

ice Scanner Security

Ghid de utilizare · scaner de securitate pentru WordPress

Versiunea 1.26.11.1 · noiembrie 2026

icecode
software developer

Dezvoltat de Poienariu Alin · icecode.ro

Ce este ice Scanner Security

ice Scanner Security este un modul WordPress gratuit care verifică tot site-ul și îți arată, pe înțeles, ce pare în neregulă și unde. Modulul **doar citește**: nu modifică, nu mută și nu șterge nimic. De aceea îl poți rula liniștit pe un site în funcțiune.

Este gândit pentru găzduirile obișnuite (shared hosting): verificările mari se fac în tranșe scurte, așa că scanarea nu se oprește din cauza limitei de timp a serverului, nici pe site-urile mari.

Ce verifică

- **Nucleul WordPress** – fiecare fișier e comparat cu amprentele oficiale WordPress.org, pentru versiunea și limba site-ului.
- **Modulele** – cele de pe WordPress.org sunt comparate cu amprentele lor oficiale; cele premium sau proprii sunt verificate după tiparele codului periculos.
- **Temele** – verificate după aceleași tipare; temele inactive sunt semnalate.
- **Cod ascuns** – cod rulat din date codificate sau trimise din exterior, decodări în lanț, cod PHP ascuns în imagini.
- **Folderul de încărcări** – fișiere PHP, imagini cu cod, SVG-uri cu scripturi și dacă rularea PHP e blocată.
- **În afara WordPress** – foldere necunoscute, arhive și copii de siguranță care se pot descărca.
- **Configurarea** – reguli periculoase în .htaccess, .user.ini și php.ini, modul de depanare, editorul de fișiere.
- **Baza de date** – administratorii (cei noi sunt evidențiați), înregistrarea deschisă, scripturi salvate în setări sau articole.
- **Schimbările** – fișierele noi sau modificate de la scanarea anterioară.

Cuprins

1. Instalarea
2. Prima scanare
3. Cum citești raportul
4. View, Ignore, Download the report
5. Setările
6. Antivirusul găzduirii (cPGuard, Imunify360)
7. Întrebări frecvente

1. Instalarea

1. Descarcă arhiva `icecodero-security-scanner-1.26.11.1.zip` de pe **icecode.ro/module-wordpress/**. Modulul se găsește și direct în panou, la Module → Adaugă modul, căutând „ice Scanner Security”.
2. În panoul WordPress mergi la **Module** → **Adaugă modul** → **Încarcă modul**, alege arhiva și apasă **Instalează acum**.
3. Apasă **Activează**. În meniul din stânga apare **ice Scanner Security**, cu pictograma scut.

> Modulul cere WordPress 6.0 sau mai nou și PHP 7.4 sau mai nou. Funcționează pe orice găzduire, inclusiv cPanel. Interfața este momentan în engleză, așa că în ghid denumirile butoanelor sunt în engleză.

