mySites.guru

Gridbox 2.20.5.0 Fixes Unauthenticated File Deletion and Stored XSS

Gridbox 2.20.5.0 fixes four flaws in the Joomla extension, including file deletion that needs no login. About 92% of the Gridbox sites we monitor are affected.

Phil E. Taylor | 4 November 2026

TL;DR

Balbooa released Gridbox 2.20.5.0 on 4 November 2026 with four security fixes for the Joomla page builder and a broad round of hardening on top. The worst of the four is a front-end task for removing temporary comment and review attachments which, in 2.20.4.2, needed no login and did not check that the file it was told to delete stayed inside the uploads folder. The other three are a second file deletion flaw on form submissions and two stored cross-site scripting flaws in the comment and review output.

Balbooa says 2.20.4.2 and earlier are affected and rates the release High. Four CVE ids have been assigned with the help of David Jardin of the Joomla Security Strike Team (CVE-2026-105607, CVE-2026-107129, CVE-2026-107130 and CVE-2026-107903), but the records were reserved and not yet published on the morning of the release, and Balbooa does not say which id is which. Roughly 92% of the Gridbox sites we monitor are on an affected version. Update to 2.20.5.0 today.

8.8
CVSS 4.0

Unauthenticated deletion of temporary comment and review attachments

HIGH

mySites.guru assessment (CVE records not yet published)

A visitor with no account could ask the site to delete a file by name, and nothing confirmed the file belonged to them or sat inside the uploads folder, so files the site needs to run were within reach.

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

No login needed | CWE-22 path traversal | Up to 2.20.4.2

▼ What does this mean?

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

How it is reached

AV:N Network: Reachable across the internet
AC:L Low: Nothing to work around, it just works
AT:N None: Works against any affected install
PR:N None: No account needed
UI:N None: Nobody has to be tricked into anything

What it does to the site

VC:N None: Nothing can be read
VI:H High: Data and files can be altered at will
VA:H High: The site can be taken down

What it does beyond the site

SC:N None: Other systems keep their data
SI:N None: Other systems keep their integrity
SA:N None: Other systems stay up

6.9
CVSS 4.0

Deletion of form submission files (IDOR)

MEDIUM

mySites.guru assessment (CVE records not yet published)

A front-end task could remove the file attached to a form submission without checking who was asking, so submissions other people had made could lose their attachments.

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

No login needed | CWE-639 IDOR | Up to 2.20.4.2

▼ What does this mean?

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

How it is reached

AV:N Network: Reachable across the internet
AC:L Low: Nothing to work around, it just works
AT:N None: Works against any affected install
PR:N None: No account needed
UI:N None: Nobody has to be tricked into anything

What it does to the site

VC:N None: Nothing can be read
VI:L Low: Some data can be altered

VA:L Low: The site slows or stutters

What it does beyond the site

SC:N None: Other systems keep their data
SI:N None: Other systems keep their integrity
SA:N None: Other systems stay up

5.3
CVSS 4.0

Stored XSS in comments, reviews and replies

MEDIUM

mySites.guru assessment (CVE records not yet published)

Script placed in a comment or review message was shown back unsanitised in the recent comments and reviews widgets and in individual reviews, so it ran in the browser of whoever viewed the page.

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

Guest posting assumed | CWE-79 stored XSS | Up to 2.20.4.2

▼ What does this mean?

CVSS 4.0 scores how severe a flaw is, from 0 (no impact) to 10 (critical). Each pair of letters in the string above is one metric; here is what this one's says.

How it is reached

AV:N Network: Reachable across the internet
AC:L Low: Nothing to work around, it just works
AT:N None: Works against any affected install
PR:N None: No account needed
UI:P Passive: Someone has to visit a page

What it does to the site

VC:N None: Nothing can be read
VI:N None: Nothing can be altered
VA:N None: The site stays up

What it does beyond the site

SC:L Low: Some data on other systems can be read
SI:L Low: Some data on other systems can be altered
SA:N None: Other systems stay up

What do the four Gridbox fixes change?

