کتابچه راهنمای

امنیت سایت وردپرس

❖ آسیب پذیری های وردپرس

❖ ترفندهای امنیت سایت وردپرس

تیم تولید محتوای یوایکس نت

WWW.UXNET.IR

مقدمه ۱
آیا وردپرس امن است؟..... ۱
آسیب‌پذیری‌های وردپرس..... ۲
حمله backdoor ۳
حمله Pharma Hacks ۴
حمله جستجوی فراگیر..... ۴
تزریق اسکریپت از طریق وب‌گاه (XSS)..... ۵
حمله DOS (Denial Of Service) ۵
راهنمای امنیت وردپرس ۲۰۲۰ ..... ۵
۱. از هاست ایمن استفاده کنید..... ۵
۲. از آخرین نسخه PHP استفاده کنید ۶
پیدا کردن نسخه PHP سایت ۸
۳. از نام کاربری و کلمه عبور هوشمندانه استفاده کنید. ۹
۴. همیشه از آخرین نسخه وردپرس، افزونه‌ها و پوسته‌ها استفاده کنید..... ۱۰
۵. صفحه ادمین وردپرس را ایمن کنید..... ۱۲
نحوه تغییر URL ورود به وردپرس ۱۲
محدود کردن تعداد دفعات تلاش برای ورود ۱۲
۶. از تأیید هویت دومرحله‌ای استفاده کنید ۱۳
۷. از HTTPS استفاده کنید ۱۴
استفاده از https چه فایده‌ای دارد؟..... ۱۴
امنیت ۱۴
سئو ۱۴
اعتماد و اعتبار ۱۴
۸. نسخه وردپرس خود را مخفی کنید..... ۱۴
۹. آخرین هدرهای امنیتی HTTP را اضافه کنید..... ۱۵
۱۰. از افزونه‌های امنیتی وردپرس استفاده کنید ۱۶
۱۱. امنیت پایگاه داده را بهبود ببخشید ۱۷
۱۲. اجازه تغییر در فایل و سرور را بررسی کنید. ۱۷

مجوزهای پرونده ۱۷
مجوزهای دایرکتوری ۱۷
مجوز دسترسی پرونده‌ها چگونه باشد؟ ۱۸
۱۳. ویرایش پرونده در داشبورد وردپرس را غیرفعال کنید ۱۹
۱۴. از HOTLINKING جلوگیری کنید ۱۹
جلوگیری از هات لینکینگ در apache ۱۹
جمع‌بندی ۱۹

چگونه امنیت سایت وردپرس را تأمین کنیم؟

مقدمه

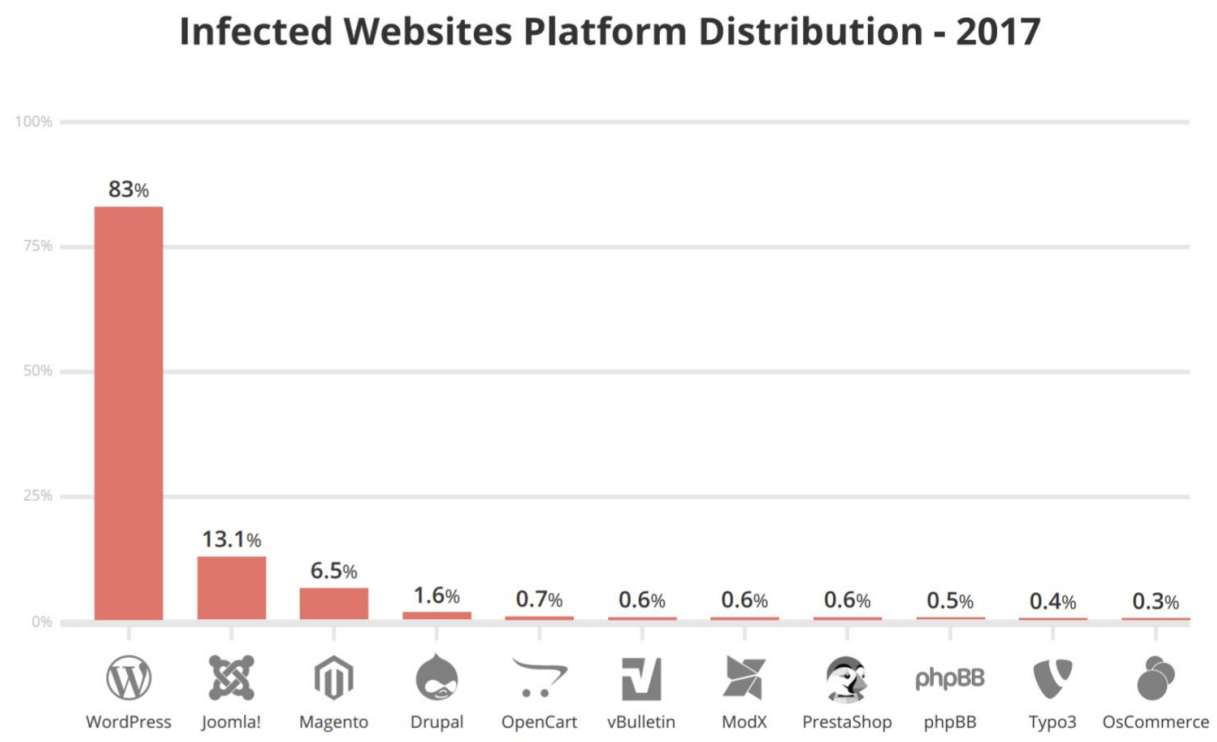
در مورد امنیت وردپرس، موارد زیادی وجود دارد که می‌توانید با رعایت آن‌ها سایتتان را در مقابل حملات هکرها و آسیب پذیری‌ها به خصوص در مورد سایت فروشگاهی و تجارت الکترونیک محافظت کنید.
امروز قصد داریم نکات، استراتژی‌ها و تکنیک‌های منحصر به فردی را برای استفاده بهتر در استفاده از سایت وردپرسی و محافظت از آن به اشتراک بگذاریم. پس تا پایان مقاله با ما همراه باشید.

آیا وردپرس امن است؟

اولین سوالی که احتمالاً در ذهن هر کس نقش می‌بندد، این است که آیا وردپرس امنیت سایت را تأمین می‌کند یا نه؟ در اکثر موارد **بله**. با این حال، وردپرس معمولاً به دلیل پیکربندی نامناسب توسط کاربر و نادیده گرفتن برخی موارد امنیتی، مستعد آسیب پذیری‌های متفاوتی خواهد بود.

> به یاد داشته باشید هنگامی که از امنیت صحبت می‌شود، منظور کاهش ریسک است و نه حذف کامل آن؛ پس هیچ عملی نیست که بتواند به طور کامل خطر نفوذ و هک سایت را به صفر برساند.

استفاده از نسخه‌های قدیمی وردپرس، افزونه‌های نامعتبر، مدیریت ضعیف سیستم، عدم آگاهی و تخصص از نکات امنیتی وردپرس، هکرها را برای آسیب رساندن به سایت‌های وردپرسی وسوسه می‌کند. حتی پیشگامان استفاده از وردپرس همیشه از بهترین شیوه‌های امنیتی استفاده نمی‌کنند؛ رویترز هک شد زیرا از نسخه قدیمی وردپرس استفاده می‌کرد.
براساس مطالعه انجام شده در سال ۲۰۱۷ توسط Sucuri که یک شرکت امنیتی چند پلتفرمه است، وردپرس همچنان پیشتاز وب سایت‌های آلوده شده توسط مهاجمان است (با ۸۳ درصد) که این رقم در سال ۲۰۱۶ حدود ۷۴ درصد بوده است.



