ویروس ها، بد افزارها، هک و خرابکاری های وردپرسی و راههای مقابله

نوشته:

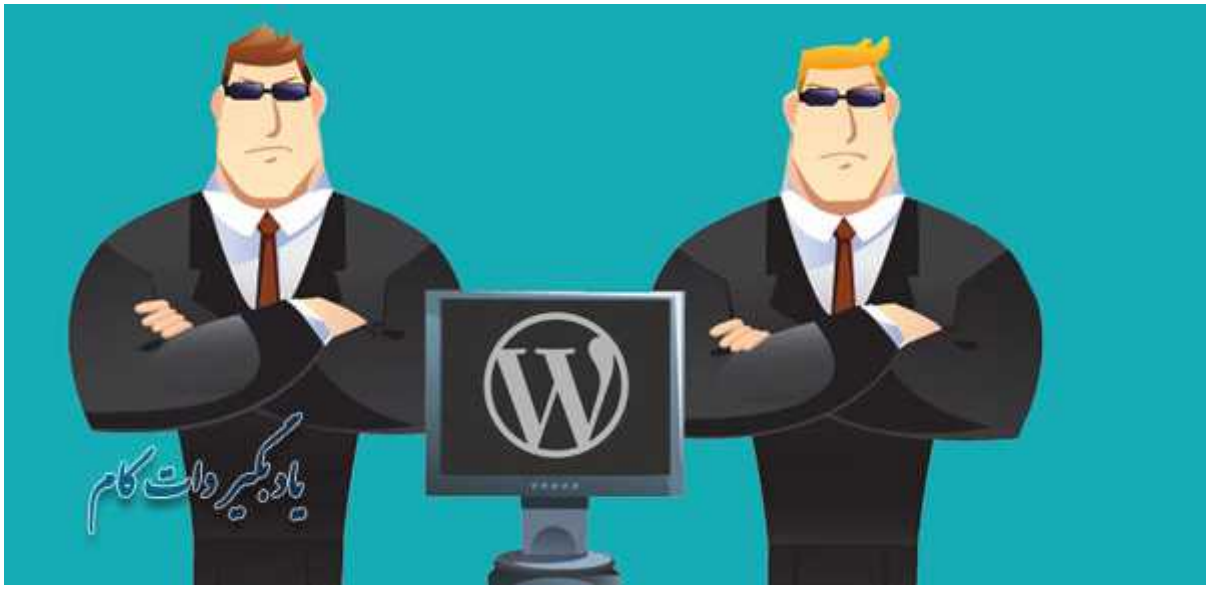
علی یزدی مقدم

برای:

یاد بگیر دات کام

ویروس ها، بد افزارها، هک و خرابکاری های وردپرسی و راههای مقابله

وردپرس یکی از پرکاربردترین سیستم های مدیریت محتوا در دنیاست که برای طراحی وب سایت از آن استفاده می کنند که کشور ما هم از این قاعده مستثنا نیست. یکی از اهداف مشترک هکر ها، اسپمرها و دیگر تبهکاران اینترنتی وب سایت های وردپرسی هستند. و به همین دلیل اگر شما هم یک وب سایت وردپرسی دارید بهتر است از امن بودن آن اطمینان حاصل کنید.



هدف بیشتر هکر ها این است که وب سایت شما را آلوده کنند. بیشتر بدافزار ها و تهدید ها شامل:

- فارما هک: به شکل فایل یا با ریختن کدهایی در بانک اطلاعاتی انجام می گیرد تا از طریق وب سایت شما به اسپمینگ بپردازند.

