Every check we run on your sites

The complete reference for every automated check mySites.guru runs on a WordPress, Joomla or generic site. 293 checks across 13 categories.

65 of them we can fix across every connected site with a single click. Where a figure is shown, it is the share of the sites we audit that currently fail that check.

mysites.guru/tools ·
28 August 2026
Blue Flame Digital
Solutions Limited

Hacked site detection

25

Signatures and behaviours that only appear on a compromised site: rogue admin accounts, planted editor profiles, malicious cron jobs and injected template code.

- [ ] **Check Files That Can Attempt To Upload Files** — Generic
  Flags files capable of accepting an uploaded file, worth investigating since that capability is how a hacker reinfects a site once the first backdoor is found.
- [ ] **Check Files That Can Send An Email (or Mass Emails!)** — Generic
  Attackers commonly plant PHP mail relays and spam scripts after a hack; this lists every file containing the word mail so you can confirm each one is legitimate.
- [ ] **Check For Malicious Cron Jobs** — Generic
  Find compromised sites: a scheduled cron job that re-drops a webshell or malware after files are cleaned
- [ ] **Check Suspect Patterns Matched Content In Files** — Generic
  Matches file contents against our pattern library, deliberately casting a wide net, so entries here need a human to read them and judge.
- [ ] **Hacked Files (100% Certain)** — Generic
  Files confirmed compromised rather than merely suspicious: a hash match against a known hack, an attacker-only filename, or a live compromise found during the scan.
- [ ] **Check Core Folders For Impostor Files** — Joomla
  Flags files sitting inside folders Joomla's core owns outright, such as the root of /administrator/, where no genuine extension has any reason to add anything.
- [ ] **Check Files That Are Not Core Files** — Joomla
  Lists every file that does not match the CMS's official core file set, which is normal for installed extensions but is also where an unnoticed upload would show up.
- [ ] **Check Files That Can Attempt To Upload Files** — Joomla
  Flags files capable of accepting an uploaded file, worth investigating since that capability is how a hacker reinfects a site once the first backdoor is found.
- [ ] **Check Files That Can Send An Email (or Mass Emails!)** — Joomla
  Flags files capable of sending email beyond the CMS's own core mailer, worth investigating since a compromised site spams using exactly this capability.
- [ ] **Check for JCE Rogue Profiles & Backdoors** — Joomla
  Find sites compromised through the JCE editor: rogue editor profiles, malicious profile imports and dropped webshells
- [ ] **Check For Malicious Cron Jobs** — Joomla
  Find compromised sites: a scheduled cron job that re-drops a webshell or malware after files are cleaned
- [ ] **Check Suspect Patterns Matched Content In Files** — Joomla
  Matches file contents against our pattern library, deliberately casting a wide net, so entries here need a human to read them and judge.
- [ ] **Hacked Files (100% Certain)** — Joomla
  Files confirmed compromised rather than merely suspicious: a hash match against a known hack, an attacker-only filename, or a live compromise found during the scan.
- [ ] **Helix Ultimate Mega Menu Hack** — Joomla
  Find compromised sites: menu items whose Helix mega-menu params carry a stored-XSS / super-user-creation payload written via the unauthenticated saveMegaMenuSettings exploit

- [ ] **Helix3 Custom Code Hack** — Joomla
  Find compromised sites: template styles whose custom-code params carry a defacement or stealth-loader payload written via the Helix3 onAjaxHelix3 exploit
- [ ] **Rogue Super Admin Accounts** — Joomla
  Find compromised sites: rogue accounts planted with a known attacker signature or a generated identity
- [ ] **SP Page Builder Rogue Icon-Font Assets** — Joomla
  Find compromised sites: rogue icon-font asset rows planted anonymously through the SP Page Builder asset.uploadCustomIcon exploit
- [ ] **Unpatched JoomShaper Security Holes** — Joomla — **1-click fix**
  Deploy JoomShaper's official Joomla 3 security patches to sites still running vulnerable, now-unsupported extensions (Helix Ultimate, SP Page Builder, Helix3)
- [ ] **Check Core WordPress Folders For Impostor Files** — WordPress
  Recursively checks wp-admin and wp-includes for any file WordPress core never shipped, exactly where a shell dropped after a hack tries to hide.
- [ ] **Check Files That Are Not Core Files** — WordPress
  Lists every file that does not match the CMS's official core file set, which is normal for installed extensions but is also where an unnoticed upload would show up.
- [ ] **Check Files That Can Attempt To Upload Files** — WordPress
  Flags files capable of accepting an uploaded file, worth investigating since that capability is how a hacker reinfects a site once the first backdoor is found.
- [ ] **Check Files That Can Send An Email (or Mass Emails!)** — WordPress
  Flags files capable of sending email beyond the CMS's own core mailer, worth investigating since a compromised site spams using exactly this capability.
- [ ] **Check For Malicious Cron Jobs** — WordPress
  Find compromised sites: a scheduled cron job that re-drops a webshell or malware after files are cleaned
- [ ] **Check Suspect Patterns Matched Content In Files** — WordPress
  Scans file contents against our library of malware patterns, catching backdoors and injected code that a plain file listing would not reveal.
- [ ] **Hacked Files (100% Certain)** — WordPress
  Files confirmed compromised rather than merely suspicious: a hash match against a known hack, an attacker-only filename, or a live compromise found during the scan.

Joomla configuration

54

Settings in Joomla Global Configuration that decide how much a mistake or a break-in can cost you.

- [ ] **$root_user Should Not Be Defined In configuration.php** — Joomla
  $root_user grants whichever account it names full Super User power regardless of that account's real permissions, so a forgotten value is a standing backdoor.
- [ ] **Action And Hide Post Install Messages** — Joomla
  This is housekeeping, not a security check: post-install messages from Joomla core and extensions carry upgrade notices worth reading and dismissing, nothing more.
- [ ] **Admin Group Should Use Default Blacklist Text Filter** — Joomla — **1-click fix**
  Without the Default Blacklist filter, the Administrator group can save unfiltered HTML in content, letting a compromised admin account plant a stored XSS payload.

