mySites.guru

Kunena 7.1.1 and 6.4.17 Fix Stored XSS and Open Member Data in the Joomla Forum Extension

Kunena 7.1.1 and 6.4.17 are security releases for the Joomla forum extension. Both fix stored XSS in posts, and only 7.1.1 closes open member data lists.

Phil E. Taylor | 10 November 2026

TL;DR

Kunena Team released Kunena 7.1.1 and Kunena 6.4.17 on 10 November 2026, both as security releases. Kunena is a third-party forum extension for Joomla, so these are flaws in the extension and Joomla itself is not involved. Both releases fix stored cross-site scripting in forum posts. Kunena 7.1.1 also adds access checks to pages that any visitor could open, including the banned-user list and each member's topic subscriptions, and 6.4.17 does not include those.

No CVE has been published for either release, and the vendor's notes do not name a single flaw. The detail in this post comes from the commits on GitHub, and the two scores below are our own assessment. Sites on Kunena 7.x should update to 7.1.1, and sites on 6.4 should update to 6.4.17 and then plan the move to 7.1.1. More than half of the Kunena sites we see run Kunena 5 or older, and those lines have no fix.

6.9
CVSS 4.0

Kunena below 7.1.1: member subscriptions, favourites and the banned-user list open to anyone

MEDIUM **mySites.guru assessment (no CVE published)**

A visitor with no account can open the banned-user list, read which topics a member follows, and remove any member's subscriptions.

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

No login needed | Fixed in 7.1.1 only | Member data

▼ 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:L Low: Some data 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

5.1
CVSS 4.0

Kunena below 7.1.1 and 6.4.17: stored XSS in forum posts

MEDIUM **mySites.guru assessment (no CVE published)**

A member who can post can save a script in a topic, and it runs in the browser of everyone who reads that topic, including moderators and administrators.

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

Forum account needed | Runs in readers' browsers | Fixed in both lines

▼ 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:L Low: Any logged-in account will do
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 Kunena 7.1.1 and 6.4.17 Fix

The GitHub release notes for 7.1.1 and 6.4.17 both say the same thing: “This is a security release, upgrading is recommended”. The 6.4.17 announcement adds two lines, “Some security issues fixed - thanks to ruud” and “Some security issues fixed - thanks to pbugbounty”, and the commits credit leediay153 for the attachment filename escaping and Nixon-H for the attachment upload category check. None of it says what the security issues were. The commits between 7.1 and 7.1.1, and those between 6.4.16 and 6.4.17, do:

Security issue	6.4.17	7.1.1
Stored XSS in the [video] BBCode tag	Fixed	Fixed
Stored XSS in the SoundCloud auto-embed	Fixed	Fixed
Stored XSS in the Instagram auto-embed	Fixed	Fixed
Attachment filenames printed unescaped	Fixed	Fixed
Attachment upload skipping the category permission check	Fixed	Fixed
Banned-user list open to any visitor	Not included	Fixed
Subscription and favourite lists open for any member	Not included	Fixed
Avatar gallery listing files from other folders	Not included	Fixed
Topic rating accepting any value	Not included	Fixed
XSS in mention, spoiler, file, IP link and Tableau output	Not included	Fixed
Two pages that did not stop on an access error	Not included	Fixed

The five issues fixed in both lines are all in what a member can post. The [video] tag inserted its video code into the page unescaped. The SoundCloud auto-embed wrote

the link into an iframe's `src` unescaped, so a crafted link could add an attribute such as `onload`, the attribute the vendor's regression test uses. The Instagram auto-embed had the same problem and a loose host check, and now accepts only instagram.com and instagr.am. The [attachment] output printed the raw filename, and the download's Content-Disposition header used it unsanitised.

The fifth is a missing authorisation check. An attachment upload with a missing or invalid category skipped that category's upload permission check altogether. Both releases now reject the request with a 403.

How Stored XSS Plays Out on a Kunena Forum

In a forum, the people who write the content are not the people who run the site. On most Joomla sites, only staff can save content that other people see. A forum hands that ability to every member who can post.

The script is saved with the post, so it does not need a victim to click a crafted link. It runs each time somebody opens the topic, in that reader's browser and with that reader's session. For another member, that is their forum account. For a moderator or an administrator, the script acts as them for as long as the page is open, and they are the people most likely to open a new or odd-looking post, because reviewing it is their job.

