چک لیست امنیت سایت وردپرس

راست‌چین
RTL-THEME

چک لیست امنیت سایت وردپرس

۸۴٪ از سایت‌های وردپرسی در دنیا مستعد هک شدن هستند و آمار نشان می‌دهد که در طول روز بیش از ۱۳۰۰۰۰ سایت وردپرسی هک می‌شوند. سوال اینجاست آیا وردپرس امن نیست؟

تفاوتی ندارد پلتفرم شما چیست، زیرا هر سایتی در معرض آلوده شدن قرار دارد. وردپرس یک سیستم مدیریت محتوای امن است؛ اما زمانی که شما استانداردهای اولیه امنیتی را رعایت نکنید وردپرس نیز به راحتی هک می‌شود. پس قبل از اینکه دیر شود با انجام یکسری اقدامات از سایت خود محافظت کنید.

برای اینکه سایت خود را به یک سپر امن در برابر حملات سایبری تبدیل کنید به دانش تخصصی نیاز ندارید. در اینجا با ساده‌ترین راهکارهای عملی یک چک لیست تهیه کرده‌ایم تا شما بتوانید به صورت گام به گام آنها را انجام دهید.

☑ وردپرس را آپدیت نگه دارید

در هر نسخه از وردپرس، حفره‌های امنیتی و مشکلات قبلی حل می‌شود، بنابراین نصب یا آپدیت وردپرس به آخرین نسخه، خطرات امنیتی را کاهش می‌دهد. در آموزش آپدیت وردپرس می‌توانید نحوه انجام این کار به دو روش دستی و خودکار مشاهده کنید.

☑ قالب و افزونه‌ها را به روزرسانی کنید

افزونه‌ها در صورتی که آپدیت نشوند می‌توانند مدخل ورود هکرها باشند. به محض انتشار بروزرسانی جدید، قالب و افزونه‌های نصب شده را آپدیت کنید. آموزش آپدیت قالب وردپرس به شما کمک می‌کند، اینکار را به سادگی انجام دهید.

☑ از قالب‌ها و افزونه‌های نال شده استفاده نکنید

به هیچ وجه از قالب‌های نال شده استفاده نکنید؛ زیرا در صورت آلوده بودن باعث مشکلاتی مانند نفوذ هکرها، سرقت اطلاعات و نمایش تبلیغات ناخواسته در سایت‌تان می‌شوند.

☑ از نام کاربری و رمز عبور ساده مثل Admin استفاده نکنید

استفاده از نام‌های کاربری و رمز عبورهای ساده مثل Admin امکان هک سایت و حملات بروت فورس را افزایش می‌دهد. در پسوردتان از ترکیب حروف بزرگ و کوچک، اعداد و سایر علایم مانند نقطه، کاما، ۳، @ و... استفاده کنید. برای افزایش امنیت صفحه ثبت‌نام/ورود، می‌توانید راهکارهای امنیت صفحه لاگین را ببینید.

بکاپ گیری دوره‌ای را فراموش نکنید

هر چند بکاپ‌گیری مانع از حملات امنیتی نمی‌شود؛ اما در صورت بروز هر مشکل با داشتن بکاپ، در زمان کوتاهی می‌توانید سایت را به سرعت به آخرین نسخه سالم برگردانید. آموزش بکاپ گرفتن در هاست Cpanel و دایرکت ادمین ببینید.

سایت خود را برای شناسایی بدافزارها (Malewares) اسکن کنید

سایتتان را به صورت دائمی با افزونه‌های امنیتی اسکن کنید تا قبل از آنکه دیر شود بدافزار را شناسایی و به طور کامل حذف کنید. افزونه‌های امنیتی برای جلوگیری از حملات، حذف بدافزارها و ارائه گزارش‌های امنیتی طراحی شده‌اند.

با فعالسازی SSL، آدرس URL خود را امن کنید

با فعالسازی SSL اطلاعات کاربران در زمان خرید اینترنتی، رمزنگاری می‌شود تا امنیت اطلاعات آنها حفظ شود. SSL نشان دهنده اعتبار شما نزد کاربر و موتورهای جستجو است. آموزش فعال سازی SSL را مشاهده کنید و یک پروتکل امن انتقال داده برای محافظت از اطلاعات کاربران ایجاد کنید.

