mySites.guru

One VEL for Every Joomla and WordPress Site

The Joomla VEL (Vulnerable Extension List) only covers Joomla and never checks your sites. mySites.guru tracks both CMSes and flags yours directly.

Phil E. Taylor | 25 August 2026

If you run Joomla sites, you might have heard of the Joomla VEL (Vulnerable Extension List). It is the community-run (well, gated, not-open, keys held by “mandville” who seems to appear and disappear as fast as buses around Brighton) list of third-party Joomla extensions with known, reported vulnerabilities. If you also run WordPress sites, you know it stops at the Joomla border. For that half of your sites you absolutely must be subscribed to Wordfence or Patchstack for alerts on WordPress plugin security announcements, an entirely separate set of feeds with no connection to the first.

Keeping on top of security announcements and a handful of vulnerable extension lists, across two different CMS platforms, is a near full-time job on its own. And even when you keep up, both lists share a bigger limitation than the effort of watching them, and it is the one that actually costs people. Neither of them knows which sites you run. They tell you that a piece of software is vulnerable somewhere in the world. They cannot tell you that *your* client’s site, the one on the old version of that exact component, is sitting there exposed right now.

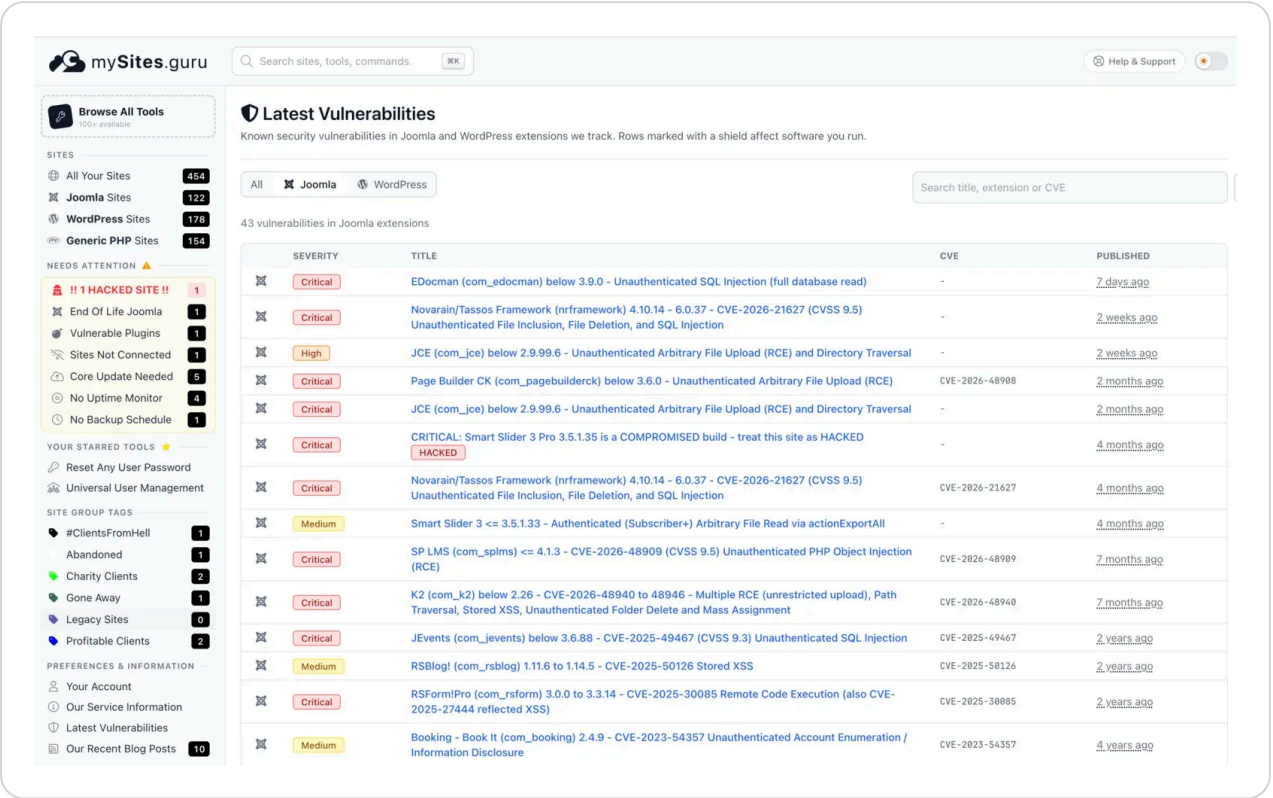
We have built the thing that closes that gap. There is a new **Latest Vulnerabilities** page inside mySites.guru: one Vulnerable Extension List for Joomla and WordPress together, wired directly into the sites you already manage.

To be clear, the tracking itself has been running for over a decade. mySites.guru has recorded extension vulnerabilities and vendor security announcements internally that whole time, and used them to flag the sites affected. What is new is the front end: we have exposed all of it so subscribers can browse it, filter it and click into it themselves. Previously this information sat buried in the Extensions pages inside mySites.guru. Now it has its own tool.