☐	**Article Options Ignored (Joomla 5.4.7 & 6.1.2)** Find Joomla 5.4.7 / 6.1.2 sites whose per-article Options are silently ignored on the front end	Joomla	
☐	**Avoid Setting $live_site Unless Absolutely Necessary** Setting $live_site overrides Joomla's automatic domain detection and is only needed on badly configured hosts, so leaving it set is usually a sign of bad advice followed, not a real fix.	Joomla	
☐	**Avoid Setting Cookie Domain/Path Unless Necessary** Joomla works out its own cookie domain and path automatically; a manually set value is rarely needed and usually reflects bad advice followed rather than a real fix.	Joomla	
☐	**Avoid Using Default Joomla Templates** Sticking with a stock Joomla template makes your site instantly recognisable to attackers, and a core update can silently overwrite any edits made to those shared files.	Joomla	
☐	**Changes To Core Joomla Files Should Be Avoided** Compares every core Joomla file against its known original hash, because hackers and old developer habits both like to alter files such as index.php directly.	Joomla	
☐	**Check Files That May Need Joomla 5 Compatibility Plugin (Beta)** Searches your files for legacy class names Joomla 5 removed, flagging extensions likely to break once the backward-compatibility plugin is switched off.	Joomla	
☐	**Debug Language Should Not Be Enabled In Production** Language debug mode prints the raw translation string constants next to the translated text on every page, exposing template and extension internals to visitors.	Joomla	**1-click fix**
☐	**Debug Mode Should Be Disabled** Debug mode prints full SQL queries, file paths and stack traces straight onto the page, handing an attacker a map of your server and database structure.	Joomla	**1-click fix** 1% fail
☐	**Disable Flash File Uploads** A crafted .swf upload could once run JavaScript in your site's origin, a known Flash XSS trick; browsers no longer run Flash, so the risk today is mostly historical.	Joomla	**1-click fix**
☐	**Disable Joomla 5.4+ Automatic Core Upgrades** Joomla 5.4 introduces unattended core auto-updates; until that process is proven in production, an automatic major-version upgrade could break your site unsupervised.	Joomla	**1-click fix**
☐	**Disable Joomla Core Update Notification Emails** Disable Joomla core update available notification emails	Joomla	**1-click fix**
☐	**Disable Log Deprecated To Prevent Huge Log Files** Logging deprecated API calls is a developer aid, and on a live site it just grows a log file nobody reads until the disk is full.	Joomla	**1-click fix**
☐	**Disable Log Everything To Prevent Huge Log Files** Log Everything writes a line for every action Joomla takes, which fills the disk on a busy site and can take the whole site down with it.	Joomla	**1-click fix**
☐	**Disable Mail To Friend To Prevent Spam** Email To Friend lets any visitor send email from your server to an address of their choosing, which spammers abuse as a free mail relay.	Joomla	**1-click fix**
☐	**Disable Plain Text Password Emails** When a user resets their password, Joomla can email the new password back to them in plain text, leaving a working credential sitting in an inbox indefinitely.	Joomla	**1-click fix** 24% fail
☐	**Disable Send Copy To Submitter To Prevent Spam** The `Send Copy To Submitter` feature can be used by spammers by allowing them to put their targets email address in the form, use this tool to disable it.	Joomla	**1-click fix**

Disable Template Module Position Preview Appending ?tp=1 to any page reveals your template's module positions and site structure to anyone, information that helps an attacker plan further attacks.	Joomla	**1-click fix**
Distributed robots.txt File Should Be Modified To Suit Your Site Flags a robots.txt that still matches the file Joomla ships by default, usually meaning nobody has told search engines what this particular site needs crawled.	Joomla	
Don't Share Site & Admin Sessions Don't share site and administrator sessions	Joomla	**1-click fix** 4.2% fail
Enable Google Recaptcha To Prevent Form Spam Without CAPTCHA, contact and registration forms are open to automated bots that flood them with spam submissions and fake account signups.	Joomla	
Enable Gzip Compression This is a performance setting, not a security one: Gzip compresses pages before sending them, cutting page weight and load time for visitors.	Joomla	**1-click fix**
Enable IP Logging For User Actions Joomla's User Action Log can record the IP address behind every login and admin action, evidence you need after a break-in to work out how an account was used.	Joomla	
Enable Joomla module versioning for safe rollback of module edits Joomla can keep previous versions of a module's settings, so a bad edit to a live module can be rolled back instead of rebuilt from memory.	Joomla	
Enable Joomla System Log Rotation Without log rotation, Joomla's system logs grow unchecked and can fill your disk, which can crash the site rather than just slow it down.	Joomla	
Enable Proof-of-Work Captcha To Prevent Form Spam Detect Joomla 6.1+ sites that have not enabled the built-in proof-of-work captcha	Joomla	
Enable Session Garbage Collection Plugin This is housekeeping, not an active threat: without this plugin your #__session table can grow unchecked on some servers, eventually slowing queries against it.	Joomla	**1-click fix**
Error Reporting Should Be Set To None In Production Anything other than None prints PHP fatal errors, file paths and stack traces on the live site, handing visitors and attackers details of your server setup.	Joomla	**1-click fix**
Fix Known Joomla 3 End Of Life Security Issues Joomla 3 stopped receiving security fixes in August 2023, so every flaw found since then stays open on the site permanently.	Joomla	**1-click fix**
Force Multi-Factor Authentication For Super Users Without forced MFA, a Super User account can be accessed with a password alone, so a leaked or guessed admin password is enough for full site control.	Joomla	**1-click fix** 99% fail
Force SSL Should Be Set To Entire Site With Force SSL set to admin-only or off, front-end pages including login and password-reset links can still be served over plain HTTP, exposing them to interception.	Joomla	**1-click fix**
Investigate Locked Scheduled Tasks Detect Joomla scheduled tasks that are stuck in a locked state	Joomla	
Joomla Cache Configuration Should Be Enabled This is a performance setting, not a security one: enabling Joomla's page cache cuts database load and speeds up page delivery under traffic.	Joomla	**1-click fix**
Joomla CMS Version Must Be Up-to-date Every unpatched Joomla release has a public list of fixed vulnerabilities that attackers scan for automatically, so an outdated version is a standing target.	Joomla	

☐	**Joomla Global Email Configuration Should Work** Sends a test email through your configured mail settings and confirms it arrives, since silent failures mean lost password resets and form submissions.	Joomla	
☐	**Joomla SEF Configuration Should Be Enabled** This is an SEO setting, not a security one: Search Engine Friendly URLs turn Joomla's index.php?option=... links into readable paths that rank and get clicked more.	Joomla	**1-click fix** 0.7% fail
☐	**Keep configuration.php Inside The Webroot** Symlinking configuration.php outside the webroot is outdated advice that adds no protection: PHP still executes the file wherever the symlink points.	Joomla	
☐	**Language update sites point to the wrong Joomla version** After a Joomla 5 to 6 upgrade, language update sites can stay pinned to the old version so language packs never update. This finds and fixes them.	Joomla	
☐	**Log And Tmp Folders Should Use Default Locations** This catches a common migration mistake, not a security risk: tmp and log paths copied from a local dev environment stop working once live, breaking installs and logging.	Joomla	
☐	**Protect /administrator/ With .htaccess Password** An .htaccess password on /administrator/ adds a second login prompt in front of Joomla's own, so a stolen or brute-forced admin password alone is not enough to reach it.	Joomla	
☐	**Publish A Privacy Policy Using Joomla Privacy Tools** This is a compliance setting: Joomla's Privacy Consent plugin needs an article assigned before it can ask visitors to consent, which most data protection laws require.	Joomla	
☐	**Remove FTP Configuration From Global Config** Joomla's FTP layer stores your hosting FTP username and password in configuration.php in plain text, a working credential for anyone who can read that file.	Joomla	4.6% fail
☐	**Robots.txt Should Not Block Media & Template Folders** This is an SEO setting: blocking /media/ or /templates/ in robots.txt stops Google fetching the CSS, JS and images it needs to render your pages properly.	Joomla	
☐	**Session Lifetime Should Use The Default Value** A longer than default session lifetime keeps a stolen login cookie valid for longer, so changing it without good reason widens the window an attacker has to reuse it.	Joomla	
☐	**Set Public, Guest And Registered Groups To 'No HTML'** Without the No HTML filter, the Public, Guest and Registered groups can submit raw HTML and script tags through any form that saves their input, an easy route to stored XSS.	Joomla	
☐	**Site Should Not Be Set To Offline** A site left offline serves the maintenance page to every visitor and to search engines, so traffic and rankings drain away while nobody notices.	Joomla	**1-click fix**
☐	**Template Manager Broken (Joomla 5.4.8 & 6.1.3)** Find Joomla 5.4.8 / 6.1.3 sites whose Template Manager cannot create overrides or folders	Joomla	
☐	**Unblock mySites.guru IP in Akeeba Admin Tools** Find sites where Akeeba Admin Tools has auto-banned the mySites.guru IP, blocking audits and snapshots	Joomla	
☐	**Use A Joomla Core Or Akeeba Admin Tools .htaccess File** Without a .htaccess file in your web root you lose the baseline security directives Joomla's own htaccess.txt or Akeeba Admin Tools would otherwise apply.	Joomla	
☐	**Use A Valid SSL Certificate To Secure Traffic** Without HTTPS, everything a visitor sends, including login forms and session cookies, travels in plain text and can be read or altered by anyone on the network path.	Joomla	