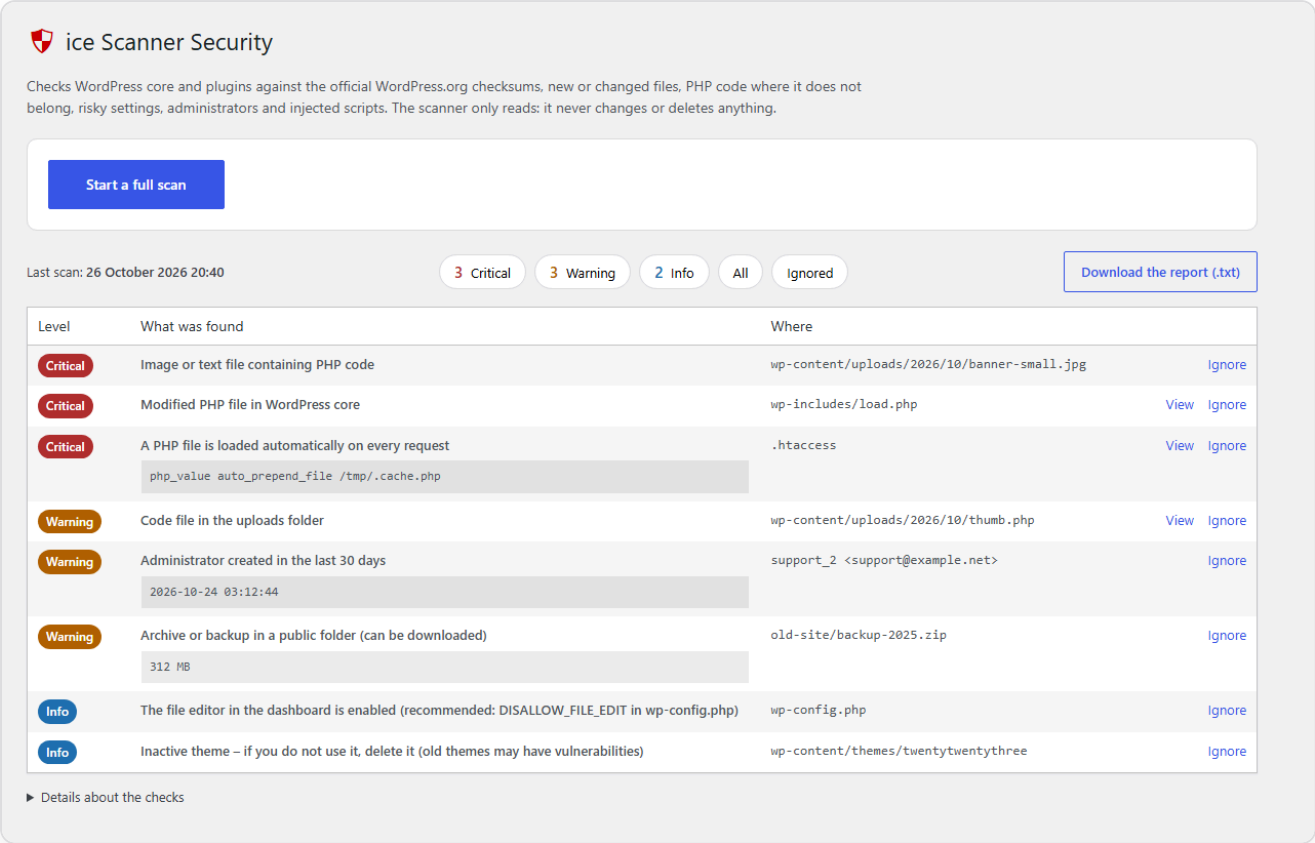
2. Prima scanare

1. Deschide **ice Scanner Security** din meniul din stânga.
2. Apasă **Start a full scan**.
3. Urmărește bara de progres: fiecare pas (nucleul, fiecare modul, fiecare temă, încărcările, baza de date) apare pe rând. Pașii mari continuă automat în tranșe.
4. La final, pagina se reîncarcă și afișează raportul.

O scanare durează de obicei între un minut și câteva minute, în funcție de mărimea site-ului. Poți lăsa pagina deschisă și lucra în alt tab.

> La prima scanare, ice Scanner Security salvează amprenta tuturor fișierelor. De la a doua scanare îți arată exact ce fișiere au apărut sau s-au schimbat între timp – cel mai bun semn că cineva a umblat la site.

3. Cum citești raportul



Raportul: constatările grupate pe niveluri, cu fișierul și, unde e cazul, fragmentul de cod.

