وردپرستان را ضد گلوله کنید

[امنیت در وردپرس]

رده بندی : متوسط تا پیشرفته

نویسنده : ملیکا اسدزاده

ارائه شده توسط وندابلاگ در آدرس : Blog.VandaHost.net

کپی برداری از این مطلب فقط با کسب اجازه از صاحب امتیاز [نویسنده و ارائه دهنده] و درج کامل منبع مجاز میباشد.

بخش اول :

در دنیای اینترنت امنیت از اهمیت بسیاری زیادی برخوردار است. گرچه متاسفانه اینطور به نظر میرسد که این روزها ما به "امنیت" فقط و فقط به طور شفاهی اهمیت میدهیم و پای عمل که میرسد از کنار خیلی مسائل به سادگی میگذریم. افراد زیادی را میبینم که از پایین بودن امنیت وردپرس حرف میزنند و چون این وسط سایت هایشان یکی دو باری هم هک شده است از این مینالند که وردپرس ضعف های امنیتی زیادی دارد و برای همین آن را سیستم مدیریت محتوای مناسبی نمیدانند. البته میپذیریم که هر اسکریپتی باگ های خاص خودش را دارد اما اینکه ما بخش مدیریت اسکریپتمان را برای همه باز بگذاریم و رمزمان از ۱۲۳۴۵ آن طرف تر نرود و تازه یوزرمان هم همان adminآشنای همیشگی باشد و عملا سایتمان را به امان خدا رها کرده باشیم و بعد که هک شدیم بیاییم و تقصیر را گردن اسکریپت بیاندازیم واقعا بی انصافی است. به نظر شخصی من و البته به نظر میلیون ها نفر دیگر در سراسر جهان، وردپرس واقعا قدرتمند است، خوب پس بیایید این بار با هم ضد گلوله کردن وردپرسمان را یاد بگیریم. اینکه در این مقاله امنیت وردپرس را هدف میگیرم دلیلش نا امنی وردپرس نیست، بلکه دلیلش این است که این اسکریپت طرفداران بسیار زیادی دارد و راحت میتوان گفت از هر ۱۰ نفری که میخواهند یک سایت راه بیاندازند دست کم ۶ نفرشان مطمئنند که باید وردپرس را انتخاب کنند.

خوب، دیگر مقدمه چینی کافی است. حالا وقت این است که با هم آستین ها را بالا برویم و به سراغ اصل کار برویم. با من همراه باشید و مراحل ضد گلوله کردن وردپرس را یک به یک به همراه من دنبال کنید.

در هنگام نصب:

اگر قرار به رعایت امنیت است، باید اولین آجر را نیز که همان نصب وردپرس است درست بگذاریم. حتما همه شنیده اید که شاعر میگوید : "خشت اول چون نهد معمار کج، تا سریا میرود دیوار کج" سریا هم میدانم با ث است.

میخواستم ببینم حواستان هست یا نه!!! خوب حالا ببینیم در زمان نصب چه نکاتی را باید رعایت کنیم:

۱ -یوزر Admin نسازید!

در کدام قانونی نوشته شده که اسم مدیر باید حتما Admin باشد؟ کمی خلاق باشید و در زمان نصب وردپرس برای مدیر یک نام کاربری عجیب و غریب در نظر بگیرید که در هیچ کجای دنیا شناخته شده نباشد. مثلا جای ادمین، نام G67BnMol0oOl1iرا انتخاب کنید. استفاده از نامی غیر از نام Admin برای مدیر، باعث میشود هکر ها مجبور شوند علاوه بر پسورد شما، نام کاربریتان را هم حدس بزنند. (البته ۱۰۰ درصد نه با مغزشان، بلکه با نرم افزار) و اگر شما رئیس سازمان CIA نباشید، احتمالا شکستن چنین ترکیبی با یک کامپیوتر خانگی، اگر پسوردتان را هم در نظر بگیریم خیلی خیلی وقت میخواهد! خیلی خیلی....

اگر کار از کار گذشته و قبلا این یوزر را ساخته اید...

اشکالی ندارد، بگذارید با هم نامش را عوض کنیم. به روش پیچیده اش کاری ندارم ولی ساده ترین روش این است:

- یک مدیر جدید در وردپرستان ایجاد کنید.
- با مدیر جدید لاگین کرده و مدیر قبلی را پاک کنید
- حواستان باشد که نوشته های مدیر قبلی را پاک نکنید و در هنگام پاک کردن مدیر قبلی، نوشته هایش را به نام کاربری جدیدتان نسبت دهید.

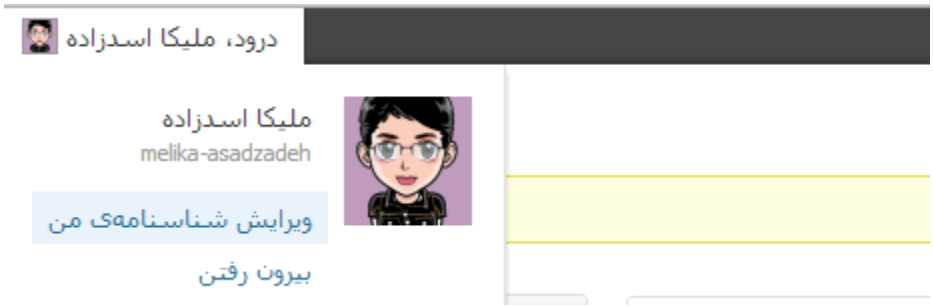
۲ - پیشوند جداول دیتابیس

در زمان نصب وقتی وردپرس از شما میپرسد که مایلید پیشوند جداول دیتابیستان به چه صورت باشد. اگر شما در این بخش تغییری ایجاد نکنید به طور پیشفرض، پیشوند جداول شما معادل wp_ خواهد بود. خوب اگر به دنبال امنیت هستید در زمان نصب حتما پیشوند جداول را به پیشوند پیچیده تری تغییر دهید چون وگرنه برای همه کاملا واضح است که پیشوند جداول یک سایت وردپرسی باید wp_ باشد. مثلا بیایید و عبارت W9b0Om_ را به عنوان پیشوند جداول انتخاب کنید.

حالا اگر نصب تمام شده و کار از کار گذشته شما دو راه پیش رو دارید. اول اینکه از طریق phpMyAdmin پیشوند ها را تغییر دهید که من این روش را توصیه نمیکنم و دوم اینکه منتظر قسمت دوم همین مقاله بمانید تا آنجا بهترین روش را به شما اموزش دهم.

۳ - نمایش عمومی نامتان را در وردپرس تغییر دهید.

