mySites.guru

Another 23 Critical Security Vulnerabilities in Gridbox for Joomla

Balbooa asked us to audit Gridbox. We found 23 vulnerabilities, including a pre-auth RCE in one request. Several are being actively exploited in the wild, and the complete fix is now out in Gridbox 2.20.2. Update every Gridbox site immediately.

Phil E. Taylor | 29 July 2026

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

Gridbox is a widely used drag-and-drop page builder for Joomla, built by Balbooa. On the sites we can see it running, it is usually the thing the whole front end depends on.

Last week we disclosed a critical authentication bypass in Gridbox, CVE-2026-61425, fixed in 2.20.1. Balbooa's response to that was to ask us to look harder: they invited a full security review of the component. We did it. This is what we found, and it is worse than any of us expected.

Twenty-three distinct vulnerabilities in one Joomla extension, including a pre-authentication remote code execution reachable in a single HTTP request. It took Balbooa three attempts to close them all, and the complete fix is now out as **Gridbox 2.20.2**. It shipped into a live incident: several of these flaws are being exploited in the wild right now, which we have watched happen in server logs and on already-compromised sites, and which the Joomla Security Strike Team has confirmed. If you run Gridbox, update to 2.20.2 today and check the site for compromise.

THE HONEST VERDICT

In twenty years of taking apart Joomla extensions, I have not seen one this badly secured. Not close.

A single component that hands an anonymous visitor code execution, administrator access, and the entire user table's password hashes, by more than one route each.

We are withholding every endpoint, parameter and proof-of-concept in this post. These issues are being exploited right now, and while the fix is public as Gridbox 2.20.2, plenty of sites are still unpatched. This is how we handle every

vulnerability we find: fix first, publish second, and never hand attackers a recipe. What follows is the shape of the problem and what you need to do.

TL;DR

- Balbooa **asked us to audit Gridbox** after our earlier disclosure. We audited **2.20.2** and found **22 vulnerabilities in the one component**, and a **23rd** surfaced days later as the attacks started
- The headline is a **pre-authentication remote code execution**: one HTTP request, no account, no session, no token, and a working PHP file is written into a web-reachable folder
- There are **two more routes to code execution**, **more ways to become an administrator with no password**, and **several unauthenticated SQL injection points**, one of which returns **every user's password hash**
- Balbooa's first fix builds did **not** close everything. We re-tested each one, and several findings were still live, including an anonymous SQL injection they believed was closed. It took **three builds** to get it right, now shipped as **Gridbox 2.20.2**
- Several issues are being **actively exploited in the wild**. We have seen the attempts in server logs and connected sites with planted administrator accounts, and the **Joomla Security Strike Team** confirmed at least three. One is a **brand-new privilege escalation**: any public registrant can create an administrator account
- The **Joomla CNA has now assigned CVEs**. The first two published, CVE-2026-65884 and CVE-2026-65885, are scored **10.0** and **9.4** Critical and both carry the exploit maturity **Attacked**, which is the CVE record officially recording that these are being used against real sites
- If you run Gridbox on any Joomla site, treat it as **at risk now**, **update to Gridbox 2.20.2 immediately**, and **check for compromise**
- This is, plainly, **the worst-secured Joomla extension we have ever audited**

Balbooa asked us to look

It is only fair to tell this in order, because Balbooa did the right thing at the start.

After our Balbooa Forms disclosure earlier in July, they came back to us unprompted, said it had prompted them to review their other products, and invited us to test Gridbox. That first look turned up the authentication bypass fixed in 2.20.1. Rather than stop there, Balbooa asked us to carry out a comprehensive audit of the whole component. We agreed, and we ran it against Gridbox 2.20.2.

Inviting an outside party to break your code is a good instinct, and a rare one. We want to say that clearly, because everything after it is hard reading.