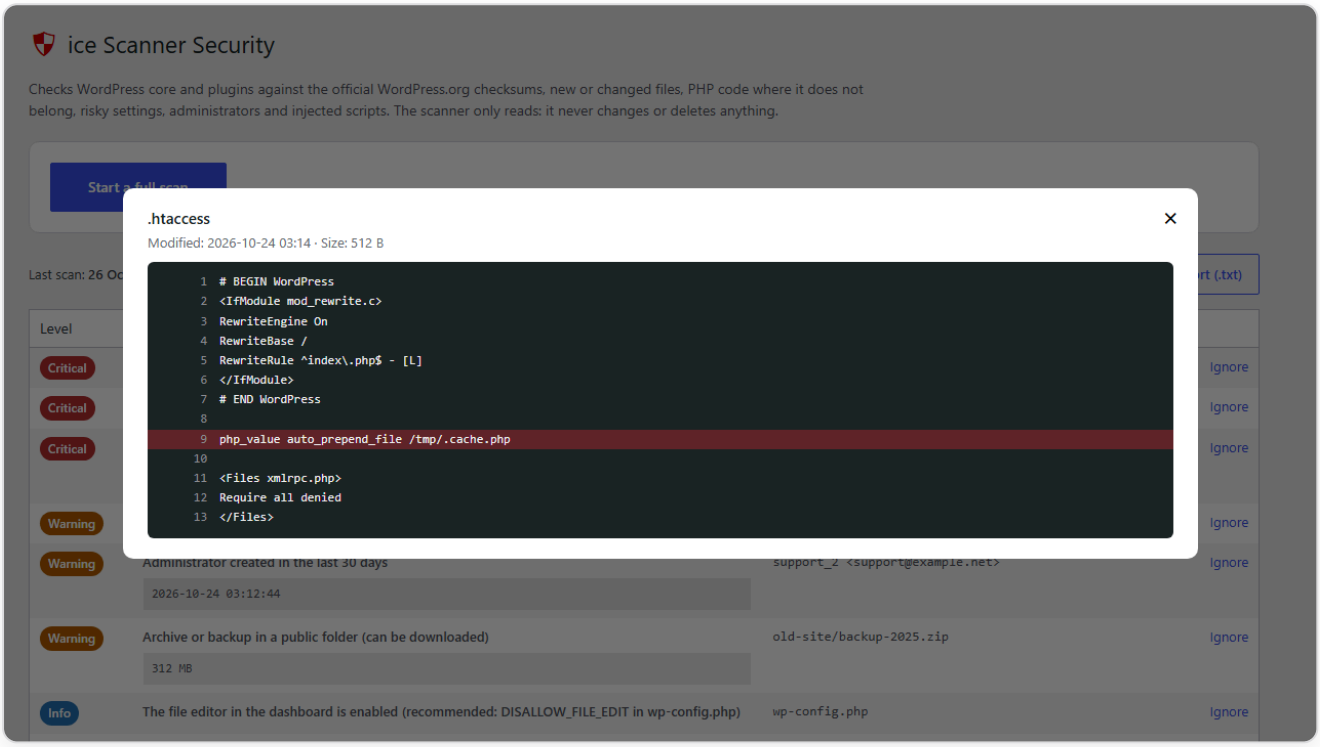
Nivel	Ce înseamnă	Ce faci
Critical	Foarte probabil un atac sau o setare periculoasă: cod modificat în nucleu, cod PHP ascuns într-o imagine, fișiere încărcate automat la fiecare cerere.	Verifici imediat. Dacă nu știi de unde vine, cere ajutorul unui specialist.
Warning	Suspect sau riscant: fișiere de cod în încărcări, administratori noi, arhive descărcabile.	Verifici dacă le cunoști; altfel le elimini.
Info	Bine de știut: lista administratorilor, teme inactive, editorul de fișiere pornit.	Recomandări, nu probleme.

Butoanele de deasupra tabelului filtrează lista: **Critical**, **Warning**, **Info**, **All** și **Ignored**. La deschidere, raportul arată automat cel mai grav nivel care are constatări.

4. View, Ignore, Download the report

View

Butonul **View** deschide fișierul direct în panou, cu rândurile din jurul problemei și linia suspectă marcată cu roșu. Fișierul `wp-config.php` nu se afișează niciodată, pentru că are parolele bazei de date.



Fereastra „View": rândul suspect din .htaccess, marcat cu roșu.

