mySites.guru

Gridbox for Joomla: One Cookie and You Are a Super User

A critical unauthenticated authentication bypass in Gridbox for Joomla let anyone become a Super User by setting a single cookie. Fixed in 2.20.1. Update now.

Phil E. Taylor | 28 August 2026

Gridbox is a widely used drag-and-drop page builder for Joomla, built by Balbooa. It runs the front end of a lot of small business and agency sites, and on the sites we can see it is usually the thing the whole design depends on.

mySites.guru found a critical unauthenticated authentication bypass in Gridbox, and Balbooa fixed it in **Gridbox 2.20.1**, released today, 20 July 2026. If you run Gridbox on any Joomla site, stop reading and go and update it.

Update, 10 August 2026: 2.20.1 is no longer the version to be on. Our full audit of Gridbox nine days after this post found 23 further vulnerabilities, several of them actively exploited, and every CVE record for that set lists 1.0.0 to 2.20.1 as affected. Balbooa has shipped 2.20.2, 2.20.2.2 and 2.20.2.3 since. Update to **2.20.2.3**.

THE FLAW

Gridbox trusted a value supplied by the visitor's own browser as proof of who they were. Set it to an administrator's username and you were logged in as that user.

No password. No login form. No existing session. One anonymous request.

mySites.guru found this and reported it privately to Balbooa, copying the Joomla Security Strike Team. The fix is in Gridbox 2.20.1. We are withholding the exact cookie, the endpoint and any proof-of-concept. This is how we handle every vulnerability we find: fix first, publish second.

TL;DR

- **A critical unauthenticated authentication bypass in Gridbox** let anyone become a Super User on a Joomla site by setting a single browser cookie
- We **confirmed it live**: an anonymous request that returned nothing became a full administrator session, and Joomla itself recorded the user as logged in
- A Joomla Super User can edit templates, which is PHP execution, so this is **full site compromise, usually full server compromise**, from one request
- **Balbooa asked us to test Gridbox.** After our Balbooa Forms disclosure earlier this month they said they had reviewed and hardened their other products, sent us a package and invited us to look. This was in the build they sent
- **Fixed in 2.20.1**, released 20 July 2026. The previous release was 2.20.0.2 in **October 2025**, so the vulnerable code shipped for at least nine months
- The changelog entry is **three words**: "Critical authentication vulnerability". No affected versions, no impact, no urgency
- **No announcement on the Gridbox blog.** The only place 2.20.1 appears there is in Balbooa's own asset URLs, because their own site is already running it
- **We were not told the release was coming**, and were never asked to verify that the fix closed what we reported
- Tracked as CVE-2026-61425, assigned through the Joomla CNA

What the flaw actually was

Authentication in a Joomla extension should come down to one question: has this person proved who they are? Gridbox answered a different question. It read a value out of the request that the visitor's own browser had supplied, took that value to be an identity, and acted on it.

Anything the browser sends is attacker-controlled. A cookie is not a credential, it is a note the visitor writes to themselves, and the only reason a session cookie means anything is that the server issued it and can recognise its own signature. A cookie whose plain value is a username has no such property. You can type it yourself.

So an anonymous visitor with no account could name an administrator and be treated as that administrator.

We confirmed it against a live Joomla install rather than reasoning about it from the source. A guest request to a gated endpoint returned nothing, as it should. The same request, with one cookie added, returned the administrator-only content in full, and Joomla's own session state recorded the visitor as logged in. That is not a permissions edge case or a theoretical weakness. It is account takeover of any user on the site, chosen by name.

On Joomla the ceiling is high, and it is worth being explicit about why this scores where it does. A Super User can edit template files from the administrator interface. Template files are PHP. So an authentication bypass that reaches Super User is a remote code execution chain, and from there the rest of the hosting account is usually reachable too. There is no configuration that makes this safe, no permission you could have set differently, and no firewall rule that helps, because the request is perfectly well formed and contains no payload to detect.

We are not publishing the cookie name, the endpoint or a proof-of-concept. The fix is out. The detail can wait.

