mySites.guru

What Site Audits Reveal About Joomla and WordPress Security

99% of Joomla sites don't force MFA and 91.8% of WordPress sites skip DISALLOW_FILE_MODS. Real audit data on which security features get used.

Phil E. Taylor | 28 August 2026

Every mySites.guru audit runs the same set of checks against every connected site, and every check gets its own column in the database. That means we can say, with real numbers rather than a guess, exactly what fraction of live Joomla and WordPress sites pass or fail any given check. We don't know of anyone else who can say this. Most security advice for Joomla and WordPress is written from what should be true, not from what actually is.

The numbers below are drawn from each site's most recent audit within a 90-day window, across the sites we audit. They are not a scolding. They are closer to a map of which security features are optional and which are not, and it turns out that distinction predicts the result better than anything about the platform itself.

The gap between available and enforced

Joomla has supported forced Multi-Factor Authentication on Super User accounts for years. It takes one setting to switch on, and once it's on, every Super User has to complete MFA to log in. 99.0% of the Joomla sites we audit don't force it. Not "don't have MFA available" - don't force it, on the single account type capable of doing the most damage to the site.

WordPress has had `DISALLOW_FILE_MODS` since version 2.6. Set that one constant in `wp-config.php` and the entire file editor and plugin/theme installer inside wp-admin switches off, which closes one of the most common paths an attacker uses once they've got a foothold: editing a theme file directly through the admin panel. 91.8% of WordPress sites we audit don't set it. Its narrower sibling, `DISALLOW_FILE_EDIT`, which only blocks the file editor and leaves plugin installation alone, fares a little better but is still unset on 60.6% of sites.

That's the pattern across almost every check on this list. When a security feature is optional, adoption sits somewhere between "rare" and "nearly nobody," regardless of how long it's existed or how well documented it is. Nobody wakes up and decides to leave MFA off for their Joomla Super User. They just never see the setting, because nothing on the site ever asks them to.

Headers nobody sends because nobody has to

Security headers are a cleaner version of the same story, because setting them is entirely within the site owner's control and requires no plugin, no extension, and no code change beyond a handful of server or `.htaccess` lines. 94.9% of the sites we audit, of either platform, have no Content-Security-Policy header - the header that tells a browser which scripts, styles and frames a page is actually allowed to load, and the single most effective defence against a compromised third-party script running freely on your site.

72.0% of Joomla sites have no Strict-Transport-Security header, so a browser that's never visited the site before has no instruction to go straight to HTTPS and will happily follow an HTTP link if one exists anywhere. X-Frame-Options is missing on 50.4% of Joomla sites, and X-Content-Type-Options on 32.4% - both one-line headers, both widely recommended for a decade, both configured on a minority of sites we see. None of these require the site owner to understand cryptography or read an RFC. They require someone to add a line to a config file once, and most people never do, because nothing breaks visibly when the header is missing.

The spread: what's everywhere and what's vanishingly rare

The interesting comparison isn't any single number, it's the range. Some failures sit close to universal. Others sit close to zero, and the reason for that gap is worth sitting with.

On the Joomla side, 60.3% of sites still have the Guided Tours plugin enabled in production, long after anyone needed the onboarding walkthrough it provides. 24.0% still email passwords in plain text rather than a reset link, and 9.0% have user registration enabled on sites that don't need public signups. These are all things a site owner would probably switch off if they ever looked, and most never look.

Compare that with the checks near the bottom. 4.6% of Joomla sites still have FTP credentials sitting in Global Configuration, a legacy feature almost nobody uses any more. 4.2% share sessions between the site and the administrator, which means a session cookie stolen on the front end can be replayed against the back end. 1.0% have debug mode on in production, leaking stack traces and file paths to anyone who requests a broken URL. 0.7% have SEF URLs turned off, which mostly hurts SEO rather than security but travels in the same neighbourhood of "settings nobody revisits." And at the very bottom, 0.1% of Joomla sites connect to the database as root - a database account with no restrictions at all, sitting behind the site's own credentials.

That bottom group is rare for a reason. Running as root, or leaving debug mode on in production, tends to be visible enough, or catastrophic enough when it goes wrong, that someone eventually notices and fixes it. A missing security header or an unforced MFA setting breaks nothing that anyone can see, so it just persists. Rare failures here are the ones that get caught. Common failures are the ones that don't announce themselves.

WordPress has the same shape, different specifics

WordPress shows the identical pattern with its own checks. 48.6% of WordPress sites still have XML-RPC enabled - it ships on by default, so this figure is less a measure of active choice and more a measure of how many sites have simply never had a reason to turn it off, despite it being a longstanding target for brute-force and amplification attacks.

At the opposite end, 3.4% of WordPress sites are accidentally blocking search engines via the "discourage search engines" setting left on from a staging environment or a migration. That's not a security failure at all, it's an availability one, but it belongs in

the same list because it shares the same root cause: a setting flipped once, for a reason that made sense at the time, and never revisited.

What this means for a portfolio of sites

None of this is really about any one site owner being careless. Across every one of these checks, the sites that pass are overwhelmingly the ones where the setting is the default, is forced by the platform, or was switched on for a completely unrelated reason. The sites that fail are the ones where a human being would have had to go looking for a setting, understand what it does, and decide to change it, with no visible consequence for leaving it alone.

