

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

بهروز منصوری

وب سایت : <http://bmansoori.ir>

ایمیل : mr.mansoori@yahoo.com

اینستاگرام : Behrouz_mansoori

تاریخچه وردپرس

وردپرس (wordpress) یک سیستم مدیریت محتوا برای سایتها و وبلاگ هاست برای محتوای آموزشی، تجاری، علمی و... همچنین قابلیت ایجاد سایت‌های اجتماعی با افزونه‌های (plugin) قدرتمند همچون buddypress. ایجاد انجمن با افزونه bbpress، ایجاد فروشگاه با افزونه Woocommerce و غیره را داراست.

وردپرس با زبان برنامه نویسی پی اچ پی (php) نوشته شده و توسط مای‌اس‌کیوال (mysql) پشتیبانی می‌شود. این سیستم کاملاً رایگان و متن باز (open source) است.

مت مولنوگ پایه‌گذار وردپرس است، نرم‌افزار کدبازی که به طور گسترده از سوی وبلاگ‌نویسان برای نوشتن وبلاگ مورد استفاده قرار می‌گیرد.

«مت چارلز مولنوگ»، در تاریخ ۱۱ ژانویه ۱۹۸۴ در هوستون تگزاس به دنیا آمد و در حال حاضر در سانفرانسیسکو کالیفرنیا زندگی می‌کند.

مولنوگ در ابتدا مدتی به مطالعه ساز ساکسیفون پرداخت و در آموزشگاه بازیگری و هنرهای نمایشی حضور می‌یافت.

اولین سیستمی که مولنوگ برای وبلاگ‌نویسی از آن استفاده کرد، سیستم b2/cafelog بود. او برای نخستین بار برای انتشار عکس‌هایی که در سفر به واشنگتن گرفته بود از این سیستم استفاده کرد. همین تجربه باعث شد که به این فکر بیفتد که خود، برای وبلاگ‌نویسی نرم‌افزاری به‌روز و سازگار با استانداردهای وب که نیازهایش را برآورده کند، بنویسد. او در ژانویه ۲۰۰۳، در وبلاگش این مطلب را اعلام کرد.

مولنوگ به سرعت با شخصی به نام «مایک لیتل» تماس گرفت و با کمک هم، این دو شروع به نوشتن وردپرس با استفاده از ۲b کردند. توسعه دهنده اصلی ۲b یعنی Michel Valdrighi هم به زودی به جمع دو نفره آنها اضافه شد.

در مارس ۲۰۰۳ او Global Multimedia Protocols Group را تأسیس کرد که در آن نخستین «میکروفرمت‌ها» نوشته شد.

او در آوریل ۲۰۰۴، سرویس نام‌آشنای Ping-O-Matic را تأسیس کرد که همانگونه که از نام آن برمی‌آید، سرویسی است که با آن می‌شود پینگ کرد و موتورهای جستجویی مانند تکنوراتی را از به‌روز شدن وبلاگ، آگاه کرد. به یاری آن می‌شود، به صورت بسیار ساده سرویس‌های بسیار زیادی از جمله بلاگ‌ولینگ محبوب وبلاگ نویسان ایرانی را پینگ کرد. در حال حاضر Ping-O-Matic روزانه یک میلیون بار پینگ می‌شود.

در می ۲۰۰۴، رقیب وردپرس یعنی موبل تایپ، اعلام کرد که قیمت‌هایش را تغییر داده است. مسئله‌ای که باعث شد هزاران کاربر موبل تایپ به فکر استفاده از نرم‌افزارهای جایگزین بیفتند. وردپرس به خوبی از این فرصت استفاده کرد.

در اکتبر ۲۰۰۴، CNET مولنوگ را استخدام کرد تا در آنجا، روی وردپرس کار کند و در اداره وبلاگ‌ها و رسانه‌های جدید به آنها کمک کند. در دسامبر ۲۰۰۴، مولنوگ bbPress را عرضه کرد، سیستمی که وی در طی چند روز تعطیلات نوشته شده بود.

در فوریه ۲۰۰۵، نسخه ۱٫۵ وردپرس آماده شد که نام Strayhorn را بر آن نهاده بودند. این نسخه ۹۰۰ هزار بار دانلود شد.

در آوریل ۲۰۰۵ شخصی متوجه شد که در سایت WordPress.org، مقاله‌های زیادی به صورت مخفی وجود دارد که با تکنیک cloaking نوشته شده‌اند. در cloaking دارنده یک سایت، کاری می‌کند که نسخه‌ای از سایت که به عنکبوت‌های جستجو عرضه می‌شود متفاوت از چیزی باشد که به بازدیدکنندگان عادی نشان داده می‌شود. مولنوک مجبور شد که مطلب را بپذیرد و همه مقالات را حذف کند.

مولنوک در اکتبر ۲۰۰۵ از CNET جدا شد. چند روز بعد او Akismet را معرفی کرد، سرویسی که جلوی کامنت‌ها و ترک‌بک‌های اسپم را می‌گیرد

در نوامبر ۲۰۰۵، شرکت در پروژه وردپرس از حالت دعوتنامه‌ای درآمد و مشارکت در آن برای همه آزاد شد.

در دسامبر ۲۰۰۵، او Automattic را معرفی کرد، سرویسی که خدمات میزبانی وبلاگ ارائه می‌دهد و نرم‌افزارهای ضد اسپم می‌سازد. اکنون، بر اساس آمار Comscore، سایت Automattic، ماهانه ۱۰۰ میلیون بازدیدکننده دارد و در میان ۲۵ سایت برتر جهان قرار دارد.

در مارس ۲۰۰۷، مجله معتبر PC World، مولنوک را به عنوان یکی از ۵۰ فرد مهم در اینترنت برگزید و در رده شانزدهم قرار داد.

وردپرس فارسی

در فروردین 1384 افزونه تاریخ شمسی در وردپرس انتشار یافت. تا پایان خرداد ماه همان سال نسخه دوم آن افزونه نیز منتشر شد و پروژه ای به نام وردپرس فارسی رسماً آغاز به کار نمود. از فروردین ماه 1386 با اضافه شدن افراد علاقه مند دیگری به این پروژه و انسجام بیشتر فعالیت ها، برنامه ریزی برای راه اندازی وب گاه و ارائه خدمات در زمینه پشتیبانی کاربران انجام

شد. وردپرس انگلیسی معمولا از نوشته های فارسی پشتیبانی نمی کرد و آن ها را به شکل علامت سوال در می آورد. پس بدین ترتیب پروژه وردپرس فارسی آغاز شد. تیم وردپرس فارسی مدعی است که تمامی بسته های ارائه شده توسط این تیم تغییری در اصل و هسته ی نرم افزار وردپرس ایجاد نکرده و همگی به صورت افزودنی هستند. محصولات تولید شده توسط تیم وردپرس فارسی همانند نرم افزار وردپرس بر مبنای مجوز جی پی ال منتشر می شوند و استفاده از آنها آزاد است. فعالیت های تیم وردپرس فارسی بر بومی سازی نرم افزار وردپرس از فعالیت های توسعه دهندگان اصلی نرم افزار وردپرس مستقل است.

نام نسخه های فارسی سازی شده وردپرس

نسخه ۲،۸ وردپرس با نام مستعار کیخسرو پورناظری

نسخه ۲،۹ وردپرس با نام مستعار محمدرضا شجریان

نسخه ۳،۰ وردپرس با نام مستعار بیژن کامکار

نسخه ۳،۱ وردپرس با نام مستعار حسن کسایی

نسخه ۳،۲ وردپرس با نام مستعار شیرمحمد اسپیندار

نسخه ۳،۳ وردپرس با نام مستعار حسین علیزاده

نسخه ۳،۴ وردپرس با نام مستعار علی اکبر شکارچی

نسخه ۳،۵ وردپرس با نام مستعار بهمن رجبی

نسخه ۳،۷،۱ وردپرس با نام مستعار حبیب الله قادر آتشگر

نسخه ۳،۸ وردپرس با نام مستعار طاهر یارویسی

نسخه ۳،۹،۱ وردپرس با نام مستعار منصور نریمان

نسخه ۴،۰ وردپرس با نام مستعار حسن ناهید

نسخه ۴،۱ وردپرس با نام مستعار داریوش پیرنیاکان

نسخه ۴،۲ وردپرس با نام مستعار سیدمحمد موسوی

نسخه ۴،۳ وردپرس با نام مستعار لوریس چکناواریان

نسخه ۴،۴،۱ وردپرس با نام مستعار فرهاد فخرالدینی

نسخه ۴،۴،۲ وردپرس بدون نام مستعار

ویژگی های سیستم مدیریت محتوا (cms) وردپرس

- نصب محلی
- هسته قابل حمل
- پشتیبانی از ساعت محلی
- قابلیت gzip
- سطح دسترسی
- مشخصات کاربران
- پویا بودن و انعطافپذیری بالا
- دارای کتابخانه پلاگین های وردپرس (رایگان)
- دارای کتابخانه قالب های وردپرس (رایگان)

- وردپرس شبکه (جهت راه اندازی سیستم وبلاگدهی با وردپرس)
- فهرست‌های آبخاری و کرکره‌ای
- شخصی‌سازی قالب‌ها، ابزارک‌ها از پنل مدیریت
- ارسال و مدیریت دیدگاه
- ده‌ها مشخصه و ویژگی دیگر

موارد استفاده از وردپرس

- پیاده سازی وبلاگ و یا سایت های شخصی
- پیاده سازی وب سایت های خبری-اطلاع رسانی
- پیاده سازی وب سایت های عکاسی
- پیاده سازی وب سایت های معرفی مشاغل
- پیاده سازی فروشگاه های آنلاین

تصاویر تعدادی از نسخه های قدیمی در وردپرس

WordPress

Post / Edit **Team** Options Categories Template Manage Links My Profile View site Logout

Post / Edit

Title: Category: Post Status: Comments: Pings: Post Password:

Excerpt:

Post:

PingBack the URLs in this post

TrackBack an URL: (Separate multiple URLs with commas.)

وردپرس 0.71 : کاربران می توانند سه حالت پست انتشار (publish) ، پیش نویس (Draft) و خصوصی (Private) داشته باشند.

WordPress

Post Edit Categories Links Users Options Templates My Profile View site Logout (admin)

Create New Post

Title:

Categories: General

Post:

Quicktags: **str** em del ins link img ul ol li b-quote pre more n-page Dict. Close Tags

PingBack the URLs in this post?

TrackBack an URL: (Separate multiple URLs with spaces.)

WordPress bookmarklet

You can drag the following link to your links bar or add it to your bookmarks and when you "Press it" it will open up a popup window with information and a link to the site you're currently browsing so you can make a quick post about it. Try it out:

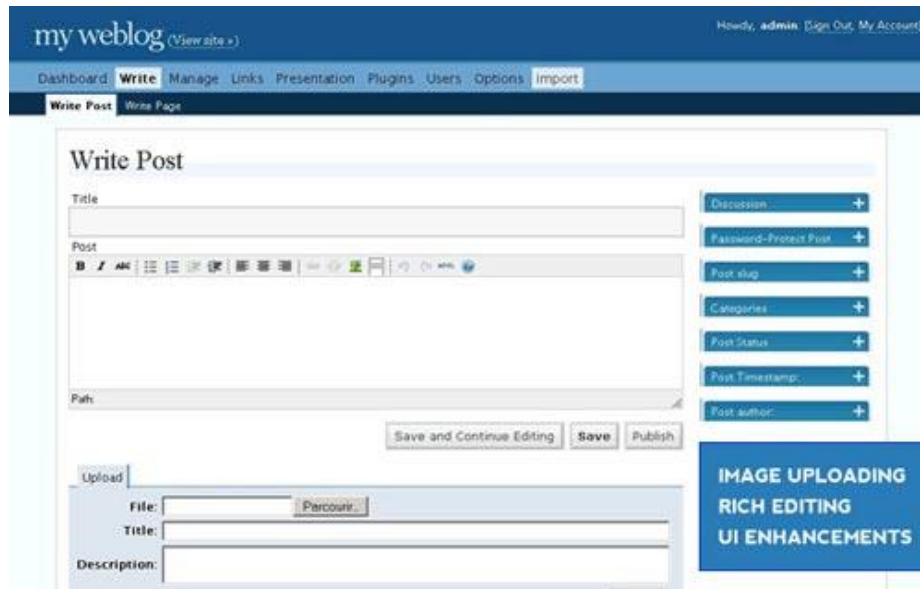
وردپرس 1.0 : اضافه شدن دسته بندی ها



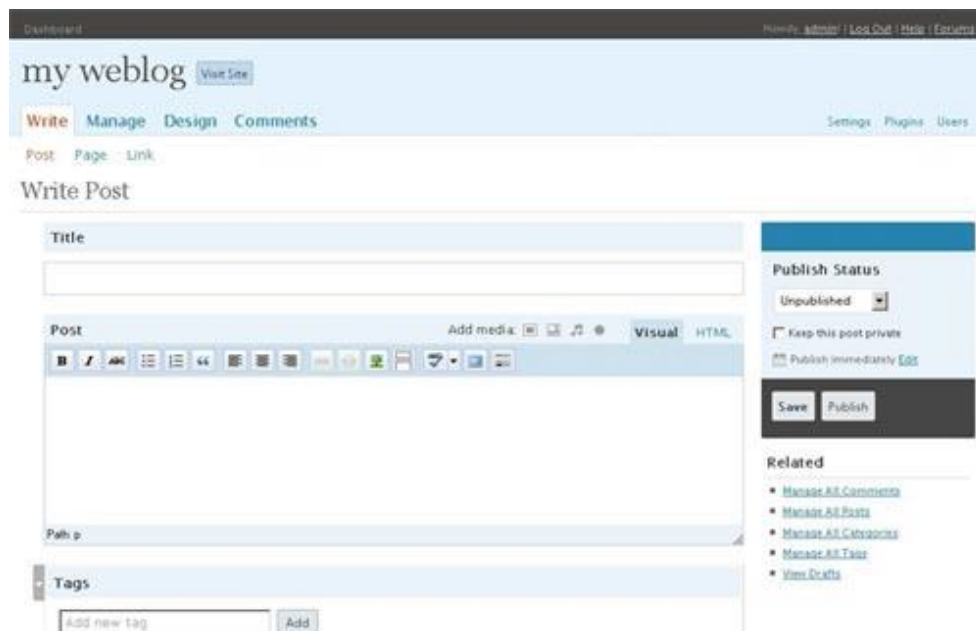
وردپرس 1.2 : اضافه شدن بخش افزونه ها (plugin)



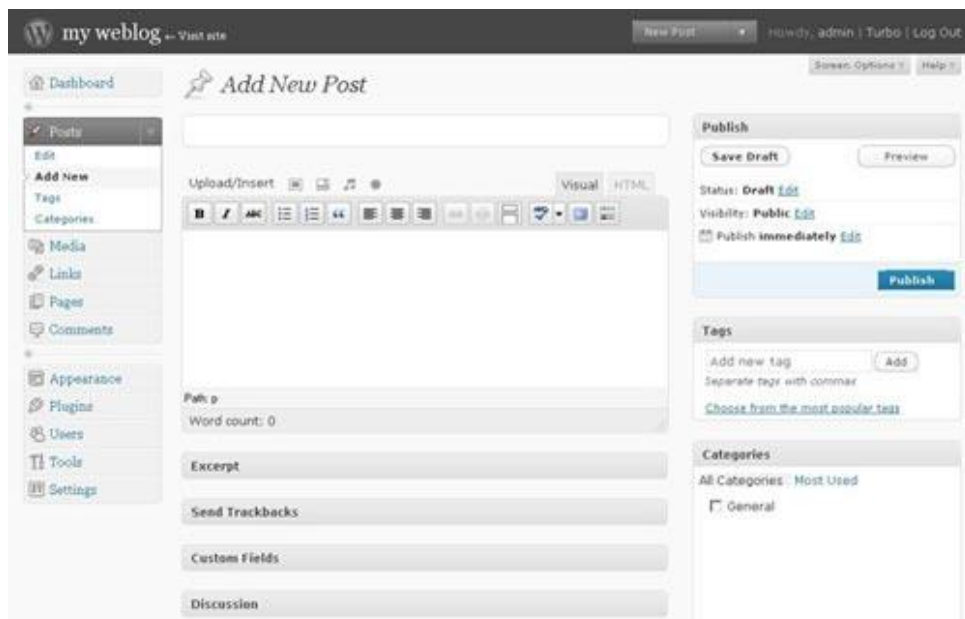
وردپرس 1.5 : اضافه شدن پیش خوان وردپرس



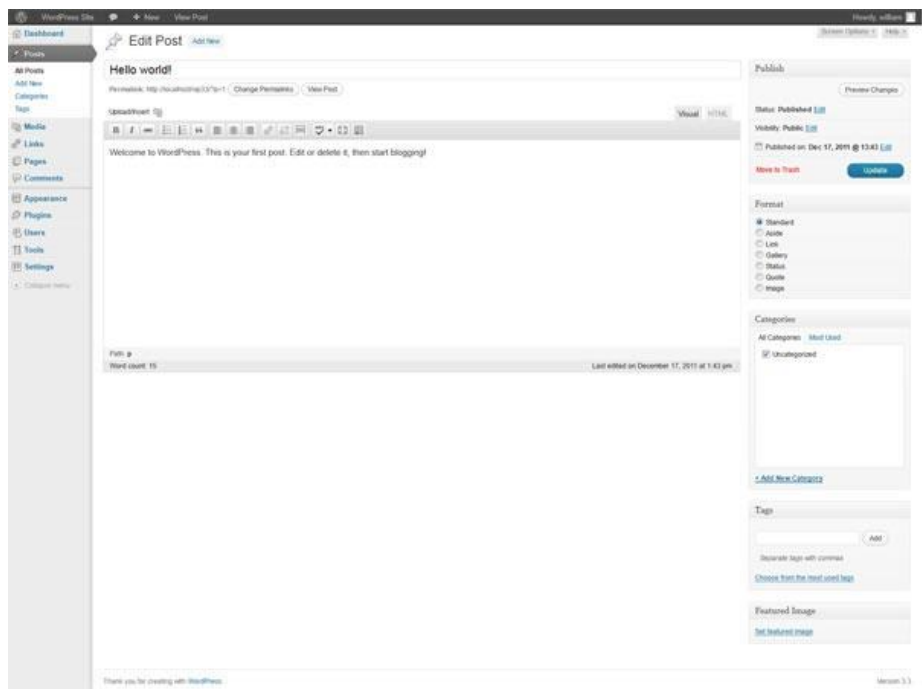
وردپرس 2 : اضافه شدن ویرایشگر پیشرفته پست ها



وردپرس 2.5 : اضافه شدن امکان آپلود تصویر



وردپرس 2.7 : افزایش امکانات در پیشخوان وردپرس



وردپرس 3.2 : اضافه شدن Full Screen Editor



وردپرس 3.5 : افزایش امکانات مدیریت رسانه ها

چرا امنیت وردپرس؟ ضرورت توجه به بحث امنیت در وردپرس

شاید اگر 10 سال پیش در مورد امنیت صحبت می کردیم، موضوعی مشخص و ملموس و مهم به شمار نمی آمد و کسی اهمیت چندانی به این موضوع نمی داد. اما به راستی چه چیزی باعث شده که امنیت به یکباره به یکی از موضوعات مهم این روزهای دنیای فناوری تبدیل شود؟

یکی از علت هایی که باعث مطرح شدن بحث امنیت در بین وب مستران شد، افزایش حملات صورت گرفته به وب سایت ها بود. متأسفانه در سال های اخیر شاهد حملات گسترده سایبری به انواع سایت های شخصی و دولتی در کشورهای مختلف بوده ایم و همان طور که همه شما خوانندگان عزیز می دانید ما زمانی که بیمار می شویم به دکتر مراجعه می کنیم و قبل از مواجهه با بیماری به فکر پیشگیری نیستیم. در بحث سایت هم تا سال های گذشته به همین شکل بود، اما خوشبختانه امروزه هر شخص، شرکت و یا سازمانی که وب سایتی را برای معرفی محصولات و خدمات خود آماده می کند ، در قدم اول به فکر افزایش امنیت و راه های مقابله با نفوذ نفوذگران است. چرا که می داند با گذشت زمان و وسیع تر شدن فعالیت وی در اینترنت، احتمال انجام حملات سایبری علیه وب سایت او افزایش می یابد.

همیشه این سوال مطرح می شود که آیا فعالیت نفوذگران و تلاش آنان برای دسترسی گرفتن به سایت ها و سرورها فقط جنبه منفی دارد یا می تواند کمکی برای وب مستران در جهت آشنایی با حفره های امنیتی (bug) باشد.

افراد زیادی اعتقاد دارند که فعالیت نفوذگران قط جنبه منفی دارد و آنها در پی ضربه زدن به مدیران سایت ها و سروها هستند و عده ای دیگر معتقداند که علاوه بر فعالیت های تخریبی عده از نفوذگران، عده دیگری از آنان با نگرش امنیتی فعالیت می کنند و با گزارش دادن حفره های امنیتی و آگاه ساختن وب مستران در افزایش امنیت سایت و سرور کمک های چشم گیری می کنند.

از نگاه نویسنده به عنوان کسی که بیش از 9 سال در حوزه نفوذ و بحث امنیت فعالیت کرده، حتی اقدام نفوذگران در اصطلاح کلاه مشکی، جهت آسیب زدن به سایت نیز می تواند تبدیل به فرصتی برای وب مستران باشد. چرا که همیشه نفوذگران یک قدم از امنیت کاران جلوتر هستند. همیشه ابتدا یک حفره امنیتی توسط نفوذگران کشف می شود و سپس امنیت کاران راهی برای برطرف کردن آن مشکل پیدا می کنند.

سوابق نفوذ به وب سایت ها

نفوذگران زمانی که به یک سایت دسترسی می گیرند بعد از تغییر ظاهر سایت یا در اصطلاح دیفیس (Deface) ، برای این که این عمل خود را در معرض نمایش دیگران قرار دهند، آدرس سایت مورد نفوذ قرار گرفته را در سایت های مخصوصی ثبت می کنند. نمونه این مدل سایت ها وب سایت www.zone-h.org می باشد که تمامی نفوذگران از کشورهای مختلف دنیا سایت های مختلف را در آن ثبت می کنند و با این کار درجه بندی بین نفوذگران انجام می شود.

در اینجا قصد دارم به تعدادی از سایت های وردپرسی که در این سایت ثبت شده است، اشاره کنم.