For context, these are the two Balbooa flaws we had already found and disclosed before this audit, both fixed:

Date fixed	Product	Vulnerability	CVE	Severity	Fixed in
9 Jul 2026	Balbooa Forms (`com_baforms`)	Unauthenticated file upload leading to remote code execution	CVE-2026-56291	Critical	2.4.1
20 Jul 2026	Gridbox (`com_gridbox`)	Unauthenticated authentication bypass to Super User	CVE-2026-61425	Critical, CVSS 4.0 10.0	2.20.1

The Balbooa Forms flaw came to us through a hosting abuse report on a live customer site and was being exploited before the fix shipped. The Gridbox authentication bypass was in the very build Balbooa sent us as hardened. This audit is the third chapter, and by some distance the worst of the three.

Before you count the 23, there was already a 10.0

It is worth being precise about the running total, because the 23 are not where this started.

Ten days earlier, Gridbox already had a critical of its own: CVE-2026-61425, an authentication bypass we scored at CVSS 4.0 **10.0**, the maximum there is. One cookie, `gridbox_username=admin`, and a visitor was logged in as the site's administrator with no password and no login. Balbooa shipped **2.20.1** on 20 July to close it. That release is the one that prompted the full audit, and the full audit is where the 23 came from.

So the tally for a single page builder, inside about three weeks, reads like this: a 10.0 authentication bypass fixed in 2.20.1, then twenty-three more fixed across three builds up to 2.20.2, and before either of them a critical unauthenticated file upload in the same vendor's Balbooa Forms (CVE-2026-56291, fixed in 2.4.1). Every one of those shipped as a "security release." Each fix was real. The uncomfortable part is how many of them there have had to be, and how often the first attempt did not finish the job.

That is the pattern to hold onto if you run Gridbox. The version you were on was almost always the fixed one, right up until the next release showed it was not. 2.20.2 is where the 23 are finally closed. Get onto it.

What a full audit of one extension turned up

We do not publish exploit detail before a fix is out, so this is deliberately the shape of the findings rather than the mechanics.

One request to code execution. The worst finding is an unauthenticated arbitrary file upload. No account, no session, no token, no chain. A single well-formed request writes a file the attacker controls into a folder the web server will run. That is a PHP shell on the server, and from there the site and usually the whole hosting account are gone. Balbooa already ship a safe upload helper elsewhere in the same codebase. This path never calls it.

And it is not the only route. There are two further ways to reach code execution, and more than one way to be treated as the site administrator without ever knowing a

password. Several endpoints accept unauthenticated SQL injection, and one of them returns the contents of the query in the response, which means an anonymous visitor can read every username and password hash out of the database in a single request. There is unauthenticated file reading that escapes the web root, unauthenticated recursive directory deletion, and anonymous tampering with other people's content.

The pattern is the point. These are not one author's bad day. The same class of mistake, trusting a value from the request, recurs across unrelated files written by different people. That points at a missing security standard rather than a handful of isolated slips, which is why we told Balbooa this needs a coordinated security release and not another point patch.

Credit where it is due. One part of the component is genuinely well built: the payment callback verification. Most of the gateway integrations properly verify a signature against a merchant secret or re-check the transaction server-side, and order totals are recomputed rather than trusted from the request. Whoever wrote that knew exactly what they were doing. It makes the state of the rest harder to explain, not easier.

The "fixed" build was not fixed

Balbooa sent us a build they described as fixing everything we reported, and asked us to confirm it before they published it. We re-tested every finding against the actual code.

Most were genuinely closed, and the release is a real structural rewrite in places rather than a set of sticking plasters. But several findings were still live in the build they proposed to ship. The one that matters most: an anonymous SQL injection that returns password hashes, which they believed they had fixed. They had moved the guard onto one entry point and left the identical flaw reachable through its siblings. We proved it still worked, with no login and no token, and reported that back the same evening.

An authentication fix, or an injection fix, is exactly the kind of change that can be almost right. This is the entire reason a reporter asks to verify a patch before it ships. We asked, we verified, and it was not there yet.

To their credit, Balbooa turned a second build around within a day. It closes the anonymous injection we had just proved, the registration flaw that was being exploited, and the other actively-exploited routes with it. On the things that mattered most, they moved fast, and it shows.

That second build still was not the finished release. Two problems remained in it: a payment callback that could be forged on sites configured a common way, and a SQL injection a logged-in low-privilege user could still reach. We reported both back and asked for one coordinated release that closed everything rather than another partial build.