- بک دورز: به هکر ها اجازه می دهند تا به وب سایت شما دسترسی داشته باشند و این کار را به کمک اف تی پی یا ادمین وردپرس انجام می دهند.
- نفوذ به کمک دانلود: در این روش هکر های از وب سایت شما سوء استفاده می کنند تا هنگام دانلود یک فایل برنامه ای کوچک را در کامپیوتر کاربر بارگذاری کند.
- دستکاری در فایل ها و بانک های اطلاعاتی: اضافه کردن کد های مخرب به فایل ها و بانک های اطلاعاتی وب سایت که به هکر ها اجازه می دهد با استفاده از این کد ها خرابکاری ها و کارهای مختلفی انجام دهند.
- فرستادن یا ریدایرکت کردن به ناکجا: کاری می کنند که صفحه مورد نظر کاربر به صفحه دیگری منتهی شود و در نهایت برنامه ای مخرب در کامپیوتر او اجرا گردد یا حتی ممکن است کاربران شما را به وب سایت های مستجحن هدایت کنند و از این راه پولی به جیب بزنند.
- فیشینگ یا دزدی اطلاعات محرمانه: این روش برای بدست آوردن اطلاعات محرمانه افراد مانند نام کاربری، رمز عبور، آدرس ایمیل، حساب بانکی و اطلاعات حساسی از این دست مورد استفاده هکر ها قرار می گیرد.

در حالیکه بسیاری فکر می کنند هک وب سایت به این معنی است که صفحه اصلی آن با پیامی از طرف هکر جایگزین می شود مانند: این وب سایت توسط گروه .... هک شده است. اما امروزه آلوده کردن وب سایت ها دیگر به روش های قدیمی انجام نمی گیرد و حتی صاحب وب سایت هم تا مدت ها نخواهد فهمید که چه اتفاقی افتاده است. حقیقت این است که دیگر صفحه اصلی وب سایت ها تغییری نمی کند و چنین کارهایی به ندرت انجام می شود، چون به این ترتیب صاحب وب سایت خیلی زود متوجه خرابکاری شده و در صدد رفع آن بر می آید.

هکر هایی که وب سایت شما را با بد افزارها آلوده می کنند به شکلی متفاوت عمل می کنند. هر چه مدت بیشتری طول بکشد تا از آلوده شدن وب سایت خود بی خبر باشید آنها فرصت بیشتری دارند تا از وب سایت شما برای ارسال ایمیل و آلوده کردن کاربرانتان استفاده کنند. حتی یک وب سایت امن وردپرسی می تواند بدون اینکه صاحبش متوجه شود هک شود. بنابراین بسیار مهم است که به صورت دوره ای وب سایت وردپرسی خود را اسکن کنید تا بتوانید هر بدافزار یا ویروس پنهان را تشخیص دهید.

در این مقاله می خواهم به شما سرویس ها و افزونه هایی را معرفی کنم که به کمک آنها مشکلات امنیتی وب سایت وردپرسی خود را شناسایی کنید.

اسکن بد افزار ها به کمک sucuri

sucuriبه عنوان یک راه حل موثر امنیتی برای شناسایی بدافزار ها اعتبار بالایی دارد. در وب سایت http://sitecheck.sucuri.netمی توانید وب سایت خود را مورد آزمایش قرار دهید تا اطمینان حاصل کنید در برابر تهدید های یک وب سایت ساخته شده با وردپرس در چه وضعیتی قرار دارد.

اسکنر sucuriوب سایت شما را برای بدافزارها، تغییرات در صفحات وب سایت و تزریق اسپم بررسی می کند. همچنین چک می کند آیا سرور وب سایت شما در لیست سیاه قرار دارد یا خیر. (ممکن است در سرور شما نفوذی رخ داده شده باشد یا اینکه وب سایت دیگری که در این وب سایت قرار دارد در حال اسپمینگ باشد.) بزرگترین محدودیت این اسکن این است که مجبورید وب سایت را خودتان به صورت دوره ای انجام دهید و هیچ اسکن دوره ای خودکاری وجود ندارد.

sucuriهمچنین یک افزونه با نام Sucuri Securityبرای وردپرس ارائه کرده است. گذشته از اینکه وب سایت شما را اسکن می کند برای وب سایت شما فایروالی می سازد تا امنیت بیشتری داشته باشد. به این ترتیب پیدا کردن حفره های مشترک وردپرس برای هکر ها مشکل تر می شود و مشخص می شود چه کسی وارد وب سایت شما شده است.

این افزونه همچنین ویژگی های برای بازیابی بانک اطلاعاتی دارد که بعد از یک حمله، بروزرسانی وردپرس، تغییر رمز عبور و موارد مشابه بسیار مفید خواهد بود.

