5 نکته جهت بهبود امنیت سایت

۵ راه مطمئن برای تامین امنیت وبسایت

نویسنده: مهران منصوری فر

۵ نکته جهت بهبود امنیت سایت

در این مقاله به آموزش ۵ نکته جهت بهبود امنیت سایت خواهیم پرداخت، با رعایت این نکات می توانید امنیت وب سایت خود را بالا ببرید.
مسئله ی امنیت وبسایت هیچ گاه به اندازه‌ی امروز بحرانی نبوده است. هکرها، حملات دیداس، هر دو نگرانی‌هایی است که نسبت به وبسایت های کسب و کار جدید وجود دارد.
هیچ چیز نمی‌تواند به اندازه‌ی اخطارهای امنیتی یا پیام گوگل – «این وبسایت قابل اعتماد نیست» – در نتایج جستجوی وبسایت شما، به اعتماد مخاطبانتان به شما لطمه وارد کند.
زمانی که یک سایت توسط هکر ها دزدیده می شود، درصورتی که یک کاربر وارد وب سایت می شود پیغامی از گوگل در سایت شما مشاهده می کند، با این عنوان که « این وب سایت قابل اعتماد نیست.» اگر وب سایت شما هک شود وب مستر تولز به شما سریعا گزارش می دهد و به راحتی می توانید مشاهده کنید چه زمانی وب سایت شما قابل دسترس هکر ها قرار گرفته است.
بدتر از این، حتما تا به حال تجربه این را داشته اید که هنگام مطالعه مطالب یک وب سایت به صفحات دیگری شامل صفحات اسپم و ارور ها و یا وب سایت های نا مربوط هدایت شوید و یا حتی سعی کنید دکمه‌ی بازگشت را بزنید اما این دکمه عمل نکند.
به وجود آمدن اینگونه مسائل باعث می شود کاربرانتان برای مراجعه مجدد به وب سایت شما با شک و تردید روبرو شوند. بازدیدکنندگان وبسایتتان را مردد نکنید.
بنابرین چه راه حلی برای مقابله با فعالیت هکر ها بر روی وب سایتمان وجود دارد؟ در ادامه به توضیح چند مورد خواهیم پرداخت، اولین راه حلی که در پایین مطرح خواهد شد مهم‌ترین راه حل است.

قدم اول: میزبان هاست مناسبی که بر روی مسائل امنیتی تمرکز کرده است را انتخاب کنید

مهم‌ترین تصمیمی که در رابطه با تأمین امنیت وبسایتتان می‌گیرید آن است که وبسایت خود را بر روی کدام میزبان هاست ایجاد می‌کنید. زمانی که گزینه‌های میزبانی گوناگون یا حتی قبل تر میزبان فعلی‌تان را از نظر سرویس های امنیتی بررسی می‌کنید باید سوالی ساده از خودتان بپرسید: میزبان هاست من چه امکاناتی در زمینه‌ی افزایش امنیت سایت برای من فراهم می‌کند؟

شما به میزبانی نیاز دارید که بتواند فضایی یک پارچه ایجاد کند تا به راحتی امکان محافظت از وب سایت شما را در مقابل هکر ها و یا حملات دیداس داشته باشد. یک میزبان هاست قدرتمند ضرورتاً باید تمام راه حل‌هایی را که در ادامه گفته می‌شود فراهم کند و بتواند آنهارا به بهترین نحو اعمال کند.

شما صاحب یک وب سایت هستید و نیازی نیست مسئولیت افزایش امنیت سایت را بر عهده بگیرید، تنها کاری که باید انجام دهید این است که تمام تمرکز خود را بر روی مطالبی که در وب سایت خود منتشر می کنید بگذارید و بتوانید با کاربران سایت ارتباط برقرار کنید، بی شک آنها می توانند در آینده مشتریان شما باشند در ادامه درباره امکاناتی که از میزبان هاست خود میخواهیم صحبت خواهیم کرد.

قدم دوم: بروز رسانی خودکار سیستم وردپرس

خوبی نرم افزارهای متن باز (open source) مانند وردپرس آن است که هزاران نفر به صورت پیوسته در حال ارتقا آن هستند. هم چنین هزاران نفر

در حال پیگیری مشکلات امنیتی و رفع آنها در این سیستم هستند. اما زمانی که ورژن‌های قبلی با مشکل روبرو می‌شوند بروزرسانی وردپرس به خودتان بستگی خواهد داشت.
این یعنی زمانی که بروزرسانی وردپرس در دسترس است فقط باید از سایتتان بکاپ (Backup) تهیه کنید تا اطلاعاتتان از دست نرود، سپس وردپرس خود را بروز کنید. مجددا این روال را در چند هفته آینده، درست زمانی که بروز رسانی جدیدی در دسترس قرار خواهد گرفت دوباره طی کنید. یک مقدار آپدیت و بکاپ گیری از سیستم وردپرس می تواند سخت و استرس زا باشد، اما انجام آن بی شک امری ضروری است. بهترین راه حل آن است که سایتتان را بروی سیستمی ایجاد کنید که بخش بروز رسانی خودکار دارد. برای این کار کافی است قسمت آپدیت خودکار را فعال کنید.
بعد از آن، میزبان هاست شما مسئولیت بروزرسانی را بر عهده می‌گیرد و فشار این کار را از روی شانه‌های شما بر می‌دارد. این سیستمی است که ارزش هزینه کردن دارد.