One Vulnerable Extension List for Joomla and WordPress

The Latest Vulnerabilities page is a single, searchable list of the extension vulnerabilities we track across both platforms. Filter it to Joomla, filter it to WordPress, or leave it on All and watch the two streams merge, newest first. Each row has a

severity, the affected extension, a CVE where one has been assigned, and the date it was published.



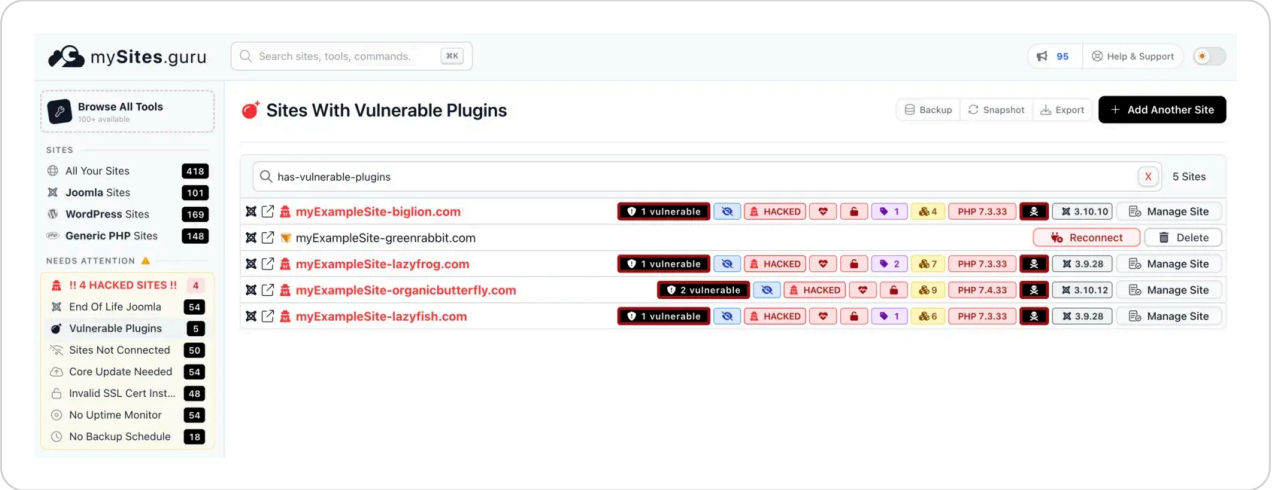
On the WordPress side, that is tens of thousands of plugin and theme records drawn from the wider vulnerability feeds.[1] On the Joomla side, it is the extension vulnerabilities we track, including feeds from the National Vulnerability Database (NVD) that auto-alert us when a CVE is announced for a Joomla extension. A large share of them are ones we found and disclosed ourselves through the Joomla CNA: Gridbox, Balbooa Forms, Events Booking, SP Page Builder, EDocman and more. Every rule has the affected version range, so a match is version-aware, not just a name that happens to look familiar.

The severity rating is the first thing the VEL does not give you. A Joomla extension entry here is Critical, High, Medium or Low, so you can filter straight to the things that will ruin your week and leave the low-risk noise for later.

Which of your sites does this vulnerability affect?