Balbooa delivered it. **The complete fix is Gridbox 2.20.2, released 29 July.** It closes the payment bypass and the last injection along with everything else we reported. Three builds is more than anyone wants a security fix to take, but every finding we reported is closed in 2.20.2, and that is the version to be on. Anything on 2.20.1 or earlier is still exposed.

Now it is being exploited

This stopped being a disclosure story and became an incident while Balbooa was still finalising the fix.

The Joomla Security Strike Team reported that **at least three Gridbox issues are being actively exploited** in the wild and urged Balbooa to publish a fix as soon as possible. Two of the three are flaws we had already reported, one of which was in the "fixed" build. The third is new, and it is nasty in its simplicity: the registration handler adds the default group to whatever groups the visitor asks for, instead of replacing them. So **anyone can register a normal account and place themselves straight into an administrator group.** No exploit skill required, just a crafted sign-up.

We are not taking anyone's word for this, our own included. We have the server access logs showing the exploitation requests arriving, and connected sites where the accounts are already planted. On one connected Joomla site our rogue admin check is holding **92 planted accounts** right now, every one stamped by the same generator: the

username `xtw18387` plus four hex characters, with a matching `xtw18387+<hex>@outlook.com` address. They arrive in batches minutes apart. On this site the run started on 27 July, two days before the Strike Team's warning.

92 Rogue Accounts

ID	USERNAME	NAME	EMAIL	REGISTERED	WHY FLAGGED
172	xtw18387561f	xtw18387561f	xtw18387+561f@outlook.com	2026-07-27 09:19:58	Account (not currently a Super User) carrying the generated username shape of a known mass-compromise campaign (username xtw18387561f, email xtw18387+561f@outlook.com) - planted by a site compromise
173	xtw183872164	xtw183872164	xtw18387+2164@outlook.com	2026-07-27 09:20:08	Account (not currently a Super User) carrying the generated username shape of a known mass-compromise campaign (username xtw183872164, email xtw18387+2164@outlook.com) - planted by a site compromise
174	xtw183876acf	xtw183876acf	xtw18387+6acf@outlook.com	2026-07-27 10:03:14	Account (not currently a Super User) carrying the generated username shape of a known mass-compromise campaign (username xtw183876acf, email xtw18387+6acf@outlook.com) - planted by a site compromise
175	xtw18387bdcb	xtw18387bdcb	xtw18387+bdcb@outlook.com	2026-07-27 10:09:57	Account (not currently a Super User) carrying the generated username shape of a known mass-compromise campaign (username xtw18387bdcb, email xtw18387+bdcb@outlook.com) - planted by a site compromise
176	xtw183872d32	xtw183872d32	xtw18387+2d32@outlook.com	2026-07-27 10:25:05	Account (not currently a Super User) carrying the generated username shape of a known mass-compromise campaign (username xtw183872d32, email xtw18387+2d32@outlook.com) - planted by a site compromise
177	xtw1838789ee	xtw1838789ee	xtw18387+89ee@outlook.com	2026-07-27 10:40:30	Account (not currently a Super User) carrying the generated username shape of a known mass-compromise campaign (username xtw1838789ee, email xtw18387+89ee@outlook.com) - planted by a site compromise
178	xtw183876cf4	xtw183876cf4	xtw18387+6cf4@outlook.com	2026-07-27 11:07:20	Account (not currently a Super User) carrying the generated username shape of a known mass-compromise campaign (username xtw183876cf4, email xtw18387+6cf4@outlook.com) - planted by a site compromise

Look at the flag on each row: not currently a Super User. The escalation does not always take, and the accounts that fail sit in the default registration group looking like ordinary sign-ups. They are still the attacker's, and they are still a way back in. If you have ever waved past a run of odd registrations because none of them were administrators, this is what that looks like.

Find planted admin accounts across every Joomla site you manage

This is exactly what our Rogue Admin check is built for. It sweeps every connected Joomla site for accounts sitting in **any** administrator group, not just Super Users, so the sign-ups that quietly escalated show up next to the ones that failed and stayed in the registration group. You can review and delete them across all your sites from one screen.

