mySites.guru

Three OrdaSoft Joomla Extensions Have Unauthenticated SQL Injections in Their Sort Order

Real Estate Manager, Vehicle Manager and Book Library for Joomla each have an SQL injection needing no login and a reflected XSS. Six CVEs and their fixes.

Phil E. Taylor | 28 September 2026

Six CVEs published today by the Joomla CNA cover three Joomla extensions from OrdaSoft: Real Estate Manager, Vehicle Manager and Book Library. Each extension has the same pair of flaws. The worse of the two is an SQL injection on the public listing pages that needs no login and scores CVSS 4.0 9.3 Critical, and the other is a reflected cross-site scripting flaw at 5.3 Medium.

If a Joomla site you manage runs any of the three, it needs updating today. Real Estate Manager is fixed in 6.7.9 and Vehicle Manager in 6.5.8. Book Library's record is less clear about its fix, which the section on versions below explains.

How mySites.guru flags these three extensions

mySites.guru records the exact version of every extension on every connected Joomla site twice a day. When the six records were published we added them to our Joomla vulnerability database, so any connected site running Real Estate Manager below 6.7.9, Vehicle Manager below 6.5.8 or Book Library below 6.4.6 is now flagged on its own site card and in its audit, with the version that resolves it. There is nothing to search for. If the extension is on the site, the flag is already there.

The records name the Free editions of each extension. OrdaSoft's Pro and ShopPro editions install under the same Joomla element and use the same version numbers, so the flag cannot tell them apart, and a Pro site below the fixed version is flagged too. Updating a Pro install that turns out to have been safe costs you a few minutes. Missing one that was not could cost you the database.

Three extensions let a visitor choose the sort column

All three extensions show lists of things: properties, vehicles, books. All three let the visitor sort those lists, and all three take the name of the sort column from the request and put it into the `ORDER BY` clause of the query that builds the page. That is the whole flaw, repeated three times with small variations.

Real Estate Manager, CVE-2026-100752

In Real Estate Manager, `site/realestatemanager.php` builds the `ORDER BY` clause for three separate front-end queries (category browsing, search results and the full property listing) from the `order_field` request parameter. The value is concatenated straight into the SQL with no allow-list of real column names and no cast.

9.3
CVSS 4.0

CRITICAL Joomla CNA · CVE-2026-100752

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

▼ 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: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

Vehicle Manager, CVE-2026-101108

Vehicle Manager reads `order_field` and `order_direction` at three public entry points in `site/vehiclemanager.php`: the category listing, search, and the all-vehicles listing. The difference here is that the code does try. It runs both values through a sanitising function that applies real escaping. Escaping does nothing for a value that

ends up in an unquoted `ORDER BY` clause, which the next section explains, so the injection works anyway.

9.3
CVSS 4.0

CRITICAL Joomla CNA · CVE-2026-101108

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

▼ 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: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

Book Library, CVE-2026-101110

Book Library's `books()` function in `site/booklibrary.php` reads the `field` and `direction` parameters and passes each through a function called `protectInjectionWithoutQuote()`. Despite the name, its only real protection is a keyword blacklist, and when it spots the word `select` it wraps the value in `$db->quote()` instead of rejecting it. The value then goes into an unquoted `ORDER BY` clause, where quoting is as useless as escaping.

The record notes two conditions for reaching the vulnerable path: a first request to prime the sort defaults stored in the session, and a trailing SQL comment containing the word `select` that satisfies the blacklist without changing what the payload does. Neither needs a login, so neither slows an attacker down much.

9.3
CVSS 4.0

CRITICAL Joomla CNA · CVE-2026-101110

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

▼ 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: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

All three records score the same way: reachable over the network, no privileges, no user interaction, and high impact on the confidentiality, integrity and availability of the data.

A malicious actor could extract your whole database: usernames, emails, password hashes, session IDs, shopping

orders, invoices, and everything else it holds. Gulp.

Why escaping cannot protect an ORDER BY clause

If you write Joomla code, or pay someone who does, this mistake turns up in extension after extension.