وردپرس به صورت پیشفرض نام کاربری شما (که مدیر هستید) را در نوشته هایتان به نمایش میگذارد. این اصلا خوب نیست. یعنی حتی اگر شما یوزری به نام ادمین هم نداشته باشید، یک نفر به سادگی میتواند به نگاه به نویسنده ی پست هایتان بفهمد که نام کاربری شما چیست. راه حل این مشکل بسیار ساده است. کافی است در وردپرس به شناسنامه تان مراجعه کنید و با وارد کردن نام و نام خانوادگیتان در این بخش، نمایش عمومی نامتان را از نام کاربریتان به نام / نام خانوادگی یا لقبتان تغییر دهید.



راهنما : با ایستادن روی نامتان در نوار بالایی مدیریت وردپرس، میتوانید به شناسنامه تان دسترسی داشته باشید.

۴ - نگذارید وردپرس لینکی به یوزر نیم شما در نوشته ها و به طور کلی طرف کاربران به نمایش بگذارد.

اگر فکر میکنید با انجام مرحله ی شماره ۲ کارتان به اتمام رسیده در اشتباهید. وردپرس عزیز لطف میکند و نام نویسنده را به یوزرش لینک میکند. البته این مسئله ممکن است در قالب های مختلف متفاوت باشد اما شما در این زمینه دو انتخاب دارید. اول اینکه با دست کاری قالبتان به طور کامل لینک نویسنده را حذف کنید. در وبلاگهایی که دارای یک نویسنده هستند این مسئله چندان هم مهم نیست اما اگر بیش از یک نویسنده داشته باشید، این مسئله کارایی بلاگتان را از بین خواهد برد. بنابراین برای حل این مشکل به شیوه ی زیر عمل کنید:

-افزونه ی Edit Author Slug را روی وردپرستان نصب کنید.

-به شناسنامه تان در وردپرس مراجعه کنید و در بخش edit author slug لینک جدیدی به یوزرتان اختصاص دهید.

به این شکل دیگر نام کاربری واقعی شما در لینک نویسنده به نمایش در نخواهد آمد و کسی به این سادگی ها قادر نخواهد بود نام کاربری واقعی شما را پیدا کند.

۵ - روی فولدر ادمین پسورد بگذارید.

دو لایه ی امنیتی همیشه بهتر از یک لایه ی امنیتی است. من که اصلا دوست ندارم اگر کسی آدرس ورود به مدیریت را در ادامه ی آدرس بلاگم تایپ کند به سادگی به صفحه ی ورود به مدیریت هدایت شود. (راستش را بخواهد اصلا دوست ندارم به صفحه ی ورود هدایت شود!) بنابراین یکی از ساده ترین کارهایی که هرگز نباید فراموش کنید این است که روی فولدر ادمینتان پسورد بگذارید. برای گذاشتن پسورد روی فولدر ادمین به شکل زیر عمل کنید:

- یک نام کاربری و یک کلمه ی عبور مناسب که علاوه بر دارا بودن امنیت مناسب، فقط و فقط از حروف و اعداد (بزرگ و کوچک مهم نیست) تشکیل شده باشد برای خود انتخاب کنید.
- روی اینجا کلیک کنید و در صفحه ای که برایتان باز میشود، در قسمت یوزر نیم، نام کاربری ای که انتخاب کردید و در قسمت پسورد، کلمه ی رمزی که انتخاب کرده اید را وارد کرده و سپس روی دکمه submit کلیک کنید. به سایر تنظیمات کاری نداشته باشید چون ما قصد نداریم از همه ی کد هایی که این سایت به ما میدهد استفاده کنیم و فقط و فقط به یوزر نیم و پسوردی که هش میکند احتیاج داریم.
- محتوایی که این سایت در بخش htpasswd. به شما تحویل میدهد را در ذخیره کنید.
- در هاست خود به یک فولدر قبل از public_html بروید. (در cpanel همان Home و در دایرکت ادمین یک فولدر پس از فولدر نام دامنه) در این جا یک فولدر با یک نام عجیب و غریب بسازید. منظورم از عجیب و غریب چیزی است هر کسی نتواند حدس بزند ولی لازم نیست از علامات و ... استفاده کنید.
- در این فولدر یک فایل بسازید با نام) htpasswd. نامش مهم نیست ولی نقطه ی اولش را لازم داریم، برای سادگی کارتان به همین htpasswd. اکتفا کنید.(
- حالا به فولدر ادمین وردپرس بروید .(wp-admin) در این فولدر یک فایل با نام htaccess. ایجاد کنید و کد زیر را البته با تغیرات لازم در آن قرار دهید :

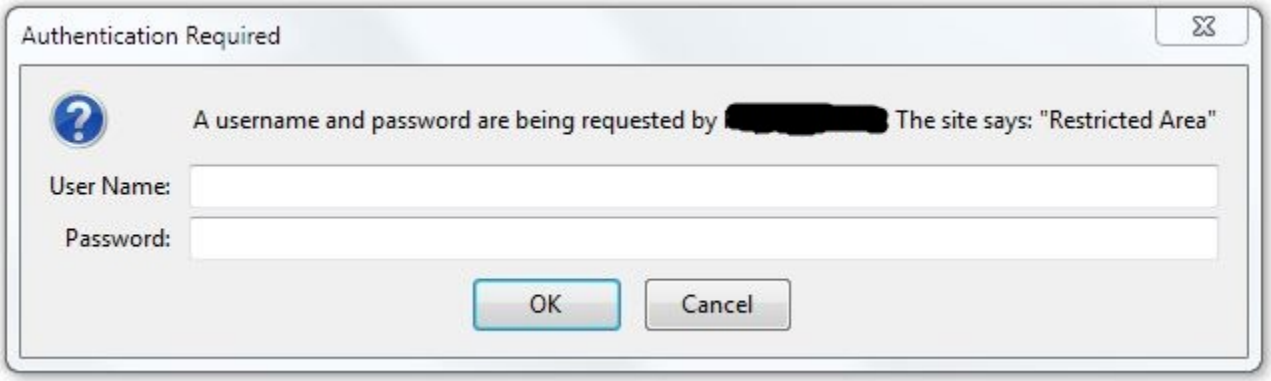
```
ErrorDocument 401 default

AuthName "Restricted Area"
AuthType Basic
AuthUserFile /home/user/samplefolder/.htpasswd
AuthGroupFile /home/user/public_html/wp-admin/
require valid-user

<Files admin-ajax.php>
   Order allow,deny
   Allow from all
   Satisfy any
</Files>
```

در کدی که در بالا برایتان نوشتم لازم است به جای user نام کاربری خودتان در هاستی که دارید را قرار دهید و بجای samplefolder نام فولدری که ساختید و فایل htpasswd. را در آن قرار دادید. (البته توجه کنید شاید مسیر شما بجای home از مسیر دیگری آغاز شود، مثلاhome2 ، home3و ....). قسمت آخر را هم به هیچ عنوان فراموش نکنید چون اگر دسترسی به فایل admin-ajax.php را مجاز نکنید بعدا در پنل مدیریت چیزی جز آشفتگی نسیبتان نخواهد شد.