سایت‌های وردپرس نسبت به سایر سایت‌ها بیشتر مورد حمله قرار می‌گیرند

وردپرس بیش از ۳۷٫۶٪ از کل وب سایت‌های اینترنتی را در اختیار دارد و با وجود صدها هزار قالب و افزونه منتشر شده خارج از سایت رسمی آن، جای تعجب نیست که آسیب‌پذیری‌هایی داشته باشد.
از سال ۲۰۲۰، تیم امنیتی وردپرس از حدود ۵۰ متخصص (این تعداد در سال ۲۰۱۷، ۲۵ نفر بود) تشکیل شده است که شامل توسعه دهندگان اصلی و محققان امنیتی است.

آسیب‌پذیری‌های وردپرس

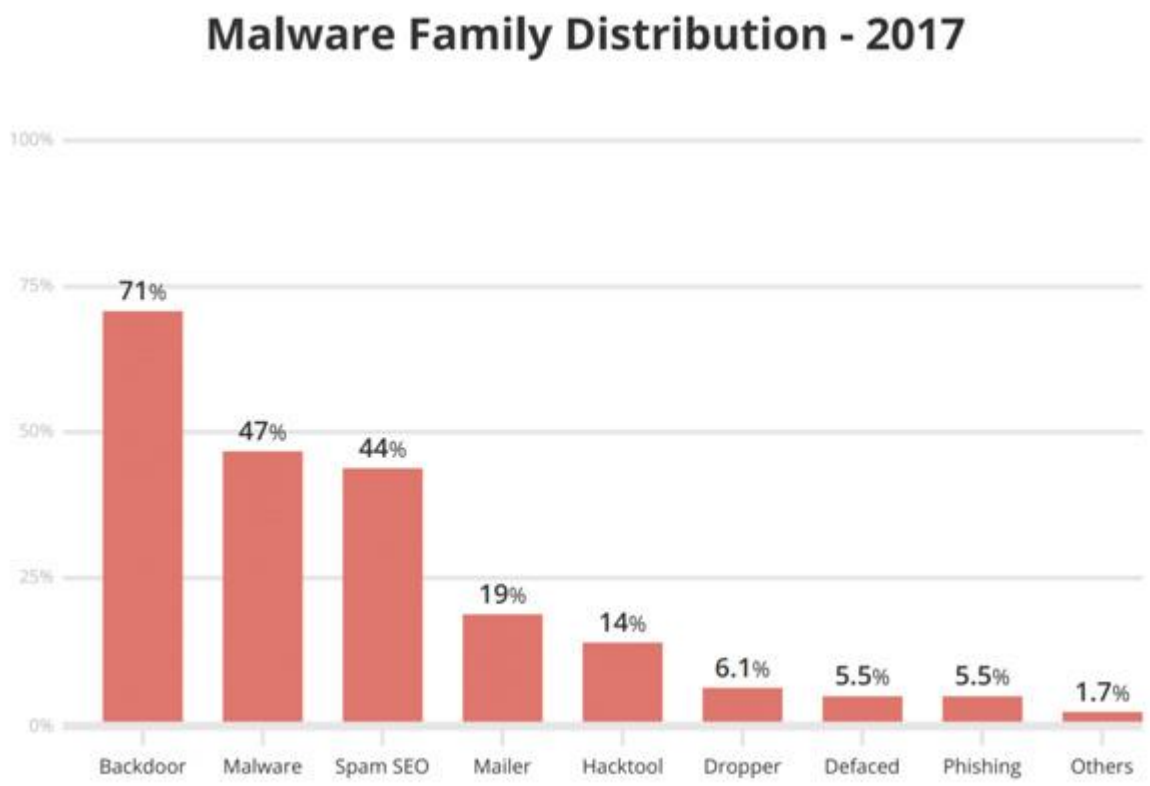
برخی از انواع مختلف آسیب‌پذیری‌های امنیتی وردپرس را در زیر مشاهده می‌کنید.

- Backdoors
- Pharma Hacks
- Brute-force Login Attempts
- Malicious Redirects
- Cross-site Scripting (XSS)
- Denial of Service

اما هر کدام دقیقاً چه هستند و چه آسیبی به سایت می‌رسانند. در ادامه به بررسی هر یک می‌پردازیم.

حمله backdoor

آسیب‌پذیری backdoor یا درِ پشتی، هکر را قادر می‌سازد تا با استفاده از راه‌های مخفی و با استفاده از روش‌های غیرعادی، به رمزگذاری‌های امنیتی برای دسترسی به سایت وردپرسی (wp-Admin، SFTP، FTP و غیره) دسترسی پیدا کند. پس از دسترسی نفوذکننده به سایت موردنظر، هکر با خرابکاری در هاست سایت، چندین سایت موجود دیگر روی آن سرور را نیز به خطر می‌اندازد.
حمله در پشتی همچنان یکی از اقداماتی است که مهاجمان پس از نفوذ انجام می‌دهند؛ به عبارتی در ٪۷۱ از سایت‌های آلوده، ردپای حمله درپشتی دیده می‌شود.



در ۷۱ درصد از حملات به سایت، ردپای حمله در پشتی دیده می‌شود

خوشبختانه پیشگیری و درمان این آسیب‌پذیری بسیار ساده است. می‌توانید سایت وردپرس خود را با ابزارهایی مانند SiteCheck اسکن کنید تا به راحتی حملات در پشتی رایج را تشخیص دهند.
احراز هویت دو مرحله‌ای، مسدود کردن IP ها، محدود کردن دسترسی مدیر و جلوگیری از اجرای غیرمجاز فایل‌های PHP، از سایت در مقابل حمله در پشتی محافظت می‌کند.

حمله Pharma Hacks

حمله فارما هک، یک حمله زیرکانه است که سئو سایت را هدف قرار می‌دهد. هکر با درج کد مخرب، باعث می‌شود موتورهای جستجو هنگام جستجوی سایت مورد نظر، تبلیغات محصولات دارویی را بازگردانند.
به تصویر زیر نگاه کنید. با جستجوی سایت مورد نظر در گوگل، نتایج پزشکی و دارویی ظاهر شده مرتبط با سایت نیستند:

فارما هک

این حمله بیش از آنکه یک بدافزار محسوب شود، به عنوان اسپم شناخته می‌شود. این حمله معمولاً صفحات پربازدید سایت را مورد حمله قرار می‌دهد و موتورهای جستجو آن را تشخیص می‌دهند. بنابراین در این حمله به دلیل محتوای نامربوط به سایت، شاهد افت رتبه سایت خواهیم بود.
برای جلوگیری از فارما هک، سرور، وردپرس، پوسته و افزونه‌های وردپرس را به روز نگه دارید.

حمله جستجوی فراگیر

تلاش برای ورود با استفاده از حمله جستجوی فراگیر یا brute-force، با استفاده از اجرای خودکار اسکریپت‌ها برای استخراج کلمات عبور ضعیف و دسترسی به سایت استفاده می‌شود. احراز هویت دو مرحله‌ای، محدود کردن تلاش برای ورود به سیستم، نظارت بر ورود غیر مجاز، مسدود کردن IP و استفاده از رمز عبور قدرتمند، از جمله ساده‌ترین و مؤثرترین روش‌ها برای جلوگیری از وقوع این حمله است. اما متأسفانه همین اقدامات امنیتی ساده نیز به درستی انجام نمی‌شود و روزانه حدود ۳۰،۰۰۰ وب سایت با استفاده از حملات brute-force مورد نفوذ قرار می‌گیرند.

تغییر مسیر مخرب

تغییر مسیرهای مخرب با استفاده از FTP، SFTP، wp-admin و سایر پروتکل‌ها، در نصب وردپرس آسیب‌پذیری درِ پشتی ایجاد کرده و کدهای تغییر مسیر را به وب سایت تزریق می‌کند.
تغییر مسیرها اغلب در پرونده htaccess. و سایر فایل‌های اصلی وردپررس به صورت رمز شده قرار می‌گیرند و ترافیک وب را به سایت‌های مخرب هدایت می‌کنند.

