

# JoomlON Security Scanner – FAQ

Häufige Fragen zu com\_joomionscanner (Joomla 5/6)

---

## Allgemein

### Löscht der Scanner verdächtige Dateien?

Nein, **nie automatisch**. Verdächtige Dateien werden ausschließlich in einen geschützten Quarantäne-Bereich verschoben (aus dem aktiven Web-Pfad entfernt, aber gesichert). Fehlalarme lassen sich jederzeit gefahrlos rückgängig machen.

### Brauche ich eine Lizenz oder ein Abo?

Nein. Der Scanner ist freie Software (GPL). Updates kommen über einen frei erreichbaren Update-Feed, ohne Lizenzschlüssel oder Registrierung.

### Funktioniert der Scanner auf Joomla 5 und 6?

Ja, beide Versionen werden unterstützt.

---

## Installation & Plugins

### Wozu zwei Plugins? Reicht nicht eins?

Die beiden Plugins haben unterschiedliche Aufgaben: Das **Task-Plugin** ermöglicht geplante (automatische) Scans über die Joomla-Aufgabenplanung. Das **System-Plugin** prüft im Hintergrund auf neue Scanner-Versionen, damit Joomla's eigene Update-Benachrichtigung zuverlässig erscheint. Nur ein System-Plugin läuft bei jedem Backend-Aufruf – ein Task-Plugin würde das nicht leisten.

### Muss ich beide Plugins aktivieren?

Für **manuelle** Scans nicht zwingend – die Komponente funktioniert auch ohne. Für **geplante** Scans ist das Task-Plugin nötig, für eine **zuverlässige Update-Anzeige** das System-Plugin. Nach der Installation erscheint ein Hinweis mit Buttons für beide.

### Warum ist ein Plugin nach der Installation deaktiviert?

Das ist Joomla's Standardverhalten: neu installierte Plugins sind grundsätzlich deaktiviert, unabhängig von der Erweiterung. Über System → Plugins oder die Aktivieren-Buttons oben auf jeder Scanner-Seite lässt sich das mit einem Klick nachholen.

---

## Scan & Kernabgleich

### Was ist der Unterschied zwischen Voll-, Integritäts- und Inhalts-Scan?

Der **Voll-Scan** führt alle Prüfungen aus (empfohlen). Der **Integritäts-Scan** vergleicht nur gegen Kernreferenz/Baseline (schneller, ohne Signatur-/Entropie-Analyse). Der **Inhalts-Scan** konzentriert sich auf Schadcode-Muster im Dateiinhalt.

### Wie genau vergleicht der Kernabgleich Dateien?

Ausschließlich per **SHA-256-Hash** – nicht per Dateigröße. Ein übereinstimmender Hash bedeutet praktisch immer identischen Inhalt (und damit auch identische Größe); ein Größenvergleich allein wäre schwächer und liefert daher keinen Zusatznutzen.

### Warum wird eine sehr große Datei nicht mit der Kernreferenz verglichen?

Dateien über der eingestellten **Max. Dateigröße** (Standard 6 MB, einstellbar bis 64 MB) werden weder inhaltlich gescannt noch gegen die Kernreferenz geshasht. Bei Bedarf den Wert in den Optionen erhöhen.

### Was bedeuten die Ampelfarben bei „Kernreferenz laden“ und „Schwachstellen-DB aktualisieren“?

**Rot** = fehlt, dringend laden. **Gelb** (nur bei der Schwachstellen-DB) = vorhanden, aber älter als 24 Stunden – Auffrischung empfohlen. **Weiß** = frisch und aktuell. Die Kernreferenz kennt kein „veraltet“: eine für die installierte Joomla-Version geladene Referenz bleibt exakt gültig, bis Joomla selbst aktualisiert wird.

### Der NVD-Import dauert sehr lange – ist das normal?

Ja, der Import läuft gehunkt über mehrere Minuten (erkennbar am Warte-Hinweis mit Spinner und pulsierendem Balken). Mit eigenem **NVD-API-Schlüssel** sind die Abfrage-Limits höher, was den Import beschleunigt.

### Brauche ich unbedingt einen NVD-API-Schlüssel?

Nein, er ist optional. Ohne Schlüssel funktioniert der Abgleich mit der VEL-Quelle weiterhin normal, nur die NVD-Abfrage ist stärker gedrosselt. Ein kostenloser Schlüssel lässt sich unter [nvd.nist.gov/developers/request-an-api-key](https://nvd.nist.gov/developers/request-an-api-key) anfordern und wird direkt auf der Scan-Seite eingetragen.

---

## Funde & Baseline

### Ich habe einen Fund als Fehlalarm markiert – warum taucht er beim nächsten Scan wieder auf?

Ein einzelner Voll-Scan leert die Fundliste komplett und baut sie neu auf. Nur die **Baseline** (gespeicherte Prüfsummen je Datei) ist dauerhaft: „In die Baseline übernehmen“ sorgt dafür, dass dieselbe Datei bei unverändertem Inhalt nicht erneut gemeldet wird. Reines „Ignorieren“ blendet einen Fund nur bis zum nächsten Voll-Scan aus.

### Warum sehe ich weniger Funde als beim letzten Scan, obwohl ich nichts geändert habe?

Als Fehlalarm/geprüft markierte Funde werden standardmäßig ausgeblendet. Ein Hinweis-Banner zeigt die Anzahl ausgeblendeter Funde mit einem Link „trotzdem anzeigen“ (Status-Filter auf „Alle“).

