mySites.guru

DJ-Classifieds 3.11.3 Fixes SQL Injection, Upload and Ownership Flaws

DJ-Classifieds 3.11.3 for Joomla fixes SQL injection, unrestricted uploads and ownership flaws. Our code review also found a PayPal-plugin code-execution path.

Phil E. Taylor | 2 November 2026

Update, 2 November 2026

DJ-Extensions has published its own security notice, rating DJ-Classifieds 3.11.3 and DJ-Classifieds Light 3.11.3 as Critical security releases. It says the upload flaw can allow unauthenticated remote code execution on sites where registration is enabled, credits the researcher Ala Arfaoui, and lists six add-ons with security fixes of their own. The post below has been updated to match.

DJ-Extensions released DJ-Classifieds 3.11.3 on 2 November 2026. The changelog that went out with the vendor's update notification lists security fixes for unrestricted uploads, SQL injection and missing ownership checks. The package appeared on the mySites.guru release feed that morning as "DJ-Classifieds Package 3.11.3", and the download sits in the DJ-Extensions customer account area.

If a Joomla site you manage runs DJ-Classifieds, update it to 3.11.3 today. The changelog names only the classes of flaw. All three check out in the 3.11.3 code, two of the SQL injections are reachable without a login under common settings, and the release also contains a fix the changelog does not mention: an `eval()` in the bundled PayPal payment plugin that ran on attacker-supplied input before PayPal verification. The vendor's security notice, published later the same day, adds the detail the changelog lacked: it rates the release Critical because the upload flaw can reach unauthenticated remote code execution where registration is enabled. That puts two code-execution paths in one release, the upload flaw on the vendor's word and the PayPal `eval()` on ours.

Update every DJ-Classifieds site to 3.11.3

Treat every version below 3.11.3 as affected, in both the full component and the Light edition. The vendor says the upload flaw can mean unauthenticated remote code execution where registration is enabled, two of the SQL injection paths need no login under common configurations, and the PayPal plugin path needs no login at all on sites that use it. If a site

is still below 3.11.2 it is also exposed to the July unauthenticated file upload, CVE-2026-61424, which the Joomla CNA scored CVSS 4.0 10.0. Those sites go first.

What DJ-Classifieds 3.11.3 fixes

Here is the release in order of severity, worst first. The upload row takes its rating from the vendor's security notice; the scores on the other rows are our own CVSS 4.0 assessment, derived from the code, not from a published advisory. There is no CVE for any of these yet.

Finding	Where it lives	Login needed	Severity
Image upload trusts the browser-sent type	Profile, category and custom-field image uploads	No, where registration is enabled	Critical (vendor)
PayPal plugin runs `eval()` on request input	Bundled PayPal payment plugin	No, on sites using that plugin	9.2 Critical
SQL injection via the location cookie	Advert and profile listings	No, when a distance feature is on	8.2 High
SQL injection via the advert id	Advert save	No, when guest posting is on	8.2 High (7.1 if login required)
Image rotate accepts any path	Image rotate action	No	6.9 Medium
Missing ownership checks	Payment, order, offer, advert copy	Yes	5.3 Medium

Image uploads trusted the browser-sent type

In 3.11.2, the profile, category and custom-field image uploads decided a file was an image from the type the browser sent with it, which the sender controls. 3.11.3 replaces that with a check on the real file content. This is the “unrestricted uploads” line in the changelog, and it is a different path from the `imageupload` task fixed in July.

The vendor’s security notice goes further than the changelog. It states that “the researcher’s report for Light 3.11.2 and a static review of the 3.11.3 patch indicate that, in a vulnerable configuration with registration enabled, the upload issue could allow unauthenticated remote code execution on the server”, and calls it “a particularly serious issue requiring an urgent update”. That statement is the basis for the Critical rating.

A malicious actor's own code runs on your server, with the same access as the website itself: reading, changing or deleting any file it can touch, planting a backdoor that survives the next update, installing malware, pulling every database credential and API key from your configuration, and using your server to attack other people. Gulp.

The bundled PayPal plugin ran eval() on request input

9.2
CVSS 4.0

PayPal plugin IPN runs eval() on attacker-supplied input

CRITICAL mySites.guru assessment

On a site using the bundled PayPal payment plugin, the IPN handler built PHP from the names of incoming POST fields and ran it with eval(), before the request was verified with PayPal. An anonymous request could reach it.

