mySites.guru

Vik Booking 1.18.21 stops guests saving script as a check-in signature

Vik Booking 1.18.21 for Joomla fixes a stored XSS in guest check-in signatures and adds CSRF checks to invoice tasks. Fourth security release in 22 days.

Phil E. Taylor | 11 November 2026

On 11 November 2026 E4J released Vik Booking 1.18.21 for Joomla, the fourth security release for the hotel booking extension in 22 days. The changelog gives the security work three short lines: “SVG and images sanitising techniques”, “Various CSRF and capability checks added” and “Various fixes and value escapings applied”. It does not say what was wrong, or who could reach it.

The first of those lines covers a flaw a guest could reach. Until 1.18.21 a guest with a confirmed booking could submit an SVG containing script as their check-in signature, and Vik Booking saved it unchanged in a folder under `/administrator/` on the site’s own domain. The fix is E4J’s work. The detail below comes from the public WordPress build of the same code, which E4J release on the same day.

TL;DR

- E4J released **Vik Booking 1.18.21** for Joomla on 11 November 2026, with WordPress build 1.8.21 the same day and an identical changelog
- It is the **fourth security release in 22 days**: 1.18.17 (20 October), 1.18.18 (21 October), 1.18.19 (26 October) and now 1.18.21
- The **guest signature** feature accepted an SVG and wrote it to disk as it arrived. A guest with a confirmed booking could store script in a `.svg` file served from the site’s own domain. It runs only when someone opens the file URL directly
- The back-end **invoice tasks** had no CSRF token check and no permission check. Both were added
- **No CVE** for either. Our CVSS 4.0 assessment is 5.1 Medium for each
- Across the Joomla sites we manage that run Vik Booking, about **62% are below 1.18.17** and have missed all four releases

5.1	**Vik Booking: stored XSS through an SVG check-in signature (no CVE)**

CVSS 4.0

MEDIUM mySites.guru assessment

The guest signature feature accepted an SVG and saved its bytes unchanged in a folder inside the web root, under /administrator/. A guest with a confirmed booking could store a .svg file containing script on the site's own domain. The script runs when someone opens the file URL directly, and a logged-in administrator who does so gives it their session.

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

Needs a confirmed booking, no account

Fires when the file is opened directly

Fixed in 1.18.21

▼ 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:P` Present: Needs a particular deployment or race to line up
`PR:N` None: No account needed
`UI:A` Active: Someone has to be talked through a few steps

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:H` High: Data on other systems can be read
`SI:H` High: Other systems can be altered
`SA:N` None: Other systems stay up

5.1 CVSS 4.0

Vik Booking: back-end invoice tasks with no CSRF token or capability check (no CVE)

MEDIUM mySites.guru assessment

The tasks that generate, re-send and download invoices accepted a request with no CSRF token, so a logged-in administrator could

be tricked into one from another site. They also had no permission check, so any back-end user could reach them without the management permission.

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

Needs a logged-in administrator to be tricked

Invoices generated or re-sent | Fixed in 1.18.21

▼ 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:A` Active: Someone has to be talked through a few steps

What it does to the site

`VC:N` None: Nothing can be read
`VI:L` Low: Some data can be altered
`VA:N` None: The site stays up

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

What changed in Vik Booking 1.18.21

Vik Booking 1.18.21 for Joomla pairs with 1.8.21 of the WordPress plugin, and the code comments say so directly: “@since 1.18.21 (J) - 1.8.21 (WP)”. Beyond the three security lines, the changelog lists four changes that support them:

- “New transient tokens model.”
- “New booking details SID default format with dedicated hook for adopting a custom format.”

- “New configuration setting for keeping certain guests related media files above the web-root directory.”
- “New configuration setting “booking details link expiration days”.”

The remaining lines are features: PMS reports, door access codes and a task manager hook.

> **What we did and did not check**
>
> The detail in this post comes from the public WordPress 1.8.20 and 1.8.21 packages of Vik Booking. The Joomla packages are commercial, so the Joomla pairing comes from the code’s own comments. We have not tested anything against a live site and are not publishing a working request.

How a Vik Booking guest signature became a script file

Vik Booking lets a guest sign at check-in. The front-end task `storesignature` and the pre-check-in controller, `site/controllers/checkin.php`, take the signature as a base64 data URI and accept three types: png, jpg or jpeg, and svg. A code comment dates that format list to 1.15.1.