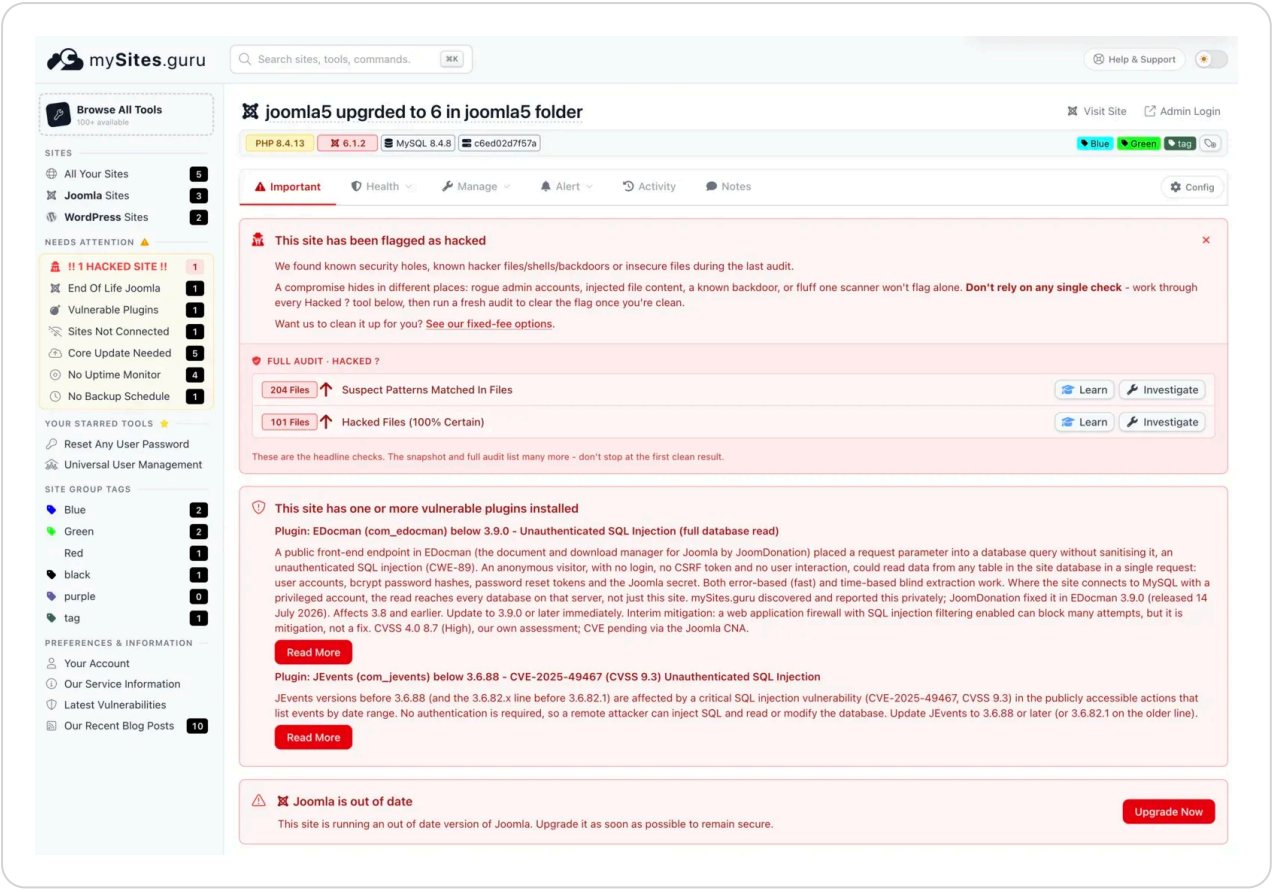
This is the part that changes the job. A vulnerability list is a lookup table until it is connected to your actual sites. mySites.guru already keeps a live inventory of every extension and every version installed on every connected Joomla and WordPress site. The Latest Vulnerabilities page cross-references that inventory against the whole list, automatically.

So a row is not just “this software is vulnerable.” A row marked with a shield is “you are running this.” Open any entry and the **Check your sites** button drops you straight into the filtered list of your own affected sites.



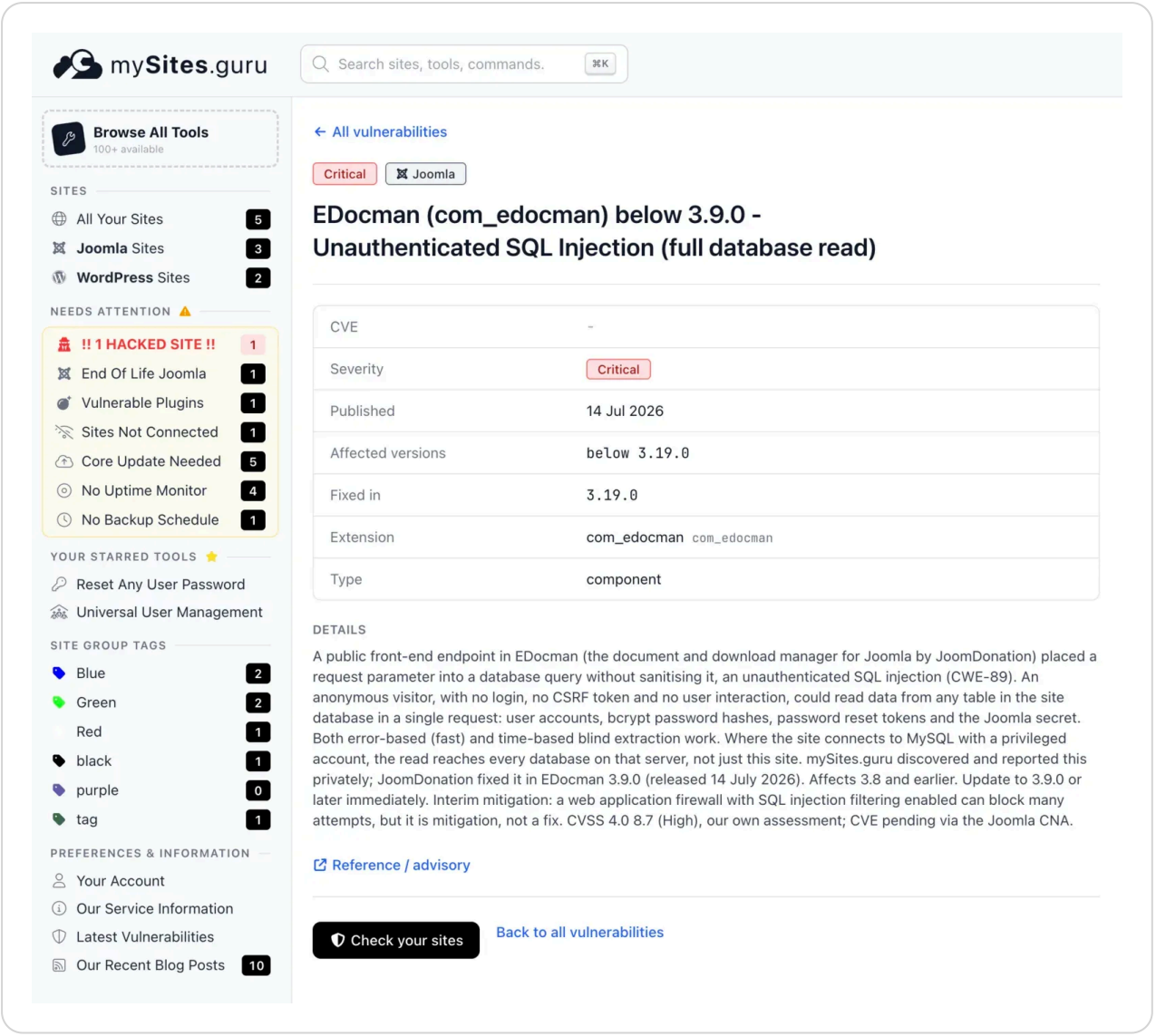
That is the whole workflow, collapsed into two clicks. A disclosure lands, you look at the list, and instead of asking “do I have anything running that,” you are already looking at the exact sites that do, with a **Manage Site** button next to each one to update the extension or investigate it. No spreadsheet of installed versions, no checking each site by hand, no wondering whether you have missed one.