The first fix is to the temporary attachments that a visitor can add while writing a comment or a review. Balbooa names it “Temporary Attachment Deletion” and says it added path traversal validation, ownership checks and CSRF protection to prevent unauthorised file deletion. In 2.20.4.2 the front-end task that removes one of those attachments had no login check and no token check. It took a file name from the request and deleted that path relative to the uploads folder, without confirming that the path stayed inside the folder or that the file belonged to the visitor asking. In 2.20.5.0 the task looks the attachment up by its id and the comment it belongs to, and deletes only that file.

This is the one to worry about. A file deletion that needs no account and accepts a path is a path traversal problem, and an attacker who can delete arbitrary files on a Joomla site can delete the files the site needs to run and take it offline. The first thing the site owner sees is a broken site, with no obvious link back to a page builder’s comment form.

The second fix is to the file attached to a form submission. Balbooa calls it “Submission File Deletion (IDOR)” and says it added authorisation and CSRF checks to prevent unauthenticated deletion of submission files. An IDOR, an insecure direct object reference, is where a request names the thing it wants acted on and the code acts on it without asking whether the caller is allowed to. 2.20.5.0 removes the old front-end task for a submission’s file altogether, which is a cleaner answer than patching it. We scored this one lower than the attachment flaw because what is at stake is other people’s submission attachments rather than the files the site runs on, the same shape as the download IDOR in Phoca Cart.

The third and fourth fixes are both stored cross-site scripting, and both are in the output side of the same comment and review features. “Recent Comments & Reviews XSS” adds message sanitisation to the front-end widgets that list recent comments and reviews. “Review XSS (getReviewById)” adds strip_tags() to individual reviews and their replies. In 2.20.4.2 a message typed into a comment or review was shown back to other visitors as it was typed, so script in the message ran in the browser of anyone

who viewed the widget or the review. Stored XSS is the kind that persists: one submission, then every page view until it is removed. Our score assumes guest commenting or reviews are enabled; where they are not, a registered account is needed to post and the score comes down.

We have seen the same output-side mistake in other Joomla extensions, in Phoca Gallery's EXIF fields and in DJ-HelpfulArticles. Any feature that takes free text from the public and shows it to an administrator or to other visitors is the place to look.

The hardening that came with it

The four named fixes are a small part of the release. 164 files changed between 2.20.4.2 and 2.20.5.0, and Balbooa lists the wider work: permission and CSRF checks on actions that create or modify data, file validation and path checks, stronger restrictions on uploaded files, tighter handling of comment and review content, CSV exports hardened against SQL injection and against spreadsheet formula injection, and server-side validation of store and booking order processing, including quantity values. The front-end comments, store, uploader and page controllers now check a CSRF token, and review and comment output now strips tags.

Spreadsheet formula injection is a bug most site owners have never heard of. A spreadsheet treats a cell that begins with certain characters as a formula and evaluates it when the file is opened. If an export puts a customer's typed input into a cell as it was typed, the customer can write a formula that runs on the computer of the person who opens the export, which is usually the shop owner. Hardening against it means neutralising those leading characters on the way out. For a store and booking extension that exports orders to CSV, that is a sensible thing to have closed.

> **A hardening release is still an update you have to apply**
>
> Balbooa puts Gridbox at 1,448 files and about 295,000 lines of code. A release that touches 164 of those files protects your sites only once 2.20.5.0 is installed on each of them.

Which Gridbox versions are affected?

Balbooa's note says 2.20.4.2 and earlier are affected, with the fix in 2.20.5.0. Our newest rule flags every connected site on 2.20.4.2 with all four CVE ids, and the older Gridbox rules have been repointed so that every earlier build now names 2.20.5.0 as the version to install.

Gridbox version	Status	What to do
2.20.5.0	Fixed	Nothing
2.20.4.2	Affected by this release's four fixes	Update to 2.20.5.0
2.20.4.0 to 2.20.4.1	Also exposed to the two Critical SQL injection flaws fixed in 2.20.4.2	Update to 2.20.5.0
2.20.3.1 and below	Also exposed to the language install CSRF and image preview path check	Update to 2.20.5.0
Below 2.20.2	Exposed to the actively exploited July flaws	Update to 2.20.5.0 urgently and check for compromise

Joomla 4, 5 and 6 all get 2.20.5.0 through the update stream. Sites on the Joomla 3 line top out at Gridbox 2.17.0.2, which has no fix for any of this year's flaws. For those sites the fix is moving to a supported Joomla.

