mySites.guru

How to Fix a Hacked Joomla or WordPress Site

Step-by-step guide to finding and cleaning hacked files on Joomla or WordPress using mySites.guru's suspect content audit and file comparison tools.

Phil E. Taylor | 30 March 2026

So it happened. Your site got hacked. Don't panic. If you're not 100% sure yet, start with how to tell if your WordPress site is actually hacked - it covers the signs vs. false alarms. For the full rundown on what happens when a WordPress site gets hacked or a Joomla site gets hacked, those guides cover warnings signs, consequences, and prevention - but this post is about the cleanup process using mySites.guru. If your Joomla site uses the Astroid Framework, check our Astroid vulnerability breakdown first - it covers the specific backdoors and cleanup steps for that attack. Extension vulnerabilities like the Novarain Framework exploit are another common entry point, particularly because shared library plugins like nrframework get bundled as silent dependencies that site owners don't realise are there.

Why Should You Back Up First (and Not Restore)?

Do it now. Back up your site. Even if it's hacked. Back up right now. Done? Good.

You'll see people recommend restoring from your last clean backup. **This should only be a last resort.** Restoring wipes away evidence that someone experienced can use to understand how you were hacked in the first place. Worse, it re-introduces the same security hole that let the attacker in.

Want an expert to just fix it?

If you'd rather hand this off, visit fix.mysites.guru and submit a request. For a one-time set fee of GBP 120, Phil will clean your site, upgrade it, lock it down and hand it back secure. Non-subscribers get a free month of mySites.guru included.

How Do You Find the Hacked Files with mySites.guru?

mySites.guru has a set of tools built specifically for this. The platform checks every line of code in your webspace to show you what's actually happening on your site.

The most popular tool for hack cleanup is the **suspect content scanner**.

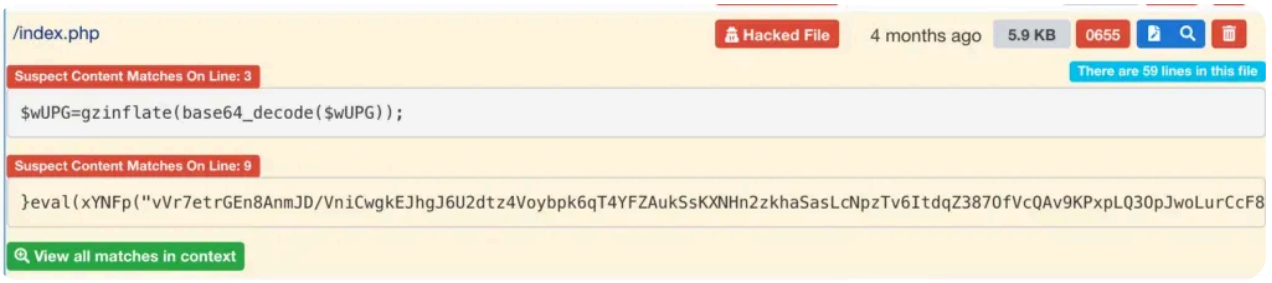
How Do You Discover Suspect Content in Your Files?

After your site has been audited, you'll find the suspect content tool in the "Hacked?" section of the Audit tab.

Clicking **Investigate** loads a real-time scan of your files:

The tool shows the file path, filename, last modified date, size, and permissions. You get buttons to edit the file, view the suspect content matches, or delete the file entirely.