- خوب حالا اگر این مراحل را درست طی کرده باشید در زمان ورود به مدیریت باید با یک پیام روبرو شوید که از شما تقاضای نام کاربری و پسورد میکند. اینجا کافی است نام کاربری و پسوردی که به تازگی برای خود انتخاب کرده اید را وارد کنید تا بتوانید به صفحه ی ورود به بخش مدیریت بروید. مثل شکل زیر:



۶ - wp-config.php جایش اینجا نیست!

خواهشا کمی بیشتر به فکر فایل کانفیگتان باشید. اگر تا امروز آن را امن نکرده اید بهتر است هر چه سریع تر به سراغش بروید و آن را به یک فولدر بالا تر از public_html سایتتان انتقال دهید. حتی الامکان دسترسی اش را هم روی ۴۴۴ بگذارید که خیالتان حسابی راحت باشد. خوشبختانه اینجا کارمان پیچیدگی زمانی که میخواهیم جای فایل کانفیگ را در جوملا عوض کنیم را ندارد. کافی است فایل کانفیگ به یک فولدر بالا تر از public_html سایتتان انتقال پیدا کند و پس از آن بقیه ی کارها پای خود وردپرس است که جای این فایل را پیدا کند.

چرا سطح دسترسی فایل htaccess. را عوض نمیکنیم؟

اگر به دنبال ضد گلوله به معنای واقعی میگردید که خوب باید دسترسی این فایل را هم روی ۴۴۴ بگذارید که نوشتن روی آن به این سادگی ها امکان پذیر نباشد اما در نظر بگیرید که این کار ممکن است در کارکرد بعضی پلاگین های امنیتی و یا پلاگین سئویی که در وردپرستان نصب کرده اید تداخل ایجاد کند. تصمیم با خودتان است!

۷ - به روز باشید

قبول دارم که گاهی به روز کردن افزونه های وردپرس کمی تا قسمتی پشیمانی به بار می آورد اما به طور کلی باید همیشه افزونه های و پوسته هایتان را به روز نگه دارید. چرایش هم کاملا واضح است. افزونه ها و پوسته های قدیمی ممکن است پر از باگ های امنیتی باشند و سایت شما را در برابرهکر ها آسیب پذیر کنند. اگر هم نگران هستید که به روز رسانی برخی از افزونه ها ممکن است سایت شما را به هم بریزد و یا یک افزونه ممکن است با ورژن وردپرس شما سازگاری نداشته باشد کافی است برای جلوگیری از هرگونه دردسر های بعدی، همیشه یک نصب وردپرس کاملا یکسان با سایتتان به صورت لوکال داشته باشید که همه ی افزونه ها را ابتدا به صورت لوکال روی آن تست کنید و بعد در صورتی که تغییرات مورد نظر در سایتتان ایرادی ایجاد نکرد، آنها را در محیط اینترنت اجرایی کنید.

۸ - حواستان به پوسته های خبیث باشد!

واقعیت این است که در ۹۹ درصد موارد وقتی افراد یک سایت وردپرسی را استارت میزنند، برای شروع کار خود از

پوسته های رایگان استفاده میکنند و از آنجایی که گربه هم محض رضای خدا موش نمیگیرد، به سادگی میتوان گفت که اگر در گوگل به دنبال پوسته های رایگان بگردید شاید از هر ۱۰ پوسته ۷ تای آنها یک جای کارشان میلنگد و اکثرشان پر از کد های base64 هستند. کد های base64 همیشه مخرب نیستند ولی از طرفی هم اگر چیزی برای مخفی کردن نداریم پس چه لزومی دارد که آن را کد کنیم؟ وقتی کدش میکنیم یعنی یک جای کار میلنگد. برای این پوسته ی خود را محک بزنید و از سلامت آن اطمینان حاصل کنید کافی است افزونه ی Theme Authenticity Checker را روی وردپرستان نصب کنید. این افزونه به شما اجازه میدهد تک تک پوسته هایی که روی سایتتان نصب کرده اید را به دنبال کد های مخرب شناخته شده جستجو کنید و حتی در مواردی در پوسته ها بهبود ایجاد کنید.

استثنا : البته همه ی مواردی که این افزونه پیدا میکند مخرب نیستند. به عنوان مثال اگر درست به خاطر داشته باشم ایمیج ریسایزر TimThumb در جایی که کسی یکی از تصاویر شما را در سایتش به کار برده باشد، برای جلوگیری از hotlinking و هدر رفتن پهنای باند شما یک خروجی تصویری به شخص خاطی نشان میدهد که در این خروجی نوشته شده این شخص اجازه ندارد به صورت مستقیم تصاویر شما را در سایتش استفاده کند. این خروجی خودش یک تصویر است که از یک کد base64 حاصل میشود. خوب طبعا اگر قرار است پهنای باند شما هدر نرود بهترین چاره همین base64 خواهد بود. حالا اگر پوسته ای که اید کد درونش استفاده شده را به دست افزونه ی TACبسپارید به شما هشدار خواهد داد که پوسته ی شما دارای کد base64 است. این هم از استثنا.

۹ - به وردپرستان نمک بزنید...

باور کنید شوخی نمیکنم. وردرپس بدون نمک مثل سالاد بدون سس است! تعریف salt در کانفیگ وردپرستان به شما کمک میکند کهسایت خود را در برابر حملات هکر ها چندین برابر امن تر کنید .salt ای که شما تعریف میکنید در رمز گذاری کلیه ی ارتباطات، ذخیره ی فایل ها و کوکی های ذخیره شده روی سیستم های کاربران به کار خواهد رفت و همه چیز را امن تر خواهد نمود. در عین حال گاهی هم ورد پرس salt ای که شما تعریف کرده اید را با یک استرینگ طولانی دیگر در هم می آمیزد و با ترکیب این دو، به بهترین شکل اطلاعات محرمانه ی شما را رمزگذاری میکند تا دسترسی به آنها به این سادگی ها ممکن نشود. حالا این salt را کجا تعریف کنیم؟

-به فایل کانفیگ وردپرستان مراجعه کنید(wp-config.php)

-در این فایل به دنبال کد های زیر بگردید :

```
define('AUTH_KEY',         'put your unique phrase here');
define('SECURE_AUTH_KEY',  'put your unique phrase here');
define('LOGGED_IN_KEY',    'put your unique phrase here');
define('NONCE_KEY',        'put your unique phrase here');
define('AUTH_SALT',        'put your unique phrase here');
define('SECURE_AUTH_SALT', 'put your unique phrase here');
define('LOGGED_IN_SALT',   'put your unique phrase here');
define('NONCE_SALT',       'put your unique phrase here');
```

- روی این لینک کلیک کنید و محتوای ایجاد شده را کپی نمایید.
- کدی که کپی کرده اید را در فایل کانفیگ وردپرس جایگزین کد های قبلی کنید و تنظیمات را ذخیره نمایید.