تزریق اسکریپت از طریق وب‌گاه (XSS)

(XSS) زمانی تفاق می‌افتد که یک اسکریپت مخرب به یک وب سایت یا برنامه قابل اعتماد تزریق شود. مهاجم از این کار برای ارسال کد مخرب، معمولاً اسکریپت‌های سمت مرورگر، به کاربر نهایی استفاده می‌کند. در این حمله هدف معمولاً گرفتن کوکی یا داده و یا حتی بازنویسی HTML صفحه است.
آسیب‌پذیری‌های تزریق اسکریپت، شایع‌ترین آسیب‌پذیری موجود در افزونه‌های وردپرس هستند.

حمله DOS (Denial Of Service)

شاید خطرناک‌ترین حمله از بین این حملات، DoS باشد. این حمله که از خطاها و اشکالات موجود در کد سوء استفاده می‌کند تا حافظه سیستم عامل‌های وب سایت را تحت‌الشعاع قرار دهد.
هکرها با سوء استفاده از نسخه‌های قدیمی و باگ‌های وردپرس با حملات DoS، میلیون‌ها وب سایت را مختل می‌کنند و از این طریق میلیاردها دلار کسب می‌کنند.
حال که با آسیب‌پذیری‌های وردپرس آشنا شدیم، باید یاد بگیریم چگونه سایتمان را در مقابل این حملات حفظ کنیم.

راهنمای امنیت وردپرس ۲۰۲۰

طبق آمار internet live stats، روزانه بیش از ۱۰۰ هزار وبسایت هک می‌شوند. اینجاست که بحث امنیت سایت و به خصوص امنیت وردپرس مطرح می‌شود. برای تأمین امنیت سایتتان گام‌های زیر را در نظر بگیرید:

۱. از هاست ایمن استفاده کنید

اولین سطح از امنیت سایت، امنیت سطح سرور است که میزبان یا هاست شما مسئول آن است. امنیت سرور شامل چندین لایه اقدامات امنیتی در سطح سخت‌افزاری و نرم‌افزاری است که سایت را در برابر تهدیدات پیشرفته، اعم از فیزیکی و مجازی ایمن می‌سازد. به همین دلیل، سرورهای هاست وردپرس باید با جدیدترین سیستم عامل‌ها به روز شوند و همچنین از لحاظ آسیب‌پذیری‌ها و بدافزارها کاملاً آزمایش و اسکن شوند.

فایروال‌های سطح سرور و سیستم‌های تشخیص نفوذ باید قبل از نصب وردپرس روی سرور وجود داشته باشند تا حتی در مراحل نصب وردپرس و مراحل ساخت وب سایت نیز امنیت سایت تأمین شود.
سرور نیز باید به گونه‌ای پیکربندی شده باشد که از پروتکل‌های رمزنگاری شبکه و انتقال فایل (مانند SFTP به جای FTP) استفاده کند تا محتوای حساس را مخفی کند.

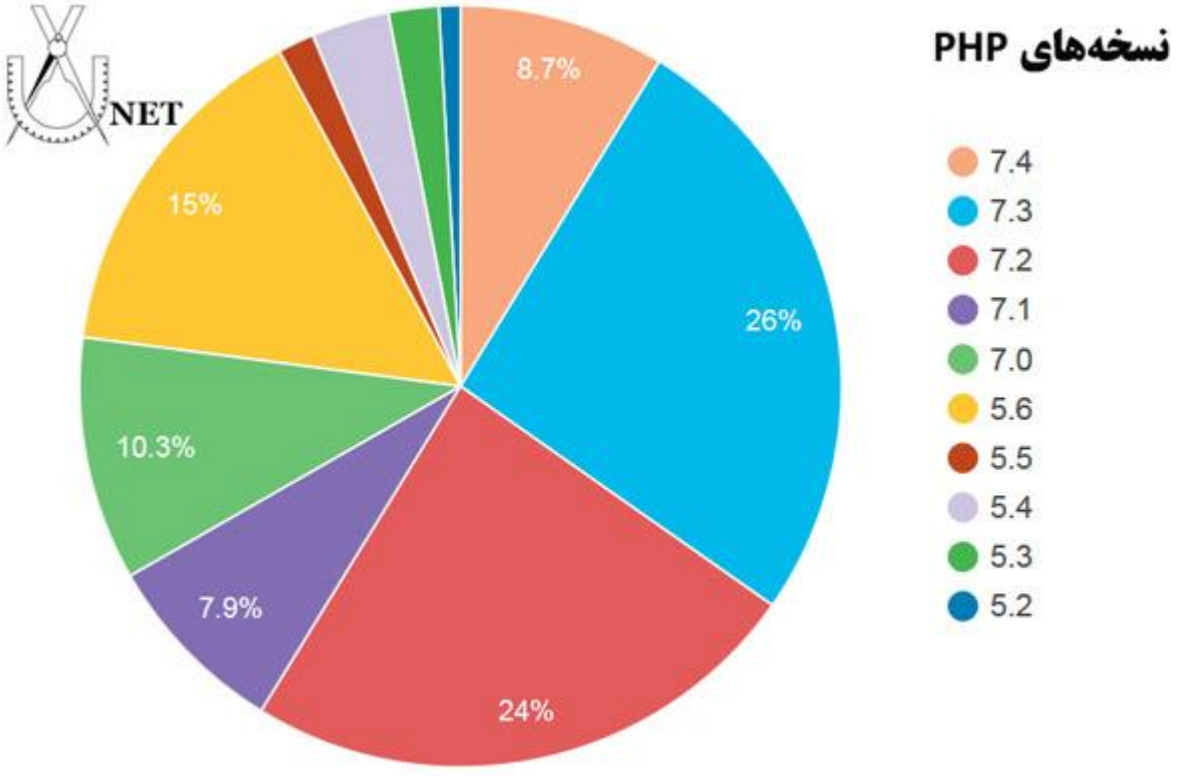
برای سایت خود از یک میزبان امن استفاده کنید

۲. از آخرین نسخه php استفاده کنید

PHP ستون فقرات سایت وردپرس شماست؛ بنابراین لازم است از آخرین نسخه آن بر روی هاست خود استفاده کنید. هر نسخه اصلی PHP معمولاً به مدت دو سال پس از انتشار کاملاً پشتیبانی می‌شود. در این مدت، اشکالات و مسائل امنیتی برطرف می‌شود و به طور مرتب بروزرسانی‌های آن منتشر می‌شود.
در حال حاضر، هر کسی که از PHP 7.1 یا پایین‌تر آن استفاده کند، دیگر پشتیبانی امنیتی ندارد و در معرض آسیب‌پذیری‌های امنیتی قرار خواهد داشت.

مدت زمان پشتیبانی نسخه هایPHP

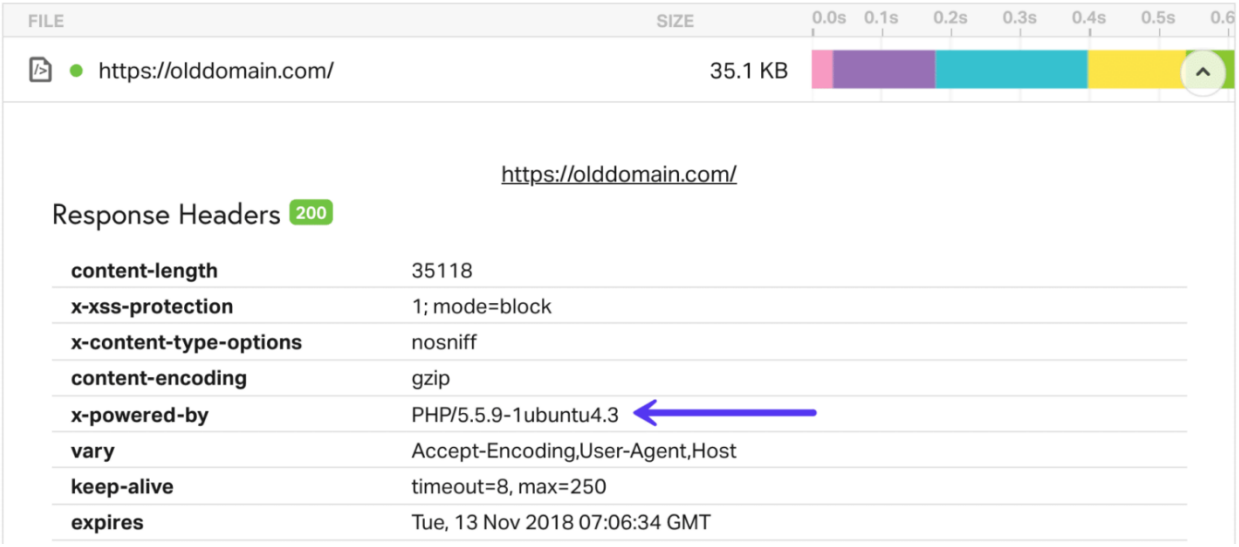
طبق صفحه رسمی وردپرس در سال ۲۰۲۰، بیش از ۲۳٫۱٪ از کاربران وردپرس هنوز هم از نسخه PHP 5.6 یا پایین‌تر استفاده می‌کنند. اگر این مورد را با PHP 7.0 و PHP 7.1 ترکیب کنیم، ۴۱٫۳٪ نسخه‌هایی استفاده می‌کنند که دیگر پشتیبانی نمی‌شود. این یک مسئله ترسناک در امنیت سایت وردپرس است!



