mySites.guru

Events Booking for Joomla exposes personal and financial data from invoices

An unauthenticated flaw in Events Booking for Joomla let anyone download any registrant's invoice, with their name, address, email and payment. Fixed in 5.8.2.

Phil E. Taylor | 21 July 2026

Active Joomla Extension security alerts: Sixteen and counting this month • **JCE** • **Quix** • **SP Page Builder**

Events Booking is one of the most widely used event registration and ticketing components for Joomla. It runs conference sign-ups, class bookings and ticket sales, so the records it holds belong to real attendees who handed over their details, and often their money, to book something. During security research on the extensions our customers rely on, **mySites.guru found an unauthenticated flaw in Events Booking that let anyone download any registrant's invoice**, reported it privately to JoomDonation, and it is now fixed in **Events Booking 5.8.2**. It is the third issue we have found and reported in this one component this month.

This one came straight on the heels of the last round. We had only just finished reporting the anonymous file upload and user-enumeration flaws. We got the 5.8.1 source the way we get a lot of things: a mySites.guru subscriber sent it over. Reading that code is exactly how this invoice flaw surfaced, which is worth sitting with for a moment. The release we could not get handed to us to check turned out to contain a fresh unauthenticated hole of its own.

An invoice is not a small thing to leak. It carries the attendee's full name, their organisation, their postal address, their email address and the amount they paid. The front-end page that generates that invoice as a PDF decided what to hand over from the registration ID number in the web address, and it never properly checked that the person asking was entitled to it. So a stranger with no account could pull up any registration's invoice by changing the ID number, then count up through the numbers to collect the lot.

mySites.guru discovered this issue and reported it privately to JoomDonation, who fixed it in Events Booking 5.8.2. As with every flaw we find, we withheld the exact request and any proof-of-concept and waited for a fix before publishing. Update to 5.8.2. A CVE has been applied for via the Joomla CNA. This is how we

handle every vulnerability we find: report first, publish second, and never ship a recipe.

TL;DR

- **Anyone could download any registrant's invoice.** The front-end invoice download handed over a registration's invoice PDF based on the ID number in the web address, without properly checking that the requester owned it. No login, no account, no special access
- **Each invoice is a full billing identity.** Name, organisation, postal address, email address and payment amount, for every registration that had an invoice
- **Count up through the IDs and you had the lot.** There was nothing to stop a short script walking the ID range and collecting every invoice on the site
- **A separate, third issue.** This is distinct from the anonymous upload and user-enumeration flaws we reported earlier this month, which were fixed in 5.8.0 and 5.8.1. **This one is fixed in 5.8.2**
- **If you already updated for the earlier flaws, update again.** Those releases did not touch the invoice flaw, so a site on 5.8.1 is still exposed until it reaches 5.8.2
- **If you cannot update immediately, turn off invoicing** as an interim measure. A firewall has nothing to block here, because there is no malformed payload, just an ordinary request for a document
- **This was potentially a reportable data breach** for any site that ran invoicing on an affected version. Invoices are personal data under the UK and EU GDPR, and the exposure is silent
- Found by reviewing the 5.8.1 source, which reached us from a subscriber rather than the vendor. Reported privately on 20 July 2026, **fixed in 5.8.2**, **CVE applied for** via the Joomla CNA. No proof-of-concept released

What the flaw was

Events Booking can issue a PDF invoice for a registration. When the invoice feature is switched on, a registrant who has paid gets an invoice, and there is a front-end page that serves it back as a download.

That page was where the problem sat. It worked out which invoice to return from the numeric registration ID passed in the request, loaded that registration, and generated the PDF. The access check that was supposed to guard it was an authorisation failure: it confirmed that a download code was supplied, but not that the code actually belonged to the registration being requested. A code is meant to be the per-registration secret that proves you own the booking. Here, any value in that slot satisfied the check, while the invoice itself was chosen by the ID number. The two were never compared.

