SQL Injection and a Captcha Bypass in the SP Page Builder Joomla Extension, found by mySites.guru

mySites.guru found an Author-level SQL injection and an unauthenticated captcha bypass in the SP Page Builder Joomla extension, both fixed in 6.9.1.

Phil E. Taylor | 14 September 2026

SP Page Builder is JoomShaper's drag-and-drop page builder for Joomla, one of the most widely installed page builders in the ecosystem. We have reported issues in it before: the June 2026 unauthenticated icon-upload zero-day fixed in 6.6.2, four flaws including a pre-auth SQL injection and an open mail relay fixed in 6.7.1, and a pre-authentication remote code execution fixed in 6.8.0. This round is the fourth, and it found five more, reported to JoomShaper on the day 6.9.0 shipped and all fixed in SP Page Builder **6.9.1**.

The two that matter most to you are a **blind SQL injection an ordinary Author can use to read your entire database**, and an **unauthenticated captcha bypass** that turns your forms back into open spam and relay targets. If you run SP Page Builder on any Joomla site, update to 6.9.1 now. Sites still on Joomla 3 cannot install it and need the separate patch described further down. If you manage more than a handful of sites, read on for how to find every affected one at once.

TL;DR

- mySites.guru found five security issues in SP Page Builder 6.9.0 and reported them privately to JoomShaper the same day the version shipped
- **Author-level blind SQL injection (High).** The com_content integration plugin reads one value out of the article-save request without an integer cast, one line below a cast that is present, and concatenates it into a query. Any account that can save an article, an Author by default, can read the whole database one character at a time, the Super User password hash included
- **Unauthenticated captcha bypass (Medium, understated).** The form addons throw away the real captcha result whenever the request claims the form is being rendered inside a module, so an anonymous visitor defeats reCAPTCHA on the contact form, the opt-in form and the form builder alike. Those three addons ship only in SP Page Builder Pro, so this one does not reach the free Lite edition
- Three more: an **Editor-level file rename** that could reach outside the web root, an **Editor-level Joomla menu takeover**, and an **Author-level file write** into the

web root

- **Update to SP Page Builder 6.9.1 immediately**
- Reported privately on 8 September 2026, all five fixed in **6.9.1**. We re-tested the released package to confirm the fixes hold
- mySites.guru already flags every connected Joomla site still running a vulnerable version

> **We fix first and publish second**
>
> mySites.guru discovered these issues and reported them to JoomShaper 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.

The worst one: an Author reads your whole database

SP Page Builder integrates with Joomla articles through a content plugin. When an article is saved, that plugin reads a value from the submitted form and uses it to look up the matching page-builder layout. The value on the line above is cast to an integer. This one is not. It is concatenated straight into the `WHERE` clause of a database query, so an attacker who can trigger an article save controls part of the SQL. On a default Joomla site the account type that can save an article through the ordinary front-end submission form is an **Author**, the lowest-trust authenticated role there is, and on any site that allows self-registration an attacker can create that account for themselves.

We proved it on a test site. The injection is blind, so nothing is echoed back, 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. Using that as a timing oracle we read the Super User's stored password hash out one character at a time. That is full read access to the entire database, from an account that can do nothing more than submit an article.

7.1
CVSS 4.0

HIGH mySites.guru assessment · CVE-2026-78375

An Author account, the lowest authenticated role on a default Joomla site and one an attacker can often self-register, reads the entire database through a blind time-based injection: every user record, every session, and the Super User password hash. The one precondition is that SP Page Builder's com_content integration plugin is enabled, which it is on any site using the builder inside articles.

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

Author account | Blind SQL injection | Full database read | Password hashes exposed

The captcha check that does not run

The second finding scores lower and is in some ways the more interesting one, because it needed no account at all. On an unpatched site it is the only one of the five an anonymous attacker can reach. SP Page Builder Pro ships three form addons: the contact form, the opt-in form, and the form builder. Each verifies its captcha in a public AJAX handler that anyone on the internet can call. All three are Pro features, so the free Lite edition was never exposed to this one.

There were two separate ways past that handler, and they are worth keeping apart because they have different histories.