### Eine unbekannte Datei mit hohem Schweregrad taucht nur unten in der ruhigen Übersichtsliste auf – ist das ein Fehler?

Nein, das kann nicht passieren: Funde ohne Code-Muster wandern nur dann in die ruhige Übersichtsliste (mit reduziertem Schweregrad „Info“), wenn ihr ursprünglicher Schweregrad unter „Mittel“ liegt. Als „Hoch“ oder „Mittel“ eingestufte Funde (z. B. eine unbekannte PHP-Datei) bleiben immer in der Hauptliste sichtbar und über alle Aktionen bedienbar.

### Was ist der Unterschied zwischen „Fremde Datei“ und „Nicht deklarierte Datei“?

**Fremde Datei** (`unknown_file`) gehört weder zum Kern noch zu einer installierten Erweiterung noch zur Baseline – komplett unbekannte Herkunft. **Nicht deklarierte Datei** (`undeclared_file`) liegt zwar im Ordner einer bekannten Erweiterung, ist aber nicht Teil von deren Installationsmanifest – wurde also nicht direkt vom Joomla-Installer/-Updater dieser Erweiterung ausgeliefert (oft harmlos, z. B. Cache-/Upload-Dateien, kann aber auch eine untergeschobene Datei sein).

### Kann ich Funde nach installierten Erweiterungen filtern?

Ja, über das Filter-Pulldown auf der Funde-Seite lässt sich gezielt nach einer installierten Erweiterung suchen und filtern.

---

# Verzeichnisschutz & Administrator-Schutz

## Was ist der Unterschied zwischen Verzeichnisschutz und Administrator-Schutz?

Der **Verzeichnisschutz** blockiert per `.htaccess` die PHP-Ausführung in kritischen Ordnern wie `images/`, `tmp/`, `cache/` – verhindert also, dass eine dort abgelegte Schaddatei ausgeführt werden kann. Der **Administrator-Schutz** ist etwas völlig anderes: eine zusätzliche Passwortabfrage (HTTP Basic Auth) vor dem gesamten `/administrator`-Bereich, unabhängig vom normalen Joomla-Login.

## „Schutz jetzt anwenden“ meldet „nicht beschreibbar“ – was tun?

Das betroffene Verzeichnis ist für den Webserver-Prozess nicht beschreibbar – häufig auf Shared-Hosting, weil PHP unter einem anderen Systembenutzer läuft als der FTP-Zugang, mit dem der Ordner ursprünglich angelegt wurde. Das lässt sich nur über den Hoster (Rechte/Besitzer korrigieren) beheben, nicht durch den Scanner selbst.

## Was passiert mit einer bereits vorhandenen `.htaccess`, wenn ich den Verzeichnisschutz anwende?

Vorhandener eigener Inhalt bleibt erhalten – nur ein klar markierter JoomION-Block wird eingefügt/aktualisiert. „Schutz entfernen“ nimmt ausschließlich diesen Block wieder heraus.

## Ich habe bereits eine `.htaccess`/`.htpasswd` in `administrator/` von einem anderen Tool – was passiert beim Aktivieren des Administrator-Schutzes?

Der Scanner erkennt das und weist explizit darauf hin. Der JoomION-Block wird dann nur ergänzt, nicht ersetzt – anschließend die Datei manuell prüfen, damit sich beide Regelwerke nicht widersprechen.

## Ich habe mein Administrator-Schutz-Passwort vergessen – was jetzt?

Über das Dashboard „Zugangsdaten setzen/ändern“ ein neues Passwort vergeben (ersetzt das alte). Ist der Zugriff auf das Backend selbst blockiert, muss die `.htaccess/.htpasswd` in `administrator/` per FTP/Datei-Manager entfernt werden.

---

# Geplante Scans & Updates

## Wie richte ich einen täglichen automatischen Scan ein?

Task-Plugin aktivieren, dann unter System → Geplante Aufgaben eine neue Aufgabe vom Typ „JoomION-Scanner“ anlegen und einen Zeitplan festlegen.

## Warum erschien ein Scanner-Update nicht sofort in den Joomla-Benachrichtigungen?

Joomlas Update-Balken ist fest an die Systemsteuerung/Dashboard-Seite gebunden und prüft nicht bei jedem Seitenaufruf neu. Das System-Plugin mildert das: es stößt bei jedem Backend-Aufruf gedrosselt (höchstens 1× pro Stunde) eine Prüfung an. Ein sofortiger, ungecachter Check ist über System → Aktualisierungen → Erweiterungen → „Nach Updates suchen“ möglich.

---

# Sicherheit & Fehlalarme

## Warum enthält der Scanner selbst Begriffe wie „eval“, „base64\_decode“ oder „webshell“ im Code?

Das ist die **Erkennungsdatenbank** des Scanners – genau diese Muster werden gesucht, um Schadcode auf der Site zu finden. Ohne sie könnte der Scanner keine Backdoors/Webshells erkennen. Sie werden nirgends ausgeführt, nur als Vergleichsmuster verwendet.

### **Ist es sicher, meinen NVD-API-Schlüssel und GitHub-Token einzutragen?**

Beide werden ausschließlich lokal in der Komponenten-Konfiguration der eigenen Site gespeichert und nicht an Dritte weitergegeben. Sie werden nur für die jeweilige offizielle API-Abfrage (NVD bzw. GitHub) verwendet, um höhere Abfrage-Limits zu erhalten.