سایت شهرداری پاتیس برزیل (Patis)

آدرس سایت : www.patis.mg.gov.br

لینک ثبت : www.zone-h.org/mirror/id/26101832

**zone-h**
unrestricted information

Home News Events Archive Archive ★ Onhold Notify Stats Register Login

Mirror saved on: 2016-04-26 01:20:00

Notified by: ProtoWave Reloaded Domain: http://patis.mg.gov.br IP address: 192.185.211.218
System: Linux Web server: nginx Notifier stats
This is a CACHE (mirror) page of the site when it was saved by our robot on 2016-04-26 01:20:00

Reivindicamos um Brasil justo e digno para todos:

Limpeza absoluta e renovadora da política. **Não podemos ter indignação seletiva**, precisamos **remover dos cargos públicos** pessoas que estão **envolvidas com corrupção**, devemos evitar misturar religião e política, pois o **estado é LAICO**. Meus inimigos estão no poder, desfrutando de privilégios imensos, enquanto a população luta por ajuda. Corruptos, safados!!! Os argumentos utilizados na votação refletem a falta de consciência de nossos representantes, REFORMA POLÍTICA JÁ. Votar pela própria família, por Deus, pela minha neta, pelo futuro dos meus filhos, e jamais esquecer o crime de responsabilidade envergonha a nossa nação. Relembrar Ustra fere a dignidade do nosso povo que com luta venceu a Ditadura Militar. **VOCÊS, POLÍTICOS CORRUPTOS, ATRASAM O AVANÇO DO NOSSO PAÍS E DESTROEM FAMÍLIAS TRABALHADORAS!!!** Em nome do povo brasileiro questionamos como é possível um mesmo partido dirigir todo o processo de afastamento de uma presidente, sem prévia corrupção provada, e ainda retendo processos adversos ao partido, não Cunha.. nós não esquecemos de você e de suas contas na Suíça, Temer tampouco caiu em esquecimento que você tem um processo de impeachment igual a Dilma.

by [coolmemes1993 - v0ldsec - Fayzor - Mask0nha - F14T - N1d4n1d4]

Home News Events Archive Archive ★ Onhold Notify Stats Register Login Disclaimer Contact

سایت شهرداری ریوکلارو برزیل (Rioclaro)

آدرس سایت : www.rioclaro.rj.gov.br

لینک ثبت: www.zone-h.org/mirror/id/26101834

zone-h
unrestricted information

Home News Events Archive Archive ✨ Onhold Notify Stats Register Login

Mirror saved on: 2016-04-26 01:20:00

Notified by: ProtoWave Reloaded Domain: http://rioclaro.rj.gov.br IP address: 177.12.161.85
System: Linux Web server: Apache Notifier state
This is a CACHE (mirror) page of the site when it was saved by our robot on 2016-04-26 01:20:00

Você caiu na hackeada da
ProtoWave

Home News Events Archive Archive ✨ Onhold Notify Stats Register Login Disclaimer Contact

سایت وزارت معدن و زمین شناسی جمهوری گینه

آدرس سایت : www.mines.gov.gn

لینک ثبت: www.zone-h.org/mirror/id/26057195

 zone-h
unrestricted information

Home News Events Archive Archive ✨ Onhold Notify Stats Register Login

Mirror saved on: 2016-04-23 00:28:27
Notified by: hamzah uygun Domain: http://mines.gov.gn IP address: 205.251.122.94
System: Linux Web server: Apache Notifier stats
This is a CACHE (mirror) page of the site when it was saved by our robot on 2016-04-23 00:28:27

(Hello Government You Security Is Down 0%)
بِعِزَّتِ اللّٰهِ عَلَى ذِيْنَاءِ نَحْبِيْ نَحْبِيْ خَاطِرِيْ مِكَسُوْرٌ وَعَلَى قَلْبِ خَابِتِ كُلِّ هَقِيْوَانِهَةٍ

Greeting : AnonGhost - Mauritania Attacker - X-Line - Azar36.exe
Empire Northern / Tanjawa AL Khawa
FB / [Hamzah Uygun](#)

Home News Events Archive Archive ✨ Onhold Notify Stats Register Login Disclaimer Contact

سایت موسسه رفاه و تامین اجتماعی آرژانتین

آدرس سایت : www.ipsst.gov.ar

لینک ثبت: www.zone-h.org/mirror/id/26004390

گزینش سرور مناسب

اولین گام برای ایجاد یک وب سایت ایمن ، استفاده از سرورهای مناسب است. سرور مناسب ، سروری است که شامل موارد زیر باشد.

بک آپ گیری به معنای واقعی داشته باشد. منظور از این حرف چیست؟ بسیاری از سایت های فروش هاست (Host) ، در تبلیغات خود اعلام می کنند که ما به صورت هفتگی نسخه پشتیبان از سایت شما تهیه خواهیم کرد ولی در عمل این کار را انجام نمی دهند و زمانی که سایت شما با مشکلی روبه رو می شود و نیاز به نسخه پشتیبان دارید به بهانه های مختلف از ارائه خدمات سرباز می زنند. پس سعی کنید از سایت هایی هاست خریداری کنید که معتبر هستند. یکی از نشانه ها برای تشخیص معتبر بودن یک سایت داشتن نماد الکترونیکی یا همان enamad است.

مورد بعدی که باید در انتخاب سرور مدنظر قرار دهید این است که ، آیا مدیران سرور در زمان حملات گسترده از نوع تکذیب سرور اقداماتی را برای مقابله انجام می دهند یا نه؟ آیا قبل از بروز مشکل بر روی سرور از آنتی دیداس های مناسب استفاده می کنند یا خیر.

این موارد را می توانید با سوال کردن از مدیر سرور متوجه شوید. موارد دیگری نیز در انتخاب سرور ایمن موثر هستند مثل اجرا نشدن شل کدها (Shell) که در واقع کدهای مخربی هستند که نفوذگران برای اجرای کامندهای خود بر روی سرور از آنها استفاده می کنند یا بسته بودن دایرکتوری ها که در صورت باز بودن، نفوذگر با دسترسی به یکی از سایت های روی سرور به راحتی به تمام سایت های دیگر روی سرور دسترسی می گیرد. موارد بعدی بسته بودن امکان سیملینک (SymLink) ، جلوگیری از روت شدن به سرور و ... هستند که البته این موارد را بدون تجربه در زمینه نفوذ نمی توانید بررسی کنید زیرا فقط یک نفوذگر می تواند به یقین بگوید کدام سرورها در این زمینه ایمن نیستند، چون قبلا روی آن سرور تست نفوذ را انجام داده اند.

زمانی که در حال خرید یک هاست برای وب سایت خود هستید به پهنای باندی که در اختیار شما قرار می دهند توجه کنید ، زیرا در صورتی که پهنای باند کمی را به شما ارائه دهند دچار مشکلاتی از جمله پایین بودن سرعت لود سایت و یا از دسترس خارج شدن سایت برای مدت کوتاه خواهید بود.

بدون شک تهیه سرور اختصاصی امنیت را چندین برابر خواهد کرد ، اما قبل از تهیه سرور اختصاصی باید هزینه های آن را نیز در نظر گرفته و بعد اقدام به تهیه سرور کنید.

اقدامات اولیه هنگام ایجاد سایت وردپرسی

حالا زمان آن رسیده که شروع به نصب وردپرس کنیم. قبل از هرچیزی نیاز به فایل وردپرس خام داریم. توجه داشته باشید که نباید وردپرس را از هر سایتی دانلود کنید ، چون امکان آلوده بودن

فایل وجود دارد. برای دانلود وردپرس خام از سایت www.wp-persian.com به عنوان مرجع وردپرس فارسی در ایران استفاده کنید.

بعد از ورود به آدرس ذکر شده ، می توانید در قسمتی که در عکس نیز مشخص شده آخرین ورژن وردپرس فارسی را دریافت کنید.

جستجو

وردپرس فارسی

خانه درباره سبزه بوسته‌ها افزونه‌ها مستندات وبلاگ انجمن دریافت

عنوان سایت وردپرسی

پیشخوان

هم‌اکنون محتوا

23 نوشته

12 برگه

52 دسته

49 برچسب

پیشخوان

خانه

به‌روزرسانی‌ها

نوشته‌ها

رسانه

پیوندها

برگه‌ها

دیدگاه‌ها

نمایش

وردپرس نرم‌افزاری تحت وب است که می‌توانید از آن برای ساختن سرویس وبلاگ‌دهی، وبسایت یا وبلاگی زیبا و قدرتمند استفاده کنید. ما بلیم با افتخار اعلام کنیم که وردپرس با ارزش و مجانی است.

هسته‌ی نرم‌افزاری وردپرس توسط هزاران داوطلب نوشته شده و گستردگی افزودنی‌ها، بوسته‌ها، مستندات و پشتیبانی این سامانه مدیریت سایت در آن حد است که آن را برای مدیریت هرگونه وبلاگ یا وبسایت با امکانات متنوع سازگار نموده.

بیش از دویست‌هزار نفر در دنیا از وردپرس فارسی برای برپا کردن خانه‌های اینترنتی خود استفاده می‌کنند. — پیوستن شما به این خانواده، باعث افتخار همه‌ی ماست.

برای شروع آماده‌اید؟ دریافت نگارش ۴.۴.۲

حمایت از ما در نهایت سادگی در وبلاگ می‌خوانید پشتیبانی

بعد از دانلود وردپرس می‌توانید وارد هاست خودتان شوید و فایل را از حالت فشرده خارج کرده و مراحل نصب را انجام دهید.

برای ایجاد سایت شما به یک دیتابیس (Database) نیاز دارید. زمانی که در حال ایجاد دیتابیس و انتخاب نام، یوزر و پسورد برای دیتابیس خود هستید ، باید توجه داشته باشید که از انتخاب عبارت های ساده مثل admin ، password ، 123456 و ... خودداری کنید. سعی کنید پسوردی که برای دیتابیس انتخاب می‌کنید ترکیبی از اعداد و حروف بزرگ و کوچک باشد. برای نمونه 90A2@2b))4m

بعد از ایجاد دیتابیس ، با وارد کردن آدرس سایت در قسمت url مرورگر ، مراحل نصب وردپرس شما شروع می‌شود. همان طور که در تصویر مشاهده می‌کنید در قدم اول از شما نام ، یوزر و پسورد دیتابیس را درخواست می‌کند که اطلاعاتی که در قسمت قبلی استفاده کردید را وارد می‌کنید.



در بخش پایین باید اطلاعات اتصال به پایگاه داده‌ی خود را وارد کنید. اگر درباره‌ی اطلاعات زیر مطمئن نیستید با مدیر سرویس میزبانی خود تماس بگیرید.

نام پایگاه داده‌ای که می‌خواهید وردپرس روی آن اجرا شود.	<input type="text" value="wordpress"/>	نام پایگاه داده
نام کاربری MySQL	<input type="text" value="نام کاربری"/>	نام کاربری
...و رمز MySQLتان.	<input type="text" value="رمز"/>	رمز
اگر localhost کار نکرد، باید این اطلاعات را از سرویس میزبانی خود بگیرید.	<input type="text" value="localhost"/>	میزبان پایگاه داده
اگر می‌خواهید چند وردپرس را در یک پایگاه داده اجرا کنید این گزینه را تغییر دهید.	<input type="text" value="wp_"/>	پیشوند جدول

اولین نکته امنیتی که در این بخش باید رعایت کنید ، تغییر پیشوند جداول هستند. وردپرس به صورت پیش فرض WP_ را به عنوان پیشوند قرار داده که بهتر است این مورد را تغییر دهیم. برای مثال به bar_ تغییر نام می دهیم. بعد از تایید ، تصویر زیر را خواهید دید.



خب، رفیق! دیگه تو این مرحله از نصب کار شما انجام شد و وردپرس میتونه با پایگاه داده ارتباط برقرار کنه، اگه آماده‌ای، وقتش شده که...

در مرحله بعدی وارد فرآیند نصب و راه اندازی وردپرس می شویم. این قسمت در بحث امنیت اهمیت فراوانی دارد. گزینه دوم در این صفحه ، از ما نام کاربری در خواست می کند. متأسفانه مشکلی که در بسیاری از سایت ها مشاهده کردم این بود که نام کاربری یا یوزرنیم (Username) بسیار ساده ای را انتخاب کرده بودند. در این بخش به هیچ وجه از عبارت هایی مثل اسم و فامیل مدیر سایت ، نام سایت ، نام شهر یا عباراتی مانند Admin ، modir و ... استفاده نکنید. در بخش های آینده به شما نشان خواهیم داد که نفوذگر چگونه با داشتن یوزرنیم شما اقدام به نفوذ به وب سایت می کند. در قدم بعدی پسورد (Password) یا همان رمز عبور مناسب برای ورود به سایت را وارد می کنیم. باز هم تاکید می کنم رمز عبور باید شامل اعداد و حروف کوچک و بزرگ باشد و به شکلی باشد که قابل حدس زدن نباشد. انتخاب شماره تلفن، کد ملی و اسم و فامیل گزینه های نادرست و ضعیفی در انتخاب رمز عبور سایت شما خواهند بود.

ذکر یک نکته در این بخش اهمیت دارد و آن این مورد که ، یوزر و پسورد انتخابی شما برای نصب وردپرس نباید با یوزر و پسورد دیتابیس شما یکسان باشد. زیرا اگر نفوذگر به هر شکلی به فایل wp-config.php سایت شما که یوزر و پسورد دیتابیس در آن قرار دارد دسترسی پیدا کند به راحتی خواهد توانست وارد وردپرس شما نیز بشود.

در قدم بعدی از شما سایت از شما درخواست وارد کردن یک ایمیل به عنوان ایمیل مدیریت را دارد. توجه داشته باشید که به هیچ وجه از ایمیل هایی که در انجمن ها و کارهای روزمره خود استفاده می کنید ، برای این بخش استفاده نکنید. اگر شما ایمیلی را در انجمنی برای ثبت نام استفاده کنید و بر حسب اتفاق آن انجمن مورد نفوذ قرار گیرد ، تمام ایمیل ها در اختیار نفوذگر خواهد بود. با این که تحت این شرایط نفوذگر دسترسی به ایمیل شما ندارد (به دلیل نداشتن پسورد) اما با استفاده از

اقداماتی که خارج از بحث این کتاب است ، وی می تواند پسورد تعدادی از ایمیل ها را به دست آورد و اگر شما نیز جزء آن تعداد محدود باشید مشکلات متعددی را خواهید داشت که از آن جمله در خطر قرار گرفتن امنیت وب سایت خواهد بود. پس سعی کنید یک حساب جدید و ترجیحا Gmail ایجاد کنید و از آن حساب رای سایت خود استفاده کنید.

خوش آمدید

به فرآیند معروف پنج دقیقه‌ای راه‌اندازی وردپرس خوش آمدید! اطلاعات زیر را تکمیل کنید تا در مسیر استفاده از گسترده‌ترین و پرتوان‌ترین نرم‌افزار نشر الکترونیک جهان قرار بگیرید.

اطلاعات مورد نیاز

لطفاً اطلاعات زیر را وارد کنید. نگران نباشید، بعداً می‌توانید تغییرشان دهید.

<input type="text"/>	عنوان سایت
<input type="text"/>	نام کاربری
برای ساختن نام کاربری فقط از حروف الفبا، اعداد، فاصله، _ ، - و علامت @ می‌توانید استفاده کنید.	
<input type="text" value="F#P7f%a!gDWX%v*(7y"/>	رمز
<input type="checkbox"/> پنهان‌سازی	قوی
مهم: به این رمز برای ورود نیاز خواهید داشت. لطفاً آن را در مکان امنی نگهداری کنید.	
<input type="text"/>	ایمیل شما
نشانی ایمیل را پیش از ادامه دادن دوباره بررسی کنید.	
<input type="checkbox"/> از موتورهای جستجو درخواست کن تا محتوای سایت را بررسی نکنند	نمایش به موتورهای جستجو
این برعهده‌ی موتورهای جستجوست تا به پیشنهاد شما احترام بگذارند.	

بسیار عالی!! وب سایت شما با موفقیت راه اندازی شد. اما این به معنی پایان کار شما در بحث امنیت نیست ، بلکه تازه شروع کار شماست.

بعد از نصب و راه اندازی وردپرس اولین قدم پاک کردن فایل های نصبی است. شما برای این که یک سایت وردپرسی را نصب کنید از فایل هایی که داخل بسته وردپرس خام شما قرار داشته استفاده کرده اید. برای دیدن این فایل می توانید به مسیر زیر در سایت خود مراجعه کنید.












www.site.com/wp-admin/install.php

توجه : به جای کلمه site ، آدرس وب سایت خود را قرار دهید.

با زدن این آدرس با صفحه زیر مواجه خواهید شد.



می بینید که این فایل در مورد نصب وردپرس است و لزومی ندارد که روی هاست ما باقی بماند ، زیرا این امکان وجود دارد که همین مورد به ظاهر ساده باعث انجام خراب کاری توسط نفوذگر شود. علاوه بر این فایل ، فایل دیگری به نام `install-helper.php` در مسیر قبلی وجود دارد که هر دوی این فایل ها باید حذف شوند و پاک کردن این فایل ها هیچ مشکلی را در روند فعالیت سایت ما ایجاد نمی کند. برای حذف این فایل ها وارد هاست می شویم ، سپس پوشه `wp-admin` را باز می کنیم و 2 فایل که در تصویر مشاهده می کنید را حذف می کنیم.

 freedoms.php	3.27 KB
 import.php	5.09 KB
 index.php	5.91 KB
 install-helper.php	5.62 KB
 install.php	15.01 KB
 link-add.php	712 bytes
 link-manager.php	3.5 KB
 link-parse-opml.php	2.04 KB
 link.php	2.56 KB
 load-scripts.php	1.77 KB
 load-styles.php	2.32 KB

بدون شک ما نباید هیچگونه اطلاعات اضافی را در اختیار نفوذگران قرار دهیم. در وردپرس دو فایل به صوت پیش فرض وجود دارد که اطلاعاتی در مورد ورژن ما در اختیار نفوذگران قرار می دهد و از آن دسته فایل هایی هستند که نبودشان مشکلی را در روند فعالیت سایت ما ایجاد نمی کنند. مورد اول `readme.html` و مورد بعدی `license.txt` است.



Version 4.4.3

Semantic Personal Publishing Platform

First Things First











Welcome. WordPress is a very special project to me. Every developer and contributor adds something unique to the mix, and together we create something beautiful that I'm proud to be a part of. Thousands of hours have gone into WordPress, and we're dedicated to making it better every day. Thank you for making it part of your world.

— Matt Mullenweg

Installation: Famous 5-minute install





1. Unzip the package in an empty directory and upload everything.
2. Open [wp-admin/install.php](#) in your browser. It will take you through the process to set up a `wp-config.php` file with your database connection details.

همون طور که در شکل مشاهده می کنید این فایل ورژن وردپرس مارا نمایش می دهد و از آن جایی که احتیاجی به این دو فایل نداریم ، آنها را پاک می کنیم. این فایل ها در مسیر اصلی هاست قرار دارند.

 wp-admin	4 KB
 wp-content	4 KB
 wp-includes	4 KB
 error_log	464 bytes
 index.php	418 bytes
 license.txt	19.46 KB
 readme.html	7.19 KB
 wp-activate.php	4.92 KB
 wp-blog-header.php	271 bytes
 wp-comments-post.php	1.34 KB

مورد بعدی بدون شک انتخاب پوسته یا قالب (theme) مناسب برای وب سایت وردپرس ما خواهد بود. زمانی که قصد انتخاب قالب را دارید حتما قالب را از سایت های معتبر تهیه کنید. در بسیاری از موارد نفوذگران کدهای مخربی را در داخل فایل های یک قالب پولی قرار می دهند و سپس اقدام به پخش رایگان آن قالب می کنند. بسیاری از وب مستران به طمع رایگان بودن قالب آن را دانلود و در سایت خود استفاده می کنند ، بی خبر از آن که در پشت پرده این کار نفوذگر به سایت آنها دسترسی کامل دارد. با توجه به این نکته باید توجه داشته باشید که از هر قالبی برای سایت خود استفاده نکنید.

زمانی که قالب مناسب را پیدا و نصب کردید وارد هاست شوید و 3 قالبی که به صورت پیش فرض در وردپرس وجود دارد را پاک کنید ، زیرا شما از این قالب ها استفاده نمی کنید و در صورتی که نفوذگر به سایت شما دسترسی بگیرد ، کدهای مخرب خود را در داخل فایل های این قالب ها مخفی می کند و پیدا کردن کدهای مخرب بسیار دشوار خواهد بود.

	Name	Size
	twentyfifteen	4 KB
	twentyfourteen	4 KB
	twentysixteen	4 KB
	index.php	28 bytes

نکته بسیار مهم دیگری که در مورد نام کاربری شما وجود دارد یکسان نبودن نام کاربری اصلی شما با نام کاربری به نمایش درآمده در سایت است. در بعضی از قالب ها ، زیر هر پست نام نویسنده آن مطلب درج می شود و اگر این نام را تغییر نداده باشید ، نفوذگر به راحتی یوزر وب سایت شما را متوجه می شود. نونه این اشتباه را در بسیاری از سایت های وردپرسی می توانید مشاهده کنید. اما راه رفع این مشکل چیست؟

برای برطرف کردن این مشکل ابتدا وارد صفحه مدیریت سایت یا همان پیشخوان وردپرس شوید. از قسمت سمت چپ و بالای سایت همانند تصویری که مشاهده می کنید بر روی "ویرایش شناسنامه من" کلیک کنید.

admin1 admin1، درود

admin1 admin1
admin1

ویرایش شناسنامه‌ی من
بیرون رفتن

بیش‌نویس سریع

نام

چه چیزی در ذهن شماست؟

ذخیره بیش‌نویس

در صفحه باز شده در کادری با عنوان "نمایش عمومی نام" می‌توانید نامی را که دوست دارید در سایت به عنوان نویسنده مطلب نمایش داده شود وارد کنید. برای مثال من "پهروز منصوری" را به عنوان نام نمایش داده شده در سایت وارد می‌کنم در حالی که یوزر اصلی من مورد دیگری است. با این کار نفوذگر به راحتی یوزر شما را متوجه نخواهد شد.