Our 5.1 score is low for a busy forum. Two requirements hold it down: the attacker needs a forum account, and somebody has to read the topic. On a forum, both happen in the normal course of a day.

What Kunena 6.4.17 Leaves Out

The six issues marked "Not included" above are fixed in 7.1.1 and absent from 6.4.17. In the 6.4.17 source, the access check on the banned-user list is still a comment reading "TODO: add authorisation".

The first two are the reason for the 6.9 score. The banned-user list, at `view=user&layout=banmanager`, had no access check, so any visitor could open it whether logged in or not. In 7.1.1 it is for moderators only. The subscription and favourite lists, and the tasks that remove subscriptions, took the user id from the request. Anyone could read which topics a member follows or keeps as favourites, a guest included in the case of topic subscriptions, and anyone could remove another member's subscriptions. In 7.1.1, subscriptions are for the member and moderators, and favourites for the member alone.

The rest of the 7.1.1-only fixes:

- The avatar gallery appended the gallery name from the request to the gallery path, so a name of `../../..` listed the files of any folder on the server. The vendor's commit notes that the raw views are not reachable at the moment. The name is now limited to one gallery folder and the list to members.
- Topic rating took the star value from the request unchecked, so one member could set a topic's average alone, and it accepted a category and a topic the member might not be able to read. It now takes 1 to 5 stars and checks the topic first.
- Further XSS was closed in the [mention] tag's title attribute, the spoiler and file tags in activity streams, the Tableau embed attributes, and the stored IP address in the moderator's IP link. Older messages posted from behind a load balancer can hold X-Forwarded-For text in that field.
- The category form and the attachment manager returned their access error instead of throwing it, so the check did not stop the page.

The 6.4.17 announcement sets an end date for the line: "The security support of Kunena 6.4.x will end by december 2026 so please think to upgrade to Kunena 7.1." The project's SECURITY.md, revised in this release, lists 7.1.x and 6.4.x as the supported versions.

Which Kunena Versions and Joomla Sites Are Affected?

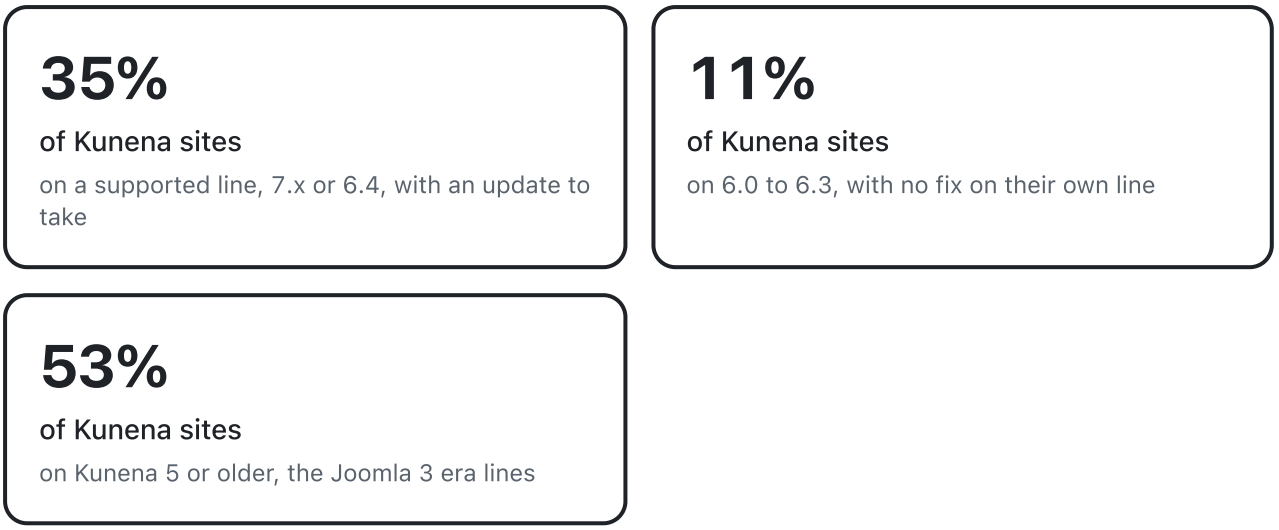
Every Kunena line we checked, from 5.2 to 7.1.0, has code that one of these releases fixes, and only 7.1.1 has the full set of fixes. There is no 7.0.12, so sites on Kunena 7.0.x get the fixes by moving to 7.1.1.

