# Unauthenticated SQL Injection in SP Property Finder found by mySites.guru

mySites.guru found an unauthenticated blind SQL injection in JoomShaper's SP Property Finder. Any visitor could read the database. Fixed in 4.1.4.

Phil E. Taylor | 10 September 2026

SP Property Finder is JoomShaper's real-estate listings component for Joomla, used to run property search sites: agents, listings, maps, enquiry forms. During a security audit of SP Property Finder 4.1.3, **mySites.guru found an unauthenticated SQL injection in the public property search, and reported it to JoomShaper before disclosing anything publicly.** JoomShaper closed it in SP Property Finder **4.1.4**.

If you run SP Property Finder on any Joomla site, update to 4.1.4 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 an **unauthenticated blind SQL injection** in SP Property Finder 4.1.3 and reported it to JoomShaper
- **Unauthenticated SQL injection (CVSS 4.0 8.7, High).** The public property search and map views placed several request values straight into the database query with no quoting or integer cast. With no login and no token, an anonymous visitor could **read the entire database**, password hashes and the site secret included
- **Unauthenticated mail relay (CVSS 4.0 6.9, Medium).** The property contact and enquiry forms took the recipient address straight from the request, so an attacker could send email to any address with a spoofed sender, from your domain and mail server, an open spam and phishing relay
- **Update to SP Property Finder 4.1.4 immediately**
- Reported privately, fixed in **4.1.4**. The changelog cites CVE-2026-78082 (SQL injection) and CVE-2026-78083 (contact-form fix); both records are reserved and not yet published
- **A month from report to release, 27 days of it silence.** Acknowledged 11 August, then quiet until we chased on 7 September with the Joomla Security Strike Team copied in; a fixed build followed within 20 hours
- mySites.guru already flags every connected Joomla site still running a vulnerable version

**How we handle what we find**

mySites.guru discovered this issue and reported it 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. Fix first, publish second, every time.

## The worst one: an anonymous request that reads the database

SP Property Finder's whole reason to exist is a public property search. A visitor filters listings by city, price, size, number of bedrooms, postcode, and the component turns those filters into a database query. Most of those filters were handled correctly. A few were not.

The postcode filter is the clearest example. The search model took the `zip` value from the request and pasted it straight onto the end of the query as `a.zip = <value>`, with none of the quoting that the neighbouring `city` and `keyword` filters use (`components/com_spproperty/models/properties.php:166`, with the same pattern in the map view at `models/maps.php:153`). The sort control had the same flaw in its `ORDER BY` clause, where the sort direction was appended raw (`properties.php:190`), and so did the price and size range dropdowns (`properties.php:131` and `:136`). A postcode and a sort direction are ordinary-looking fields, which is exactly why the missing quoting is easy to overlook.

There is no login, no token and no CSRF check in front of any of it. The property search is meant to be used by anonymous visitors, so the endpoint is open by design, and the missing input handling turns that open endpoint into an unauthenticated 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 enquiry.

We confirmed it on our own SP Property Finder test install, two ways. A boolean proof: a crafted postcode that asked the database a true-or-false question about another table (does a user with this ID exist, does this character of the admin password hash match)

changed which listings came back, letting an answer be read out one bit at a time. And a time-based proof: a value that made the database pause for a measurable few seconds against an instant baseline, which shows the injected code ran inside a real query even when nothing is visible on the page. We did not extract any real data beyond confirming the admin username and the first byte of its hash on our own lab box.

> **This one leaves no trace**
>
> 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.

## Read-only, but not harmless

It is worth being precise about what this injection can and cannot do, because the honest answer is more useful than the scary one.

It is a read-only injection. It sits inside a `SELECT` that fetches property listings, and Joomla's database driver does not run stacked queries, so there is no way to turn it into an `INSERT`, `UPDATE` or `DELETE`. An attacker cannot use this bug on its own to add an administrator, change a price, or write a file. That is why we score it High rather than Critical: the impact is a total loss of confidentiality, with integrity and availability untouched.

Read-only does not mean small. The injection reads the whole database, not just SP Property Finder's own tables, so "confidentiality" here means every row on the site is exposed to an anonymous request. On a property site that includes the personal data the component holds, the enquirer names, email addresses and phone numbers submitted through contact and booking forms, the agent records, and the booking and enquiry history. It includes unpublished and draft listings and any prices not yet meant to be public. It includes the Joomla `#__users` table, with usernames, email addresses

and password hashes, the session table, and the site secret. There is no table the query cannot reach: if it is in the database, an anonymous visitor can read it.