نسخه‌های php

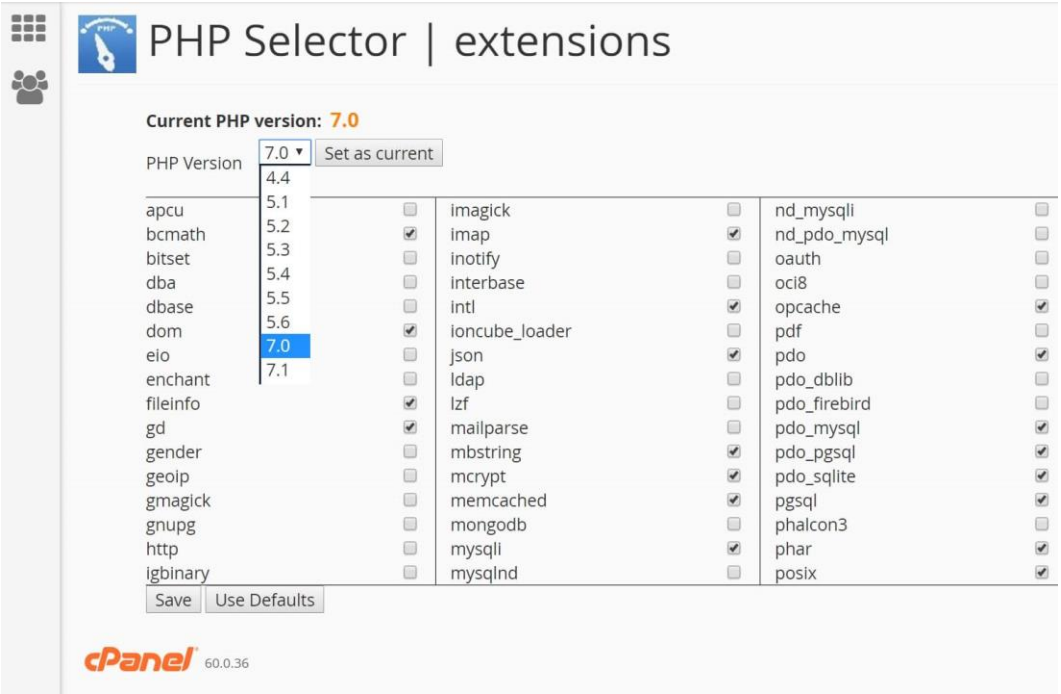
پیدا کردن نسخه PHP سایت

نمی‌دانید سایتتان از کدام نسخه PHP استفاده می‌کند؟ برخی میزبان‌ها معمولاً نسخه php را در درخواست header سایت قرار می‌دهند. یک راه سریع برای بررسی نسخه php این است که سایت خود را از طریق Pingdom تست کنید. روی اولین درخواست کلیک کنید و به دنبال پارامتر X-Powered-By باشید. به طور معمول این پارامتر نسخه PHP را نشان می‌دهد که سرور شما در حال حاضر از آن استفاده می‌کند. با این حال، *بسیاری از هاست‌ها* به دلایل امنیتی این سربرگ را حذف می‌کنند.



فهمیدن نسخه php سایت با استفاده از pingdom

اگر از cPanel استفاده می‌کنید، معمولاً می‌توانید با کلیک بر روی "PHP Select" در زیر دسته نرم‌افزار، بین نسخه‌های PHP جابجا شوید.



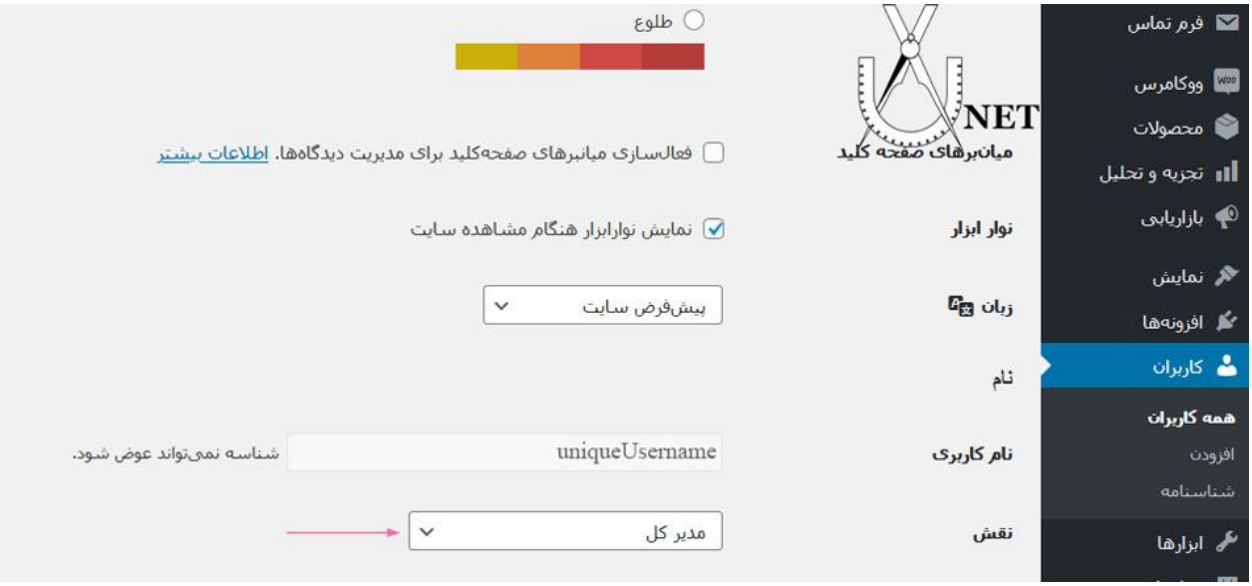
انتخاب نسخه php در سی پنل

۳. از نام کاربری و کلمه عبور هوشمندانه استفاده کنید.

یکی از بهترین راه‌ها برای رعایت موارد امنیتی وردپرس، استفاده از نام کاربری و رمز عبور هوشمند است. ساده به نظر می‌رسد؟ بله ولی بسیاری از مردم برای بخاطر سپاری رمز عبور خود معمولاً از رمزهای عبور بسیار ساده و قابل حدس استفاده می‌کنند.

