four

Reported and fixed in the same release:

Finding	Who can reach it	What it does
Incomplete CSRF protection on checkout and profile controllers	Any page a logged-in shopper visits	Checkout flow actions and `saveAddress()` ran without verifying the request came from the site, so a crafted page could overwrite a billing or shipping address before order confirmation, with nothing shown to the

Finding	Who can reach it	What it does
		shopper. That sub-case is the consequential one, because it redirects a paid order's goods.
Any order can be marked Failed by anyone	None	A failed PayPal signature check was passed down as an ordinary error rather than stopping processing, and any error made the handler set the named order to Failed regardless of its real status. An anonymous POST with a guessed order id flips a pending, confirmed or shipped order straight to Failed.
Predictable, forgeable order access token	Needs the site secret	The token guarding order lookup and digital downloads was derived from the site secret and the order id rather than generated randomly, and never rotated, so anyone who learns that secret can mint the access token for every order

Finding	Who can reach it	What it does
		on the shop. This is why the file read above matters twice over.
Unescaped request data in the PayPal notify redirect	Victim must follow a crafted link	The notify handler concatenated every value from `$_REQUEST` into the query string of its follow-on redirect with no encoding, so a separator in a submitted value injected extra parameters into the next request. The least serious of the six.

All six findings at a glance. The scores are J2Commerce's own CVSS 4.0 figures from the advisory, published alongside the release:

Finding	CVE	Login needed	Severity
Unauthenticated blind SQL injection in the storefront product list	CVE-2026-81567	None	8.7 High
Arbitrary file read via the download handler	CVE-2026-81568	Download token	8.7 High
Any order can be marked Failed by anyone	CVE-2026-	None	8.7 High

Finding	CVE	Login needed	Severity
	82189		
Incomplete CSRF protection on checkout and profile controllers	CVE-2026-78081	None, per action	7.1 High
Predictable, forgeable order access token	CVE-2026-82190	Needs the site secret	5.1 Medium
Unescaped request data reflected into the PayPal notify redirect	CVE-2026-82191	None	4.5 Medium

All six CVE records were still reserved at cve.org when this went out, so the vendor's advisory is the source for the scores above, and J2Commerce marks three of them as draft figures. If a published record later disagrees, the record is the authority and we will correct this post.

Why round two exists at all

Round two happened because we retested the August fix release rather than closing the ticket, and it is worth saying why that mattered. Two of these six, the anonymous SQL injection and the file read, were not in the original report and had nothing to do with the CSRF work J2Commerce was fixing. They surfaced only because we went back through the code that shipped alongside the round-one fix.

The vendor's first fix build had to be rejected, too. It closed the cart CSRF gaps correctly but left both of those criticals open, and it shipped with its version number unchanged, so no Joomla site would ever have been offered it and no scanner would have told the difference between patched and unpatched. The corrected build fixed the version string and closed the rest. A fix release deserves the same scrutiny as the code it fixes, which is the reusable lesson here for anyone shipping security patches.

Joomla 3, and the deadline J2Commerce has already set

Most of the shops these six flaws affect sit on the branch with the least time left. Six in ten of the affected installs we can see are on Joomla 3, which reached its own end of life on 17 August 2023 and has had no free security fixes from the Joomla project since. Paid Extended Long Term Support is the only supported route after that date, and very few of these shops are on it.

On 3 September 2026 J2Commerce set a date for the shop extension too. J2Store 3 stops receiving security patches on 19 October 2026, two years to the day after the company took J2Store over. From that date the 3.x line gets no security fixes, no support and no further releases of any kind, including for anything found afterwards. J2Store 4 has its own date a year later, on 19 October 2027.

A Joomla 3 shop on J2Store 3 therefore has two deadlines stacked on top of each other, one that passed three years ago and one about five weeks out, and 3.3.23 is among the last builds that will ever answer either. That is the real context for the six issues above. Today's release closes the anonymous database read. It does nothing about the arrangement that produced it, which is a shop extension sitting on a platform the project itself stopped patching for free in 2023.

The measured state of those shops is worse than the deadline alone suggests. Seven in ten of the Joomla 3 installs caught by this release are below 3.3.21, which puts them behind all three of this year's advisories rather than just this one. For a shop in that position 19 October is close to a formality, because nothing has been applied for months anyway.