Use Default Update Channel To Prevent Accidental Series Jump A non-default update channel can quietly offer a pre-release or next major series build, so a routine update could jump your site onto an untested Joomla version.	Joomla	**1-click fix**
Your Favicon Should Be Changed From Default Joomla Icon Checks your homepage for the stock Joomla favicon: this is a cosmetic branding signal, not a security issue, but it tells visitors the site was never finished.	Joomla	

WordPress configuration

40

The wp-config.php constants and admin settings that harden a WordPress install, and the ones that quietly leave it open.

Allow Search Engines To Index This Site Ensure you NEVER discourage search engines from crawling your live site by checking this WordPress feature is not enabled.	WordPress	**1-click fix** 3.4% fail
Avoid Using Default Distributed Salt Values The authentication salts in wp-config.php protect login cookies, so leaving them as "put your unique phrase here" makes forging a session trivial.	WordPress	
Changes To Core WordPress Files Should Be Avoided Compares your WordPress core files against the official file hashes for your version and flags anything that has been altered, a common sign of tampering.	WordPress	
Config Constant: Disable File Editing Through Admin Console with DISALLOW_FILE_EDIT Use DISALLOW_FILE_EDIT to lock down important parts of your admin	WordPress	**1-click fix** 60.7% fail
Config Constant: Disable Plugin Installs with DISALLOW_FILE_MODS constant Disabling plugin and theme installations when in WordPress Admin on a live site can ensure stability and stop admins breaking sites.	WordPress	**1-click fix** 91.9% fail
Config Constant: Disable save queries debug with SAVEQUERIES constant Disable SAVEQUERIES unless you are debugging a problem on a development site	WordPress	**1-click fix**
Config Constant: Disable Script debugging with SCRIPT_DEBUG constant Disable SCRIPT_DEBUG so that minified assets (Javascript files) are loaded	WordPress	**1-click fix**
Config Constant: Disable unfiltered file uploads with ALLOW_UNFILTERED_UPLOADS We highly recommend you disable ALLOW_UNFILTERED_UPLOADS to filter all uploads by users - and only enable when you need to.	WordPress	**1-click fix**
Config Constant: Disable WP_AI_SUPPORT to turn off WordPress AI features Disable the WordPress 7.0+ built-in AI client by defining WP_AI_SUPPORT to false in wp-config.php	WordPress	**1-click fix**
Config Constant: Disable WP_DEBUG In Production Ensure that your live sites dont have the WP_DEBUG constant enabled in production	WordPress	**1-click fix**
Config Constant: Disable WP_DEBUG_DISPLAY In Production Ensure that your live sites dont have the WP_DEBUG_DISPLAY constant enabled in production	WordPress	**1-click fix**
Config Constant: Disable WP_DEBUG_LOG In Production Ensure that your live sites dont have the WP_DEBUG_LOG constant enabled in production	WordPress	**1-click fix**
Config Constant: Disallow Unfiltered Content with DISALLOW_UNFILTERED_HTML Use DISALLOW_UNFILTERED_HTML to increase security on WordPress sites and not allow users full HTML use.	WordPress	**1-click fix**

Config Constant: Enable Auto Upgrades with AUTOMATIC_UPDATER_DISABLED constant WordPress can install its own security releases unattended, which for most sites closes a known hole faster than anyone would get round to it by hand.	WordPress	**1-click fix**
Config Constant: Enable FORCE_SSL_ADMIN to secure admin connections Use FORCE_SSL_ADMIN to ensure secure connections to your WordPress Admin Console	WordPress	**1-click fix**
Config Constant: Enable FORCE_SSL_LOGIN to secure login connections (@Deprecated) FORCE_SSL_LOGIN forces the login page over HTTPS but was deprecated in WordPress 4.0 for FORCE_SSL_ADMIN, and some plugins still look for the old name.	WordPress	**1-click fix**
Config Constant: Enable Minor Upgrades only with WP_AUTO_UPDATE_CORE constant Force WordPress to only apply minor updates instead of major ones automatically	WordPress	**1-click fix**
Config Constant: Enable WP_POST_REVISIONS to limit number of revisions saved to 10 Use WP_POST_REVISIONS to limit number of revisions saved to the database	WordPress	**1-click fix**
Config Constant: Prohibit Database Repair with WP_ALLOW_REPAIR constant Use WP_ALLOW_REPAIR to set to false to prohibit repairing of the db on production sites	WordPress	**1-click fix**
Config Constant: Set AUTOSAVE_INTERVAL to 30 seconds to prevent data loss Use AUTOSAVE_INTERVAL to change the interval between auto-saves to prevent losing your drafts	WordPress	**1-click fix**
Disable Emojis Disable the script to render emojis in WordPress posts as a micro-optimisation	WordPress	**1-click fix**
Disable Frontend Menu Bar When Logged In If you dont need the menubar on the frontend, disable it!	WordPress	**1-click fix**
Disable Links In User Comments To Prevent Spam Deter users spamming your comments with links, by removing the hyperlinks in comments	WordPress	**1-click fix**
Disable the "Howdy," greeting Because its not the 1990's anymore...	WordPress	**1-click fix**
Disable WordPress Application Passwords for APIs We highly recommend you disable WordPress Application Passwords for APIs unless you know of a reason that you need it enabled.	WordPress	**1-click fix**
Disable XML-RPC in WordPress Disable third party access to your site over XML-RPC for better security and prevent access, and brute force attempts	WordPress	**1-click fix** 48.7% fail
Password Protect WP-Admin A .htaccess/.htpasswd prompt on /wp-admin/ adds a second login before an attacker ever reaches WordPress's own login form, and that is hard to automate around.	WordPress	
Remove Default Tagline "Just Another WordPress Site" The unedited "Just Another WordPress Site" tagline is one of the clearest signals to an attacker scouting for abandoned or badly maintained sites.	WordPress	
Remove jQuery Migrate Script Disable the jQuery script in WordPress if you dont need if	WordPress	**1-click fix**
Remove Plugin Admin Nag Screens Because plugin developers abuse your admin console far too much nowadays	WordPress	**1-click fix**

