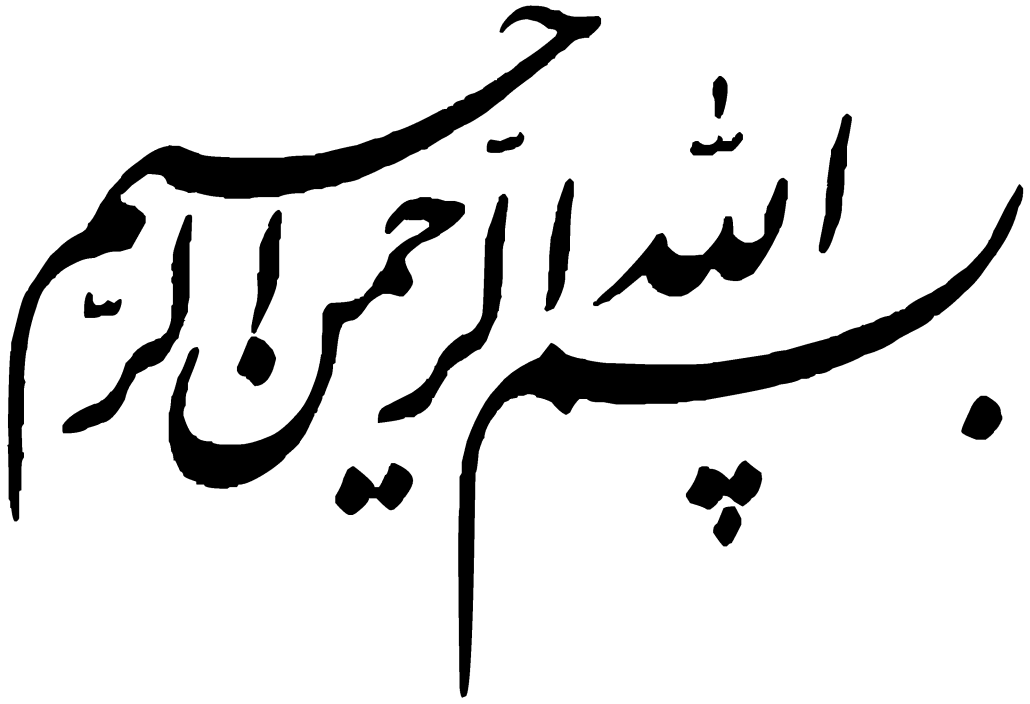

بسم الله الرحمن الرحیم

راهنمای امنیت در جوملا

تهیه و تنظیم : مصطفی سعیدی

سال انتشار : ۱۳۹٤

شماره کتاب : ۳

منبع : سرزمین کتاب

کتاب های دیگر سرزمین کتاب :

دانلود کتاب بررسی تخصصی سخت افزار کامپیوتر (شماره ۱)

دانلود کتاب آموزش کوهنوردی (شماره ۲)

(منتظر کتاب های بعدی باشید ...)

سخنی با شما :

دوستان عزیز و گرامی برای اطلاع از جدیدترین کتاب های آموزشی که توسط وب سایت سرزمین کتاب منتشر می شود می توانید به آدرس زیر مراجعه نمائید :

www.sarzaminketab.ir

و همچنین می توانید هر گونه نظر و انتقادی را به ایمیل زیر ارسال کنید :

info@sarzaminketab.ir

سرزمین کتاب در تلاش است تا کتاب های مفید و کاربردی بیشتری را خدمتتان ارائه کند. شما دوستان عزیز با نظرات گرم خود می توانید ما را در این راه یاری نمائید.

لطفا ما را دنبال کنید !

فهرست

مقدمه

در همین ابتدا از شما خواهش میکنم هر جایی که میتوانید این کتاب را منتشر نمایید شاید بتوانید به دوستان خود در جاهای دیگر هم کمک کنید. و در دومین کلام به سمعتون میرسانیم که گرچه سعی شده است این مقاله کامل باشد و دید مفیدی از بحث امنیت خصوصا در سایت های جوملایی به شما دهد اما باز هم هیچ کتاب ، مقاله و سایتی نمیتواند ادعا کند که ۱۰۰٪ کامل است . به کلامی دیگر هیچ سایتی ایمن نیست منتها ممکن است حمله کننده هنوز راه نفوذ به ان را پیدا ننموده باشد . این موضوع هم ربطی به مدیریت جوملا ، ورد پرس و ... ندارد بلکه تمامی سایت ها حتما راه نفوذی دارند.