Kunena line	Joomla needed for the fix	Fix	What to do
7.1.0	5.4, 6.1 or 6.2	7.1.1	Update to 7.1.1
7.0.x	5.4, 6.1 or 6.2	7.1.1, no 7.0.12	Move to 7.1.1
6.4.0 to 6.4.16	5.0 to 6.2	6.4.17, partial	Update now, plan 7.1.1
6.0 to 6.3	5.0 or later	None on these lines	Move to 6.4.17 or 7.1.1
5.x	No fix on Joomla 3	None, final release 14 December 2022	Plan the Joomla 3 migration
Older than 5	No fix	None, unsupported	Plan the Joomla 3 migration

Kunena 6.4.17 runs on Joomla 5.0 to 6.2 with PHP 8.1 to 8.4, and on Joomla 6 it needs the compatibility plugin. The source of Kunena 6.0.10, 6.2.6 and 6.3.10 has the same old Instagram embed pattern and the same “TODO: add authorisation” on the banned-user list, and Kunena does not offer 6.3 sites the update to 6.4, “because some users has still Joomla! 4.4.x”. The post on extension vendors dropping Joomla 4 covers how often a security fix now sits behind a Joomla upgrade.

Kunena 5 is the hard case. Kunena 5.2.14, released on 14 December 2022, was the final release for Joomla 3.10, and its source has the unescaped [video] code and the same TODO. Kunena stopped supporting Joomla 3 eight months before Joomla did, a pattern covered in the post on the Joomla 3 end of life. Kunena’s position on Joomla 3 is set out at joomla3security.com/vendors/kunena/.

Hours after the release, none of the Kunena sites in the mySites.guru database was on a fixed version yet. This is how they were spread across the lines:



Sites running the Kunena component in the mySites.guru database, seen in the last 30 days, on 10 November 2026.

Kunena 5.x alone accounts for 36.0% of them, and a further 16.8% are older than that. For the largest group of Kunena forums in our data, this release changes nothing.

What To Do on a Kunena Forum Now

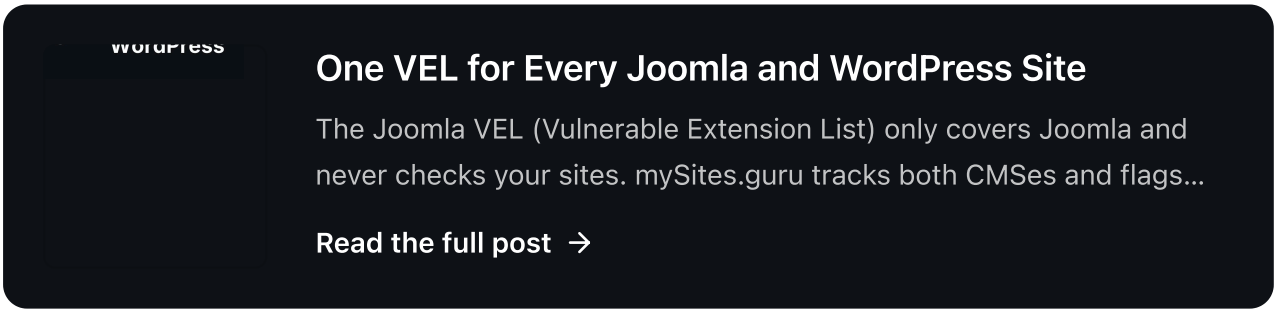
1. On Kunena 7.1.0 or 7.0.x, update to 7.1.1. It needs Joomla 5.4, 6.1 or 6.2 and PHP 8.3 or later.
2. On Kunena 6.4, update to 6.4.17 now. Then plan the move to 7.1.1, because 6.4.17 lacks the 7.1.1-only fixes and its security support ends in December 2026.
3. On Kunena 6.0 to 6.3, get the site to Joomla 5 and install 6.4.17, or to Joomla 5.4 or 6 and install 7.1.1.
4. On Kunena 5 with Joomla 3, there is no fix to install. The forum's future depends on the Joomla 3 migration, and joomla3security.com/options/ sets out the choice between staying, patching and migrating.
5. Until a site is updated, turn off the SoundCloud and Instagram auto-embed settings in Kunena's configuration. That closes those two paths only, and the update is still needed.
6. If you are worried about a forum that takes open registrations, review recent posts by new members for odd video or embed tags.