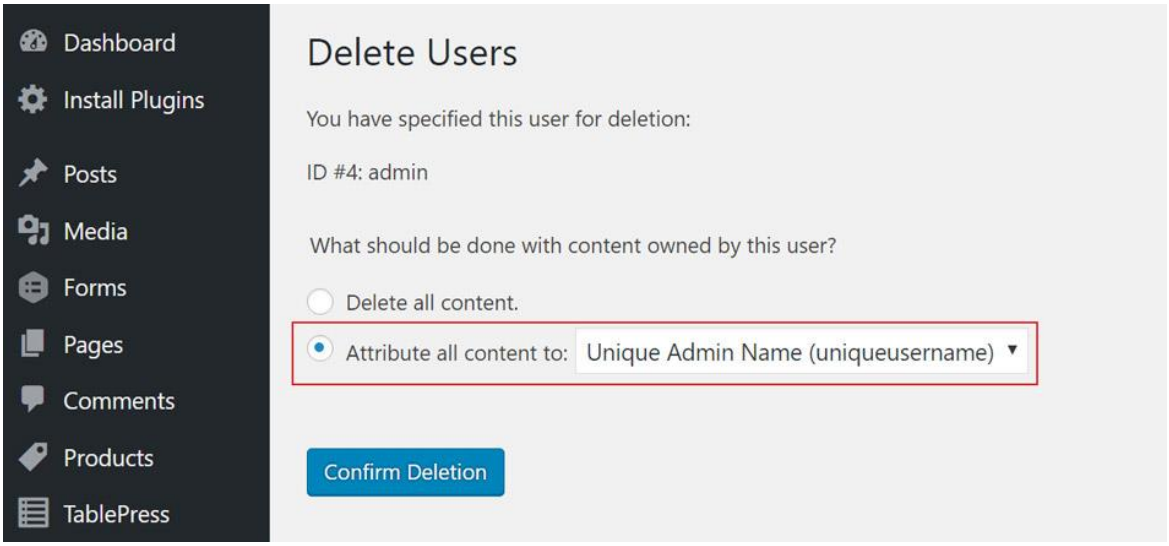
استفاده از کلمات عبور مختلف برای هر وب سایت نیز مهم است. بهترین راه برای ذخیره آن‌ها بصورت محلی در یک پایگاه داده رمزگذاری شده بر روی کامپیوترتان است. یک ابزار رایگان خوب برای این کار KeePass است.

در پیشخوان مدیریت سایت وردپرس هرگز نباید از نام کاربری پیش فرض "admin" استفاده کنید. یک نام کاربری وردپرس منحصر به فرد ایجاد کنید و در صورت وجود، کاربر "admin" را حذف کنید. شما می‌توانید این کار را با اضافه کردن یک کاربر جدید در قسمت "کاربران" در داشبورد وردپرس و اختصاص دادن نقش "administrator"به آن انجام دهید.



تغییر نقش کاربر به مدیر کل

پس از اختصاص نقش مدیر به کاربر جدید، کاربر پیش‌فرض را حذف کنید. اطمینان حاصل کنید که وقتی روی حذف کلیک می‌کنید، گزینه "Attribute all content to" را انتخاب کرده باشید. با این کار مدیر جدید به عنوان نویسنده پست‌های قبلی معرفی می‌شود.



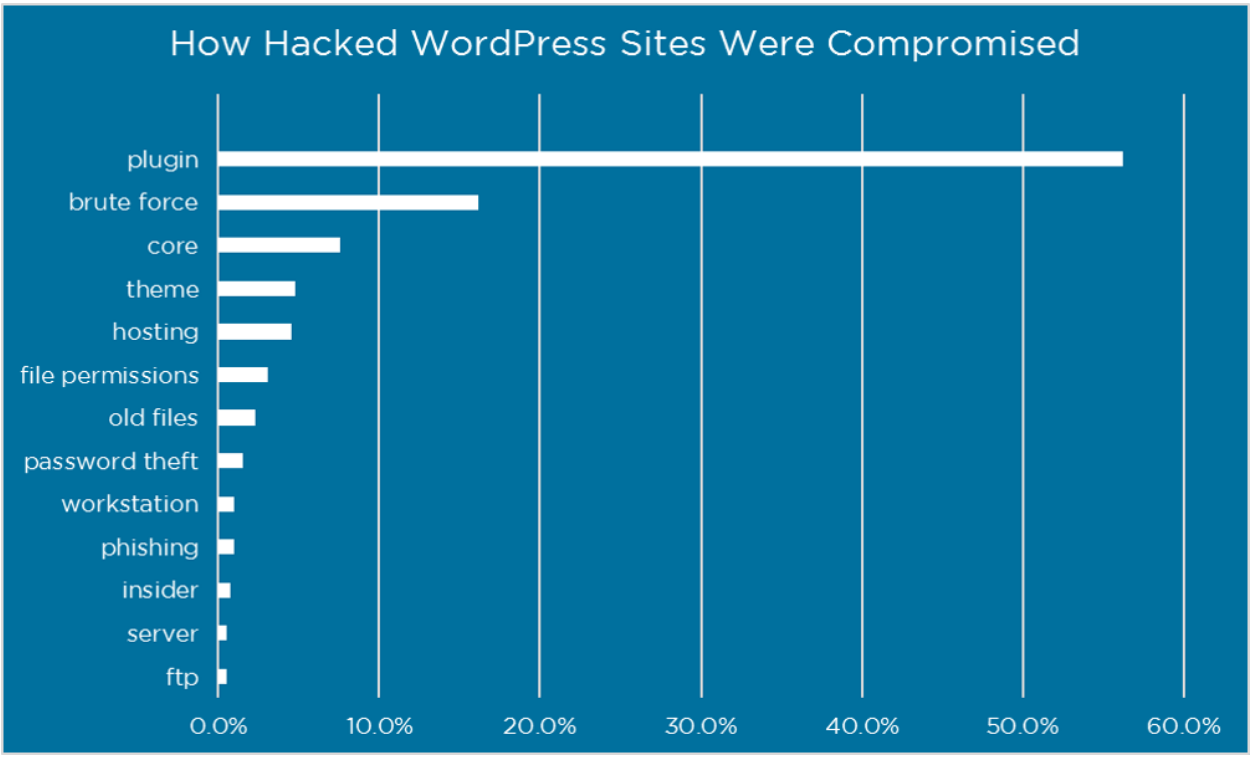
انتصاب نوشته‌های به کاربر جدید

۴. همیشه از آخرین نسخه وردپرس، افزونه‌ها و پوسته‌ها استفاده کنید

یکی دیگر از راه‌های بسیار مهم برای امنیت وردپرس، این است که همیشه آن را به روز کنید. این بروزرسانی‌ها شامل هسته، افزونه‌ها و پوسته وردپرس (هر دو مورد از مخزن وردپرس و نسخه پولی) است. افرونه‌های وردپرس قطعاً بنا به دلایلی بروزرسانی می‌شوند و این موارد شامل پیشرفت‌های امنیتی و رفع اشکالات کدنویسی هستند.

بسیاری از کاربران از بروزرسانی افزونه‌ها یا پوسته‌های سایت خود می‌ترسند. بسیاری از آن‌ها معتقدند که "بروزرسانی سایتشان را خراب می‌کند" یا "تغییرات اصلی از بین می‌رود" یا "افزونه X کار نمی‌کند" یا " به عملکرد جدید افزونه احتیاجی ندارند".

آیا می‌دانید در سال ۲۰۱۶، آسیب‌پذیری‌های افزونه وردپرس بزرگ‌ترین عامل نفوذ به وب‌سایت بود و ۵۵,۹٪ از راه نفوذ مخرب به سایت از این طریق بوده است؟



https://www.wordfence.com/blog/2016/03/attackers-gain-access-wordpress-sites

همچنین توصیه می‌کنیم فقط افزونه‌های قابل اعتماد را نصب کنید. برای نصب افزونه ناشناس حتماً به مخزن افزونه وردپرس مراجعه کرده و نظرات کاربران را در مورد آن بررسی کنید. به هیچ عنوان از سایت‌های ناشناس برای دانلود افزونه استفاده نکنید.

برای اسکن کردن افزونه یا فایل‌های پوسته، می‌توانید از یک ابزار آنلاین مانند VirusTotal استفاده کنید تا ببینید که آیا بدافزاری در افزونه را تشخیص می‌دهد یا خیر.