قصد ما در این کتاب سعی در قفل و زنجیر کردن سایت است که مسلما کار را برای دوست هکرمان سخت تر میکند. یک نکته هم در رابطه با هکر ها بگم اصولا هکر ها میباید یا دارای سواد بالایی باشند و یا از سواد نسبی خوبی برخوردار باشند به همین دلیل این دسته از افراد اکثرا در استخدام شرکت های امنیتی بزرگ هستند و حقوق بسیار بالایی هم دارند و قابل احترام هستند اما خود هکر ها به ۲ دسته تقسیم میشوند اصطلاحا هکر های سفید و سیاه که خوب از لقبی هم برای خودشون انتخاب میکنند مشخصه هر کدام دارای چه خصوصیاتی هستند البته خود این دسته ها هم به شعب مختلف تقسیم میشه و حتی زبان نگارش مخصوص خودشون هم دارند . خلاصه دنیاییه ! در این مقاله قصد نداریم به این تاریخچه بپردازیم تنها قصد ما بهبود امنیت است لذا از این مقال میگذریم . قبل از هر چیز باید بدانید یک هکر میتواند از ۲ طریق کلی سایت شما هک کند ۱- از سمت سرور ۲- از سمت سایت

حمله از سمت سرور

در این حالت حمله کننده به سرور دسترسی دارد و آنچنان کاری از شما بر نمیاید هر چقدر هم امنیت سایتتان را بالا بررید فایده ای ندارد چرا که حمله کننده اصلا به سایت شما کاری ندارد و به منابع سرور دسترسی دارد . اما یک کار دیگر میتوانید انجام دهید.

۱- اول اینکه سروری انتخاب کنید که قبل هک نشده باشد . برای این انتخاب باید به شنیده های خود اعتماد کنید و یا پاشنه ها را بالا بکشید و شروع کنید به جستجو در سایت هایی که تصاویر هک سایت ها را میگذارند سپس سرور ان ها را پیدا نمایید و ...

۲- در هنگام خرید هاست باید به مواردی که مربوط به تنظیمات سرور است دقت کنید از جمله به موارد زیر :

۱. قبل از خرید هاست از سرپرست سرور بپرسید که آیا در PHP از su_php استفاده میکنند با خیر ؟ استفاده از این حالت به معنای ان است که فایل های موجود در هاست شما تحت کنترل خود دارنده اکانت که شما باشید میباشد و نیازی به تنظیمات GLOBAL نیست به زبان ساده تر در این حالت سطح دسترسی ۷۵۵ توسط اسکریپت قابل نگارش تشخیص داده میشود و نیازی نیست که شما این سطح دسترسی ها را به ۷۷۷ تغییر دهید . وقتی دسترسی یک پوشه را روی ۷۷۷ قرار میدهید به معنای ان است که محتویات آن را برای عموم آزاد کرده اید !
۲. register_globals در سرور که سایت جوملایی روی آن قرار دارد باید خاموش باشد.
۳. safe_mode در سروری که یک سایت جوملایی بر روی آن قرار دارد باید خاموش باشد.
۴. گزینه allow_url_fopen در سروری که یک سایت جوملایی بر روی آن قرار دارد باید خاموش باشد.

۵. allow_url_include در سروری که یک سایت جوملایی بر روی آن قرار دارد باید خاموش باشد.
۶. گزینه disable_functions در سروری که یک سایت جوملایی روی ان قرار دارد باید فعال باشد.
۷. همین موارد هم باید برای open_basedir صدق میکند منتها اگر سرور از su_php استفاده کرده باشد این گزینه دیگر دارای اهمیت نیست.

۳- یکی دیگر از مواردی که در هنگام خرید هاست باید از سرپرست فنی سرور بپرسید این است که آیا بر روی سرور برنامه های امنیتی مثل آنتی شل نصب است یا خیر ؟ شل ها برنامه های کوچکی هستند به هکر ها قدرت دسترسی به برخی منابع را میدهند . اگر جواب سرپرست سرور بلی بود اسم برنامه را هم بپرسید و در مورد ان تحقیق کنید . هزینه این برنامه برای سرور ها بسیار بالا است و تا ۳۰۰ دلار هم میرسد به همین دلیل برخی سرور ها از این امر غفلت میکنند

۴- از سرپرست سایتتان بپرسید که آیا برای ورود به phpmyadmin دوباره نام کاربری و رمز عبور پرسیده میشود و یا خیر ؟

این ها حداقل مواردی است که قبل از خرید باید از سرپرست هاستتان بپرسید به دلیل آنکه در این مقاله قصد داریم راه کار ارئه دهیم تا اینکه روش ها را توضیح دهیم به هین دلیل از ذکر مفاهیم بالا خودداری میکنیم و تنها به اینکه این موارد باید در سرور دارای چه تنظیماتی باشد اکتفا میکنیم . گروه جومینا امیدوار است که مدیران سرور ها هم این مقاله را بخوانند تنظیمات سرورهای خود را بهینه نمایند. البته همانطور که عرض شد این ها حداقل ها هستند.