۱۰ - پلاگین های اجرایPHP

به خودتان لطف کنید و اگر این پلاگین ها را واقعا نیاز ندارید آنها را هرگز نصب نکنید. خوب حتما میپرسید چرا. دست کم به دو دلیل. اول اینکه ذخیره ی کد پی اچ پی در پایگاه داده اصلا جالب نیست. وقتی شما کد پی اچ پی را در یک پلاگین مخصوص اجرای PHP در وردپرس ذخیره میکنید، وقتی که قرار است این کد اجرا شود، ابتدا باید یک بار از

دیتابیس خوانده شود و بعد به عنوان داده های زبان PHP تفسیر شود. این یک دلیل. و دلیل دیگر اینکه اجازه بدهید بنده پسورد وبسایت شما را پیدا کنم تا با همین پلاگین دوست داشتنی، وبسایت دوست داشتنی تر شما را تبدیل به یک بد افزار کنم. بعد هم از بلاک شدن سایتتان توسط گوگل و ... لذت ببرید. پس در این زمینه دقت به خرج دهید.

HTML-۱۱ را در نظرات غیر فعال کنید.

یکی از هکر های عزیز همین چند وقت پیش دوره افتاده بود و با همین HTML های مثلا دوست داشتنی و از طریق ارسال نظر در وردپرس دیگران را هک میکرد و دیگران مات و مبهوت میمانند که چه شد که اینطوری شد! بله اینطوریا بود که اونطوریا شد! اصلا و اصلا به صلاح نیست که شما به کاربرانتان اجازه ارسال HTML در نظرات بدهید. به طور پیشفرض اگر یک کاربر از تگ های HTML در نظرش استفاده کند، قالب شما آن بخش از نظر را که دارای کد HTML هست با همین زبان تفسیر کرده و نتیجه ی آن را به نمایش میگذارید اما اگر شما از قبل استفاده از HTML را در نظرات ممنوع کرده باشید، هر گار کاربر یکی از تگ های این زبان را در نظرش به کار ببرد، نتیجه به جای اینکه تفسیر شود، به عنوان تکست ساده به نمایش در خواهد آمد. خوب پس همین حالا دست به کار شوید به شیوه ی زیر استفاده از HTML را در نظرات وبسایتتان ممنوع کنید:

- در بخش مدیریت وردپرس از منوی "نمایش" زیر منوی "ویرایشگر" را انتخاب کنید تا به محل ویرایش فایل های قالبتان هدایت شوید.
- فایل functions.php را برای ویرایش انتخاب نمایید و کد زیر را به آن اضافه کنید :

```
// This will occur when the comment is posted
function plc_comment_post( $incoming_comment ) {

    // convert everything in a comment to display literally
    $incoming_comment['comment_content'] =
htmlspecialchars($incoming_comment['comment_content']);

    // the one exception is single quotes, which cannot be #039; because WordPress marks it as spam
    $incoming_comment['comment_content'] = str_replace( "'", '&apos;',
$incoming_comment['comment_content'] );

    return( $incoming_comment );
}

// This will occur before a comment is displayed
function plc_comment_display( $comment_to_display ) {

    // Put the single quotes back in
    $comment_to_display = str_replace( '&apos;', "'", $comment_to_display );

    return $comment_to_display;
}

add_filter( 'preprocess_comment', 'plc_comment_post', '', 1 );
add_filter( 'comment_text', 'plc_comment_display', '', 1 );
add_filter( 'comment_text_rss', 'plc_comment_display', '', 1 );
add_filter( 'comment_excerpt', 'plc_comment_display', '', 1 );
// This stops WordPress from trying to automatically make hyperlinks on text:
remove_filter( 'comment_text', 'make_clickable', 9 );
```

- تغییرات را در فایل مورد نظر ذخیره کنید.

خوب حالا هر کسی که در نظرات شما HTML ارسال کند، نتیجه اش نمایش کد های درهم و برهم HTML خواهد بود و نه اجرا و تفسیر این کد ها.

این مقاله هنوز هم ادامه دارد و تا به اینجای کار هنوز هم سایت وردپرسی شما دارای حداکثر امنیت نیست. درواقع بخش مهمی از این مقاله را نگه داشته ام تا در قسمت دوم راجع به آن با شما صحبت کنم. دلیلش هم این است که در قسمت آینده ابزاری مناسب برای اعمال سایر تنظیمات امنیتی به شما معرفی خواهم کرد که میتواند در هر مرحله با چند کلیک ساده کار شما را راه بیاندازد. بنابراین این قسمت از آموزش را به خوبی روی سایتتان اجرا کنید و منتظر قسمت دوم باشید تا در قسمت آینده با کمک هم به هدف خود که امن کردن سایت وردپرسیمان است برسیم.

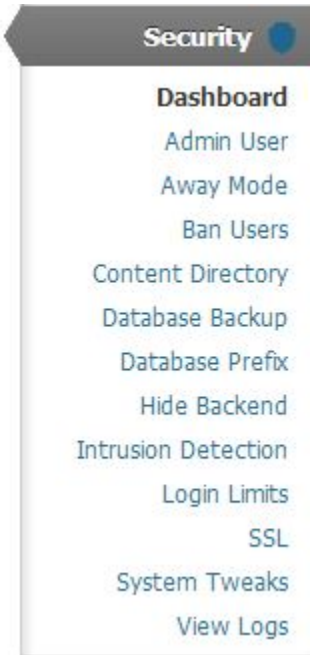
بخش دوم :

همانطور که قول داده بودم، در این بخش به شما یک پلاگین بسیار قوی و کاربردی معرفی میکنیم که ادامه ی این مطلب را با استفاده از این پلاگین امنیتی عالی با هم دنبال کنیم.

Better WP Security

Better WP Security نام افزونه ای است که قرار است ادامه ی کارمان را با آن پیگیری کنیم. این افزونه را میتوانید از **این آدرس** دریافت کرده و بر روی وردپرس خود نصب کنید. خوشبختانه این افزونه از جمله افزونه هایی است که آپدیت های منظمی دارد و به همین جهت همیشه با آخرین ورژن وردپرس سازگار است. توجه داشته باشید که برای ادامه ی آموزش حتما و حتما به این افزونه نیاز دارید. بنابراین پیش از خواندن ادامه ی مطلب آن را بر روی وردپرس خود نصب کنید.

