Summer 2026: Everything New in mySites.guru

Everything new in mySites.guru this summer: 38 new tools, 40 improvements, and the 19 Joomla extension vulnerabilities we found and disclosed ourselves.

Phil E. Taylor | 24 August 2026

5 LIVE **Joomla extension security alerts** latest 22 Aug Fabrik 4.7.2 · ZOO: unauth RCE · Phoca Cart: unauth SQLi · JCE 2.9.99.10 · SP Page Builder RCE

If you already pay for mySites.guru, most of what follows is sitting in your account right now, and there is a fair chance you have not spotted it yet.

That is the strange thing about shipping steadily. The work arrives a piece at a time. A new check appears in an audit you were already running. A button turns up on a page you have opened a hundred times. Every one of them goes into the changelog in the left menu of your dashboard the day it ships, but not everybody reads a changelog, so this is the highlight reel.

Between 1 June and 24 August 2026 we added 38 new tools and features to mySites.guru, and improved 40 more that already existed. This is the first time we have written any of it up in one place, and it is the first of a seasonal series. Autumn will get its own.

What follows is a tour of all of it, grouped by the problem it solves rather than the order it shipped, with a link straight into each tool. If you are not a subscriber, read it as the answer to a fair question: what does a platform like this actually do with three months, and would you rather be the person running those checks by hand?

Summer 2026, in six numbers

- **38** new tools and features, 1 June to 24 August
- **40** improvements to tools that already existed
- **60** new Joomla extension vulnerability rules, out of **221** we now track
- **19** Joomla extension vulnerabilities we found and disclosed ourselves in the first month alone
- **43** changes this year that exist because a customer asked for them
- **90** five-star reviews left over the same three months

Making hacked files stand out from suspect content

The biggest change is a split. Until June your audit had one list called Suspect Content, and it mixed two very different things: files we are certain are compromised, and files that merely matched a heuristic pattern and are worth a look. Lumping them together had an honest and predictable result, which is that people learned to skim past the lot. There is now a separate **Hacked Files (100% Certain)** tool listing only what we are sure about, and Suspect Content shows only the pattern matches. If you have ever wondered which findings actually need you, that is the answer. Here is what the two lists mean.

Then the detection itself. The JCE compromise got a dedicated check that finds the rogue editor profiles the attack creates and the webshells it drops, removes both, and points you at the mass-update tools so the site cannot be breached the same way again. The full guide is here, and thanks to Marc for the push. Days later the scanner learned the mutations: renamed webshells, disguised droppers and obfuscated variants the first signatures missed.

The Helix Ultimate template framework got the same treatment twice. In July we started detecting menu code injected into a Helix mega menu, off the back of the unauthenticated menu write we disclosed in Helix Ultimate 2.2.7. Three weeks after that an attacker shipped a variant that broke out of the CSS class attribute and hid scripts behind font and image file extensions, so the check was rewritten to inspect every mega-menu setting at any depth, and the clean-up now blanks only the settings that actually matched. A separate check finds menu items drawing a correctly styled but completely empty mega-menu dropdown, usually under Home, left behind by a legacy layout setting from old Helix versions. That one is not a hack, a working mega menu is never touched, and one click fixes it.

Smaller, and worth knowing about: double-extension files like `config.php.bak` and `shell.php.json`, where a `.php` hidden behind a second extension can still be executed or quietly leak your source code; PHP files disguised specifically behind a `.json` extension; the `admin_mori` and `memetkaan` worm accounts, now caught by username in the Rogue Super Admin check; and backdoor detection that matches

known shell filenames before it reads a single byte, which makes audits faster as well as more accurate.

Cron Jobs reads the scheduled jobs on your server and flags any that match known malware patterns. Cron is how an attacker survives a file clean. You delete the webshell, a scheduled job puts it back an hour later, and you spend a fortnight wondering why the site keeps coming back. It went out in July and has since learned to leave your host's own cron-auditing scripts alone, since those search crontabs for exactly the words we do. Here is why we built it.

Finally, the Multiple .htaccess Files tool gained a one-click button that deletes every stray `.htaccess` across your webspace in a single server-side pass, preserving your root file and the known hardening files. We have seen sites carrying close to 9,000 of them.

