



چک‌لیست کامل امنیت وردپرس

۱. ورود و احراز هویت

- حذف نام کاربری admin و ساخت یوزر مدیر با نام غیر قابل حدس
- انتخاب رمز قوی بالای ۱۶ کاراکتر برای همه مدیران
- تغییر آدرس ورود از wp-admin.php به آدرس اختصاصی
- محدود کردن تلاش ورود ناموفق (Limit Login Attempts)
- فعال‌سازی کپچا در فرم ورود، ثبت‌نام و نظرات
- غیرفعال کردن گزینه «نمایش راهنمایی خطا در ورود» که مشخص می‌کند یوزر اشتباه است یا پسورد
- تنظیم خروج خودکار کاربران بعد از ۴۸ ساعت عدم فعالیت

۲. کاربران و دسترسی‌ها

- غیرفعال کردن ثبت‌نام عمومی در تنظیمات > عمومی اگر فروشگاه یا عضویت نداری
- بررسی نقش کاربران و دادن حداقل دسترسی لازم
- حذف کاربران قدیمی، تستی و غیرفعال
- اجبار همه کاربران به استفاده از رمز قوی
- غیرفعال کردن ویرایش فایل قالب و افزونه از پیشخوان



۳. هسته، قالب و افزونه

- به روزرسانی همیشه هسته وردپرس، قالب و افزونه‌ها به آخرین نسخه
- حذف کامل قالب‌ها و افزونه‌های غیرفعال و بلااستفاده
- دانلود قالب و افزونه فقط از مخزن وردپرس، ژاکت یا راست‌چین — هرگز نال‌شده نصب نکن
- فعال‌سازی آپدیت خودکار برای به‌روزرسانی‌های امنیتی جزئی
- بررسی هفتگی افزونه‌های آسیب‌پذیر با Wordfence Scan

۴. افزونه امنیتی و فایروال

- نصب یکی از این‌ها Wordfence Security یا Solid Security (iThemes)
- فعال‌سازی فایروال (WAF) در حالت Extended Protection
- فعال‌سازی اسکن خودکار بدافزار هفته‌ای یک‌بار
- مسدود کردن IP های با حمله مکرر
- فعال‌سازی اعلان ایمیلی برای ورود مدیر و تغییر فایل‌ها

۵. هاردنینگ وردپرس

- غیرفعال کردن XML-RPC اگر به اپلیکیشن موبایل یا اتصال خاص نیاز نداری
- غیرفعال کردن اجرای PHP در پوشه uploads با فایل htaccess.



- محافظت از فایل wp-config.php و htaccess با محدود کردن دسترسی به ۴۴۰ و ۴۴۴

- مخفی کردن نسخه وردپرس از سورس سایت
- غیرفعال کردن REST API برای کاربران مهمان اگر لازم نیست
- جلوگیری از نمایش لیست فایل‌ها در پوشه‌ها (Directory Listing)
- تغییر پیشوند دیتابیس از wp_ به پیشوند رندوم هنگام نصب

۶. سرور و هاست

- فعال بودن گواهی SSL و اجبار کل سایت به https
- فعال‌سازی HSTS در هاست
- استفاده از PHP نسخه ۸.۱ یا ۸.۲
- فعال بودن ModSecurity و LiteSpeed Security در هاست
- جدا بودن هاست بکاپ از هاست اصلی
- غیرفعال بودن FTP ناامن و استفاده از SFTP با رمز قوی
- تغییر پورت پیش‌فرض دایرکت‌ادمین / سی‌پنل در سرور مجازی

۷. بکاپ و مانیتورینگ

- تنظیم بکاپ خودکار روزانه دیتابیس + هفتگی فول‌بکاپ
- ذخیره بکاپ در فضای ابری مثل گوگل‌درایو، نه فقط روی همان هاست



- تست یکبار ریستور بکاپ برای مطمئن شدن از سالم بودن آن
- فعال سازی لاگ فعالیت کاربران با افزونه WP Activity Log
- بررسی ماهانه لینک های اسپم و تغییرات مشکوک در فایل ها

۸. اشتباهات رایج که هک می شوی

- عدم استفاده از یک رمز برای هاست، وردپرس و ایمیل
- عدم ورود به پیشخوان با وای فای عمومی بدون VPN
- عدم دادن دسترسی مدیر به طراح یا سئوکار — فقط Editor یا Shop Manager کافی است
- اسکن کامپیوتر شخصی با آنتی ویروس، چون خیلی از هک ها از سیستم خودت شروع می شود