وقتی این افزونه را نصب کنید، در سایدبار مدیریت وردپرس شما یک منوی جدید با عنوان Security مشاهده خواهد شد. برای دسترسی به تنظیمات این پلاگین کافی است وارد این منو شوید. (مطابق تصویر زیر)



این پلاگین در ابتدای نصب به شما توصیه های بسیاری جهت بهبود امنیتتان خواهد کرد اما ما فعلا به آن مسائل کاری نداریم و میخواهیم مسیر خودمان را دنبال کنیم. بنابراین مراحل را به شکل زیر با من دنبال کنید.

ادمین را از دید دشمن دور کنید!

وقتی از ساده ترین افراد یا حتی حرفه ای ترین افراد بپرسید که فلان سایت با چه CMS ای ساخته شده، قبل از اینکه خود را درگیر مسائل پیچیده کنند، ساده ترین احتمال را در نظر میگیرند و شروع میکنند به تایپ کردن آدرس متداول ادمین در CMS های مختلف در انتهای نام سایت مورد نظر. مثلا www.domain.com/administrator برای سایت های راه اندازی شده با جوملا یا www.domain.com/wp-admin برای سایت های راه اندازی شده با

وردپرس. هر کدام از این درخواست ها که به نتیجه برسد، میفهمند که این سایت از چه اسکریپتی استفاده میکند. (مثال بود ها! بعدا به اینجا گیر ندهید) خوب خودتان بگویید. مسخره نیست که هر کسی از راه برسد بتواند آدرس ادمین شما را پیدا کند؟ اصلا حتی اگر روی فولدرش پسورد هم گذاشته باشید، یا از سخت ترین رمز عبور و نام کاربری دنیا استفاده کنید و یا حتی ارورهای لاگین را غیرفعال کرده باشید که هکر بیچاره (!) نفهمد یوزر را اشتباه وارد میکند یا رمز عبور را! قبول کنید در دسترس بودن ادمین توسط همه، خیلی خیلی بی احتیاطی است.
با استفاده از پلاگینی که همین الان نصب کردیم میتوانیم کاری کنیم که از این به بعد بخش ادمین شما فقط با یک URLعجیب و غریب باز شود. برای این کار به شکل زیر عمل کنید:

- در پلاگین به بخش Hide بروید.
- Admin Slug را به هر عبارتی که مایلید برای ورود به بخش مدیریت استفاده کنید تغییر دهید.
- اگر امکان ثبت نام در بلاگ شما فعال نیست، Login Slugرا معادل Admin Slug تعریف کنید و اگر نه به آن مقدار متفاوتی اختصاص دهید.
- گزینه ی Generate New Secret Key را فعال کنید.
- تغییرات را ذخیره کنید.

از این بعد باید با آدرس جدیدی که تعریف کرده اید وارد ادمین شوید. وارد کردن آدرس قبلی wp-admin در مرورگر به خطای ۴۰۴ خواهد انجامید. (و قیافه ی خیلی ها تماشایی خواهد شد)

نکته ی مهم : آدرس ادمین را گم نکنید و از آن مهم تر اینکه Secret Key خود را حتما در جایی امن یادداشت کنید Secret Key .کلیدی است که لازم است به صفحه ی ورود به ادمین وردپرس پاس داده شود تا شما اجازه داشته باشید آدرس wp-admin را مورد استفاده قرار دهید. شاید هرگز به این کلید نیاز پیدا نکنید ولی شاید یک روز پلاگین یا قالبی نصب کنید که کمی بد قلق (؟) باشد و شما را به دردسر بیاندازد. آن موقع میتوانید خودتان به صورت دستی لینک ورود صحیح را با استفاده از این کلید تولید کرده و مورد استفاده قرار دهید.
در بلاگ هایی که امکان ثبت نام در آنها فعال است، میتوانید آدرس صفحه ی لاگین و ثبت نام یوزر ها را نیز به همین شکل تغییر دهید. به طور کلی استفاده از امکان عضویت در بلاگ های عادی اصلا توصیه نمیشود مگر اینکه بخواهید وردپرس خود را تبدیل به شبکه ی اجتماعی، سایت بازی، فروشگاه و یا فروم کنید.

مجرمان را دستگیر کنید

بدیهی است که اگر یک نفر در سایت شما در حال گردش باشد و مثلا ۱۰ بار پشت سر هم به صفحه ی ۴۰۴ برخورد کند یک جای کارش میلنگد (فرض میکنیم سایت شما در حالت طبیعی به سر ببرد) میپرسید چرا؟ پاسخ بسیار واضح است. بخاطر اینکه ۱۰ بار ۴۰۴ پشت سر هم یعنی اینکه مثلا من نشسته ام دارم با آدرس بلا گ شما انقدر بازی میکنم ت ادمینتان را پیدا کنم و سعی کنم وارد شوم. خوب حالا چکار کنیم که اگر یکی این کار را کرد سریع متوجه شویم و جلوی خرابکاری اش را بگیریم؟ برای این کار به صورت زیر عمل کنید:

- در بخش تنظیمات پلاگین به تب Detect بروید.
- Enable 404 Detection را فعال کنید.
- Email 404 Notification را فعال کنید.
- ایمیلی که مایلید در صورت بروز چنین مسئله ای از طریق آن از موضوع آگاهی پیدا کنید را وارد کنید.
- در بخش White List 404 میتوانید اگر آی پی ثابت دارید، آی پی خود یا آی پی های بات های گوگل را وارد کنید تا

در صورت برخورد پشت سر هم به ۴۰۴ بن نشوند.

- تغییرات را ذخیره کنید.

تنظیمات پیش فرض این بخش برای یک سایت عادی کاملا مناسب هستند. مثلا در بخش Check Period گفته شده که خطاهای ۴۰۴ فقط در۵ دقیقه ی گذشته مورد بررسی قرار بگیرند و در بخش Error Treshold گفته شده که کاربر پس از برخورد به ۲۰ صفحه ی ۴۰۴ باید بن شود. هر بار بن شدن کاربر ۱۵ دقیقه ادامه خواهد داشت و در صورتی که ۳ بار این مسئله تکرار شود، آی پی خاطی برای همیشه از دسترسی به سایت شما محروم خواهد شد.

چرا File Change Detection را فعال نکردیم؟

بخاطر اینکه در قسمت قبلی مقاله جای فایل کانفیگ را عوض کردیم و حالا که بالا تر از دایرکتوری نصب وردپرس ما قرار گرفته دیگر با این پلاگین قابل مانیتور نیست. اگر هم بخواهیم htaccess ها را مانیتور کنیم باید به پلاگین بگوییم که مثلا دایرکتوری اصلی وردپرسمان را مانیتور کند. همینجاست که همه چیز دردسر ساز میشود. از فردا میبینید که اگر یک عکس هم آپلود کنید این پلاگین به شما میگوید که تغییری در فلان فولدر ایجاد شده. در بلاگی که از همه جهت امن شده باشد این گزینه خیلی هم مهم نیست ولی اگر حوصله ی مرتب کردن ایمیلتان را دارید حتما از این امکان نهایت استفاده را بکنید.