★★★★★

"If you think you've manually cleaned your Joomla site of all hacked files, you're 100% wrong. This program is absolutely incredible, and it finds Every File that is hacked or suspect."

Mike K
15 July 2026

AI, now that it earns its keep

Every company rushed to add "AI-powered" to their product: chatbots that frustrated users, buzzwords with nothing behind them. We sat that out, and people asked why.

For over a decade we have secured Joomla and WordPress sites. We knew the audit system worked well at finding threats, but it casts a wide net, and a wide net means false positives. Users had to read the code themselves or wait for us to review files by hand. So we spent months testing before shipping anything: thousands of files

analysed, AI results compared against expert review, accuracy and cost measured. The question was never whether AI was fashionable. It was whether AI could reliably do the thing users struggle with, which is reading PHP, spotting suspicious patterns, and telling legitimate code apart from malware. It can.

False positives have cost our users hours of manual review for over a decade. This is the thing that addresses it, which is why this summer went on putting it everywhere it belongs.

“Analyse Files with AI” used to live on one tool. It is now on nearly every file list in the product: Hidden Files, SQL Files, Renamed Files, Mass Mailers, Upload Files, Modified Files and many more. If a tool hands you a list of files, you can bulk-scan them.

Two changes made that practical rather than expensive. Analysis now skips machine-generated cache files and Akeeba backup logs, so your spend goes on files that could plausibly be malicious instead of on noise. And there is a one-click key test on the AI Integration page that confirms your key is live and lists the models it can use, at no charge. When analysis does fail because a provider key has run out of credit, the error now says so in plain English and links you straight to that test, rather than showing you a raw API response.

One more thing, because people do ask. mySites.guru is not a vibe-coded side project. Plenty of those are appearing right now, and a fair number of them will be gone as quickly as they arrived, which is a problem when you have handed one of them the keys to every site you manage. This is a full-time job and has been since 2012. The platform was built long before AI was mainstream, it is written and maintained by hand, and it is going to stay that way. We use AI the way any competent developer uses it now, which is to work faster. We do not use it to generate a product nobody understands.

The part people miss: AI analysis is bring your own API key. You add a key from Anthropic or OpenAI, it is admin-gated, and it does nothing at all until you turn it on. We do not resell tokens and there is no markup. The model list was refreshed in May to the current generation from each series, so the dropdown now offers Claude Opus 4.7, Sonnet 4.6 and Haiku 4.5 alongside GPT-5, GPT-5 Mini, GPT-4o Mini and o3. How the whole thing works.

The case for centralised management

This is the half of the product that justifies itself when you manage more than about ten sites.

Two new Joomla audit checks come with a toggle rather than instructions. **Force SSL Should Be Set To Entire Site** warns when a site does not force HTTPS site-wide, which can expose login and password-reset links over plain HTTP, and you flip it on from the audit result. **Force Multi-Factor Authentication For Super Users** flags Joomla 4.2 and newer where MFA is not enforced for the Super Users group, and turns enforcement on the same way.

Akeeba Admin Tools has a habit of auto-banning our IP address, which silently breaks audits, snapshots, backups and updates on that site. We now detect it and unblock with one click, both from the tools list and from the connection troubleshooting wizard, with no SSH or hosting login needed.

Joomla itself supplied a good deal of this summer's work. Sites upgraded to Joomla 6 were being left with language update sites still pointed at the previous version, which silently stops language packs updating, so snapshots now flag it and fix it in one click. Joomla 5.4.7 and 6.1.2 shipped a regression where every per-article Option is ignored on the front end, so your snapshot counts the affected articles per site and Tools will apply Joomla's official hotfix on request, only to an unmodified core file, and only when the result matches Joomla's own patched file byte for byte. Then Joomla 5.4.8 and 6.1.3 broke the Template Manager, so a new tool shows which of your sites are affected and applies or removes the fix from Joomla PR #48274, checking the file before and after every write.