It does not stop at the list, either. Open an affected site and the same vulnerability detail is waiting on its Important tab, flagged next to everything else that needs your attention, with the full write-up rather than a bare extension name.



What each entry tells you

Click any row and you get the full picture on one page: the severity, the CVE, the published date, the affected version range, the version it was fixed in, the extension element, and a plain-English description of what the flaw actually is and how bad it gets.



For the ones we found ourselves, that description is written from having reproduced the flaw against a real install, not paraphrased from a one-line changelog. When a vendor ships a fix with three words of explanation, as Balbooa did with the Gridbox authentication bypass, the detail page is where the missing context lives: what the flaw is, whether it needs authentication, and what it hands an attacker.

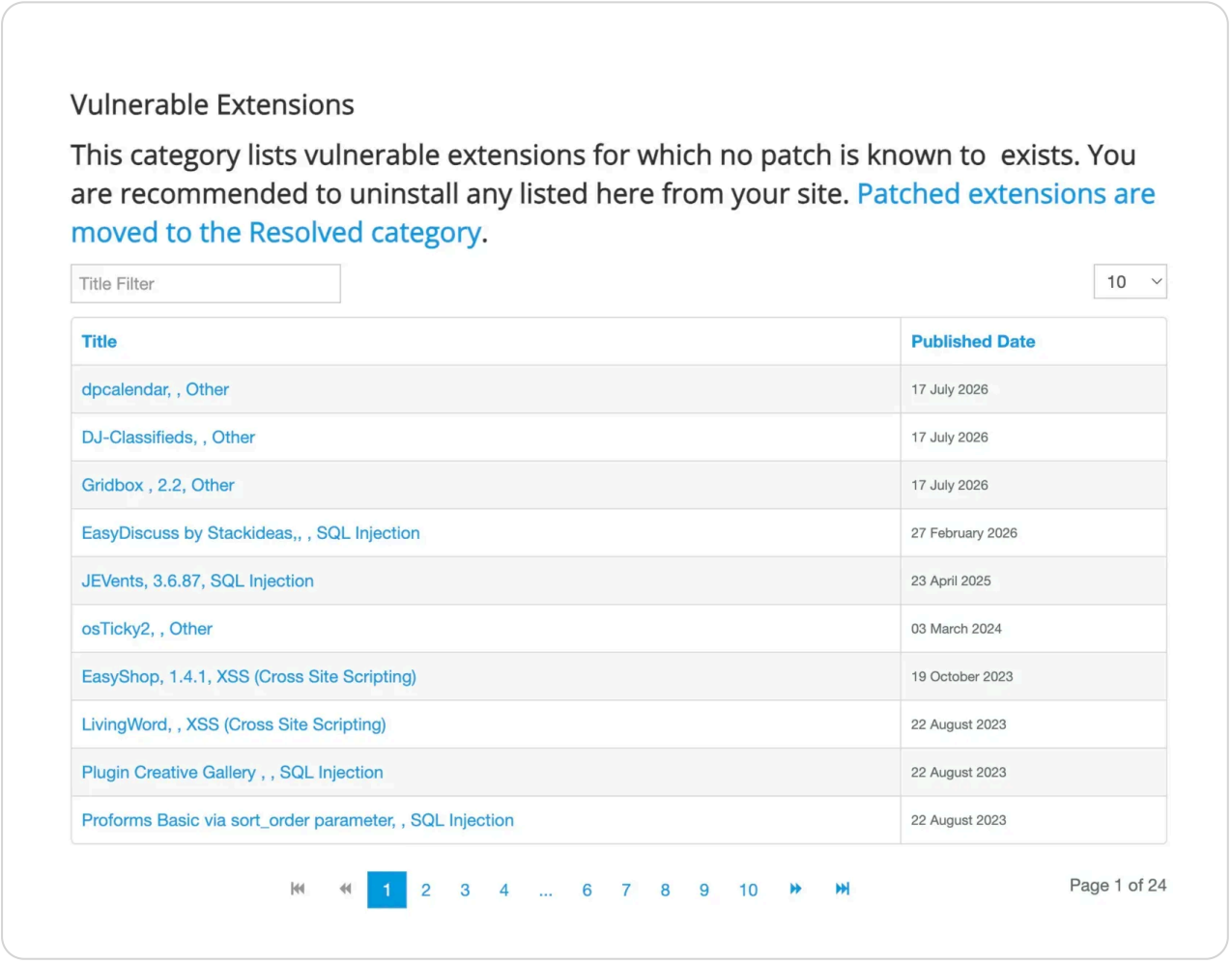
What the Joomla VEL is, and what it leaves out