The result was a classic insecure direct object reference. The server handed the document to whoever asked, based on a number the caller controlled, and the number was sequential. There was no login check, no CSRF token and, critically, no ownership check. The component's own pages only ever request the invoice for a booking the visitor actually made, so in normal use it looked harmless. The server never enforced what the browser assumed.

THE WHOLE FLAW IN ONE LINE

The invoice download checked that a code was supplied, not that it belonged to the invoice, so the document was handed to anyone who asked for it by ID number.

We are withholding the exact request and any working proof-of-concept even though it is fixed. This section is enough to understand the risk and act on it, and not enough to be a recipe against sites that have not updated yet.

We proved it against a clean install of Events Booking 5.8.1 to be sure it was real and not a quirk of one configuration. To keep the lab honest we created a single test registration, retrieved its invoice as an anonymous visitor, confirmed the personal and

payment details were all present, and removed the test data afterwards. We did not touch any live site, and there is no site of yours involved in this research.

For contrast, the sibling invoice-style downloads in the same component, the certificate and the ticket, were not affected. They work out the registration from the code itself rather than trusting a separate ID number, so a wrong code simply resolves to no record. The invoice download was the one place where the ID chose the document and the code was only checked for being present. One inconsistent check is all it takes.

Update to 5.8.2

Earlier in July we reported two other unauthenticated flaws in Events Booking, an anonymous file upload that was on by default and a leak of every user's name and email. Those were fixed across 5.8.0 and 5.8.1. This invoice flaw is separate, and it is fixed in 5.8.2. If you updated to 5.8.1 for the earlier flaws and assumed Events Booking was sorted, this one was still open on your site until 5.8.2, so update again.

There is one wrinkle worth knowing if you go looking at the files. The 5.8.1 you have is not necessarily the 5.8.1 someone else has. Somewhere between our private report on 20 July and the official 5.8.2 release, JoomDonation backported the same fix into the 5.8.1 package without changing its version number. So for a period the 5.8.1 on the download server was the insecure build we proved the flaw against, and after that the 5.8.1 on the download server carried the fix, both under the one version string. A site reading "5.8.1" in its admin cannot tell you which of the two it installed. Updating to 5.8.2 is what removes the doubt: it is the release where the fix and the version number line up.

DO THIS NOW

Update Events Booking to 5.8.2 on every site, including any you already took to 5.8.1.

Run the update through System, Update, Extensions in each site's Joomla admin, and confirm the version under Components, Events Booking afterwards.

> If you cannot update straight away, turn off the invoice feature in the Events Booking configuration as an interim measure and switch it back on once you are on 5.8.2.

A firewall or .htaccess would not have stopped your invoices being exposed!

A word on firewalls, because it is the first question we get. A web application firewall is worth having, but it would not have saved you here. There was no SQL, no script tag, no malformed payload for it to catch. The attacker was asking for a document the site is designed to serve, at a URL that looked completely ordinary, and simply changing one number. Rules that block injection attempts have nothing to match on. The update is the fix, not the firewall.

An .htaccess file is the other thing people reach for, and it deserves its own mention because so many site owners treat one as a security blanket. It can deny access to a folder or block a file type, which genuinely helps against some attacks, but it had nothing to work with here. The invoice download was an ordinary, permitted request to an ordinary, permitted URL, so there was no forbidden path to deny and no extension to filter. We have written before about why your .htaccess will not stop a Joomla hack, and this is a clean example. The invoice feature was working exactly as built, just answering the wrong person, and a directory rule cannot see that.

Knowing which of your sites need it

The awkward part of a security release is that “we updated Events Booking” is not the same as “every site is on 5.8.2”. You need to know precisely which sites run Events Booking, which ones are still below 5.8.2, and get to each of them.