	نام
شناسه نمی‌تواند عوض شود.	شناسه
admin1	
	نام
بهرروز	
	نام خانوادگی
منصورک	
	لقب (لازم)
admin1	
	نمایش عمومی نام
admin1 admin1	
	اطلاعات تماس
	ایمیل (لازم)
admin1admin1admin1	
	وبلاگ

محافظت از wp-config

wp-config.php یکی از فایل‌های هسته وردپرس می‌باشد. این فایل شامل اطلاعاتی در مورد پایگاه داده مانند نام (معمولاً localhost) ، نام کاربری و گذرواژه هاست می‌باشد. این اطلاعات به وردپرس اجازه می‌دهند تا برای ذخیره سازی و دریافت اطلاعاتی (مثل پست ها ، کاربران ، تنظیمات و ...) با پایگاه داده در ارتباط باشد. همچنین از این فایل برای تعریف تنظیمات پیشرفته وردپرس نیز استفاده می‌شود.

فایل wp-config.php در بسته پیش فرض که از سایت وردپرس دانلود می‌کنید قرار ندارد. به جای این فایل ، یک فایل با نام wp-config-sample.php وجود دارد که می‌توانید آن را تغییر نام داده و به عنوان فایل wp-config.php استفاده کنید.

یکی از بخش های مهمی که در فایل wp-config.php قرار دارد ، بخش وارد کردن پایگاه داده است که در تصویر مشاهده می کنید.

```
1 // ** MySQL settings - You can get this info from your web host ** //
2 /** The name of the database for WordPress */
3 define('DB_NAME', 'database_name_here');
4 /** MySQL database username */
5 define('DB_USER', 'username_here');
6 /** MySQL database password */
7 define('DB_PASSWORD', 'password_here');
8 /** MySQL hostname */
9 define('DB_HOST', 'localhost');
```

بقیه بخش های فایل wp-config.php را در تصویر مشاهده می کنید.

```
1 /** Database Charset to use in creating database tables. */
2 define('DB_CHARSET', 'utf8');
3 /** The Database Collate type. Don't change this if in doubt. */
4 define('DB_COLLATE', '');
5 /**#@+
6  * Authentication Unique Keys and Salts.
7  *
8  * Change these to different unique phrases!
9  * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/
WordPress.org secret-key service}
10  * You can change these at any point in time to invalidate all existing cookies. This will
force all users to have to log in again.
11  *
12  * @since 2.6.0
13  */
14 define('AUTH_KEY', 'put your unique phrase here');
15 define('SECURE_AUTH_KEY', 'put your unique phrase here');
16 define('LOGGED_IN_KEY', 'put your unique phrase here');
17 define('NONCE_KEY', 'put your unique phrase here');
18 define('AUTH_SALT', 'put your unique phrase here');
19 define('SECURE_AUTH_SALT', 'put your unique phrase here');
20 define('LOGGED_IN_SALT', 'put your unique phrase here');
21 define('NONCE_SALT', 'put your unique phrase here');
22 /**#@-*/
23 /**
24  * WordPress Database Table prefix.
25  *
26  * You can have multiple installations in one database if you give each a unique
27  * prefix. Only numbers, letters, and underscores please!
28  */
```

در این بخش ها تنظیمات پیشرفته تری برای پیکربندی عناصر دیگر پایگاه در اختیار شما قرار گرفته است. همچنین می توان یک کلید سری (secret keys) اختصاصی در این فایل قرار دهید تا امنیت سایت شما چندین برابر شود.

برای این کار ابتدا به آدرس زیر مراجعه کنید.

<https://api.wordpress.org/secret-key/1.1/salt>

بعد از وارد شدن اطلاعاتی را به این شکل در اختیار شما قرار می دهد.

```
define('AUTH_KEY', 'fXT 0_2|S]WcQLbHsH)?3i/iH=ViRR=f=<+o>V/>s^J-(e80#>miL+)%tZHEdBWr');
define('SECURE_AUTH_KEY', '`H/cx{Dg;T}!p>:q6%2f|^sWCQmu~p+5k@JDJv/58.6^U|!]8E=@K%LTMDzhYdSi');
define('LOGGED_IN_KEY', ')>WPIPIMQ/A*J|3/km]4=(./cH>!Z~V7t9BFb0`f6StZCvt)hb9yP <OVA?pGs;A');
define('NONCE_KEY', 'o%AfC#x{#AzHuw{vyZ6=RftJ$0J_Ux5lq<3;sCbsyNFTLfahk!Y2zH/vZoO2iWeY');
define('AUTH_SALT', 'o<xkI++AGrh|X*6~8Q<y<vPy4})7|iyG(?SpD+NQLTTt<)3[1QWdu(Aa>S1Yw,ui');
define('SECURE_AUTH_SALT', 'Scmb*BEg`:{#|^:W >i7Z%a1MwP&}2J5$..%YfG#_{D0a742fCbK-(%Bu7K]/yW_');
define('LOGGED_IN_SALT', 'p>v]E+e@-E3%rSBX[aMAJV]W?7npx1Ymk|vM[!M-vP4O?;5wqW%? mX,(Q(pPu#!');
define('NONCE_SALT', '`skW).!|I@dO}2bX`}n FHF1SB.m^.P{z#SYj{Lp>1F(-bWV^1 k/8CIW+R2TXt)');
```

این اطلاعات را کپی کرده و در جای مخصوص در wp-config قرار دهید و ذخیره کنید.

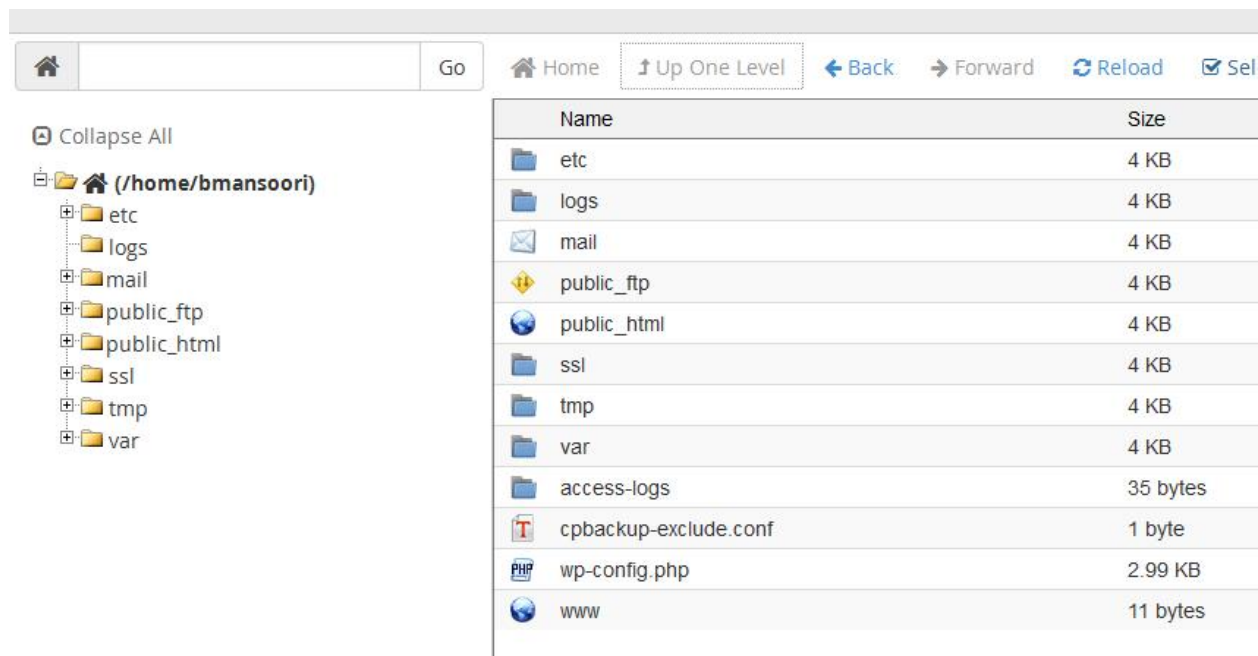
البته بعد از انتشار وردپرس 3.9.2 دیگر نیازی به وارد کردن دستی این کدها در فایل کانفیگ نیست

و وردپرس به طور خودکار این بخش را تکمیل خواهد کرد. ولی برای اطمینان 1 بار بررسی کنید.

تغییر مسیر فایل wp-config

قدم بعدی برای افزایش امنیت و حفاظت از فایل wp-config تغییر مسیر این فایل می باشد. wp-config از آن دسته فایل هایی است که نفوذگران سعی در پیدا کردن آن و به دست آوردن اطلاعات درون آن دارند ، زیرا با داشتن این اطلاعات می توانند به دیتابیس سایت متصل شوند و حتی در سایت برای خود یوزر و پسوردی را به عنوان مدیر سایت ایجاد کنند.

وردپرس در حالت پیشفرض و بدون اعمال هیچگونه تغییرات خاص ، می تواند فایل تنظیمات خودش را حتی زمانی که یک سطح بالاتر از محل نصب خودش باشد نیز پیدا کند. یعنی اگر شما فایل wp-config را از public_html به Home جابه جا کنید ، وردپرس بدون مشکل این فایل را یافته و مورد استفاده قرار خواهد داد. برای تغییر مسیر wp-config ابتدا آن را به بخش Home منتقل می کنیم.



فایل شما باید در مسیر Home قرار گیرد و دقیقا کنار فایل هایی باشد که در تصویر بالا مشاهده می کنید. در این حالت فایل شما در دسترس نفوذگران نخواهد بود و امنیت وب سایت وردپرس شما 1 مرحله افزایش یافته است.

مشکلات پیش فرض وردپرس در صفحه ورود

سیستم مدیریت محتوای وردپرس علارغم نکات مثبت زیادی که دارد ، مشکلاتی نیز به همراه دارد. یکی از مواردی که به صورت پیش فرض و ثابت در همه ورژن های وردپرس وجود دارد و امنیت وب سایت را به خطر می اندازد ، وجود صفحه ورود ثابت به بخش مدیریت سایت است. همان طور که اطلاع دارید صفحه ورود به بخش مدیریت در همه ورژن های وردپرس wp-login.php است و این مورد از آن جهت باعث کاهش امنیت می شود که نفوذگر نیازی برای یافتن صفحه مدیریت ندارد ، زیرا این صفحه همیشه ثابت است و در کمترین زمان می تواند وارد آن شود. برای این که

بدانیم چرا این مورد خطرناک است نیاز داریم تا در ابتدا با حملاتی موسوم به Brute Force آشنا شویم.

حملات Brute Force

بروت فورس نوعی از حملات کرکینگ می‌باشد که هدف از آن تلاش برای یافتن یک مقدار مثلاً رمز عبور یا پیدا کردن مقدار خالصی است که قبل از رمزگذاری شدن وجود داشته است.

مختصری در مورد حملات کرکینگ (Cracking)

پیش از توضیح دادن حملات بروت فورس که خود نوعی از حملات کرکینگ است، ابتدا توضیح مختصری درباره حملات کرکینگ بدهیم. در حملات کرکینگ (Cracking) هکر با استفاده از ابزارهای مخصوص در تلاش برای یافتن مقدار اولیه یک عبارت رمزگذاری شده و یا پیدا کردن یک مقدار حساس مثلاً رمز عبوری است که حتی عبارت رمزگذاری شده آن را هم در دست ندارد.

حملات کرکینگ اغلب از الگوی خاصی پیروی نکرده و با بررسی همه احتمالات موجود و یا مقادیری که احتمال صحیح بودن آنها بیشتر است، انجام می‌پذیرد از این رو حملات کرکینگ را به بخش‌های مختلفی تقسیم کرده اند. دو مورد از مهمترین اینها حملات دیکشنری (Dictionary) و حملات بروت فورس (Brute Force) است.

بروت فورس (Brute Force) چیست؟

در این نوع از حملات نفوذگر با استفاده از ابزار به بررسی همه احتمالات موجود می‌پردازد تا موفق به یافتن مقدار حساسی مانند رمز عبور یک سایت شود. چون در این نوع از حملات ، همه احتمالات

بررسی می شود ، برای عباراتی با اندازه بیش از 5-6 کاراکتر (برای کامپیوترهای عادی) پرهزینه و بی ارزش خواهد بود.

در اینجا به توضیح در مورد مثالی می پردازم تا به درک صحیحی از پرهزینه بودن این پروسه برسید. برای مثال نفوذگر Handshake یک شبکه وای فای که از امنیت WPA یا WPA2 استفاده می کند را بدست آورده استدر این مرحله نفوذگر اقدام به بروت فورس کردن آن در سیستم خود یا یک سیستم قدرتمند مانند سرور مجازی (VPS) می کند.

چون نفوذگر مقدار رمزگذاری شده را در دست دارد، به این نوع حمله، بروت فورس آفلاین گفته می شود. روش کار به این صورت خواهد بود که ابتدا اقدام به بررسی همه احتمالات و ترکیب های موجود ۸ رقمی می کند. چون حداقل تعداد کاراکتر رمز وای فای باید ۸ کاراکتر باشد. در حمله بروت فورس نفوذگر کاراکترها را مشخص کرده سپس اقدام به کرک کردن آن مقدار رمزگذاری شده می کند. برای مثال از عبارت ۰۰۰۰۰۰۰۰ شروع کرده و بعد ۰۰۰۰۰۰۰۱ و ۰۰۰۰۰۰۱۱ و ... و ۹۹۹۹۹۹۹۸ و ۹۹۹۹۹۹۹۹ را امتحان می کند و زمانی که اعداد به پایان رسید همین کار را برای حروف انجام خواهد داد.

در هر بار رمزگذاری کردن یک عبارت، مقدار رمزگذاری شده جدید با مقدار رمزگذاری شده در هندشیک شبکه وای فای مقایسه می شود. هر گاه که هر دو مقدار یکی بود، یعنی رمز وای فای همان است اما اگر مقادیر یکی نباشند، سراغ ترکیب بعدی می رود.

همان طور که متوجه شدید حملات بروت فورس برای رمزهایی که فقط از اعداد یا کاراکترهای کمی استفاده شده باشد موثر خواهد بود. مثلا یک رمز 8 رقمی که از اعداد 0 تا 9 استفاده شده است می تواند در کمتر از روز با یک کامپیوتر عادی به دست آید.

حال به موضوع اصلی میپردازیم. بروت فورس چگونه می تواند تهدیدی برای سایت های وردپرسی باشد؟

برای توضیح این مورد کافیهست به ذکر این نکته بپردازیم که اگر نفوذگر به نام کاربری ما دست پیدا کند این حمله را روی صفحه ورود سایت ما پیاده سازی می کند. در این حالت نفوذگر یوزرنیم (Username) را دارد و فقط نیاز به پسورد (Password) ، برای تسترسی گرفتن به وب سایت وردپرسی را دارد. اما نفوذگر چگونه می تواند یوزرنیم ما را پیدا کند؟

مشکل مشخص شدن یوزر مدیریت در سایت های وردپرسی

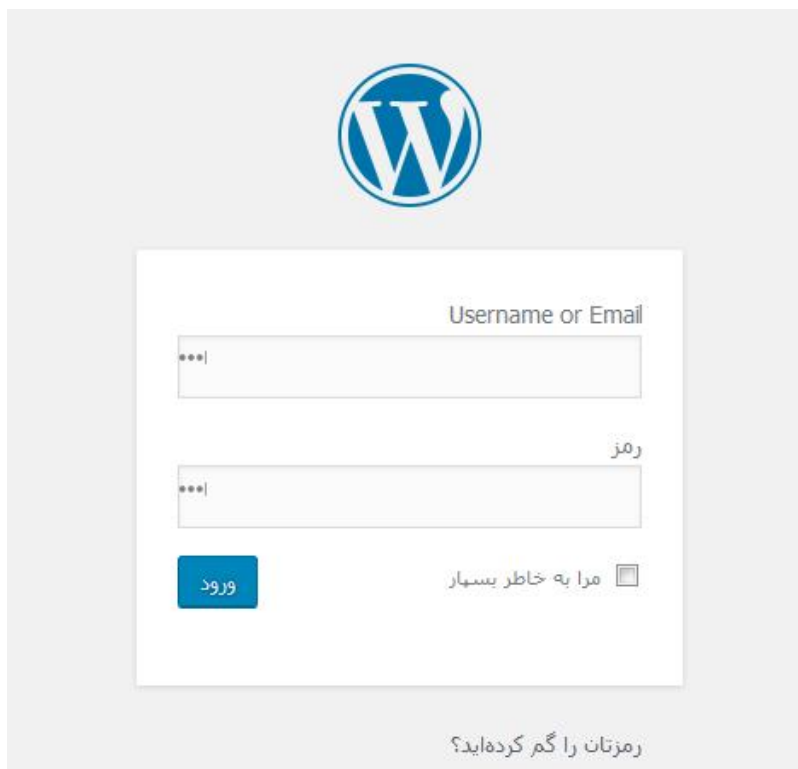
راه های مختلفی وجود دارد که نفوذگر می تواند به کمک آن ها یوزر ما را پیدا کند.

الف – نمایش نام کاربری در پست ها

همان طور که قبلا نیز اشاره کردیم ، در بعضی از پوسته های وردپرسی این امکان وجود دارد که در زیر یک مطلب ، نام نویسنده مشخص شود. در صورتی که شما از قسمت پروفایل ، نام نمایشی در سایت را تغییر نداده باشید این مورد می تواند خطرناک باشد ، زیرا نفوذگر به سادگی نام کاربری شما را پیدا کرده است. برای تغییر این مورد در پیشخوان وردپرس از قسمت بالا سمت چپ بر روی "ویرایش شناسنامه من" کلیک کنید و در قسمت "نمایش عمومی نام" ، نام دیگری را برای خود انتخاب کنید.

ب – کمک صفحه ورود به نفوذگران

مشکلی به صورت پیش فرض در وردپرس وجود دارد و آن نمایش خطاهایی است که به نفوذگران در یافتن نام کاربری مدیر کمک می کند. برای درک بهتر این موضوع به تصاویر نگاه کنید.



The image shows the WordPress login interface. At the top center is the WordPress logo, a blue 'W' inside a circle. Below it is a white rectangular form with a light gray border. Inside the form, there are two input fields. The first field is labeled 'Username or Email' and contains three asterisks. The second field is labeled 'رمز' (Password) and also contains three asterisks. Below the second field is a blue button with the Persian word 'ورود' (Login) written on it. To the right of the button is a checkbox with the Persian text 'مرا به خاطر بسپار' (Remember me) next to it. At the bottom of the form, there is a link that says 'رمزتان را گم کرده‌اید؟' (Lost your password?).

در اینجا ما در صفحه ورود یک سایت وردپرسی هستیم و از ما درخواست وارد کردن یوزر و پسورد را دارد.

من در قدم اول یوزر اشتباهی را وارد می کنم تا نتیجه را مشاهده کنیم. لطف به پیغام خطایی که وردپرس نمایش می دهد توجه کنید.



خطا: نام کاربری نادرست است. رمزتان را گم کرده‌اید؟

Username or Email

رمز

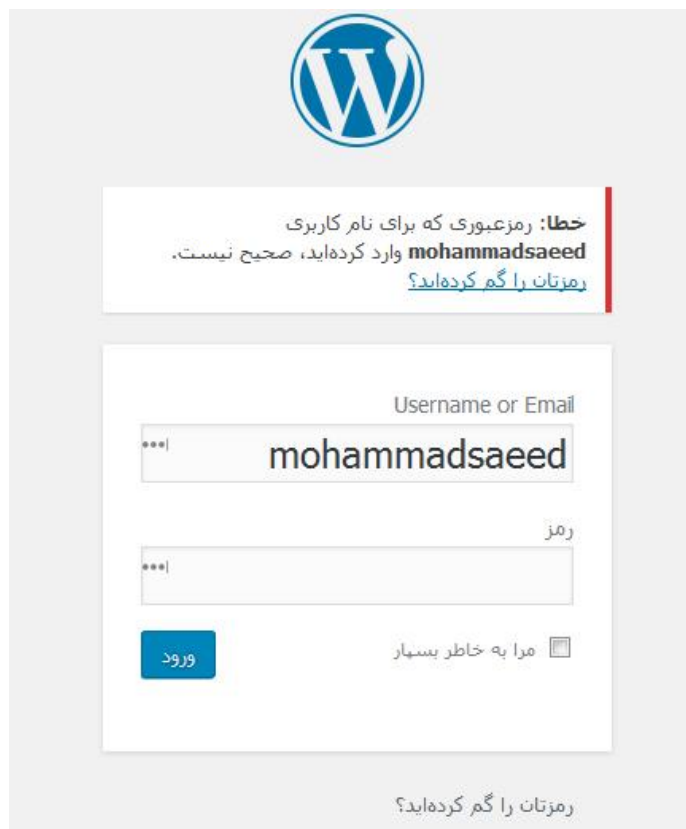
ورود

مرا به خاطر بسپار

رمزتان را گم کرده‌اید؟

همان طور که در تصویر مشاهده می کنید ، پیغام خطا به این شکل است. "نام کاربری نادرست است".

حالا من یوزر یا همان نام کاربری صحیح را وارد می کنم و فقط پسورد را اشتباه میزنم.



The image shows the WordPress login interface. At the top center is the WordPress logo. Below it, a red-bordered box contains an error message in Persian: "خطا: رمزعبوری که برای نام کاربری mohammdsaeed وارد کرده‌اید، صحیح نیست. رمزتان را گم کرده‌اید؟". Below this is the login form with two input fields. The first field is labeled "Username or Email" and contains the text "mohammdsaeed". The second field is labeled "رمز" (Password) and is empty. A blue "ورود" (Login) button is at the bottom left of the form. To its right is a checkbox labeled "مرا به خاطر بسپار" (Remember me). At the bottom of the form area, there is a link that says "رمزتان را گم کرده‌اید؟" (Lost your password?).

باز هم پیغام خطایی را داریم اما به این شکل. " رمز عبوری که برای نام کاربری mohammdsaeed وارد کردید ، صحیح نیست.

در این پیغام خطا نکته ای مهم قرار دارد.وردپرس با این خطا به ما می گوید نام کاربری که وارد کرده اید درست است اما پیورد را اشتباه وارد کرده اید ، زیرا در خطا نوشته شده است که رمز عبوری که برای نام کاربری mohammdsaeed وارد کرده اید صحیح نیست و حرفی از اشتباه بودن نام کاربری زده نشده است.

پس همانطور که می بینید این مورد می تواند راهنمایی بسیار عالی برای نفوذگران باشد. نفوذگر با قرار دادن عباراتی مثل admin ، modir ، اسم شما ، فامیل شما ، شماره وبایل شما و ... می تواند مواردی که حدس می زند شما به عنوان نام کاربری انتخاب کرده اید را بررسی کند.

در ادامه روش سدوم که نفوذگر می تواند به کمک آن نام کاربری را پیدا کند ذکر می کنیم و سپس راه های رفع این مشکلات را بررسی می کنیم.