بکاپ، بکاپ، بکاپ

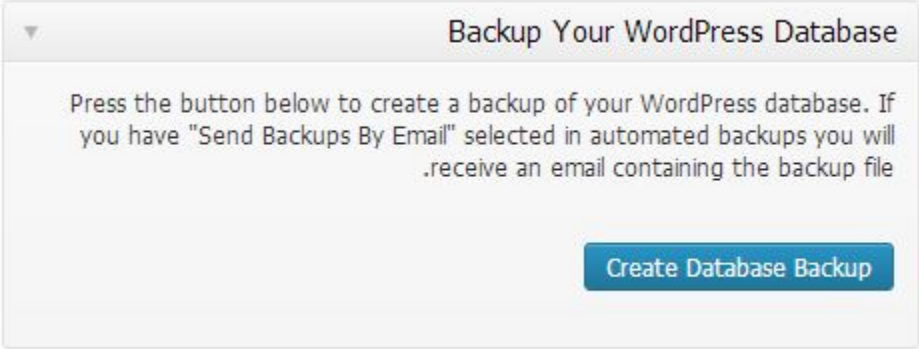
هیچ کس از ۱ دقیقه ی دیگر خبر ندارد. همیشه باید طوری زندگی کنیم که بعدا حسرت گذشته را نخوریم. فول بکاپ که هرگز فراموش نشود، اما اگر سلطان اینترنت پر سرعت نیستید (!) بهتر است همیشه یک بکاپ از دیتابیس خود داشته باشید. برای اکثر افرادی که به تولید محتوا میپردازند، داشتن یک نسخه ی پشتیبان از نوشته هایشان واقعا نعمت است. درست است که در این حالت تصاویرتان و به طور کلی فایل های چند رسانه ای شما بین زمین و هوا میمانند ولی خوب این را که درست کنید میتوانید برای بخش های دیگر هم یک فکری بکنید. بنابراین بیایید این پلاگین را برای ایجاد بکاپ های منظم از دیتابیس تنظیم کنیم:

- در تنظیمات پلاگین به تب Backup بروید.
- گزینه ی Enable Scheduled Backups را فعال کنید.
- فاصله ی بین بکاپها را تعیین کنید. بر چه اساس؟ مثلا من اینجا شاید ماهی یک بار یک مطلب بنویسم. پس همین مقدار پیش فرض ۳ روز یک بار را نگه میدارم. اما شاید شما روزی ۲۰ مطلب در بلاگتان منتشر کنید. اینجاست که لازم است فاصله را از روز به ساعت تغییر دهید و مثلا فاصله ی بکاپ ها را بر روی ۳ ساعت یک بار قرار دهید.
- گزینه ی send backups by email خیلی مهم است، فعال کردن این گزینه فراموشتان نشود. یک وقت دیدید مثلا هاستتان در آمریکا بود و خدا تصمیم گرفت طوفانی بفرستد و دیتاسنتری که سرور شما در آن قرار دارد را با خاک یکسان کند . بگذارید یک بکاپ در یک نقطه ی دیگر دنیا به ایمیلتان اتچ شده باشد!
- آدرس ایمیلی که مایلید بکاپ ها به آن ارسال شوند را وارد کنید.
- در آخر تعیین کنید چه تعداد از بکاپ ها لازم است روی هاست نگه داشته شوند. باز هم این به همان بحثی بر میگردد که چند وقت یک بار آپدیت میکنید.
- تنظیمات را ذخیره کنید.

یادتونه؟ [کاملا با دقت و با مسئولیت خودتان انجام دهید]

یادتان هست که در قسمت اول مقاله گفتیم که اگر در ابتدای کار پیشوند جداول دیتابیس خود را عوض نکرده اید هنوز هم دیر نشده؟ بله، بله، اجازه بدهید حالا پیشوند جداول را عوض کنیم:

- همانطور که هنوز در بخش Backup قرار دارید، با کلیک بر روی دکمه ی Create Database Backup یک نسخه ی پشتیبان از پایگاه داده ی خود تهیه کنید.



خوب حالا در تنظیمات پلاگین به بخش Prefix بروید و بر روی دکمه ی Change Database Table Prefix کلیک کنید. با این کار پیشوند جداول پایگاه داده ی شما همگی با مقداری رندم جایگزین میشوند. بعد از انجام این کار اگر وردپرستان بالا نیامد شکه نشوید. خونسرد باشید، به فایل کانفیگ وردپرستان مراجعه کنید و در آن مقدار $table_prefix را به مقدار جدید پیشوند جداولتان تغییر دهید. اگر وردپرس بالا نیامد از کجا بدانید این مقدار چه بوده است؟ خوب از phpMyAdmin بپرسید!

امکان ویرایش فایل را در بخش مدیریت غیر فعال کنید

درست است که تا اینجا برای امن کردن وردپرس عزیزمان خیلی تلاش کردیم اما فرض کنید یک اتفاقی این وسط افتاد یا مثلا بخشی از کار را فراموش کرده بودید و یک شخص فرصت طلب به بخش مدیریت وردپرس شما دسترسی پیدا کرد. وردپرس به صورت پیش فرض به شما اجازه میدهد که کد های قالب و پلاگین هایتان را از طریق بخش مدیریت ویرایش کرده و در آنها تغییر ایجاد کنید. در این بخش تصمیم داریم این امکان را غیر فعال کنیم تا اگر یک هکر بد و بی ادب سراغمان آمد، دست کم راهش به هاستمان باز نشود و دستش برای انجام خرابکاری کمی بسته تر باشد. برای اینکه ویرایش فایل را در بخش مدیریت وردپرس غیر فعال کنیم به صورت زیر عمل میکنیم:

- در تنظیمات پلاگین به بخش Tweaks بروید.
- در پایین صفحه گزینه ی Turn off file editor in WordPress Back-end را فعال کرده و تنظیمات را ذخیره کنید.
- توجه داشته باشید که اگر از قبل سطح دسترسی فایل wp-config را ۴۴۴ کرده باشید، اینجا به مشکل برخورد خواهید کرد.
- یک توجه دیگر هم داشته باشید که اگر این تنظیم جدید را اعمال کنید و بعد فراموش کنید که در انتهای کار سطح دسترسی فایل wp-config را به ۴۴۴ برگردانید، مثل این میماند که هیچ کاری نکرده اید. چون مثلا من وارد بخش مدیریت شما میشوم، میبینم ادیتوری وجود ندارد، به تنظیمات پلاگین مراجعه میکنم و آن را دوباره فعال میکنم! دستم هم درد نکند! شما هم خسته نباشید!