The catch is that a full database read is a short step from full compromise. The Joomla session table lives in the same database, so an attacker who can read arbitrary tables can read a logged-in administrator's session token and step straight into the admin panel with it, no password required. From there, installing a malicious extension is a normal administrator action. Reading the password hashes offers a slower second route through offline cracking. "Read-only" describes the bug, not how far the damage reaches.

## The second finding: an open mail relay

The property pages have contact and enquiry forms, so a visitor can ask an agent about a listing. To send that email, the form told the server who to send it to, and the server believed it. The recipient address was taken straight from the submitted request and used as-is, with no server-side lookup of the real agent and nothing to stop a visitor changing it (`controllers/agents.php` and `controllers/properties.php`, neither of which has a CSRF token on the send).

Because the recipient comes from the request, an attacker could point it at any address they liked, set the sender to anything they liked, and make the site send arbitrary email. The result is an unauthenticated open mail relay: any SP Property Finder site with a contact form on a published listing 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. The correct fix, which the update makes, is for the server to look up the real recipient from the property or agent record it already holds, rather than trusting one supplied by the browser.

## Does 4.1.4 actually fix it?

We tested it rather than reading the changelog, because a fix release and a fixed bug are not always the same thing. With this same vendor in August we reported a SQL injection, watched the patch harden the exact method we named, and found the identical flaw still reachable through the function directly below it.

The check worth doing is a before and after on one install. We ran our original attack requests against 4.1.3, confirmed every one of them still worked, then sent the identical requests to 4.1.4. That order matters more than it sounds: a patched site returning no results looks exactly like a site where the filter stopped being applied at all, and only the control run separates the two.

On 4.1.4 the postcode filter still filters and no longer injects. A value crafted to break out of the query comes back treated as ordinary text, and the database reports no error behind it. The sort control is checked against a fixed list of permitted columns and directions, so anything else falls back to the default ordering instead of reaching the query at all. The price and size ranges are validated as numbers before use. The map view got the same treatment as the property list, closing the second route to the same flaw.

The contact forms were rebuilt rather than patched around. The recipient is looked up in the database from the property or agent being enquired about, so the browser cannot influence who receives the mail, and both endpoints require a valid session token before they will send anything.

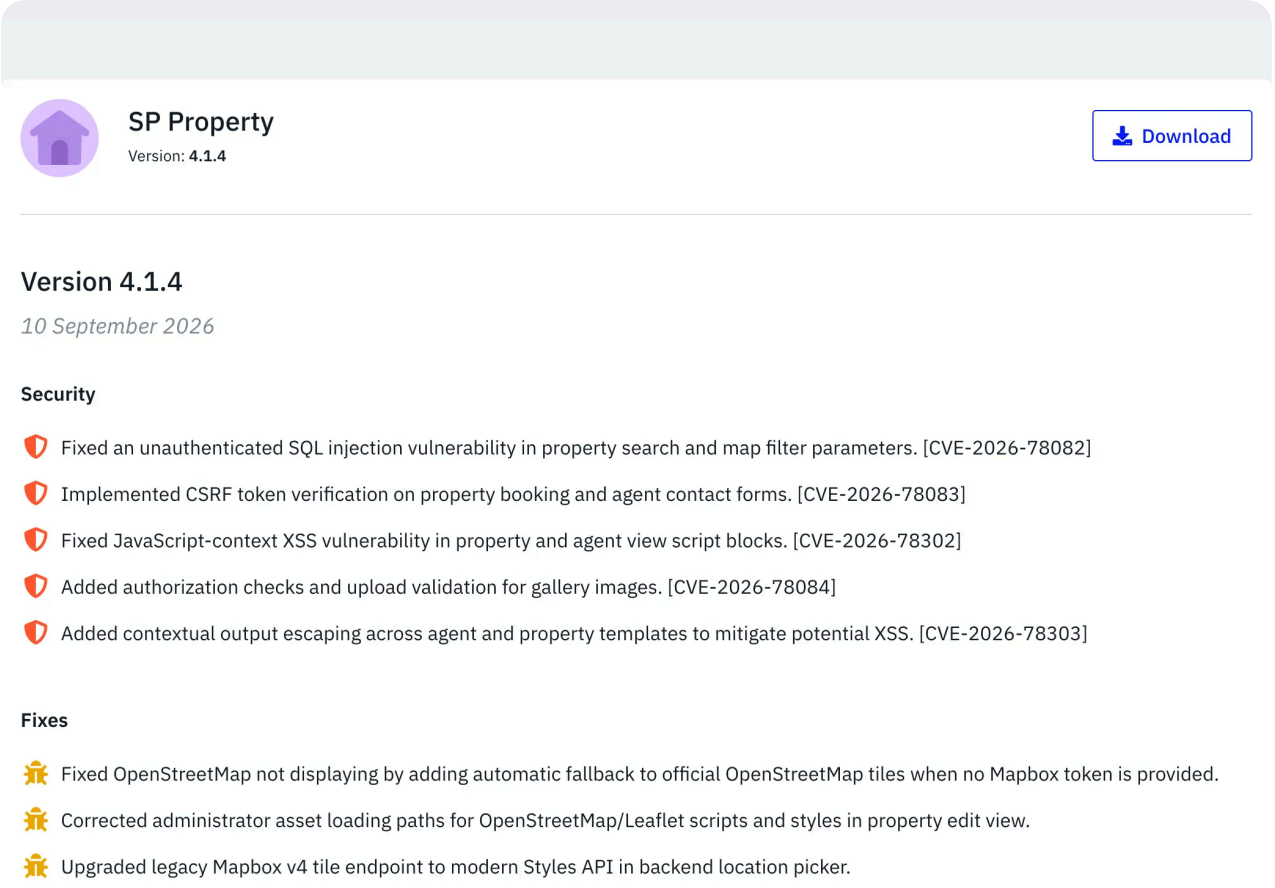
## Fixed properly, shipped with no announcement, credited to no one