That is the job mySites.guru does. It keeps a live inventory of every extension and version on every Joomla and WordPress site in your account, so you can search for Events Booking once and see every site running it, and the version each is on, in

seconds, without opening a single admin panel. We have added this issue to our Joomla vulnerability database, so every connected site below 5.8.2 is flagged automatically, and the mass updater rolls the update out from one screen. You should not have to read about a Joomla security issue and then audit a portfolio of client sites by hand to find out whether it is your problem, still less do it three times for the same extension in one month.

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.

Booking components leak your customers, not just your site

We keep finding this class of bug in the extensions built to talk to strangers, and it is worth being explicit about why booking and registration components carry a heavier consequence than most.

A page builder flaw leaks your site. A booking component flaw leaks your customers. The whole purpose of the extension is to collect personal details from the public, and take their money, and store both. So the data at risk was never yours in the first place, it was entrusted to you. The same logic runs through the newsletter tools, form builders and document managers where we keep finding the same pattern this month: AcyMailing, Balbooa Forms, EDocman, DPCalendar. They are all built to talk to strangers, so a missing check in one of them talks to strangers too. The recurring shape is an AJAX or front-end endpoint that trusts the browser instead of re-checking on the server.

None of that is an argument for avoiding Events Booking. It is a capable, long-established component, and much of the code we have reviewed is in better shape than most of what we audit, with the payment verification in particular done properly. Capable software still ships ordinary bugs, and an authorisation check that confirms the wrong thing is about as ordinary as they come. The point is not that the extension is bad. It is that the invoices it holds are your legal responsibility, and one inconsistent check handed them out until 5.8.2 closed it.

What to do right now

- **Update Events Booking to 5.8.2** or later on every affected site. This is the fix, and it is the one action that actually closes the invoice flaw
- **Update even if you already went to 5.8.1.** That earlier release fixed the anonymous upload and user-enumeration flaws and not this one, so 5.8.1 is not far enough
- **If you cannot update immediately**, turn off the invoice feature in the Events Booking configuration as an interim measure, and switch it back on once you are on 5.8.2
- **Do not rely on a firewall for this one.** There was no payload to filter, so there was nothing for it to block
- **Treat past invoices as potentially read.** If a site ran the invoice feature on a public event while on an affected version, assume the invoices could have been collected, and talk to whoever owns data protection where you work
- **If you manage multiple sites**, let mySites.guru show you which ones are still below 5.8.2 rather than checking by hand

Disclosure and Severity

HIGH Our own assessment; CVE applied for, fixed in 5.8.2

8.7
CVSS 4.0

Unauthenticated and exploitable over the internet in a single request with no user interaction. It exposed the full billing details of every invoiced registrant, which is a serious loss of confidentiality, but it was a read-only disclosure with no write or availability impact, which is what keeps it out of the critical range.

No login needed | Exploitable over the internet | Fixed in 5.8.2 | Personal and financial data | No firewall mitigation

Our assessment is **CVSS 4.0 8.7 (High)**, vector `AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N`. Reachable over the network (`AV:N`) with no added complexity or attack requirements (`AC:L`, `AT:N`), needing no privileges (`PR:N`) and no user interaction (`UI:N`). It causes a high loss of confidentiality on the vulnerable system (`VC:H`), the full billing details of every invoiced registrant, with no integrity or availability impact (`VI:N`, `VA:N`) and nothing carried into a downstream system (`SC:N`, `SI:N`, `SA:N`). The read-only nature is what holds it below the critical range. The Joomla CNA will assign its own score alongside the CVE.

Field	Detail
CVE	Applied for via the Joomla CNA, not yet assigned, crediting Phil Taylor of mySites.guru
Component	Events Booking for Joomla (`com_eventbooking`)
Vendor	JoomDonation / Ossolution (joomdonation.com)
Type	Authorisation bypass through a user-controlled key (CWE-639), an insecure direct object reference
CVSS 4.0	8.7 (High), `AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N` (our own assessment)
Impact	Anonymous read of any registrant's invoice, including full name, organisation, postal address, email address and payment amount
Finder	Phil Taylor, mySites.guru
Affected versions	Every release up to and including 5.8.1 with the invoice feature in use

Field	Detail
Fixed in	5.8.2

We follow a report-first, publish-second process: private disclosure to the vendor, a window for a patch, then a public write-up without a proof-of-concept.