The official VEL lives at extensions.joomla.org/vulnerable-extensions/vulnerable/ (the memorable `vel.joomla.org` address redirects there). It is run by a volunteer team under the Joomla Extensions Directory, and it covers third-party components, modules, plugins and templates. Joomla core is out of scope, because that is the Joomla

Security Strike Team's job. That split is worth noticing: Joomla's own security structure treats core and extensions as two different problems, and puts a dedicated team on each. Third-party code is not a footnote to the risk, it is most of the risk.

The VEL does its job well within its limits (although it has been largely abandoned), and it is honest about those limits. Its own about page has the line that the list "is compiled from found information and may not be an up to date accurate list." Reports come in manually, by email or a form, and a volunteer team processes them. There is no CVSS score on an entry, just a vulnerability type and a date. And there are only a few hundred entries, because it depends on someone taking the time to report each one.

To see how thin that gets in practice, here is the live list on the day this was written.



Vulnerable Extensions

This category lists vulnerable extensions for which no patch is known to exists. You are recommended to uninstall any listed here from your site. Patched extensions are moved to the Resolved category.

Title Filter

10

Title	Published Date
dpcalendar, , Other	17 July 2026
DJ-Classifieds, , Other	17 July 2026
Gridbox , 2.2, Other	17 July 2026
EasyDiscuss by Stackideas,, , SQL Injection	27 February 2026
JEVents, 3.6.87, SQL Injection	23 April 2025
osTicky2, , Other	03 March 2024
EasyShop, 1.4.1, XSS (Cross Site Scripting)	19 October 2023
LivingWord, , XSS (Cross Site Scripting)	22 August 2023
Plugin Creative Gallery , , SQL Injection	22 August 2023
Proforms Basic via sort_order parameter, , SQL Injection	22 August 2023