Route one: declare the form is in a module

The handler reads a value called `view_type` straight from the request, and when that value says the form is being rendered inside a module, the code throws away the real captcha result and replaces it with a check of whether the submitted string is simply non-empty:

```
$res = Factory::getApplication()->triggerEvent('onCheckAnswer', [$gcaptcha
if ($view_type == 'module') {
    $res = ($gcaptcha != null || strlen($gcaptcha) != 0) ? [true] : [false
}
```

The first line asks Google whether the reCAPTCHA token is valid. The second line overwrites that answer with “did they type anything at all”. Because `view_type` comes from the request and nothing checks it against reality, an attacker just declares `view_type=module` and the captcha is gone. We confirmed it against a form configured for reCAPTCHA: the exact same junk token was rejected as a normal page submission and accepted once we flipped that one field, then reached the mailing-platform submission behind the form.

That shortcut was present in all three form addons, in identical form, down to the comment above it.

6.9
CVSS 4.0

MEDIUM **mySites.guru assessment · CVE-2026-79701**

Scored Medium because nothing on the Joomla site itself changes, which understates the real cost. An anonymous visitor defeats the captcha the site owner configured, so every SP Page Builder Pro form becomes an open target for spam, list poisoning and mail sent from the site's own identity, on a site whose owner believes the forms are protected.

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

No login needed · Exploitable over the internet · Captcha not verified

Route two: the captcha that grades its own homework

The second route is the one JoomShaper’s changelog describes, and it has the longer history. SP Page Builder’s built-in question captcha asks the visitor something simple

and checks the answer. In the opt-in form, that check read:

```
} else if ($captcha_type == 'default' && md5($captcha_question) != $captch
```

The question, the answer and the captcha type all came out of the submitted request. Both sides of that comparison belong to the attacker, so posting any question, its own MD5, and `captcha_type=default` passes every time. Because the type came from the request too, a form the site owner had configured for reCAPTCHA could be downgraded to the question captcha on the way in, with nothing on the page to show it.

We had seen this pattern before. Reporting the July mail relay we noted in passing that the contact form's question captcha compared two attacker-supplied values and so verified nothing. That was context for the relay finding rather than a finding of its own, and no CVE covers it. JoomShaper did fix it, in the contact form and in the form builder, and that fix shipped in 6.9.0 with a comment above it reading "Read the expected answer from the stored addon, never from the request."

The opt-in form, the third member of the same family, sitting in the same directory and running the same code, received neither the comment nor the fix. That untouched line is what we reported on 8 September, in the very release that had just repaired its two siblings.

6.9.1 closes both routes in all three addons at once. The captcha type, the expected answer and whether a captcha is required at all are now read from the stored addon, and the captcha plugin's answer is the one that counts, in every render context. The changelog credits only the opt-in form, which undersells the work: the module shortcut is gone from the contact form and the form builder too.

The other three

Reported and fixed in the same 6.9.1 release, all three needing a low-trust logged-in account rather than an anonymous visitor:

Finding	Who can reach it	What it does
Media file rename outside the web root	Editor	The rename endpoint took a target path from the request without confining it to the media folders, so a chosen file could be renamed to a path that climbed out of the web root. Renaming the wrong core file takes the site down.
Joomla menu takeover	Editor	The “add to menu” action called Joomla’s menu-item model directly, skipping the com_menus permission check, so an Editor could create menu items or overwrite an existing one, the site’s home item included.
File write into the web root	Author	The upload endpoint accepted a destination folder from the request without confining it, letting an Author write an uploaded file into directories across the web root rather than only the dated media folder.

6.9.1 adds a real permission check to the menu action, and confines both media paths to the configured media folders, rejecting any attempt to climb above them.

All five findings at a glance, against the six CVE numbers JoomShaper published in the 6.9.1 changelog. Six rather than five because the captcha bypass was split into one record per route, which is the right call: they are separate defects with separate histories. The scores are mySites.guru’s own assessments from the mechanics, with the two headline findings scored in full above.