IPهای مشکوک را مسدود کنید

DDOS یکی از رایج‌ترین حملات است که از سمت مجموعه‌ای از IPها به صورت انبوه انجام می‌شود. گزارش‌های سایت‌تان به شما نشان می‌دهند که سایت تحت حملات DDOS است یا خیر. با استفاده از وردفنس، گزارشات حملات را مشاهده کرده و از دسترسی به صفحه ورود و پیشخوان وردپرس توسط افراد غیرمجاز جلوگیری کنید.

Firewall نرم افزاری و سخت افزاری را فعال کنید

هنگام خرید یک هاست، مطمئن شوید که هاستینگ فایروال نرم‌افزاری و سخت‌افزاری را بر روی سرورهای خود فعال دارد. معمولا این ویژگی در معرفی امکانات یک شرکت هاستینگ توضیح داده شده است.

تنظیمات امنیتی در هاست فعال باشد

در سی پنل چک کنید که مواردی مانند Virus Scanner و IP Block یا Mod Security فعال باشد. شرکت‌های هاستینگ با فعال کردن ماژول‌ها و نرم افزارهای مختلف برای جلوگیری از اسپم و ویروس‌ها می‌توانند تاثیر زیادی در جلوگیری از حملات هکرها داشته باشند.

از هاست اختصاصی استفاده کنید

بسیاری از کاربران به خاطر هزینه کمتر، اقدام به خرید هاست‌های اشتراکی می‌کنند. این نوع هاست، میزبان چند نوع سایت به صورت همزمان است و در صورتی که برای یکی از سایت‌ها مشکلی ایجاد شود، ممکن است سایت شما هم درگیر شده و هک شود. بهتر است یک هاست اختصاصی خریداری کنید تا علاوه بر تامین امنیت سایت‌تان، سرعت و عملکرد بهتری داشته باشد. نکات مهم خرید هاست را ببینید تا بهترین هاست را برای سایت‌تان انتخاب کنید.

پشتیبانی هاست را نادیده نگیرید

شاید بپرسید که پشتیبانی یک هاست چگونه در تامین امنیت موثر است؟ پشتیبانی تاثیر مستقیمی ندارد؛ باید مطمئن شوید اگر به هر دلیلی مشکلی برای سایت شما ایجاد شود، پشتیبانی هاست پاسخ‌گو است یا خیر؟ آیا اقدامات خاصی برای برگرداندن سایت انجام می‌دهد؟

فایل WP-Content را تغییر داده و مخفی کنید

امنیت فایل‌های موجود در wp-content اهمیت بالایی دارد؛ نام و محل این فایل را با استفاده از افزونه‌های امنیتی مانند (wp hide & security enhancer) تغییر دهید تا هکرها به راحتی به این فایل دسترسی پیدا نکنند.

از اجرای فایل php جلوگیری کنید

در دایرکتوری‌هایی که نیازی به اجرای کدهای php نیست اجرای کد را غیر فعال کنید به عنوان مثال برای /wp-content/uploads کد deny from all را در فایل htaccess اضافه کنید.

Directory Browsing را غیر فعال کنید

اگر بعد از آدرس سایتتان /wp-content/uploads وارد کنید و پوشه‌های سایت نمایش داده شوند یک زنگ خطر برای امنیت سایت است. با فعال بودن دسترسی به این پوشه، هکرها می‌توانند اطلاعات بسیاری را در مورد قالب، افزونه‌ها و کدهای وب‌سایت شما پیدا کرده و حفره‌های سایت‌تان را کشف کنند. با آموزش غیرفعال کردن Directory Browsing راه نفوذ هکرها به سایت را ببندید.

ورود دو مرحله‌ای (حراز هویت دو عاملی) را فعال کنید

استفاده از ورود دو مرحله‌ای با شماره تلفن، به افزایش امنیت صفحه ورود کمک می‌کند. در سایت‌های وردپرس می‌توانید با افزونه‌های مدیریت ورود/ثبت‌نام کاربران مثل آیتم سکیوریتی، ورود دو مرحله‌ای را فعال کنید.

آدرس پنل مدیریت وردپرس را تغییر دهید

تمامی هکرها و بدافزارهای مخرب به آدرس پیش‌فرض صفحه ورود به پیشخوان که همان wp-admin است دسترسی دارند. با تغییر آدرس ورود به پیشخوان از حملات بروت فورس جلوگیری کرده و مانع از دسترسی هکرها به اطلاعات سایت خود شوید.

