Deep Security Audit for WordPress & Joomla

Surface-level scanners miss hidden malware. File-level audits check every line of code against 20,000+ patterns to find backdoors other tools miss.

Phil E. Taylor | 30 March 2026

Think your WordPress or Joomla site is clean? Surface-level scanners only see what a browser sees. A proper security audit digs into every file in your webspace - and that's exactly what the mySites.guru audit does. Want to try it? Run a free site audit with no credit card required. If you suspect you've already been compromised, here's how to tell if your WordPress site has been hacked. If you're specifically looking for malware, our dedicated WordPress malware scanner and WordPress vulnerability scanner give you focused results for those two threat categories. If the worst has already happened, our WordPress hacked guide and Joomla hacked guide walk you through recovery step by step.

In this post I'll walk through how the mySites.guru security audit works, what it checks, and why it catches things that other tools miss.

Connect unlimited sites to the mySites.guru service, then you can run **UNLIMITED** audits of your **UNLIMITED** sites on demand, or schedule them to run daily, weekly or monthly.

> *"Some other services **claim** to have an "audit" tool. Most of the time they mean they have implemented the Sucuri SiteCheck API, which only "scans" your site as a visiting browser would, **it doesn't check the files in your webspace**, and **doesn't find anything that is hidden under the surface** of your rendered webpages. **Be warned.** Not all "Audits" are in-depth and comprehensive!*
>
> *Make sure you compare apples with apples. Not everyone claiming to be an "apple" is."*

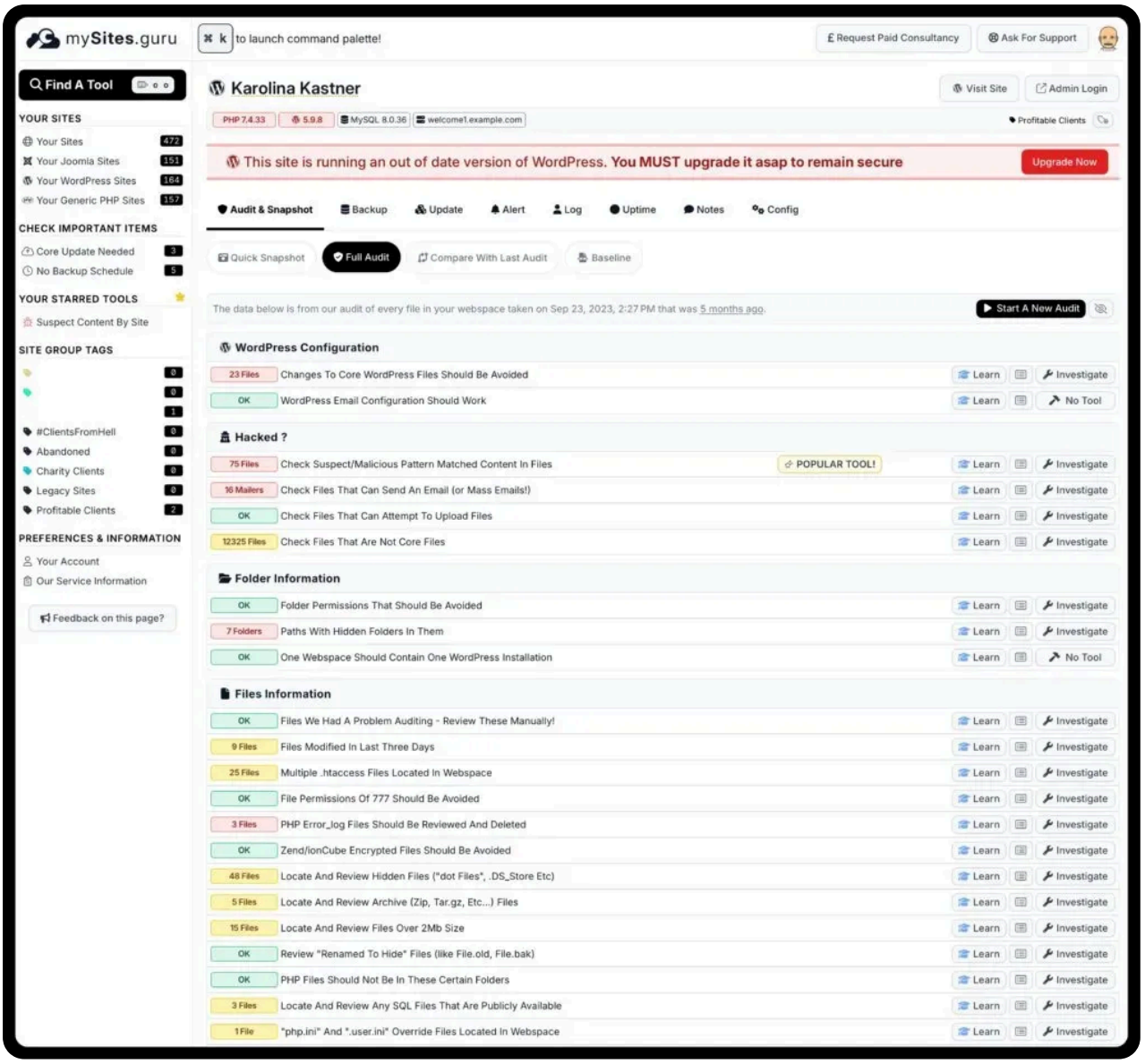
At the start of every audit we also run our snapshot tools, capturing over 100 quick checks of your site. Added to the audit that's even more checks! These include WordPress configuration checks like removing the admin bar logo, debug constant management, and cleaning up default Sample Page and Hello World content, each with a one-click fix.