CVE	Finding	Who	Editions	Our CVSS 4.0
CVE-2026-78375	Blind SQL injection, full database read	Author	Pro and Lite	7.1 High

CVE	Finding	Who	Editions	Our CVSS 4.0
CVE-2026-79700	Captcha bypass, opt-in form, settings taken from the request	Anonymous	Pro only	6.9 Medium
CVE-2026-79701	Captcha bypass, all three form addons rendered in a module	Anonymous	Pro only	6.9 Medium
CVE-2026-81564	Media file rename reaching outside the web root	Editor	Pro and Lite	7.2 High
CVE-2026-81565	Joomla menu create and overwrite without com_menus rights	Editor	Pro and Lite	7.1 High
CVE-2026-81566	File write into the web root media tree	Author	Pro and Lite	5.3 Medium

These CVE records are not published yet

The six identifiers above come from JoomShaper's own 6.9.1 changelog, and so does the mapping from each number to each fix. None of the records was published when we checked, so there is no official CVSS score, no affected-version range and no credit line to read yet, and scanners that work from published CVE data cannot see any of this. Treat our scores as ours until the records appear.

The pattern, four rounds in

This is the fourth consecutive round of findings we have reported in SP Page Builder, and each has told the same story: the fix reaches the exact file that was reported, and not the siblings running the same code. The 6.8.0 remote code execution sat in the method directly below the one hardened in 6.7.1. The question captcha above had been repaired in two of the three form addons in 6.9.0, with the corrected code sitting a few files away from the third as a template for the fix that was never applied.

The rename finding turns out to be a sharper version of the same problem, and JoomShaper documented it themselves. The comment they shipped above the fixed

line in 6.9.1 records that an internal commit on 7 September had weakened the check from an AND to an OR, reopening the arbitrary file rename and undoing an earlier fix for the same issue. We reported it the next day, not knowing any of that. A bug they had already closed once was live again for roughly twenty-four hours before an outsider found it.

Two things are worth saying about that. Writing it down in the shipped source, naming the commit and the regression, is more candid than most vendors manage, and the same comment says a regression guard now exists to stop it happening a third time. And it makes the case better than we could: a security fix can be undone as easily as it can be missed.

None of this makes SP Page Builder unusually bad. It is a large, capable, heavily used component, and the vendor fixes what we send them, quickly. The lesson is one every developer can borrow: when you fix a security bug, grep for the pattern across the whole codebase, then write the test that fails if anyone takes the fix back out.

Why keeping SP Page Builder patched matters

SP Page Builder is a mainstream choice, not a niche add-on. Across the Joomla sites mySites.guru actively monitors, **roughly one in four, about 23%, run it**. Only YOOtheme Pro is on more, and between them those two account for most of the Joomla page-builder market we can see: the next most common builder after them appears on well under a tenth as many sites. A flaw in a component with that kind of reach exposes a large slice of the whole Joomla web at once, and attackers know exactly which component to point a scanner at.

The version spread is the encouraging half of the picture. About 72% of the SP Page Builder installs we monitor were already on 6.8.0 or 6.9.0, the two most recent releases before this fix, so most site owners do take these updates and 6.9.1 will reach them through the normal updater.

The tail is where it gets difficult. Roughly a fifth are on SP Page Builder 5.x or older, and 86% of those sites are still running Joomla 3, where the 6.x package cannot install at

all. Taken together, about **one in five SP Page Builder installs we monitor sits on a Joomla 3 site**, with no route to 6.9.1 whatsoever.

That reach is also why the “needs an Author account” or “needs the content plugin enabled” caveats on some of these findings matter less than they sound. On a base this large there are always sites that allow self-registration, sites that use the builder inside articles, and sites with a stale low-trust account no one has thought about in years. A precondition that trims the exposure on one site does nothing to the total across tens of thousands.

Joomla 3 sites need a different package

JoomShaper released a third package on the same day: the Joomla 3 Security Patch for SP Page Builder, version 1.0.2. It back-ports four of the five fixes to the Joomla 3 branch. The captcha work is not part of it.

The bigger limitation is who can install it. The patch checks the installed version and will not run on anything except SP Page Builder 5.6.1 exactly. Across the Joomla 3 sites we monitor that run SP Page Builder, **only about 3% are on 5.6.1**. For the other 97%, this patch will not install, and neither will 6.9.1.