برای جلوگیری از هک شدن، ورژن وردپرس را مخفی کنید

هکرها هر چه اطلاعات کمتری از سایت شما بدانند کارشان سخت‌تر است. ارائه اطلاعات در مورد نسخه وردپرس؛ به خصوص اگر از نسخه قدیمی استفاده کنید، به هکرها کمک می‌کند تا آسیب پذیری سایت شما را سریعتر شناسایی کنند. با پلاگین Hide My WP انجام این کار آسان است.

مانیتورینگ فعالیت کاربران را فراموش نکنید

هر گونه فعالیت غیرعادی و تغییراتی که ممکن است وب سایت را به خطر بیندازند، به خصوص دسترسی به صفحه مدیریت را بررسی و شناسایی کنید. این فعالیت‌ها با افزونه‌های امنیتی قابل بررسی هستند. قبل از آن سطح دسترسی کاربران را بررسی کنید.

امکان نمایش خطا را غیرفعال کنید.

کافیست به فایل WP_Config بروید و debug را false کنید تا خطا و پیام‌های اخطار سایت برای کاربران نمایش داده نشوند. آموزش این کار را در غیرفعالسازی نمایش خطا در وردپرس ببینید تا مانع از پیدا کردن فرصت نفوذ مهاجمان به سایت شوید.

ویرایش فایل را غیر فعال کنید

افراد مشکوک و غیرمجاز می‌توانند از ویرایشگر فایل وردپرس استفاده کرده و به فایل‌های شما دسترسی پیدا کنند. محدود کردن ویرایش فایل‌ها با wp-config.php کمک می‌کند تا گام بزرگی برای جلوگیری از هک سایت‌تان بردارید.

برای دسترسی به پوشه‌های هاست، با htaccess محدودیت بگذارید

با وبرایش فایل htaccess می‌توانید برای اجرای کد PHP در پوشه‌های خاص، مجوز تعریف کرده و از فایل wp-config.php محافظت کنید.

پیشوند پیش فرض پایگاه داده را تغییر دهید

پیشوند پیش‌فرض جداول پایگاه داده wp_ است؛ با تغییر این کاراکترهای پیش‌فرض از حملات SQL injection جلوگیری کنید. در آموزش تغییر پیشوند جداول وردپرس نحوه انجام این کار را ببینید.

فایل XML-RPC را در وردپرس غیرفعال کنید

مهاجمان می‌توانند در حملات Brute Force و DDoS از ضعف XML-RPC استفاده کرده و به سایت شما نفوذ کنند. برای جلوگیری از هک سایت با این روش، آموزش مقابله با حملات XML-RPC را ببینید.

از سرقت پهنای باند هاست یا Hotlinking جلوگیری کنید.

بعضی از وب‌سایت‌ها لینک محتواهایی مانند تصاویر شما را در سایت خود قرار می‌دهند؛ این مساله منابع سرور شما را اشغال کرده و سرعت وب‌سایت شما را کند می‌کند. با ویرایش فایل htaccess می‌توانید دسترسی سایت‌ها به محتوای خود را ببندید.

مجوزهای فایل را مدیریت کنید

شما می‌توانید از طریق هاست مشخص کنید کدام کاربران مجوز تغییر، ویرایش و اجرای فایل‌ها را داشته باشند.

نکات مهم

- از سایت‌هایی مثل Patchstack و ویروس توتال برای شناسایی آسیب‌پذیری‌های موجود در قالب‌ها و افزونه‌های خود استفاده کنید.
- بکاپ‌هایی که تهیه می‌کنید را در سیستم کامپیوتر، فلش، گوگل داریو و غیره هم ذخیره کنید تا همیشه یک نسخه سالم از وب سایت را داشته باشید.

اگر به دنبال راهکارهای تخصصی‌تر برای افزایش امنیت سایت هستید، دوره کانفینیتی راست چین صفر تا صد شناسایی و رفع سریع آسیب‌پذیری‌ها را آموزش داده تا از اطلاعات ارزشمند سایت خود محافظت کنید.

راست‌چین
RTL-THEME

امیدوارم مهم‌ترین اقدامات حیاتی «تامین امنیت سایت» را گام به گام انجام دهید

تا سایت شما در لیست سایت‌های هک شده قرار نگیرد.