Click on a filename and the platform retrieves the file from your site, runs it against the pattern matching engine, and highlights the exact lines that look suspicious:

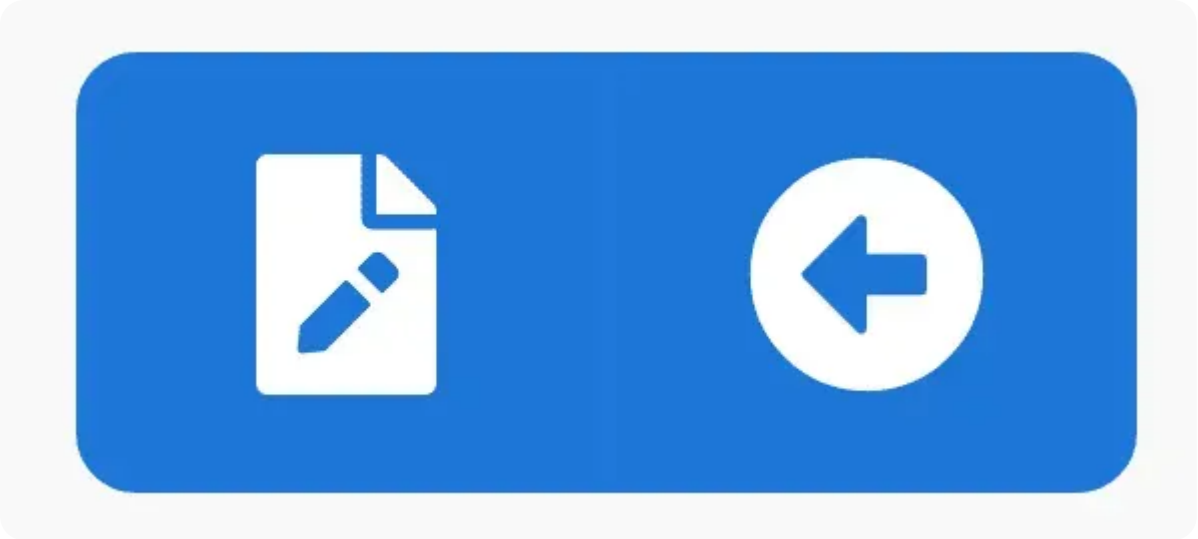


How Do You Revert Core Joomla and WordPress Files?

In the example above, index.php has two lines of injected code. You could edit those lines out manually, but there's a faster way.