The audit first compiles a list of all the folders in your webspace - without exceptions - and then grabs a list of the files in those folders.

We then run an exhaustive process which includes:

- Identifying it the file is a core Joomla or WordPress file
- If it's a core file, identifying if that file has been modified since release
- If the core file is modified, doing a comparison with the original file
- Storing the md5 hash of the file for future comparison
- Looping through every single line of code in every single file
- Searching every single line of code, for one of nearly 2000 patterns of previous hacks we have seen, and if found marking a file as "suspect"
- Checking the md5 hash of the file against over 14,000 specific md5 hashes of previously declared "hacked" files. There are no false positives, each of these 14,000 md5 hashes has been manually checked and confirmed to match a file which is hacked
- We check the created, modified and other metadata of each file, including the EXIF data on images (where hacks are known to reside!)
- We identify any encrypted files, PHP error logs, Archive files, files over 2mb in size, zero byte files and many other classifications. See our guide on cleaning up dangerous files for details on why these matter.

Once the audit is over we notify you so you can login to and review the results. The screenshot below shows the first three sections of the audit tab.



Example Audit Results (truncated)

As you can see we display the audit results in the same format as the snapshot tab, with the number of problems, name of the tool, a link to any video, a helpful learn more page, and a button used to investigate our findings.

Suspect files tool

Our most popular tool is the suspect content tool.

This is the tool that lists all the files that have matched either our 20000ish regex patterns, or one of our 14,000 md5 hashes. Just because a file is listed doesnt mean its hacked, unless we specifically state so, as the regex pattern matches are designed to raise false positives and highlight other things (like hidden spammy links to template providers!).

If your file is a known backdoor for a hacker - we mark it as such!

Example hacked file, this one is an insecure form that allows anyone to upload any file their like to the webspace!

This example is a "pretend" image that actually has hackers code embedded into the image to allow the hacker to run any PHP code it likes - this specific example is part of a larger hack

By clicking any of the file names, you can see a preview of the section of the file we think is suspect. You can also see when it was modified, its size, and its permissions.

You can use our tools to edit the file directly in mySites.guru and then save the changes, and we will upload them to your site - no need to find your FTP Client! You can also delete the whole file with a single click.