There is a second problem, and it is the one we had already asked JoomShaper to avoid. The patch installs as a Joomla file package: it overwrites files in place and leaves the component’s own version reading 5.6.1, exactly as before. To any updater, and to any scanner that works from version numbers, a Joomla 3 site that has applied it looks identical to one that has not. That is also why our own vulnerability rule for this round stops at the 6.x line rather than flagging 5.6.1: a site that did everything right would have no way to clear the warning.

We have written this paragraph before. JoomShaper’s third Joomla 3 security patch for Helix Ultimate reused the version string `2.1.4-j3sec` for the same reason, leaving Joomla 3 sites unable to tell whether they held it. The same objection is why we sent back their first fix build for this round on 8 September. A security patch you cannot detect is one you cannot manage across more than a handful of sites.

How we handle it instead

Version numbers being useless here is why mySites.guru does not use them for these packages. For all three of JoomShaper's Joomla 3 security patches, Helix Ultimate and Helix3 as well as SP Page Builder, we look inside the installed files for a string that only exists in a given release of the patch. That answers two separate questions that a version number cannot: whether any patch has been applied at all, and whether the one applied is the current release. As of today that check knows about SP Page Builder patch 1.0.2, so a Joomla 3 site still on 1.0.1 reports as outdated instead of showing a green tick it has not earned.

We also host the vendor's own package, pinned by SHA-256 so what reaches the site is the file JoomShaper published rather than a copy of it, and install it through Joomla's native installer from the mySites.guru UI in one click, with a revert. Using the vendor's whole package matters: the patched files call methods that only exist in other patched files, so splicing one file at a time produces a site that fatals.

None of that helps the SP Page Builder 3.8.x sites, which are the largest group on Joomla 3. The vendor's package installs onto 5.6.1 and nothing else, so those sites get no official fix at all, and there is no version of this that ends with a comfortable answer for them. Joomla 3 reached end of life in August 2023 and the extensions built for it are following it out. The fix there is the migration you have been putting off rather than any patch.

In the meantime, the findings that need a logged-in account are the ones to think about hardest on those sites: audit who holds Author and Editor, and turn off self-registration if nothing depends on it.

Every SP Page Builder flaw we have reported

Four rounds in five months, each found by reading the code or the access logs, each reported privately to JoomShaper before any public detail. In order:

June 2026, fixed in 6.6.2

Found in live exploitation. CVE-2026-48908, CVSS 10.0, added to the CISA Known Exploited Vulnerabilities catalog.

- `asset.uploadCustomIcon` **unauthenticated upload to remote code execution.** No login, no file-type check: an anonymous visitor could upload and run a PHP web shell. We traced it in real access logs being used to plant hidden Super User accounts, so we treated it as a zero day and published the same day. Every version up to 6.6.1 was affected. Full write-up.

July 2026, fixed in 6.7.1

Reported privately in an audit of 6.7.0, pre-release build shared 23 July, fixed on 27 July. CVE-2026-65766, CVE-2026-65877, CVE-2026-65878, CVE-2026-65879, credited to Phil Taylor.

- **Pre-authentication SQL injection** in the Dynamic Content endpoint, reachable with only the CSRF token Joomla hands every anonymous visitor, reading the whole database.
- **Unauthenticated open mail relay** in the contact-form addons, because every copy of the extension shipped the same hardcoded secret that was supposed to protect the recipient address.
- **Author-level SQL injection** in the media manager search.
- **Author-level arbitrary file delete.**

Full write-up.

August 2026, fixed in 6.8.0

Reported 27 July, fixed on 12 August, sixteen days after 6.7.1. CVE-2026-67285, CVSS 9.3 Critical, and CVE-2026-67286, Medium, credited to Phil Taylor.

- **Unauthenticated PHP file inclusion** in the Dynamic Content “load more” endpoint: pre-authentication remote code execution, sitting in the method directly below the one 6.7.1 had just hardened, so the previous fix release was itself vulnerable.