☐	**Remove post shortlink head tags** Remove the WordPress post shortlink HTML head tags if not needed	WordPress	**1-click fix**
☐	**Remove The Default "Hello World!" Post** WordPress installs with a sample "Hello World!" post by default, and leaving it published is one of the clearest signs nobody has ever touched the site.	WordPress	
☐	**Remove The Default "Sample Page"** WordPress installs with a placeholder "Sample Page" by default, and a live copy signals an unfinished or unmaintained site to anyone who lands on it.	WordPress	
☐	**Remove WordPress & Plugin Generator Tags And Version Numbers** Remove the WordPress Generator HTML tag and version numbers from your public pages	WordPress	**1-click fix**
☐	**Remove WordPress Admin Footer Banner** Disable the this for fewer bytes to transfer and less visual clutter.	WordPress	**1-click fix**
☐	**Remove WordPress Logo Menu top left of Admin Console** Remove the WordPress logo, fewer bytes to transfer and less visual clutter!	WordPress	**1-click fix**
☐	**Use A Valid SSL Certificate To Secure Traffic** Checks whether your site URL starts with https, since traffic sent over plain HTTP, including login credentials, can be read or altered on the network path.	WordPress	
☐	**WordPress Address Should Normally Equal Site Address** WP_HOME and WP_SITEURL control where WordPress thinks it lives, and an unexplained mismatch usually means an unfinished migration or a hijacked redirect.	WordPress	
☐	**WordPress Email Configuration Should Work** Sends a test email from your site and confirms it actually arrives, catching a broken mail setup before you notice password resets have stopped working.	WordPress	
☐	**WordPress Version Must Be Up-to-date** Every WordPress release fixes security issues found in the one before it, so anything short of the latest version leaves published vulnerabilities unpatched.	WordPress	

Security headers

20

The HTTP response headers a browser uses to decide what your pages are allowed to do.

☐	**Content-Security-Policy Header Blocks Attacks** Sets which scripts and resources your pages are allowed to load, so injected code from an XSS attack has nowhere left to execute from.	Generic	94.9% fail
☐	**Expect-CT Tells Browsers To Expect Certificate Transparency** Expect-CT asked browsers to verify a certificate was publicly logged, but the header is obsolete now that every trusted certificate must be logged anyway.	Generic	
☐	**Permissions-Policy Controls Which Features Can Be Used In The Browser** Controls which browser features, such as camera, microphone and geolocation, your pages and any embedded content are allowed to request.	Generic	
☐	**Referrer-Policy Sets How Much Info Is Leaked When Linking Off Site** Controls how much of your page's URL gets sent to the destination site when a visitor clicks an outbound link, which can otherwise leak private paths.	Generic	
☐	**Remove Deprecated Feature-Policy Header** Feature-Policy used to restrict access to browser features like the camera and microphone, but it is deprecated in favour of Permissions-Policy, so remove it.	Generic	

Strict-Transport-Security (HSTS) Enforces The Use Of HTTPS Tells the browser to only ever connect over HTTPS for a set period, an instruction that is hard to undo once a visitor's browser has cached it.	Generic	
X-Content-Type-Options Stops Browsers MIME Sniffing The Content Type Stops the browser guessing a file's type from its content instead of trusting the declared type, which is how a disguised file can end up executed as a script.	Generic	
X-Frame-Options Controls Whether Your Site Can Be Framed Controls whether another site can load your pages inside a frame, which stops clickjacking attacks that trick visitors into clicking something invisible.	Generic	
Permissions-Policy Controls Which Features Can Be Used In The Browser Permissions-Policy lets a site switch off browser features such as camera, microphone and geolocation, so a compromised script cannot invoke them.	Joomla	
Referrer-Policy Sets How Much Info Is Leaked When Linking Off Site Without a Referrer-Policy header, a visitor clicking an outbound link can leak the full page URL, tokens and IDs included, to the destination site's logs.	Joomla	
Remove Deprecated Feature-Policy Header Feature-Policy was the browser header gating camera, microphone and similar APIs before Permissions-Policy replaced it, so serving it now is dead weight.	Joomla	
Strict-Transport-Security (HSTS) Enforces The Use Of HTTPS HSTS tells the browser to always use HTTPS for future visits, but the setting is cached for the duration you set, so a bad header is hard to undo quickly.	Joomla	72% fail
X-Content-Type-Options Stops Browsers MIME Sniffing The Content Type Without this header, a browser may guess a file's type from its content, letting an uploaded file dressed as an image execute as a script instead.	Joomla	32.4% fail
X-Frame-Options Controls Whether Your Site Can Be Framed Without X-Frame-Options, another site can load your pages inside an invisible frame and trick a visitor into clicking buttons they cannot see: clickjacking.	Joomla	50.4% fail
Permissions-Policy Controls Which Features Can Be Used In The Browser Controls which browser features, such as camera, microphone and geolocation, your pages and any embedded content are allowed to request.	WordPress	
Referrer-Policy Sets How Much Info Is Leaked When Linking Off Site Controls how much of your page's URL gets sent to the destination site when a visitor clicks an outbound link, which can otherwise leak private paths.	WordPress	
Remove Deprecated Feature-Policy Header Feature-Policy used to restrict access to browser features like the camera and microphone, but it is deprecated in favour of Permissions-Policy, so remove it.	WordPress	
Strict-Transport-Security (HSTS) Enforces The Use Of HTTPS Tells the browser to only ever connect over HTTPS for a set period, an instruction that is hard to undo once a visitor's browser has cached it.	WordPress	
X-Content-Type-Options Stops Browsers MIME Sniffing The Content Type Stops the browser guessing a file's type from its content instead of trusting the declared type, which is how a disguised file can end up executed as a script.	WordPress	
X-Frame-Options Controls Whether Your Site Can Be Framed Controls whether another site can load your pages inside a frame, which stops clickjacking attacks that trick visitors into clicking something invisible.	WordPress	

Database integrity

10

How the database is named, who connects to it, and what else it can reach.