پ - به دست آوردن نام کاربری از طریق url

در این روش نفوذگر با اضافه کردن عبارت کوتاهی بعد از آدرس سایت و در قسمت url می تواند نام کاربری شما را پیدا کند. به این مورد توجه کنید.

<https://www.pardazmizban.com/?author=1>

من عبارت `?author=1` را جلوی نام سایت قرار می دهم. این دستور به این معنی است که نام نویسنده اول سایت را می خواهم. بدون شک اولین نویسنده سایت مدیر سایت خواهد بود. حالا نتیجه به 2 شکل می تواند باشد. در حالت اول نتیجه مانند تصویر زیر در url نمایان می شود.

<https://www.pardazmizban.com/author/mohammasaeed/>

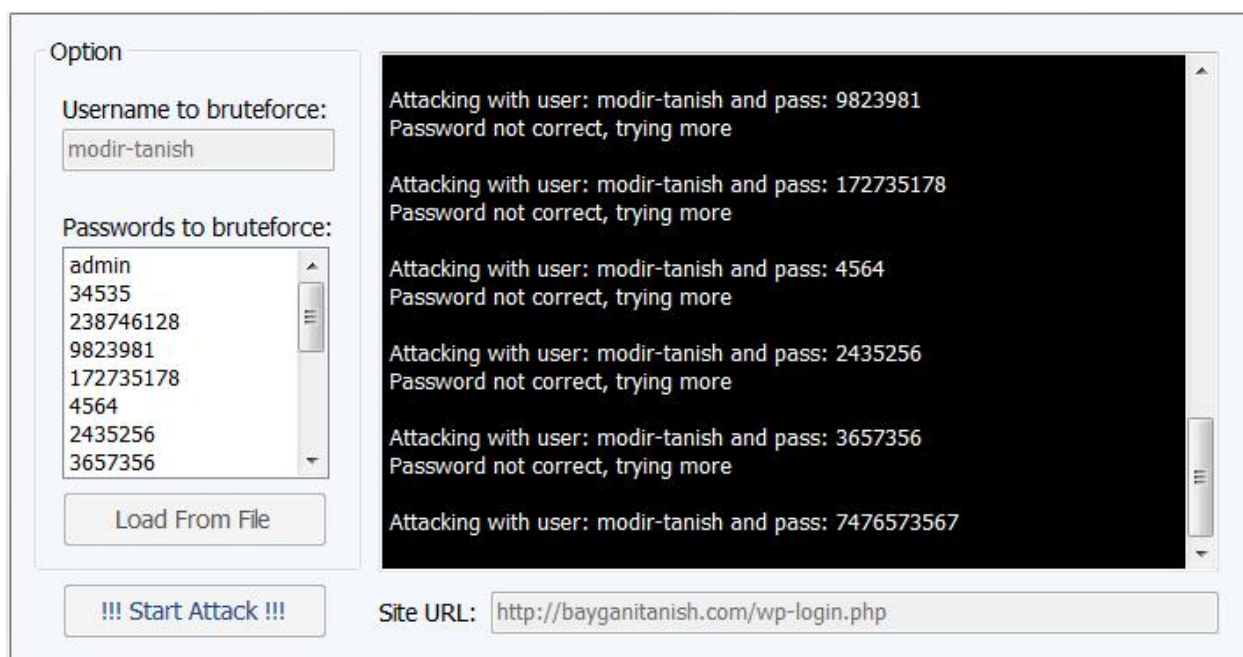
همانطور که مشاهده می کنید نام کاربری را جلوی عبارت author به نمایش گذاشت و ما به راحتی نام کاربری سایت را متوجه شدیم.

در حالت دوم در url تغییری ایجاد نمی شود ولی در صفحه سایت می توانیم نام کاربری را مشاهده کنیم و نام کاربری فرد به صورت واضح نوشته می شود. برای مثال به صورت خواهد بود :
admin

شما بعد از دیدن این مورد متوجه می شوید که نام کاربری سایت admin است.

نکته : گاهی اوقات نام کاربری در title صفحه ، در مرورگر مشخص می شود.


بعد از این که نفوذگر یوزر شما را به یکی از روش های ذکر شده به دست آورد ، از طریق برنامه ها شروع به انجام عملیات بروت فورس می کند. در این جا تصویری از یک برنامه به عنوان نمونه قرار می دهیم.



همانطور که در تصویر مشاهده می کنید ، ما صفحه ورود سایت به همراه یوزر ادمین را وارد کردیم و برنامه پسوردهایی که به صورت لیست وارد کردیم را چک می کند تا به نتیجه برسد.

رفع مشکل مشخص شدن یوزر مدیریت در سایت های وردپرسی

برای رفع مشکل نشان دادن نام کاربری با استفاده از `?author=1` تنها کافیست که از افزونه های مناسب برای رفع این مشکل استفاده کنیم. دو افزونه `SF Author Url Control` و `SX User Name Security` برای رفع این مشکل بسیار کار آمد خواهند بود.



SF Author Url Control

Allows administrators or capable users to change the users profile url.

[Download Version 1.2](#)

[Description](#) [Installation](#) [FAQ](#) [Screenshots](#) [Changelog](#) [Stats](#) [Support](#) [Reviews](#) [Developers](#)



*Don't show
your real login
to everyone*

SX User Name Security

SeoMix

SX User Name Security prevents WordPress from showing your real Login by overriding the body_class function, User Nicename, Nickname and Display Name.

[Download Version 2.3](#)

[Description](#) [Installation](#) [FAQ](#) [Screenshots](#) [Changelog](#) [Stats](#) [Support](#) [Reviews](#) [Developers](#)

همان طور که در تصویر مشاهده می کنید ، می توانید این افزونه ها را از مرجع رسمی وردپرس به آدرس wordpress.org دریافت کنید.

بعد از فعال سازی هر دو افزونه ، وارد پروفایل شخصی خود شوید و در قسمت Profile Url Slug نامی که دوست دارید به نمایش گذاشته شود را وارد کنید.



author/ (Leave empty for default value: author8) Profile URL slug

برای نمونه من کلمه `SOrry` رو به عنوان نام کاربری که نمایش داده خواهد شد وارد کردم. نتیجه را بررسی می کنیم.



همان طور که در تصویر مشاهده می کنید با وارد کردن عبارت `?author=1` به جای نمایش دادن نام کاربری اصلی ، نامی که در مرحله قبل قرار دادیم را نمایش می دهد.

به همین سادگی این مشکل برطرف شد.

سراغ رفع کردن مشکل بعدی یعنی نمایش دادن خطا و راهنمایی نفوذگران با استفاده از تحلیل پیغام خطاها می رویم. برای رفع این مشکل 2 روش وجود دارد. مورد اول استفاده از افزونه `Limit Login Attempts` است. با استفاده از این افزونه علاوه بر این که پیغام خطاها اصلاح می شوند برای ورود به سایت محدودیت نیز اعمال می شود. برای مثال تنظیم می کنیم که اگر 3 بار پسورد اشتباه وارد شد ، آن ip خاص به مدت 1 ساعت امکان تست دوباره را نداشته باشد.

راه دیگری که برای رفع این مشکل وجود دارد ، نیازی به نصب افزونه ندارد.

ابتدا وارد پیشخوان وردپرس می شویم. از قسمت نمایش ، ویرایشگر را انتخاب می کنیم. وارد توابع پوسته (function.php) و کدی را قبل از دستور بسته شدن php قرار می دهیم. به تصویر نگاه کنید.

```

// Main Functions
require_once ( get_template_directory() . '/framework/functions/theme-functions.php' );
require_once ( get_template_directory() . '/framework/functions/common-scripts.php' );
require_once ( get_template_directory() . '/framework/functions/mega-menus.php' );
require_once ( get_template_directory() . '/framework/functions/page-layout.php' );
require_once ( get_template_directory() . '/framework/functions/breadcrumbs.php' );
require_once ( get_template_directory() . '/framework/functions/tie-views.php' );
require_once ( get_template_directory() . '/framework/functions/translation.php' );
require_once ( get_template_directory() . '/framework/widgets.php' );
require_once ( get_template_directory() . '/framework/admin/framework-admin.php' );
require_once ( get_template_directory() . '/framework/shortcodes/shortcodes.php' );

if( tie_get_option( 'live_search' ) )
    require_once ( get_template_directory() . '/framework/functions/search-live.php' );

if( !tie_get_option( 'disable_argam_lite' ) )
    require_once ( get_template_directory() . '/framework/functions/argam-lite.php' );
}
?>

```

در قسمتی که مشخص شده کد زیر را وارد می کنیم.

```

function failed_login () {
return 'the login information you have entered is incorrect.';
}
add_filter ( 'login_errors', 'failed_login' );

```

به جای عبارت نوشته شده جلوی return می توانید از عبارتی فارسی نیز استفاده کنید. به تصویر زیر نگاه کنید.

```

// Main Functions
require_once ( get_template_directory() . '/framework/functions/theme-functions.php' );
require_once ( get_template_directory() . '/framework/functions/common-scripts.php' );
require_once ( get_template_directory() . '/framework/functions/mega-menus.php' );
require_once ( get_template_directory() . '/framework/functions/pagenavi.php' );
require_once ( get_template_directory() . '/framework/functions/breadcrumbs.php' );
require_once ( get_template_directory() . '/framework/functions/tie-views.php' );
require_once ( get_template_directory() . '/framework/functions/translation.php' );
require_once ( get_template_directory() . '/framework/widgets.php' );
require_once ( get_template_directory() . '/framework/admin/framework-admin.php' );
require_once ( get_template_directory() . '/framework/shortcodes/shortcodes.php' );

if ( tie_get_option( 'live_search' ) )
    require_once ( get_template_directory() . '/framework/functions/search-live.php' );

if ( !tie_get_option( 'disable_argam_lite' ) )
    require_once ( get_template_directory() . '/framework/functions/argam-lite.php' );

function failed_login () {
    return 'اطلاعات شما اشتباه است. آبیی شما ذخیره شد. در صورت بروز مشکل در سایت این آبیی در اختیار مقامات قضایی قرار داده خواهد شد.';
}
add_filter ( 'login_errors', 'failed_login' );
?>

```

همان طور که مشاهده می کنید من از یک جمله فارسی استفاده کرده ام و برای ترساندن نفوذگر از جملات خاص هم استفاده کرده ام. حال نوبت آن رسیده که وارد صفحه ورود شویم و یکبار بررسی کنیم.

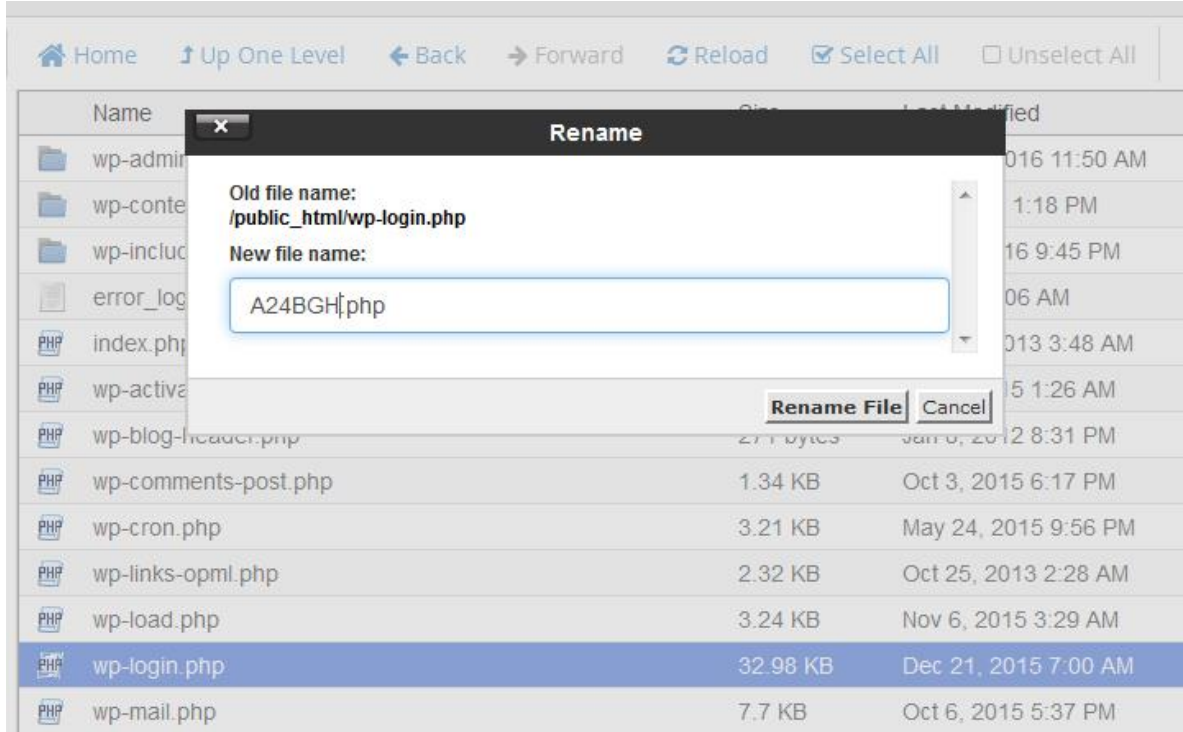


حالا در صورت نادرست بودن پسورد ، اگر یوزر را درست وارد کنیم یا اشتباه وارد کنیم ، در هر دو حالت با این پیغام خطا مواجه می شویم.در این حالت نفوذگر نمی تواند از خطا کمک بگیرد زیرا این خطاها هیچ اطلاعاتی را در اختیار نفوذگر قرار نمی دهند.

رفع مشکل صفحه ورود ثابت در وردپرس

همان طور که قبلا اشاره کردیم ، یکی از مشکلات اصلی در وردپرس وجود صفحه مدیریت پیش فرض است.ثابت بودن صفحه ورود باعث می شود نفوذگر بدون کمترین تلاشی به این صفحه دست پیدا کند.برای رفع این مشکل نیاز به انجام چند اقدام ساده ولی حیاتی است.

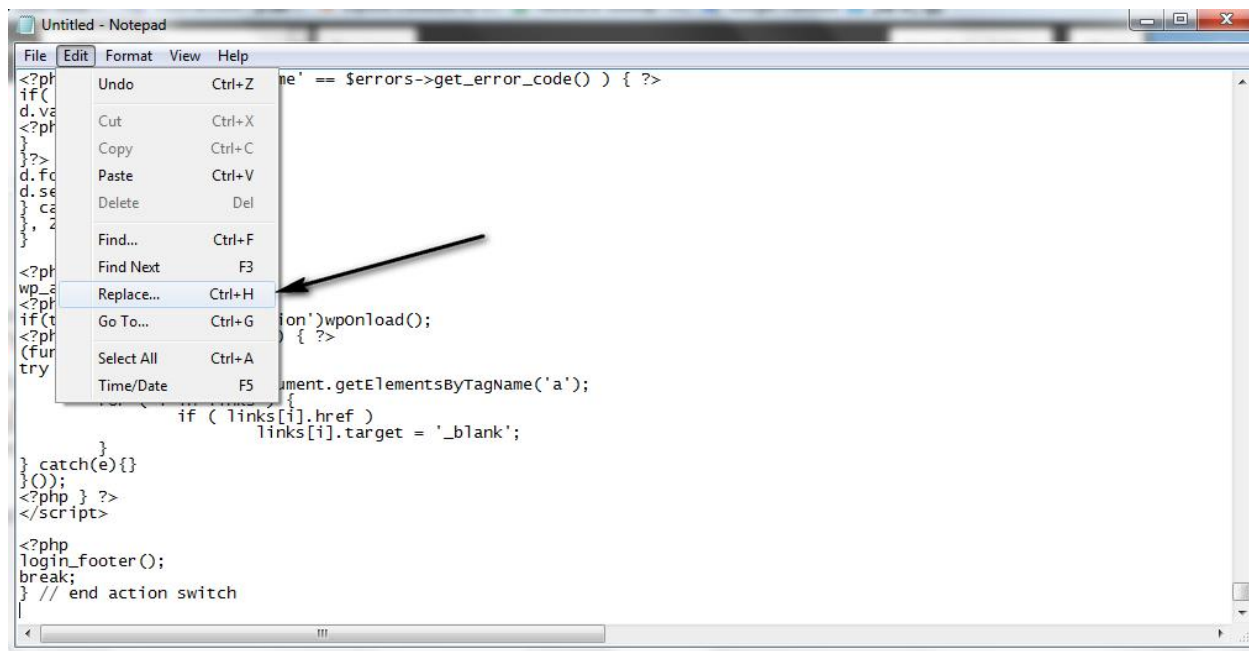
برای این منظور ابتدا وارد هاست (Host) ، وب سایت خود می شویم و از قسمت `public_html` فایل `wp-login.php` را پیدا کرده ، روی آن کلیک راست کرده و گزینه `Rename` را می زنیم.حالا نامی جدید برای صفحه ورود سایت وارد می کنیم.(توجه داشته باشید که از نامی استفاده کنید که قابل حدس زدن نباشد.برای مثال `A24BGH.php`).



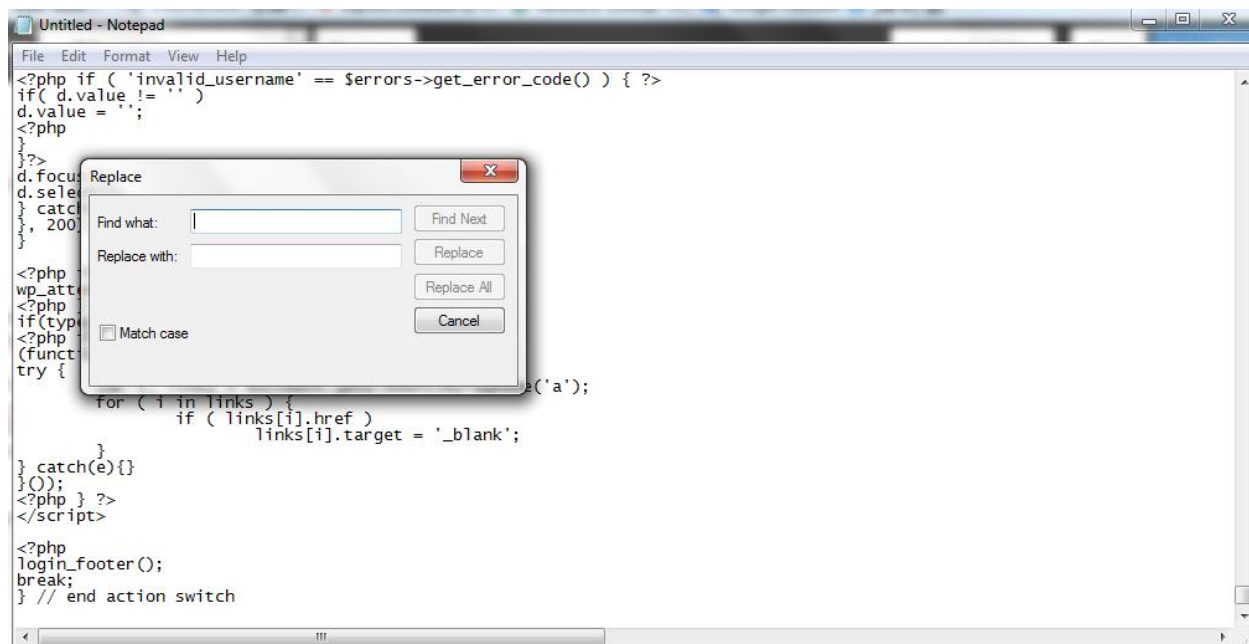
به عنوان قدم بعدی روی فایل که تغییر نام داده اید کلیک راست کرده و گزینه ویرایش (Edit) را انتخاب کنید.

برای راحتی کار تمام کدهای موجود در این فایل را با زدن دکمه های $ctrl + A$ در حالت انتخاب قرار داده ، سپس کپی کنید و در یک فایل Notepad می ریزیم.

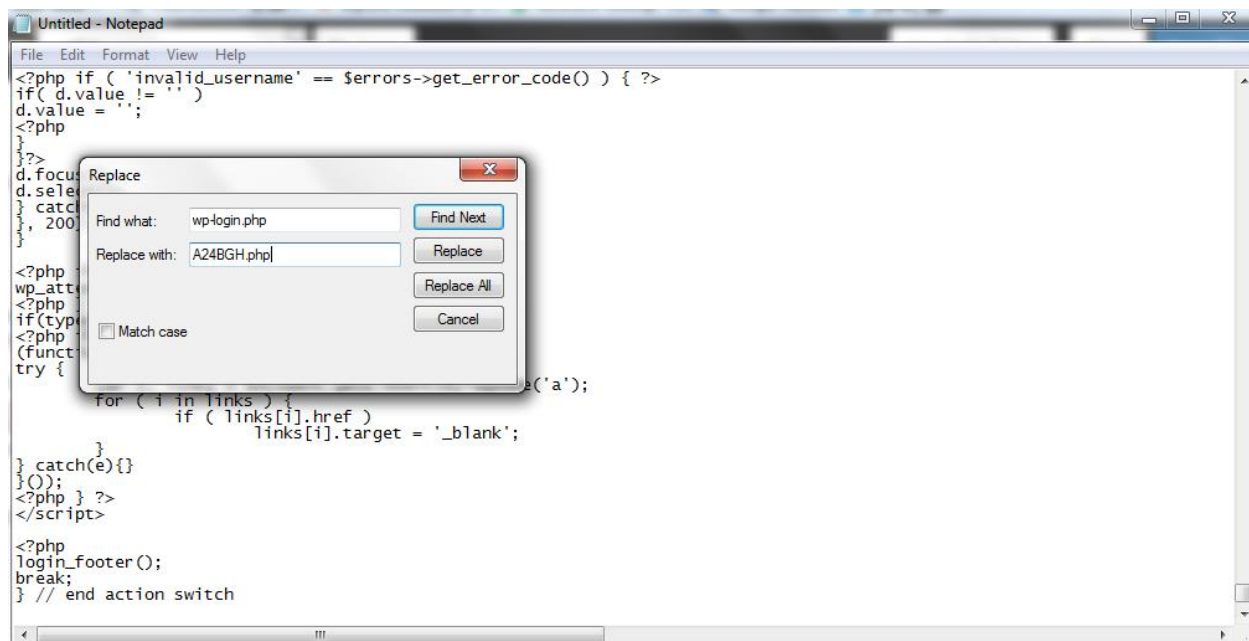
حالا در Notepad روی گزینه Edit کلیک کرده و Replace را انتخاب کنید.



پس از انتخاب این گزینه یک پنجره جدید به شکل زیر باز خواهد شد.