What you should do right now

1. Update Gridbox to 2.20.5.0 on every Joomla site that runs it, through Joomla's Update tab or the mySites.guru mass updater.
2. Confirm the version afterwards: open System, Manage, Extensions and check that Gridbox reads 2.20.5.0.
3. If a site sat on an affected version, check it for missing or changed files and backdoors. The attachment deletion flaw is destructive rather than quiet, so a site

that was hit is likely to be broken, but a partial deletion can leave a site limping in ways that look like an unrelated fault.

4. Look for administrator accounts you did not create. The stored XSS runs in the browser of whoever views the comment or review, and an administrator viewing it from the front end is the account an attacker would most like to borrow.
5. If guest commenting or reviews are enabled on a site that does not need them, this is a good week to turn them off.

There is no public report of exploitation, none of the four ids is on the CISA KEV list, and neither Balbooa nor the Joomla Security Strike Team has said anything either way. The checks above are what you do when you cannot rule it out.

Find administrator accounts you never created

mySites.guru checks every connected site for this automatically and flags it the moment it appears. It runs as part of the full audit on every connected site.

Check your site for free →

How do I find every Gridbox site I manage?

mySites.guru keeps a live inventory of the extensions on each connected Joomla and WordPress site. Search for Gridbox once and you get every site running it, the version each is on and whether an update is waiting. On the morning of the release, about 86% of the Gridbox sites we monitor were on 2.20.4.2, the release from 27 October, a week earlier. About 8% had already moved to 2.20.5.0 within hours of it appearing, which leaves roughly 92% on an affected version.

Most Gridbox sites moved to 2.20.4.2 inside a week, so they are being kept up to date. They now need doing again, eight days on. Connected sites on 2.20.4.2 are flagged automatically with all four CVE ids, and the mass updater pushes 2.20.5.0 to all of them from one screen. That is part of the subscription, not a separate purchase.

Six Gridbox security releases since July

2.20.1 fixed the cookie authentication bypass in July. 2.20.2 fixed the 23 flaws from our audit later that month. 2.20.3.1 fixed the blog author SQL injection on 21 September. 2.20.4.0 fixed the language install CSRF and image preview path check on 8 October. 2.20.4.2 fixed two unauthenticated SQL injection flaws, both CVSS 9.3 Critical, on 27 October. 2.20.5.0 is the sixth.

It is also the first of the six where Balbooa found the issues itself. The previous five all began with someone outside the company: our own research in July, then independent researchers reporting what they found. This time Balbooa describes an in-depth internal review of the product, using automated security analysis tools together with its own knowledge of how Gridbox is built, and says it identified the four independently. No outside reporter is named, and there is nothing of ours in it.

That is the right direction, and after five posts that were harder on Balbooa, we are glad to say so. A vendor that fixes only what it is sent will keep getting sent things, because each report points the next researcher at the neighbouring parameter, which is how 2.20.3.1 and 2.20.4.2 ended up closing the same mistake in the same listing code five weeks apart. A vendor that reads its own code with the same eyes a researcher would, and changes 164 files rather than two, has a chance of getting ahead of the queue. What the review turned up, two file deletion routes that needed no login, is also a fair measure of how much was still there to find.



Read the full post →

Disclosure and severity

This is not a mySites.guru finding. Balbooa identified the four issues through its own internal review and thanks David Jardin of the Joomla Security Strike Team for his assistance with the CVE assignments. The four ids, CVE-2026-105607, CVE-2026-107129, CVE-2026-107130 and CVE-2026-107903, were reserved but not yet published on the morning of the release, and Balbooa does not say which id belongs to which issue, so neither do we.