SQL escaping and parameter binding both protect a value, something the database treats as data, like the text in a search box or the number in an ID. Escaping works by making sure the attacker cannot close the quotes the value sits inside. A column name in `ORDER BY` is part of the query's structure rather than a value: it sits in the query with no quotes around it, and a prepared statement cannot bind it as a parameter. There is no quote for the attacker to close, so anything they send is read as SQL from the first character.

That is why Vehicle Manager's properly escaped sort value and Book Library's quoted one are both still injectable. The fix for a sort parameter is to compare it against a fixed list of the columns the listing is allowed to sort by, and to fall back to a default when it matches none of them. Joomla's own list models do exactly this with their `filter_fields` allow-list. The direction parameter gets the same treatment, reduced to `ASC` or `DESC` and nothing else.

The reflected cross-site scripting flaws

The second CVE on each extension is less severe but has the same shape across all three: a `title` request parameter written back into the page inside a double-quoted HTML attribute with no escaping. A double quote in the parameter closes the attribute, and whatever follows, including a `<script>` tag, runs in the browser of anyone who opens the crafted link.

- In Real Estate Manager (CVE-2026-100753), the "leave a review" form on the public property page fills its title field straight from the request. The comment field

next to it gets partial tag-stripping, the title field gets none.

- In Vehicle Manager (CVE-2026-101109), the public vehicle page (`task=view`) echoes the `title` parameter into an attribute with no output encoding.
- In Book Library (CVE-2026-101111), the book page template, `site/views/view_book/tmpl/default.php`, runs `echo $_REQUEST["title"];` inside an attribute.

5.3
CVSS 4.0

MEDIUM **Joomla CNA · CVE-2026-100753**

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

▼ 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:P` Passive: Someone has to visit a page

What it does to the site

`VC:L` Low: Some data 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

5.3
CVSS 4.0

MEDIUM **Joomla CNA · CVE-2026-101109**

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

▼ 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:P` Passive: Someone has to visit a page

What it does to the site

`VC:L` Low: Some data 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

5.3
CVSS 4.0

MEDIUM Joomla CNA · CVE-2026-101111

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

▼ 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:P` Passive: Someone has to visit a page

What it does to the site

`VC:L` Low: Some data 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 scores are lower because the victim has to open a link someone sent them. The link points at your own domain, though, which is what makes a phishing email convincing, and if the person who clicks it is logged in to the Joomla administrator, the script runs with their session.

Which versions fix each extension

Extension	Joomla element	Affected	Fixed in
Real Estate Manager	`com_realestatemanager`	1.0.0 to 6.7.8	6.7.9
Vehicle Manager	`com_vehiclemanager`	1.0.0 to 6.5.7	6.5.8
Book Library	`com_booklibrary`	1.0.0 to 6.4.5 or 6.4.6	6.4.6 or the release after it

Real Estate Manager and Vehicle Manager are straightforward: the title and the affected range in each record agree. Book Library's records do not. Their titles give the fix as "< 6.4.6", while their structured affected range runs from 1.0.0 up to and including 6.4.6. One of the two is a typing slip, and there is no vendor changelog to say which.

> **Book Library: take the newest release**
>
> mySites.guru flags Book Library below 6.4.6, which is what the record titles say. If OrdaSoft offers anything newer than 6.4.6, install that instead, so the question of which half of the record is right stops mattering.

What OrdaSoft has published

As far as we can find, OrdaSoft has published no advisory. Its site has no changelog entry, no security page and no mention of any of the six CVE numbers. The only

reference in each record is the OrdaSoft home page, and the product pages' own release lists stop well short of the versions now in circulation. The fixed version numbers in this post come from the CVE records alone.

That matches what happened eight days ago with OS Gallery, another OrdaSoft extension, whose four CVEs also named a fixed release that the vendor did not announce. All six of today's records credit the same finder as the OS Gallery ones, Ala Arfaoui, and between the two batches the same kind of flaw keeps turning up. If you run other OrdaSoft components, keep a close eye on them.

What the mySites.guru database shows

These are not common extensions. Only a small number of sites in the mySites.guru database run each one, and on the day the records were published, every install we can see with a readable version number is on an affected release. That is normal on day one of a disclosure, and it is also why a CVE record alone does not get anyone to update, which is why we flag affected sites on the day rather than waiting for owners to notice.