Open the Rogue Admin check

Active exploitation changes the maths for everyone running Gridbox. The fix being out does not make you safe, applying it does. Assume attackers have already tried this on your site, update to 2.20.2, and check whether they got in before you did.

Why this is the worst we have seen

We audit Joomla extensions constantly, and we have written up a lot of serious flaws this year alone. Most extensions with a bad bug have one bad bug. What sets Gridbox apart is not any single finding, bad as the pre-auth RCE is. It is that nearly every category of critical web vulnerability is present in the same component at once, that more than one of them needs no authentication at all, that the vendor's own fix left several live, and that it is now being exploited before a complete fix is public.

In two decades of this work, that combination is unique in my experience. I do not say that for effect. I say it because if you run Gridbox, you should act as if your site is a target today.

What you should do right now

TREAT EVERY GRIDBOX SITE AS AT RISK NOW

Several of these flaws are being actively exploited and need no login. There is no configuration or firewall rule that makes an unauthenticated code-execution request safe.

Update every Gridbox site to 2.20.2 now, and check any affected site for compromise.

1. **Update Gridbox to 2.20.2** now. Joomla's Extensions updater will offer it, or download it from your Balbooa account. Balbooa's own notes are on their Gridbox security release page.

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 now**, on any site that has been running Gridbox. Look for administrator accounts you did not create, and use our Rogue Admin check to find them in any group across every connected site at once. The pre-auth RCE writes a PHP shell into a web-reachable folder, which is exactly what our Suspect Content tool is built to surface: it matches a file's contents against more than 1,500 patterns taken from real hacks, not just known-bad hashes. Our guides to finding hacked files and backdoors and fixing a hacked Joomla site walk through the whole triage.
4. **Rotate credentials** and treat the Joomla secret as exposed on any busy site that has been reachable while running an affected version. Anyone who got in will have left themselves a way back, so do not assume a single clean file scan means they are gone, check every crontab, not just yours, and watch for reinfection.
5. **Consider disabling Gridbox** on any high-value site you cannot patch immediately, if the design can tolerate it, until the fixed release is installed.

How do I find every Gridbox site I manage?

The awkward question after any extension flaw is which of your sites actually run the thing. Past about ten sites, logging into each Joomla admin to read the extensions list stops being realistic, which is exactly how old versions survive.

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. Across the Joomla sites we manage, **several hundred** run Gridbox, which is a lot of sites to reach one at a time while a flaw is being exploited.

View every Gridbox install across your sites

Open your Extension Inventory

Search for Gridbox across every connected Joomla site and find anything on an affected version. Not a subscriber? Sign up free and connect your sites.

We have added the affected range, every version below 2.20.2, 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.

Stay ahead of the next one

There will be another one. Joomla runs on thousands of third-party extensions, and the ones that accept anonymous input keep producing findings like this. The hard part was never the update. It is knowing a fix exists at all, then knowing which of your sites are affected and getting to them first, before someone else does.

Get free email alerts when a Joomla extension flaw 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.

The 23 vulnerabilities in full

Here is the complete set, described by class and impact rather than by exploit detail. Thirteen of these were proved live against a test install; the rest were read in the source during the audit. “Access required” is what an attacker needs before they can use it, and “None (anonymous)” means no account and no login at all.

#	Vulnerability	Class	Access required
1	File upload written into a web-reachable folder, in one request	Remote code execution	None (anonymous)
2	SQL injection that returns every user's password hash in the response	SQL injection	None (anonymous)
3	Password reset of any account	Account takeover	None (anonymous)
4	Login as any user, including an administrator	Authentication bypass	None (anonymous)
5	File upload with no extension check	Remote code execution	Author
6	Arbitrary file write (the vendor's earlier fix was incomplete)	Remote code execution	Editor
7	Administrator password hash exposed through a client-readable cookie	Credential disclosure	Any XSS or log access
8	Recursive directory deletion	Destructive file operation	None (anonymous)
9	Arbitrary file read that escapes the web root	Information disclosure	None (anonymous)
10	A second unauthenticated SQL injection	SQL injection	None (anonymous)
11	Forging ownership of other users' comments and reviews	Data tampering	None (anonymous)
12	Full server filesystem enumeration	Information disclosure	None (anonymous)
13	Path and exception information disclosure	Information disclosure	None (anonymous)
14	Five further SQL injection points	SQL injection	None (anonymous)