فعال کردن گزینه ای که در بالا از آن صحبت کردیم، هیچ کار جادویی ای انجام نمیدهد. تنها کاری که میکند به سادگی کد زیر را به فایل wp-config شما اضافه میکند :

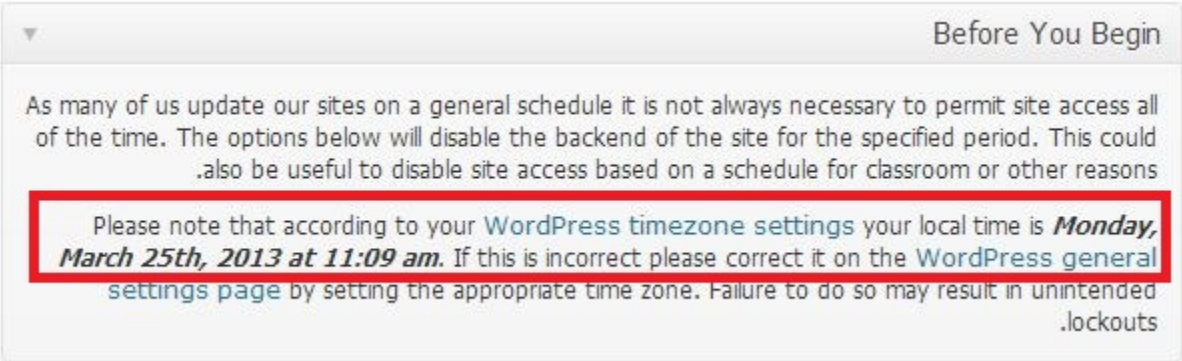
```
define('DISALLOW_FILE_EDIT', true);
```

ولی خوب همیشه استفاده از پلاگین ساده تر است. نه؟

تعطیل کنید! بعد پی کارتان بروید!

جدا عرض میکنم! تعطیل کنید بعد پی کارتان بروید. فرض کنیم شما ۵ روز اول عید را مسافرت بوده اید. تمایلی هم به دسترسی به بلاگتان نداشته اید. یا اصلا جایی بودید که از اینترنت خبری نبوده. (خدا رو هزار مرتبه شکر هرکی اینو بخونه زبونش فارسیه وگرنه تا یک قرن بعد به جمله ی "از اینترنت خبری نبوده" میخندیدن! ایهاالناس ما همه جا یه شعبه مک دونالد نداریم!) خوب وقتی قرار نیست به ادمین وردپرستان دسترسی داشته باشید، اصلا برای چه آن را باز میگذارید؟ منطق حکم میکند که دسترسی به بخش ادمین در این ۵ روز که مسافرت هستید غیر فعال باشد. یا اصلا فرض کنیم که شما سه روز در هفته در بین ساعات ۸ صبح تا ۳ بعد از ظهر کلاس دارید یا مثلا سر کار میروید یا هر چیز دیگر .... (شغل رویایی، سه روز در هفته، ۸ صبح تا ۳ بعد از ظهر) اینجا هم عقل حکم میکند که دسترسی به مدیریت را در این بازه های زمانی غیر فعال کنید. چطور این کار را انجام دهیم؟

- در تنظیمات پلاگین به بخش Away مراجعه کنید.
- پیش از هر چیز توجه کنید که حتما ساعت تنظیم شده در وردپرس شما با ساعت کنونی کشور هماهنگ باشد که بعدا دچار مشکل نشوید. پلاگین در بخش Away ساعت کنونی وردپرستان را به شما نمایش میدهد:



- گزینه ی Enable Away Mode را فعال کنید.
- از بین گزینه های One Time و Daily یکی را بر اساس نیاز خود انتخاب نمایید. One Time برای مواقعی است که مثلا فقط میخواهید از روز اول تا ۵ام عید، دسترسی به مدیریت غیر فعال شود. Daily برای شرایطی است که میخواهید هر روز طی ساعات خاصی، مثلا در هنگام شب، دسترسی به مدیریت امکان پذیر نباشد.
- در صورتی که گزینه ی OneTime را انتخاب کرده اید لازم است تاریخ شروع و پایان را تنظیم نمایید.
- در صورتی که گزینه ی Daily را انتخاب کرده اید لازم است ساعت شروع و پایان را تنظیم نمایید.
- در پایان تغییرات را ذخیره کنید.

من شخصا عملکرد این بخش را تست نکرده ام. لطفا در استفاده ازاین بخش نهایت دقت را به عمل آورید.

کارهای کوچک، نتایج بزرگ....

اگر از ابتدای مطلب با من همراه بوده اید، حتما یادتان هست که در ابتدای نصب پلاگین گفتم که این پلاگین پیشنهاد های زیادی برای بهبود امنیت به شما ارائه خواهد کرد. خود حالا اجازه بدهید کمی به این پیشنهاد های خورده ریز رسیدگی کنیم که تاثیرات واقعا خوبی هم در بالا بردن سطح امنیت وبلاگتان خواهند داشت. در تنظیمات پلاگین به بخش Tweaks مراجعه کنید و مراحل را با من پی گیری کنید. توجه داشته باشید که فقط گزینه های مهم را بررسی میکنیم و به تمام گزینه ها کاری نداریم:

Server Tweaks

Protect Files: فعال کردن این گزینه، دسترسی عمومی به فایل های readme.php, wp-config.php, readme.html, install.php, .htaccessو در نهایت wp-includes را غیر ممکن میسازد. میتوانید آن را فعال کنید اما به وضوح در زیرش نوشته شده که این کار ممکن است با بعضی پلاگین ها تداخل ایجاد کند.

Disable Directory Browsing : فرض کنید یک دایرکتوری دارید که درونش هیچ فایل ایندکسی وجود ندارد و امکان مرور فایلهای درون آن نیز غیر فعال نشده است. نتیجه میشود اینکه مثلا یکی بیاید کل فایل های موجود در پوشه ای که عکس هایتان را در آن آپلود کرده اید بدزدد. یا مثلا اگر بکاپی از چیزی، یک جایی نگه داشته باشید به دست دیگران بیفتد و ... حالا اگر این گزینه را فعال کنید، یک دایرکتوری اگر ایندکسی نداشته باشد، محتوایش را در اختیار بازدید کننده قرار نمیدهد. در کنترل پنل دایرکت ادمین این امکان به صورت پیشفرض فعال است. یعنی دایرکتوری ای که ایندکس ندارد، در صورت فراخوانی، خطای ۴۰۳ بر میگرداند ولی در cPanel خدا به خیر کند! بنابراین استفاده از این گزینه برای سی پنلی ها توصیه میشود.