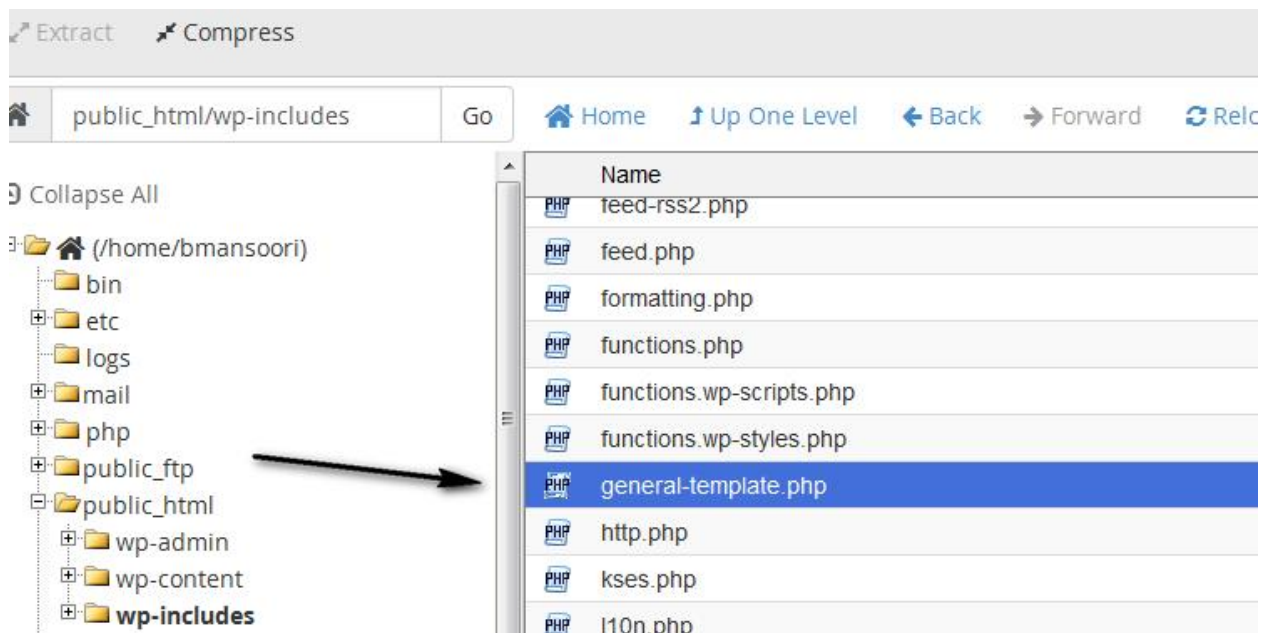


در این پنجره در کادر اول (Find what) عبارت wp-login.php و در کادر دوم (Replace with) نام جدید صفحه ورود سایت که در این مثال A24BGH.php است را وارد می کنیم و بعد روی گزینه Replace All کلیک می کنیم.



بعد از انجام این کار 12 مورد تغییر خواهد کرد. حال دوباره این کد را کپی می کنیم و جایگزین کد اصلی در هاست می کنیم و save میزنیم.

تا اینجای کار اگر شما صفحه wp-login.php را وارد کنید با پیغام خطا 404 روبرو می شوید و اگر A24BGH.php را بزنید صفحه ورود به بخش مدیریت ، برای شما نمایان خواهد شد. اما در این جا مشکلی وجود دارد که باید برطرف شود. اگر من به عنوان مدیر سایت یوزر و پسورد را در صفحه جدید وارد کنم عملیت ورود بدون مشکل اجرا می شود ولی زمانی که می خواهم از صفحه پیشخوان مدیریت خارج شوم با خطای 404 مواجه خواهم شد. برای رفع این مشکل وارد پوشه wp-includes در قسمت public_html می شویم و فایل general-template.php را پیدا کرده و آن را ویرایش می کنیم.



دقیقا مواردی را که در مرحله قبل انجام دادیم ، در این بخش نیز انجام می دهیم. یعنی تمام کدهای این فایل را کپی می کنیم و در یک فایل Notepad میریزیم ، سپس تمام wp-login.php ها را با A24BGH.php تغییر می دهیم و بعد کد جدید را به هاست منتقل می کنیم و جایگزین کدهای اصلی کرده و save می کنیم.(در این بخش 5 مورد تغییر خواهد کرد).

کار هنوز تمام نشده !! یک مشکل وجود دارد. درست است که که صفحه را تغییر دادیم ولی اگر نفوذگر عبارت wp-admin را بعد از آدرس سایت وارد کند ، سایت بلافاصله نفوذگر را به صفحه مدیریت اصلی سایت ما که در این مثال A24BGH.php است منتقل می کند. این عمل ریدایرکت کردن ، تمام محاسبات و زحمت های ما را از بین می برد. پس باید این مشکل را برطرف کنیم. برای رفع این مشکل دوباره فایل general-template.php را ویرایش می کنیم و تابعی که در تصویر مشاهده می کنید را پیدا می کنیم.

```

* @param string $redirect Path to redirect to on login.
* @param bool $force_reauth Whether to force reauthorization, even if a cookie is present. Default is false.
* @return string A log in URL.
*/
function wp_login_url($redirect = '', $force_reauth = false) {
    $login_url = site_url('A24BGH.php', 'login');

    if ( !empty($redirect) )
        $login_url = add_query_arg('redirect_to', urlencode($redirect), $login_url);

    if ( $force_reauth )
        $login_url = add_query_arg('reauth', '1', $login_url);

    /**
     * Filter the login URL.
     *
     * @since 2.8.0
     * @since 4.2.0 The `$force_reauth` parameter was added.
     *
     * @param string $login_url The login URL.
     * @param string $redirect The path to redirect to on login, if supplied.
     * @param bool $force_reauth Whether to force reauthorization, even if a cookie is present.
     */
    return apply_filters( 'login_url', $login_url, $redirect, $force_reauth );
}

/**
 * Returns the URL that allows the user to register on the site.
 */

```

اگر از طریق تصویر کد مخصوص را پیدا نکردید کد را در برنامه Notepad++ قرار دهید و در خط 311 ، به دنبال تابع مورد نظر باشید.حالا عبارت A24BGH.php را به index.php تغییر دهید تا در صورتی که فردی wp-admin را وارد کرد به جای ریدایرکت شدن به صفحه مدیریت ، به صفحه اول سایت منتقل شود.

به همین راحتی امنیت وب سایت خودمان را با استفاده از تغییر نام صفحه ورود به بخش مدیریت ، بالا می بریم.البته شما می توانید برای انجام این موارد از افزونه ها (plugin) استفاده کنید ، اما این کار توصیه نمی شود.چون در بسیاری از موارد همین افزونه ها خطرناک می شوند.خیلی از مواقع نفوذگران در افزونه ها حفره های امنیتی پیدا می کنند و از طریق این حفره ها به سایت ها نفوذ می کنند.

پرمیشن (Permission) چیست؟

پرمیشن به معنای سطح دسترسی است.با استفاده از این ویژگی می توانیم سطح دسترسی کاربران گروه های مختلف ، به فایل ها و فولدرهای درون هاست خود را ، کم و زیاد کنیم.سطح دسترسی امر

مهمی است زیرا در صورت اعمال اشتباه آن بر روی یک فایل می توانید اجازه ویرایش آن را به عموم افراد بدهید.

فایل هایی وجود دارند که نباید توسط همگان قابل ویرایش باشند. بدین منظور می بایست سطح دسترسی آن را به نحوی تنظیم نماییم که این فایل غیر قابل ویرایش باشد. همچنین ممکن است فایل هایی وجود داشته باشند که برای دانلود بر روی سایت خودمان قرار می دهیم ، پس این فایل ها باید دارای سطح دسترسی باشند که کاربران بتوانند به راحتی آن ها را دانلود کنند.

پرمیشنی که بر روی فایل ها و فولدرها ایجاد می نماییم عددی 3 رقمی می باشد که در رقم آن معنا و مفهوم خاصی دارد.

403
ACCESS DENIED
You do not have permission to view this resource



در صورتی که فایلی دارای سطح دسترسی محدود شده باشد و بخواهید به آن دسترسی پیدا کنید با خطای Forbidden 403 مواجه خواهید شد.

Server Error

403 - Forbidden: Access is denied.

You do not have permission to view this directory or page using the credentials that you supplied.

در ادامه شما را با انواع سطح دسترسی ها و کاربران آشنا خواهیم کرد.

انواع سطح دسترسی ها :

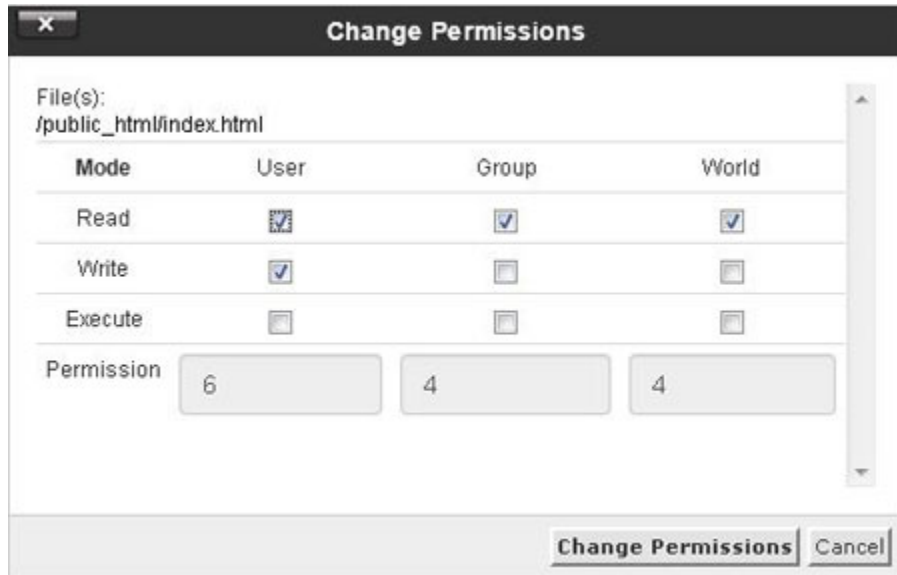
- خواندن: سطح دسترسی خواندن یا Read بدین معنا می باشد که شما می توانید یک فایل یا فولدری را بخوانید .
- نوشتن: سطح دسترسی نوشتن یا Write بدین معنا می باشد که شما می توانید بر روی فایل موردنظر ویرایش انجام دهید.
- اجرا: سطح دسترسی اجرا یا Execute بدین معنا می باشد که شما می توانید یک فایلی را اجرا نمایید.

در ادامه با مثال هایی که زده خواهد شد با مفهوم این سطح دسترسی ها بیشتر آشنا خواهید شد.

انواع کاربران :

- کاربر / یوزر: کاربر اصلی یا Owner می باشد که بیشترین سطح دسترسی را خواهد داشت. همان یوزر هاست.
- گروه : گروه ها / Groups تابع یوزر اصلی می باشند.
- جهان/عموم: منظور از عموم یا World تمامی کسانی که سایت را مشاهده می کنند.

در ادامه با انواع دسترسی هایی که به هرکدام از این گروه های کاربری داده می شود بیشتر آشنا خواهید شد.



انواع حالت های سطح دسترسی های هر گروه کاربری:

- سطح دسترسی ها برای هر گروه کاربری « Owner، Group، World » به 8 حالت ممکن می باشد:
- 0: هیچ یا None می باشد. بدین معنی که هیچ سطح دسترسی برای خواندن، نوشتن و اجرا وجود ندارد.
- 1: اجرا یا Execute می باشد. بدین معنی که سطح دسترسی برای گروه کاربری مورد نظر برای اجرای فایل ها و فولدر ها را فراهم می کند.

• 2: نوشتن یا Write می باشد. بدین معنی که سطح دسترسی برای گروه کاربری مورد نظر برای نوشتن یا ویرایش فایل ها و فولدر ها را فراهم می کند.

• 3: نوشتن و اجرا یا Write and Execute می باشد. بدین معنی که سطح دسترسی برای گروه کاربری مورد نظر برای نوشتن و اجرای فایل ها و فولدر ها را فراهم می کند.

• 4: خواندن یا Read می باشد. بدین معنی که سطح دسترسی برای گروه کاربری مورد نظر برای خواندن فایل یا فولدر ها را فراهم می کند.

• 5: خواندن و اجرا یا Read and Execute می باشد. بدین معنی که سطح دسترسی برای گروه کاربری مورد نظر برای خواندن و اجرای فایل یا فولدرها را فراهم می کند.

• 6: خواندن و نوشتن یا Read and Write می باشد. بدین معنی که سطح دسترسی برای گروه کاربری مورد نظر را برای خواندن و نوشتن فایل یا فولدر ها را فراهم می کند.

• 7: هر 3 سطح دسترسی خواندن، اجرا و نوشتن یا Read and Write and Execute می باشد. بدین معنی که سطح دسترسی برای گروه کاربری مورد نظر را برای خواندن، نوشتن و اجرای فایل یا فولدر ها را فراهم می کند.

برای نمایش دادن سطح دسترسی ها از حروف زیر استفاده می شود:

سطح دسترسی r: Read

سطح دسترسی w: Write

سطح دسترسی x: Execute

چند نمونه سطح دسترسی :

-rw- r- r	۶۴۴	File	Index.html
rwX r-X r-X	۷۵۵	Folder	joomla
— — -r	۴۰۰	File	Config
— rwX r-X	۷۵۰	File	Wp-config
-rw- rw- rw	۶۶۶	example	example
— — rwX	۷۰۰	example	example
— -rw- r	۶۴۰	example	example

برخی از کدهای سطح دسترسی برای فایل ها

- 600 فایل مورد نظر را غیر قابل دسترس می نماید
- 644 فایل مورد نظر را برای عموم قابل خواندن می نماید مانند اسناد HTML
- 666 فایل مورد نظر را قابل خواندن و ویرایش می نماید
- 755 فایل مورد نظر را برای عموم قابل خواندن و اجرا شدن می نمایدمانند CGI Scripts
- 777 فایل مورد نظر را برای عموم قابل نوشتن و اجرا می نماید استفاده از این سطح دسترسی با احتیاط توصیه می گردد

برخی از کدهای سطح دسترسی برای پوشه ها

- 711 فایل های درون یک پوشه را قابل خواندن می نماید محتویات پوشه قابل خواندن نمی باشد
- 755 فایل ها و محتویات درون یک پوشه را برای عموم قابل خواندن می نماید

777 دسترسی کامل جهت خواندن، نوشتن و حذف کردن یک پوشه برای عموم را می دهد استفاده از این سطح دسترسی با احتیاط توصیه می گردد

نکته: سطح دسترسی 777 معمولا توصیه نمی گردد. این نوع سطح دسترسی همانطور که در جدول بالا مشاهده نمودید دسترسی بسیار کاملی در همه ی زمینه ها به تمامی کاربران داده می شود.

نکته: اگر سطح دسترسی ها به درستی تنظیم نشوند با خطای Internal Server Error مواجه خواهید شد. اکثرا به دلیل سطح دسترسی ها و محتوای فایل htaccess خطای Internal Server Error ایجاد می گردد.

Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator, webmaster@localhost and inform them of the time the error occurred, and anything you might have done that may have caused the error.

توصیح می شود که فایل wp-config.php و فایل htaccess را به پرمیژن 600 تغییر دهید.

به روز رسانی های پی در پی

یکی از نکات مهم در مورد امنیت وردپرس به روز رسانی مرتب آن می باشد. بدون شک یکی از دلایل ارائه ورژن جدید از وردپرس و یا یک افزونه برطرف شدن تعدادی از حفره های امنیتی است. پس باید توجه داشته باشید که به محض منتشر شدن ورژن جدیدی از یک افزونه و یا منتشر شدن ورژن جدیدی از نسخه وردپرس آن را به روز رسانی کنید.

برعکس بسیاری از سایت ها که با زبان های php و asp طراحی شده اند و به دلیل مشکلات در کدهای اصلی خود سایت دچار مشکل می شوند و مورد نفوذ قرار میگیرند ، در وردپرس بیشترین علتی که سایت دچار مشکل می شود مشکلات افزونه هاست.برای مثال زمانی که افزونه سئو دچار مشکل شد در یک روز چندین هزار سایت در سراسر دنیا مورد نفوذ قرار گرفت.پس از این مطلب می توان فهمید که به روز رسانی ها چقدر می تواند موثر باشد.

نکته دیگری که لازم است در مورد افزونه ها بدانید این است که ، زمانی که قصد نصب کردن نرم افزاری از مخزن وردپرس را دارید به تاریخ آخرین به روز رسانی آن دقت کنید.برای مثال به تصویر زیر که از محل افزودن افزونه ها گرفته شده دقت کنید.

<p>نصب</p> <p>اکسپت</p> <p>جزئیات بیشتر</p> <p>Akismet checks your comments against the Akismet Web service to see if they look like .spam or not</p> <p>بدست Automattic</p> <p>تازه ترین به روزرسانی: 4 هفته قبل</p> <p>با نگارش وردپرس شما سازگار است ✓</p> <p>بیش از یک میلیون نصب فعال (516) ★★★★★</p>	<p>نصب</p> <p>Theme Check</p> <p>جزئیات بیشتر</p> <p>A simple and easy way to test your theme for all the latest WordPress standards and practices. A great theme development tool</p> <p>بدست Otto42, pross</p> <p>تازه ترین به روزرسانی: 2 هفته قبل</p> <p>با نگارش وردپرس شما سازگار است ✓</p> <p>بیش از یک میلیون نصب فعال (135) ★★★★★</p>
<p>نصب</p> <p>bbPress</p> <p>جزئیات بیشتر</p> <p>bbPress is forum software, made the WordPress way</p> <p>بدست The bbPress Community</p> <p>تازه ترین به روزرسانی: 1 ماه قبل</p> <p>با نگارش وردپرس شما سازگار است ✓</p> <p>بیش از 300,000 نصب فعال (190) ★★★★★</p>	<p>نصب</p> <p>WP Super Cache</p> <p>جزئیات بیشتر</p> <p>A very fast caching engine for WordPress .that produces static html files</p> <p>بدست Automattic</p> <p>تازه ترین به روزرسانی: 1 ماه قبل</p> <p>با نگارش وردپرس شما سازگار است ✓</p> <p>بیش از یک میلیون نصب فعال (827) ★★★★★</p>

همان طور که در تصویر مشاهده می کنید این افزونه ها برای نصب مناسب هستند زیرا به ترتیب 2 هفته ، 4 هفته و 1 ماه پیش به روز رسانی شده اند و ورژن جدیدی را منتشر کرده اند که نشان از فعال بودن تیم برنامه نویسی آنها دارد. اما حالا به تصویر زیر توجه کنید.

<p><input type="button" value="نصب"/></p> <p>SEO Ready Links Export</p> <p>جزییات بیشتر</p> <p>SEO Ready Links is an SEO tool that exports a list of pages and blog post urls in your website for download</p> <p>بدست Ultranooodle Technologies</p>	<p><input type="button" value="نصب"/></p> <p>SEO All</p> <p>جزییات بیشتر</p> <p>一款真正意义上的面向中文用户的多功能SEO插件</p> <p>بدست Naizui</p>
<p>تازه‌ترین به‌روزرسانی: 8 ماه قبل</p> <p>با نگارش وردپرس شما آزمایش نشده است</p> <p>(2) ★★★★★</p> <p>+100 نصب فعال</p>	<p>تازه‌ترین به‌روزرسانی: 1 سال قبل</p> <p>با نگارش وردپرس شما آزمایش نشده است</p> <p>(0) ☆☆☆☆☆</p> <p>+0 نصب فعال</p>

همان طور که مشاهده می کنید این افزونه ها 8 ماه پیش و 1 سال پیش به روز رسانی شده اند. با اندکی توجه به این نتیجه میرسیم که احتمال این که در این مدت زمان طولانی دچار حفره امنیتی شده باشند بسیار زیاد است پس نصب کردن آنها منطقی نیست. البته این تنها راه برای پی بردن به این نکته نیست و راه های دیگری مثل بررسی سایت های ثبت اکسپلویت وجود دارد.

ابتدا باید شما را با مفهوم اکسپلویت آشنا کنم.

اغلب موارد نفوذگرها و برنامه نویس ها هنگامی که سعی به نفوذ به یک کامپیوتر یا یک برنامه را دارند مداوم به آنها داده هایی را تحویل می دهند که برنامه آنها را پردازش کند و خروجی خود را نمایش دهد در این هنگام نفوذگر با تناسب بستن میان داده ها و خروجی ها به عملکرد کلی برنامه پی برده و سعی می کند که با داده هایی که برنامه برای انجام آنها دچار خطا می شود به انها صدمه وارد کند. و از جهتی چون چک کردن برنامه های مختلف و کدها وقت زیادی را می گیرد فرد نفوذگر وقتی نحوه ی صدمه زدن به برنامه را کشف کرد برنامه ای را برای این منظور می نویسد که خودکار کارهای مورد نظر وی را انجام دهد. به همین دلیل هنگامی که یک مشکل امنیتی پیدا می شود فرد برنامه نویس کدی را با مضمون اکسپلویت قرار می دهد که نقش وی را بهتر و سریع تر انجام دهد.

به زبان ساده تر اکسپلویت ها کدهای مخربی هستند که نفوذگران از آنها برای نفوذ استفاده می کنند.

این اکسپلویت ها می توانند برای افزونه های وردپرس نیز استفاده شوند. برای مشاهده نمونه ای از

این اکسپلویت ها به سایت معتبر exploit-db.com مراجعه می کنیم.

با ورود به سایت با این صفحه مواجه خواهید شد.



[Home](#) [Exploits](#) [Shellcode](#) [Papers](#) [Google Hacking Database](#) [Submit](#) [Search](#)

Offensive Security Exploit Database Archive

35484

The **Exploit Database** – ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**. New to the site? [Learn about the Exploit Database](#).

Exploits Archived



همان طور که در تصویر هم مشاهده می کنید در قسمت بالا سمت راست سایت تعداد اکسپلویت های ثبت شده تا این لحظه مشخص شده است. همچنین شما می توانید از منوی بالای بر روی **search** کلیک کنید تا موردی که مد نظر دارید را جستجو کنید.

با کلیک بر روی گزینه جستجو به این صفحه هدایت خواهید شد.

Search the Exploit Database

Search the Database for Exploits, Papers, and Shellcode. You can even search by **CVE** and **OSVDB** identifiers.