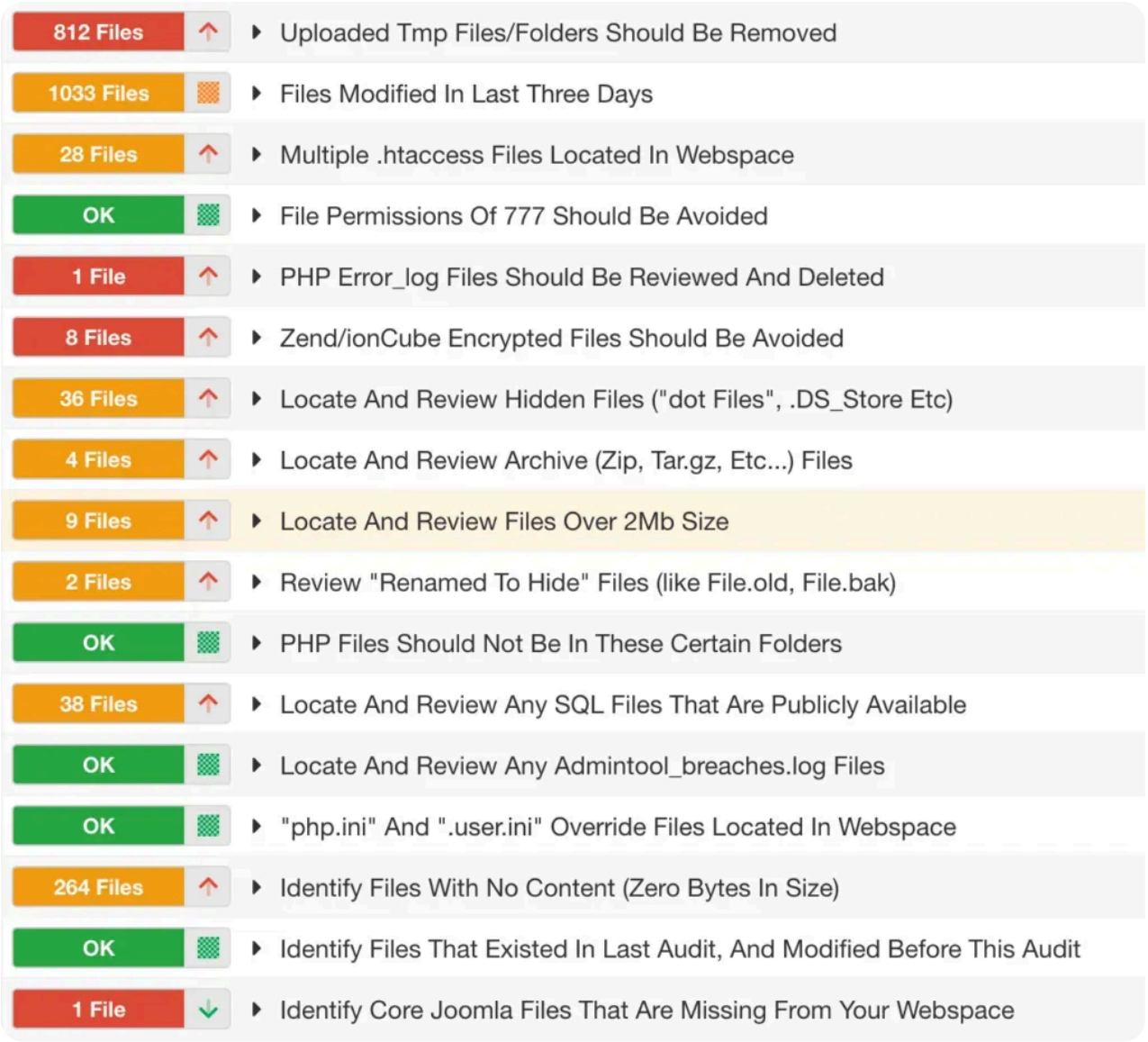
The first tool in the Audit tab is the **core file integrity check** - it lists every core file (Joomla or WordPress) that has been modified since release. Click on a file and you get a side-by-side diff: the original on the left, your modified version on the right.

Click the blue arrow and the original file is restored in a single click - overwriting the hacked version and reverting all changes.



What Other Audit Tools Help Investigate a Hack?

The suspect content scanner and core file diff are just two of the tools available. The full security audit toolset includes checks for:



Not every flagged file is malicious. Some are hidden dot-files left behind by tools or hosting providers that are harmless but worth knowing about. Work through each tool and you'll know exactly what needs cleaning.

How Do You Set Up Monitoring to Catch Future Hacks Early?

Once your site is clean, set up monitoring so you'll know immediately if something changes again.

mySites.guru lets you add unlimited sites and run unlimited backups, snapshots, and audits. The real-time file monitoring checks a configurable list of critical files on every page load and emails you if any of them are modified.

Finding a hack the same day it happens is a completely different situation from discovering it three months later.

> ⚠️ **Always back up before making changes**
>
> Before editing or restoring any files, take a fresh backup. If something goes wrong during cleanup, you need a way to get back to where you started.

Run a free audit on your site to see what mySites.guru finds.

This is part of our WordPress and Joomla security guide for agencies.

Frequently Asked Questions

Should I restore from a backup immediately after my site is hacked?

No - restoring too early destroys evidence needed to identify the original vulnerability and will likely reintroduce the same security hole that allowed the hack in the first place.

How does the mySites.guru suspect content tool work?

It scans every file in your webspace in real time, flags files with suspicious code patterns, and lets you view the exact matching lines, edit files, or restore original core files with a single click.

Can mySites.guru alert me if files change after a hack is cleaned up?

Yes, mySites.guru monitors a configurable list of files on every page load and sends email alerts in real time if any of those files are modified.

What does it cost to have Phil Taylor fix my hacked site?