- **Unauthenticated arbitrary directory creation and file write** on the same endpoint.

Full write-up.

September 2026, fixed in 6.9.1

Reported 8 September, the day 6.9.0 shipped, fixed in 6.9.1 on 14 September. Six CVE numbers, CVE-2026-78375, CVE-2026-79700, CVE-2026-79701, CVE-2026-81564, CVE-2026-81565 and CVE-2026-81566, none published yet.

- The five issues in this post: the **Author-level blind SQL injection** reading the whole database, the **unauthenticated captcha bypass** on the Pro form addons, the **Editor-level file rename** reaching outside the web root, the **Editor-level Joomla menu takeover**, and the **Author-level web-root file write**.

JoomShaper's 6.9.1 changelog describes all six fixes in plain language and, a few hours after release, added the CVE number against each one. Both are real improvements on the one-line security notes of earlier releases, and together they let any site owner judge the urgency without waiting for us. What the changelog does not say is where the findings came from. That is consistent across our rounds with this vendor: the CVE records for the July and August findings credit Phil Taylor of mySites.guru, and JoomShaper's own changelogs for those same releases did not. Until these six records are published with their credit lines, the only public account of who found them is this page.

How mySites.guru helps

You do not have to audit each site by hand. mySites.guru tracks the exact version of every extension on every Joomla site it monitors, and flags any site running a version we know to be vulnerable, this one included. Instead of opening each site to check whether it is on SP Page Builder 6.9.1 yet, you get a single list of the ones that are not, and you can update them from the same screen.

That is the whole point of watching a portfolio of client sites in one place: a flaw like this stops being a site-by-site scramble and becomes one filtered list and a batch update.

Field	Detail
Component	SP Page Builder for Joomla (`com_sppagebuilder`), including the com_content integration plugin
Vendor	JoomShaper (joomshaper.com)
Type	Author-level blind SQL injection (CWE-89); unauthenticated captcha bypass (CWE-287 / CWE-804); missing authorisation and path confinement (CWE-862 / CWE-22)
CVSS 4.0	mySites.guru assessments, given per finding above. The published CNA records are the authority once they appear
CVE	CVE-2026-78375, CVE-2026-79700, CVE-2026-79701, CVE-2026-81564, CVE-2026-81565, CVE-2026-81566. Named in JoomShaper's 6.9.1 changelog; none published at the time of writing
Impact	Full database read from an Author account; anonymous captcha bypass on all three Pro form addons; Editor-level file rename and menu takeover; Author-level web-root file write
Finder	Phil Taylor, mySites.guru
Affected versions	SP Page Builder 6.9.0 and earlier. Four of the five affect Pro and the free Lite edition alike; the captcha bypass is Pro-only
Fixed in	SP Page Builder 6.9.1 (Pro and Lite), released 14 September 2026. Joomla 3 Security Patch 1.0.2 back-ports four of the five, and installs only over SP Page Builder 5.6.1
Reported	8 September 2026, 12:47 BST, privately to JoomShaper with the Joomla security team copied in
Acknowledged	8 September 2026. A first fix build arrived the same afternoon and was rejected; a second on 9 September was accepted
Fix verified by mySites.guru	Against the released 6.9.1 Pro package, 14 September 2026

Timeline

8 September 2026

Reported privately, the day 6.9.0 shipped

Five issues, reported to JoomShaper with the Joomla security team copied in: an Author-level blind SQL injection reading the whole database, an unauthenticated captcha bypass on the form addons, an Editor-level file rename reaching outside the web root, an Editor-level Joomla menu takeover, and an Author-level web-root file write. All five confirmed by live exploitation on a Joomla 5 test site.

8 September 2026

JoomShaper acknowledged and sent a first fix build, which we rejected

Support confirmed within the hour and the development team returned a package the same afternoon. We retested it and sent it back for two reasons. It closed four of the five but left the captcha reachable by a second route, which we then named in all three form addons. And its manifest still read 6.9.0, identical to the vulnerable release, so Joomla's updater would never have offered it and no scanner could tell a patched site from an unpatched one.

9 September 2026

A second build, which we accepted

JoomShaper sent a revised package the next morning. We retested it and replied that it was much improved and could be released.