The fix itself is good work, and we say so above. What surrounds it is the pattern we have written about before with this vendor.

It also took a month, and most of that month was waiting. We reported the flaw on 10 August and 4.1.4 shipped on 10 September. JoomShaper acknowledged the report on 11 August, naming the affected parameters back to us, then went silent for 27 days. The build only appeared after we chased on 7 September and copied the Joomla

Security Strike Team on the thread, at which point a fixed package reached us within 20 hours. The engineering, once it started, was quick and correct. What it took to start was a chase, with the Joomla Security Strike Team copied in to see the response time for themselves.

JoomShaper released SP Property Finder 4.1.4 on 10 September 2026 with no security announcement and no advisory. It exists as a changelog on the download page, the security entries sitting above routine map and asset-loading tidy-ups with nothing to mark them apart.




Two of those five CVEs are the issues we reported. CVE-2026-78082 is the SQL injection. CVE-2026-78083 is the contact-form fix, which the changelog files under “CSRF token verification on property booking and agent contact forms”, wording that closes the flaw without naming what it was: an unauthenticated mail relay sending mail from the site’s own domain. The other three cover an XSS issue, a gallery upload issue and template output escaping, and are not our findings. All five records were reserved

and unpublished at MITRE when this went out, so none of them resolves to a public record yet.

The changelog names no reporter. We had asked JoomShaper to tell us when 4.1.4 went public and were not told; we found the release through our own version tracking. It is the same shape we described with SP Page Builder and EasyStore earlier in the year: a complete, well-built fix, shipped without a word to the person who reported it. We have no complaint about the engineering, only about being left to find the release ourselves and about a changelog that describes a mail relay as a token check.

## Which versions are affected?

SP Property Finder **4.1.3**, the version we audited, and **every earlier version** that shares the same front-end search models are affected. JoomShaper fixed the issue in SP Property Finder **4.1.4**. If you run any earlier version, assume your site is affected and update now: the search endpoint needs no login, so if the site is online, it is reachable.

> **If you are on 4.1.3 or earlier**
>
> Assume your site is affected and update now. The SQL injection needs no login and no token, so a public property search page is all an attacker needs to reach it.

## How do you update SP Property Finder 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 Property Finder 4.1.4. If you manage more than

one site, use the mySites.guru mass update feature to upgrade SP Property Finder across every affected site from one dashboard.

3. **Confirm the version.** After updating, check SP Property Finder reports 4.1.4 or later.
4. **Clear caches.** Clear Joomla's cache and any CDN or page cache. Property search pages are often cached, which is worth knowing here: page caching hid the flaw from casual testing during our audit, because identical requests returned an identical cached page.
5. **Rotate secrets if you were exposed.** If a vulnerable version was live and public for any length of time, rotate the Joomla secret and any stored API keys, and treat password hashes as potentially known.