Filter Request Methodو Filter Suspicious Query Strings : دو گزینه ی خیلی دوست داشتنی. اولی باعث میشود که وردپرس شما درخواست هایی که در آنها از متد هایTrack ، Deleteو یا Trace استفاده شده باشد را نپذیرد و دومی اگر یک نفر یک استرینگ بلند و بالا (به مقاصد پلید) به سایت شما بفرستد، حالش را درون قوطی خواهد کرد! این دو گزینه در حالت عادی و با پلاگین های رایج وردپرس تداخلی ندارند اما [الان که خوب فکر میکنم میبینم که] اگر مطالبتان را مثلا در فیس بوک به اشتراک بگذارند و بعد یکی بخواهد از لینک به اشتراک گذاشته شده در فیس بوک به بلاگ شما سر بزند، احتمالا با صفحه ی سفید مواجه خواهد شد و نکته ی دیگر اینکه شاید مجبور باشید که تنظیمات feedburner تان را نیز بر همین اساس کمی تغییر دهید. به هر حال اولویت هایتان را بسنجید و بر اساس نیازتان تصمیم بگیرید که میخواهید این گزینه ها را فعال کنید یا نه.

Header Tweaks

Remove WordPress Generator Meta Tag : وردپرس خیلی علاقه دارد به همه بگوید که این سایت با فلان ورژن بنده و با فلان مشخصات ساخته شده است و طبیعتا این برای خیلی از افراد میتواند راه ورود به وبلاگ شما را هموار کند. این گزینه را فعال کنید.

Remove EditURI Header : در این لحظه که دارید این مطلب را میخوانید فکر نمیکنم خطر امنیتی گذارش شده ی مهلکی در رابطه با استفاده از XML-RPC در وردپرس وجود داشته باشد ولی اگر شما کارتان این است که مثل بچه های خوب، برای نوشتن پست وارد ادمین وردپرستان میشوید و کاری به جای دیگری ندارید، بنابراین هیچ نیازی هم نیست که وردپرستان اطلاعات لازم برای XML-RPC را در هدرش منتشر کند.این گزینه را هم فعال کنید.

اگر از وردپرس multi-site استفاده نمیکنید که هیچ. اما اگر در حالت multi-site به سر میبرید، در بخش **Dashboard Tweaks** میتوانید تعیین کنید که آپدیت ها به یوزرهای دیگری که از شما سایت دارند ولی قادر به آپدیت پلاگینها نیستند، نشان داده نشود.

بعد هم **Strong Password Tweaks** را داریم که به شما اجازه میدهد تعیین کنید که مثلا پایین ترین سطح کاربری هم که در سایت شما عضو میشود میبایست از رمزعبور های پیچیده و قابل قبول برای ثبت نام استفاده کند و از این حرف ها!

Other Tweaks

Remove WordPress Login Error Messages : بله بله. با فعال کردن این گزینه، اگر کسی از ترکیب غلط رمز عبور و نام کاربری استفاده کند، وردپرس مثل بچه های ۲ ساله ی ساده لوح به او نخواهد گفت که مثلا هکر جونم، نام کاربریت درسته ولی رمزت نه....

Display Random Version Number to All non-Administrative Users : فعال کردن این گزینه که خیلی هم مفید است، باعث میشود که وردپرس شما هرکجا که باید ورژن را به نحوی به نمایش بگذارد از اطلاعات رندوم استفاده کند. (البته نه برای ادمین) مثلا امروز به یکی میگوید من ورژن ۲,۱ هستم! فردا میگوید ۳,۵ میباشم!

Prevent Long URL Strings : این گزینه از لحاظ امنیتی گزینه ی بسیار خوبی است و باعث میشود که هکر ها نتوانند فرصتی برای حملات SQL Injection و سایر حملاتی که از URL انجام پذیر هستند پیدا کنند. اما استفاده از این گزینه بی دردسر هم نیست. بعد از استفاده از این گزینه متوجه خواهید شد که در دسته بندی های شما هر پیوند یکتایی که از حد معینی طولانی تر باشد به صفحه ی سفید منتهی خواهد شد. بنابراین با دقت و بر اساس نیاز این گزینه استفاده نمایید.

گزینه های دیگری هم در این بخش بودند که یا خیلی مهم نبودند و یا قبلا آنها را بررسی کرده بودیم. به هر حال همیشه یادتان باشد که خودتان خوب گشت و گزار کنید و فقط به مطالبی که خوانده اید اکتفا نکنید.

این را هم بگویم که به سادگی از این افزونه دست نکشید. مثلا من هیچ صحبتی درباره ی بخش Ban نکردم در حالی که این بخش هم تا حد بسیار زیادی در بالا بردن امنیت وبلاگتان به شما کمک خواهد کرد. یا مثلا بخش Login و بسیاری از مسائل دیگر. اما دست کم الان مطمئنم که ماهی گیری را یاد گرفته اید. بنابراین نوبت شماست که با ابزاری که در اختیارتان گذاشته شده، انقدر تمرین کنید که به یک ماهیگیر حرفه ای تبدیل شوید.
خوب این بخش از مقاله هم به پایان رسید و حرفهایی که در این رابطه برای گفتن به شما عزیزان داشتم تمام شد. در طول نوشتن این مقاله دو مشکل که مدتی بود ذهنم را مشغول کرده بود ولی چون مدت طولانی بود به سراغ این پلاگین نیامده بودم، پاسخش از ذهنم دور مانده بود، برایم حل شدند. بنابراین نوشتن این مقاله دست کم برای خودم خیلی مفید بود و خوشحالم که آن را نوشتم.

کمی خودمانی تر : [ترول باز که هستید؟] یاد اون ترولی افتادم که مادره میره مسافرت به به پسرش میگه ۱۰۰ دلار برای غذا توی اتاقت گذاشتم که اگر اتاقت رو مرتب کنی پیداش میکنی. خدا رو شکر من ۱۰۰ دلاریمو پیدا کردم!

همین. امیدوارم که این مقاله برای شما هم سودمند بوده باشد و هکر ها را حسابی از خود ناامید کرده باشید. اگر شما هم روشی برای امنیت بیشتر به ذهنتان میرسد که در این مقاله به آن اشاره ای نشده، حتما در بخش نظرات آن را با دیگران به اشتراک بگذارید. اگر هم ایرادی در نوشته دیده میشود، اولا به بزرگواری خود ببخشید و دوما به آن اشاره کنید تا تصحیح شود.

امیدوارم از این آموزش لذت برده باشید

Blog.vandahost.net