It also explains why the same handful of checks keep showing up across completely unrelated incidents. A shared session between the front end and the administrator, a Super User without forced MFA, a missing Content-Security-Policy header: none of these cause a hack on their own, but each one removes a barrier that would otherwise have slowed an attacker down or contained the damage once they were in. The sites that get hurt worst tend to be the ones where several of these optional settings were left off at once, not because any single one was the cause, but because nothing stood between the initial foothold and the rest of the site.

That’s the argument for treating these as things to check rather than things to remember. A checklist you run once at onboarding tells you what a site looked like on the day you looked. A check that runs against every connected site on every snapshot tells you the moment any of these regresses, whether that’s a header dropped during a server migration or a debug flag left on after a deploy. The full set of checks behind these figures, including the ones not covered here, is in the tools reference.

Frequently Asked Questions

What percentage of Joomla sites don't force multi-factor authentication on Super Users?

99.0% of Joomla sites we audit do not force Multi-Factor Authentication on Super User accounts, even though Joomla has supported enforced MFA for years. It is available and almost nobody turns it on.

How common is it for WordPress sites to leave XML-RPC enabled?

48.6% of WordPress sites we audit still have XML-RPC enabled. It is on by default, so this is closer to a measure of how many sites have never actively disabled it than a measure of active choice.

Why do so many sites skip security settings that are already available in Joomla and WordPress?

Across every check we track, the pattern is the same: optional security settings go unused near-universally, and the ones that are enabled by default or forced by the platform get much higher compliance. The gap is between available and enforced, not between good and bad site owners.

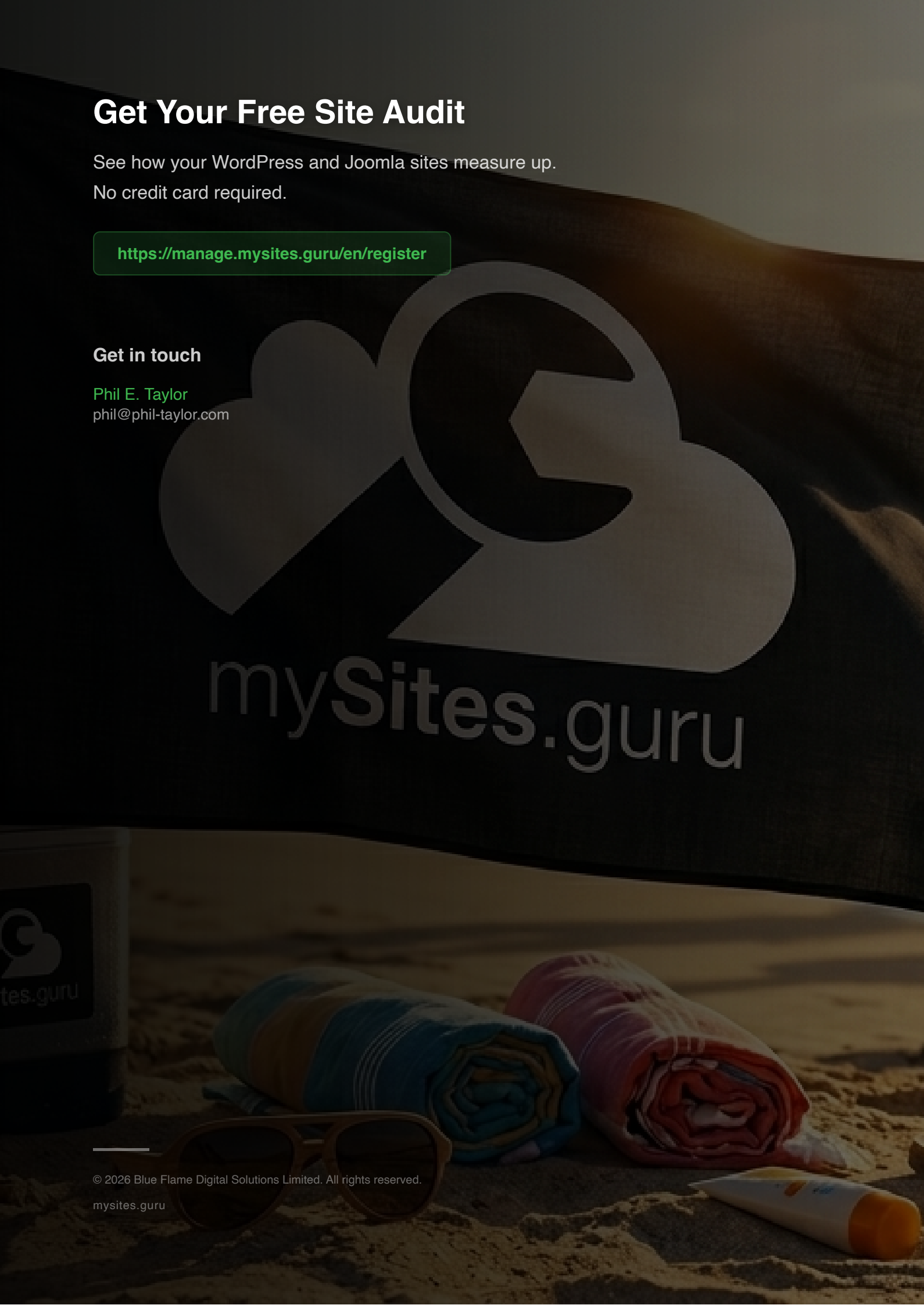
Written and edited by a human, with AI assistance. Our approach to AI

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