Patch now, but plan to migrate

The right move for a shop still on J2Store 3 is patch now, migrate soon. Update to 3.3.23 to close what is open, then use the time it buys to plan the move to J2Store 4, or on to J2Commerce 6, rather than treating the patch as somewhere to stay. We cover that route, and why the shop migration and the Joomla migration are one project rather than two, in J2Store 3 stops getting security fixes on 19 October 2026.

Shops on 4.0.x and 4.1.x have no such deadline. They still need the update today, and 4.1.8 is the branch that continues into Joomla 6.

Was any of this being exploited?

J2Commerce states it has no evidence that any of these six were exploited on a live store, and neither do we. No proof of concept has been published for any of them. This post describes mechanisms rather than requests, and we are holding the exact payloads back until enough sites have updated.

The honest caveat is which one to check for. The anonymous SQL injection is the one worth going back through a busy shop's logs for, because it is reachable without a login and a timing-based extraction leaves a recognisable run of near-identical requests to the product list. The file read and the order-status change leave much less behind. If you ran an affected build, the highest-value review is recent order-state changes with no matching payment, the same advice as round one, plus any unusual burst of product-list requests.

How mySites.guru helps

You do not have to open each shop by hand. mySites.guru records the exact version of every extension on every Joomla site it monitors, so J2Store installs across your whole account list appear on one screen with their versions, and any shop below the fix version for its branch is flagged automatically. Instead of logging into each site to check whether it is updated yet, you get one filtered list of the ones that are not, and can act on them together.

That matters more here than usual, because the fix version is not one number. A shop on Joomla 3 needs 3.3.23, a shop on Joomla 5 needs 4.1.8, and 4.1.8 sorts above 3.3.23 while 3.3.23 is the newer release on its own branch. Checking that by eye across a list of client sites is exactly the sort of thing people get wrong at four in the afternoon. If you want to see it against your own sites first, the free audit covers it.

Field	Detail
Component	J2Store for Joomla (`com_j2store`)
Vendor	J2Commerce (j2commerce.com)
Type	Unauthenticated SQL injection (CWE-89); path traversal file read (CWE-22, CWE-73); business logic error (CWE-840, CWE-345); missing CSRF protection (CWE-352); insufficiently random values (CWE-330); improper output encoding (CWE-116)
CVE	CVE-2026-78081, CVE-2026-81567, CVE-2026-81568, CVE-2026-82189, CVE-2026-82190, CVE-2026-82191
CVSS 4.0	4.5 to 8.7, per the J2Commerce advisory. Records reserved at cve.org at time of writing
Impact	Anonymous full database read; arbitrary file read leaking the site secret; anonymous order-status change; missing CSRF across checkout and profile; forgeable order token; reflected parameter injection in the PayPal redirect
Finder	Phil Taylor, mySites.guru
Affected versions	3.3.22 and earlier, 4.0.22 and earlier, 4.1.7 and earlier
Fixed in	J2Store 3.3.23 (Joomla 3), 4.0.23 (Joomla 4), 4.1.8 (Joomla 5 and 6)
Reported	1 September 2026 (privately to J2Commerce)
Acknowledged	5 September 2026 (J2Commerce confirmed the findings)
Fixed	15 September 2026

Timeline

2026-08-25

Round one: five issues reported to J2Commerce

The PayPal callback forgery, the reflected XSS, the anonymous cart tampering, the guest-address disclosure and the Apps delegation

chain, all fixed on 31 August in 3.3.22, 4.0.22 and 4.1.7 and published as five CVEs crediting mySites.guru.

2026-09-01

Round two opened after retesting the fix release

Reviewing 3.3.22 turned up more: incomplete CSRF protection across the cart and checkout controllers, and shipping-price tampering. Reported to J2Commerce the same day, and confirmed by the vendor on 5 September.

2026-09-07

First fix build rejected on retest

The vendor's first attempt closed the cart CSRF gaps but left two unreported criticals open, an anonymous storefront SQL injection and an arbitrary file read, and shipped with the version number unchanged so no site would have been offered it. We retested it and sent it back.