If Kunena is on a site where extension updates wait for somebody to notice them, the guide to enabling Joomla extension auto-updates covers how to set that up and which extensions it suits.

How mySites.guru Flags Kunena

On 10 November 2026 we added a rule that flags every connected Joomla site running the Kunena component from 6.0.0 to below 6.4.17, or from 7.0.0 to below 7.1.1. The rule covers the 6.x and 7.x lines. Kunena installs as a package of a component, a library and several plugins, and the rule matches the component only, so sitemap plugins from other vendors that use the com_kunena name are not flagged.

Flagged sites appear in the vulnerable extension list with their installed version, so you can see which forums are one update from the fix and which need a Joomla upgrade first. The mass updater then bulk updates Joomla extensions across many sites in one run. The Kunena rules have their own page at Kunena vulnerabilities, every rule we hold is on the public vulnerabilities page, and the flags and the updater are part of the subscription.



For a site that has already been hacked, fix.mySites.guru patches it, audits it for backdoors and hands it back secure for a single fixed fee, usually the same day.

Timeline

2022-12-14 **Kunena 5.2.14, final Joomla 3 release**

Kunena Team's last release for Joomla 3.10. The Kunena 5 line has no fix for the issues closed in 7.1.1 and 6.4.17.

2026-10-23 **Kunena 7.0.11 and 6.4.16 released**

The releases before the security fixes. The 7.0 line gets no 7.0.12.

2026-10-31 **Kunena 7.1 released**

It reports its version as 7.1.0, and it is the line that 7.0 sites move to for the fixes.

2026-11-10 **Kunena 7.1.1 and 6.4.17 released**

Kunena Team releases both as security releases, crediting ruud, pbugbounty, leediay153 and Nixon-H.

2026-11-10 **mySites.guru flags affected sites**

A rule flags connected Joomla sites on Kunena 6.0 to 6.4.16 and 7.0 to 7.1.0.

Further Reading

- Kunena 7.1.1 on GitHub - the release notes, which say it is a security release and that upgrading is recommended.
- Kunena 6.4.17 on GitHub - the same one-line notice for the 6.4 line.
- Kunena 7.1.1 released as security release - Kunena Team's announcement, with the Joomla and PHP requirements.
- Kunena 6.4.17 security release - the 6.4 announcement, with the credits and the end of 6.4.x security support.
- Commits between Kunena 7.1 and 7.1.1 - the code changes, which are the only place the individual fixes are described.

- Joomla extension vendors dropping Joomla 4 - why a security fix increasingly needs a newer Joomla first.

Frequently Asked Questions

Which Kunena versions fix the security issues?

Kunena 7.1.1 and Kunena 6.4.17, both released by Kunena Team on 10 November 2026. Kunena 7.1.1 has every fix. Kunena 6.4.17 has the stored XSS and attachment fixes, and leaves out the access control fixes that are in 7.1.1.

Is there a CVE for Kunena 7.1.1 or 6.4.17?

No. No CVE has been published or named for either release, and the vendor gives no severity score. The two scores in this post, 6.9 Medium and 5.1 Medium under CVSS 4.0, are the mySites.guru assessment.

Does Kunena 6.4.17 fix everything that Kunena 7.1.1 fixes?

No. In 6.4.17 the banned-user list still has no access check, and the fixes for subscription and favourite lists, the avatar gallery, topic rating and several further XSS paths are in 7.1.1 only. Kunena Team also says security support for 6.4.x ends in December 2026.

Is there a fix for Kunena 5 on Joomla 3?

No. Kunena 5.2.14, released on 14 December 2022, was the final release for Joomla 3.10, and its source has the same unescaped video tag and the same unchecked banned-user list. A fixed Kunena needs Joomla 5 or later.