Balbooa rates the release at a maximum severity of High. The scores on this page are our own CVSS 4.0 assessment from reading the two packages, labelled as provisional on each card: 8.8 High for the attachment deletion, 6.9 Medium for the submission file deletion, and 5.3 Medium for the two stored XSS flaws taken together. Our worst score agrees with Balbooa's rating. Once the CNA publishes the records we will quote its vectors and scores here instead, because those are what scanners and other advisories will show you.

If a site has already been hit, or you would rather someone else made sure, fix.mySites.guru cleans the site up, audits it for backdoors and hands it back secure for a single fixed fee, usually the same day.

Timeline

2026-09-21 — **Gridbox 2.20.3.1 fixes an unauthenticated blog author SQL injection**

The first SQL injection fix in the public blog post listing code.

2026-10-08 — **Gridbox 2.20.4.0 fixes a language install CSRF and an image preview path check**

Reported by Sergiy Tryzhychynskyi, coordinated by the Joomla Security Strike Team.

2026-10-27 — **Gridbox 2.20.4.2 fixes two unauthenticated SQL injection flaws**

Reported by Artur Błażewicz, coordinated by David Jardin of the Joomla Security Strike Team. Both scored CVSS 4.0 9.3 Critical by the Joomla CNA.

2026-11-04 — **Gridbox 2.20.5.0 fixes unauthenticated file deletion and stored XSS**

Four flaws found by Balbooa's own internal review, with CVE ids assigned with the help of David Jardin of the Joomla Security Strike Team. The CVE records are reserved but not yet published.

2026-11-04 — **mySites.guru flags every affected site**

Connected sites on 2.20.4.2 are flagged automatically with all four CVE ids, and the older Gridbox rules now point to 2.20.5.0.

Further Reading

- Balbooa: Gridbox 2.20.5.0. Security Deep Dive - the vendor's own release note.
- Gridbox 2.20.4.2 Fixes Two Unauthenticated SQL Injection Flaws - the previous release, eight days earlier.
- Gridbox 2.20.4.0 Fixes a Language Install CSRF and an Image Path Check - the October release before it.
- Blind SQL Injection in Gridbox's Blog Author - the 2.20.3.1 fix.
- Another 23 Critical Security Vulnerabilities in Gridbox for Joomla - the July audit.
- Gridbox for Joomla: One Cookie and You Are a Super User - the July authentication bypass.

- OWASP: Cross Site Scripting (XSS) - how stored XSS works and why output has to be sanitised.
- CWE-22: Improper Limitation of a Pathname to a Restricted Directory - the path traversal weakness class.
- CWE-639: Authorization Bypass Through User-Controlled Key - the IDOR weakness class.

Frequently Asked Questions

What does Gridbox 2.20.5.0 fix?

Four security flaws in the Joomla extension plus a broad round of hardening. Two are file deletion flaws, one in the temporary attachments used by comments and reviews and one in form submission files, and two are stored cross-site scripting flaws in the front-end comment and review output. Balbooa found all four itself and rates the worst of them High.

Which Gridbox versions are affected?

Balbooa lists 2.20.4.2 and earlier as affected, with the fix in 2.20.5.0. Sites on 2.20.4.0 or 2.20.4.1 also still have the two Critical SQL injection flaws fixed in 2.20.4.2, and sites below 2.20.2 have the actively exploited July flaws as well. All of them should go straight to 2.20.5.0.

Can an anonymous visitor exploit the file deletion flaw?

In 2.20.4.2 the front-end task that removed a temporary comment or review attachment had no login check and no token check, and did not confirm that the file it was asked to delete stayed inside the uploads folder. Balbooa's fix adds path traversal validation, ownership checks and CSRF protection.

Is there a CVE?

Four ids have been assigned with the help of David Jardin of the Joomla Security Strike Team: CVE-2026-105607, CVE-2026-107129, CVE-2026-107130 and CVE-2026-107903. The records were reserved but not yet published on the morning of the release, and Balbooa does not say which id belongs to which issue. The scores in this post are our own provisional assessment until the records appear.

Have these flaws been exploited?

There is no public report of exploitation, none of the four ids is on the CISA KEV list, and neither Balbooa nor the Joomla Security Strike Team has said anything either way. If a site sat on an affected version, check for missing or changed files and for administrator accounts you did not create.