What to do today

1. Update Real Estate Manager to 6.7.9 or later, Vehicle Manager to 6.5.8 or later, and Book Library to the newest release OrdaSoft offers.
2. If you cannot update today, disable the component in the Joomla extension manager. The injection is on public pages that answer whether or not a menu item links to them, so unpublishing a menu item does not close it.
3. Treat the database as read on any site that sat on an affected version: reset Super User passwords, rotate the Joomla secret, and replace any stored API keys or mail credentials.
4. Check the Super User and Administrator groups for accounts your team did not create.

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 →

What to check after the flag

The version flag tells you a site is exposed. It does not tell you whether anyone got there first, and an SQL injection that needs no login is the kind that gets scripted and sprayed at any site that answers the right URL. The useful checks come after the flag.

mySites.guru runs them as part of the subscription, unattended, on every connected site. The rogue admin check lists Super Users added outside the normal flow across your whole account in one view. The malware and file scanners look for code dropped on the server once an attacker has a password. And the vulnerable extension list explains how version flags like these three work for every Joomla and WordPress extension we track. Doing the same by hand means logging in to every site, one at a time, every time a vendor like OrdaSoft has a bad week.

If one of your sites already shows signs of compromise, work through our Joomla hacked-site guide or have us fix it for you.

If you manage Joomla sites for clients, mySites.guru flags every connected site the day a fix like this is published, and the free audit shows what it finds on your own sites first.

Further Reading

- CVE-2026-100752 record - Real Estate Manager SQL injection, CWE-89.
- CVE-2026-101108 record - Vehicle Manager SQL injection, CWE-89.
- CVE-2026-101110 record - Book Library SQL injection, CWE-89.
- CVE-2026-100753 record - Real Estate Manager reflected XSS, CWE-79.
- CVE-2026-101109 record - Vehicle Manager reflected XSS, CWE-79.
- CVE-2026-101111 record - Book Library reflected XSS, CWE-79.
- OWASP SQL Injection Prevention Cheat Sheet - see its section on allow-list input validation for table and column names.
- OS Gallery 6.2.7 fixes an unauthenticated SQL injection and two authenticated RCEs - the previous OrdaSoft disclosure, from the same researcher.

Frequently Asked Questions

Which versions of Real Estate Manager, Vehicle Manager and Book Library are affected?

Real Estate Manager from 1.0.0 to 6.7.8, fixed in 6.7.9. Vehicle Manager from 1.0.0 to 6.5.7, fixed in 6.5.8. Book Library from 1.0.0, with the CVE record naming 6.4.6 as the fix in its title while its affected range runs up to and including 6.4.6. Each extension has two CVEs, an SQL injection and a reflected cross-site scripting flaw, and both are fixed by the same release.

Does the SQL injection need a login?

No. In all three extensions the vulnerable code sits on public listing pages, the category, search and all-items views that any visitor can open. The attacker controls the column name the listing is sorted by, and that value goes into the ORDER BY clause of the query. The CVE records score all three at CVSS 4.0 9.3 Critical, with no privileges and no user interaction required.

Are the Pro editions affected too?

The six CVE records name the Free editions of each extension. OrdaSoft's Pro and ShopPro editions install under the same Joomla element and share the version numbering, and the records say nothing about them either way. mySites.guru cannot tell the editions apart from the version number, so a Pro install below the fixed version is flagged as well. Updating a Pro install costs little; missing an affected one could cost a database.

Is this a Joomla vulnerability?

These are Joomla extension vulnerabilities in third-party components from OrdaSoft, not flaws in Joomla itself. A Joomla site without Real Estate Manager, Vehicle Manager or Book Library installed is not affected. The Joomla CNA assigns CVE identifiers to third-party extensions as well as to Joomla core, which is why the records are titled 'Joomla Extension'.

Why does escaping the value not stop an ORDER BY injection?

Escaping protects a value that sits inside quotes, by making sure the attacker cannot close the quote. A column name in an ORDER BY clause is not quoted, so there is no quote to close, and the attacker's input is read as SQL straight away. Vehicle Manager's code escapes the sort value correctly and is still injectable for exactly this reason. The fix for a sort parameter is an allow-list of real column names, never escaping.

How do I find every site running these extensions?