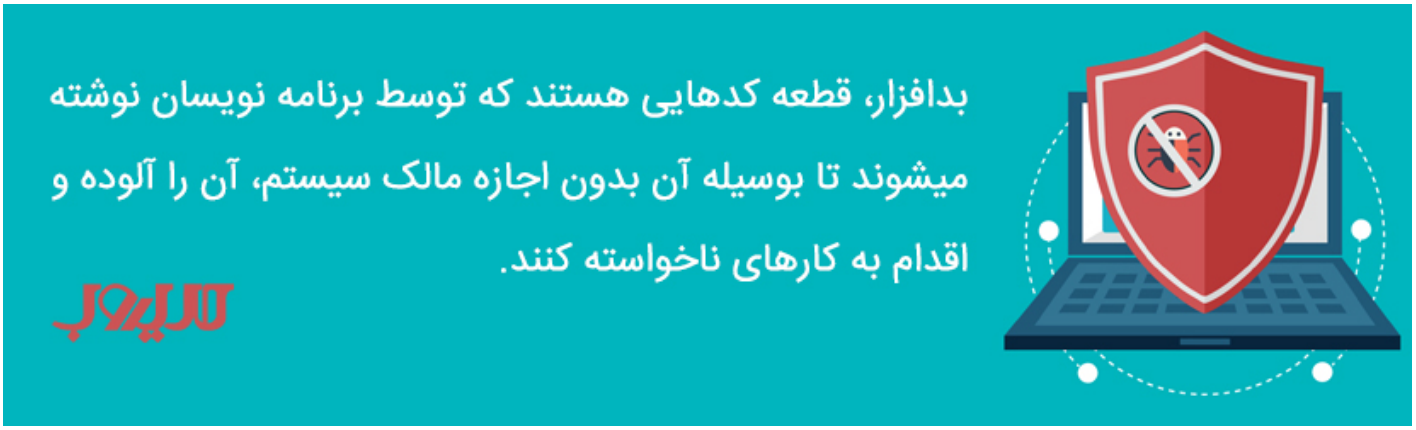
قدم سوم: بررسی افزونه ها قبل از نصب و استفاده

سؤال بعد آن است که آیا افزونه ها و ابزار هایی که بر روی سیستم وردپرس خود نصب می‌کنید، مشکلات امنیتی دارند؟
افزونه ها و کدهای اتصال تقلبی دو مشکل اساسی به وجود می‌آورند، اول دسترسی هکرها را به سایت شما آسان می‌کند. دوم آنکه به سرعت و اجرای سایت شما آسیب می رساند. به همین دلیل، استفاده از افزونه ها و ابزار

هایی که قابل اعتمادند، ایده‌ی هوشمندانه‌ای است. بهترین راه نصب افزونه های وردپرس مخزن وردپرس می باشد.
امنیت افزونه ها هم مسئله‌ی مهمی است. در ابتدا باید به دقت افزونه هایی را که می‌خواهید به فضای سایت شما وارد شوند را انتخاب کنید، و بعد مدام آن‌ها را رصد کنید تا مطمئن شوید همیشه بروز هستند.
قبل از آنکه راه حل سوم به پایان برسد لازم است نکته‌ای را تذکر دهم، اگر از افزونه هایی استفاده می‌کنید که به سرعت بروز رسانی نمی‌شوند، آن‌ها را عوض کنید. این بدان معناست که بروزرسانی افزونه ها مسئله‌ی مهمی برای میزبان هاست شما نیست. استفاده از افزونه های قدیمی، بهترین دستورالعمل برای فجایع امنیتی است.
در ادامه دو مبحث دیگر در حوزه‌ی امنیت را که شما و میزبان هاست باید به آن اهمیت دهید را مطرح می‌کنیم.