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

No login needed | Needs the PayPal plugin enabled

Our finding, not vendor-listed

▼ 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:N` None: Nobody has to be tricked into anything

What it does to the site

`VC:H` High: Everything the site holds 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

DJ-Classifieds ships its own PayPal payment plugin. Its job is to receive PayPal's Instant Payment Notification, a server-to-server POST that confirms a payment, and the correct design verifies that notification with PayPal before trusting a word of it.

In 3.11.2 the handler did something else first. It looped over the POST fields and, for each one, ran `eval()` on a string built from the field's name. The field names come straight from the request, so an attacker who could shape them could get their own PHP to run. This happened before the plugin asked PayPal whether the notification was genuine, so the PayPal check that is meant to be the gate never stood between the attacker and the `eval()`.

The payment view reaches this handler with no login and no CSRF token, so on a site that has the PayPal plugin enabled the path is anonymous, with the same outcome as the upload flaw above.

3.11.3 deletes the loop entirely, so no request input reaches `eval()`.

Neither the changelog nor the vendor's security notice mentions this fix, so this is our finding rather than a flaw the vendor disclosed. It also only affects sites that use the bundled PayPal plugin, while the upload flaw above needs only registration to be enabled, so the vendor's finding comes first.

A location cookie reached the listing queries unescaped

8.2
CVSS 4.0

SQL injection through the djcf_latlon location cookie

HIGH **mySites.guru assessment**

The visitor-set djcf_latlon cookie was concatenated into the distance-sort SQL on the public advert and profile listings, so its value could be read as SQL and used to read the database.

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

No login needed

Needs a distance column or geolocation search enabled

▼ 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:N` None: Nobody has to be tricked into anything

What it does to the site

`VC:H` High: Everything the site holds can be read
`VI:N` None: Nothing 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

DJ-Classifieds can sort and filter listings by distance from the visitor, and it keeps the visitor's coordinates in a cookie called `djcf_latlon`. On the public advert and profile listings, that cookie value was split on an underscore and dropped straight into the distance calculation in the SQL, with no escaping and no numeric cast.

A cookie is entirely under the visitor's control, so a value shaped as SQL was read as SQL. The listings are public, so no login is involved. The path runs when a distance column or a geolocation search is enabled, which is a common setup for a classifieds site that groups adverts by location. A `SELECT`-based injection like this reads data, so the realistic outcome is reading the database, including the user table, which is why the confidentiality impact is High.

3.11.3 casts the coordinates to numbers before they reach the query, in the listings and in the maps module, the search module, the Leaflet plugin and the Google Maps layout that shared the same pattern.

The advert id was bound from the form into a query

8.2
CVSS 4.0

SQL injection through the advert id on save

HIGH mySites.guru assessment

The advert save bound the whole submitted form onto the record, including the id, then concatenated that id into a query. A crafted id was read as SQL. Unauthenticated where guest posting is allowed.

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

No login when guest posting is on | 7.1 if login required | Needs a valid form token

▼ 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:N None: Nobody has to be tricked into anything

What it does to the site

VC:H High: Everything the site holds can be read
VI:N None: Nothing 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

When an advert is saved, the save handler bound the entire submitted form onto the advert record and then used the record's id in a query. The id was cast to an integer for the ownership check, but the raw submitted value was what reached the query, so a value such as `0 UNION SELECT ...` passed the integer check as a harmless `0` while the full string was concatenated into the SQL.

The save needs a form token, which any visitor can read from the public add-advert page, so the token is not a barrier. Whether a login is needed depends on one setting: when guest advert posting is enabled, the save is reachable without an account, and many classifieds sites run that way. With guest posting off, it needs any registered user, which lowers the score to 7.1. Like the cookie injection, this is a `SELECT` path, so the realistic impact is reading the database.

3.11.3 stops the save binding server-controlled columns such as the id from the form, and resets the id to the loaded, ownership-checked record before any query uses it.

The image rotate action accepted any path

6.9
CVSS 4.0

Path traversal in the image rotate action

MEDIUM mySites.guru assessment

The front-end image rotate action took a file path from the request and rotated it in place, with no confinement, so an anonymous request

could rotate or corrupt any image file the path could reach.