Balbooa asked us to test it

This is the part of the story we did not expect, and it is only fair to Balbooa to tell it in the right order.

Earlier this month we found and disclosed an unauthenticated file upload flaw in Balbooa Forms, which became CVE-2026-56291. That one came to us through a hosting abuse report on a customer's live site, and Balbooa responded well: they took the report seriously and shipped a fix inside a day.

On 17 July, Balbooa came back to us unprompted. They thanked us for the earlier disclosure, said it had prompted them to review their other products, and told us they had already hardened Gridbox. Then they sent us a package and invited us to test it:

> **Balbooa, 17 July**
>
> As a result, we've been reviewing the security of our other products as well. From what we understand, you use automated tools to identify potential vulnerabilities, so we took the opportunity to harden several areas in Gridbox that we believed could potentially be improved. If you have some time, we'd be interested to know whether your tools uncover anything we've missed.

That is a good instinct, and we want to say so clearly, because a vendor volunteering their code for review is rarer than it should be. We ran it the same day.

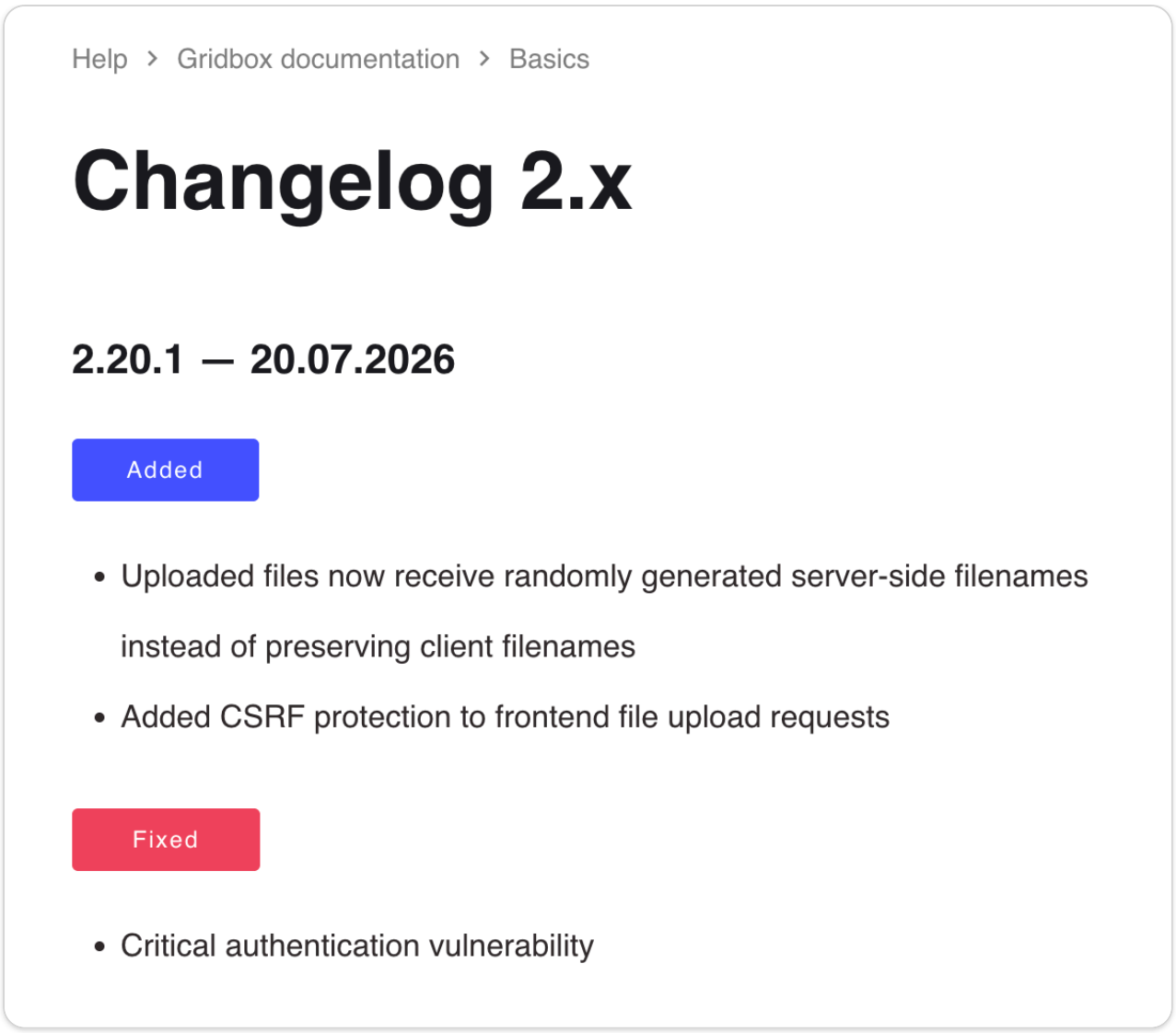
The authentication bypass was in the build they sent us as hardened. We reported it back within the hour, copying the Joomla Security Strike Team, and told them that every site running the extension should be treated as compromiseable immediately.