#	Vulnerability	Class	Access required
15	Arbitrary font and file upload	Remote code execution	Editor
16	Arbitrary extension installation	Remote code execution	Backend user
17	Arbitrary file read and delete	Information disclosure / destructive	Backend user
18	Forgeable payment signature with no shared secret required	Payment bypass	None (anonymous)
19	Payment transaction not bound to the order	Payment bypass	None (anonymous)
20	TLS certificate verification disabled on gateway calls	Transport security	Network position
21	Stored cross-site scripting via a comment avatar	Cross-site scripting	None (anonymous)
22	No CSRF protection anywhere in the administrator area	Cross-site request forgery	Tricking a logged-in admin
23	Registration that puts the visitor in whatever group they ask for, including an administrator group	Privilege escalation	None (anonymous)

Number 23 is not from the audit. It surfaced alongside the active exploitation: the registration handler adds the default group to whatever groups a visitor asks for instead of replacing them, so **any public user can register themselves straight into an administrator group**. That one, the arbitrary file read (9), and the arbitrary file write (6) are the three the Joomla Security Strike Team reports are being exploited right now.

The CVE assignments

The Joomla CNA has now assigned CVE IDs for this set. It has grouped them by shared root cause rather than issuing one per finding, on the reasoning that most of these are the same systemic gap repeating: no access control on the task, no CSRF token, no check on what the request is asking the component to do. So the CVE count is lower than the count of vulnerabilities, and one ID can cover several rows of the table above.

Two records have published so far, and both are Critical:

CVE	What it covers	CVSS 4.0	CWE
CVE-2026-65884	Registration accepts the user's own group IDs, so an anonymous visitor can sign up with administrator permissions. This is number 23 in the table above, the one being exploited in the wild	**10.0 Critical**, exploit maturity Attacked	CWE-284 Improper Access Control
CVE-2026-65885	Authenticated arbitrary file upload. The record notes it becomes remote code execution when chained with CVE-2026-65884, because the account it needs is one the attacker can create for themselves	**9.4 Critical**, exploit maturity Attacked	CWE-434 Unrestricted Upload of File with Dangerous Type

Two details in those records are worth pulling out. Both list the affected range as **1.0.0 to 2.20.1**, which is every Gridbox release there has ever been up to the fix. And both set the exploit maturity to **Attacked** with an urgency of Red, which is the CVE record's own way of recording that this is being used against real sites rather than sitting as a theoretical risk. That is independent corroboration of what we were seeing in the logs.

Nine further IDs are reserved against these findings and have not published yet: CVE-2026-65886, CVE-2026-65887, CVE-2026-65888, CVE-2026-65889, CVE-2026-65890, CVE-2026-65947, CVE-2026-66488, CVE-2026-66489 and CVE-2026-66490. Until they go live there is no public mapping of which ID covers which finding, so treat the list above as the part you can act on today. We will update this post as the rest publish.

Disclosure and Severity

10.0
CVSS 4.0

CRITICAL

The Joomla CNA's score for CVE-2026-65884, and our own for the pre-auth RCE

The published CVE record for the registration privilege escalation is scored 10.0 with the exploit maturity set to Attacked. We independently scored the worst of the twenty-three, an unauthenticated arbitrary file upload, at the same 10.0: exploitable over the internet in a single request, with no account and no user interaction, yielding remote code execution. Several other findings need no login either, and the Joomla Security Strike Team reports at least three are being actively exploited.