I'm not a robot  [Privacy](#) [Terms](#)

[Advanced search](#)

در کادر اول می توانید اسم افزونه ای که مدنظر دارید را وارد کنید تا مجموعه اکسپلویت های ثبت شده برای آن افزونه تا این لحظه را مشاهده کنید. من در کادر عبارت wordpress را وارد می کنم تا جستجو کلی تری را داشته باشم.

با وارد کردن این عبارت نتایج زیر را به من نمایش می دهد.

907 total entries
<< prev 1 2 3 4 5 6 7 8 9 10 next >>

Date ▾	D	A	V	Title	Platform	Author
2016-06-06	↓	📄	🔍	WordPress Simple Backup Plugin 2.7.11 - Multiple Vulnerabilities	php	PizzaHatHacker
2016-06-06	↓	📄	🔍	WordPress WP Mobile Detector Plugin 3.5 - Arbitrary File Upload	php	Aaditya Purani
2016-06-06	↓	-	🔍	WordPress Creative Multi-Purpose Theme 9.1.3 - Stored XSS	php	wp0Day.com
2016-06-06	↓	-	🔍	WordPress WP PRO Advertising System Plugin 4.6.18 - SQL Injection	php	wp0Day.com
2016-06-06	↓	-	🔍	WordPress Newspaper Theme 6.7.1 - Privilege Escalation	php	wp0Day.com
2016-06-06	↓	-	🔍	WordPress Uncode Theme 1.3.1 - Arbitrary File Upload	php	wp0Day.com
2016-06-06	↓	📄	🔍	WordPress Double Opt-In for Download Plugin 2.0.9 - SQL Injection	php	Kacper Szurek
2016-05-02	↓	📄	🔍	WordPress Ghost Plugin 0.5.5 - Unrestricted Export Download	php	Josh Brody
2016-04-18	↓	📄	🔍	WordPress leenk.me Plugin 2.5.0 - CSRF/XSS	php	cor3sm4sh3r
2016-04-18	↓	📄	🔍	WordPress Kento Post View Counter Plugin 2.8 - CSRF/XSS	php	cor3sm4sh3r
2016-04-01	↓	📄	✅	WordPress Advanced Video Plugin 1.0 - Local File Inclusion (LFI)	php	evait security.
2016-03-27	↓	📄	🔍	WordPress Plugin IMDb Profile Widget 1.0.8 - Local File Inclusion	php	CrashBanicot
2016-03-27	↓	📄	🔍	WordPress Photocart Link Plugin 1.6 - Local File Inclusion	php	CrashBanicot

همان طور که مشاهده می کنید تا این لحظه 907 اکسپلویت برای این سیستم مدیریت محتوا ثبت شده که در ستون اول تاریخ ثبت شدن ، در ستون وسط نام اکسپلویت و در ستون آخر نام فردی که ثبت کرده است نوشته شده است. همان طور که مشاهده می کنید بیشتر اکسپلویت های ثبت شده برای این سیستم مدیریت محتوا مربوط به افزونه ها است. مثل افزونه بک آپ گیری و

در اینجا 2 سایت که عملکردی مشابه دارند را برای شما دوستان عزیز قرار می دهم.

<https://packetstormsecurity.com>

<http://0day.today>

مقابله با اسپم (مشکل همیشگی مدیران سایت های وردپرس)

قبل از شروع بحث در این مورد پیشنهاد می‌کنم به تصویر زیر نگاه کنید.

The screenshot shows a forum interface with a search bar at the top left containing '7,046 مورد'. The main header reads 'دیدگاه‌ها' (Opinions) and 'همه | در انتظار بررسی (5,297) | تایید شده | جفتگ (73) | زباله‌دان (1)'. Below this are filters for 'کارهای دسته‌جمعی' (Group tasks), 'اجرا' (Execute), and 'همه نوع دیدگاه' (All types of opinions). The main content area displays a list of posts, each with a user profile picture, name, and details. The first post is by 'odedfbbvpa' with a profile picture of a person and details: '/anmcoffuyylw.com', 'jvxwkj@kgdtgz.com', and '46.161.9.32'. The second post is by 'cialis generico' with a profile picture of a person and details: '/compraracia1isgenericobarato.net', 'robertma34@mail.ru', and '37.113.28.34'. The third post is by 'scottienaborgj70' with a profile picture of a person and details: 'landnd.com/nike-shoes-...', '...air-max-2013-online-8_11.ht', 'sibalajdez@live.com', and '186 128 6 0'. The right sidebar contains a navigation menu with items like 'نوشته‌ها' (Posts), 'رسانه' (Media), 'پیوندها' (Links), 'برگه‌ها' (Pages), 'دیدگاه‌ها' (Opinions) with a count of 5,297, 'نمایش' (Display), 'افزونه‌ها' (Add-ons) with a count of 12, 'کاربران' (Users), 'ابزارها' (Tools), 'تنظیمات' (Settings), 'وردپرس فارسی' (WordPress Persian), 'Downloads', 'WP Security', 'WPTouch', and 'جمع کردن فهرست' (Collapse list).

در تصویر مشاهده می‌کنید که این سایت مجموعاً 7000 نظر دارد که تعداد 5300 تا از این نظرات

تایید نشده‌اند. آیا به راستی این سایت اینقدر بزرگ و محبوب است؟ خیر

این نظرات فقط اسپم هست که اگر به متن نظرات دقت کنید مشخص است.

حالا که با مفهوم کلی کار آشنا شدید به توضیح در مورد روش جلوگیری از آن می‌پردازیم.

برای رفع این مشکل کافیست افزونه دوست داشتنی Askiment را نصب کنید.

این افزونه یکی از جالب‌ترین و پرطرفدارترین افزونه‌های وردپرس است. جالب اینجاست که حتی

نیاز به دانلود و نصب هم ندارید زیرا به صورت پیش‌فرض همراه وردپرس نصب می‌شود. اما به هر

حال برای فعال‌سازی آن نیاز به یک کلید API دارید. در طراحی سایت ارزان و مبارزه با اسپم بدون

این افزونه تقریباً شانس برای مقابله ندارید. البته هنوز این افزونه جای کار دارد و گاهی نظرات

عادی هم spam شناسایی می‌شوند که شما می‌توانید به صورت دستی آنها را درست کنید.

لینک های داخل کامنت ها را nofollow کنید

یکی از اهداف اسپم کارها این است که لینک سایت خودشان را پخش کنند . شما می توانید لینک هایی که در میان دیدگاه ها (comments) قرار می گیرند را nofollow کنید، با اینکار هم سایت شما بیشتر در امان است و هم این که اسپم گذار کمتر به هدفی که مدنظر داشته می رسد، زیرا لینک های nofollow ارزش چندانی برای سئو ندارند.

با استفاده از cookie ها جلوی اسپم گذاری در نظرات را بگیرید

به پیشنهاد می کنم حتما افزونه cookies for comments را دانلود کنید، نحوه کار افزونه نیز ساده است و معمولا به جز فعال سازی کار دیگری نیاز ندارید. حالا ممکنه بپرسید فعال بودن کوکی ها چه ربطی به ضد اسپم دارد؟؟؟ معمولا spammer ها اسکریپت های خودکاری هستند که کامنت میگذارند، این اسکریپت ها برای اینکه فشار کمتری به سرورهای خود بیاورند و بتوانند سایت های بیشتری را اسپم کنند معمولا فقط یک بار فایل های static یک دامنه را دانلود می کنند، منظور از فایل های استاتیک سایت استایل ها، فایل های جاوااسکریپت و ... است. حالا اگر ما یک مکانیزم کوکی برای بخش نظرات داشته باشیم، اگر یک کاربر اسپمر را شناسایی کنیم می توانیم جلوی اسپم گذاری بیشتر را بگیریم.

با تکنولوژی Honeypot اسپم هارو شناسایی کنید!

روبات های spammer معمولا به گونه ای طراحی شده اند که در قسمت کامنت سایت هر فیلدی را که ببینند پر می کنند ، اما honeypot یک ترفند دارد و اون هم این است که یک فیلد اضافه به بخش کامنت ها اضافه می کنند که فقط و فقط خود spammer script ها قادر به دیدن آن هستند و

نه کاربران عادی، در نتیجه اگر این فیلد در هنگام فرستادن دیدگاه پر شود می فهمیم که کاربر ما اسپمر است.

از کد امنیتی Captcha استفاده کنید

بهترین افزونه در این زمینه WP-reCAPTCHA است که با زدن نام این افزونه در پنل وردپرس می توانید آن را مشاهده کنید و نصب کنید. با استفاده از این افزونه کاربرها مجبور می شوند با وارد کردن حروف امنیتی تصویر در هم ریخته کامنت بگذارند که می تواند کمک زیادی به جلوگیری از اسپم در طراحی سایت ارزان کند.

گذاشتن کامنت در صفحات رسانه ها را ممنوع کنید

وردپرس به صورت پیشفرض برای هر رسانه مثل تصویر، صوت و ویدیو، یک صفحه خاص به نام صفحه رسانه ایجاد می کند که در صورت رفتن به آن صفحه کاربر حتی می تواند در آن دیدگاه نز وارد کند. شما باید برای جلوگیری از هرزنامه در بخش نظرات، باید بخش نظرات در این صفحات را غیر فعال کنید.

یک روش دیگر به جای کد تایید برای مبارزه با SPAM

توصیه من به شما استفاده از Captcha است، اما همه ما از اینکه به اجبار ، حروف داخل تصاویر عجیب و غریب را بخوانیم متنفر هستیم.پس علاوه بر روشی که گفته شد یک روش دیگر را پیشنهاد می کنم. استفاده از پلاگین Math Quiz راه حل دیگر ما است.. این افزونه اجازه می دهد یک مسئله خیلی خیلی ساده ریاضی را برای کاربران طرح کنید مثلا نتیجه $2 + 2$ را وارد کنید. نکته قابل توجه این که شما دو تنظیم متفاوت از این افزونه را دارید و می توانید سوال ریاضی امنیتی را ، هم به

صورت تصویر و هم به صورت متن در کامنت ها قرار دهید که در صورتی که از تصویر استفاده کنید ، ضریب امنیتی بالاتری دارد.

آشنایی با حملات منع سرویس (DDos) و راه های مقابله با آن

ابتدا لازم است بدانیم حمله DDOS چیست؟ حمله ddos یا dos مخفف (denial of service attack) به زبان ساده یعنی سرازیر کردن تقاضاهای زیاد به یک سرور (کامپیوتر قربانی یا هدف) و استفاده بیش از حد از منابع (پردازنده، پایگاه داده، پهنای باند، حافظه و...) به طوری که سرویس دهی عادی آن به کاربرانش دچار اختلال شده یا از دسترس خارج شود (به دلیل حجم بالای پردازش یا به اصطلاح overload شدن عملیات های سرور)، در این نوع حمله ها در یک لحظه یا در طی یک زمان به صورت مداوم از طریق کامپیوترهای مختلف که ممکن است خواسته یا حتی ناخواسته مورد استفاده قرار گرفته باشند، به یک سرور (با آی پی مشخص) درخواست دریافت اطلاعات می شود و به دلیل محدود بودن قدرت پردازش سرور به کاربران در وضعیت عادی (یعنی قدرت سرور را به تعداد کاربرانش در حالت عادی در نظر گرفته اند نه حالت غیر طبیعی)، مثل حالتی که کامپیوترهای رومیزی دچار کندی یا توقف کامل می شوند، دچار وقفه در سرویس دهی یا حتی down شدن آن می شود.

چه کسانی حمله ddos را انجام می دهند؟

اصولا حمله های ddos با انگیزه های متفاوت ممکن است توسط یک یا چند نفر و یا حتی گروهی از افراد صورت گیرد، اما آماری که تا به امروز به ثبت رسیده، حکایت از انگیزه های بیشتر فردی یا چند نفره داشته است، به طور مثال ممکن است افرادی برای از سر راه برداشتن ناجوانمردانه رقیبشان در وب، دست به این نوع اعمال بزنند تا مخاطبان آن سایت یا سرور دچار دلسردی شده و از آن فاصله بگیرند یا برعکس عده ای نفوذگر، خیرخواهانه به سایتی ضد اجتماعی یا به فرض جنگ طلب حمله ddos کنند، لذا گستره افراد و انگیزه ها، بسته به نوع مورد، متفاوت خواهد بود، اما آنچه مسلم

است معمولا انسان ها پشت این حملات هستند یا ترکیبی از اندیشه انسان و به کارگیری سیستم، سرور و ابزارهای خاص (DDOS tools) دست به دست هم می دهند تا یک حمله ddos شکل بگیرد.

علائم حمله ddos چیست؟

خوشبختانه یکی از موارد مثبت این نوع حملات این است که به سرعت می توان به نحوه عملکرد سرویس مشکوک شد و جلوی اختلال بیشتر را گرفت، پس از اینکه سروری مورد حمله ddos قرار می گیرد ممکن است با توجه به اهداف و شیوه به کار رفته یک قسمت از منابع یا همه ی قسمت های آن دچار اختلال شود، در زیر لیستی از این علائم را ذکر می کنیم.

– کندی در پاسخگویی به درخواست ها

سروری که مود حمله قرار گرفته باشد، معمولا خیلی کند و با وقفه به درخواست بارگذاری صفحات پاسخ می دهد، البته این نشانه همیشه دلیل حمله ddos نیست، چرا که این اتفاق به طور طبیعی نیز برای سرورها و سایتهای با بازدید بالا ممکن است رخ دهد یا کنترل این امر بستگی زیادی به قدرت سخت افزاری سرور و تنظیمات آن دارد.

– عدم اتصال به پایگاه داده

گاهی ممکن است صفحات استاتیک که نیازی به اتصال پایگاه داده ندارند به راحتی بارگذاری شوند، ولی اتصال به پایگاه داده برای صفحات داینامیک برقرار نشود، در چنین مواقعی معمولا پیام تکمیل ظرفیت اتصال به پایگاه داده یا too many connection ظاهر خواهد شد، بهترین کار در چنین حالتی این است که با تنظیم یک دستور هدر HTTP 500، به ربات های جستجوگر بگوییم که سایت ما فعلا دچار مشکلی است و بعدا مراجعه نمایید!، چرا که در غیر اینصورت با وجود down بودن دیتابیس

سرور، ربات ها با دریافت وضعیت HTTP 200، صفحه خالی را ایندکس می کنند که این حالت اصلا مناسب نیست، در php این کار را با دستورات header می توان انجام داد.

```
header('HTTP/1.0 500 Internal Server Error');header('HTTP/1.0 500 Internal Server Error;('
```

– مصرف بیش از حد منابع سرور

یکی دیگر از نشانه های حمله ddos می تواند مصرف بیش از حد و غیر طبیعی منابع سرور مثل حافظه و یا پهنای باند در یک بازه زمانی کوتاه باشد.

– افزایش انفجاری درخواست ها

یکی دیگر از نشانه های حمله ddos، وجود شمار زیادی درخواست http به سرور است که با مشاهده فایل log و قسمت آمار، می توان به این موضوع پی برد.

– اختلالات در سرویس های جانبی نظیر ایمیل

گاهی مواقع حملات ddos سرویس های جانبی یک سرور نظیر سرویس ایمیل را هدف می گیرند، در این مواقع ارسال و دریافت ایمیل ممکن است به کندی صورت گیرد یا دچار وقفه شود، البته همانطور که گفتیم، هر وقفه و اختلالی به معنی حمله ddos نیست، تنها به عنوان یک نشانه می توان آن را محسوب کرد.

در حمله ddos از چه روش هایی استفاده می شود؟

چند روش به عنوان شایع ترین ها در این نوع حملات استفاده می شود، که در زیر به آنها به طور مختصر و جهت آشنایی اشاره می کنیم:

– روش Ping Flood یا طوفان درخواست ها

در این شیوه مهاجم سعی می کند با ارسال درخواست ها (یا بسته های ping) به سمت کامپیوتر هدف (قربانی)، و با تکرار این عمل، کل منابع سرور را اشغال کند تا در نهایت آن را به طور کامل از کار بیندازد، در این شیوه معمولا از کامپیوترهای موجود در یک شبکه یا از سرورهایی به طور همزمان درخواست به سمت سرور قربانی ارسال می شود تا در نهایت موجب از کار افتادن آن شود.

– روش Smurf attack یا استفاده از نقص تنظیمات

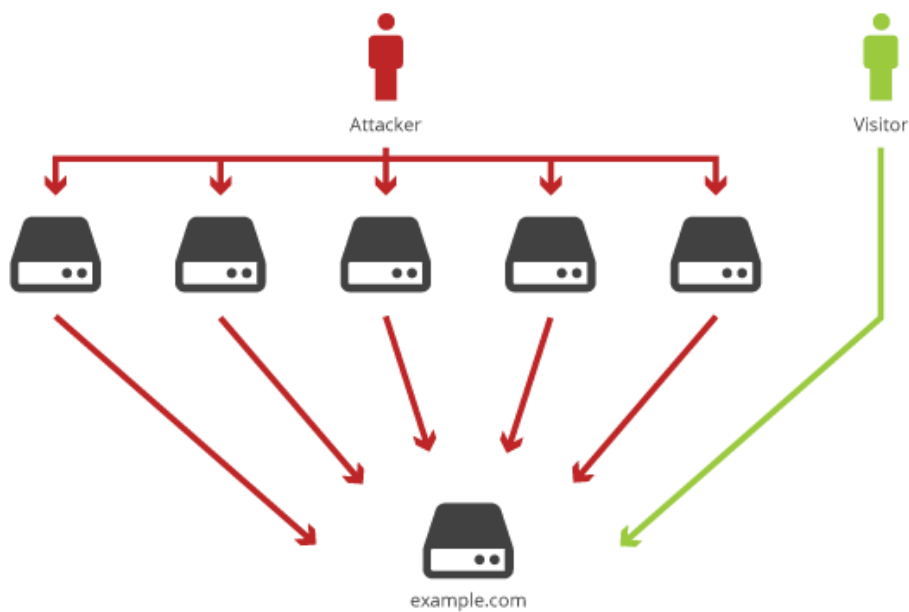
یک Smurf attack نوع خاصی از طوفان درخواستها به یک سرور است که طی آن به دلیل وجود ضعف در تنظیمات سرویس، اجازه ارسال بسته هایی از اطلاعات به تمام کامپیوتر های موجود در یک شبکه در عوض ارسال آن به یک کامپیوتر خاص از طریق آدرس Broadcast آنها است، آدرس Broadcast می تواند به عنوان مثال آی پی اشتراکی سایت های موجود در یک سرور باشد؛ در این حالت اگر تنظیمات سرور به درستی انجام نشده باشد، ارسال یک درخواست به این آی پی، موجب تقسیم شدن آن بین تمام زیر شاخه ها و در نتیجه overload شدن سرور می شود.

– حملات موسوم به SYN flood یا SYN

روش اخیر نیز در عمل مشابه با موارد گفته شده است، با این تفاوت که در اینجا مهاجم با ارسال درخواستهایی از نوع بسته های TCP/SYN در پشت چهره ای عادی و تایید شده به عنوان یک کاربر معمولی، از سرور تقاضای اتصال می کند که پس از ارسال پاسخ درخواست، هیچ جوابی به پاسخ سرور داده نمی شود تا اتصال نیمه باز همچنان برقرار باشد (سرور در انتظار پاسخ مهاجم مدتی صبر می کند)، در این بین با افزایش این اتصالات نیمه باز، منابع سرور اشغال شده و نهایتا موجب بروز اختلال و از کار افتادن آن می شود.

– روش Teardrop attacks یا Teardrop attacks

در این شیوه رشته ای از آی پی های ناقص به هم متصل شده و شبیه به هم را به سرور ارسال می کنند که اگر تنظیمات قسمت TCP/IP fragmentation re-assembly سرور دچار نقص در تشخیص آنها باشد، موجب بروز مشکل اضافه بار یا overload در سرور خواهد شد.



حمله ddos چقدر طول می کشد؟

یکی از سوال های همیشگی در چنین موقعیت هایی این است که یک حمله ddos چقدر طول می کشد و ظرف چه مدتی به پایان می رسد، پاسخ این سوال نیز می تواند یک جمله باشد: تا زمانی که به پایان رسد! این موضع بستگی به میزان سماجت مهاجم و ضعف مدافع دارد، یعنی اگر مهاجم بر ادامه حملات خود اصرار داشته باشد و در مقابل مدافع که همان مدیران سرور هستند نتوانند از عهده کنترل اوضاع بر آیند، ممکن است حمله ddos ساعت ها یا روزها به طول انجامد، در خوش بینانه ترین حالت ظرف چند دقیقه و در بدترین حالت چندین و چند روز و به دفعات ممکن است طول بکشد.


برای جلوگیری از حمله ddos چه کارهایی را انجام دهیم؟

واقعیت این است که کنترل حمله های ddos پس از وقوع کمی دشوارتر از پیشگیری از آن است، امروزه در سایتها و انجمن های زیادی به افراد آموزش شیوه های نفوذ و ایجاد حمله های ddos داده می شود که این امر با افزایش شمار کاربران اینترنت (که می توانند میانجی و قربانی بالقوه برای حمله به سرورها باشند) رو به گسترش است، البته آسیب پذیری در این رابطه، بیشتر به امنیت سرور برمی گردد تا به امنیت سایت شما، در مورد سرور می توان پس از اطمینان از حمله ddos، آی پی هایی را که بیشترین تقاضا را به سرور داشته اند و ناشناس هستند، توسط فایروال ها بلاک و مسدود کرد، یا با نصب بسته های امنیتی خاص و به روزرسانی و ارتقا سخت افزاری و نرم افزاری، آسیب پذیری سرور را کاهش داد، آگاهی از روند عادی سرور نیز می تواند کمک بزرگی در این خصوص محسوب شود، چرا که اگر مدیر سرور نسبت به عادی یا غیر عادی بودن ترافیک آن، آشنایی داشته باشد، به سرعت می تواند پی به وجود این نوع حمله ها ببرد و در جهت رفع آن برآید، به عنوان یک کاربر در سرویس های میزبانی وب، بهترین کار این است که به محض مشکوک بودن به چنین حمله هایی، موضوع را به هاست خود اطلاع دهید تا در کوتاه ترین زمان جلوی آن گرفته شود.

البته این ها تنها اقدامات ما نخواهند بود. در وردپرس افزونه ای برای این کار تعبیه شده که می توانید از مسیر زیر آن را دانلود و روی وب سایت خود فعال کنید.

<https://wordpress.org/plugins/cloudflare>

بعد از وارد شدن به آدرس بالا صفحه ای به این شکل مشاهده می کنید که می توانید با زدن دانلود آن را دریافت کنید.



The CloudFlare WordPress Plugin ensures your WordPress blog is running optimally on the CloudFlare platform.