`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 | Image files only

▼ 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

The front-end image rotate action took a file path from the request, joined it to the site root, and rotated the image at that path in place. It did not check that the path stayed inside the upload folder and did not reject `..` segments, so an anonymous request could point it at an image anywhere the path could reach and have the component re-encode it.

This one does not read data or run code. It can only rotate or corrupt image files the web server can write, so the impact is limited tampering and the loss of those image assets, which is why it scores Medium rather than higher. It is still reachable with no login and no token.

3.11.3 confines the action to the temporary upload folder, resolves the real path and rejects anything that climbs out of it.

Payment and advert-copy actions did not check ownership

5.3
CVSS 4.0

Missing ownership checks on payment and advert copy

MEDIUM **mySites.guru assessment**

A logged-in user could act on payments, orders, offers and adverts belonging to another user, because the code checked that someone was logged in but not that the record was theirs.

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

Login required | Acts on another user's records

▼ 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: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

Several actions checked that a user was logged in but not that the record they were acting on belonged to them. In 3.11.2 a logged-in user could reach another user’s payment, order or offer, and could copy another user’s advert and its images. This is the “missing ownership checks” line in the changelog, and it is the one class here that

needs a login, so it is a logged-in user reaching another user's data rather than an anonymous one.

3.11.3 adds an owner check to the payment, order, offer and advert-copy paths, and to the advert-copy images, allowing a configured administrator through but no one else.

How mySites.guru flags DJ-Classifieds below 3.11.3

mySites.guru records every installed extension and its version on every connected site twice a day, and flags any site running a version listed in its Joomla vulnerability database on the site's own card and in its audit. The Joomla element for this component is `com_djclassifieds`.

Connected sites running DJ-Classifieds below 3.11.3 are flagged, with 3.11.3 shown as the version that resolves it. Sites still below 3.11.2 were already flagged for the July upload flaw, so for them this release changes the target version as well.

DJ-Classifieds Light and the add-ons

DJ-Classifieds Light 3.11.3 has the same changelog as the full component, and the vendor rates it Critical for the same reason. Light installs under the same `com_djclassifieds` element, so mySites.guru flags a Light site below 3.11.3 the same way.

Ten add-ons were released at 3.11.3 alongside it, and six of them include security changes: Alta User Points, Files Attachments, GDPR, Multicategories, Subscription Plans and Shipping. The Files Attachments changelog lists the same three classes as the component, unrestricted uploads, SQL injection and ownership checks, and all six include the type-casting security improvements. The other four, Bad Words, Conditional Fields, Search Alerts and Ghost Ads, were updated at the same time but are not marked as security updates. Update whichever add-ons a site has installed along with the component.

How this relates to the July DJ-Classifieds upload fix

DJ-Classifieds 3.11.2, released on 20 July 2026, fixed an unauthenticated file upload in the front-end `imageupload` task. mySites.guru found that one in a customer's server logs and reported it privately, and DJ-Extensions released the fix three days later. It is tracked as CVE-2026-61424, scored CVSS 4.0 10.0 by the Joomla CNA. Separately, CVE-2025-54474 was an authenticated SQL injection in 3.9.2 to 3.10.1, fixed in 3.10.2.

That makes 3.11.3 at least the third DJ-Classifieds security release in recent months. The 3.11.3 upload fix is a different path from the July one: 3.11.2 fixed the `imageupload` task, while 3.11.3 fixes the browser-sent type check described above. A site owner does not need to tell the two apart. Update to 3.11.3 and both are closed.

Not a mySites.guru finding, and no CVE yet

These are not flaws we reported to DJ-Extensions. The vendor's notice credits the researcher Ala Arfaoui. We found the July upload flaw and reported it privately, For 3.11.3, the detail above comes from the released code, the changelog a DJ-Classifieds user forwarded to us, and the vendor's security notice. The PayPal `eval()` finding is ours from the diff; it appears in neither.

