mySites.guru

Pre-Authentication SQL Injection and Mail Relay in SP Page Builder found by mySites.guru

mySites.guru found four vulnerabilities in SP Page Builder for Joomla: a pre-auth SQL injection, an unauthenticated mail relay, and two more. Fixed in 6.7.1.

Phil E. Taylor | 27 July 2026

Active Joomla Extension security alerts: Nineteen and counting this month • Helix3 defacements • JCE • EasyStore • Regular Labs • Gridbox

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 that was being exploited in the wild and fixed in 6.6.2. During a later audit of SP Page Builder 6.7.0, **mySites.guru found four further vulnerabilities, and reported them to JoomShaper before disclosing anything publicly.** JoomShaper closed all four in SP Page Builder **6.7.1**.

If you run SP Page Builder on any Joomla site, update to 6.7.1 now. 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 **four vulnerabilities** in SP Page Builder 6.7.0 and reported them to JoomShaper
- **Pre-authentication SQL injection (CVSS 4.0 8.7, High).** The Dynamic Content endpoint placed a request value straight into the database query's `ORDER BY`. It is protected only by a CSRF token, which Joomla hands to every anonymous visitor, so it is effectively pre-auth. An attacker could **read the entire database**, password hashes included
- **Unauthenticated mail relay (CVSS 4.0 6.9, Medium).** The contact-form addons protected the recipient address with a secret that was **hardcoded identically into every copy of the extension**. Because the secret was public in the shipped source, an attacker could forge it and send email to any recipient with a spoofed sender, from your domain and mail server, an open spam and phishing relay
- **Authenticated SQL injection (CVSS 4.0 7.1, High).** The media manager's search and date filters placed request input into the database query unescaped. Reachable by a low-privilege author

- **Authenticated arbitrary file delete (CVSS 4.0 7.2, High).** A media action deleted a file at a request-supplied path with no traversal guard, so a low-privilege author could delete `configuration.php` or a protective `.htaccess`
- **Update to SP Page Builder 6.7.1 immediately**
- Reported privately, fixed in **6.7.1** on 27 July 2026. The Joomla CNA assigned four CVEs the same day: **CVE-2026-65766, CVE-2026-65877, CVE-2026-65878 and CVE-2026-65879**
- mySites.guru already flags every connected Joomla site still running a vulnerable version

> mySites.guru discovered these issues and reported them to JoomShaper before publishing details. We withheld the exact requests and any proof-of-concept until a fix was available and site owners had a reasonable window to update. This is how we handle every vulnerability we find: fix first, publish second.

The worst one: an anonymous request that reads the database

SP Page Builder's Dynamic Content feature renders lists of content, articles, tags and custom collections, through a front-end endpoint. For the tags source, it built the query's sort clause by pasting a `direction` value taken **raw from the request body** onto the end of `ORDER BY title` (`dynamic_content.php:232`, with the same pattern duplicated at `CollectionData.php:2004`). A sort direction is one of the places you cannot safely quote a value, so it has to be restricted to `ASC` or `DESC`. This path did not restrict it.

The only thing standing in front of the endpoint is a CSRF token check, and that is not the barrier it looks like. Joomla issues a valid token to **every** visitor, including anonymous ones, the moment they load any page. A scripted attacker simply fetches a token and sends it back, so in practical terms this is a pre-authentication SQL injection:

an anonymous attacker could read any table in the Joomla database, from user accounts and password hashes to the site secret and every stored record.

We confirmed it on our own SP Page Builder test install with a time-based proof: a crafted `direction` value that made the database pause for a measurable few seconds against an instant baseline, while a normal request returned the expected tag data, which together show the injected code ran inside a real query. We did not extract real data. The fix restricts the direction to `ASC` or `DESC` before it reaches the query, in both places, and puts a permission check in front of the endpoint so an anonymous visitor cannot reach it at all.

> A database read leaves your site looking untouched: no file changes, no new admin user, nothing for an integrity scanner to catch. If a vulnerable version was ever live, treat the database as potentially copied, rotate the Joomla secret and any stored API keys, and assume password hashes are known.

The one that surprised us: an open mail relay from a shared secret

This is the finding worth dwelling on, because the root cause is a design decision rather than a slip. SP Page Builder's contact-form addons, `ajax_contact` and `form_builder`, let a site owner set where form submissions are emailed. To stop a visitor tampering with that recipient, the addon signs it with a secret and checks the signature on submission. Sound idea. The problem is the secret: it is a single string **hardcoded into the addon source (`site.php:24`), identical in every copy of SP Page Builder ever shipped**.

