

قائمة التحقق: حماية موقعك من PHP2Shell

CHECKLIST: PROTECT YOUR WEBSITE FROM PHP2SHELL



Techno Committee · Life Pulse Volunteer Team · October 2026

لجنة التكنو · فريق نبضة حياة التطوعي · أكتوبر 2026

1. تحقق خلال 10 دقائق STEP 1: CHECK IN 10 MINUTES

هل موقعي يعمل بـ PHP؟ (WordPress, Joomla, Laravel, أغلب المتاجر: نعم) ☐
Does my site run PHP? (WordPress, Joomla, Laravel, most stores: yes)

ما نسخة PHP؟ WordPress: الأدوات ← صحة الموقع ← معلومات ← الخادم. غير كذا: اسأل الاستضافة ☐
Which PHP version? WordPress: Tools, Site Health, Info, Server. Otherwise ask your host

هل النسخة ضمن النسخ الآمنة؟ ☐
Is it one of the safe versions below?

8.2.35

8.3.36

8.4.27

8.5.12

2. الإصلاح STEP 2: THE FIX

نسخة احتياطية كاملة (الملفات + قاعدة البيانات) قبل أي شيء ☐
Full backup (files + database) before anything else

تحديث PHP من لوحة الاستضافة (cPanel / Plesk / CloudPanel) أو عبر المطور ☐
Update PHP from the hosting panel (cPanel / Plesk / CloudPanel) or via your developer

سيرفر خاص على Ubuntu/Debian: apt update && apt upgrade ثم إعادة تشغيل php-fpm ☐
Own server on Ubuntu/Debian: apt update && apt upgrade, then restart php-fpm

تأكد إن الموقع يفتح وبشغل بعد التحديث (الصفحة الرئيسية، تسجيل الدخول، نموذج اتصال) ☐
Confirm the site works after updating (home page, login, a contact form)

3. إذا ما تقدر تحدّث اليوم STEP 3: IF YOU CANNOT UPDATE TODAY

فعل Cloudflare (البروكسي البرتقالي) أو أي جدار حماية WAF ☐
Enable Cloudflare (orange proxy) or any WAF

في php.ini: session.upload_progress.enabled = Off وقلّل post_max_size ☐
In php.ini: session.upload_progress.enabled = Off, and reduce post_max_size

لا تعرّض لوحات الإدارة للإنترنت بدون حماية إضافية ☐
Do not expose admin panels to the internet without extra protection

4. بعد التحديث STEP 4: AFTER UPDATING

افحص الموقع بأداة فحص خارجية ☐
Scan the site with an external scanner

غيّر كلمات مرور الإدارة والاستضافة ☐
Change admin and hosting passwords

أبلغ أي جهة تعرفها عندها موقع ☐
Tell any organisation you know that runs a website

راجع الملفات المعدلة آخر 7 أيام ☐
Review files modified in the last 7 days

علامات تدل إن الموقع مخترق: ملفات .php جديدة ما تعرفها، صفحات غريبة، بطء مفاجئ، تحويل الزوار لمواقع ثانية، أو تحذير من Google. إذا شفت أي منها: افصل الموقع مؤقتاً وتواصل مع مختص.

Signs of compromise: unknown new .php files, strange pages, sudden slowness, visitors redirected elsewhere, or a Google warning. If you see any: take the site offline temporarily and contact a specialist.