No CVE has been published for any of these fixes. The researcher may still request numbers, or the Joomla CNA may assign them, as happened with the July flaw. A missing CVE is paperwork that has not caught up, not a verdict on severity, so do not wait for one before updating. We have covered DJ-Extensions before, on DJ-HelpfulArticles 1.3, and this release sits in a longer run of Joomla extension disclosures where the fix often arrives before the paperwork does.

What to do today on every Joomla site running DJ-Classifieds

1. Take a backup, then update every DJ-Classifieds and DJ-Classifieds Light site to 3.11.3. The download is on the release page for each product, and access follows the permissions for that product.
2. If any site is still below 3.11.2, do that one first. It is also exposed to the July unauthenticated upload, CVE-2026-61424, and that one was being probed in the wild before its fix was released.
3. Update any installed add-ons to their 3.11.3 releases, starting with the six that have security fixes, then check that advert creation and editing, image and attachment uploads and the add-on features still work, as the vendor recommends.
4. Look in the component upload folder, `tmp/djupload` under the web root by default, for files you did not put there.
5. Check the Joomla Super User and Administrator groups for accounts you did not create.
6. Look for recently modified PHP files across the whole site, not just the upload folder.

Find Super User accounts you did not create

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 →

Flag every Joomla site the day a fix is released

A release like this one is a list-building problem before it is an update problem: which of your sites run DJ-Classifieds, on which version, and which of those are still below 3.11.2. By hand that is a login per site. On mySites.guru the subscription answers it

from the twice-daily snapshot, and every connected site running an affected version is flagged the day a fix is released, with the version that resolves it.

The follow-up checks run as part of the same subscription. The rogue admin check above lists Super Users added outside the normal flow, and the Joomla malware scanner looks for code dropped on the server once someone has a way in. If a site already shows signs of compromise, start with the Joomla hacked-site guide, or have us clean it for you.

If you manage Joomla sites for clients, see what the subscription costs, or run the free audit to see what it finds on your own sites first.

Further Reading

- DJ-Classifieds 3.11.3 security update - the vendor's security notice, covering the component, the Light edition and the add-ons.
- DJ-Classifieds changelog - the vendor's public changelog page.
- DJ-Classifieds unauthenticated file upload - our July post on CVE-2026-61424, fixed in 3.11.2.
- CWE-89: SQL Injection - MITRE's definition of the injection weakness class.
- CWE-434: Unrestricted Upload of File with Dangerous Type - MITRE's definition of the upload weakness class.
- OWASP SQL Injection Prevention Cheat Sheet - parameterised queries, the standard fix for the injection class.

Frequently Asked Questions

What does DJ-Classifieds 3.11.3 fix?

The vendor changelog lists security fixes for unrestricted uploads, SQL injection and missing ownership checks. The 3.11.3 code confirms all three: a location cookie reaching the listing search queries unescaped, the advert id being bound from the submitted form into a query, image uploads trusting the browser-sent type, and payment and advert-copy actions not checking who owns the record. The diff also removes an eval() in the bundled PayPal payment plugin that ran on attacker-supplied input before PayPal verification, which the changelog does not mention.

Is there a CVE for the DJ-Classifieds 3.11.3 fixes?

Not at the time of writing. We do not know whether any have been requested. Numbers may still be requested by the researcher the vendor credits, Ala Arfaoui, or assigned by the Joomla CNA. A missing CVE means the paperwork has not caught up, not that the flaws are minor, so do not wait for one before updating.

Did mySites.guru find these DJ-Classifieds flaws?

No. DJ-Extensions credits the researcher Ala Arfaoui. We found the previous DJ-Classifieds flaw, the unauthenticated file upload fixed in 3.11.2 and tracked as CVE-2026-61424, and reported it privately. The detail in this post comes from the 3.11.3 code and the vendor's notice, and the PayPal eval() finding is ours. The scores below are our own CVSS 4.0 assessment, not a published advisory; the Critical rating on the upload flaw is the vendor's.

I am still on DJ-Classifieds 3.11.1 or older. How urgent is this?

Very. Anything below 3.11.2 is also exposed to the July unauthenticated file upload, CVE-2026-61424, which the Joomla CNA scored CVSS 4.0 10.0 and which was being probed in the wild before the fix was released. Updating to 3.11.3 closes that and everything 3.11.3 itself fixes in one step.

How do I get the DJ-Classifieds 3.11.3 download?