The JoomShaper Joomla 3 patch tool grew twice: it now deploys the latest Helix Ultimate fixes, and backports the SP Page Builder CSRF, rate-limiting and SQL-quoting fixes across 17 files, which matters because JoomShaper stopped shipping Joomla 3 security fixes, backing up each patched file individually rather than all or nothing. Sites still on an earlier patch are flagged so you can re-apply the newer one. It also spots a Helix Ultimate template style that has been wiped, which is what makes a site lose its header, logo and mega menu while the rest of the page still renders. That is the

signature of the Helix3 defacement wave that lives in your database rather than your files.

Elsewhere, a new **User Accounts and Access** check finds users who belong to no user group on Joomla or hold no role on WordPress, and lets you assign or remove them in one click. User search gained last-login, password-reset and blocked-status columns, sortable, with bulk-blocking across your Joomla sites and CSV export. And Joomla 3 sites carrying unpatched end-of-life security issues now show a patch count badge on your sites list that takes you straight to the fix.

★★★★★

"In the past week I've been notified regarding new extension security updates and vulnerabilities, and with a 1 button click, all 20 were patched."

P Paul Bailey
9 June 2026

The vulnerabilities we found ourselves

The vulnerability rules above have to come from somewhere. Increasingly, they come from us.

Between mid-June and late July we found and responsibly disclosed nineteen separate security vulnerabilities across seventeen popular Joomla extensions. Most were critical. Five rated the maximum CVSS 4.0 score of 10.0. Every one was reported privately to the vendor first.

It did not stop in July. Gridbox turned out to have an authentication bypass where one cookie made you a Super User, and then another 23 critical issues on a second pass. EasyStore was exposing customer invoices and accepting forged orders. SP Page Builder gave up a pre-authentication SQL injection and an open mail relay in July, then

unauthenticated remote code execution in August. Phoca Cart had a front-end SQL injection. JEM has five issues and, at the time of writing, no stable fix.

We are not the only people doing this, and that is a good thing. But we do it differently in one respect: we publish the standard we hold ourselves to, including what we expect from a vendor handling a report, because the handling is usually the part that goes wrong. Cotton Cloud patched the login and left the data. Page Builder CK shipped a fix that did not fix it.

Every one of those findings becomes a vulnerability rule in your account within hours, usually before the vendor has shipped anything. That is where a good number of this summer's 60 new Joomla extension rules came from. When you get an alert saying a site is running something vulnerable, there is a reasonable chance we are the ones who found it.

Knowing before we have to tell you

There is now a public Latest Vulnerabilities page listing every Joomla and WordPress vulnerability we track, searchable, filterable by platform and severity, with no login required. Why we published it.

Better than looking, though, is being told. A daily digest now emails you when a newly vulnerable extension turns up on one of your sites. It lists only what is new since the last one, so a site that fixes one vulnerability and gains another still reaches you, and whatever is already on your sites counts as the starting point so you are not emailed about the backlog. Thanks to Christian for that one. Alongside it, the vulnerable extensions panel on a site's Manage page now shows a severity badge for each finding, says which version fixes it, and links straight to the full advisory. There is also a weekly digest for any site still flagged as hacked, so a compromise cannot quietly slip off your radar.

On the site itself, warnings that used to stack above the tabs now live in a red **Important** tab that only appears when a site needs attention and opens itself when it does, so you arrive on what needs fixing. Near-realtime file change alerts on Joomla

sites watch `/index.php` and `libraries/src/Layout/LayoutHelper.php` by default, both long-standing favourites with attackers. Downtime notification emails now name the server your site is hosted on, which makes a whole-host outage obvious at a glance rather than after the fifth email. Thanks Troy. Uptime alerts also link to the full explanation of how our monitoring works, including why a site that never went down can still be reported as down.

If you drive mySites.guru from an AI assistant, the MCP server gained a `get_site_vulnerabilities` tool, so you can ask which vulnerable extensions a site is running and get back the CVE, the severity and the version that fixes each one. Setting that up.

★★★★★

"I have to say the attention and notifications to users as related to JCE and SP PageBuilder exploits, site scans and recommended fixes have elevated mySites far beyond what we ever signed up for years ago when all we wanted was a quick way to automate backups."

Mark
Image Build · 16 June 2026

Getting out of your way

Not everything is security. A good deal of the summer went on the friction you notice every day and never get round to reporting.