[Download Version 1.3.24](#)

[Description](#) [Installation](#) [Changelog](#) [Stats](#) [Support](#) [Reviews](#) [Developers](#)

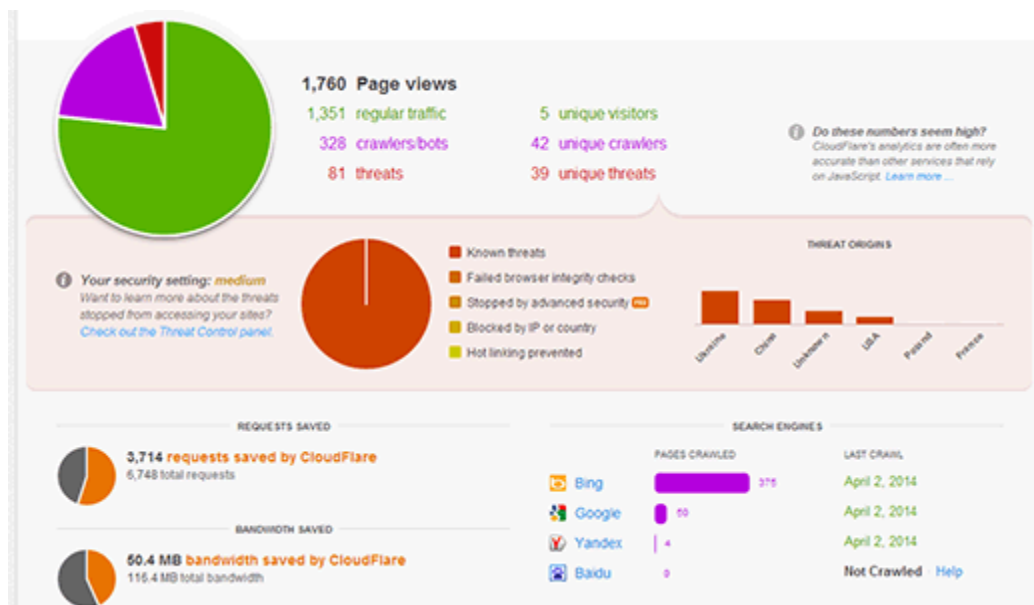
نکته ای که در اینجا حائز اهمیت است این است که این افزونه به صورت 100% توان مقابله با این حملات را ندارد. اگر شما می خواهید قدرت این افزونه را افزایش دهید بهتر است به آدرس زیر مراجعه و اکانت VIP مربوط به این افزونه را دریافت کنید که قدرت بیشتری دارد.

<https://www.cloudflare.com>

در قدم بعدی باید توضیحاتی در مورد این افزونه و نحوه نصب و پیکربندی آن به شما دوستان عزیز ارائه کنم.

ابتدا شما را بیشتر با CloudFlare آشنا می کنم. CloudFlare یک سرویس چند منظوره افزایش سرعت ، امنیت و توان وب سایت و سرور است . همچنین دارای قابلیت content delivery network با مخفف CDN می باشد . بسیاری از کاربران کلودفلر را به عنوان یک محافظ در مقابل حملات دی داس (DDoS Protection) می شناسند.

این سرویس دارای دو پنل است که به صورت رایگان و ماهیانه که با پرداخت هزینه در اختیار مشتریان قرار می گیرد.



تفاوت CloudFlare و MaxCDN چیست ؟

CloudFlare و MaxCDN هر دو دارای سرویس های متفاوتی هستند . MaxCDN نیز یکی از سرویس های CDN است که مناسب ترین گزینه برای کاربران می باشد . کلودفلر ، بیشتر بر روی امنیت و کنترل اسپم ها متمرکز شده است

خدمات MaxCDN با استفاده از DNS وب سایت شما راه اندازی میشه . CloudFlare نیز از طریق DNS راه اندازی خواهد شد و کلودفلر از شما می خواهد که DNS وب سایت خود را به سرور های خودش وصل کنید

کلودفلر برای بهینه سازی سرعت صفحات وب سایت شما و جلوگیری از ربات های مخرب ، حمله ها ،
قطعی سایت و ... بهتر است . MaxCDN برای افزایش سرعت و بازدید تمام جهان از وب سایت شما
بهتر است

معایب و مشکلات CloudFlare

کاربرانی که کلودفلر را اسفاده کرده ، گزارش کرده اند که تفاوت قابل توجهی در بارگذاری صفحات
مشاهده نکرده اند . همچنین بسیاری شکایت کرده اند که کلودفلر برخی از بازدیدکنندگان قانونی را
برای دسترسی به وب سایت خود بلوک میکند و این یک تجربه بد برای کسانی می شود که ممکن است
برای اولین بار از این وب سایت دیدن می کنند و ممکن است هرگز دیگر به آن مراجعه نکنند.

آموزش اضافه کردن CloudFlare به سایت وردپرس

قبل از راه اندازی کلودفلر ، به منظور بهبود سرعت وب سایت ، مطمئن شوید که سرور سایت شما
آهسته نیست . اگر شما فکر می کنید که سرور شما آهسته و مناسب نیست پس در قدم اول باید آن
را تعویض کرده و سرور های ارائه دهنده وردپرس منتقل کنید .

برای راه اندازی کلودفلر شما اول باید در وب سایت آن ثبت نام کنید . به سایت cloudflare.com
رفته و بر روی لینک ثبت نام کلیک کنید.



Create a CloudFlare Account

Email

Confirm Email

Password

Confirm Password

I agree to [CloudFlare's terms and conditions](#) and [privacy policy](#).

[Create Account](#)

[< Log in](#) [Help](#)

اطلاعات مورد نیاز را برای ثبت نام وارد کرده و در نهایت بر روی گزینه Create account now کلیک کنید . در قسمت Add a Webiste آدرس وب سایت خود را وارد کنید.

Get Started With CloudFlare



Add Website

Add your first website. You can add more after this signup process.



Add DNS Records

We will scan your DNS records. You can modify your DNS records before moving on.



Select Plan

Select the plan that meets your needs.



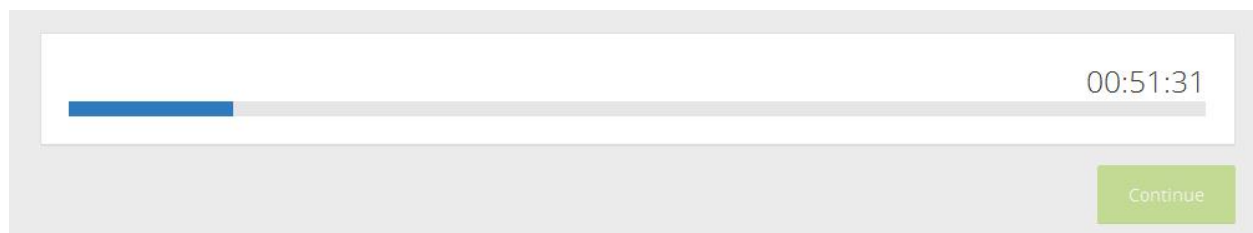
Update Nameservers

Sign into your registrar to update your current nameservers with CloudFlare nameservers.

Add a website

There is no downtime when you add a domain.

در این قسمت کلودفلر قصد اسکن سایت شما را دارد تا DNS های شما شناسایی شوند . این کار در حدود ۶۰ ثانیه طول میکشه و در طول این زمان یک ویدیو اطلاعاتی در مورد کلودفلر برای شما نمایش داده خواهد شد و شما آموزش می دهد که چطور کلودفلر را راه اندازی کنید.



پس از اسکن وب سایت شما ، کلودفلر یک لیست از تمام DNS ها و رکورد های ثبت شده را به شما نشان می دهد . در عکس زیر مشاهده می کنید که کلودفلر از شما ثبت DNS و دامنه را می خواهد . در صورتی که تمایل دارید DNS ها از طریق CloudFlare انتقال پیدا کنند بر روی آیکن نارنجی رنگ کلیک کنید . رنگ خاکستری رنگ نیز DNS هایی هستند که کلودفلر را دور زدند . شما باید مطمئن شوید که دامنه و زیر دامنه اصلی بر روی کلودفلر فعال هستند.

Select a CloudFlare Plan

Select a CloudFlare Plan

Free Website \$0/month

- ✔ Basic Security Protection
- ✔ Fast Website Performance
- ✔ SSL (Limited Browsers)
- ✔ Always Online

[Learn More >](#)

Pro Website \$20/month

کلودفلر همچنین FTP و SSH را در دامنه شما اضافه خواهد کرد . اگر دامنه شما برای اتصال از FTP و SSH استفاده می کند نام آن ها به این شکل خواهد بود . برای FTP به این شکل `ftp.yourdomain.com` و برای SSH به این صورت `ssh.yourdomain.com` خواهد بود

در این مرحله ما در قسمت Choose a plan را به صورت پیش فرض ، پلن Free را انتخاب می کنیم ، سپس روی دکمه continue برای ادامه راه اندازی کلیک می کنیم.

تغییر نام سرور ها به CloudFlare

نکته : تغییر نام سرور ها ممکن است زمان زیادی طول بکشد و به همین دلیل ممکن است وب سایت شما برای برخی از کاربران غیر قابل دسترس باشد.

برای تغییر نام سرور در دامنه خود نیاز به حساب کاربری هاست خود دارید . بسیاری از هاست ها دارای پنل مدیریت هستند که تنظیمات را شما در پنل مدیریت باید انجام دهید .

Change Your Nameservers

Your website will not experience any downtime when you change your nameservers.

Please visit your registrar's dashboard to change your nameservers to the following.

i The transfer process can take up to 24 hours. There will be no downtime when you switch your name servers. Traffic will gracefully roll from your old name servers to the new name servers without interruption. Your site will remain available throughout the switch.

Current Nameservers

ns1.pardazmizban.com

ns2.pardazmizban.com

Change Nameservers to:

ed.ns.cloudflare.com

emma.ns.cloudflare.com

[Help](#) ▶

Cancel

Continue

در مرحله آخر به شما دو DNS از طرف سایت کلود فلر ارائه میشود که باید آنها را به جای DNS های دامنه ای که به کلود فلر معرفی کرده اید قرار دهید یا در واقع DNS جدید کلود فلر را با DNS های قبلی جایگزین کنید و پس از آن ، روی دکمه یا گزینه continue کلیک کنید . در نهایت پس از بروز شدن DNS های دامنه ، شما به سرور کلود فلر متصل می شوید.

روش دیگر برای مقابله با دیداس که ساده ترین راه و می توان گفت سریع ترین راه است block کردن آیپی است که دیداس از طرف آن انجام شده.تصویر زیر را مشاهده کنید.

بازدید در یک نگاه	
1 کاربر(های) حاضر:	
بازدید کننده	بازدید
18	30,507
67	31,132
امروز:	
دیروز:	

آمار بازدید در این سایت کاملا نمایانگر این مسئله است که سایت زیر حمله دیداس قرار گرفته. چون بازدید 30 هزار تایی آن هم برای 18 بازدید کننده مسئله ای طبیعی نیست. اما راه چاره چیست؟ ابتدا باید ببینیم این بازدیدهای جعلی یا بهتر است بگوییم حملات از چه آیپی صورت گرفته است. برای این کار از قابلیت‌ای که در افزونه آمار وردپرس وجود دارد استفاده می‌کنیم.

Top Visitors							
رتبه	بازدیدها	برجم	کشور	آیپی	عامل کاربر	بلت فرم	نگارش
1	29217	?	Unknown	195.154.240.246	MSIE	Windows	9.0
2	1258	?	Unknown	74.91.17.218	Unknown	Unknown	Unknown
3	6	?	Unknown	2.187.253.17	Unknown	Unknown	Unknown
4	3	?	Unknown	188.68.48.243	Java	Unknown	1.8.0
5	3	?	Unknown	69.28.92.242	Firefox	Windows	48.0
6	2	?	Unknown	184.73.124.174	Chrome	Macintosh	50.0.2661.102
7	2	?	Unknown	134.249.51.75	Firefox	Linux	38.0
8	2	?	Unknown	54.149.172.209	Chrome	Macintosh	50.0.2661.102
9	2	?	Unknown	54.90.13.230	Chrome	Macintosh	50.0.2661.102
10	2	?	Unknown	54.194.32.54	Chrome	Macintosh	50.0.2661.102

همان طور که در تصویر مشاهده می‌کنید بیشتر بازدیدها از یک آیپی مشخص صورت گرفته. پس تنها با مسدود کردن این آیپی مشکل به صورت موقت حل می‌شود. برای مسدود کردن افزونه‌های مختلفی را در وردپرس در اختیار داریم. اما من پیشنهاد می‌کنم از خود است این کار را انجام دهید. ابتدا وارد محیط cpanel شوید و از قسمت security روی گزینه IP Blocker کلیک کنید.



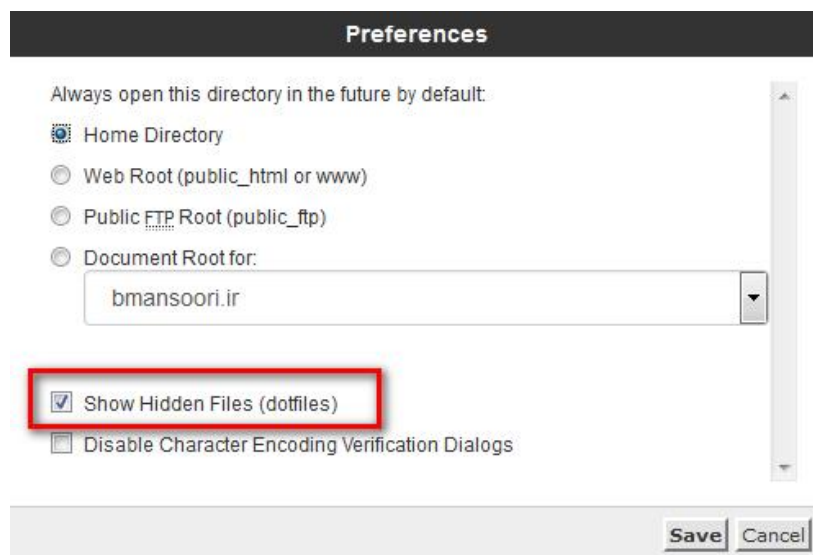
در صفحه باز شده کافایت آدرس آبیی که به دست آوردید را در کادر وارد کنید و ثبت کنید. آن آبیی برای همیشه در لیست بلاک سایت شما قرار میگیرد و حمله متوقف می شود.

فایل htaccess چیست؟

امروزه در اکثر سیستم های مدیریت محتوا مثل وردپرس یک فایل در شاخه اصلی هاست به اسم htaccess وجود دارد. این فایل را در حقیقت با نام distributed configuration files می شناسند و در واقع برای کنترل آپاچی هستند که روی یک شاخه و تمام زیر شاخه های آن عمل می کند. این فایلها برای کارکرد در کنار فایلهای معمولی HTML یا PHP قرار میگیرن ، میشه گفت این فایل اسم ندارد بلکه فقط از بخش پسوند تشکیل شده و به صورت htaccess دیده میشود.

htaccess یک فایل مخفی است که می تواند در هر فولدري باشد و همانطور که ذکر شد عملیات های سرور مربوط به آن فولدر و زیر شاخه هایش را تنظیم میکند ، مثلا میتوانید دسترسی یکسری از فایل ها را محدود کنید تا از آن فایل ها محافظت شود ، URL را تنظیم کنید یا مدیریت فایلهاى قابل کش و خصوصیات آنها بپردازید و...

این فایل در سرور به صورت فایل مخفی است و برای نمایش آن کافی است مثلاً در سی پنل ، هنگامی که بر روی file manager کلیک میکنید تیک گزینه show hide files را فعال کنید تا بعد از باز شدن پنجره مدیریت فایلها تمام فایل های مخفی قابل رویت باشند.



آموزش htaccess ، امنیت و مدیریت بهینه وردپرس با آن

در این آموزش برای اینکه تنظیمات برای تمام فولدرهای بخش اصلی سایت اعمال بشه ، من از فایل htaccess موجود در فولدر public_html استفاده میکنم. حال اگه این فایل در پوشه public_html شما وجود نداشت کافی هست از منوی سی پنل گزینه newfile را انتخاب کنید و سپس htaccess را وارد کنید ، باز تاکید میکنم این فایل نام ندارد و نقطه را باید در ابتدای محل درج عنوان وارد کنید و سپس عبارت htaccess را تایپ کنید.

اگر این فایل از قبل موجود بود بهتر است یک کپی از آن را به عنوان بک آپ ذخیره کنید. و در صورت وجود کد داخل آن بهتر است در آخر خط یک بار اینتر را بزنید و دستورات آموزش داده شده در اینجا را بعد آن وارد کنید.

1) محافظت از خود فایل .htaccess :

برای جلوگیری از سرقت اطلاعات خود فایل htaccess کد زیر را در ابتدای فایل htaccess قرار می دهیم :

```
<files ".htaccess">  
order allow,deny  
deny from all  
</files>
```

2) جلوگیری از سرقت فایل ها و فولدرهای درون هاست :

بیشتر وقت ها اطلاعاتی مثل فایل های قالب اختصاصی شما که بر روی هاست قرار دارند و یا فایل هایی که به صورت Zip شده در هاست خود ذخیره کرده اید به راحتی با مرور هاست شما توسط سایرین کشف و به سرقت میروند. برای جلوگیری از این امر کد زیر را در انتهای فایل htaccess قرار دهید.

Options All -Indexes

3) معرفی زبان پیشفرض (DefaultCharset) :

برای اینکه زبان پیشفرض استفاده شده را به مرورگرها معرفی کنید در بیشتر مواقع آن را در قسمت هدر کدهای سایت قرار میدهید. با دستور کوتاه زیر به آپاچی میگوییم که همیشه صفحات را با زبان خاصی ارسال کن. این عمل برای سئو سایت تاثیر خوبی داره.

```
# pass the default character set  
AddDefaultCharset utf-8
```

4) تعیین صفحات سفارشی برای صفحات خطا :

با دستور زیر می توانید صفحاتی را که برای نمایش هنگام ایجاد خطا، طراحی و در پوشه error قرار داده اید را جایگزین صفحات خطای پیشفرض سرور کنید و خطای مورد نظر خودتان را به کاربر نشان دهید. معرفی و تعیین صفحات خطا برای سئو سایت تاثیر خوبی دارد.

```
ErrorDocument 401 /error/401.php  
ErrorDocument 403 /error/403.php  
ErrorDocument 404 /error/404.php  
ErrorDocument 500 /error/500.php
```

چند خطای آپاچی برای نمونه :

- خطای ۴۰۱ : دسترسی به آدرس وارد شده غیر مجاز است.
- خطای ۴۰۳: دسترسی به این آدرس ممنوع می باشد.
- خطای ۴۰۴: آدرس مورد نظر یافت نشد.
- خطای ۵۰۰: خطای داخلی سرور بوجود آمده است.

5) بن کردن اسپم ها با htaccess (محدودیت دسترسی از طریق آی پی) :

از آنجا که دیدگاه های اسپم واقعا روی اعصاب هستند و مخصوصا اگر سایتتان پیشرفت داشته باشد این دیدگاه ها به صورت وحشیانه هجوم میاورند که ما کلا میخواهیم آی پی آن ها را مسدود کنیم.

```
<Limit GET POST>  
order allow,deny  
deny from 200.49.176.139  
allow from all  
</Limit>
```

دستور “allow from all” یعنی همه آی پی ها به جز آی پی های مسدود شده دسترسی دارند. اگه قصد داشته باشیم فقط به آی پی های خاص اجازه دسترسی بدهیم کافیسست ، کدی به این شکل وارد کنید “allow from 188.50.38.143” و به جای آی پی درج شده آی پی مورد نظر خودتان را وارد کنید.

با دستور “deny from 200.49.176.139” نیز اجازه دسترسی این آی پی را میگیریم که می توانید به هر تعداد که دوست داشتید از آن زیر هم اضافه کنید. با این کد هم دیگه هیچ آی پی اجازه ورود نخواهد داشت حتی خود شما “deny from all”.

نکته : بعضی مواقع قرار دادن “<Limit GET POST>” و “<Limit/>” در ابتدا و انتهای تعیین دسترسی ها مشکلاتی را ایجاد میکند که در این صورت آنها را از ابتدا و انتهای کدها بردارید.

6) جلوگیری از ارسال دیدگاه اسپم در وردپرس :

افزونه Askimet افزونه شناخته شده ای در زمینه جلوگیری از ارسال اسپم هست که در بسته اصلی خود وردپرس هم وجود دارد ، اما شما میتوانید با استفاده از کد زیر از ارسال هرزنامه به سایت جلوگیری کنید. دقت داشته باشید که در خط چهارم آدرس سایت خودتان را وارد کنید.

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} POST
RewriteCond %{REQUEST_URI} .wp-comments-post\.php*
RewriteCond %{HTTP_REFERER} !.*yourblog.com.* [OR]
RewriteCond %{HTTP_USER_AGENT} ^$
RewriteRule (.*) ^http://%{REMOTE_ADDR}/$ [R=301,L]
```

7) حذف category از آدرس وردپرسی شما :

شاید شما هم دوست داشته باشید کلمه /category/ را از آدرس وردپرسی خودتان حذف کنید. این کار علاوه بر اینکه باعث جمع و جور شدن URL شما میشود تا حدودی هم در سئو سایت شما موثر است.

```
RewriteRule ^category/(.+)$ http://www.yourblog.com/$1 [R=301,L]
```

8) تغییر عنوان و پسوند فایل پیشفرض index در هنگام بارگذاری :

حتما تا حالا متوجه شده اید که در هنگام فراخوانی یک آدرس پیشفرض یکی از فایل های index.html یا index.php یا ... بارگزاری میشوند. حال اگه دوست داشتین این سنت رو بشکنین می تونین از کد زیر استفاده کنید. با قرار دادن آن هنگام فراخوانی به دنبال file.php میگردد و اگر نبود به دنبال file.html خواهد بود.

```
DirectoryIndex file.php file.html
```

9) بالا بردن امنیت فایل wp-config در htaccess :

برای جلوگیری از سرقت اطلاعات فایل حیاتی و جلوگیری از دسترسی به اطلاعات پایگاه داده سایت کد زیر را دهید :

```
<files wp-config.php>  
order allow,deny  
deny from all  
</files>
```

10) ایجاد محدودیت در آپلود فایل :

با کد زیر حداکثر حجم فایل قابل آپلود را ۲۰ مگابایت تنظیم می کنیم.