By hand, you log in to each Joomla site and read its extension list. mySites.guru records every installed extension and its version on every connected site twice a day, and flags any site running an affected version of these three OrdaSoft extensions on its own site card.

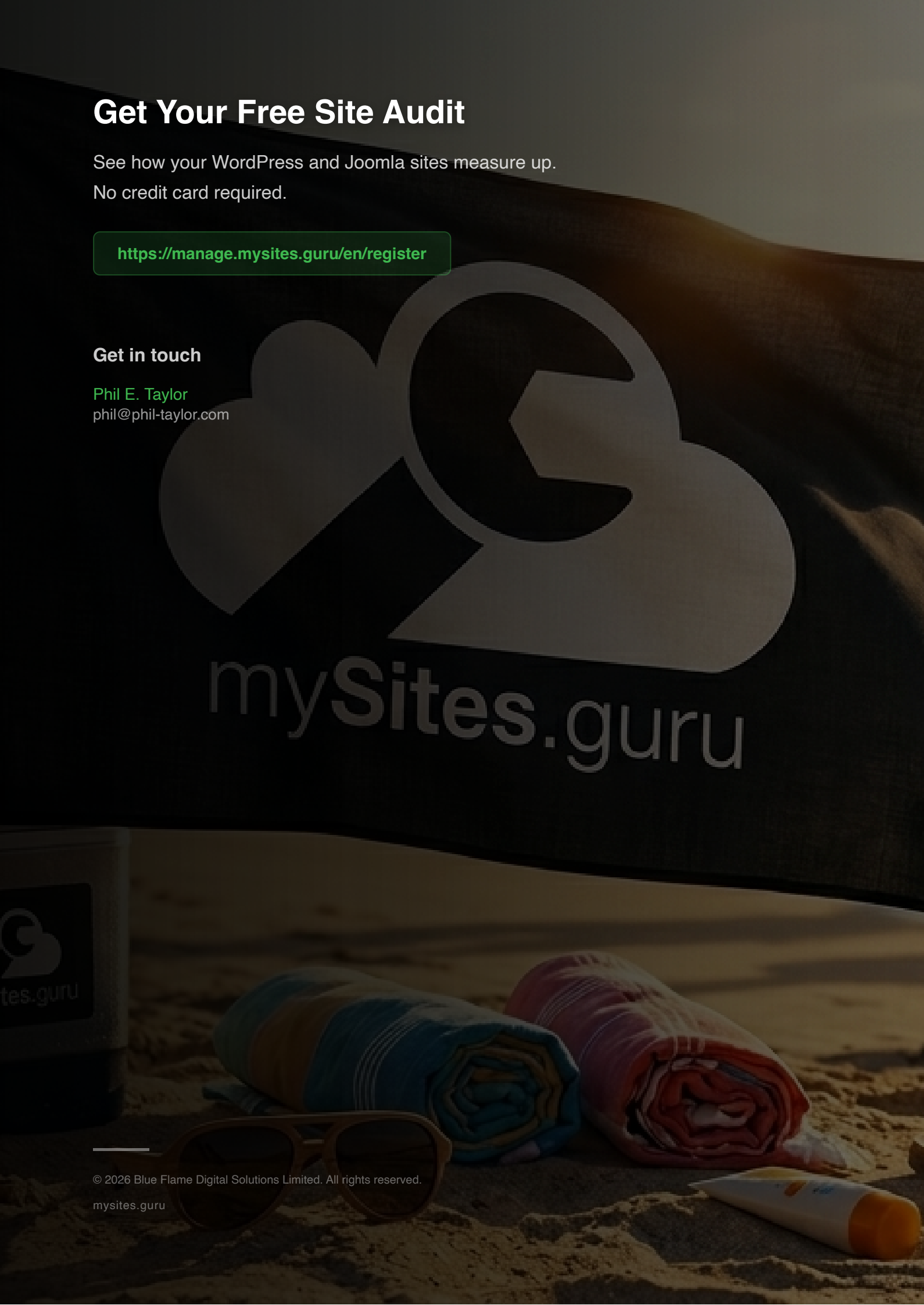
AI MODIFIED Written and edited by a human, with AI assistance. Our approach to AI

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