RAPORT EXEMPLU — DATE FICTIVE

Raport Audit de Securitate WordPress

Exemplu ilustrativ al formatului și nivelului de detaliu pe care îl primești — pachet Audit Complet.

SITE ANALIZAT	DATA RAPORTULUI	PACHET	ID RAPORT
demo-magazin-online.ro	03 iulie 2026	Audit Complet	LOTCA-EX-0417

62/100

Necesită atenție

Site-ul funcționează, dar are câteva probleme critice care merită rezolvate curând — nimic ireparabil, dar nici de ignorat.

3	5	4
CRITICE	IMPORTANTE	RECOMANDATE

Acesta este un raport exemplu. Site-ul, datele și problemele de mai jos sunt fictive — au rolul de a arăta cum arată un raport real: pe zone, cu severitate clară (Critic / Important / Recomandat) și recomandare pentru fiecare. Raportul tău va reflecta exact situația site-ului tău, nu un șablon generic.

1. Malware & backdoor-uri

CRITIC

Fișier PHP suspect în wp-content/uploads/2019/temp-cache.php

Cod obfuscat (base64_decode + eval), tipic pentru un backdoor folosit pentru acces neautorizat.

Recomandare: eliminare imediată a fișierului, schimbarea tuturor parolelor (WP, hosting, FTP) și scanare completă a serverului.

RECOMANDAT

Nicio infecție activă în restul instalării

Fișierele core WordPress și temele active sunt curate — nimic modificat neautorizat.

Recomandare: menține scanări periodice, mai ales după instalarea de plugin-uri noi.

2. Plugin-uri & teme

CRITIC

Plugin fals, deghizat în „WP Cache Booster Pro"

Nu există în repository-ul oficial WordPress — a fost încărcat manual printr-un fișier .zip și imită numele unui plugin de caching cunoscut. Codul contactează un server extern și descarcă fișiere suplimentare la fiecare rulare.

Recomandare: elimină imediat pluginul, verifică fișierele nou create în ultimele 30 de zile și schimbă toate parolele de acces.

IMPORTANT

Plugin premium „nulled" (piratat) instalat: Advanced Custom Fields Pro

Versiune descărcată de pe un site terț, cu verificarea licenței dezactivată manual în cod. Nu primește actualizări oficiale de securitate, iar fișierele au fost modificate față de originalul distribuit de autor.

Recomandare: înlocuiește cu o licență originală sau o alternativă gratuită din repository-ul oficial și verifică pluginul pentru cod adăugat suplimentar.

IMPORTANT

Plugin de formular de contact neactualizat din 2021

Versiune abandonată, cu o vulnerabilitate cunoscută de tip XSS (script injectat prin câmpurile formularului).

Recomandare: înlocuire cu o alternativă întreținută activ sau actualizare la ultima versiune disponibilă.

RECOMANDAT

Tema activă e la zi; 2 teme neutilizate sunt încă instalate

Nu sunt active, dar rămân o suprafață de atac inutilă dacă nu sunt actualizate.

Recomandare: șterge temele neutilizate din Aspect → Teme.

3. Hardening & configurare

IMPORTANT

XML-RPC activ și expus public

Vector comun pentru atacuri brute-force și amplificare DDoS (pingback.ping).

Recomandare: dezactivează XML-RPC dacă nu e folosit de aplicații externe (Jetpack, app mobil etc.).

IMPORTANT

Zona de administrare nu forțează conexiune SSL

wp-config.php nu are FORCE_SSL_ADMIN activ — datele de logare pot circula necriptate în anumite condiții.

Recomandare: activează FORCE_SSL_ADMIN și confirmă certificatul SSL e valid pe tot domeniul.

4. Utilizatori & bază de date

CRITIC

Cont administrator cu username „admin" și parolă slabă

Combinație frecvent testată automat de roboți — cel mai comun punct de intrare pentru atacuri brute-force.

Recomandare: redenumește contul, setează o parolă unică de minim 16 caractere și activează autentificare în doi pași.

RECOMANDAT

Prefixul tabelelor din baza de date e cel implicit (wp_)

Nu e o vulnerabilitate în sine, dar simplifică unele atacuri automate de tip SQL injection.

Recomandare: schimbă prefixul cu ocazia următorului backup major.

5. Expunere publică

IMPORTANT

Fișier de backup accesibil public

/wp-content/backup-2024.zip poate fi descărcat de oricine — conține baza de date completă.

Recomandare: mută backup-urile în afara directorului public sau într-o zonă protejată prin parolă.

RECOMANDAT

Fișierul readme.html implicit expune versiunea WordPress

Informație minoră, dar utilă unui atacator pentru a ținti vulnerabilități cunoscute ale versiunii respective.

Recomandare: șterge sau blochează accesul la readme.html.

Ce facem întâi — ordinea recomandată

1. Elimină fișierul backdoor și pluginul fals „WP Cache Booster Pro", apoi schimbă toate parolele de acces (Critic).
2. Redenumește contul de administrator și activează autentificare în doi pași (Critic).
3. Mută sau protejează backup-ul expus public (Important).
4. Înlocuiește pluginul „nulled" (Advanced Custom Fields Pro) cu o licență originală sau o alternativă din repository-ul oficial (Important).
5. Actualizează sau înlocuiește plugin-ul de formular vulnerabil (Important).
6. Dezactivează XML-RPC și activează FORCE_SSL_ADMIN (Important).
7. Rezolvă punctele „Recomandat" cu ocazia următoarei mentenanțe.

Notă: pentru pachetul **Audit + Remediere**, primești și un raport „înainte / după" — exact ca acesta, dar cu fiecare problemă marcată ca rezolvată, plus ce am schimbat concret. Acesta a fost un exemplu — raportul tău va reflecta situația reală a site-ului tău, nu un șablon generic.