کد گارد

کد گارد یک سرویس پشتیبان گیری است که برای شما به صورت خودکار نسخه های پشتیبان تهیه می کند و می تواند نسخه پشتیبان وب سایت شما را با یک کلیک بازگرداند. این سرویس همچنین برای تغییراتی که هر روز رخ می دهد وب سایت شما را مانیتورینگ می کند و در صورتی که بدافزاری تشخیص دهد، هشدار هایی صادر می کند.

این ارزانترین و به صرفه ترین سرویس پولی برای پشتیبان گیری است است که قابلیت مانیتورینگ دارد.

Theme Authenticity checker

Theme Authenticity checkerهر قالبی را که در ورد پرس شما نصب شده باشد بررسی می کند تا هر نوع خرابکاری را کشف کند. امروزه اکثر کسانی که در ایران ادعای طراحی وب سایت می کنند در حقیقت فقط وردپرس نصب می کنند و از قالب های آماده ای استفاده می کنند که آلوده به کدهای مخرب یا لینک هایی در فوتر سایت هستند و به علت دانش ضعیفی که در این زمینه دارند، حتی گاه خود هم خبر ندارند مشتری خود را مورد سوءاستفاده طراح قالب قرار داده اند و از آن بدتر صاحب وب سایت است که برای طراحی هزینه ای هم پرداخت کرده است و پس از مدتی طولانی متوجه می شود وب سایتش در لیست سیاه سرور های مختلف قرار گرفته است چون او بدون اینکه خود متوجه بشود در حال اسپمینگ برای دیگران است طراح اصلی قالب از این کار سود زیادی به جیب می زند و قربانی هم کسی است که از این قالب های غیر استاندارد استفاده می کند .
Theme Authenticity checkerمی تواند به شما کمک کند برخی از آنها را شناسایی کنید و البته راه امن استفاده از قالب رایگان این است که قالب مناسب خود را از وب سایت اصلی ورد پرس یعنی http://wordpress.orgدانلود کنید چون طراحانی می توانند قالب خود را در وب سایت رسمی ورد پرس قرار دهند که همه شرایط را رعایت کرده باشند و قالب استانداردی طراحی کرده باشند همچنین می توانید در این وب سایت نظر افراد حرفه ای را بخوانید و تصمیم بگیرید آیا این قالب وردپرس به درد شما می خورد یا خیر Theme Authenticity checker .همچنین می تواند کد های مخرب Base64را شناسایی کند.

WP Antivirus Site Protection

WP Antivirus Site Protectionدر حقیقت یک وب افزونه امنیتی وردپرس است که توسط SiteGuardingارائه شده است و می تواند وب سایت شما را برای وجود بکدور ها، روت کیت ها، تراجان ها، کرم ها، ابزار های مخرب، بدافزارها و اسپای ویر ها جستجو کند .همچنین فایل های قالب شما را بررسی می کند، قابلیت دیگر ارزشمند آن این است که می تواند افزونه های شما را هم بررسی کند تا از امن بودن و غیر مخرب بودن آنها اطمینان حاصل شود و در نهایت قابلیت دیگری هم به آن اضافه شده

است که باز هم این افزونه امنیتی ورد پرس را کاملتر کند و آن قابلیت اسکن فایل هایی است که در وردپرس خود آپلود می کنید.

اگر از این نرم افزار به صورت رایگان استفاده کنید وب سایت شما را هر هفته اسکن می کند. و در صورتی که نسخه پولی آنرا خریداری کنید اسکن روزانه انجام می دهد و نسخه کاملتر آن هم شامل ابزار برای از بین بردن ویروس ها و بد افزار هاست.

AntiVirus

AntiVirusیک افزونه رایگان وردپرس است که به صورت روزانه وب سایت شما را اسکن می کند. این افزونه هشداری برای وجود ویروس در نوار ابزار مدیریت وردپرس اضافه می کند. همچنین در صورتی که هر گونه بدافزاری را تشخیص دهد با ایمیل به شما اطلاع خواهد داد.