You can now add up to 50 tags per site, up from 10. The Site Access list when adding or editing a team member has a search box and grows to show every site instead of sitting in a short scroll box, which matters once you pass about thirty sites. Thanks Tim. The Manage Site menu opens on click, with dropdowns that float over the page, instead of revealing on hover and shifting the content under your cursor.

Browse All Tools and the ⌘K quick launcher now list every audit check we run, not just the popular ones, so you can check a single issue across all your sites from one place. The “taking snapshot” dialog shows an honest elapsed timer with reassurance that updates the longer it runs, rather than a spinner that tells you nothing. The Locate And Review Files Over 2Mb tool sorts by file size, largest first. Thanks Adi.

Backup, Snapshot and Export now show how many sites they will actually touch once you have filtered your list, so the button reads Snapshot (12) rather than just Snapshot. Thanks Adi again. The extensions CSV export honours the filters you have on screen and covers every extension type your site reported.

Backups got three fixes worth having. Runs started from mySites.guru now carry a description saying what the site was running and what started the run, such as “Joomla 5.4.8 - Manual - mySites.guru”, where every backup used to get the same fixed label and archives taken either side of a core update were impossible to tell apart. Manual, scheduled, bulk, API and MCP runs are each named. The backups list shows each archive’s description and comment under the date, including any comment you typed in Akeeba itself, which we were already being sent and were throwing away. And after an automatic extension update we now take a snapshot five minutes later, so the extension versions you see are the ones you just updated to rather than yesterday’s.

Paperwork you can hand a client

Agencies get asked for this, usually at the worst moment, and usually by a client’s compliance team.

Our Data Processing Agreement is now published in full: the complete sub-processor list, our technical and organisational measures, and exactly what data does and does not leave your connected sites. It is Article 28 GDPR compliant and you can accept it in one click if your process needs a dated record.

The Privacy page was rewritten to set out how little actually leaves a connected site. Routine monitoring sends counts and version numbers rather than content. Malware

scan hashes stay in your own site's database. Backups never reach us at all. The vendor list was corrected at the same time.

We also published a security disclosure policy covering the platform and the connector: where to send a report, what is in scope, how quickly we respond, and the safe harbour you get for good-faith research. There is a machine-readable copy at `/.well-known/security.txt` and a CycloneDX software bill of materials that we regenerate on every dependency change.

For the more practical kind of paperwork, there is a shareable reference page for web hosts listing every IP we connect from, the endpoints your connector calls out to, and exactly what to allow through the firewall in each direction. No login needed, so you can send the link straight to a hosting support desk. And the contact page now leads with any current platform issues, shows the three newest changelog entries, and answers 38 of the questions we get asked most.

Forty-three of these started as an email

This is the number I am proudest of, so it gets its own section.

Forty-three of the changes we made in the last twelve months exist because a customer wrote in and told us something. Not a feature request form, not a public roadmap board with votes on it. An email, usually two lines long, usually apologetic about bothering us.

Some of them are exactly what you would expect. Adi wanted the large-files tool sorted by size, largest first, and later pointed out that a bulk action should tell you how many sites it is about to touch, so the button now reads Snapshot (12). Laurent wanted the update results filtered by site tag, and got coloured tag pills under the search box. Tim wanted a search box on the team-member site-access list, which had quietly outgrown its scroll box. Isidro wanted the Reload button on the By Site view to stay on the By Site view. Julian pointed out that our alert emails were unreadable in dark mode. Small things. Somebody's daily irritation, fixed because there is one person to tell and he replies.

The ones I did not expect are the ones where a customer corrected the detection engine itself.

Andrés noticed the vulnerability matcher was flagging Slider Revolution installs as old as 6.7.x against an advisory that only covered 7.0.0 to 7.0.10, because the matcher was comparing against the patched version and ignoring the bottom of the range. That was wrong for every customer, not just his. Andrzej found two more in one week: a WordPress plugin flagged against a fixed version that only exists in the paid tier, so there was nothing to update to, and advisories writing a version as 4.3.0 while the plugin reports 4.3, which flagged people who had already updated. Marc caught the JCE compromise check reporting a *defensive* `.htaccess` as a backdoor, because a directory that denies PHP execution was being read as one that enables it. Scott found that the robots.txt one-click fix was reporting “Fixed!” on files with Windows line endings without changing anything at all, which is the worst kind of bug because it looks like success.