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.

## What the sites we monitor look like today

We keep a live inventory of every extension on every connected Joomla site, so we can see how SP Property Finder is versioned across the ones we monitor. Here is the spread on the day 4.1.4 shipped.

**94%**
still on a version below 4.1.4
on the day the fix shipped

**52%**
on 4.1.3, the version we audited
the build the injection was proved against

**15%**
on a release older than the 4.1 line
some on the 1.x and 3.x branches, years behind

**6%**
already updated to 4.1.4
within hours of release

Measured 10 September 2026 across connected Joomla sites running com_spproperty with a snapshot in the previous 30 days. Percentages of that group, a small population, not of all managed sites.

Release day is too early to judge an update rate, so the 94% is expected rather than damning. The figures that matter are the half still on 4.1.3, the exact build we proved the injection against, and the sites several releases behind on the 1.x and 3.x branches, where a security release is easy to miss entirely. On the day a fix ships for a public, unauthenticated, whole-database read, almost every affected site is still running the code that leaks. Closing that gap is deliberate work, and it is the work the next section is about.

## How do I find every SP Property Finder 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 Property Finder once and get back every connected site running it, the version each one is on, and whether an update is available.

View every SP Property Finder install across your sites

Open your Extension Inventory

Search for SP Property Finder across every connected Joomla site and filter for anything earlier than 4.1.4. Not a subscriber? Sign up free and connect your sites.

## Why search and listing components keep producing this

A property search is attack surface for the same reason it is useful: it takes input from anonymous visitors and turns it into a database query. A filter for postcode, price or bedroom count cannot require a login, because the whole point is that visitors use it. Every one of those public filters is a place where request input meets the database, and when the code behind them concatenates that input into the SQL instead of quoting it, an anonymous visitor becomes an anonymous attacker.

We have seen the same shape across the Joomla ecosystem this year, from the SP Page Builder pre-auth SQL injection in the same vendor's flagship builder, to Quix and DPCalendar, and the wider month of Joomla disclosures. The lesson is the same each time: the components that accept input from anonymous visitors need updating the moment a fix exists, which makes these updates security-critical rather than routine maintenance.

## 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 main finding is a SQL injection (CWE-89) reachable by an anonymous visitor over the network, with no login and no token. It is read-only, which caps the direct impact at

a total loss of confidentiality: full read access to the database, integrity and availability untouched. The secondary finding is an unauthenticated mail relay: the property contact forms trust a request-supplied recipient, yielding arbitrary mail sending with sender spoofing.

SP Property Finder 4.1.4 shipped on 10 September 2026 citing CVE-2026-78082 for the SQL injection and CVE-2026-78083 for the contact-form fix. Both records were reserved and unpublished at MITRE and the NVD when this was written, so neither resolves yet.

We score every issue under CVSS 4.0. The unauthenticated 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.

**8.7**
CVSS 4.0

HIGH **mySites.guru assessment**

Reachable over the internet through the public property search, with no login and no token. Ends in full read access to the site database, password hashes and the site secret included.

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

No login needed | Exploitable over the internet | Full database read | Password hashes exposed

**6.9**
CVSS 4.0

MEDIUM **mySites.guru assessment**

The property contact forms trusted a recipient address supplied by the browser, so the site could be made to send mail to anyone with a spoofed sender. Scored Medium because nothing on the Joomla site itself changes, which understates the real cost: phishing sent from your own domain and mail server.

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

No login needed | Sender spoofing | Mail sent from your domain

Each finding, scored under CVSS 4.0:

| Finding | Vector (`CVSS:4.0/...`) |
|---|---|
| Unauthenticated SQL injection (full DB read) | `AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/` |
| Unauthenticated mail relay (sender spoofing) | `AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/` |