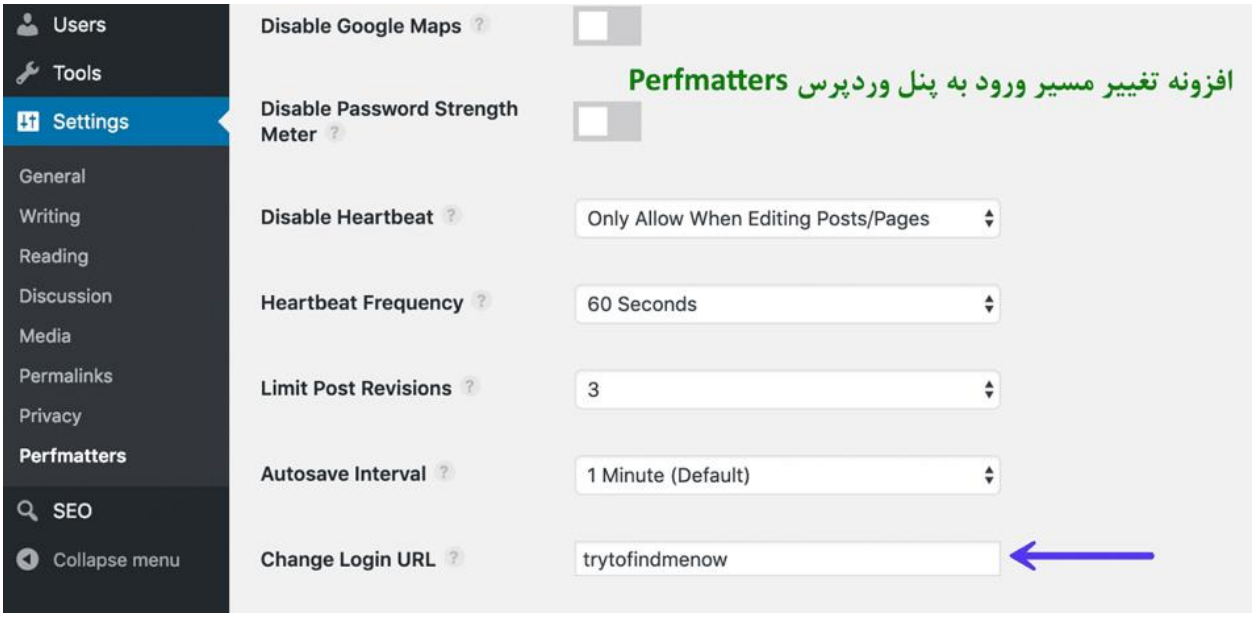
۵. صفحه ادمین وردپرس را ایمن کنید

گاهی اوقات استراتژی پنهان کردن می‌تواند امنیت را افزایش دهد. قفل کردن قسمت ورود به وردپرس راهی خوب برای تقویت امنیت سایت است. دو روش عالی برای این کار وجود دارد؛ ابتدا با تغییر URL پیش فرض wp-admin، مسیر ورود به سیستم را تغییر دهید و سپس تعداد دفعات تلاش برای ورود کاربر را نیز محدود کنید.

✓ نحوه تغییر URL ورود به وردپرس

به طور پیش فرض URL ورود به سایت وردپرس domain.com/wp-admin است. یکی از مشکلات این امر این است که همه ربات‌ها، هکرها و اسکریپت‌های موجود نیز این را می‌دانند.

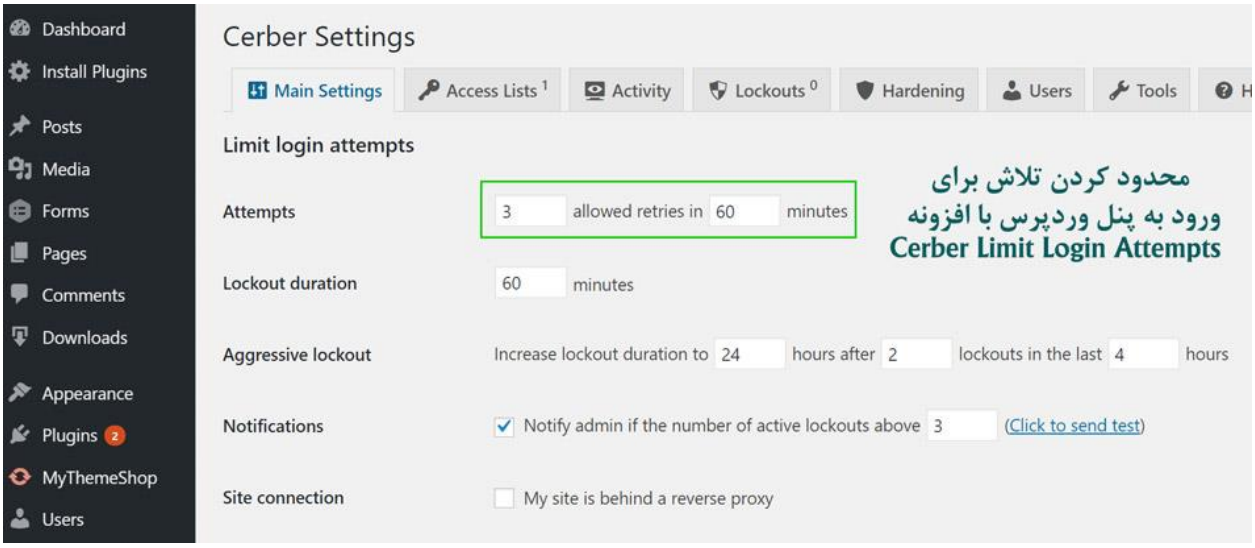
برای تغییر URL ورود به سیستم وردپرس، توصیه می‌کنیم از افزونه رایگان ورود به سیستم WPS Hide یا افزونه پریمیوم Perfmatters استفاده کنید. هر دو افزونه یک فیلد ورودی ساده دارند. فقط به یاد داشته باشید آدرسی منحصر به فرد را انتخاب کنید که قبلاً در لیست وجود نداشته باشد.



تغییر آدرس ورود به پنل وردپرس

✓ محدود کردن تعداد دفعات تلاش برای ورود

در حالی که راه‌حل فوق برای تغییر URL ورود می‌تواند به کاهش تلاش‌های ورود به سیستم کمک کند، محدود کردن تعداد دفعات وارد کردن رمز عبور نیز می‌تواند بسیار مؤثر باشد. افزونه رایگان Cerber Limit Login Attempts راهی عالی برای تنظیم آسان مدت زمان بسته شدن، تلاش برای ورود به سیستم و لیست‌های سفید و سیاه IP است.



محدود کردن ورود به پنل وردپرس

۶. از تأیید هویت دو مرحله‌ای استفاده کنید

مهم نیست که رمز عبور شما چقدر ایمن باشد، همیشه این خطر وجود دارد که کسی آن را کشف کند. احراز هویت دو عاملی یا دو مرحله‌ای، شامل یک فرآیند دو مرحله‌ای است که در آن نه تنها به رمز عبور خود برای ورود به سیستم بلکه به رمز دیگری هم برای ورود به سیستم نیاز دارید. این گذرواژه عموماً یک متن (SMS)، تماس تلفنی یا گذرواژه یک بار مصرف مبتنی بر زمان (TOTP) است.

در بیشتر موارد، این ترفند در جلوگیری از حملات جستجوی جامع به سایت وردپرس ۱۰۰ درصد مؤثر است؛ زیرا تقریباً غیرممکن است که مهاجم هم رمز عبور و هم تلفن همراه شما را در اختیار داشته باشد.

احراز هویت دومرحله‌ای

برای فعال‌سازی تأیید دو مرحله‌ای ورود به وردپرس، می‌توانید از افزونه‌های زیر استفاده کنید:

- Google Authenticator
- Two Factor Authentication

پس از نصب و پیکربندی یکی از افزونه‌های فوق، به طور معمول یک قسمت دیگر در صفحه ورود به وردپرس اضافه می شود تا کد امنیتی خود را وارد کنید.
این روش می‌تواند به راحتی با تغییر URL پیش‌فرض ورود به وردپرس که قبلاً به آن پرداختیم، ترکیب شود. بنابراین نه تنها آدرس صفحه ورود شما مخفی خواهد بود؛ بلکه کلمه عبورتان نیز غیرقابل حدس است.