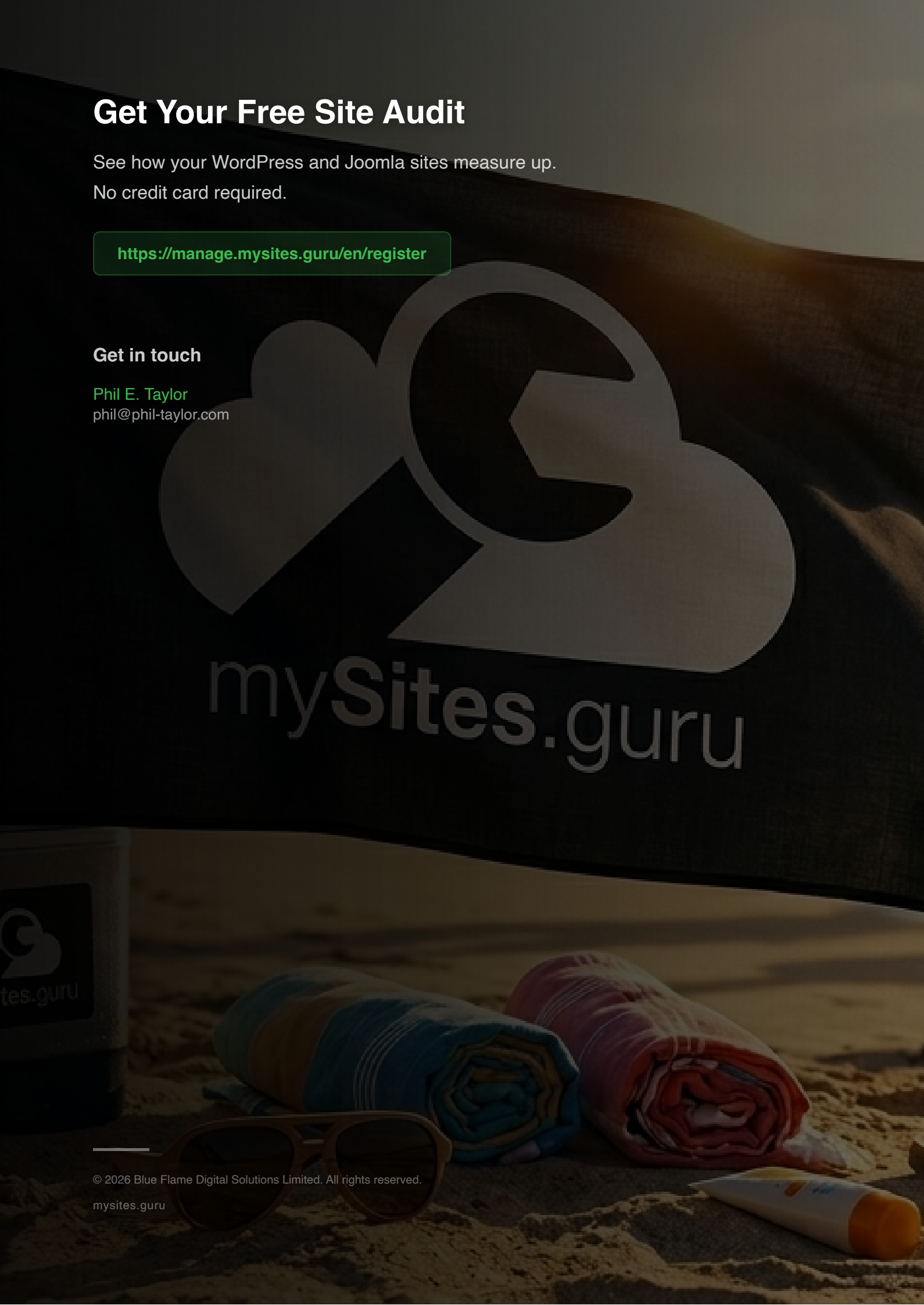
Written and edited by a human, with AI assistance. Our approach to AI

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.