Pat went further and contributed a signature. The Rogue Super Admin Accounts tool now flags accounts created with the `joomla@test.com` address, because Pat had seen it on compromised sites and told us.

And then there is the one that still surprises me. In July a customer sent us a raw access log from their host, asking what a pattern in it meant. It was an active zero-day in Balbooa Forms, unpatched, letting an anonymous visitor upload a file and run code. We wrote the detection, warned every affected account directly, and published the workaround before the vendor had a fix. That disclosure started as one person forwarding a log file because something looked odd.

Marc, Adi, Laurent, Anne, Chris, Cathy, Tim, Mike, Antonis, Sven, Diggles, Andrés, Mirko, Isidro, Martijn, Nico, Troy, Scott, Julian, Frédéric, Peter, Andrzej, Wilm, Pat and Christian: thank you. The changelog credits every one of you by name, which is the least we can do.

If something in your account annoys you, or looks wrong, tell us. That is not a platitude, it is where forty-three of this year’s improvements came from.

And the nine months before that

Summer was busy, but it was not the whole year. Briefly, and in no particular order.

AI arrived in stages, starting last October with sending suspect content files to Claude or OpenAI, becoming full malware analysis in January. The public API got its OAuth and identifier work over the winter and was finally documented properly in June, and an MCP server went live the same month so you can drive your whole account from an AI assistant, ChatGPT included.

While we are here, two things that turned up on this blog in February are not new at all, and it would be cheeky to count them: passkey login has worked since 2020, and the Raycast extension for Mac has been around for years too. We had simply never written either of them up, which is its own kind of failure.

Two hosting compatibility checkers went up ahead of the big platform releases, one for Joomla 6 and one for WordPress 7, each comparing your server's PHP and database versions against the official requirements. Joomla backward compatibility plugin status became trackable across every Joomla 5 and 6 site, with a remote toggle so you never log in to turn it off. Module versioning for Joomla 6.1 got a one-click enable, so module config changes can be rolled back.

Locked Joomla scheduled task detection went into the snapshot for Joomla 4.1 and up, thanks to Marc. A new tool audits and toggles the `WP_AI_SUPPORT` constant across WordPress 7 sites. Every blog post here became downloadable as a PDF. You can finally delete team members, which took an embarrassing number of years and a push from Tim. Three user tools appeared at once for both platforms: inactive users, unactivated users and blocked users, each with block, unblock and delete. Theme and template lists gained CSV export. And the Joomla 3 end-of-life security patch tool was updated in January to carry every known fix for a version that is no longer supported.

What you are actually paying for

Speed of response. Two of the tools above exist only because Joomla shipped a regression and there was no upstream fix yet. When 5.4.8 and 6.1.3 broke the Template Manager so that creating overrides and folders failed, the tool that identifies affected sites and applies the community fix went out four days later. If you manage sites for clients, the gap between a platform breaking and someone handing you a fix is the thing you are actually buying.

Detection that keeps up. The Helix Ultimate mega-menu check was written in July and rewritten three weeks later, because an attacker adapted to it and started hiding scripts behind font and image file extensions. That is the normal shape of this work. A signature list nobody revisits is worse than no signature list, because it tells you that you looked. The JCE checks went the same way, twice, in a single month.

One person to tell. Everything in the section above happened because somebody wrote in and there was somebody to write to. That is worth more than any single tool on this page, and it is the part a feature list never shows you.

What is coming next

There is a long to-do list. There always is, and some of it has been sat on there for a year.

Most of the next batch will come from somebody writing in, though, rather than off that list. Forty-three times in the last twelve months that is exactly what happened, and autumn will go the same way. So if something is missing, or slow, or in the wrong place, get in touch and say so. A request from somebody managing sites all day is worth more than anything we would sit here and invent.