Hacked hashes

04b7a6c9243a604a41230ed34a65f26e	/html.php
38341b81ed79d907c52b31ab682d89f7	/exporter.php
90fb440139127885e80d609d1e20ede8	/libraries/simplepie.lib.php
e90f6b6ed01d2763312bc1e0fcc5c5eb	/simplepie.lib.php
853863ea47d297e20991ce7c101be9a1	/libraries/simplepie/simplepie.lib.php
0067549af911cf2e20de8f409c1f85a3	/cache/cache-db.php
009b1dc7053eeb9845258e1246086002	/libraries/joomla/access/rule.php
b0faf9d72d89f58cc584169525fd32de	/administrator/components/com_joomlaupdate/views/sort-f7.php
393f3f84ad6fb3a0cb85190fa35f3dcf	/pz.htm
4f613ca5170f9c7bba2e7b63ba1624fb	/anon.htm
5ab7216006cf8269307ee158eca749cf	/libraries/simplepie/simplepie.lib.php
e655cd5cf94762b39e14374081d4638b	/cache/cache-db.php

Example export from our database.

One of the things that sets us apart from most other services, is that we crowdsource data on hacks and backdoors.

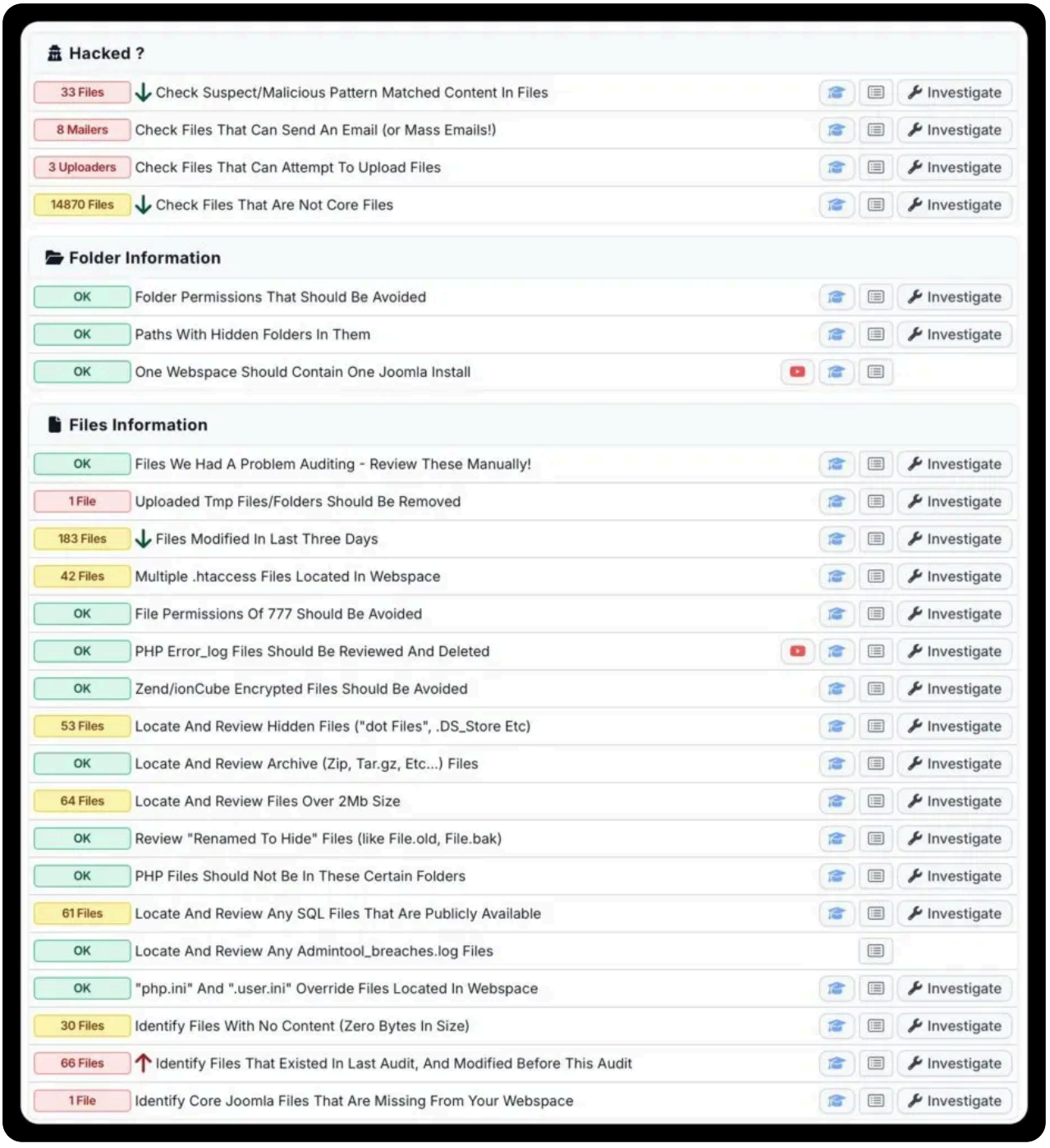
In practice, this means that once a hack is discovered and confirmed on one Joomla site (for example), patterns and regexp are created, approved, and rolled out to the 80,000+ sites the next time they are audited. Including your sites!