محدودیت اصلی این افزونه این است که فقط قالبی را که در حال اجراست اسکن می کند و دیگر قالب های نصب شده را اسکن نمی کند. و اگر قالب های غیر فعال خود را پاک کنید مشکلی برای شما نخواهد بود.

AntiVirusیک اسکنر رایگان مفید است که می تواند وب سایت وردپرسی شما را برای وجود کد های مخرب اسکن کند.

Anti-Maleware

Anti-Malewareوب سایت شما را برای وجود بد افزار ها اسکن می کند و به صورت خودکار هر تهدیدی را که تشخیص دهد از بین می برد. این افزونه می تواند ورود شما و البته هکرها را به وب سایت ورد پرسی خودتان را کمی سخت تر کند.

Quttera Web Malware Scanner

Quttera Web Malware Scannerمی تواند وب سایت شما را برای تهدید هایی از قبیل بکدور ها، کدهای مخرب، کد های مخفی و.. اسکن کند. در نهایت گزارشی برای شما نمایش داده می شود و لیستی از فایل های مشکوک و توصیه هایی برای پاک سازی آنها ارائه می دهد.

Wemahu

Wemahuیک افزونه وردپرسی است که می تواند کد های مشکوک را در وب سایت شما شناسایی کند. این افزونه می تواند وب سایت شما را بر اساس یک برنامه از پیش تعیین شده اسکن کند و از طریق ایمیل گزارشی در اختیار شما قرار دهد.

wordefense

wordefenseیک از پرکاربرد ترین افزونه های امنیتی وردپرس است که در بین کاربران محبوبیت بالایی دارد. این افزونه می تواند فایل های هسته وردپرس، فایل های قالب و افزونه های مختلف را در برابر تهدید های شناخته شده اسکن کند.

همچنین گزارشی از تغییرات ایجاد شده در وب سایت شما ارائه می دهد، گزینه های مختلفی برای بستن یا سخت تر کردن مسیر نفوذ در اختیار شما قرار می دهد و امنیت بیشتری فراهم می کند.

wordefense یک راه حل امنیتی عالی برای وردپرس است که همه چیز را به صورت یکجا در اختیار شما قرار می دهد و می تواند وب سایت شما را برای تهدید های مختلف اسکن کند.

WP Changes Tracker

WP Changes Trackerمانند نرم افزار های امنیتی که در مورد آن صحبت کردیم برای پیدا کردن بدافزار ها مورد استفاده قرار نمی گیرد بلکه ابزار مناسبی است برای اینکه بتوانید به کمک آن تغییراتی که در وردپرس شما ایجاد شده است را بیابید. این بررسی شامل بانک اطلاعاتی، فایل های مربوط به افزونه ها و فایل های قالب می شود.

اگر هک شده باشید با استفاده از این اطلاعات ممکن است بتوانید مشاهده کنید که دقیقا چه تغییراتی ایجاد شده است و چگونه وب سایت وردپرسی شما به خطر افتاده است. این افزونه همچنین برای ردگیری تغییراتی که ممکن است توسط همکاران شما خواسته یا ناخواسته در وردپرس ایجاد شده است مفید باشد.

WP Changes Trackerبه شما نشان می دهد که چه تغییراتی در وب سایت شما ایجاد شده است.

WP Secutrity Audit Log

و یک افزونه جایگزین خوب برای افزونه قبلی WP Secutrity Audit Logاست که به کمک آن می توانید تغییرات ایجاد شده را به خوبی ردگیری کنید. این افزونه یک گزارش یا لاگ از هر تغییر کوچکی در وردپرس تهیه می کند. هشدار های امنیتی می تواند برای شما ارسال شود که از آن جمله می توان به اقدام به ورود با نام یا رمز عبور اشتباه، اقدام جهت ایجاد تغییرات در فایل ها و نصب افزونه ها اشاره کرد.

توصیه می کنم وب وردپرس خود را به صورت منظم برای کد های مخرب و تغییرات اسکن کنید. و باید یکی از وسواس های شما این باشد که هر حرکت مشکوکی را در وب سایت خود بررسی کنید تا در صورت نفوذ هکر ها و خرابکارهای اینترنتی در همان پله های اولیه مانع از نفوذ آنها شوید.

علی یزدی مقدم