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 Property Finder for Joomla (`com_spproperty`) |
| Vendor | JoomShaper (joomshaper.com) |
| Type | Unauthenticated SQL injection (CWE-89); unauthenticated mail relay (CWE-640 / CWE-79-adjacent) |
| CVSS 4.0 | 8.7 (High) SQL injection; 6.9 (Medium) mail relay |
| CVE | CVE-2026-78082 (SQL injection) and CVE-2026-78083 (contact-form fix), cited in the 4.1.4 changelog; both reserved and unpublished at the time of writing |
| Impact | Anonymous read of the whole database including password hashes and the site secret; unauthenticated arbitrary mail sending with sender spoofing |
| Finder | Phil Taylor, mySites.guru |

| Field | Detail |
| --- | --- |
| Affected versions | 4.1.3 and all earlier versions sharing the front-end search models |
| Fixed in | SP Property Finder 4.1.4 |
| Reported | 10 August 2026 (privately to JoomShaper) |
| Acknowledged | 11 August 2026 (JoomShaper confirmed receipt) |
| Fixed | 10 September 2026 (SP Property Finder 4.1.4) |
| CVE cited in changelog | CVE-2026-78082 and CVE-2026-78083, both reserved |

## Timeline

**2026-08-10**

### Reported privately to JoomShaper

An unauthenticated SQL injection reading the whole database including password hashes and the site secret, plus an unauthenticated mail relay, both in SP Property Finder. All public detail withheld.

**2026-08-11**

### JoomShaper acknowledges the report

The vendor confirmed receipt within a day and named the affected parameters back to us, so the report had reached someone technical rather than a support queue.

**2026-09-07**

### We chase, 27 days after the acknowledgement, copying the Strike Team

Nothing had been heard since 11 August. The chase copied the Joomla Security Strike Team, and a fixed build followed within 20 hours.

**2026-09-08**

### JoomShaper sends a fixed build for checking

We retested it against our original attack requests, with a control run on the vulnerable version first, and confirmed every reported flaw was

closed. Nothing changed for site owners at this point, because the build was not public yet.

**2026-09-10** — **JoomShaper ships 4.1.4 with no announcement**

Released with no security announcement and no advisory, as a changelog on the download page. We had asked to be told when it went out and were not; we found the release ourselves. It is the same build JoomShaper sent for sign-off, so our verification stands.

**2026-09-10** — **The release cites five CVEs, two of them ours**

CVE-2026-78082 for the SQL injection and CVE-2026-78083 for the contact-form fix are the two we reported; three more cover issues we did not. The changelog credits no reporter, and all five records are reserved and unpublished at MITRE.

## Further Reading

- Our SP Page Builder SQL injection and mail relay disclosure - the same vendor, the same pairing of a database read and a mail relay, in a different component.
- Our DPCalendar and Quix Page Builder SQL injection disclosures, 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 this one.
- CWE-89: SQL Injection - the canonical reference for this weakness class.
- JoomShaper downloads - the vendor's download page, where 4.1.4 appears.

# Frequently Asked Questions

### What is the SP Property Finder vulnerability?

mySites.guru found an unauthenticated blind SQL injection in SP Property Finder, the real-estate listings component for Joomla by JoomShaper. The public property search and map views built parts of their database query by pasting request values straight into the SQL, so an anonymous visitor with no login could read any table in the Joomla database, password hashes and the site secret included. A second, smaller issue turned the property contact and enquiry forms into an unauthenticated mail relay, because the recipient address was taken straight from the request with nothing to stop an attacker changing it. Both were reported privately to JoomShaper and fixed in SP Property Finder 4.1.4, released on 10 September 2026. The changelog cites CVE-2026-78082 for the SQL injection and CVE-2026-78083 for the contact-form fix, alongside three further CVEs for issues we did not report. All five records were reserved and not yet published when this was written.

### Is SP Property Finder 4.1.4 safe now?

Yes. We retested SP Property Finder 4.1.4 with the same attack requests we originally reported, and none of them work any more. The search filters now pass every value through the database's quoting and integer-casting instead of concatenating it into the query, the sort control is checked against a fixed list of permitted columns and directions, and the contact forms look up the recipient in the database instead of trusting one supplied by the browser. If you run any earlier version, assume you are affected and update now. Updating closes the hole, but it does not undo any database read that already happened, so if a vulnerable version was live for a while, treat password hashes and the site secret as potentially known.

### Which SP Property Finder versions are affected?

SP Property Finder 4.1.3 and earlier are affected. The vulnerable code is in the shared front-end list models used by the property and map views, so every install serving a public property search is exposed regardless of edition. JoomShaper fixed it in SP Property Finder 4.1.4. If you run any earlier version, update now.

### How do I know if my sites are affected?

If you run SP Property Finder on a version earlier than 4.1.4, 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 logging into each one to check.