A secret that ships in the product is not a secret. Anyone with a copy of the extension, which is anyone, can read it and forge a valid signature offline. With that, an attacker could set the form's recipient to any address they liked, and its sender to anything they liked, and make the site send arbitrary email. Two smaller weaknesses removed the remaining friction: the built-in "default" captcha compared two values that both came

from the attacker (`site.php:460`), so it verified nothing, and the CSRF check switched itself off whenever Joomla page caching was enabled (`site.php:257`), a common production setting.

The upshot is an unauthenticated open mail relay. Any SP Page Builder site with a contact form on a published page could be made to send email to any recipient, with a spoofed sender, **from the site's own domain and mail server**. That is a spam and phishing platform running on your domain's reputation, and the fastest way to get your legitimate mail blacklisted. We proved it on our test install: an anonymous request delivered a message to an address of our choosing with a spoofed sender, and the server reported success. The correct fix, which the update makes, is to derive the signature from the site's **own** secret, unique per install, rather than a constant shared by every copy.

> Hardcoding a secret into shipped source is a recurring class of bug (CWE-798). The moment the same key protects every install, it protects none of them. Joomla already gives each site a unique secret for exactly this purpose; that is what per-site signing should use.

The two that need a low-privilege login

The remaining two issues need an account, but only a low-privilege one: a Joomla user who can edit their own page-builder content, the sort of author account many sites hand out freely. Neither should be dismissed on that basis.

The **media manager's JSON view** built its search query by pasting the `search` and `date` request values directly into the SQL with no escaping (`media.php` , in `getDateFilters()` and `getTotalMedia()`), a SQL injection reachable by that low-privilege author, and with no CSRF token on the view. The **media delete action** removed a file at a path taken from the request, with only cosmetic filtering and none of the traversal guard the sibling delete paths use (`media.php:804`), so an author holding only the create permission could delete any file in the web root, `configuration.php` or

a protective `.htaccess` included. Deleting the wrong file can break a site or strip a defence ahead of a further attack. The fixes add the missing input validation and the missing path boundary check.

Which versions are affected?

SP Page Builder **6.7.0**, the current release at the time of disclosure, and **every earlier version** are affected by this set of issues. JoomShaper fixed them in SP Page Builder **6.7.1**. This is separate from the June 2026 icon-upload flaw fixed in 6.6.2: you want to be on 6.6.2 or later for that one, and 6.7.1 or later for these.

> If you run any version of SP Page Builder earlier than 6.7.1, assume your site is affected and update now. The critical SQL injection and the mail relay both need no real login, so if the site is online, the endpoints are reachable.

How do you update SP Page Builder safely?

1. **Take a backup first.** Before any extension update on a production Joomla site, back up the database and files. If you use mySites.guru, trigger a snapshot or a full backup first.
2. **Update through Joomla's Extensions manager, or in bulk from mySites.guru.** On a single site, open the Joomla administrator, go to System, then Update, then Extensions, and let Joomla pull SP Page Builder 6.7.1. If you manage more than one site, use the mySites.guru mass update feature to upgrade SP Page Builder across every affected site from one dashboard.
3. **Confirm the version.** After updating, check SP Page Builder reports 6.7.1 or later.
4. **Clear caches.** Clear Joomla's cache and any CDN or page cache.

Updating closes the door. It does not undo any data an attacker may already have read through the SQL injection, so if you handle sensitive data and were on a vulnerable version for a while, treat credentials and exposed data as potentially known.

How do I find every SP Page Builder site I manage?

Up to about ten sites, you can log in to each Joomla admin and check. Past that, you need a single view. mySites.guru keeps a live inventory of every extension, template and framework on every Joomla and WordPress site in your account. You search for SP Page Builder once and get back every connected site running it, the version each one is on, and whether an update is available.

View every SP Page Builder install across your sites

Open your Extension Inventory

Search for SP Page Builder across every connected Joomla site and filter for anything earlier than 6.7.1. Not a subscriber? Sign up free and connect your sites.

Why page builders keep producing this

Page builders make attractive targets for the same reason they are useful: they render content through front-end endpoints that anonymous visitors are meant to reach. An element that loads a list of tags, a contact form that accepts a submission, none of it can require a login, because the whole point is that visitors use it. Every one of those public endpoints is attack surface, and when the code behind them trusts request input, an anonymous visitor becomes an anonymous attacker.