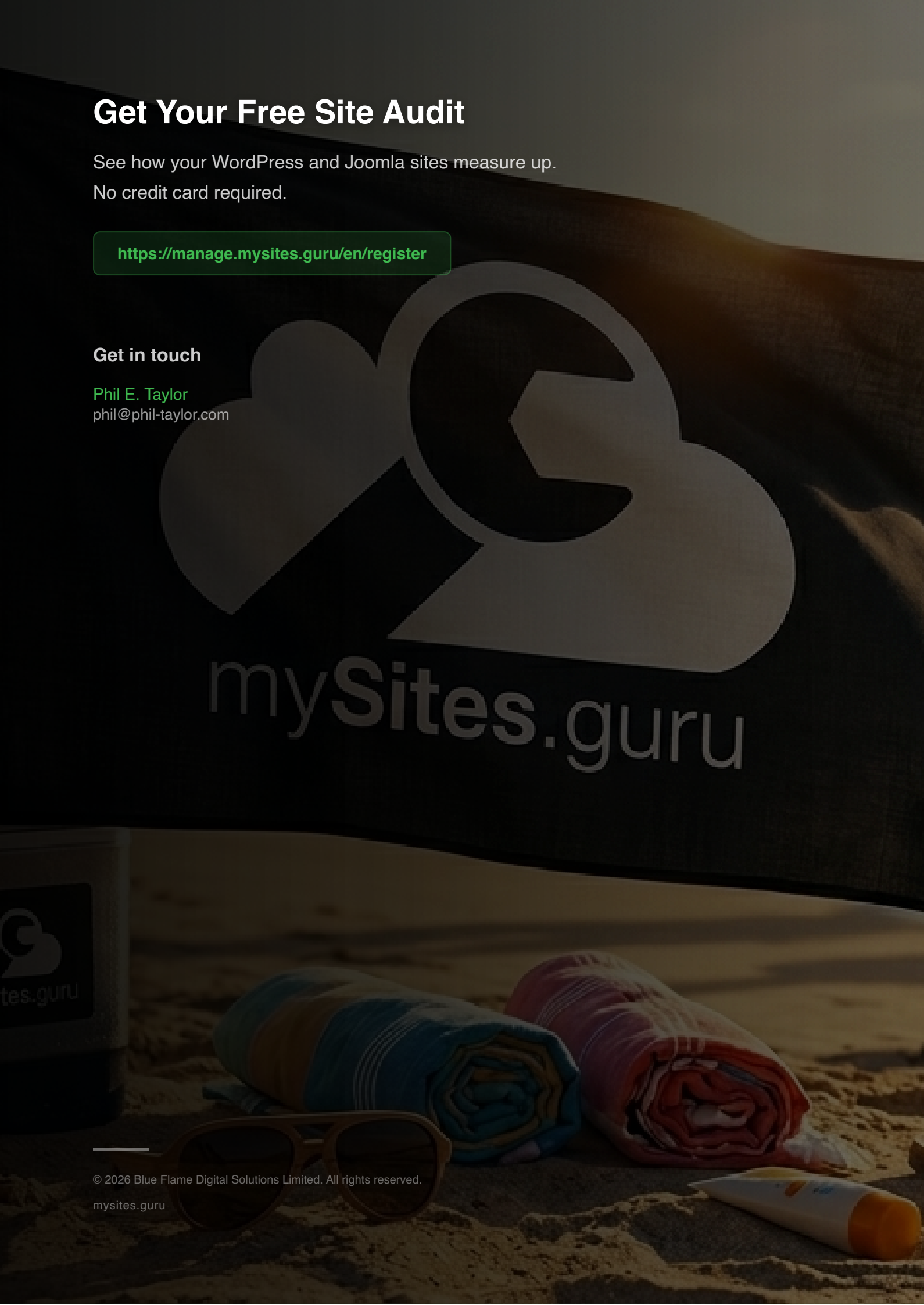
A one-time set fee of GBP 120. Phil cleans the site, upgrades it, locks it down, and hands it back secure. Non-subscribers also get a free month of mySites.guru.

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