Date	Event
20 July 2026	A mySites.guru subscriber sends over the Events Booking 5.8.1 source. Reviewing it, mySites.guru identifies and confirms a separate authorisation flaw in the invoice download, proven on a clean install with test data only and no live site involved.
20 July 2026	mySites.guru reports the invoice flaw privately to JoomDonation, with all public detail withheld. JoomDonation confirms it the same day.
21 July 2026	JoomDonation ships the fix in Events Booking 5.8.2, adding the missing ownership check to the invoice download. mySites.guru confirms a wrong code now resolves to no invoice, and applies for a CVE via the Joomla CNA.
21 July 2026	mySites.guru publishes this write-up. No proof-of-concept is released.

Further Reading

- The Events Booking upload and enumeration flaws fixed in 5.8.1 - the two issues that earlier release did close, and the disclosure story behind them.
- A month of Joomla extension vulnerabilities we found and disclosed - the full run this is part of.
- Why AJAX endpoints are a CMS security blind spot - the recurring public-endpoint pattern behind findings like this.
- CWE-639: Authorization Bypass Through User-Controlled Key and the OWASP IDOR Prevention Cheat Sheet - the canonical references for this weakness class.
- OWASP Vulnerability Disclosure Cheat Sheet and the CERT Guide to Coordinated Vulnerability Disclosure - the practice behind the report-first process above.

- Events Booking product page - the vendor's official page, where 5.8.2 is available to download.

Frequently Asked Questions

What is the Events Booking invoice flaw?

It was an unauthenticated access control flaw in Events Booking for Joomla by JoomDonation. The front-end page that serves a registration's invoice as a PDF decided what to hand over from the registration ID in the web address, and it did not properly check that the person asking was entitled to that invoice. So an anonymous visitor, with no account and no login, could download any registrant's invoice by changing the ID number, and step through the numbers to collect the lot. Each invoice carries the registrant's full name, organisation, postal address, email address and the amount they paid. It is fixed in Events Booking 5.8.2.

Is this the same as the earlier Events Booking flaws?

No, it is a separate, third issue. Earlier in July we reported an anonymous file upload and a user-enumeration flaw in Events Booking, which were fixed across 5.8.0 and 5.8.1. This invoice flaw is different, and it is fixed in 5.8.2. If you already updated to 5.8.1 for the earlier flaws, update again to 5.8.2 to close this one.

How do I protect my site?

Update Events Booking to 5.8.2 or later, which is the fix. In each site, run the update through System, Update, Extensions in the Joomla admin. If you cannot update immediately, turn off the invoice feature as an interim measure: open Components, Events Booking, Configuration and switch off the setting that generates downloadable PDF invoices. Turn it back on once you are on 5.8.2.

Is this a reportable data breach?

It can be. An invoice holds a named person's postal address, email address and a payment amount, which under the UK GDPR and the EU GDPR is personal data you are the controller of. If your site ran the invoice feature on a public event while on an affected version, an unauthenticated stranger being able to read those invoices is a personal data breach you are expected to assess, and potentially report to your regulator within 72 hours. The exposure is silent, so most sites cannot tell from their logs alone whether anyone did it.