قدم چهارم: از سایتتان در برابر حملات دیداس محافظت کنید
آیا تا به حال راجع به حملات دیداس چیزی شنیده‌اید؟
شما مطمئناً اصطلاح آن را شنیده‌اید حتی اگر معنای دقیق آن را ندانید.
حمله‌ی منع سرویس – دیداس – به معنی سرازیر کردن تقاضاهای زیاد به یک سرور و استفاده بیش از حد از منابع (پردازنده، پایگاه داده؛ پهنای باند، حافظه و ...) به طوری که به دلیل حجم بالای پردازش سرویس دهی آن به کاربرانش دچار اختلال شده یا از دسترس خارج شود.
باید اطمینان حاصل کنید که سایت میزبان شما، مجهز به تکنولوژی‌ای باشد

تـا بتوانـد حمـلات را بـه سـرعت شناسـایی کنـد، در عیـن حـال مهاجمـان تکـراری بـر همیـن اسـاس شناسـایی و مهـار می‌شـوند.
بایـد هوشـیار باشـید و از میزبانتـان بپرسـید، چگونـه حمـلات دیـداس را کنتـرل می‌کننـد، همچنیـن بایـد امیـدوار باشـید، بـا جزئیـات کامـل بـه شـما توضیـح دهنـد.
حمـلات دیـداس را بایـد جـدی بگیریـد و راه حـل جـدی و قابـل اجرایـی را بـرای آن پیـدا کنیـد.



قدم پنجم: بد افزار ها را رصد کنید

در نهایت، باید بدافزارها مدام رصد شوند. جای بحث در این مورد نیست.
اگـر چـه ممکـن اسـت همـواره همـه‌ی پوشـه‌ها و فایل‌هـای وبسـایتتان را بازرسـی کنیـد، امـا چگونـه می‌توانیـد متوجـه هکرهایـی کـه وارد شـده و چیـزی را بـر جـای گذاشـته‌اند شـوید؟
همـه‌ی هک‌هـا و بـد کدهـا بـه سـرعت خودشـان را بـه صـورت عمومـی و واضـح نمایـان نمی‌کننـد.
اگـر در سـایتتان یـک بمـب سـاعتی کار گذاشـته شـده اسـت – واقعـاً اگـر چیـزی در وبسـایتتان وجـود دارد کـه خودتـان آن را قـرار نداده‌ایـد – بایـد راجـع بـه آن آگاه باشـید تـا بتوانیـد واکنشـی بـه آن نشـان دهیـد.
سـایت‌ها و شـرکت‌های مختلفـی وجـود دارنـد کـه بررسـی و تحلیـل وب سـایت را بـر عهـده می‌گیرنـد. بنابرایـن لازم نیسـت دائمـاً نگـران هکـر هـا یـا حمـلات

دیـداس باشـید. بـه عـلاوه بسـیاری از آن‌هـا می‌تواننـد تهدیدهـای پیشـرفته تـر مثـل بدافزارهـای شـرطی و انـواع حمـلات سـایبری را هـم اسـکن کننـد.
امنیـت مناسـب فضـای وب نبایـد بـه عنـوان یـک مزیـت اضافـی در نظـر گرفتـه شـود کـه بـرای آن پـول اضافـی پرداخـت کـرد. امنیـت قـوی بخشـی از امکاناتـی اسـت کـه هـر شـرکت ارائـه کننـده فضـای میزبانـی بایـد آن را ارائـه دهـد.

بعد از همه‌ی این مراحل چه باید کرد؟

خـوب اسـت کـه یکـی از کارهایـی را کـه در ادامـه گفتـه می‌شـود را انتخـاب کنیـد و بـه آن عمـل کنیـد.
یـک لیسـت یـا تقویـم چرخـان درسـت کنیـد تـا هـر هفتـه بـه شـما یـادآوری کنـد کـه بروزرسـانی وردپـرس و افزونـه هـا را بررسـی کنیـد.
در ایـن صـورت اگـر حتـی بـه وب سـایت وردپرسـی خـود وارد نشـوید یـا پیـام هشـدار را از دسـت بدهیـد، حداقـل هـر دو هفتـه وب مسـتر تولـز را بررسـی می‌کنید.
حـال اگـر میزبـان وب شـما مجهـز بـه بروزرسـانی خـودکار وردپـرس و حتـی زمینـه و افزونـه هـای اصلـی اسـت، دیگـر نیـازی بـه ایـن کار نیسـت. فقـط بایـد مطمئـن شـوید کـه گزینـه‌ی بروزرسـانی خـودکار فعـال اسـت. در ایـن صـورت می‌توانیـد از قـدم دوم اسـتفاده کنیـد.
اگـر در ایـن رابطـه اطـلاع دقیقـی از عملکـرد پذیرنده‌تـان نداریـد، از آن بپرسـید کـه چگونـه از سـایتتان در برابـر حمـلات دیـداس و هکـر هـا محافظـت می‌کنـد. بایـد ایـن کار را از طریـق میزبانـی هاسـت خـود انجـام دهیـد.