☐	**Backup Tables Should Be Removed From Database** Tables left over from a backup or migration, typically prefixed bak_, sit in the same database as your live data, so a compromise of one exposes the other too.	Joomla	
☐	**Database User Should Not Be "root"** A root database user turns one SQL injection into access to every database on the server, not just this site's.	Joomla	0.1% fail
☐	**DB User Should Only Have Access To One Database** If your database credentials can also see other databases on the server, one SQL injection on this site can reach every database that user has access to.	Joomla	
☐	**Default Database Prefix Should Not Be Set As jos_** jos_ was Joomla's fixed table prefix in early versions, so keeping it makes every table name guessable, one less obstacle an SQL injection has to clear.	Joomla	
☐	**Enable User Action Log Auto Purge After 30 Days** Joomla's action log records logins and configuration changes but never expires entries by default, so without a purge it grows indefinitely unread.	Joomla	
☐	**Joomla Core Database Schema Should Match Installed Joomla Version** The #__schema table records which database updates have run, and a mismatch against your Joomla version means an upgrade left tables only partly migrated.	Joomla	
☐	**Database User Should Not Be "root"** A root database user turns one SQL injection into access to every database on the server, not just this site's.	WordPress	
☐	**DB User Should Only Have Access To One Database** Checks how many databases your MySQL credentials can see: if one is compromised, broader access means every other database on the account is exposed too.	WordPress	
☐	**Default Database Prefix Should Not Be Set As wp_** Checks whether your tables still use the default wp_ prefix, which lets an attacker with partial access guess table names instead of having to find them.	WordPress	
☐	**Pending Database Migrations** Checks whether WordPress core has pending database schema updates it has not yet run, which can leave the site behaving inconsistently after an update.	WordPress	

User accounts and access

33

Who can log in, how they prove it, and how many accounts nobody has used in years.

☐	**Avoid MD5 Hashed Passwords (May Indicate Hacked Site)** Looks for 32-character MD5 password hashes in the users table, which Joomla never creates itself and which point to manual tampering with the database.	Joomla	
☐	**Blocked Users** Counts accounts an administrator has blocked from logging in, since a growing pile of them usually means spam or abuse nobody has finished dealing with.	Joomla	
☐	**Check For Joomla.user.helper.XXXX Usernames (2016 Hack Indicator)** Looks for usernames matching Joomla.user.helper.XXXX, the pattern a 2016 mass-hack created automatically, so finding one means the site was compromised.	Joomla	

☐	**Default Group For New Users Should Not Be Admin Or Super Admin** Checks which user group new registrations are placed into by default, because finding it set to Super Admin is a known sign the site has been hacked.	Joomla	
☐	**Disable User Registration Unless Required** Checks whether public account registration is switched on, since an open signup form invites spam bots and gives attackers an easy foothold.	Joomla	**1-click fix** 9% fail
☐	**Enable Two-Factor Authentication Plugins** Checks whether any Two-Factor Authentication plugin is enabled site-wide, since nobody can turn on 2FA if no plugin offers it.	Joomla	**1-click fix**
☐	**Inactive Users (180+ Days)** Lists non-admin accounts that have not logged in for 180 days or more, since an unused account is a credential nobody is watching.	Joomla	
☐	**Limit The Number Of Super Admins To One** Find sites where more than one account holds full Super User rights	Joomla	
☐	**Privacy: Process Confirmed Export Requests** Flags GDPR data export requests the user has confirmed by email, which now sit on a legal deadline until you actually export their data.	Joomla	
☐	**Privacy: Process Confirmed Remove Requests** Flags GDPR erasure requests the user has confirmed by email, which now sit on a legal deadline until you actually delete their data.	Joomla	
☐	**Privacy: Remove Completed Export Requests** Flags GDPR data export requests that have already been fulfilled but are still stored on the site, and should be cleared out once delivered.	Joomla	
☐	**Privacy: Remove Completed Remove Requests** Flags GDPR erasure requests that have already been carried out but are still logged on the site, and should be cleared out now the data is gone.	Joomla	
☐	**Privacy: Review Overdue Privacy Requests** Flags GDPR export or erasure requests that have passed their statutory deadline and now need immediate action to avoid a compliance breach.	Joomla	
☐	**Privacy: Review Pending Export Requests** Flags GDPR data export requests still waiting on the requester's email confirmation, the first stage of a legal deadline you need to track.	Joomla	
☐	**Privacy: Review Pending Remove Requests** Flags GDPR erasure requests still waiting on the requester's email confirmation, the first stage of a legal deadline you need to track.	Joomla	
☐	**Remove "Never Logged In" Accounts** Lists accounts that have never once logged in, usually spam registrations or abandoned signups that still count as personal data you are holding.	Joomla	
☐	**Super Admin Should Not Have Username "admin"** Checks for a Super Admin account using the username admin, which hands an attacker half the credentials they need to log in as you.	Joomla	
☐	**Unactivated Users** Lists registered accounts still waiting on email activation, since a large or growing backlog is usually spam signups rather than real visitors.	Joomla	
☐	**Use Two-Factor Authentication On All Super User Accounts** Checks every Super Admin account for two-factor or multi-factor authentication, since a stolen password alone should never be enough to log in as one.	Joomla	

☐	**Users In No User Group** Find users who belong to no user group across all your sites	Joomla	
☐	**"Anyone can register" should be disabled unless required** Checks whether WordPress lets anyone create an account, which widens the attack surface for any exploit that only needs a logged-in user.	WordPress	**1-click fix**
☐	**Avoid MD5 Hashed Passwords (May Indicate Hacked Site)** WordPress has not stored passwords as raw MD5 since 2008, so finding one today usually means the database was edited directly, not through WordPress.	WordPress	
☐	**Avoid Using "admin" As A Username** Looks for a WordPress account named exactly admin, which hands a brute-force attacker half the login before they have guessed anything.	WordPress	
☐	**Blocked Users** Lists WordPress accounts you have blocked from logging in, so you can confirm each one still deserves to stay blocked or delete it outright.	WordPress	
☐	**Inactive Users (180+ Days)** Lists WordPress accounts that have not logged in for 180 or more days, the ones nobody would notice being misused if compromised.	WordPress	
☐	**Limit The Number Of Administrators To One** Counts WordPress accounts in the Administrator role: every extra one is another set of credentials that can compromise the whole site.	WordPress	
☐	**New User Default Role Should Not Be Administrator** Checks the role WordPress assigns to new sign-ups: finding it set to Administrator is a common sign the site has already been compromised.	WordPress	
☐	**Privacy: Keep Pending Export Requests At Zero** Flags GDPR data export requests still waiting to be actioned, which risks missing the statutory deadline for responding to the user.	WordPress	
☐	**Privacy: Keep Pending Remove Requests At Zero** Flags GDPR erasure requests still waiting to be actioned, which risks missing the statutory deadline for responding to the user.	WordPress	
☐	**Privacy: Remove Completed Export Requests** Flags GDPR data export requests already fulfilled but still logged in WordPress, which is queue clutter you should clear out.	WordPress	
☐	**Privacy: Remove Completed Remove Requests** Flags GDPR erasure requests already fulfilled but still logged in WordPress, which is queue clutter you should clear out.	WordPress	
☐	**Unactivated Users** Lists WordPress accounts with a live activation link that was never completed, left over from sign-ups nobody finished.	WordPress	
☐	**Users With No Role** Find users who have no role across all your WordPress sites	WordPress	

Hosting environment

25

What the server underneath the site is actually running.