Balbooa's reply was to ask us to quote for a paid security audit of Gridbox. We declined, because we have our hands full running mySites.guru, but we repeated that what we had already gave them had to be fixed straight away, asked to see a fixed build so we could verify it actually closed the hole, and offered to coordinate the disclosure and the CVE with them.

Three days later the fix shipped, and we found out from someone else.

The changelog, in full

Here is what a Gridbox administrator sees today. This is the entire public description of a flaw that hands anonymous visitors a Super User account:



The complete public record of the Gridbox authentication bypass, as published by the vendor on 20 July 2026.

Three words. “Critical authentication vulnerability.”

We are not asking for a proof-of-concept in a changelog. Nobody sensible publishes exploit detail alongside a patch. But there is an enormous amount of room between an exploit and three words, and everything a site owner needs to make a decision lives in that space:

No affected version range

This is the single most important fact in any security release, and it is missing. A Gridbox administrator on 2.19 has no way to know whether this applies to them. Neither

does one on 2.16, or 2.12. The version immediately before 2.20.1 was 2.20.0.2, released on **21 October 2025**, which means the vulnerable code had been shipping for at least nine months and probably far longer. None of that is stated.

No description of impact

"Authentication vulnerability" covers everything from a session that expires too slowly to what actually happened here. A reader has no way to distinguish the two, so most will assume the mild version, because most vulnerabilities are the mild version.

No urgency

There is no "update immediately", no severity rating, no note that sites should be checked for compromise. The entry sits in the same visual style as "Incorrect time zone in the calendar" from the previous release.

Two more security fixes filed as features

Look at the Added section in that screenshot. Randomised server-side upload filenames, and CSRF protection on frontend file upload requests. Those are not features. They are the same two hardening measures we watched JoomDonation bolt onto Events Booking last week after an unauthenticated upload flaw, and they belong under Fixed with an explanation. Filed under Added, they read as improvements rather than as repairs to something that was wrong.

No announcement anywhere else

A changelog is a reference document. People read it when they already suspect something. For a critical flaw the vendor also has to push the information out, and Balbooa runs exactly the right channel for that: a Gridbox blog where they write about releases.

There is nothing there about this.

We checked the page on the day of release. The words “security”, “vulnerability”, “critical” and “authentication” do not appear on it at all. The only place the string 2.20.1 appears anywhere on that page is inside the cache-busting query strings on Balbooa’s own stylesheets and scripts, which is its own small detail: their website is already running the patched version while their customers have been told nothing.

So the sum total of public communication about a Super User authentication bypass is three words in a document you have to already know to go and read.

What coordinated disclosure would have looked like

We wrote about this last week in the context of another vendor, and we would rather not make a habit of it, but the same gap has opened twice in a fortnight and it is worth being concrete about what was missing.

Coordinated disclosure is a documented process. ISO/IEC 29147 covers how a vendor should handle and publish vulnerability information, ISO/IEC 30111 covers the handling process behind it, and the CERT Guide to Coordinated Vulnerability Disclosure is the practitioner reference. They agree on the vendor’s obligations, and four of them apply here.