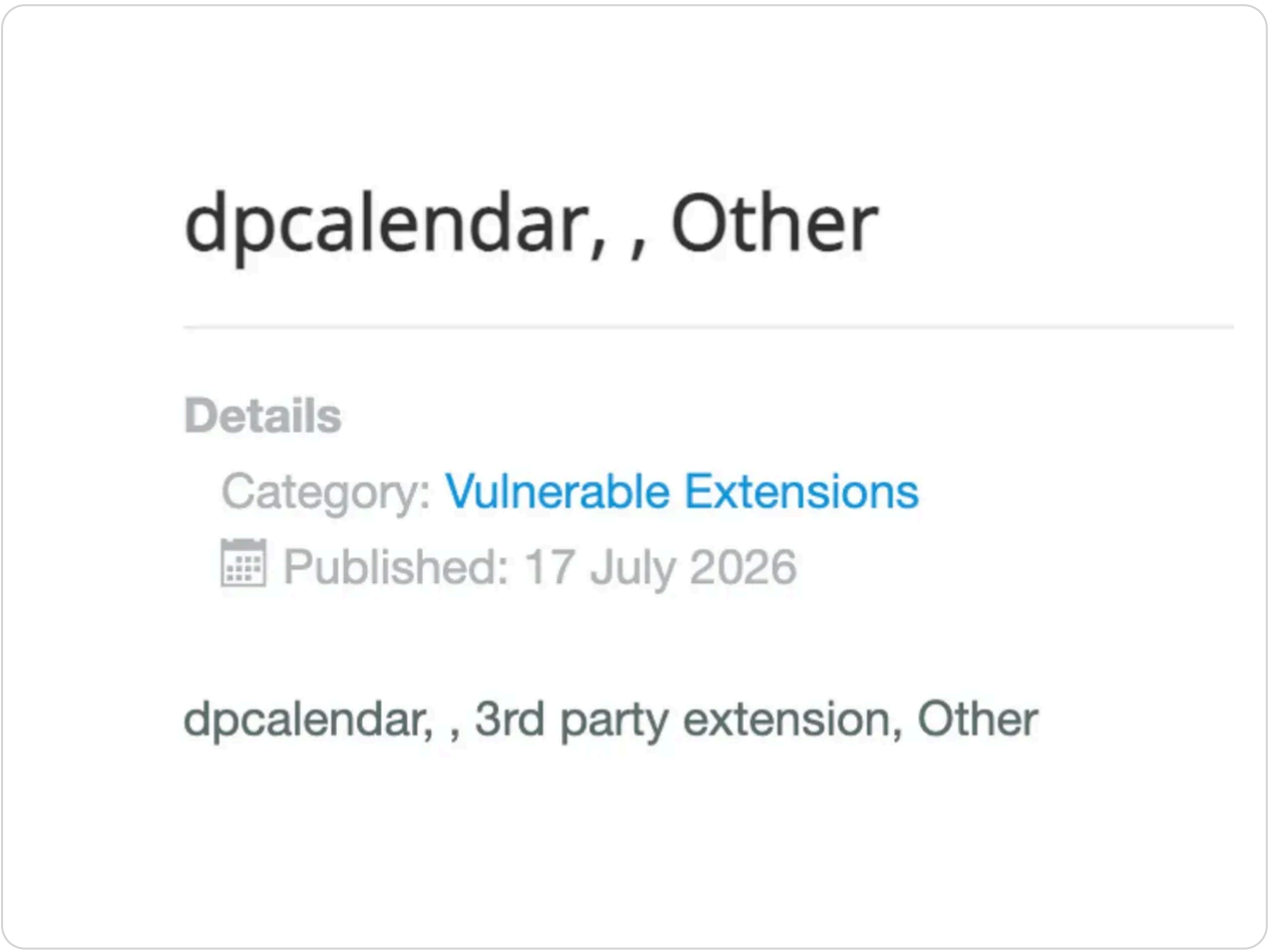
1 2 3 4 ... 6 7 8 9 10

Page 1 of 24

This is page one, the most recent entries, and it already reaches back to 2023. Joomla's official list of currently-vulnerable extensions is adding a handful of entries a year, which is nowhere near the pace of a live threat landscape. The three newest, all

dated 17 July 2026, are DPCalendar, DJ-Classifieds and Gridbox, and they are on the list because we reported them.

Now open one. This is the VEL's complete entry for DPCalendar, a component with a serious unauthenticated SQL injection that lets an anonymous visitor read the entire site database:



That is the whole page. "dpcalendar, , 3rd party extension, Other." No affected version, so you cannot tell whether your install is one of the vulnerable ones. No CVE. No severity. No description of the flaw, no fixed version, and no advice beyond the category page's blanket "uninstall any listed here." A site owner who lands there has learned the name of a component they almost certainly already knew they had, and nothing else. An entry that is not actionable is not doing the one job a vulnerability list exists to do.

None of that is a criticism of the volunteers who keep the VEL running on their own time. It is a small, manual, best-effort list, it is Joomla-only, and for long stretches it has

been close to dormant. If your world is bigger than that, you need something bigger than that.

Why third-party extensions are the real risk surface

It is worth being blunt about where the danger is, because it shapes where you should spend your attention. Patchstack's State of WordPress Security in 2026 report, published in February 2026 and covering the 2025 data, found 11,334 new WordPress vulnerabilities disclosed that year. Ninety-one percent were in plugins, nine percent in themes, and just six were in WordPress core.

Joomla does not publish a headline number like that, but its security structure says the same thing in a different way. Core gets the Joomla Security Strike Team. Extensions get the VEL. The project itself treats third-party code as a separate, large risk surface worth its own dedicated volunteer effort. Keeping core patched is necessary and it is also the easy part. The messy, sprawling risk is the dozens of extensions on each site, each on its own version, each shipped by a different vendor with a different idea of what "security update" means.

That is exactly the surface a portfolio-wide list is built for. One vulnerable component across two hundred sites is not two hundred problems you find one at a time. It is one search.

Why a volunteer list can never keep up

Managing CVE and security information at the pace it now moves is close to a full-time job on its own. Wordfence alone publishes new vulnerability reports at a rate north of two hundred a week. No volunteer effort keeps up with that, and the Joomla ecosystem is chronically short of experienced volunteers, so the VEL has always run behind, and on its current model it always will.

There is talk of a resurgence, and the Joomla project is making some small improvements to how vulnerable extensions are handled (this pull request is a start,

and it is good to see). But small tweaks to a volunteer-run list do not change the arithmetic. They cannot make it reactive, and they cannot connect it to your sites.

We can say that because we are at the coal face. mySites.guru is in daily contact with the best part of a hundred thousand Joomla and WordPress sites, we take in reports from those sites every day, and a large share of the recent Joomla entries on the official VEL are ours. That is a different vantage point entirely from a list that updates whenever a report happens to arrive. When you are looking after five hundred Joomla sites, the useful question is never whether an extension is vulnerable in the abstract. It is which of your five hundred are running it, and on what version. That is what mySites.guru was built to answer.

How is the mySites.guru list different from the official Joomla VEL?

Four ways, and none of them are about replacing it.

First, coverage: the VEL is Joomla-only, this covers Joomla and WordPress in one list.

Second, detail: every entry has a severity and, where one exists, a CVE, rather than a bare vulnerability-type label.

Third, and this is the one that matters, it is connected to your sites. The VEL tells you a piece of software is vulnerable. mySites.guru tells you that three of your clients are running it, and takes you to them.