☐	**PHP Disabled Functions Should Be Minimised** Reports any core PHP functions your host has disabled: blocking functions like this is not real hardening and often just breaks site features.	Generic

☐	**PHP Display Errors Configuration Should Be Off** Checks whether PHP is set to print errors on the page, which can leak file paths, database details and other internals to any visitor who triggers one.	Generic
☐	**PHP File Uploads Should Be Enabled** Checks that the PHP file_uploads setting is on: with it disabled, uploading media, installing extensions and applying updates all silently fail.	Generic
☐	**PHP Magic Quotes Should Be Off** Magic quotes was removed from PHP entirely in PHP 5.4 (2012), so finding it reported as enabled means the site is running an ancient, unsupported PHP build.	Generic
☐	**PHP Register Globals Should Be Off** Register globals was removed from PHP in version 5.4 (2012): finding it on means the host is running a release with no security patches in over a decade.	Generic
☐	**PHP Safe Mode Should Be Off** Safe mode was removed from PHP in version 5.4 (2012): finding it enabled today means the server is stuck on a release with no security support at all.	Generic
☐	**PHP Session Path Should Be Writable** Checks that PHP can write to its configured session save path, because without it the site cannot keep any visitor, including you, logged in.	Generic
☐	**PHP Version Should Be Latest Supported Series** Compares the live PHP version against the currently supported series: an outdated release means known vulnerabilities in PHP itself go unpatched.	Generic
☐	**PHP Disabled Functions Should Be Minimised** Disabling PHP functions in php.ini gives a false sense of security and breaks legitimate code without stopping an attacker who can already run PHP.	Joomla
☐	**PHP Display Errors Configuration Should Be Off** A production site with display_errors on will print file paths and stack traces straight onto the page, handing an attacker a map of your server.	Joomla
☐	**PHP Extension fileinfo Must Be Installed For Media Manager** Joomla 4.3 and later require the fileinfo PHP extension for Media Manager to work at all, and some cPanel hosts disable or omit it by default.	Joomla
☐	**PHP File Uploads Should Be Enabled** Some hosts disable file_uploads to look secure, but Joomla needs it for Media Manager and extensions, so turning it off breaks the site, not secures it.	Joomla
☐	**PHP Magic Quotes Should Be Off** Magic Quotes was removed from PHP in version 5.4 (2012), so finding it enabled means the server runs an unsupported PHP release with no security fixes since.	Joomla
☐	**PHP Register Globals Should Be Off** Register Globals let request data overwrite script variables and was removed from PHP in 5.4 (2012), so finding it on means a decade of missed security fixes.	Joomla
☐	**PHP Safe Mode Should Be Off** Safe Mode never gave the isolation it promised and was removed from PHP in 5.4 (2012), so finding it on means a decade or more without a single security fix.	Joomla
☐	**PHP Session Path Should Be Writable** PHP writes session files to keep visitors logged in between requests, so an unwritable session path silently breaks login and admin sessions across the site.	Joomla
☐	**PHP Version Should Be Latest Supported Series** Running a PHP release below the latest supported minor version means missing bug fixes and security patches that the newer release already has.	Joomla

- [ ] **PHP Disabled Functions Should Be Minimised** — WordPress
  Checks your host's PHP disable_functions setting and flags any entries, since disabling core PHP functions is not real security and just breaks features.
- [ ] **PHP Display Errors Configuration Should Be Off** — WordPress
  Checks whether PHP's display_errors setting is switched on, which can leak file paths and other internal details to anyone who triggers an error.
- [ ] **PHP File Uploads Should Be Enabled** — WordPress
  Checks whether PHP's file_uploads setting is enabled, since WordPress needs it for media uploads, plugin installs and theme updates to work at all.
- [ ] **PHP Magic Quotes Should Be Off** — WordPress
  Checks for PHP's magic_quotes settings, removed from PHP itself in 2012, so finding either active means the server runs a long-unsupported PHP version.
- [ ] **PHP Register Globals Should Be Off** — WordPress
  Checks for PHP's register_globals setting, removed from PHP itself in 2012, so finding it switched on means the server runs a long-unsupported PHP version.
- [ ] **PHP Safe Mode Should Be Off** — WordPress
  Checks for PHP's safe_mode setting, removed from PHP itself in 2012, so finding it enabled means the server runs a long-unsupported PHP version.
- [ ] **PHP Session Path Should Be Writable** — WordPress
  Checks whether PHP's configured session save path is writable, since WordPress cannot keep users logged in or maintain any session state without it.
- [ ] **PHP Version Should Be Latest Supported Series** — WordPress
  Checks your PHP version against the currently supported release series, since an outdated PHP version stops receiving security patches from php.net.

Files

56

Files that should not be there, files that changed, and files that are missing.

- [ ] **"php.ini" and ".user.ini" Override Files Located In Webspace** — Generic
  Finds php.ini and .user.ini files that silently override PHP's settings for a single folder, worth knowing about even when you put them there yourself.
- [ ] **File Permissions Of 777 Should Be Avoided** — Generic
  Finds files and folders set to permission 777, which lets any other user on a shared server read, write and execute them, not just your account.
- [ ] **Files Modified Between Audits** — Generic
  Compares the MD5 hash of every file against the previous audit and flags any that changed, catching edits that fall outside the three-day recent-changes window.
- [ ] **Files Modified In Last Three Days** — Generic
  Lists every file changed in the last three days by its modification time, so a sudden burst of edits you did not make stands out fast.
- [ ] **Files That Could Not Be Audited, Review Manually** — Generic
  Lists files our scanner timed out on, often large or complex scripts, so you know which parts of the webspace this audit did not actually cover.
- [ ] **Identify Files With No Content (Zero Bytes In Size)** — Generic
  Finds files that exist but hold no data at all, sometimes a hacker's waymarker, sometimes a blank index.php stopping directory listings, so each needs a look.