Tell the reporter the release is coming

We asked to be kept in the loop and offered to coordinate. The release went out on 20 July and we learned about it from the Joomla Security Strike Team, not from Balbooa. There is no version of coordinated disclosure in which the reporter finds out from a third party.

Ask the reporter to verify the fix before you ship it

This is the step that protects the vendor, not the researcher. We explicitly asked for a fixed build so we could confirm the hole was actually closed, and were never sent one. We have not been able to verify 2.20.1 against what we reported. It looks right from the outside and we have no reason to think it is wrong, but nobody who found the flaw has

checked the patch, and that is a risk Balbooa did not need to take. The fix for an authentication bypass is exactly the kind of change that can be almost right.

Publish an advisory a customer can act on

An affected version range, a severity, an impact description and an instruction. This costs one paragraph.

Agree the disclosure timing once, in advance

Fix a date with the reporter, publish together, request the CVE. Instead the patch went out unannounced, which starts the clock anyway, because anyone can now compare 2.20.0.2 with 2.20.1 and find the change. A silent security release does not buy quiet. It buys a head start for whoever is diffing releases, and leaves defenders reading three words.

None of this requires a security team or a budget. It is an email to the person who reported it and a paragraph on a blog.

What you should do right now

UPDATE TODAY, NOT THIS WEEK

Every Joomla site running Gridbox below 2.20.1 should be treated as trivially compromiseable by anyone who knows the trick.

The patch is public, so the flaw can be recovered by comparing two releases. There is no mitigating configuration and no firewall rule that helps.

1. **Update Gridbox to 2.20.1** on every Joomla site you manage. Joomla's Extensions updater will offer it, or download it from your Balbooa account.
2. **Take a backup first**, as with any extension update on a production site. If you use mySites.guru, trigger a snapshot so you have a clean point to return to.

3. **Check for compromise on any site that has been running an affected version.** This is an authentication bypass, so the thing to look for is what an attacker does after logging in: unexpected Super User accounts, recently modified template files, and administrator logins you cannot account for. Our guides to finding hacked files and backdoors and fixing a hacked Joomla site cover the process.
4. **Rotate credentials** on any site you have reason to worry about, and treat the Joomla secret as exposed if the site was reachable and busy.
5. **Do not wait for formalities.** The flaw is now tracked as CVE-2026-61425, but the fix already exists and the patch is public. Update regardless of any advisory catching up.

Which versions are affected?

We confirmed the bypass in **2.20.0.1**, which is the build Balbooa sent us. Being straight about the limits of that: we tested one version, and the vendor has published no affected range, so we cannot tell you when the flawed code first appeared.

What we can tell you is that the release immediately before the fix was **2.20.0.2, dated 21 October 2025**. Nine months of releases separate those two entries, which means the vulnerable code was in the shipping product for at least that long.

Treat every Gridbox below 2.20.1 as affected. The fixed version for this flaw is **2.20.1**.

That was true on the day, and it is out of date now: the audit that followed found 23 more vulnerabilities affecting everything up to and including 2.20.1. The current release is **2.20.2.3**.

Across the Joomla sites connected to mySites.guru we can see the Gridbox component on **447 sites**. At the time of writing **244 of those are still on 2.20.0.2**, the last release before the fix, and only 137 have picked up 2.20.1. That split is why the missing announcement matters: the update exists, and most sites have no idea they need it.

How do I find every Gridbox site I manage?

The awkward question after any extension security release is which of your sites actually run the thing. Up to about ten sites you can log into each Joomla admin and read the installed extensions list. Past that you need a single view, which is exactly why version numbers get so old.

mySites.guru keeps a live inventory of every extension, template and framework on every Joomla and WordPress site in your account. Search for Gridbox once and get back every connected site running it, the version each one is on, and whether an update is available. That is the same query that produced the numbers above.

View every Gridbox install across your sites

Open your Extension Inventory

Search for Gridbox across every connected Joomla site and filter for anything below 2.20.1. Not a subscriber? Sign up free and connect your sites.