The rest gets decided for us. A Joomla extension vulnerability turns up and a detection rule has to follow it, sometimes within hours. An attacker adapts to a check and the check gets rewritten, which happened twice this summer. And when the same question arrives in support three weeks running, it usually turns into a feature, because a question asked that often is telling us something is missing.

Which is why there is no roadmap with dates on it. The changelog in the left menu of your mySites.guru dashboard is the closest thing to one, written up the day each thing ships. If you want to know what is coming next, check there first.

Ninety people said so this summer

Between 1 June and 24 August, 90 people left a five-star review.

★★★★★

“So I'm just two weeks (or so...) here at mySites.guru. What should I say? Perfect. Secure. Reliable. And damn fast! Thank you, Phil, you saved my customers and my soul! :-) Greetings from Germany!”

Klaus Brandt
1 August 2026

★★★★★

“Life changing. Amazing capability and TOP QUALITY design and interface. Would have added years to my life if I had discovered this earlier. I am dramatically more productive and my 25+ Joomla sites have never been better maintained or run more smoothly.”

TC
29 July 2026

★★★★★

“Helicopter view for your sites & Timesaver for resolving technical issues or mass install (and so much more). A must have for everyone with many

Joomla! and Wordpress installations."

Tim
ictineo.nl · 5 August 2026

★★★★★

"Saves time, saves money, saves websites from being hacked. What more could you ask for???"

Peter Dowse
Marketeam, Brisbane · 7 August 2026

Every reviewer is a real person with a real name, and that is deliberate. There are no anonymous testimonials on this site and nothing is paid for. WP Mayor also reviewed mySites.guru independently and scored it 4.6 out of 5, which is worth reading precisely because we had no say in it. If you would rather read the recurring themes than the raw list, that is here, and we have since counted what all ninety of this summer's reviews mention, which threw up a result we did not expect.

If any of this sounds like your week, the free site audit is the honest way to find out, and it does not need a card.

The next one

This becomes a seasonal post, so autumn 2026 gets the same treatment: what shipped, why, and who asked for it.

Subscribers do not need to wait for it. Everything here appeared in the dashboard changelog as it happened, in the left menu, with a badge showing whether it was new, improved or fixed. This post is a summary for people who would rather read the story once than follow it a line at a time.

Frequently Asked Questions

Does any of this cost extra?

No. Every tool and improvement described here is part of the existing mySites.guru subscription, and nothing above is a paid add-on. There is one thing that needs something from you: AI malware analysis runs on your own Anthropic or OpenAI API key, which those providers bill you for directly. We do not resell it and we do not add a markup. It is admin-gated and off until you turn it on.

How do I see what is new without waiting for a blog post?

Open Changelog in the left menu of your dashboard. Every user-facing change is posted there as it ships, with a coloured badge showing whether it is new, improved, fixed or a security item. New entries are announced in the left menu and in the page header until you have seen them. The three newest entries also now appear on the contact page, so you can check whether we already know about something before you write in.

I have started getting emails I did not ask for. How do I stop them?

Two new digests started this summer: a weekly one for sites still flagged as hacked, and a daily one when a newly vulnerable extension turns up on one of your sites. Both can be turned off per user under [Account then Notifications](https://manage.mysites.guru/en/account/notifications/), and the vulnerable-extension digest can also be turned off for a single site under Settings on that site's Manage page. Site hacked notifications have had a per-user opt-out since April.

What is the difference between Suspect Content and Hacked Files (100% Certain)?

Until June they were one list. Hacked Files (100% Certain) now shows only files we are certain are compromised, so everything in it needs action. Suspect Content now shows only heuristic pattern matches, which are worth reviewing but are not on their own proof that a site is hacked. Splitting them means a confirmed compromise is no longer buried among findings that turn out to be legitimate code.

Do the new checks run on their own, or do I have to do something?

They run automatically on the next snapshot or full audit of each site, so you do not need to enable anything. If you would rather not wait for the scheduled run, start a snapshot or an audit from the site's Manage page, or run one across your whole account from the sites list.

A few of the items here are settings rather than checks, such as skipping the audit email test on a particular site, and those you do have to switch on yourself.

Will there be another one of these?