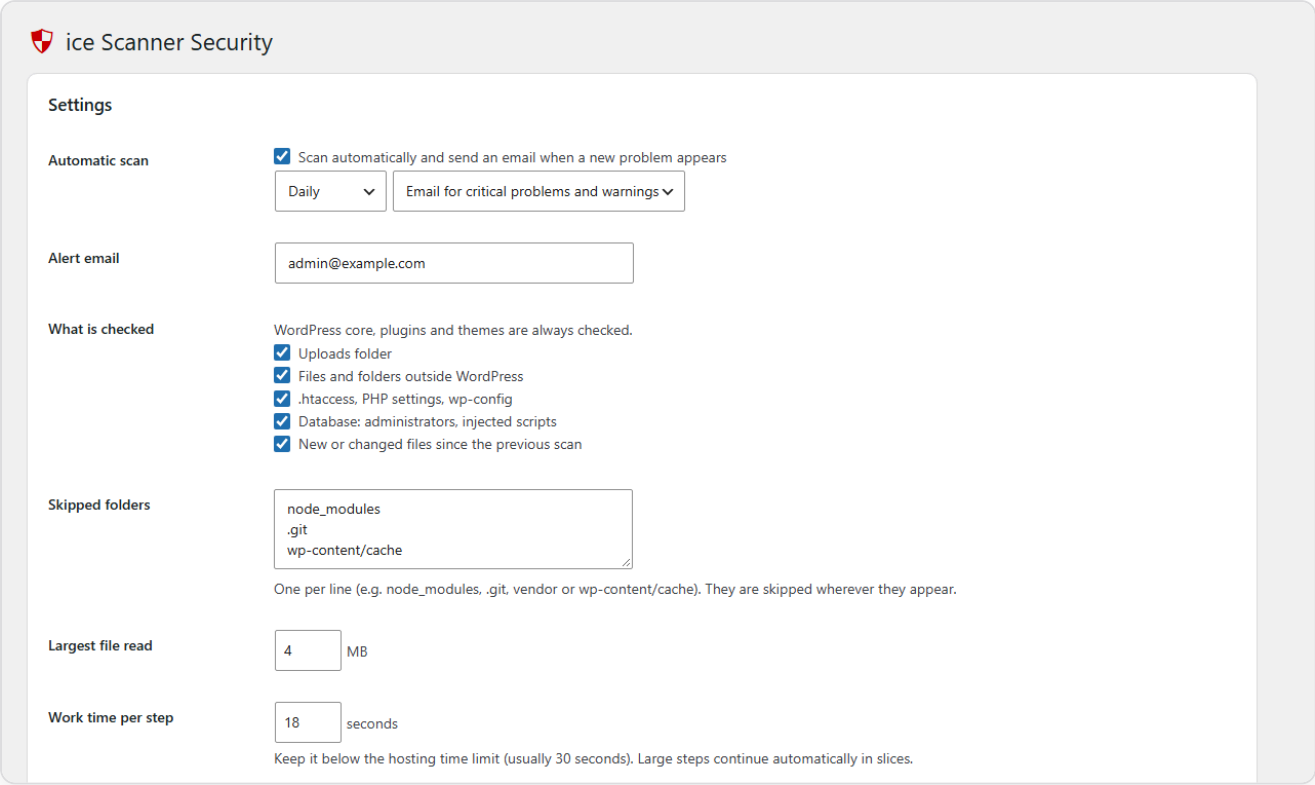
Ignore

Dacă ai verificat o constatare și știi că e în regulă (de exemplu, un modul care folosește intenționat un fișier în uploads), apasă **Ignore**. Constatarea nu mai apare la scanările următoare și nu mai e numărată. O găsești oricând la filtrul **Ignored**, de unde o poți readuce cu **Restore**.

Download the report

Download the report (.txt) salvează lista constatărilor într-un fișier text, util pentru arhivă sau pentru a-l trimite unui specialist.

5. Setările



Setările se află sub raport, pe aceeași pagină.

Setare	Ce face
Automatic scan	Scanează singur de două ori pe zi, zilnic sau săptămânal și îți trimite un email *doar* când apare o problemă nouă. Poți alege emailuri pentru probleme critice și de atenție sau doar pentru cele critice.
Alert email	Adresa la care primești alertele. Implicit, emailul administratorului site-ului.
What is checked	Poți opri pașii opționali: încărcări, fișiere din afara WordPress, configurare, baza de date, schimbări. Nucleul, modulele și temele se verifică mereu.
Skipped folders	Câte unul pe rând (de exemplu `node_modules`, `.git`, `wp-content/cache`). Se sar oriunde apar – util pentru folderele mari de cache sau copii de siguranță.
Largest file read	Fișierele mai mari (de obicei arhive sau imagini mari) nu se citesc. Implicit 4 MB.
Work time per step	Câte secunde lucrează scanerul la o cerere. Păstrează-l sub limita găzduirii (de obicei 30 s). Implicit 18 s.

6. Antivirusul găzduirii

Un scaner de securitate conține tiparele codului periculos pe care îl caută. Din acest motiv, unele antivirusuri de pe servere îl pot considera suspect și îi pot muta fișierele în carantină. Dacă modulul dispare sau nu mai pornește, adaugă folderul `wp-content/plugins/icecodero-security-scanner` la excepții, apoi încarcă modulul din nou:

- **cPGuard**: cPanel → Security → cPGuard → Settings → Virus Scanner → **Whitelist Files**.
- **Imunify360**: fișierele găsite apar în cPanel → Imunify360; cere firmei de găzduire să adauge folderul la lista de excepții Imunify360.

7. Întrebări frecvente

Modulul îmi schimbă sau îmi șterge fișiere?

Nu. Toate verificările doar citesc. Orice reparație rămâne decizia ta.

Încetinește site-ul?

Nu. Scanerul rulează doar când îl pornești tu sau la scanarea automată. Vizitatorii nu simt nimic.

Ce date trimite în afara site-ului?

Doar versiunea WordPress, limba site-ului și numele și versiunile modulelor, către WordPress.org, ca să descarce amprentele oficiale – aceleași informații pe care WordPress le trimite oricum la verificarea actualizărilor. Nu trimite nimic despre conținut, utilizatori sau vizitatori.

Scanarea se oprește pe un site mare.

Scade „Work time per step” (de exemplu la 10 secunde) și adaugă la „Skipped folders” folderele mari care nu trebuie verificate.

> Ai nevoie de ajutor cu un site compromis sau vrei un modul WordPress făcut pentru tine? Scrie-ne la **alin.poienariu@icecode.ro**.