We have seen the same shape across the ecosystem this year, from PageBuilder CK to Quix and the wider month of Joomla disclosures. Page builders are worth using. The ones that accept input from anonymous visitors simply need updating the moment a fix exists, which makes these updates security-critical rather than feature maintenance.

On the engineering, JoomShaper did the right things. They shared a pre-release build for us to verify, fixed all four issues, hardened a couple of related weaknesses we flagged while checking that build, and told their users to update in a public security notice covering both the Pro and free editions.

On the disclosure, once again they gave mySites.guru no acknowledgement. They shared that pre-release build on 23 July, then shipped the final 6.7.1 without telling us it was going out. Their changelog also plays the severity down: a pre-authentication SQL injection that hands an anonymous visitor your entire database is written up as "improved input validation and access control", and an unauthenticated open mail relay as "improved submission verification". A site owner reading that has no way to tell how serious either was. We saw the same pattern from the same vendor days earlier with EasyStore, where three serious flaws were closed as routine changelog lines with no advisory and no credit.

Stay ahead of the next one

There will be another, because Joomla runs on thousands of third-party extensions and the ones that accept input from anonymous visitors keep producing bugs like these. The hard part is never the update itself. It is knowing a fix exists, knowing which of your sites are affected, and getting to them before an attacker does.

That is the job mySites.guru does for you. It keeps a live inventory of every extension on every Joomla and WordPress site in your account, flags the ones with a known vulnerability, and lets you push the update to all of them from one screen.

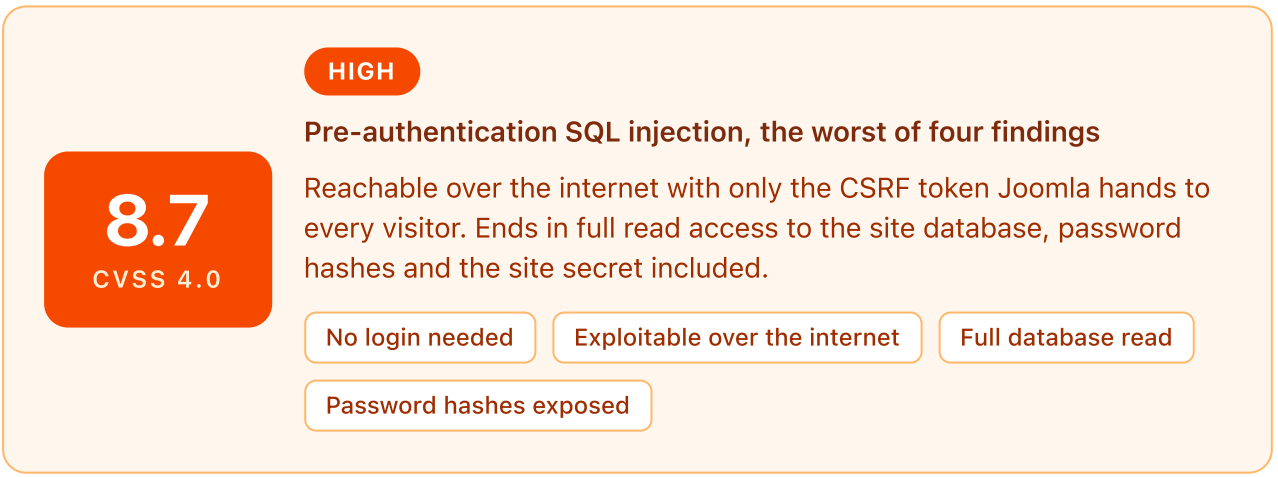
Want the alerts and the tooling to act on them? Start with a free audit on one site and see your full extension inventory, or sign up for mySites.guru to get vulnerability alerts and one-click updates across every site you manage.

Disclosure and severity

The worst finding is a SQL injection (CWE-89) reachable by an anonymous visitor over the network, gated only by a CSRF token that Joomla issues to everyone. The mail relay stems from a hardcoded, product-wide secret (CWE-798) and yields unauthenticated arbitrary mail sending with sender spoofing. The remaining two, a media-manager SQL injection and an arbitrary file delete via path traversal (CWE-22), need a low-privilege authenticated author.

The Joomla CNA assigned four CVE IDs for these findings on 27 July 2026, the day 6.7.1 shipped: CVE-2026-65766, CVE-2026-65877, CVE-2026-65878 and CVE-2026-65879. The records are reserved rather than published, so each one currently carries no public description and no CNA score of its own, and the CNA has not stated which ID covers which finding. We will add that mapping here once the records publish.