☐	**Locate And Review Any SQL Files That Are Publicly Available** Finds .sql files sitting in a publicly reachable location, which is how a full database backup, including password hashes, ends up downloadable by anyone.	Generic
☐	**Locate And Review Archive Files (Zip, Tar.gz, Etc)** Finds zip, tar and gzip archives in your webspace, which take up space unnecessarily and are also how attackers bulk-upload a whole toolkit of files in one go.	Generic
☐	**Locate And Review Files Over 2Mb Size** Lists every file over 2MB so you can see what is actually using your disk space, since attackers also favour large archives to smuggle in many files at once.	Generic
☐	**Locate And Review Hidden Files ("dot Files", .DS_Store Etc)** Lists every file whose name starts with a dot, including .htaccess by design, because attackers also favour dot-prefixed names to stay off a normal file listing.	Generic
☐	**Multiple .htaccess Files Located In Webspace** Counts .htaccess files across the whole webspace; a site needs one, so more than a handful outside the root is unusual and worth investigating.	Generic
☐	**PHP error_log Files Should Be Reviewed And Deleted** Finds PHP error_log files, which record file paths and code errors that a well-running site should not be generating, and that an attacker can read for reconnaissance.	Generic
☐	**PHP Files Should Not Be In These Certain Folders** Flags PHP files sitting inside the /images folder, a favourite hiding place for an uploaded backdoor because nobody expects code to run from there.	Generic
☐	**Review Renamed Files (.old, .bak, .orig)** Finds files renamed with a .bak, .backup or .old ending, commonly a config file left with old credentials in it, or a copy of a hacked file kept for later.	Generic
☐	**Zend/ionCube Encrypted Files Should Be Avoided** Encoded PHP files hide their real source code from our scanner, so a Zend Guard or ionCube file could be running anything, including a backdoor.	Generic
☐	**"php.ini" and ".user.ini" Override Files Located In Webspace** Finds php.ini and .user.ini files that silently override PHP's settings for a single folder, worth knowing about even when you put them there yourself.	Joomla
☐	**Akeeba Kickstart Should Not Be Left In Webspace** Kickstart is a one-time restore tool that can overwrite your entire site with any archive an attacker supplies, so leaving it in place after use is a standing takeover risk.	Joomla
☐	**File Permissions Of 777 Should Be Avoided** Finds files and folders set to permission 777, which lets any other user on a shared server read, write and execute them, not just your account.	Joomla
☐	**Files Modified Between Audits** Compares the MD5 hash of every file against the previous audit and flags any that changed, catching edits that fall outside the three-day recent-changes window.	Joomla
☐	**Files Modified In Last Three Days** Lists every file changed in the last three days by its modification time, so a sudden burst of edits you did not make stands out fast.	Joomla
☐	**Files That Could Not Be Audited, Review Manually** Lists files our scanner timed out on, often large or complex scripts, so you know which parts of the webspace this audit did not actually cover.	Joomla
☐	**Forum Post Assistant Should Not Be Left In Webspace** The fpa.php diagnostic script dumps detailed system, PHP and configuration information that helps an attacker profile your server, so it should never stay public.	Joomla

☐	**Identify Files With No Content (Zero Bytes In Size)** Finds files that exist but hold no data at all, sometimes a hacker's waymarker, sometimes a blank index.php stopping directory listings, so each needs a look.	Joomla
☐	**Identify Missing Core Joomla Files** Compares your webspace against the official Joomla file list and flags anything missing, whether from a failed update or deliberate deletion to cover tracks.	Joomla
☐	**Locate And Review Any admintool_breaches.log Files** Finds admintool_breaches.log files written by the Admin Tools security extension when it blocks an attack, worth reviewing as a record of attempted break-ins.	Joomla
☐	**Locate And Review Any SQL Files That Are Publicly Available** Finds .sql files sitting in a publicly reachable location, which is how a full database backup, including password hashes, ends up downloadable by anyone.	Joomla
☐	**Locate And Review Archive Files (Zip, Tar.gz, Etc)** Finds zip, tar and gzip archives in your webspace, which take up space unnecessarily and are also how attackers bulk-upload a whole toolkit of files in one go.	Joomla
☐	**Locate And Review Double Extension Files (name.php.xxx)** Locate files where .php is not the final extension (name.php.json) - a common malware-evasion pattern	Joomla
☐	**Locate And Review Files Over 2Mb Size** Lists every file over 2MB so you can see what is actually using your disk space, since attackers also favour large archives to smuggle in many files at once.	Joomla
☐	**Locate And Review Hidden Files ("dot Files", .DS_Store Etc)** Lists every file whose name starts with a dot, including .htaccess by design, because attackers also favour dot-prefixed names to stay off a normal file listing.	Joomla
☐	**Multiple .htaccess Files Located In Webspace** Counts .htaccess files across the whole webspace; a site needs one, so more than a handful outside the root is unusual and worth investigating.	Joomla
☐	**PHP error_log Files Should Be Reviewed And Deleted** Finds PHP error_log files, which record file paths and code errors that a well-running site should not be generating, and that an attacker can read for reconnaissance.	Joomla
☐	**PHP Files Should Not Be In These Certain Folders** Flags PHP files sitting inside the /images folder, a favourite hiding place for an uploaded backdoor because nobody expects code to run from there.	Joomla
☐	**Remove Unneeded Joomla Core "fluff"** Remove the left over core fluff files that Joomla installs, like build files, and text files for readmes etc.	Joomla
☐	**Review Renamed Files (.old, .bak, .orig)** Finds files renamed with a .bak, .backup or .old ending, commonly a config file left with old credentials in it, or a copy of a hacked file kept for later.	Joomla
☐	**Uploaded Tmp Files/Folders Should Be Removed** Finds leftover folders in Joomla's tmp directory from extension installs, which can contain PHP files that are still callable directly from a browser.	Joomla
☐	**Zend/ionCube Encrypted Files Should Be Avoided** Encoded PHP files hide their real source code from our scanner, so a Zend Guard or ionCube file could be running anything, including a backdoor.	Joomla
☐	**"php.ini" and ".user.ini" Override Files Located In Webspace** Finds php.ini and .user.ini files that silently override PHP's settings for a single folder, worth knowing about even when you put them there yourself.	WordPress

☐	**File Permissions Of 777 Should Be Avoided** Finds files and folders set to permission 777, which lets any other user on a shared server read, write and execute them, not just your account.	WordPress
☐	**Files Modified Between Audits** Compares the MD5 hash of every file against the previous audit and flags any that changed, catching edits that fall outside the three-day recent-changes window.	WordPress
☐	**Files Modified In Last Three Days** Lists every file changed in the last three days by its modification time, so a sudden burst of edits you did not make stands out fast.	WordPress
☐	**Files That Could Not Be Audited, Review Manually** Lists files our audit could not finish checking, usually because they exceeded your server's time limit or file size during the scan, so review them manually.	WordPress
☐	**Identify Files With No Content (Zero Bytes In Size)** Finds files that exist but hold no data at all, sometimes a hacker's waymarker, sometimes a blank index.php stopping directory listings, so each needs a look.	WordPress
☐	**Identify Missing Core WordPress Files** Compares your webspace against the WordPress core file list and flags anything missing, which can mean a broken upgrade or files deleted to hide a compromise.	WordPress
☐	**Investigate And Remove /wp-content/debug.log** A world-readable debug.log from the WP_DEBUG_LOG setting can log database queries, file paths and PHP errors, handing a visitor detail about your internals.	WordPress
☐	**Locate And Review Any SQL Files That Are Publicly Available** Finds .sql files sitting in a publicly reachable location, which is how a full database backup, including password hashes, ends up downloadable by anyone.	WordPress
☐	**Locate And Review Archive Files (Zip, Tar.gz, Etc)** Finds zip, tar and gzip archives in your webspace, which take up space unnecessarily and are also how attackers bulk-upload a whole toolkit of files in one go.	WordPress
☐	**Locate And Review Double Extension Files (name.php.xxx)** Locate files where .php is not the final extension (name.php.json) - a common malware-evasion pattern	WordPress
☐	**Locate And Review Files Over 2Mb Size** Lists every file over 2MB so you can see what is actually using your disk space, since attackers also favour large archives to smuggle in many files at once.	WordPress
☐	**Locate And Review Hidden Files ("dot Files", .DS_Store Etc)** Lists every file whose name starts with a dot, including .htaccess by design, because attackers also favour dot-prefixed names to stay off a normal file listing.	WordPress
☐	**Multiple .htaccess Files Located In Webspace** Counts .htaccess files across the whole webspace; a site needs one, so more than a handful outside the root is unusual and worth investigating.	WordPress
☐	**PHP error_log Files Should Be Reviewed And Deleted** Finds PHP error_log files, which record file paths and code errors that a well-running site should not be generating, and that an attacker can read for reconnaissance.	WordPress
☐	**PHP Files Should Not Be In These Certain Folders** Flags PHP files sitting inside the /images folder, a favourite hiding place for an uploaded backdoor because nobody expects code to run from there.	WordPress
☐	**Review Renamed Files (.old, .bak, .orig)** Finds files renamed with a .bak, .backup or .old ending, commonly a config file left with old credentials in it, or a copy of a hacked file kept for later.	WordPress