Fourth, it is active. It is maintained by mySites.guru and can be added to within seconds of us discovering something new, with no wait on a volunteer team to receive and process a report. When we confirm a flaw, every connected site is being checked against it almost immediately.

The official VEL is still worth reading, and we still contribute the flaws we find back into the wider ecosystem. If you manage a handful of Joomla sites and nothing else, it may be all you need. The moment you are managing more sites than you can hold in your

head, or any WordPress alongside your Joomla, a static list you have to cross-reference by hand stops scaling. That is the point this was built for.

Why is this behind a paywall?

mySites.guru has never been a free service. It is a subscription product, and this is a feature inside it, built for the paying subscribers who get value from it. It is not a community resource for the Joomla project and was never offered as one. The vulnerability list sits alongside the extension inventory, the updates, the backups and the audits, and it comes with the subscription the same way everything else does. If you want our data, out of our database, you subscribe.

The raw ingredients are free if that is what you are after. Every CVE we list is published by the NVD and anyone can read it. Wordfence publish their WordPress vulnerability database. The Joomla VEL is public, for as long as anyone is still updating it. Nobody is stopping you watching all of those yourself.

What the subscription pays for is the work wrapped around that data: collating it, researching it, investigating the flaws ourselves, and then cross-matching the whole lot against the extensions actually installed on the sites actually in your account. That means you are not sitting across four vulnerability databases hoping you catch it when somebody drops a zero-day at three in the morning. It arrives in one place, already matched to your sites.

That is where the value is for anyone running sites in volume. When something new hits SP Page Builder, one click tells you which of your sites run it and on what version. For a digital agency looking after five hundred sites, some of them a decade old and inherited from somebody else, having that answer in seconds instead of an afternoon is the entire point. At £19.99 a month for unlimited sites, it works out at pennies per site to never cross-reference a vulnerability by hand again.

How do I see my affected sites right now?

If you already have sites connected to mySites.guru, open the Latest Vulnerabilities page from the sidebar, or hit **Check your sites** on any entry. Anything you are running that is vulnerable is flagged, and the Vulnerable Plugins filter on your sites list has been doing the site-by-site version of this for a while.

If you are not connected yet, that is the first step. Add your sites and mySites.guru builds the inventory of every extension and version across all of them, then keeps it cross-referenced against the vulnerability list from then on. The next time a disclosure lands, whether it is Joomla or WordPress, you will not be asking whether it affects you. You will already be looking at the list of sites that need updating.

Further reading

- Joomla Vulnerable Extensions List, official about page
- Wordfence Intelligence, WordPress Vulnerability Database
- Patchstack, State of WordPress Security in 2026
- Manage every extension across all your Joomla sites

Manage all your Joomla and WordPress sites in one place

One dashboard for every site you look after: a live inventory of every extension and version, both platforms in one vulnerability list, and every affected site flagged the moment something is disclosed. Updates, backups and audits from the same screen.

Add your sites and see what is vulnerable

Not ready to connect anything yet? Run a free audit on a single site to see its full extension inventory and where it stands, or read more about managing multiple Joomla sites and multiple WordPress sites from one dashboard.

1. The WordPress vulnerability data in the mySites.guru list is republished from the Wordfence Intelligence vulnerability database and the MITRE CVE program. Both licences require their text to be reproduced in any copy, so they are set out in full below. The Joomla entries are mySites.guru's own research and curation.

Copyright 2012-2024 Defiant Inc. Defiant hereby grants you a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, sublicense, and distribute this software vulnerability information. Any copy of the software vulnerability information you make for such purposes is authorized provided that you include a hyperlink to this vulnerability record and reproduce Defiant's copyright designation and this license in any such copy.

Copyright 1999-2024 The MITRE Corporation. CVE Usage: MITRE hereby grants you a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, sublicense, and distribute Common Vulnerabilities and Exposures (CVE). Any copy you make for such purposes is authorized provided that you reproduce MITRE's copyright designation and this license in any such copy. ↩

Frequently Asked Questions

What is the Joomla VEL (Vulnerable Extension List)?

The VEL, or Vulnerable Extension List, is a community-run list of third-party Joomla extensions with publicly reported vulnerabilities, hosted at extensions.joomla.org/vulnerable-extensions/vulnerable/. It is maintained by a volunteer team under the Joomla Extensions Directory, covers components, modules, plugins and templates, and deliberately excludes Joomla core, which is the Joomla Security Strike Team's job. It is manual, best-effort, and its own about page states it may not be an accurate or up to date list.

Does the Joomla VEL cover WordPress?

No. The VEL is Joomla-only, by design. WordPress has its own separate ecosystem of vulnerability feeds such as Wordfence Intelligence, WPScan and Patchstack. If you run both Joomla and WordPress sites, you have to watch at least two completely different sources. mySites.guru's Latest Vulnerabilities page merges both into one list, filterable by platform.

How do I know which of my sites are affected by a vulnerability?