This means you benefit from the discovery of emerging hacks and trends we see on other sites. Our system is totally dynamic and self-improving, even without human interaction and people often find hacks on their site when they add them to mySites.guru, that have been left dormant for years, or badly cleaned on previous clean ups.

Fully automated detection improvements

We can also manually improve the audit (and we do) multiple times a day, and with our automatic rollout/upgrade of our tools connector on your site - you get the very latest protection without having to manually upgrade our connector!

File information tools



One of the main sections in the mySites.guru audit tab is the list of File Information Tools.

These allow you to investigate a list of files that match certain classifications, such as encrypted files, or files over 2mb. The audit also surfaces hidden dot-files and dot-folders that most file managers never show you and that hackers routinely exploit.

Over the years these are the tools we have used to identify new and emerging hacks, or to look for something specific, like files that allow file uploads or sending email for example. The audit also includes a dedicated email configuration check that sends a real test email from your site and verifies it arrives.

What makes this audit different?

The mySites.guru audit is unlike any other service you will read about.

We do not buy in someone else's API, all our hack detection is based on over a decade of real life hacks for Joomla and WordPress (and not generic rule based detection like others)

If your site is hacked, mySites.guru will discover that, and inform you, and give you the tools you need to fix your site yourself! A real-world example: the Astroid Framework vulnerability was detected across thousands of sites through our md5 hash matching and suspect content patterns. See our breakdown of the Novarain Framework vulnerability for another example of how hidden extension dependencies create security blind spots that only a file-level audit catches. After all, mySites.guru was created because, at the time, I was doing all this manually myself to fix hacked client sites and I needed a way to automate much of what I did.

Out of your depth and need help?

If the mySites.guru audit finds your Joomla or WordPress site is hacked, and you are unsure how to fix it with our tools, or just want us to take care of everything for you, you

can escalate this to us using the service at https://fix.mysites.guru/ for **SET FEE priced hack fixes.**

Not a subscriber yet? Start with a free site audit - no credit card, no commitment. Connect your site and see what's hiding in your webspace.

See how these tools fit into a broader strategy in our security guide for agencies.

Frequently Asked Questions

How does the mySites.guru audit detect hacks?

It checks every line of every file in your webspace against nearly 20,000 regex patterns and over 14,000 manually confirmed MD5 hashes of known hacked files - far deeper than surface-level scanners.

What is the difference between the mySites.guru audit and tools like Sucuri SiteCheck?

Sucuri SiteCheck only scans what a visiting browser sees, whereas mySites.guru inspects the actual files in your webspace, including hidden and obfuscated content that would never appear in a rendered page.

What happens when a new hack is discovered on one site?

