

JoomlON Security Scanner – FAQ

Frequently asked questions about com_joomionscanner (Joomla 5/6)

General

Does the scanner delete suspicious files?

No, **never automatically**. Suspicious files are only moved to a protected quarantine area (removed from the active web path, but kept safe). False positives can always be undone safely.

Do I need a licence or a subscription?

No. The scanner is free software (GPL). Updates come through a freely reachable update feed, without a licence key or registration.

Does the scanner work on Joomla 5 and 6?

Yes, both versions are supported.

Installation & plugins

Why two plugins? Wouldn't one be enough?

The two plugins have different jobs: the **task plugin** enables scheduled (automatic) scans via the Joomla task scheduler. The **system plugin** checks in the background for new scanner versions, so Joomla's own update notification appears reliably. Only a system plugin runs on every backend request – a task plugin would not achieve that.

Do I have to enable both plugins?

Not strictly for **manual** scans – the component works without them too. **Scheduled** scans need the task plugin, a **reliable update display** needs the system plugin. After installation a notice appears with buttons for both.

Why is a plugin disabled right after installation?

That is standard Joomla behaviour: newly installed plugins are always disabled by default, regardless of the extension. You can enable them with one click via System → Plugins or the enable buttons at the top of every scanner page.

Scan & core comparison

What is the difference between full, integrity and content scan?

The **full scan** runs every check (recommended). The **integrity scan** only compares against the core reference/baseline (faster, no signature/entropy analysis). The **content scan** focuses on malicious-code patterns in file content.

Exactly how does the core comparison compare files?

Exclusively via **SHA-256 hash** – not by file size. A matching hash practically always means identical content (and therefore identical size); a size comparison alone would be weaker and add no extra value.

Why isn't a very large file compared against the core reference?

Files above the configured **max file size** (default 6 MB, adjustable up to 64 MB) are neither scanned content-wise nor hashed against the core reference. Increase the value in the options if needed.

What do the traffic-light colours on "Load core reference" and "Update vulnerability DB" mean?

Red = missing, load urgently. **Yellow** (vulnerability DB only) = present but older than 24 hours – a refresh is recommended. **White** = fresh and up to date. The core reference has no "stale" state: a reference loaded for the installed Joomla version stays exactly valid until Joomla itself is updated.

The NVD import takes a very long time – is that normal?

Yes, the import runs in chunks over several minutes (shown by the waiting notice with a spinner and a pulsing bar). With your own **NVD API key** the query limits are higher, which speeds up the import.

Do I really need an NVD API key?

No, it is optional. Without a key the comparison against the VEL source still works normally, only the NVD query is more heavily throttled. A free key can be requested at nvd.nist.gov/developers/request-an-api-key and entered directly on the Scan page.

Findings & baseline

I marked a finding as a false positive – why does it reappear after the next scan?

A single full scan clears the findings list completely and rebuilds it. Only the **baseline** (stored checksums per file) is permanent: "add to the baseline" ensures the same file is not reported again as long as its content stays unchanged. Plain "ignore" only hides a finding until the next full scan.

Why do I see fewer findings than last time, even though I haven't changed anything?

Findings marked as a false positive/reviewed are hidden by default. A notice banner shows the number of hidden findings with a "show anyway" link (sets the status filter to "all").

An unknown file with high severity only shows up in the quiet overview list at the bottom – is that a bug?

No, that cannot happen: findings without a code pattern only move into the quiet overview list (with severity reduced to "Info") if their original severity is below "Medium". Findings rated "High" or "Medium" (e.g. an unknown PHP file) always stay visible in the main list and remain actionable through every button.

What is the difference between "foreign file" and "undeclared file"?

Foreign file (`unknown_file`) belongs neither to the core, nor to an installed extension, nor to the baseline – completely unknown origin. **Undeclared file** (`undeclared_file`) sits inside the folder of a known extension but is not part of that extension's install manifest – so it was not shipped directly by that extension's Joomla installer/updater (often harmless, e.g. cache/upload files, but can also be a file that was slipped in).

Can I filter findings by installed extension?

Yes, the filter dropdown on the Findings page lets you search and filter by a specific installed extension.

Directory protection & administrator protection

What is the difference between directory protection and administrator protection?

Directory protection uses `.htaccess` to block PHP execution in critical folders like `images/`, `tmp/`, `cache/` – preventing a malicious file placed there from being executed. **Administrator protection** is something entirely different: an extra password prompt (HTTP Basic Auth) in front of the entire `/administrator` area, independent of the normal Joomla login.

"Apply protection now" reports "not writable" – what do I do?

The affected directory is not writable for the webserver process – common on shared hosting, because PHP runs under a different system user than the FTP account the folder was originally created with. This can only be fixed via your host (correcting permissions/ownership), not by the scanner itself.

What happens to an existing `.htaccess` when I apply directory protection?

Any existing custom content is preserved – only a clearly marked JoomION block is inserted/updated.

"Remove protection" only takes that block back out again.

I already have a `.htaccess`/`.htpasswd` in administrator/ from another tool – what happens when I enable administrator protection?

The scanner detects this and shows an explicit warning. The JoomION block is then only appended, not replacing the existing content – check the file manually afterwards so the two rule sets don't contradict each other.

I forgot my administrator-protection password – what now?

Use "Set/change credentials" on the dashboard to set a new password (replaces the old one). If access to the backend itself is blocked, the `.htaccess`/`.htpasswd` in `administrator/` must be removed via FTP/file manager.

Scheduled scans & updates

How do I set up a daily automatic scan?

Enable the task plugin, then create a new task of type "JoomION Scanner" under System → Scheduled Tasks and set a schedule.

Why didn't a scanner update show up immediately in Joomla's notifications?

Joomla's update banner is tied to the Control Panel/Dashboard page and doesn't re-check on every page load. The system plugin mitigates this: it triggers a throttled check (at most once per hour) on every backend page load. An immediate, uncached check is available via System → Update → Extensions → "Find updates".

Security & false positives

Why does the scanner itself contain terms like "eval", "base64_decode" or "webshell" in its code?

That is the scanner's **detection database** – these are exactly the patterns it searches for to find malicious code on the site. Without them the scanner could not detect backdoors/web shells. They are never executed, only used as comparison patterns.

Is it safe to enter my NVD API key and GitHub token?

Both are stored exclusively locally in your own site's component configuration and are not passed on to third parties. They are only used for the respective official API query (NVD or GitHub) to get higher query limits.