When a fix ships we add the affected range to our vulnerability database, so every connected site still on a vulnerable version of Gridbox is flagged automatically, and the mass updater pushes the update to all of them from one screen.

Credit where it is due

We have been hard on the communications here, so it is worth separating them from everything else.

Balbooa did something most vendors never do: after taking one disclosure on the chin they went looking for problems in their other products, and then invited an outside party to test the result. That instinct is good, and the fix itself arrived in three days, which is fast by any standard in this ecosystem.

The bug is also an ordinary kind of mistake. Trusting a value from the request is the oldest error in web authentication, and it is in a great deal of shipped code written by people who know better.

What let this down was everything after the fix was written. The patch went out without telling the person who reported it, without anyone verifying it closed the hole, described in three words, with no affected versions and no announcement. A good engineering response and a poor communications response are different things, and only one of them was the problem here.

Stay ahead of the next one

There will be another one. Joomla runs on thousands of third-party extensions, and the ones that touch authentication or accept anonymous input keep producing findings like this. The hard part was never the update. It is knowing a fix exists at all, which in this case the vendor has made unusually difficult, then knowing which of your sites are affected and getting to them first.

Get free email alerts when a Joomla vulnerability breaks

We email a plain-English alert the moment a serious flaw like this one is disclosed, with the affected versions and what to do. No charge, unsubscribe any time.

Subscribe to security alerts

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

10.0

CRITICAL

Our own assessment; tracked as CVE-2026-61425 via the Joomla CNA

Unauthenticated, exploitable over the internet in a single request, with no user interaction, yielding a Super User account. On Joomla that reaches PHP execution through template editing, so confidentiality,

CVSS 4.0

integrity and availability all fall, for the site and usually for the hosting account behind it.

No login needed | Single request | Full Super User takeover | Leads to code execution | No firewall mitigation

Field	Detail
Extension	Gridbox for Joomla (`com_gridbox`)
Vendor	Balbooa (balbooa.com)
Type	Authentication bypass using an attacker-controlled value (CWE-290, CWE-565)
CVSS 4.0	10.0 (Critical), our own assessment. The published CVE record scores it 9.4 on a vector requiring high privileges, which does not match what we reproduced. See the note below
CVE	CVE-2026-61425 (assigned via the Joomla CNA). The published record gives the affected range as "< 1.6.0". See the note below
Impact	Unauthenticated takeover of any account, including Super User, leading to code execution
Confirmed in	2.20.0.1
Affected versions	Not published by the vendor. Treat everything below 2.20.1 as affected
Fixed in	2.20.1, released 20 July 2026
Finder	Phil Taylor, mySites.guru

The full timeline is at the foot of this post.

A note on the published CVE record

The record for CVE-2026-61425 has since published, and two fields in it do not match what we reported and reproduced.

It describes the issue as an “authenticated bypass” and scores it **9.4 Critical** on a CVSS 4.0 vector with `PR:H`, meaning high privileges are needed before the attack works. We reproduced it with **no account and no session at all**: one cookie on an anonymous request returned a Super User session. On our reading the vector is `PR:N`, which is what takes the score to 10.0.

The record also gives the affected range as **“Gridbox < 1.6.0”**. We confirmed the flaw in **2.20.0.1**, and Balbooa fixed it in **2.20.1**, so that range excludes every version we actually tested, including the one the vendor patched.

We are keeping our own account here because we proved it live. If you are deciding what to do about a Gridbox install, use the versions in this post rather than the range in the record.

Timeline

2026-07-09

Balbooa ships the unrelated Forms fix, and reviews its other products

The file upload flaw in Balbooa Forms, later CVE-2026-56291, was also reported by mySites.guru. Fixing it prompted the vendor to look at the rest of the range.

2026-07-17

Balbooa contacts us unprompted and sends a build to test

The vendor says the earlier report prompted a review, that Gridbox has been hardened, and invites us to test the package.

2026-07-17

We find the authentication bypass in the hardened build

Reported back to Balbooa the same day, copying the Joomla Security Strike Team, with the advice that every site running the extension should be treated as compromiseable.