We score every issue under CVSS 4.0. The pre-authentication SQL injection comes out at **8.7, High**, the top of the High band, where CVSS 4.0 caps a single maximal impact reached with no privileges. A full-database read is a total loss of confidentiality regardless of where the number falls.



Each finding, scored under CVSS 4.0:

Finding	Vector (`CVSS:4.0/...`)	Score	Severity
Pre-authentication SQL injection (full DB read)	`AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N`	8.7	High

Finding	Vector (`CVSS:4.0/...`)	Score	Severity
Authenticated arbitrary file delete	`AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N`	7.2	High
Authenticated media-manager SQL injection	`AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N`	7.1	High
Unauthenticated mail relay (sender spoofing)	`AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:L/SA:N`	6.9	Medium

CVSS 4.0 scores the mail relay **6.9, Medium**, because the direct impact on the Joomla system is low: it reads and changes nothing on the site itself. That number understates the practical risk, which is phishing sent from your own domain and mail server, and the mail-reputation damage that follows. We treat it as a priority fix regardless.

Field	Detail
Component	SP Page Builder for Joomla (`com_sppagebuilder`)
Vendor	JoomShaper (joomshaper.com)
Type	Pre-auth SQL injection (CWE-89); unauthenticated mail relay via hardcoded secret (CWE-798); authenticated SQL injection (CWE-89); authenticated arbitrary file delete (CWE-22)
CVSS 4.0	8.7 (High) pre-auth SQL injection; 7.2 (High) file delete; 7.1 (High) media SQL injection; 6.9 (Medium) mail relay
CVE	CVE-2026-65766, CVE-2026-65877, CVE-2026-65878 and CVE-2026-65879, assigned via the Joomla CNA on 27 July 2026; records not yet published, so the mapping of each ID to each finding will be added when they publish
Impact	Anonymous read of the whole database including password hashes; unauthenticated arbitrary mail sending with sender spoofing; low-privilege database read and web-root file deletion
Finder	Phil Taylor, mySites.guru

Field	Detail
Affected versions	6.7.0 and all earlier versions
Fixed in	SP Page Builder 6.7.1
Reported	21 July 2026 (privately to JoomShaper)
Acknowledged	22 July 2026 (JoomShaper confirmed receipt, team informed)
Verified	23 July 2026 (mySites.guru confirmed all four fixes in a JoomShaper pre-release build)
Fixed	27 July 2026 (SP Page Builder 6.7.1)
CVE assigned	27 July 2026 (four IDs via the Joomla CNA, records pending publication)

Further Reading

- The June 2026 SP Page Builder icon-upload zero-day - the earlier, separate flaw in the same component, exploited in the wild and fixed in 6.6.2.
- Our Quix Page Builder SQL injection disclosure and the month of Joomla security disclosures - the same class of bug across the ecosystem.
- Why AJAX endpoints are a CMS security blind spot - the recurring public-endpoint pattern behind flaws like these.
- CWE-89: SQL Injection, CWE-798: Use of Hard-coded Credentials and CWE-22: Path Traversal - the canonical references for these weakness classes.
- JoomShaper - the vendor’s site, where SP Page Builder 6.7.1 is available.

Frequently Asked Questions

What are the SP Page Builder vulnerabilities?

mySites.guru found four security issues in SP Page Builder, the page builder for Joomla by JoomShaper. The most serious is a pre-authentication SQL injection in the Dynamic Content endpoint, reachable with only the CSRF token that Joomla hands to every anonymous visitor, which let an attacker read the whole site database. A second flaw turned the contact-form addons into an unauthenticated open mail relay, because every copy of the extension shipped the same hardcoded secret used to protect the recipient address. Two further flaws needed a low-privilege author account: a SQL injection in the media manager's search, and an arbitrary file delete. All four were reported privately to JoomShaper and fixed in SP Page Builder 6.7.1. The Joomla CNA assigned four CVEs on 27 July 2026: CVE-2026-65766, CVE-2026-65877, CVE-2026-65878 and CVE-2026-65879.

Is this the same as the June 2026 SP Page Builder zero-day?

No. This is a separate set of issues we found in a later audit of SP Page Builder 6.7.0. The June 2026 flaw was an unauthenticated file upload in the icon-upload endpoint, actively exploited in the wild and fixed in 6.6.2. These four are different, in different parts of the component, and were reported privately before any public detail. Sites should be on 6.6.2 or later for the June fix and 6.7.1 or later for these.

Which SP Page Builder versions are affected?

SP Page Builder 6.7.0 and earlier are affected by this set of issues. JoomShaper fixed them in SP Page Builder 6.7.1. If you run any earlier version, assume you are affected and update now.