The VEL and the WordPress feeds are reference lists, not personalised. They tell you a piece of software is vulnerable somewhere, but not whether you run it. mySites.guru keeps a live inventory of every extension and version on every connected Joomla and WordPress site and cross-references it against the vulnerability list automatically. Any site running an affected version is flagged, and you click straight through to that site to update or investigate.

Where does mySites.guru get its vulnerability data?

From several places. On the WordPress side, tens of thousands of plugin and theme records from the wider feeds. On the Joomla side, published CVEs from the Joomla CNA and other sources, plus a large number of vulnerabilities mySites.guru found and disclosed itself, including flaws in Gridbox, Balbooa Forms, Events Booking, SP Page Builder and others. Each rule carries the affected version range, so matching is version-aware, not just name-aware.

Is this the same as the official Joomla VEL?

No, and it is not trying to replace it. The official VEL is the community reference for reported Joomla extension issues and remains worth reading. mySites.guru's list is wider (Joomla and WordPress), carries a severity rating and a CVE where one exists, and is wired into your

actual sites so you see which ones are affected. Think of it as the VEL idea extended across both platforms and connected to your own portfolio.

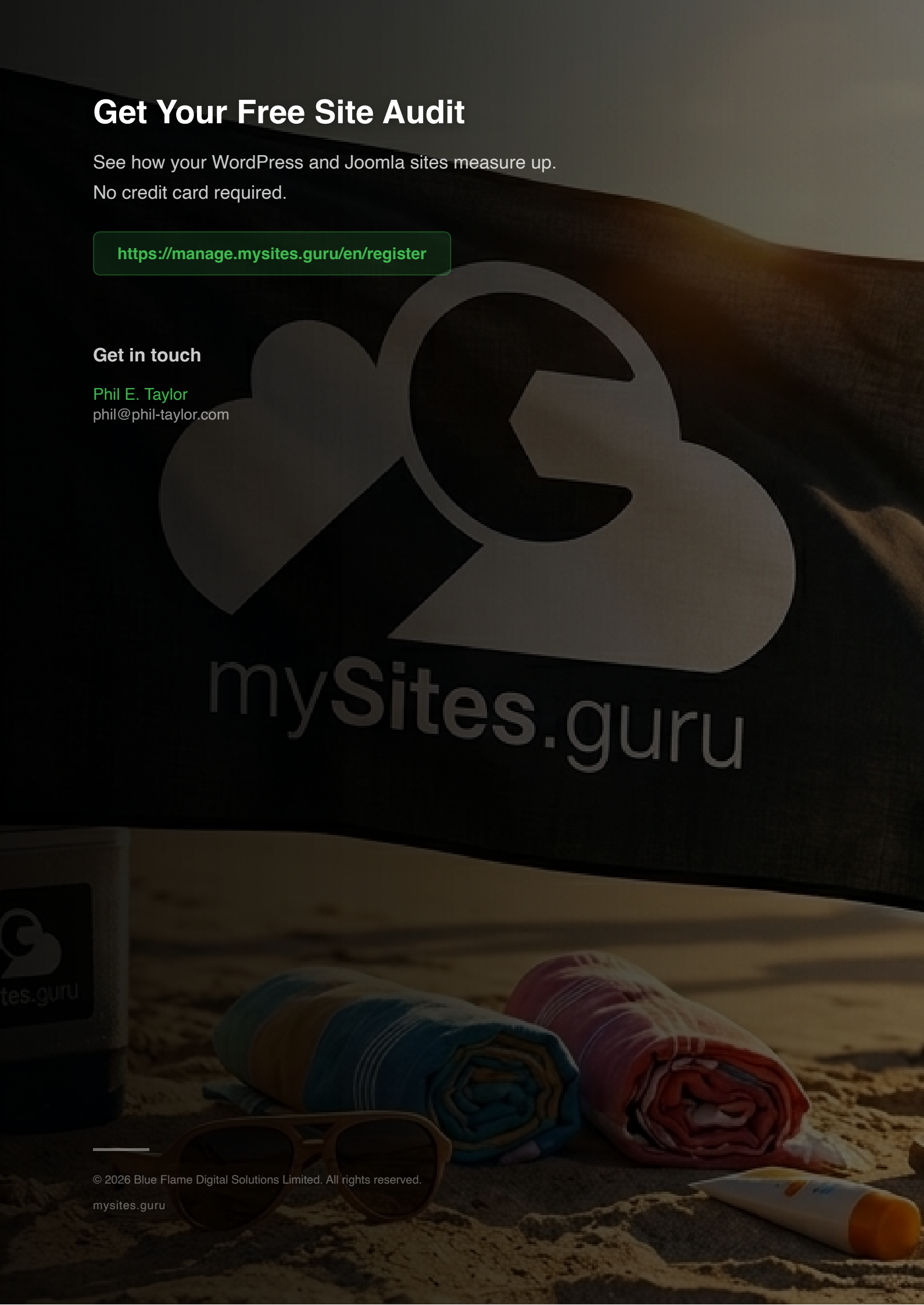
Written and edited by a human, with AI assistance. Our approach to AI

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

© 2026 Blue Flame Digital Solutions Limited. All rights reserved.