14 September 2026

SP Page Builder 6.9.1 ships, and we verify it

Pro and Lite both released as 6.9.1, alongside a separate Joomla 3 Security Patch. We read the released Pro package and confirmed all five fixes are present, that the manifests really declare 6.9.1, and that the captcha route is closed in all three form addons rather than only the one the changelog names.

14 September 2026

Six CVE identifiers appear in the vendor changelog

Later the same day JoomShaper added CVE numbers to the 6.9.1 changelog: CVE-2026-78375, CVE-2026-79700, CVE-2026-79701, CVE-2026-81564, CVE-2026-81565 and CVE-2026-81566. Six rather than five, because the captcha bypass was split into one record

per route. None of the records is published yet, so there is no public CVSS score, affected range or credit line to read.

Further Reading

- Our previous SP Page Builder round: SQL injection and mail relay - fixed in 6.7.1, and the round where we first noted the captcha that verifies nothing.
- JoomShaper's SP Page Builder download page - the 6.9.1 changelog, which describes all five fixes in plain language.
- The pre-auth remote code execution we found in 6.7.1 - a flaw in the method directly below the one the previous fix hardened, fixed in 6.8.0.
- The June 2026 SP Page Builder icon-upload zero-day - an earlier, separate flaw in the same component, exploited in the wild and fixed in 6.6.2.
- Why AJAX endpoints are a CMS security blind spot - the recurring public-endpoint pattern behind flaws like these.
- CWE-89: SQL Injection and CWE-804: Guessable CAPTCHA - the standard references for these weakness classes.
- JoomShaper - the vendor's site, where SP Page Builder 6.9.1 is available.

Frequently Asked Questions

What did mySites.guru find in SP Page Builder 6.9.0?

Five separate issues, all confirmed by exploiting them on a Joomla 5 test site. The worst is a blind SQL injection reachable by anyone who can save an article, which on a default Joomla site is an ordinary Author. It reads the whole database one character at a time, password hashes included. Alongside it: an unauthenticated captcha bypass on the form addons, which are a Pro-only feature, an Editor-level file rename that could reach outside the web root, an Editor-level Joomla menu takeover, and an Author-level file write into the web root. All five are fixed in SP Page Builder 6.9.1.

Which SP Page Builder versions are affected?

SP Page Builder 6.9.0 and earlier. Four of the five reach both the Pro and the free Lite edition. The captcha bypass is Pro-only, because the three form addons it affects ship only in Pro. Everything is fixed in SP Page Builder 6.9.1, released on 14 September 2026, which JoomShaper links to six CVE numbers. If you run any earlier version, assume you are affected and update now. Joomla 3 sites cannot install 6.9.1 at all. JoomShaper published a separate Joomla 3 Security Patch, version 1.0.2, which back-ports four of the five fixes, but it installs only over SP Page Builder 5.6.1, which is about 3% of the Joomla 3 sites we monitor. mySites.guru detects that patch by its file contents rather than a version number, and can apply the vendor's own package in one click.

Is the SQL injection exploitable without a login?

No. It needs an account that can save an article, which is an Author on a default Joomla site, and it needs SP Page Builder's com_content integration plugin enabled, which it is on any site that uses SP Page Builder inside articles. That still puts the whole database within reach of the lowest-trust account type on the site, and on any site that allows self-registration an attacker can create that account themselves. The captcha bypass, by contrast, needs no account at all.

How do I know if my sites are affected?

If you run SP Page Builder on a version earlier than 6.9.1, assume you are affected and update. mySites.guru flags every connected Joomla site running a vulnerable version automatically, so you get told which sites need attention rather than checking each one by hand.

Is this the same as the captcha issue you reported before?

It is the same class of bug in a sibling file. While reporting the July mail relay we noted in passing that SP Page Builder's built-in question captcha compared two values that both came from the attacker, so it verified nothing. JoomShaper fixed that pattern in the contact form and the form builder in 6.9.0. The opt-in form, the third addon of the same family, never received it, and that untouched line is what we reported on 8 September. A second and separate route affected all three addons: the real captcha result was discarded whenever the request claimed the form was rendered inside a module. Both routes are closed in 6.9.1.