Before 1.18.21 the decoded bytes were written to disk as they arrived. The file went into `administrator/components/com_vikbooking/resources/idscans/`, a folder inside the web root, named after the booking id, the booking SID and the customer id, with its extension taken from the submitted type. An SVG is an image format that can contain script, so an SVG with script inside it became a `.svg` file served from the site’s own domain.

The code sets conditions. The request needs a valid CSRF form token, which anyone on the signature page has. The booking’s sid and ts must match, its status must be “confirmed”, its check-out must not have passed, and a customer record must be linked to it. No Joomla account is involved. Getting a confirmed booking can mean making an ordinary one and, on sites that take payment up front, paying for it.

What keeps this at Medium is how the script fires. The site and administrator pages show the signature through an `<img>` tag, which does not run script. It runs when someone opens the file URL directly, for example from a link they are sent. Because the file is under `/administrator/` on the site's own origin, a logged-in administrator who opens it gives the script their session.

How did Vik Booking 1.18.21 fix the signature upload?

A new function, `VikBooking::sanitizeImageBytes()`, checks that the bytes match the declared type. For an SVG it rejects any DOCTYPE or ENTITY declaration, then rebuilds the image with DOMDocument from an allowlist of drawing tags in the SVG namespace: svg, g, path, polyline, polygon, line, rect, circle and ellipse. Any other tag or attribute is removed. The function is applied in `storesignature`, in the pre-check-in controller and in the back-end `createcheckindoc` task.

The new configuration setting goes further and moves guest media files above the web root altogether. They are then served through a new `mediafiles` controller that requires a token and the `core.vbo.bookings` permission.

Two smaller front-end changes sit alongside. Values submitted in the booking form's custom fields now go through `strip_tags`, and the field keys of the front-end inquiry form are filtered to letters, digits, underscore and hyphen. Booking extensions take files and free text from strangers by design, and Vik Booking is not the only one caught out by it: Events Booking had its own unauthenticated upload problem.

The back-end invoice tasks in Vik Booking 1.18.21

"Various CSRF and capability checks added" covers the administrator side. The invoice tasks `geninvoices`, `resendinvoices` and `downloadinvoices` gained a CSRF token check and a `core.vbo.management` permission check. Before, a logged-in administrator could be tricked into a request from another site that generated, re-sent or downloaded invoices, and a back-end user without the management permission could reach the same tasks.

Creating a booking from the calendar view now needs a token and the `core.vbo.bookings` permission, and creating rates from the tariffs view now needs a token. Several back-end views gained output escaping as well.

Four Vik Booking security releases in 22 days

The run started with 1.18.17 on 20 October 2026. 1.18.18 followed on 21 October with “Fixes applied for the automated security plugin review findings.”, and 1.18.19 on 26 October with “XSS prevention with custom fields management functions.” 1.18.21 on 11 November makes four in 22 days.

There is no Joomla 1.18.20. The WordPress build had a 1.8.20 on 27 October, listing “Fixed invalid capability check affecting front-end pages.” and “Security improvements.”, and the front-end change we saw in it was the booking room-options parameter being validated as numeric. The Joomla numbering goes straight from 1.18.19 to 1.18.21.

We covered the first three releases in the 1.18.19 post.



Vik Booking 1.18.19 is its third security release in a week, with fixes for Vik Rent Car and Vik Rent Items

Vik Booking 1.18.19, Vik Rent Car 1.15.13 and Vik Rent Items 1.8.6 fix a CSRF gap and stored XSS. Three Vik Booking security release…

Read the full post →

How many sites have taken the Vik Booking updates?

More than a third took the last one, and most have taken none. Across the Joomla sites we manage that run Vik Booking, about 37% were on 1.18.19 on the day 1.18.21 came out, up from about 9% on 26 October, the day 1.18.19 was released. None were on 1.18.21 yet.

The other 63% are still below 1.18.19, and nearly all of them, about 62% of the total, are below 1.18.17. Those sites have missed all four releases in the run. About 36% are below 1.18.0.

“SVG and images sanitising techniques” reads like housekeeping, and an owner deciding whether an update can wait until next month has nothing else to go on. A security release note should say what was fixed, who could reach it and which versions are affected. After fifteen years of looking after client sites, I would put vague release notes near the top of the reasons an important update gets put off.