Who can exploit the stored XSS in a Kunena forum?

Any member who is allowed to post. The script is saved with the post and runs in the browser of everyone who reads the topic, including moderators and administrators, using their logged-in session.



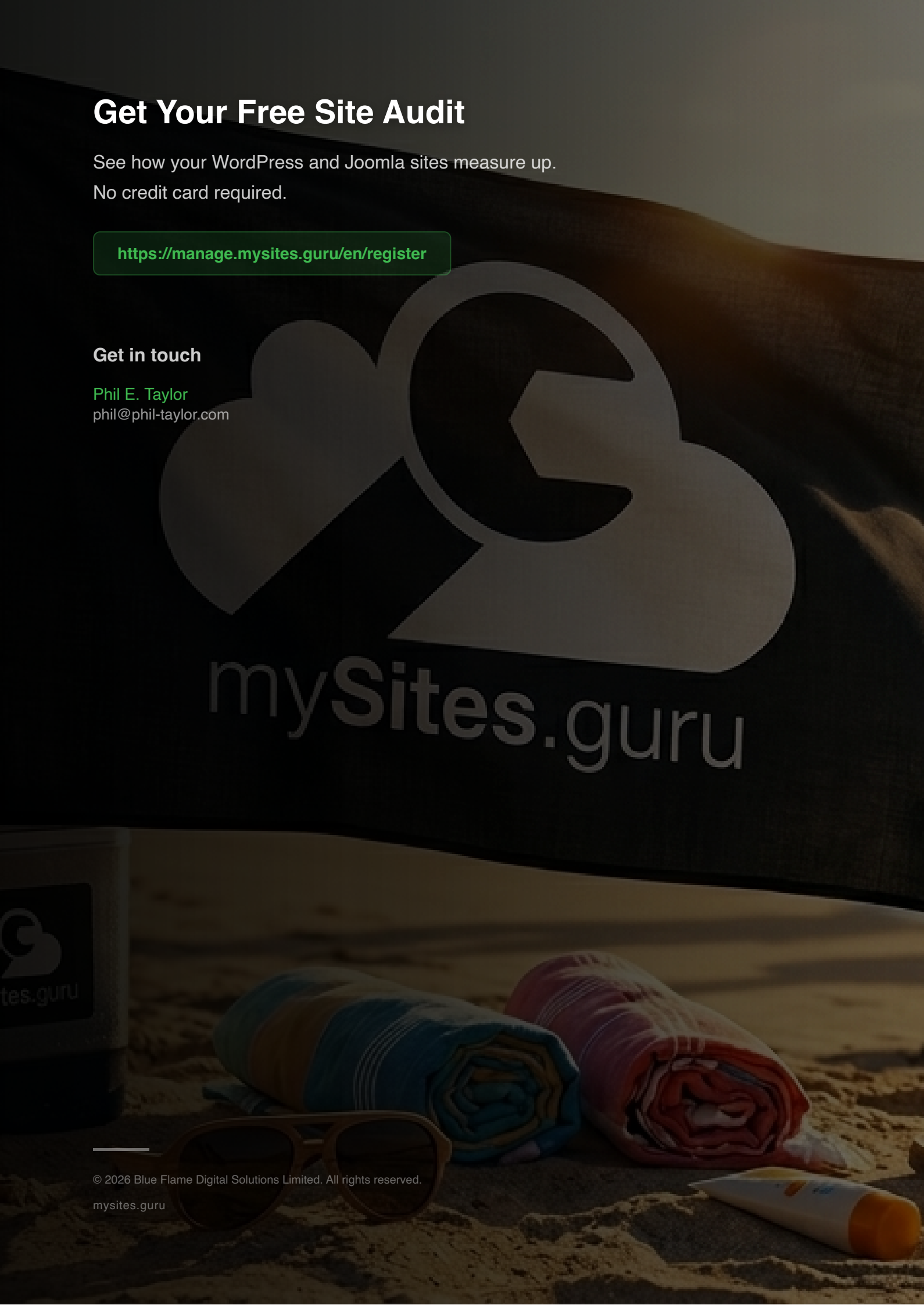
Written and edited by a human, with AI assistance. Our approach to AI

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.