- [ ] **Scan For Files Not Bundled With WordPress Core** — WordPress
  Checks wp-admin and wp-includes, folders WordPress core owns exclusively, for files never shipped in a WordPress release and with no reason to be there.
- [ ] **Zend/ionCube Encrypted Files Should Be Avoided** — WordPress
  Encoded PHP files hide their real source code from our scanner, so a Zend Guard or ionCube file could be running anything, including a backdoor.

Folders

10

Folder permissions, writable paths, and directories left behind by an install.

- [ ] **Folder Permissions That Should Be Avoided** — Generic
  Scans every folder for 0777 (world-writable) permissions, which let any other process on a shared server read, write or replace your files.
- [ ] **Paths With Hidden Folders In Them** — Generic
  Looks for folders with a dot-prefixed name, which some FTP clients and file managers hide by default, making them a handy place to stash something malicious.
- [ ] **"tmp/logs" Folders Should Be Writable** — Joomla
  Checks whether the tmp and logs folders configured in Joomla are writable, since Joomla writes temporary files and its error log there and breaks without access.
- [ ] **Folder Permissions That Should Be Avoided** — Joomla
  Scans every folder for 0777 (world-writable) permissions, which let any other process on a shared server read, write or replace your files.
- [ ] **Installation Folders Should Be Deleted** — Joomla
  Checks for a leftover Joomla installation folder, even one renamed to hide it, since leaving it in place risks someone finding and misusing it.
- [ ] **One Webspace Should Contain One Joomla Installation** — Joomla
  Counts how many Joomla installations exist inside the same webspace, since more than one risks a compromise in one spreading straight into the other.
- [ ] **Paths With Hidden Folders In Them** — Joomla
  Looks for folders with a dot-prefixed name, which some FTP clients and file managers hide by default, making them a handy place to stash something malicious.
- [ ] **Folder Permissions That Should Be Avoided** — WordPress
  Scans every folder for 0777 (world-writable) permissions, which let any other process on a shared server read, write or replace your files.
- [ ] **One Webspace Should Contain One WordPress Installation** — WordPress
  Counts how many WordPress installations exist inside the same webspace, since more than one risks a compromise in one spreading straight into the other.
- [ ] **Paths With Hidden Folders In Them** — WordPress
  Looks for folders with a dot-prefixed name, which some FTP clients and file managers hide by default, making them a handy place to stash something malicious.

Extensions and plugins

8

The third-party code with the same privileges as the CMS itself.

- [ ] **"Behaviour - Backward Compatibility 6" Plugin (plg_behaviour_compat6, J5 Classes) - Warning! LEARN before disabling!** — Joomla — **1-click fix**
  Reports whether the plugin that keeps deprecated Joomla 5 classes working is still enabled, letting old extensions run before the next major upgrade.

"Behaviour - Backward Compatibility" Plugin (plg_behaviour_compat, J4 Classes) - Warning! LEARN before disabling! Reports whether the plugin keeping deprecated Joomla 4 classes working on Joomla 5 is still enabled, delaying extension updates needed for Joomla 6.	Joomla	**1-click fix**
Disable Joomla Guided Tours Plugin In Production Checks whether the Guided Tours plugin is published: it ships enabled by default and is an unnecessary surface once you know the admin console.	Joomla	**1-click fix** 60.3% fail
Disable Sample Data In Production Detect and disable the Joomla Sample Data module and its install plugins	Joomla	**1-click fix**
Enable Image Thumbnails To Speed Up Media Manager In Joomla 4.3+ Checks whether thumbnail generation is switched on in the Local filesystem plugin, since Media Manager becomes noticeably slower to browse without it.	Joomla	**1-click fix**
Privacy: Publish Privacy Consent Plugin Checks whether the built-in Joomla privacy consent plugin is enabled, which is what actually records that a user agreed before you process their data.	Joomla	
User Action Log Plugins Should Be Enabled Checks whether the Joomla action log plugins are enabled, so there is a record of who changed what if the site is later compromised.	Joomla	
Delete Files For Deactivated Plugins A deactivated plugin's files still sit on disk and can still be reactivated or reached directly, so any known vulnerability in its code remains part of your attack surface.	WordPress	

Discussion settings

5

Comment handling, and the settings that decide how much spam you moderate.

Disable Comments On New Articles If you dont need commenting on posts, then you should disable it to stop spamming	WordPress	**1-click fix**
Keep Comments Requiring Moderation At Zero Counts comments sitting in the moderation queue, because a growing backlog usually means spam is getting through the filters faster than anyone reviews it.	WordPress	
Keep Trashed Comments At Zero Counts comments sitting in the trash, which stay in the database taking up space until someone empties the bin permanently.	WordPress	
Require Comment Author Name And Email Checks whether commenters must supply a name and email address before submitting, a basic barrier against automated spam comments.	WordPress	**1-click fix**
Require Registration And Login To Comment Checks whether visitors must have a registered account before they can post a comment, since an open comment form is a magnet for spam bots.	WordPress	**1-click fix**

Writing settings

6

Post revisions, autosaves and the content the database keeps forever by default.

Default Post Category Should Not Be Uncategorised Checks whether new posts still default to the built-in Uncategorised category, a sign nobody has ever set up a proper category structure for the content.	WordPress	

- [ ] **Remove Auto-Save Revisions From The Database** — WordPress
  Counts WordPress's automatic autosave revisions sitting in the database, which build up unchecked and add nothing but extra rows to every query.
- [ ] **Remove Draft Posts And Pages From The Database** — WordPress
  Counts draft posts and pages left in the database, which build up over years of editing and add weight to both the database and its backups.
- [ ] **Remove Old Post Revisions From The Database** — WordPress
  Counts saved post revisions sitting in the database, which build up with every edit and slow every query as the table grows without limit.
- [ ] **Remove Post Via Email Settings Unless Required** — WordPress
  Checks whether WordPress's Post via Email feature is configured, since it stores your mailbox password on the site and lets anyone who finds the address post content.
- [ ] **Remove Trashed Posts And Pages From The Database** — WordPress
  Counts posts and pages sitting in the Trash, which stay in the database taking up space until someone empties it or WordPress does after 30 days.

Appearance 1

The active theme, and whether it is the one you think it is.

- [ ] **Avoid Using Default WordPress Themes** — WordPress
  Compares your active theme's name against every default WordPress theme ever shipped, since a stock theme is both a giveaway and a known target.