2026-09-11

Six CVE identifiers assigned by the Joomla CNA

After the second report, the Joomla CNA assigned six identifiers covering the CSRF gaps, the storefront SQL injection, the file read, the order-status change, the order token and the PayPal redirect. A corrected build followed the same night and passed retest on 12 September.

2026-09-15

3.3.23, 4.0.23 and 4.1.8 released

J2Commerce shipped all three branches together with a full advisory naming every CVE, its CVSS vector and the affected files, and crediting mySites.guru for the discovery and disclosure of all six.

Further Reading

- J2Store 3.3.22, 4.0.22 and 4.1.7 fix five flaws we reported - round one, the five issues fixed in the August release these six sit on top of.
- J2Commerce security advisory for 3.3.23, 4.0.23 and 4.1.8 - the vendor's own write-up, with the CVSS vectors, the affected files and the per-issue mitigations.

- J2Store 3 stops getting security fixes on 19 October 2026 - why 3.3.23 is close to the last security build that branch will ever get, and what that means for the shops still on it.
- A month of Joomla security disclosures - the wider set of extension flaws we reported, of which the J2Store rounds are one thread.
- Why AJAX endpoints are a CMS security blind spot - the recurring pattern behind several of these: a request reaching a query or a file path while the framework's CSRF check does not apply, with nothing on the page to say so.
- CWE-89: SQL Injection, CWE-352: Cross-Site Request Forgery and CWE-22: Path Traversal - the standard references for the three worst issues here.

Frequently Asked Questions

What did mySites.guru find in J2Store?

Six issues, on top of the five fixed in the August release. The worst is a blind SQL injection in the storefront product list that needs no login at all and reads the whole database, password hashes included. Alongside it: incomplete CSRF protection across the checkout and profile controllers, an arbitrary file read through the download handler, an anonymous request that can mark any order Failed, a forgeable order access token, and unescaped request data reflected into the PayPal notify redirect. All six are fixed in J2Store 3.3.23, 4.0.23 and 4.1.8.

Which J2Store versions are affected?

All six affect every supported branch, which J2Commerce confirmed in its advisory. If you run Joomla 3 you need J2Store 3.3.23, on Joomla 4 you need 4.0.23, and on Joomla 5 or Joomla 6 you need 4.1.8. Anything below those on its own branch is affected, so 3.3.22 and earlier, 4.0.22 and earlier, and 4.1.7 and earlier all need updating.

Is the SQL injection exploitable without a login?

Yes. The storefront product list and product-tags list both read a filter value straight from the request without quoting it and concatenate it into a database query, reachable anonymously with no account and no CSRF token. It is blind, so nothing is echoed back, but the query can be made to pause on a correct guess, which is enough to read the database one character at a time. J2Commerce scores it 8.7 High, and it is the reason to update every shop now.

Will updating break my checkout?

It can, and J2Commerce flagged this in the advisory. The fix adds an anti-CSRF token to the cart, checkout and profile forms, so any custom template override or third-party add-on that ships its own copies of those templates needs the same token adding to its forms. Easy Checkout is named specifically. Until those are updated, the affected actions return an Invalid Token error. Check your overrides before you update a live shop, not after.

Should I patch J2Store 3 or migrate off it?

Migrate. J2Commerce has set 19 October 2026 as the end of life date for the J2Store 3 branch, so 3.3.23 is one of the last security builds it will ever receive. Applying 3.3.23 closes these six issues today, but the branch stops getting fixes within weeks, so treat the

update as buying time to plan the move to J2Store 4 or J2Commerce 6 rather than as a destination.

Was any of this being exploited?

J2Commerce says it has no evidence any of the six were exploited on a live store, and neither do we. We are holding back the exact requests and payloads until enough sites have updated. The anonymous SQL injection is the one worth checking a busy shop's logs for, since it is reachable without a login and leaves query patterns behind; the file read and the order-status change leave much less trace.

How do I find every J2Store install across the sites I manage?

By hand you would log into each Joomla site and read its extension list, which is slow enough that it gets skipped. mySites.guru keeps an extension inventory for every connected site, so searching for J2Store returns every install with its version on one screen, and any shop below the fix version for its branch is flagged automatically.