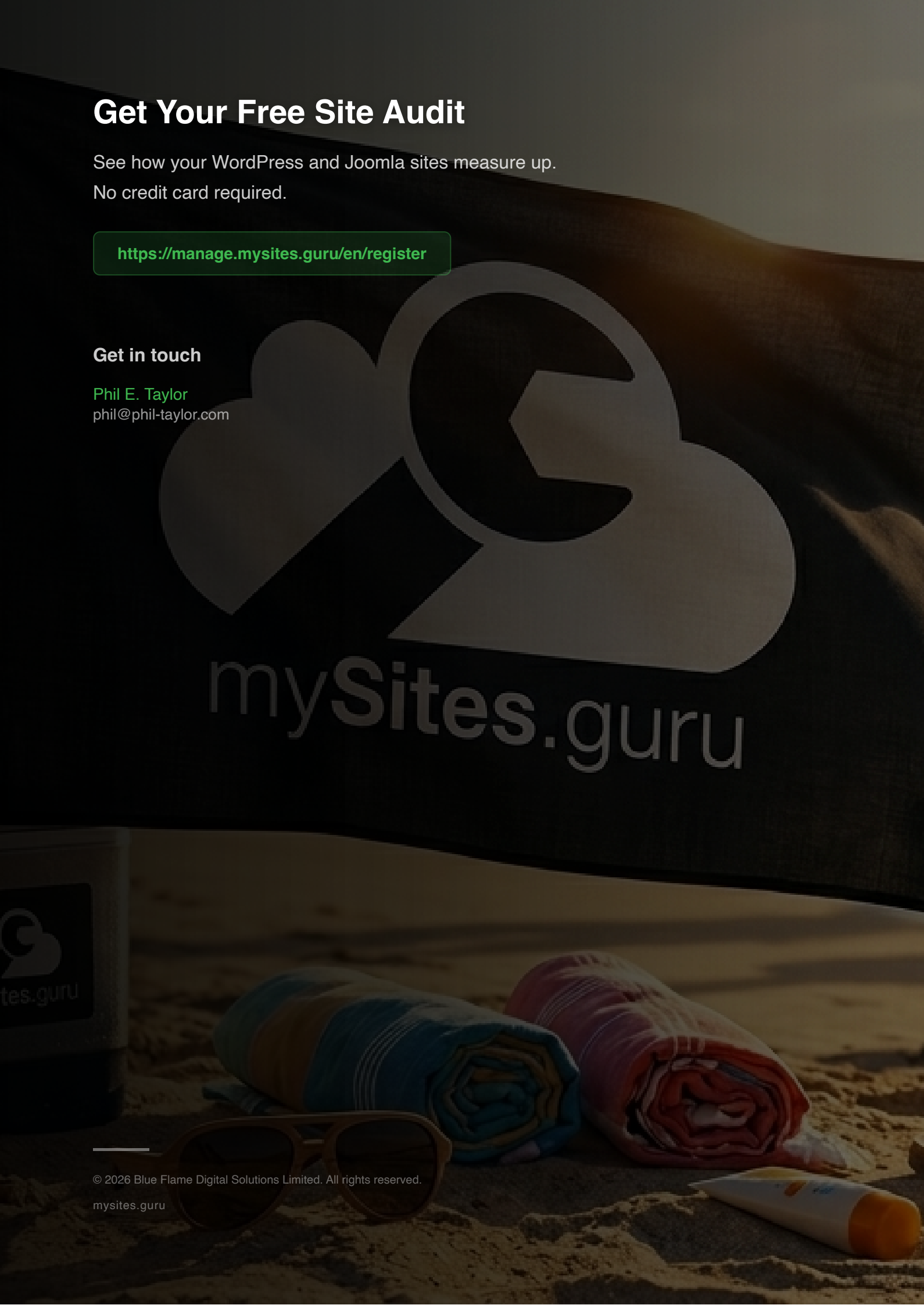
mySites.guru crowdsources hack patterns, so a newly confirmed hack on one site is automatically added to the detection database and checked against all 80,000+ connected sites on their next audit.

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