۷. از HTTPS استفاده کنید

یکی از راه‌هایی که برای سخت کردن نفوذ مهاجم به سایت وردپرس نادیده گرفته می‌شود، نصب یک گواهی SSL و اجرای سایت خود از طریق HTTPS است.

➢ اما استفاده از https چه فایده‌ای دارد؟

۱. امنیت

بزرگترین دلیل استفاده از https اضافه کردن امنیت به سایت و بخصوص سایت‌های فروشگاهی است. این پروتکل ارتباط بین مرورگر و سایت را ایمن کرده و از حملاتی مانند حمله مرد میانی (MITM) جلوگیری می‌کند.

۲. سئو

گوگل رسماً اعلام کرده که HTTPS به عنوان یک عامل رتبه بندی در نظر گرفته می‌شود. پس استفاده از این پروتکل می‌تواند یک مزیت رقابتی نسبت به سایر رقبا ایجاد کند.

۳. اعتماد و اعتبار

طبق نظرسنجی از GlobalSign، ۲۸,۹ درصد از بازدیدکنندگان به دنبال نوار آدرس سبز در مرورگر خود هستند و ۷۷٪ آن‌ها نگران رهگیری یا سوء استفاده آنلاین از اطلاعاتشان می‌باشند. با دیدن این نوار سبزرنگ در مرورگر، بلافاصله مشتری اطمینان می‌یابد که امنیت اطلاعاتش فراهم می‌شود.

۸. نسخه وردپرس خود را مخفی کنید

هرچه دیگران کمتر درمورد پیکربندی سایت وردپرس شما بدانند، بهتر است. اگر مشخص شود که از نسخه قدیمی وردپرس استفاده می‌کنید، نسبت به امتحان شانس خود برای نفوذ به سایتتان حساس‌تر خواهند شد. به طور پیش فرض، نسخه وردپرس در سورس کد هدر سایت نشان داده می‌شود.

```
</script>
<script type='text/javascript' src='http://testing.dev/ds-plugins/ds-
<!--[if lt IE 9]>
<script type='text/javascript' src='http://testing.dev/wp-content/the
<![endif]-->
<link rel='https://api.w.org/' href='http://testing.dev/wp-json/' />
<link rel="EditURI" type="application/rsd+xml" title="RSD" href="http
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http
<meta name="generator" content="WordPress 4.6.1" />
        <style type="text/css">
            li#wp-admin-bar-ds-cli .ab-icon:before {
                font-family: 'serverpress';
                position: relative;
```

نسخه وردپرس در سورس کد

مجدداً توصیه می‌کنیم وردپرس خود را همیشه به روز نگه دارید، بنابراین نیازی نیست که نگران این موضوع باشید.

برای حذف نمایش ورژن وردپرس، کد زیر را به فایل function.php موجود در پوسته اضافه کنید:

```
function wp_version_remove_version() {
return '';
}
add_filter('the_generator',
'wp_version_remove_version');
```

توجه: اگر ویرایش کد این فایل به درستی انجام نشود، می‌تواند سایت شما را خراب کند.

۹. آخرین هدرهای امنیتی HTTP را اضافه کنید

قدم دیگری که می‌توانید برای سخت کردن امنیت وردپرس خود بردارید، استفاده از هدرهای امنیتی HTTP است. این‌ها معمولاً در سطح سرور وب پیکربندی شده‌اند و به مرورگر می‌گویند که هنگام اداره محتوای سایتتان چگونه رفتار کند. هدرهای امنیتی HTTP زیادی وجود دارد، اما مهم‌ترین آن‌ها عبارتند از:

- Content-Security Policy
- X-XSS-Protection
- Strict-Transport-Security
- X-Frame-Options
- Public-Key-Pins
- X-Content-Type

می‌توانید با استفاده Devtools گوگل کروم و نگاه کردن به هدر سایت، بررسی کنید که در حال حاضر کدام یک از موارد مذکور در سایت وردپرس شما در حال اجرا هستند.

هدرهای امنیتی http

همچنین می‌توانید وب سایت وردپرس خود را با ابزار رایگان Securityheaders.io بررسی کنید. این ابزار هدرهای امنیتی HTTP فعال روی سایت را نمایش می‌دهد. اگر مطمئن نیستید که چگونه آن‌ها را پیاده سازی کنید، از پشتیبانی هاست خود کمک بگیرید.

بررسی هدرهای امنیتی باSecurityheaders

۱۰. از افزونه‌های امنیتی وردپرس استفاده کنید

افزونه‌های بسیاری وجود دارد که به امنیت بیشتر سایت وردپرسی کمک می‌کنند. برخی از آن‌ها عبارتند از:

- Sucuri Security
- iThemes Security
- WordFence Security
- WP fail2ban

- SecuPress

ویژگی مشترک و بسیار مهم تمامی این افزونه‌های امنیتی، این است که شامل یک برنامه کنترلی هستند. به این صورت که نصب وردپرس شما را بازرسی می‌کنند و به دنبال تغییراتی که درپرونده‌های اصلی فایل‌های وردپرس رخ داده است، می‌گردند.

افزونه دیگری که در این قسمت می‌تواند مفید باشد، WP Security Audit Log plugin است. این افزونه خصوصاً برای وردپرس چند-سایته و یا سایت با چند نویسنده مفید است. این افزونه به تضمین بهره‌وری کاربر کمک می‌کند و به مدیران اجازه می‌دهد تا همه آنچه را که تغییر می‌یابد، ببینند مانند: ورود به سیستم؛ تغییر رمز عبور؛ تغییرات قالب؛ تغییرات ویجت و ابزار؛ ایجاد پست جدید؛ به روزرسانی‌های وردپرس و غیره.

۱۱. امنیت پایگاه داده را بهبود ببخشید

چند روش برای بهتر کردن امنیت در پایگاه‌داده وردپرس وجود دارد. اولین مورد استفاده از نام پایگاه‌داده هوشمندانه است. به عنوان مثال اگر نام سایتتان "wordpresstricks" است، به صورت پیشفرض احتمالاً نام پایگاه داده سایت نیز "wp_wordpresstricks" خواهد بود. با انتخاب نامی هوشمندانه برای دیتابیس خود، تشخیص و دسترسی هکر به سایتتان را سخت‌تر کنید.

توصیه دوم استفاده از پیشوند متفاوت برای جدول پایگاه‌داده است. به طور پیشفرض وردپرس از "wp_" برای نام‌گذاری جداول استفاده می‌کند.

۱۲. اجازه تغییر در فایل و سرور را بررسی کنید.

اگر مجوزهای دسترسی به فایل‌ها خیلی سست باشد، به راحتی سایتتان مورد حمله قرار خواهد گرفت. از طرفی اگر مجوزها بیش از حد سخت و بدون انعطاف باشد، کارایی سایتتان مختل خواهد شد. بنابراین لازم است مجوزهای دسترسی را به درستی پیکربندی کنید.