From the DJ-Classifieds 3.11.3 release page, or the Light release page for the Light edition; access follows the permissions for each product. Update notifications go to subscribers, which is how the 3.11.3 changelog reached us before the public changelog page listed the release. The vendor recommends a backup first.



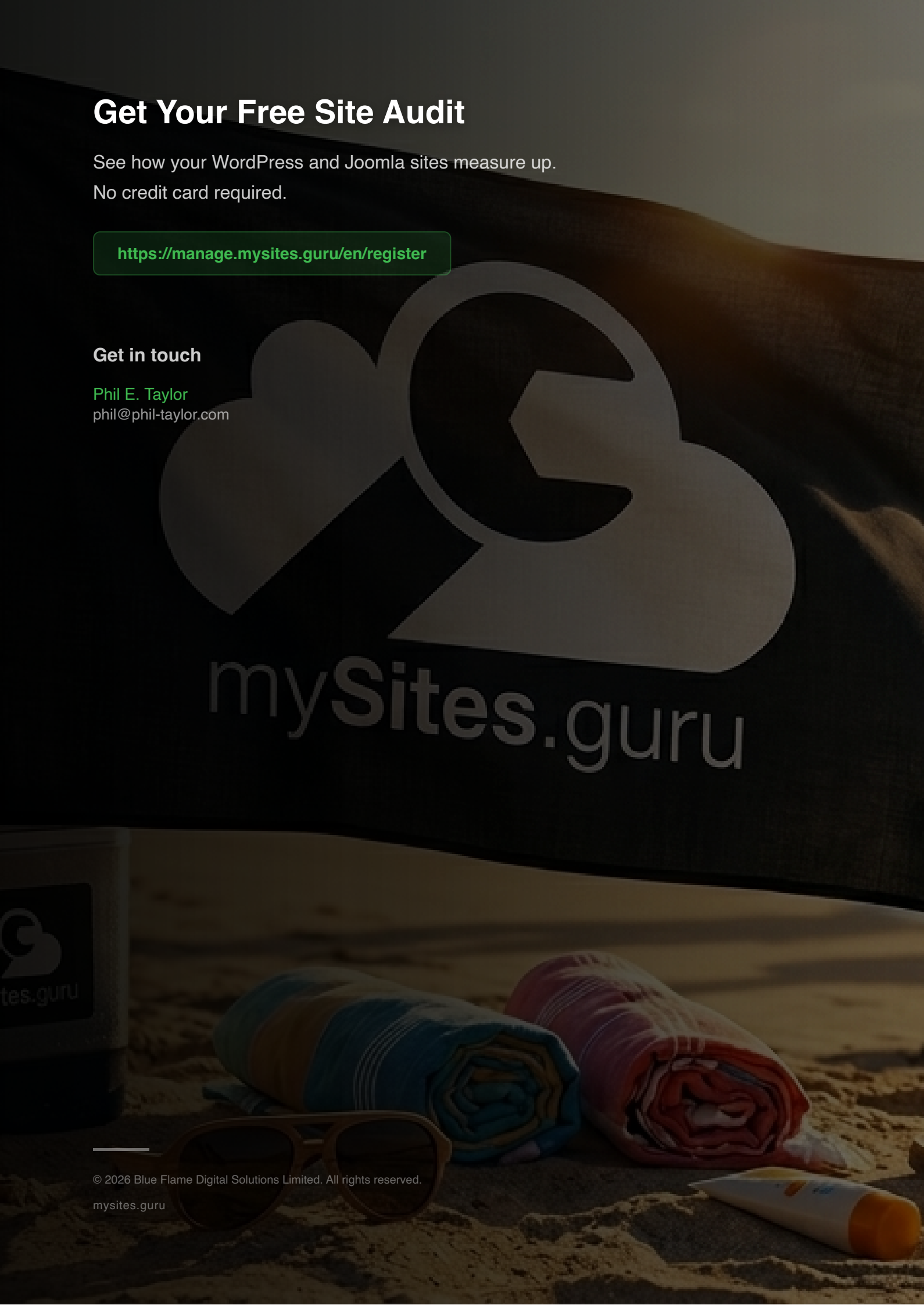
Written and edited by a human, with AI assistance. Our approach to AI

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.