2026-07-17

Balbooa acknowledges the report and asks us to quote for a paid audit

The request is for a commercial security audit of Gridbox.

2026-07-20

We decline the paid audit and restate the fix must come first

We ask for a fixed build in order to verify it, and offer to coordinate the disclosure and the CVE.

2026-07-20

Gridbox 2.20.1 is published without notice to us

The fix ships without asking for verification. We learn of the release from the Joomla Security Strike Team. The changelog calls it a "Critical authentication vulnerability" with no affected version range, and no announcement appears on the Gridbox blog.

2026-07-20

CVE-2026-61425 is assigned, and we flag every affected site

Every connected site below 2.20.1 is flagged against our vulnerability rules, and we publish this write-up with no proof of concept.

Further Reading

- Another 23 critical vulnerabilities in Gridbox - the full audit that followed this disclosure, and the reason 2.20.1 is no longer enough.
- Our Balbooa Forms disclosure - the same vendor, the flaw that started this, and the reason they invited us to look at Gridbox.
- Events Booking: anyone could upload files to your server - a different vendor with the same communications problem, published last week.
- A month of Joomla extension vulnerabilities - the full run of findings this has been part of.
- CWE-290: Authentication Bypass by Spoofing and CWE-565: Reliance on Cookies without Validation and Integrity Checking - the canonical references for this weakness class.

- ISO/IEC 29147 and the CERT Guide to Coordinated Vulnerability Disclosure - what the disclosure process is supposed to look like.
- Gridbox changelog - where 2.20.1 is documented, in three words.

Frequently Asked Questions

What is the Gridbox authentication vulnerability?

Gridbox, the Joomla page builder by Balbooa, trusted a value supplied by the visitor's own browser as proof of who they were. Setting that value to an administrator's username was enough to be logged in as that user, with no password, no login form and no existing session. mySites.guru confirmed it live against a Joomla install: an anonymous request became a full Super User session. Balbooa fixed it in Gridbox 2.20.1, released 20 July 2026.

Which Gridbox versions are affected?

We confirmed the flaw in 2.20.0.1. Balbooa has published no affected version range at all, and the release before 2.20.1 was 2.20.0.2 back in October 2025, so the vulnerable code was shipping for at least nine months. Treat every version below 2.20.1 as affected until the vendor says otherwise. The fixed version for this flaw is 2.20.1, but do not stop there: the full audit that followed found 23 more vulnerabilities affecting everything up to and including 2.20.1, and the current release is 2.20.2.3.

How serious is it?

As serious as it gets. It needs no account, no password, no user interaction and no existing session, and it hands the attacker a Super User on your Joomla site. From a Joomla Super User, template editing gives you PHP execution, so this is a full site and often a full server compromise from a single anonymous request. We assess it as CVSS 4.0 10.0 Critical, and it is tracked as CVE-2026-61425, assigned through the Joomla CNA. The published CVE record scores it 9.4 on a vector that requires high privileges and gives the affected range as below 1.6.0, neither of which matches what we reproduced against 2.20.0.1 with no account at all.

Did mySites.guru find this?

Yes, though the circumstances are worth stating plainly. After we disclosed the unauthenticated file upload flaw in Balbooa Forms (CVE-2026-56291) earlier in July, Balbooa contacted us, said they had reviewed and hardened their other products, sent us a Gridbox package and invited us to test it. We tested the build they sent and found the authentication bypass in it.

What did Balbooa's changelog say about it?

Three words: "Critical authentication vulnerability", under a Fixed heading. No affected version range, no explanation of impact, no urgency, and no advice to update immediately.

Two further security fixes in the same release, randomised upload filenames and CSRF protection on frontend file uploads, are listed under Added as though they were features.

How do I find every Gridbox site I manage?

mySites.guru keeps a live inventory of every extension and version on every connected Joomla and WordPress site. Search for Gridbox once and get back every site running it, the version each is on, and whether an update is available. Every connected site still on a vulnerable version is flagged automatically against our vulnerability database.