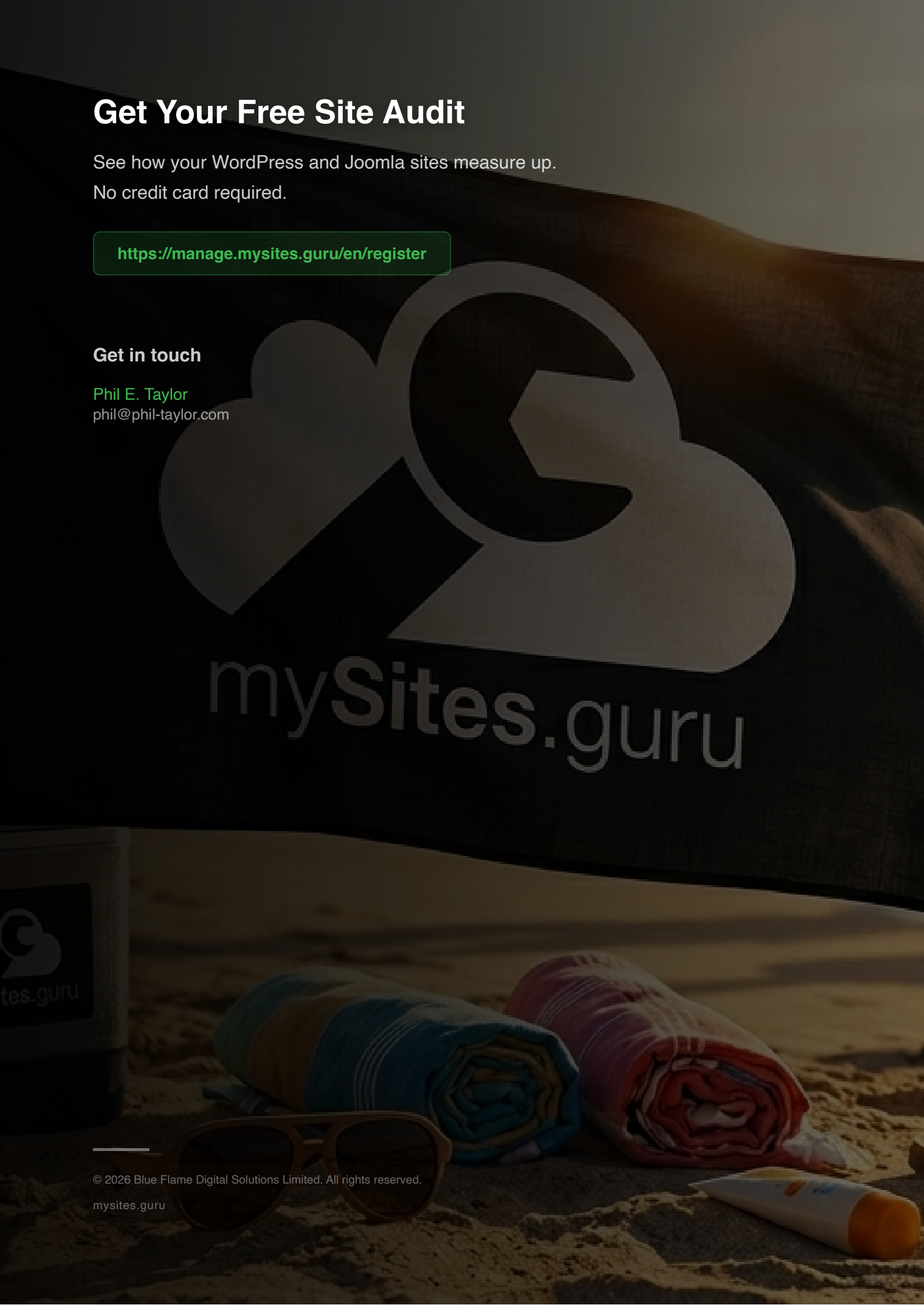
Yes. This is the first of a seasonal series, so the next one covers autumn 2026. Subscribers do not have to wait for it, because everything in these posts appears in the dashboard changelog as it ships. The seasonal post is a summary written for people who would rather read the story once than follow it a line at a time.

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