How do I know if my sites are affected?

If you run SP Page Builder on a version earlier than 6.7.1, 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.

What is a mail relay flaw and why does it matter?

A mail relay flaw lets someone send email through your server that they should not be able to. Here, an attacker could make a site with an SP Page Builder contact form send email to any recipient, with a spoofed sender, from your own domain and mail server. That is a ready-made spam and phishing platform running under your domain's reputation, which can

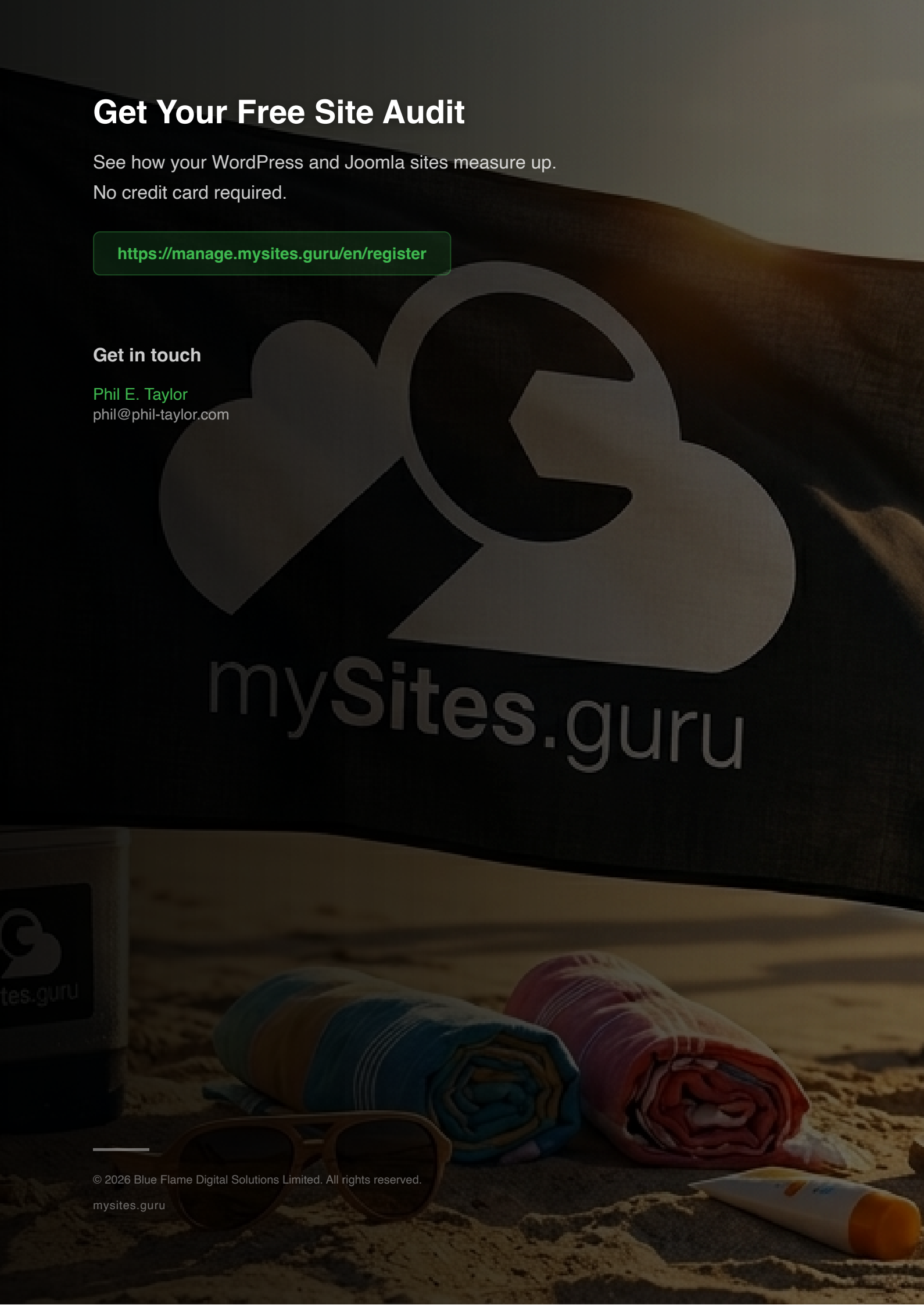
get your legitimate mail blacklisted. It mattered because the secret meant to prevent it was hardcoded identically into every copy of the extension, so it was never really secret.

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