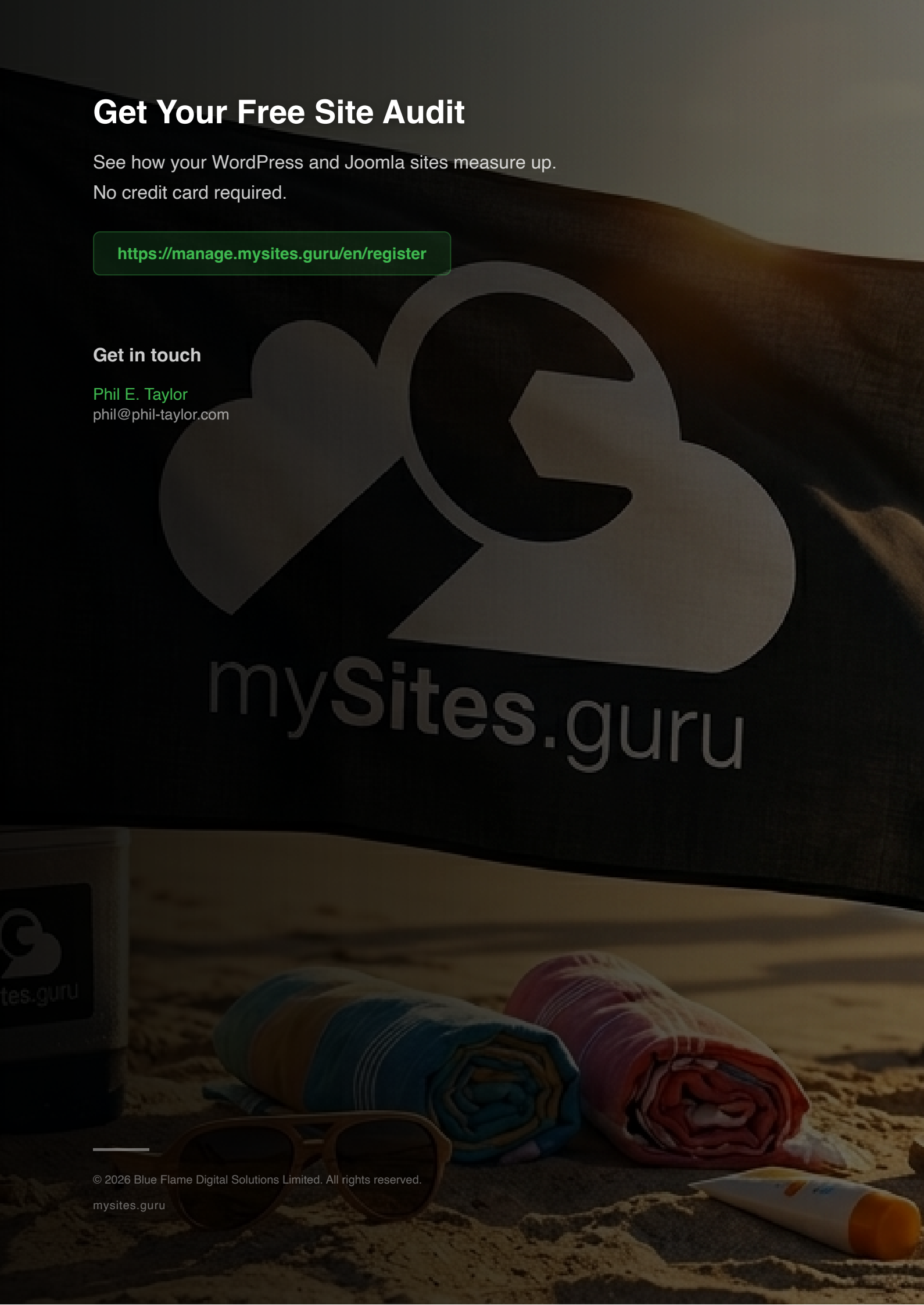
Written and edited by a human, with AI assistance. Our approach to AI

Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.

No credit card required.

https://manage.mysites.guru/en/register



Get in touch

Phil E. Taylor
phil@phil-taylor.com

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