مجوزهای پرونده

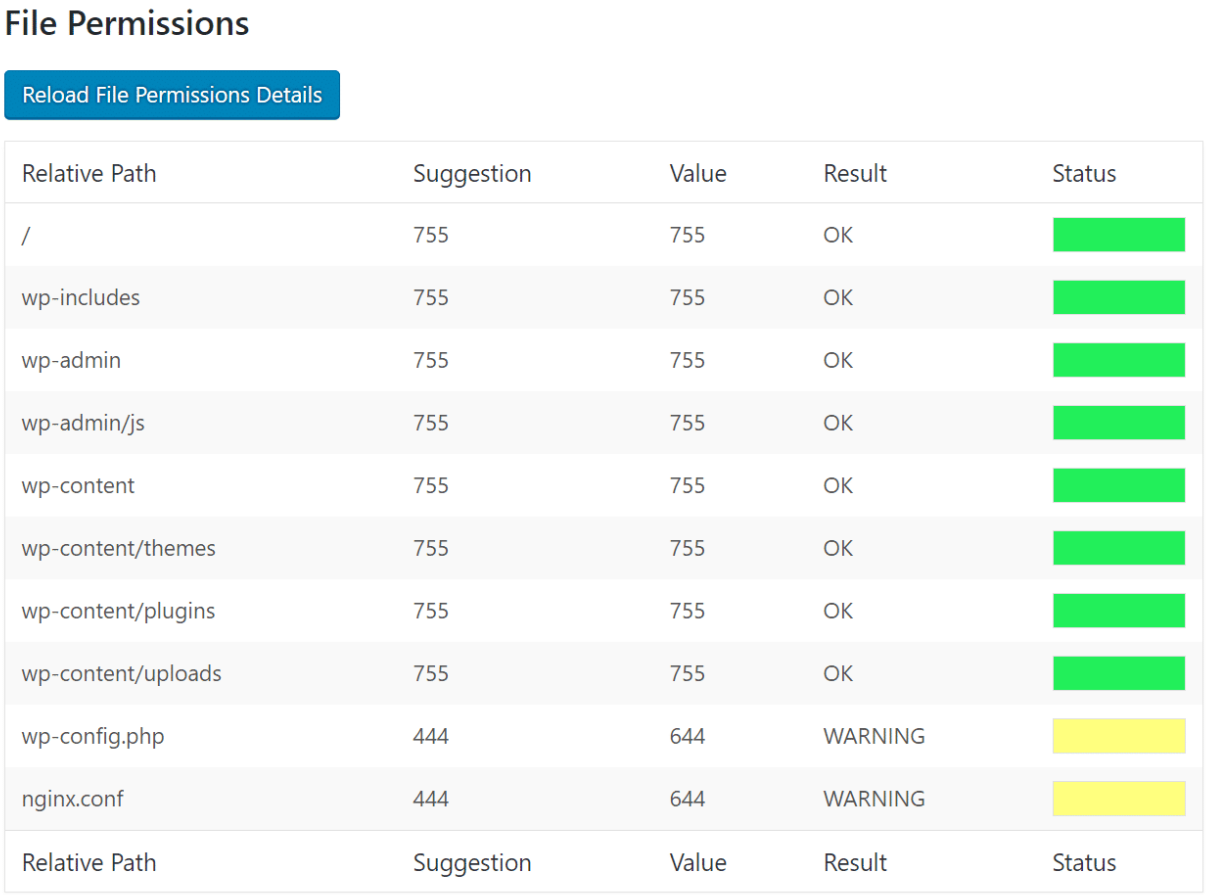
- Read: اگرکاربر حق خواندن پرونده را داشته باشد، مجوزهای خواندن اختصاص داده می‌شود.
- Write: اگر کاربر حق نوشتن یا تغییر پرونده را داشته باشد، مجوزهای نوشتن اختصاص داده می‌شوند.
- Execute: اگر کاربر حق داشته باشد اسکریپت اجرا کند، مجوزهای اجرا را خواهد داشت.

مجوزهای دایرکتوری

- Read: اگر کاربر حق دسترسی به محتویات پوشه/دایرکتوری مشخص شده را داشته باشد، مجوزهای خواندن اختصاص داده می‌شود.

- Write: اگر کاربر حق داشته باشد فایل‌های داخل پوشه/فهرست را اضافه یا حذف کند، مجوزهای نوشتن را خواهد داشت.
- Execution: اگر کاربر حق دسترسی به دایرکتوری واقعی و اجرای توابع و دستورات را داشته باشد، از جمله امکان حذف داده‌ها در پوشه/دایرکتوری از طریق اجرای کد، مجوز اجرا اختصاص می‌یابد.

برای بررسی دسترسی‌ها بر روی سایت، از افزونه رایگان مانند iThemes Security استفاده کنید.



بررسی مجوز دسترسی باiThemes Security

مجوز دسترسی پرونده‌ها چگونه باشد؟

- مجوز کلیه پرونده‌ها باید ۶۴۴ یا ۶۴۰ باشد. به استثناء wp-config.php که باید ۴۴۰ یا ۴۰۰ باشد تا سایر کاربران روی سرور نتوانند آن را بخوانند.
- مجوز همه دایرکتوری‌ها باید ۷۵۵ یا ۷۵۰ باشند.
- مجوز هیچ دایرکتوری نباید ۷۷۷ باشد، حتی دایرکتوری‌های آپلود.

۱۳. ویرایش پرونده در داشبورد وردپرس را غیرفعال کنید

بسیاری از سایت‌های وردپرس دارای چندین کاربر هستند که می‌توانند امنیت وردپرس را پیچیده‌تر کند. ممکن است به اشتباه به سایر نویسندگان اجازه ویرایش کد را بدهید؛ به همین دلیل، غیرفعال کردن "ویرایشگرپوسته" در وردپرس می‌تواند مفید باشد.

اگر سایت وردپرس شما هک شده است، اولین کاری که ممکن است هکر انجام دهد این است که فایل‌های موجود در قسمت "ویرایشگر پوسته" را ویرایش کند. این کار یک روش سریع برای اجرای کدهای مخرب در سایت شماست. اگر از ابتدا از طریق داشبورد به این امر دسترسی نداشته باشد، نمی‌تواند از این طریق سایت را مختل کند.

کد زیر را در پرونده wp-config.php خود قرار دهید تا قابلیت "edit_themes"، "edit_plugins" و "edit_files" همه کاربران حذف شود.

```
define('DISALLOW_FILE_EDIT', true);
```

۱۴. از hotlinking جلوگیری کنید

مفهوم هات لینک بسیار ساده است. شما تصویری را در اینترنت پیدا می‌کنید و از آدرسی که تصویر در آن جا قرار دارد، به طور مستقیم در سایت خود استفاده می‌کنید. در واقع با وجود اینکه تصویر را در سایت خود بارگذاری نکرده‌اید، ولی از آن تصویر استفاده می‌کنید. Hotlinking باعث استفاده از پهنای باند سایت مبدأ می‌شود و در نتیجه هزینه اضافی برای آن سایت ایجاد می‌کند.

➢ جلوگیری از هات لینکینگ در apache

کد زیر را به پرونده htaccess. خود اضافه کنید:

```
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http(s)?://(www\.)?yourdomain.com [NC]
RewriteRule \.(jpg|jpeg|png|gif)$ http://dropbox.com/hotlink-placeholder.jpg [NC,R,L]
```

سطر سوم مرجع مجاز را مشخص می‌کند؛ سایتی که مجاز به لینک مستقیم به تصویر است،که در واقع سایت خودتان است. اگر می‌خواهید به چندین سایت اجازه لینک‌دهی دهید؛ می‌توانید این سطر را کپی کرده و سایر دامنه‌ها را نیز به آن اضافه کنید.

جمع‌بندی

همان‌طور که مشاهده می‌کنید، روش‌های مختلفی وجود دارد که می‌توانید امنیت سایت وردپرس را بهبود ببخشید. استفاده از کلمات عبور هوشمندانه، به روز نگه داشتن هسته و افزونه‌ها و انتخاب یک میزبان امن وردپرس مدیریت شده، معدود مواردی هستند که باعث می‌شود خیالتان در قبال امنیت سایت راحت باشد.

خدمات یوایکس نت

- طراحی و بازطراحی سایت
- سئو و بهینه‌سازی
- طراحی تجربه‌کاربری وب سایت و اپلیکیشن (UX)
- تولید محتوای سایت و شبکه‌های اجتماعی
- طراحی گرافیک اختصاصی
- تحلیل و بررسی سایت

برای کسب اطلاعات بیشتر و تماس با ما، به وب سایت UXNET.IR مراجعه نمایید.