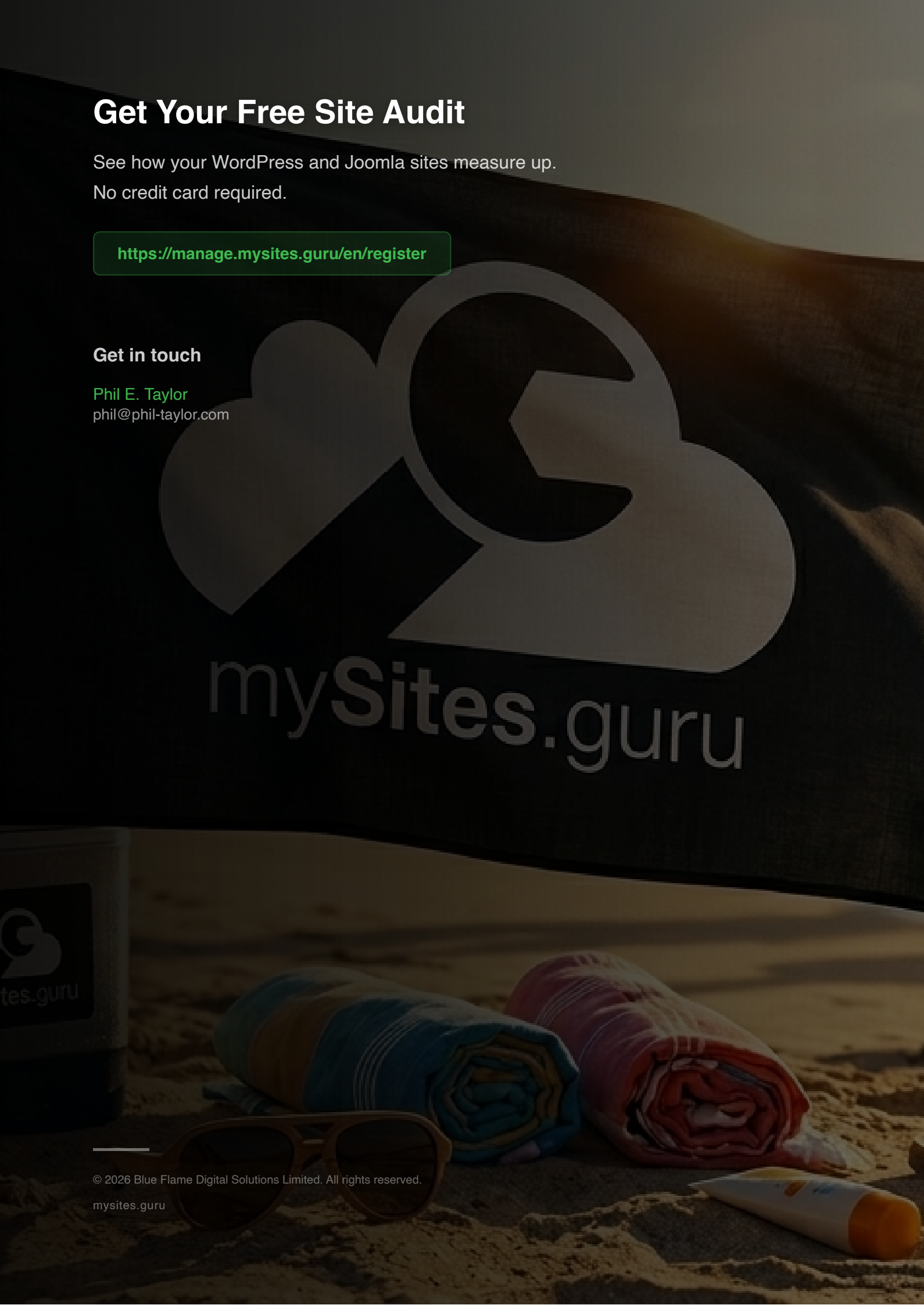
AI MODIFIED Written and edited by a human, with AI assistance. Our approach to AI

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