What to do

1. Update Vik Booking to 1.18.21 on every Joomla site that runs it.
2. After updating, turn on the new setting that keeps guest media files above the web root.
3. Look in `administrator/components/com_vikbooking/resources/idscans/` for `.svg` signature files. Open none of them in a browser. Read them as text and check for script.
4. Treat any site below 1.18.17 as four security releases behind, not one.

How mySites.guru flags Vik Booking below 1.18.21

mySites.guru added a rule to its vulnerability database on 11 November 2026, and every connected Joomla site running Vik Booking below 1.18.21 now shows it on its dashboard. The rule sits beside the 26 October one for versions below 1.18.19, so a site behind both shows both advisories.

Joomla itself gives no security flag on an extension update, so 1.18.21 appears in the update list looking like any other release. The update can go out across the flagged sites with the mass updater, whether you look after a handful of sites or a large portfolio of Joomla sites, and it is part of every subscription.

Timeline

2026-10-20 — **Vik Booking 1.18.17 is released**

The first release in the run, with CSRF preventions.

2026-10-21 — **Vik Booking 1.18.18 is released**

The changelog reads 'Fixes applied for the automated security plugin review findings.'

2026-10-26 — **Vik Booking 1.18.19 is released**

The changelog lists 'XSS prevention with custom fields management functions.'

2026-10-26 — **mySites.guru flags Vik Booking below 1.18.19**

Every connected Joomla site running an older version shows the advisory on its dashboard.

2026-10-27 — **WordPress-only build 1.8.20**

Its changelog lists 'Fixed invalid capability check affecting front-end pages.' and 'Security improvements.' No Joomla 1.18.20 was published.

2026-11-11 — **Vik Booking 1.18.21 is released**

The changelog lists 'Various CSRF and capability checks added.' and 'SVG and images sanitising techniques.' The fixes are E4J's work.

2026-11-11 — **mySites.guru flags every connected Joomla site below 1.18.21**

The new rule sits beside the 26 October one, so a site behind both shows both advisories.

Further Reading

- Vik Booking 1.18.21 changelog - E4J's own release notes for the Joomla build.
- Vik Booking on wordpress.org - the WordPress build, 1.8.21, released the same day with an identical changelog.
- CWE-79: Improper Neutralization of Input During Web Page Generation - the weakness class behind the script in a signature file.
- CWE-434: Unrestricted Upload of File with Dangerous Type - the weakness class behind saving a submitted SVG as it arrived.
- CWE-352: Cross-Site Request Forgery - the weakness class behind the unchecked invoice tasks.

Frequently Asked Questions

What did Vik Booking 1.18.21 fix?

The main fix is in the guest signature feature. Before 1.18.21 a guest with a confirmed booking could submit an SVG containing script as their check-in signature, and it was saved unchanged inside the web root. The release also adds CSRF token and permission checks to back-end invoice, calendar booking and tariff tasks, and strips tags from values submitted in the booking form's custom fields.

Who could exploit the Vik Booking signature upload?

Anyone with a confirmed booking whose check-out date has not passed and which has a customer record linked to it. No Joomla account is needed. On many sites that means making an ordinary booking, and on sites that take payment up front, paying for it.

Does the script run when an administrator views the booking?

No. The site and administrator pages show the signature through an img tag, which does not run script inside an SVG. The script runs when someone opens the file's own URL directly, for example from a link they are sent. The file is on the site's own domain, so a logged-in administrator who opens it gives the script their session.

Is there a CVE for the Vik Booking 1.18.21 fixes?

No. Neither fix has a CVE. The two 5.1 Medium scores in this post are our own CVSS 4.0 assessments, and the fixes are E4J's work. We did not find or report the flaws.

Is there a Vik Booking 1.18.20 for Joomla?

No Joomla 1.18.20 changelog exists. The Joomla numbering goes from 1.18.19 on 26 October 2026 to 1.18.21 on 11 November. The WordPress build did have a 1.8.20 on 27 October, listing a fixed capability check affecting front-end pages and security improvements.

What should I do after updating to Vik Booking 1.18.21?

Turn on the new configuration setting that keeps guest media files above the web root. Then look in administrator/components/com_vikbooking/resources/idscans/ for .svg signature files. Do not open any of them in a browser; read them as text and check for script.