No login needed | Single request | Remote code execution | Actively exploited | No firewall mitigation

Field	Detail
Extension	Gridbox for Joomla (`com_gridbox`)
Vendor	Balbooa (balbooa.com)
Findings	23: 22 from the audit, plus a 23rd privilege escalation surfaced by the active exploitation
Headline type	Unauthenticated file upload leading to remote code execution (CWE-434), alongside SQL injection (CWE-89) and authentication bypass (CWE-287)
CVSS 4.0	10.0 (Critical) for CVE-2026-65884, scored by the Joomla CNA. 9.4 (Critical) for CVE-2026-65885. We separately scored the headline pre-auth RCE at 10.0
CVE	CVE-2026-65884 and CVE-2026-65885 published by the Joomla CNA on 29 July, with nine more IDs reserved and grouped by shared root cause. The earlier authentication bypass is CVE-2026-61425
Impact	Unauthenticated remote code execution, administrator takeover, and disclosure of every user's password hash

Field	Detail
Active exploitation	Observed by mySites.guru in server access logs and on compromised sites, reported by the Joomla Security Strike Team on 29 July 2026 (at least three issues), and recorded in both published CVE records as exploit maturity Attacked with an urgency of Red
Audited in	Gridbox 2.20.2
Affected versions	Every version below 2.20.2. The CVE records state the range as 1.0.0 to 2.20.1
Fixed in	Gridbox 2.20.2, see Balbooa's security release announcement
Finder	Phil Taylor, mySites.guru. The published CVE records credit Phil Taylor and Pascal Lohmann

Further Reading

- Balbooa's Gridbox 2.20.2 security release - the vendor's own advisory and the fixed download.
- CVE-2026-65884 and CVE-2026-65885 - the first two published records for these findings, both Critical and both marked as being exploited.
- Gridbox: one cookie and you are a Super User - the earlier authentication bypass, CVE-2026-61425, that led to this audit.
- Our Balbooa Forms disclosure - the same vendor, the flaw that started the whole exchange.
- Finding rogue admin accounts across every Joomla site - the tool we used to spot the planted accounts in this attack, in any group and not just Super Users.
- Suspect content vs hacked files - the two tools for finding the shells a file-upload RCE leaves behind.
- Hacked yesterday, exploited today - how quickly disclosure turns into exploitation, which is the whole reason we fix before we publish.

- A month of Joomla extension vulnerabilities - the wider run of findings this is part of.
- How to fix a hacked Joomla or WordPress site - what to do if a site running Gridbox has already been hit.
- Joomla Security Strike Team - who reported the active exploitation.

Frequently Asked Questions

How many vulnerabilities were found in Gridbox?

Twenty-three, all in a single component. Twenty-two came out of the full security audit of Gridbox 2.20.2 that Balbooa asked us to carry out, and a twenty-third, a registration flaw that lets any visitor sign themselves into an administrator group, surfaced when the attacks started. They include a pre-authentication remote code execution reachable in one HTTP request, two more routes to code execution, more ways to become the site administrator without a password, and several unauthenticated SQL injection points, one of which returns every user's password hash. Several are being actively exploited in the wild: we have seen the attempts in server access logs and connected Joomla sites where attackers had already planted administrator accounts, and the Joomla Security Strike Team reported at least three under active exploitation. The complete fix is Gridbox 2.20.2.

Is Gridbox being actively exploited?

Yes. We have direct evidence of it: exploitation attempts in server access logs and connected Joomla sites where attackers had already planted administrator accounts. The Joomla Security Strike Team has also reported that at least three Gridbox issues are being actively exploited, including a privilege escalation that lets any public registrant create an administrator account. The complete fix is Gridbox 2.20.2. Update every Gridbox site to it now and check for compromise.

Which CVEs cover the Gridbox vulnerabilities?

The Joomla CNA has assigned CVE IDs for this set, grouped by shared root cause rather than one per finding, so there are fewer CVEs than vulnerabilities. Two have published so far. CVE-2026-65884 is the registration flaw that lets an anonymous visitor create an account with administrator permissions, scored CVSS 4.0 10.0 Critical. CVE-2026-65885 is an authenticated arbitrary file upload scored 9.4 Critical, which chains with the first one into remote code execution because the account it needs is one the attacker can create for themselves. Both records carry the exploit maturity Attacked, the CVE record's own marker that exploitation is already underway, and both list every version from 1.0.0 to 2.20.1 as affected. Nine further IDs are reserved and not yet public. The earlier Gridbox authentication bypass is CVE-2026-61425, fixed in 2.20.1.

What should I do if I run Gridbox?