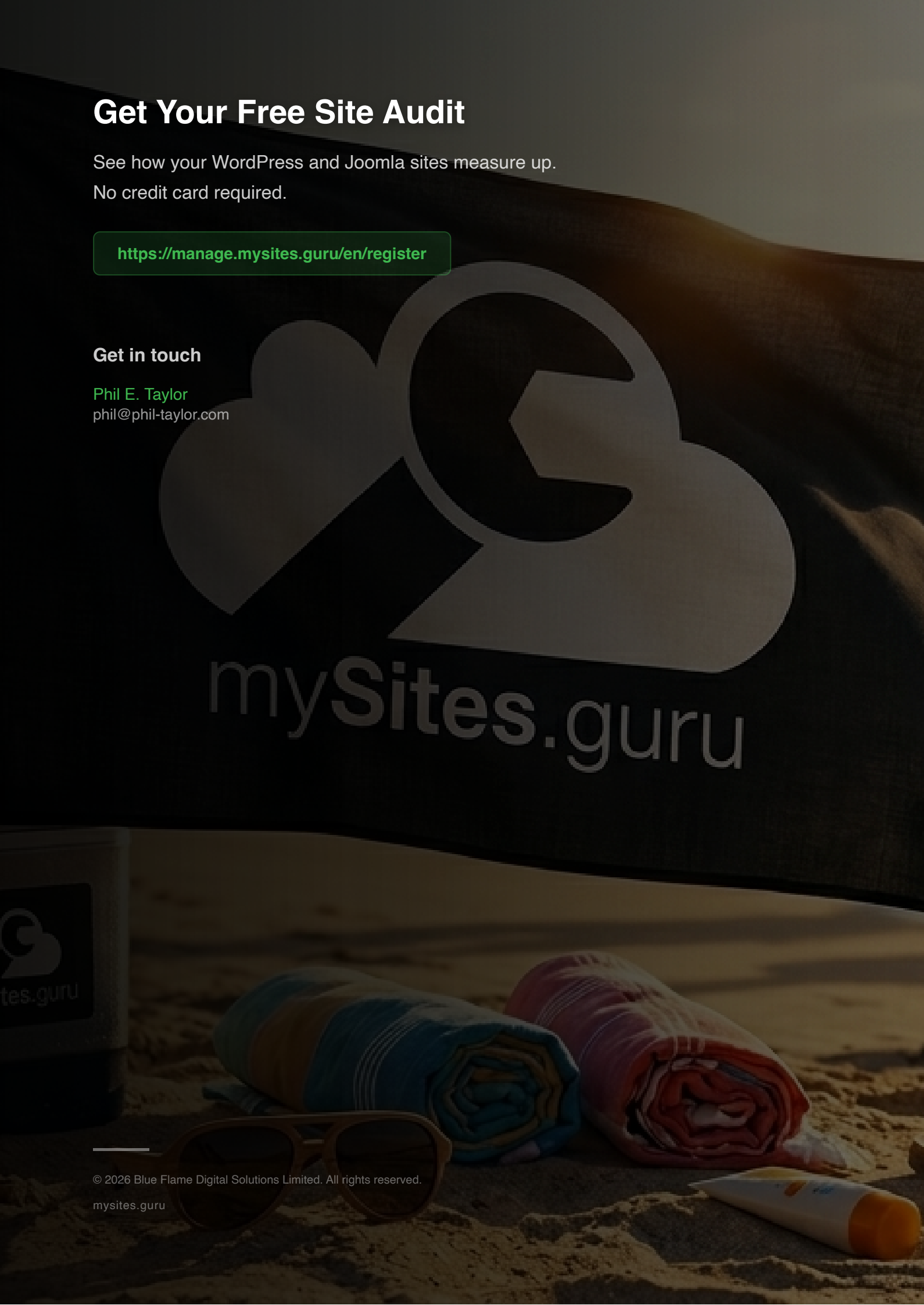
Written and edited by a human, with AI assistance. Our approach to AI

Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.

No credit card required.

https://manage.mysites.guru/en/register



Get in touch

Phil E. Taylor
phil@phil-taylor.com