Does mySites.guru flag sites running Vik Booking below 1.18.21?

Yes. Since 11 November 2026 mySites.guru flags every connected Joomla site running Vik Booking below 1.18.21 on its dashboard. The rule sits beside the 26 October rule for versions below 1.18.19, so a site behind both shows both advisories.

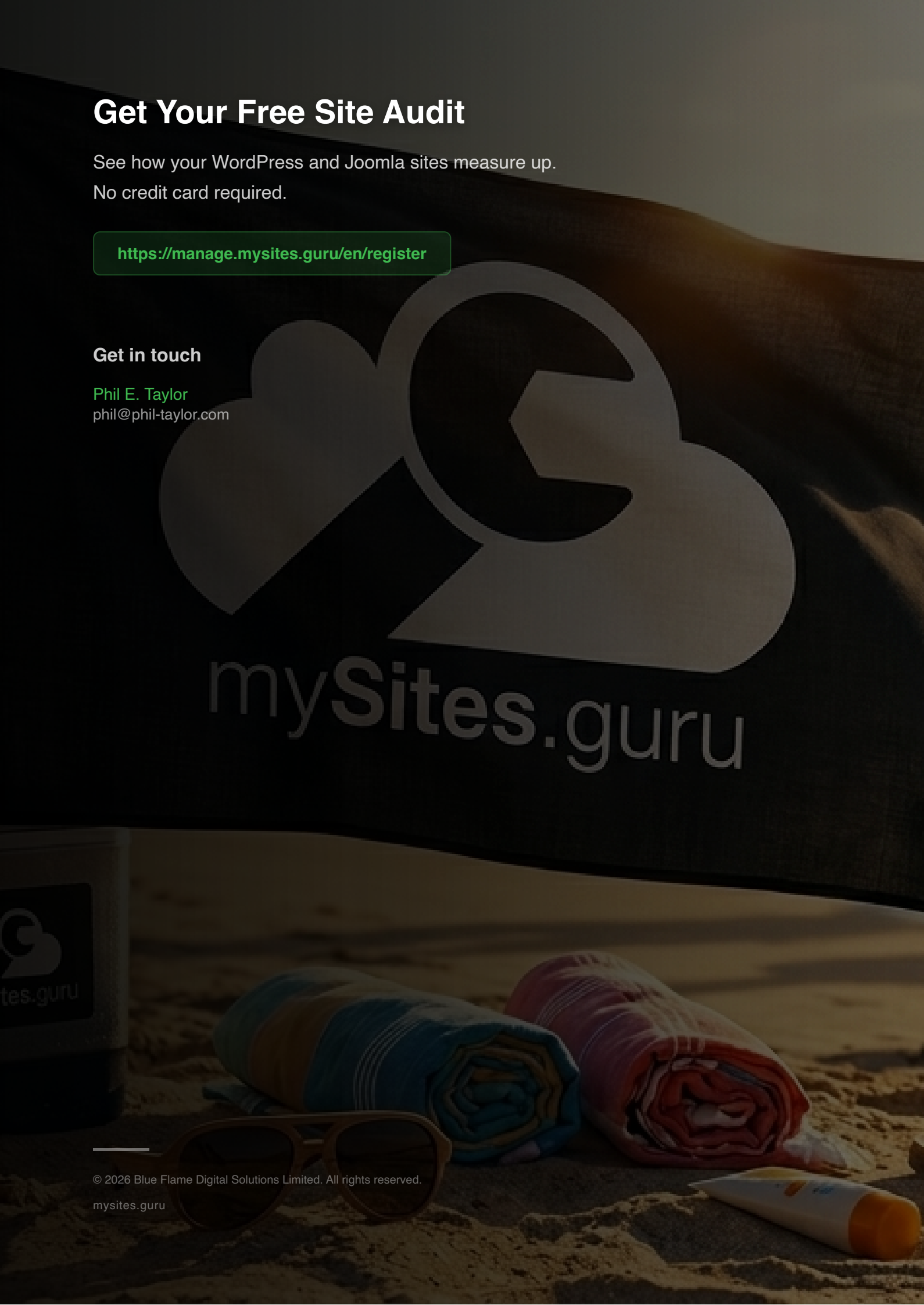
AI MODIFIED Written and edited by a human, with AI assistance. Our approach to AI

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.