Update Gridbox to 2.20.2 immediately, then check any site that has been running an affected version for signs of compromise: administrator accounts you did not create, PHP

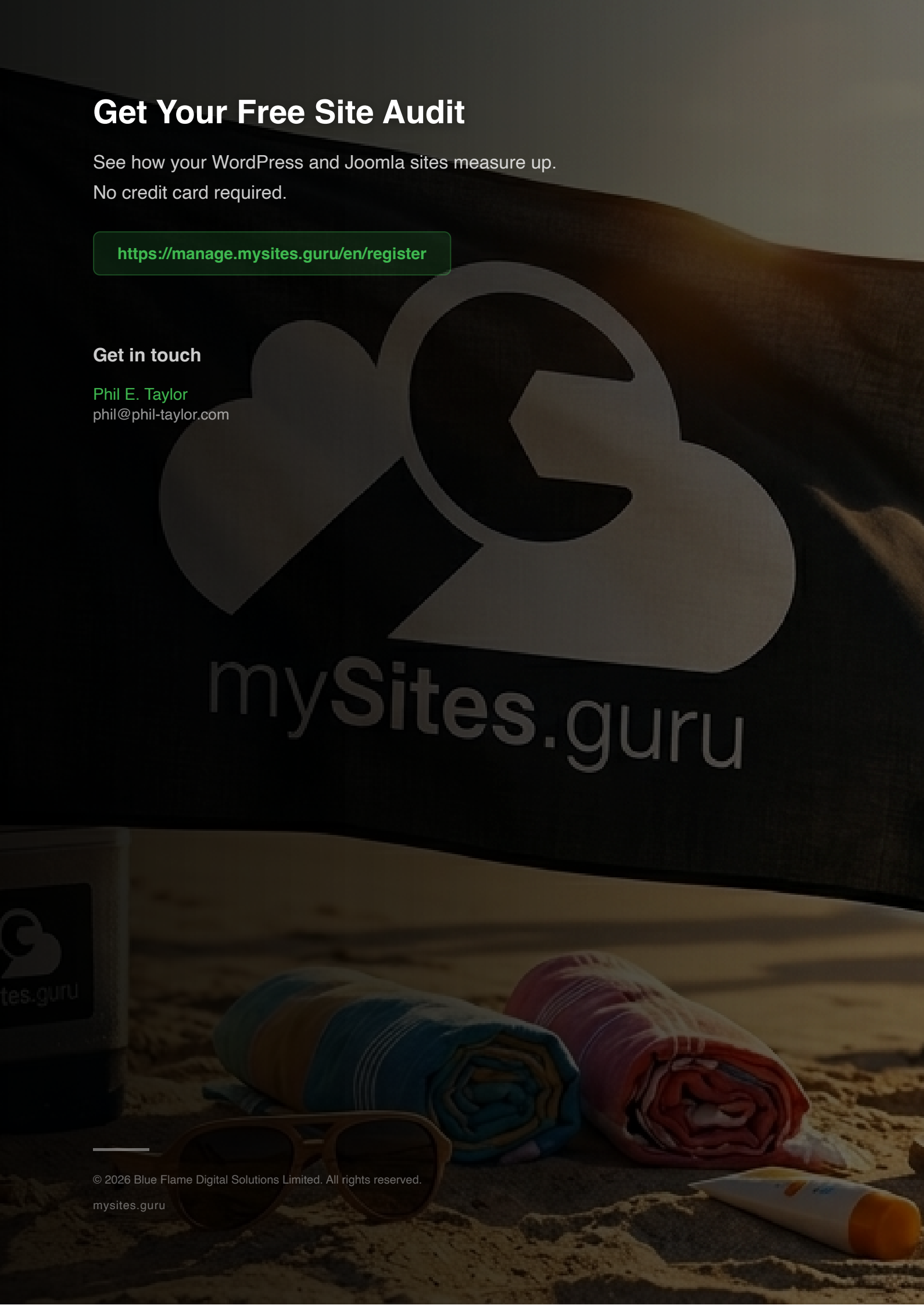
files in upload folders, recently modified files, and logins you cannot account for. mySites.guru flags every connected site running an affected version, finds rogue admin accounts across all of them from one screen, and lets you update them all at once.

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