**Can this vulnerability be used to take over the site?**

Not directly. This is a read-only injection: it reads data out of the database but cannot write to it, so it cannot on its own add an admin user or plant a file. The realistic escalation is indirect. By reading the Joomla session table an attacker could steal a logged-in administrator's session and take over the admin panel from there, and by reading the password hashes they could try to crack them offline. That is why we score it High rather than Critical, and why a database read still needs treating as serious: it looks like nothing happened, because nothing on disk changes.

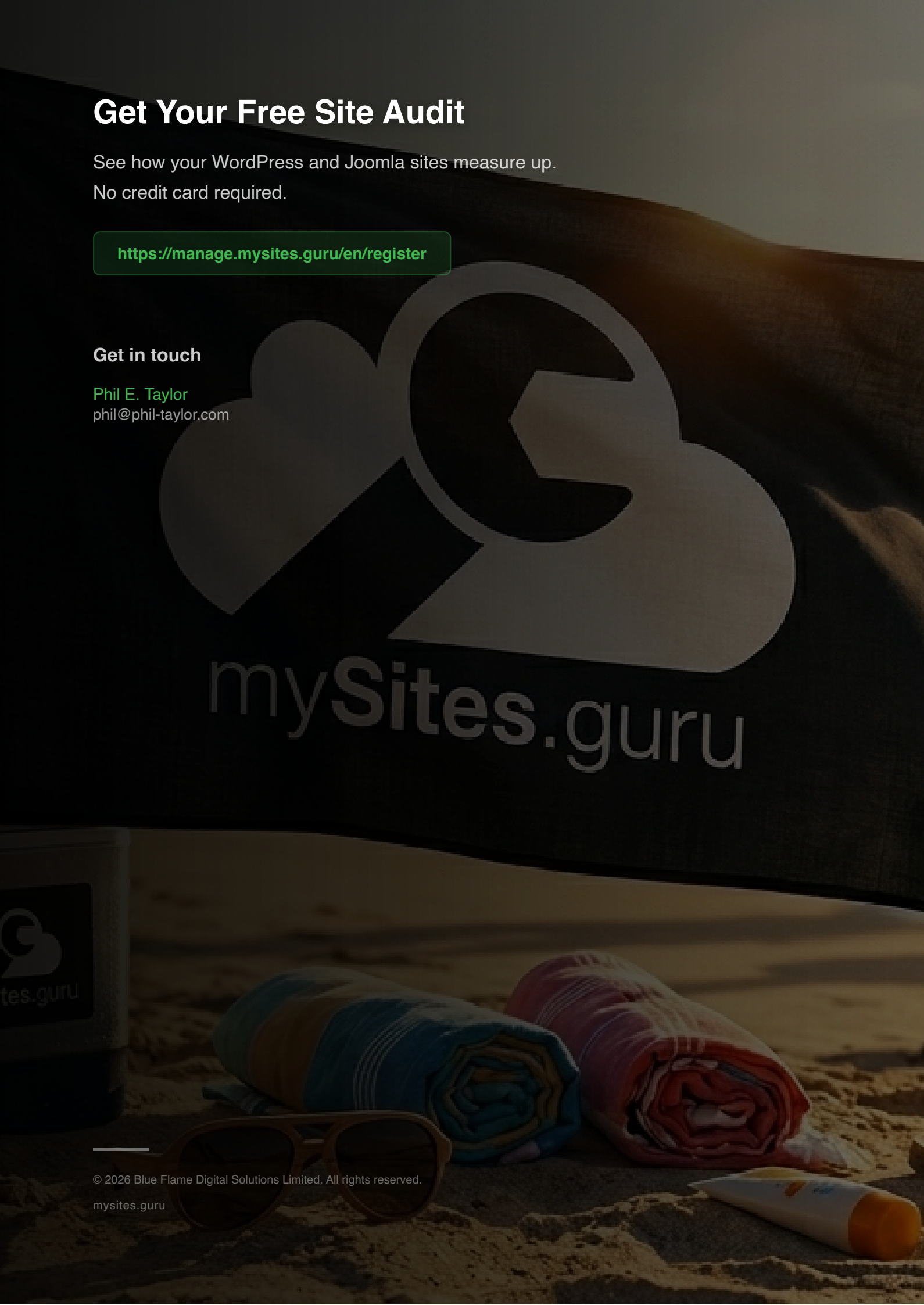

Written and edited by a human, with AI assistance. Our approach to AI

# 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