```
php_value upload_max_filesize 20M
```

11) جلوگیری از سرقت پهنای باند و فایلها و عکسها :

خیلی وقت ها اتفاق می افتد مدیران سایتهای دیگر آدرس عکس یا فایلها را کپی میکنند و در سایت خودشان استفاده میکنند. با این عمل در حقیقت هنگام درخواست برای نمایش آنها این درخواست به سرور شما ارسال میشود و در نهایت از پهنای باند شما کاسته میشود. برای جلوگیری از این کار و ایجاد محدودیت برای نمایش فایل ها کد زیر را در فایل htaccess قرار دهید :

```
RewriteEngine On
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www\.)?site.com/.*$ [NC]
RewriteRule \.(gif|jpg|swf|flv|png)$ /feed/ [R=302,L]
```

12) افزایش امنیت محتوای فولدر wp-includes :

کافیست کد زیر را در htaccess قرار دهید :

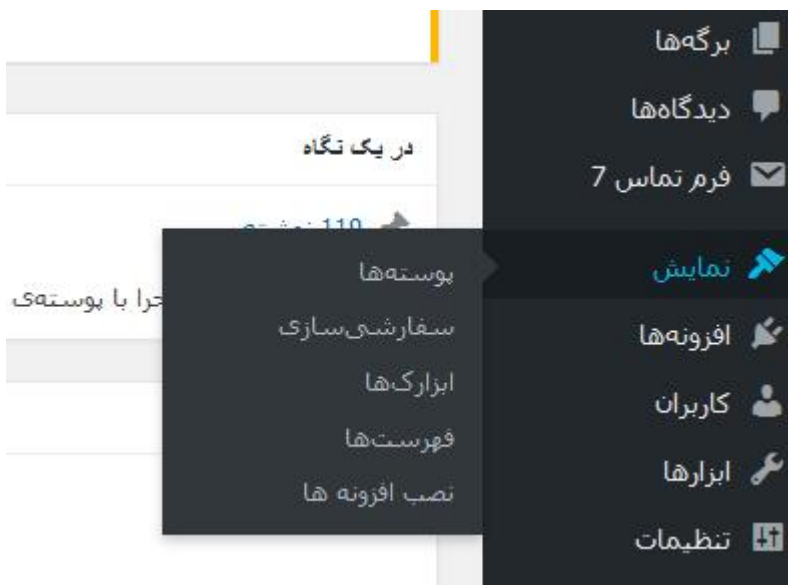
```
# Block the include-only files.
RewriteEngine On
RewriteBase /
RewriteRule ^wp-admin/includes/ - [F,L]
RewriteRule !^wp-includes/ - [S=3]
RewriteRule ^wp-includes/[^\.]\.php$ - [F,L]
RewriteRule ^wp-includes/js/tinymce/langs/\.php - [F,L]
RewriteRule ^wp-includes/theme-compat/ - [F,L]
```

غیر فعال کردن امکان ویرایشگر در پوسته و افزونه

برای بسیاری از مدیران و توسعه دهندگان وردپرس دسترسی مدیران تازه کار ! به ویرایشگر پوسته ها و افزونه ها یکی از مشکلات بزرگ محسوب می شود ، کاربرانی که با ویرایش یک کلمه ساده کل سایت را دچار مشکل می کنند .

برای اینکار کافی است کد زیر را به انتهای فایل functions.php قالب اضافه کرده و آن را ذخیره کنید :

```
// Disable the theme / plugin text editor in Admin  
define('DISALLOW_FILE_EDIT', true);
```



همان طور که در تصویر مشاهده می کنید گزینه ویرایشگر در صفحه مدیریت وردپرس حذف شد و این مورد علاوه بر این که نگرانی ما در مورد مدیران تازه کار را برطرف می کند تا حدی موجب افزایش امنیت سایت نیز می شود. چون اگر نفوذگر به روشی یوزر و پسورد سایت ما را به دست آورد نمی

تواند درهای پشتی (Backdoor) را در سایت ما ایجاد کند و یاد کدهای مخربی مثل شل کدها را جایگزین کدهای ما کند.

ایمن کردن سایت وردپرسی در برابر موتور های جستجوگر

هر روزه تعداد زیادی آسیب پذیری در افزونه ها (Plugins) و قالب های (Templates) وردپرس پیدا می شود و نفوذگران با استفاده از گوگل هکینگ می توانند به راحتی سایت های که از افزونه یا قالب آسیب پذیر استفاده می کنند پیدا کنند و اگر شما از همان افزونه یا قالب استفاده کنید ، آدرس سایت شما نیز برای نفوذگر نمایش داده می شود در نتیجه نفوذگر به راحتی به سایت شما نفوذ می کند. به همین دلیل ما باید سایت خود را در برابر موتور های جستجوگر ایمن کنیم ، در ادامه روش هایی برای این کار معرفی خواهیم کرد.

اولین روش این است که پوشه های مهم wp-admin ، wp-content و wp-includes را از دید موتور های جستجوگر خارج کنیم ، تا در نتیجه های جستجو قرار نگیرد.

برای اینکار ابتدا فایل robot.txt را در هاست خود بسازید و متن زیر را در آن قرار دهید.

Disallow: /wp-content

Disallow: /wp-admin

Disallow: /wp-includes

همه ی افزونه ها و قالب ها دارای فایلی به نام readme.txt هستند که درون آن ها مشخصات افزونه یا قالب نوشته شده است که برای اسکنرهایی مانند sqlmap بسیار مفید هستند ، این فایل ها را حذف کنید .

Name	Size	Last Modified	Type	Permissions
admin	4 KB	Apr 30, 2016 6:15 PM	httpd/unix-directory	0755
images	4 KB	Apr 30, 2016 6:15 PM	httpd/unix-directory	0755
includes	4 KB	Apr 30, 2016 6:15 PM	httpd/unix-directory	0755
languages	4 KB	Apr 30, 2016 6:15 PM	httpd/unix-directory	0755
modules	4 KB	Apr 30, 2016 6:15 PM	httpd/unix-directory	0755
license.txt	795 bytes	Jan 8, 2016 4:47 AM	text/plain	0644
readme.txt	4.46 KB	Apr 30, 2016 6:13 PM	text/plain	0644
settings.php	3.65 KB	Mar 4, 2016 4:36 PM	application/x-httpd-php	0644
uninstall.php	456 bytes	Sep 6, 2011 12:10 PM	application/x-httpd-php	0644
wp-contact-form-7.php	1.71 KB	Apr 30, 2016 6:13 PM	application/x-httpd-php	0644

با استفاده از روش های بالا سایت خود را در برابر موتور های جستجوگر امن کرده اید.

جلوگیری از ساخت فایل Error_log در وردپرس

حتما فایل error_log را در پوشه public_html خود مشاهده کرده اید و سوال شما این است که فایل error_log چیست؟ این فایل که یک فایل متنی است و قابل اجرا نیست.

این فایل برای خطا های وب سایت شما می باشد. فرض کنید یک برنامه تحت وب با پسوند php نوشته اید و برنامه شما ناقص می باشد در صورتی که نمایش خطا php در تنظیمات php.ini سرور شما روشن باشد بعد از اجرا آن فایل خطا به شما نمایش داده می شود اما در صورتی که نمایش خطا در سرور شما خاموش باشد شما با یک صفحه سفید مواجه می شوید و دیگر اطلاع ندارید که کدام خطا برنامه شما ایراد دارد. در فایل error_log حتی در صورتی که نمایش خطا php شما خاموش باشد خطا به این فایل اضافه می شود به همراه تاریخ و زمان دقیق.

در نظر داشته باشید در هاست اشتراکی برای امنیت بیشتر معمولا مدیر سرور امکان نمایش خطا php را خاموش می کند تا از استفاده نفوذگرها از خطا جلوگیری کنند. به همین دلیل همیشه لازم است این فایل را بررسی کنید.

شما می توانید با ویرایش و یا دانلود این فایل محتوا این فایل را بررسی کنید.

error_log اجازه پیدا کردن دایرکتوری و یوزر هاست به نفوذگر را می دهد که یک امتیاز مثبت برای نفوذ به سایت به شمار میرود از آنجایی که ابزارهایی وجود دارد چه به صورت عمومی چه به صورت خصوصی که می توان پنل هاست یا cpanel یا ... را با تست پسورد های زیاد مورد نفوذ قرار داد. جهت جلوگیری از ایجاد فایل error_log توی وردپرس کد زیر رو به wp-config.php اضافه کنید.

```
define('WP_DEBUG', false);  
  
if (WP_DEBUG) {  
  
define('WP_DEBUG_DISPLAY', false);  
  
@ini_set('log_errors', 'off');  
  
@ini_set('display_errors', 'off');  
  
@ini_set('error_log', 'wp_error.log');  
  
{
```

توجه داشته باشید که حذف محتوا یا حذف فایل error_log مشکلی برای سایت شما ایجاد نمی کند ، بنابراین می توانید این فایل را به کلی حذف کنید. اما اگر بعد از حذف مشاهده کردید که دوباره ایجاد شده بهتر است از کد بالا استفاده کنید.

پلاگین های امنیتی پرکاربرد در وردپرس

امروزه طراحان وب بیشتر از پیش تمایل به استفاده از ابزارهای از پیش طراحی شده و یا قالب های آماده را دارند. برخی از ابزار های مورد استفاده وردپرس رایگان بوده و برخی دیگر با پرداخت هزینه همراه می باشند. در واقع تعداد کسانی که برای اهداف خاصی، قالب های (Themes) خاصی ایجاد می کنند، انگشت شمار می باشند.

با توجه به استفاده روزافزون از قالب ها و افزونه های از پیش طراحی شده، امکان مخفی شدن کدهای آلوده، backdoor ها ، حفره های امنیتی و در نتیجه ی آن هک شدن سایت شما دور از انتظار نمی باشد. همچنین گاهی اوقات نیز پیوندهایی (backlinks) به آدرس های مورد نظر نفوذگرها در لایه های اصلی سایت قرار داده می شود؛ این در حالی است که کاربران عادی ممکن است هیچ گاه از وجود چنین کدهای مخربی در سایت باخبر نشوند.

لذا با توجه به این که نفوذگرها همواره درصدد یافتن راه های نفوذ به سایت های مختلف هستند، وب سایت شما نیاز به ایجاد دیوارهای امنیتی در مقابل چنین حملاتی داشته و می بایست نسبت به ایمن نمودن هر چه بیشتر سایت خود اقدام نمایید.

با توجه به موارد بالا و نیاز مبرم به ایمن نمودن سایت ها، استفاده از پلاگین های امنیتی از حیاتی ترین نیاز های هر وب سایت وردپرس می باشد؛ لذا در اینجا به معرفی اجمالی بهترین پلاگین های امنیتی وردپرس می پردازم.

برخی از مشهور ترین و قدرتمند ترین پلاگین های امنیتی وردپرس به شرح زیر می باشند:

1- پلاگین TAC یا Theme Authenticity Checker

پلاگین TAC پلاگین امنیتی وردپرس بوده ، که جهت اسکن نمودن فایل های اصلی قالب وردپرس به کار رفته و کلیه کد های مخرب موجود در قالب های نصب شده روی وردپرس را مشخص می نماید. این کدهای مخرب شامل لینک های پایین صفحات وب و کدهای Base64 باشند.

پس از شناسایی کدهای مخرب، نام قالب و مسیر فایل مربوطه به همراه شماره خط کد مخرب و قسمتی از آن نمایش داده می شود که به راحتی می توان آن را آنالیز و حذف نمود.

2- پلاگین Exploit Scanner

پلاگین امنیتی Exploit Scanner جهت اسکن کردن کلیدهای فایل‌ها و دیتابیس سایت مورد استفاده قرار می‌گیرد و قادر است هر چیزی مشکوکی را روی سایت شما شناسایی نموده و نمایش دهد.

هنگام استفاده از پلاگین Exploit Scanner توجه نمایید که این پلاگین امنیتی وردپرس، از حمله نفوذگرها به سایت شما جلوگیری نمی‌کند؛ همچنین فایل‌های مخرب را نیز حذف نمی‌نماید بلکه تنها به مدیر سایت جهت شناسایی و تشخیص فایل‌های آلوده کمک می‌کند و سپس ادمین می‌بایست نسبت به حذف فایل‌های آلوده به صورت دستی اقدام نماید.

3- پلاگین Sucuri Security

پلاگین Sucuri یکی از مشهورترین پلاگین‌های امنیتی وردپرس جهت اسکن بدافزارها می‌باشد. مهمترین ویژگی‌های پلاگین Sucuri، مانیتور نمودن کلیدهای فایل‌های آپلود شده در وردپرس، مانیتورینگ بلک لیست‌ها، هشدارهای امنیتی و غیره می‌باشد. حتی شما می‌توانید از نسخه رایگان و دسترسی از راه دور (remote malware scanning) پلاگین امنیتی Sucuri جهت اسکن بدافزارها یعنی Sucuri SiteCheck Scanner نیز استفاده نمایید.

همچنین این پلاگین شامل افزونه‌ی فایروال قدرتمندی نیز می‌باشد که با تهیه و استفاده از آن می‌توانید سایت خود را در مقابل حملات هکرها ایمن‌تر نمایید.

4- پلاگین Anti-Malware

پلاگین امنیتی Anti-Malware قادر است ویروس‌ها، تهدیدها و سایر فعالیت‌های مخرب را روی سایت‌های وردپرس شناسایی نموده و آن‌ها را حذف نماید. از جمله برخی از قابلیت‌های مهم آن،

امکان سفارشی سازی اسکن، اسکن کامل سایت، اسکن سریع، حذف خودکار تهدید های امنیتی روی سایت وردپرس و غیره می باشد.

5- پلاگین WP Antivirus Site Protection

پلاگین WP Antivirus Site Protection از دیگر پلاگین های امنیتی جهت اسکن قالب های وردپرس و تمامی فایل های آپلود شده روی سایت می باشد.

مهمترین قابلیت این پلاگین، امکان اسکن تک تک فایل های آپلود شده، آپدیت نمودن مرتب دیتابیس های ویروسی، حذف کلیه بدافزارها، ارسال هشدارها و پیغام های امنیتی توسط ایمیل و غیره می باشد.

6- پلاگین AntiVirus for WordPress

پلاگین AntiVirus for WordPress یکی از پلاگین های محافظتی وردپرس بسیار راحت و ساده می باشد و برای اسکن نمودن قالب های نصب شده وردپرس و یافتن کدهای مخرب مناسب می باشد.

با استفاده از این پلاگین، در پنل ادمین وردپرس هشدارهای مربوط به کدهای مخرب نمایش داده می شوند. همچنین پلاگین AntiVirus for WordPress بصورت روزانه قالب ها را اسکن نموده و در صورت یافتن موارد مشکوک آن را به ادمین سایت، ایمیل خواهد کرد. همچنین امکان قرار دادن سایت شما را در لیست whitelist ها نیز فراهم می نماید.

7- پلاگین Quttera Web Malware Scanner

پلاگین امنیتی Quttera Web Malware Scanner جهت اسکن وب سایت در مقابل حملات تزریق کدهای مخرب (malicious code injection)، ویروس ها، کرم ها ، بدافزارها ، تروجان ها و غیره مورد استفاده قرار می گیرد.

همچنین پلاگین Quttera Web Malware Scanner ویژگی های خوبی نظیر موارد زیر را نیز در اختیار ادمین سایت قرار می دهد:

- اسکن و شناسایی بدافزار های ناشناخته
- وضعیت بلک لیست ها
- شامل موتورهای اسکن با هوش مصنوعی
- شناسایی لینک های خارجی
- و غیره

8- پلاگین Wordfence

از دیگر پلاگین های امنیتی، پلاگین Wordfence می باشد. در واقع این پلاگین نقش دفاعی در مقابل تهدیدات سایبری دارد.

پلاگین Wordfence قابلیت های بسیار خوبی را جهت حفاظت آنی و بی درنگ در مقابل حملات شناخته شده، اسکن backdoors های شناخته شده و نیز مسدود نمودن کلید شبکه های مخرب را در صورت شناسایی آن ها ، ارائه می دهد.

9- پلاگین Wemahu

پلاگین امنیتی Wemahu، از دیگر پلاگین های قدرتمند وردپرس جهت شناسایی کدهای مخرب در فایل ها و قالب های سایت وردپرس می باشد.

با استفاده از پلاگین Wemahu شما قادر خواهید بود فایل هایی که تغییر یافته اند را مانیتور نموده و همچنین امکان زمان بندی سایت جهت اسکن با این پلاگین میسر می شود و نتایج اسکن برای ادمین سایت ایمیل خواهد شد.

10 – پلاگین 6Scan Security

پلاگین امنیتی دیگر 6Scan Security می باشد که امکانات متعددی نظیر اسکن سایت، بکاپ گیری اتوماتیک، فایروال های دینامیکی، آنالیز زنده سایت و غیره را فراهم می کند.

برخلاف پلاگین های امنیتی دیگر، این پلاگین از الگوریتم های پیچیده ای جهت شناسایی و برطرف نمودن مشکلات امنیتی سایت استفاده می کند.

11 – پلاگین Centrorra

پلاگین Centrorra از دیگر پلاگین های امنیتی مشهور و قدرتمند سیستم مدیریت محتوا وردپرس می باشد. از مزایای این پلاگین این است که می تواند از حملات احتمالی و هک شدن سایت وردپرس جلوگیری نماید.

با استفاده از پلاگین Centrorra امکان شناسایی و کشف کدهای مخرب مخفی شده، تزریق دیتابیس (SQL injection)، تهدیدات امنیتی، اسپم ها و یا هر نوع آسیب پذیری دیگر فراهم می شود.

همچنین امکان ارسال هشدار های امنیتی به ادمین سایت توسط ایمیل را نیز دارا است و شما ابزار های مفید دیگری نظیر آنتی اسپم ها و مدیریت IP نیز می باشد.

تغییر دوره ای پسورد

نکته دیگری که برای افزایش امنیت سایت باید در نظر داشته باشید این است که پسورد هاست و پسورد مدیریت وردپرس را به صورت دوره ای تغییر بدید تا اگر فرد دیگری به هاست یا پنل مدیریت سایت شما دسترسی دارد و در پشتی برای خود ایجاد نکرده دسترسی خود را از دست بدهد.

تهیه دوره ای نسخه پشتیبان

یکی از مسائلی که بعد از مورد نفوذ قرار گرفتن سایت و در اصطلاح خراب شدن سایت اهمیت دارد داشتن نسخه پشتیبان است. معمولاً سرورها به صورت هفتگی از سایت شما بک آپ تهیه می کنند. اما اگر خود سرور دچار مشکل شود آن وقت تکلیف چیست؟ در حالت خوشبینانه اگر سرور هم دچار مشکل نشود نسخه پشتیبانی که سرور به شما می دهد مربوط بخ چند روز پیش است و بسیاری از مطالب شما از بین رفته است و به ناچار باید دوباره تمام آن مطالب را از اول قرار دهید.

حالا اگر پست ها و مطالب سایت شما به صورت اختصاصی باشد و برای نوشتن هر کدام دقایق زیادی رو صرف کرده باشید این موضوع بیشتر عذاب آور می شود. پس باید توجه داشته باشید که در قدم اول یک نسخه پشتیبان کانل از کل هاست تهیه کنید. برای این کار وارد هاست ، بخش File manager و سپس public_html شوید.

تمام فایل ها را در حالت انتخاب قرار داده و روز گزینه Compress کلیک کنید. در پنجره باز شده تیک گزینه Zip Archive را بزنید و بعد گزینه Compress File را کلیک کنید. در این حالت بک آپ از قالب و وردپرس تهیه می شود و تنها باید آن را دانلود و در جایی ایمن نگه داری کنید تا در صورت بروز مشکل بتوانید استفاده کنید.

قدم بعدی تهیه نسخه پشتیبان از دیتابیس است. هر مطلبی که در سایت قرار می دهید در دیتابیس ذخیره می شود. پس برخلاف مورد قبل ه فقط یکبار تهیه می شود این مورد را سعی کنید پایان هر روز یا یک روز درمیان انجام دهید.

برای ان کار وارد هاست می شویم ، از قسمت Databases برو روی phpMyAdmin کلیک می کنیم.



اندکی صبر می کنیم تا صفحه باز شود. سپس از قسمت سمت چپ دیتابیس سایت را پیدا کرده و روی آن کلیک می کنیم. سپس از قسمت سمت راست بالا بر روی گزینه Export کلیک می کنیم.

Table	Action	Rows	Type	Collation	Size	Overhe
wp_bp_option_tree	Browse Structure Search Insert Empty Drop	83	MyISAM	utf8_general_ci	12 KiB	
wp_commentmeta	Browse Structure Search Insert Empty Drop	~38	InnoDB	utf8mb4_unicode_ci	48 KiB	
wp_comments	Browse Structure Search Insert Empty Drop	~15	InnoDB	utf8mb4_unicode_ci	96 KiB	
wp_cptch_images	Browse Structure Search Insert Empty Drop	~112	InnoDB	utf8_general_ci	16 KiB	
wp_cptch_packages	Browse Structure Search Insert Empty Drop	~12	InnoDB	utf8_general_ci	16 KiB	
wp_cptch_whitelist	Browse Structure Search Insert Empty Drop	~0	InnoDB	utf8_general_ci	32 KiB	
wp_itsec_lockouts	Browse Structure Search Insert Empty Drop	~0	InnoDB	utf8mb4_unicode_ci	96 KiB	
wp_itsec_log	Browse Structure Search Insert Empty Drop	~0	InnoDB	utf8mb4_unicode_ci	48 KiB	
wp_itsec_temp	Browse Structure Search Insert Empty Drop	~0	InnoDB	utf8mb4_unicode_ci	80 KiB	

بدون تغییر در گزینه ها بر روی دکمه GO کلیک می کنیم. پیامی در صفحه ایجاد می شود که از ما برای ذخیره سازی سوال می کند. روی OK کلیک می کنیم. به همین راحتی ما از دیتابیس خود یک نسخه پشتیبان تهیه کردیم.

توجه داشته باشید که تهیه نسخه پشتیبان یکی از مهم ترین مسائل در تامین امنیت سایت است که متأسفانه توسط بسیاری از وب مستران عزیز کشورمان ناده گرفته می شود.

مباحث آموزشی ما در زمینه تامین امنیت سایت های وردپرسی همین جا به پایان رسید. امیدوارم که مطالب این کتاب برای شما دوست عزیز مفید واقع شود.

در صورتی که قصد دارید در مورد امنیت مطالب دیگری رو یاد بگیرید به صفحه شخصی من در سایت فرانش مراجعه کنید.

<https://faranesh.com/author/mansoori>

<http://bmansoori.ir>