GENISOFT WEB

# Genisoft Security Scanner

Installation and user guide · version 5.0.2

## 1. Overview

Genisoft Security Scanner is a **read-only** security scanner for PrestaShop. It never modifies, deletes, quarantines, includes or executes any file or database row: it inspects and reports, so it is safe to run on a live shop.

It looks for traces of an intrusion in two places: **the database** (where an infection survives a file cleanup) and **the shop files**.

## 2. Compatibility and requirements

- PrestaShop 1.7.1 to 9.x (tested on 1.7.1.2, 1.7.4.4, 1.7.6.9, 1.7.7.8 and 9.2.0).
- PHP 5.6 to 8.4 (PrestaShop 9 itself requires PHP 8.1 or later).
- English and French interface; texts go through the PrestaShop translation system.
- No external service: everything runs on your hosting.

## 3. Installation

1. In the back office: **Modules > Module Manager > Upload a module**, then drop the zip file.
2. Open **Advanced Parameters > Security Scanner** (or the module's "Configure" button).
3. Run a first database check, then a first file scan.

## 4. Dashboard sections

| Section | What it does |
|---|---|
| **1 · Database check** | Looks for hidden code in settings and content, administrator accounts, back-office pages and module hooks, scheduled tasks, SQL triggers/routines/events/views, webservice keys and Admin API clients, the shop domain and media servers. |
| **2 · File scan** | Looks for webshells, droppers, remote downloaders and front-office card skimmers. Step-by-step scan with progress, time estimate, pause and resume. |
| **3 · Automatic scan (cron)** | One URL to schedule from your hosting panel to check the shop regularly. |
| **4 · Email alerts** | One email, sent through the shop's own mail settings, when a new confirmed threat appears. |
| **5 · Ignored files** | Files you marked as safe: they are no longer reported while their content stays the same. |
| **6 · History and changes** | Compares each scan with the previous one: a file that appears between two scans is the typical sign of a re-infection. CSV exports. |
| **7 · Known vulnerable modules** | Flags installed modules with a publicly known critical vulnerability (list limited to a few modules). |

## 5. Understanding the results

- **Critical**: malicious beyond reasonable doubt. Act without delay.
- **To review**: needs your decision, because the item may be legitimate (for example an unusual administrator account or module).
- **Information**: context or housekeeping, never counted as a threat.
- Each finding says **what to do** and links to the relevant back-office page.
- SuperAdmin accounts are listed until you confirm you know them. A new or changed SuperAdmin is raised again.

> Check each detection before deleting a file: the scanner deletes nothing, and a “To review” finding can be legitimate.

## 6. Scheduling the automatic scan

Copy the URL shown in the “Automatic scan” section into your hosting scheduler (cron), for example once a day at 3 am. Keep this URL secret: it contains a token that protects it.

From the command line, in the shop folder:

```
php index.php "fc=module&module=genisoftsecurity&controller=cron"
```

Each run checks the database, continues the file scan and the change inventory, then sends a single email if something new needs your attention.

## 7. Privacy and security

- Every action requires the back-office permission of the Security Scanner tab (“view” to run scans, “edit” to change settings or mark items as reviewed).
- Only SELECT and SHOW statements are sent to the database. Password hashes and reset tokens are never read.
- Scan state and results are stored in a randomly named folder protected by a deny-all .htaccess. Database results (which include administrator emails) are stored in the module table, not in files.
- Uninstalling removes the module's settings, its table and every file the scans wrote.

## 8. Limits you should know

- It is a **detection** tool: it repairs nothing and cannot guarantee a shop is clean. A scan with no result does not prove there was no intrusion.
- The vulnerable-module list only covers a few modules.
- A module needs PrestaShop to boot: on a shop too damaged to start, it cannot run.
- A large shop can take several minutes to scan; the scan stops if you leave the page, use “Resume” to continue.

## 9. Support

Genisoft Web · contact@genisoft.fr · answers by email. Please give the PrestaShop version, the PHP version and the message displayed.

© 2026 Genisoft Web · contact@genisoft.fr · www.genisoft.fr