How do I find every Events Booking site I manage?

mySites.guru keeps a live inventory of every extension and version on every connected Joomla and WordPress site. Search for Events Booking once and get back every site running it and the version each is on. Every connected site below 5.8.2 is flagged automatically

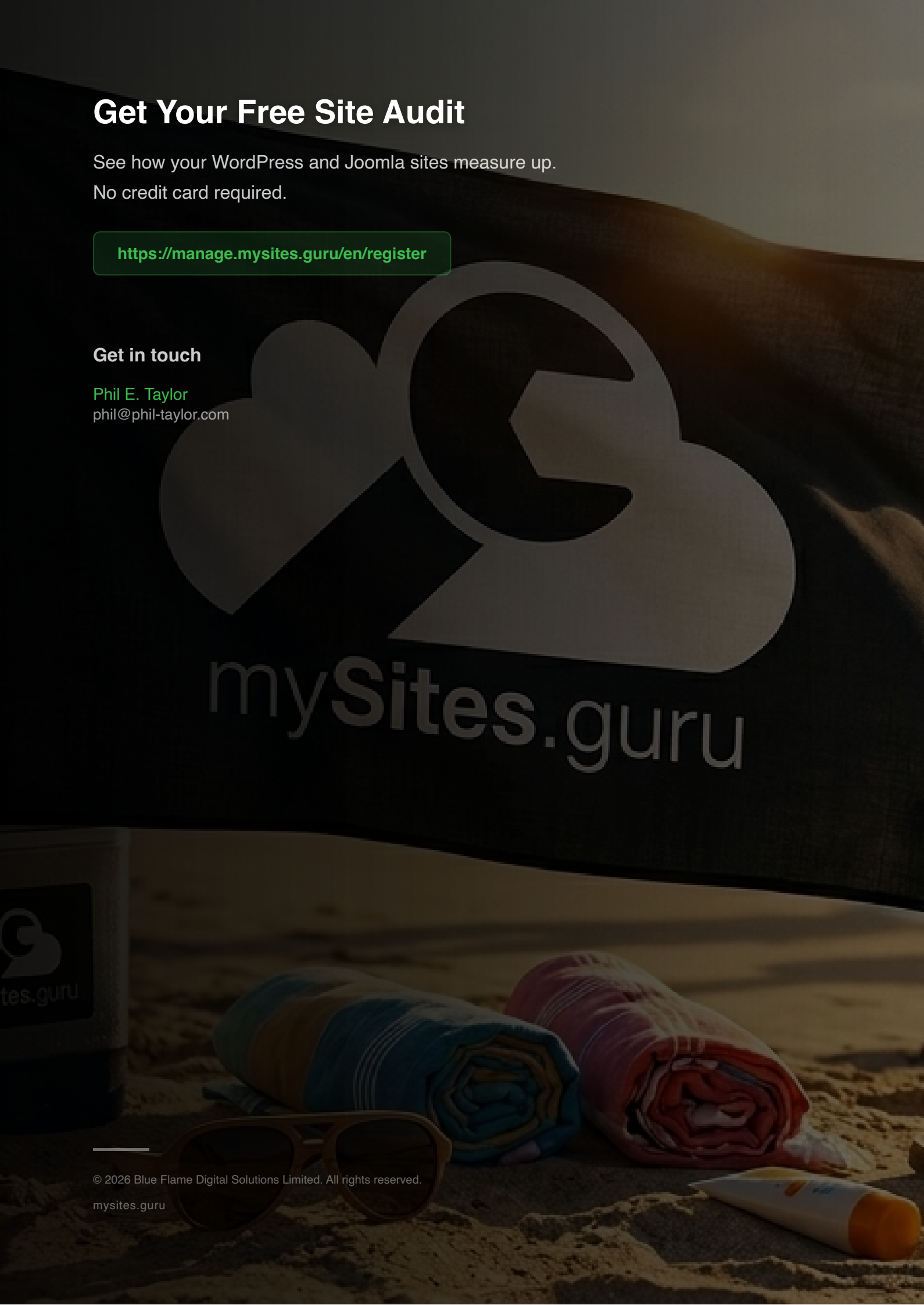
against our vulnerability database, so you do not have to check a portfolio of client sites by hand.

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