حمله از سمت سایت

این حمله ها به روش های گوناگونی انجام میشود که مهمترین های آن استفاده از :

POST_$

GET_$

COOKIE_$

()eval

_decode۶۴base

Allow_url_fopen

فیلتر دستورات SQL

Allow_url_include

می باشد. قبلا در سایت جومینا یک پلاگین امنیتی معرفی شده بود که با نصب آن امنیت سایت در مقابل این حملات بالا میرفت این پلاگین را میتوانید از اینجا دریافت و نصب و فعال کنید . نکته ای که رابطه با این پلاگین بود درج کپی رایتی بود که در پایین سایت قرار داشت برای این که کپی رایت هم بردارید. وارد فایل jhackguard.php شوید و خط

" = replacement$

را با عبارت زیر جایگزین کنید.

;"" = replacement$

به این ترتیب کپی رایت هم حذف میشود دوباره فایل را فشرده نموده و نصب کنید.

بسیار خوب حال که جلوی این حمله ها را گرفتیم میباید وارد مرحله بعدی شویم در این مرحله کارهای دیگری باید انجام دهید که به ترتیب برای شما فهرست شده و اموزش داده می شود.

تغییر نام کاربری Admin

پس از نصب و راه اندازی جوملا ۱,۵ شما به عنوان مدیر سایت (Super Administrator)، با نام کاربری ای که به طور پیش فرض admin است، می توانید وارد بخش مدیریت سایت شوید. همه ی نصب های جدید جوملا با این حساب کاربری انجام شده و سیستم برای این حساب کاربری از شما گذرواژه و نام کاربری می خواهد. خیلی خوب تا اینجا همه چیز مرتب است.

اما ۵۰ درصد از ترکیب گذرواژه و نام کاربری در معرض خطر است و هر کسی می تواند گذرواژه را حدس زده و وارد محیط مدیریتی شود، چرا که همه از شناسه ی این حساب کاربری (Admin) که فوق العاده محرمانه است باخبرند، پس با تغییر نام کاربری به یک واژه ی سخت تر می توانید دسترسی به حساب را مشکل تر کنید. با این کار شما یکی از راه های نفوذ به سیستم را برای نفوذگران مسدود خواهید کرد و امنیت را تا حد زیادی افزایش خواهید داد. در این صورت یک هکر در آن واحد برای دستیابی به دو چیز، دو بار بایستی حدس بزند. یک بار برای گذر واژه و بار دیگر برای نام کاربری! پس کار هکرها مشکل تر می شود.

برای تغییر نام کاربری که به طور پیش فرض admin می باشد، به ترتیب زیر عمل کنید:

ورود به محیط منوی مدیریت کاربر برای این کار شما می بایست با همان نام کاربری admin (شناسه پیش فرض joomla) وارد بخش مدیریت سایت شده و از منوی سایت مدیریت کاربر را برگزینید.

در صورتی که تعداد کاربران زیاد بود، می توانید با استفاده از گزینه های *****ی که در بالای لیست کاربران قرار دارد برای یافتن کاربر مورد نظر استفاده نمایید. پس از لیست کشویی "انتخاب گروه" مدیریت سایت را انتخاب نمایید.

حالا با کلیک بر روی نام کاربری مدیر سایت یا انتخاب نام مدیر سایت و سپس زدن دکمه ی ویرایش می توانید نام کاربری مدیریت را تغییر دهید و در صورت تمایل همه ی اطلاعات مدیر سایت را ویرایش کنید.(بهتر است نام کاربری شما ترکیبی از اعداد و حروف باشد)

"ویرایش نام کاربری مدیر" حالا در فیلد "نام کاربری" به جای شناسه ی admin شناسه ی دلخواه خود را وارد کنید.

به خاطر داشته باشید حتما پس از اعمال تغییرات، تنظیمات را ذخیره کنید.

حال می توانید با نام کاربری جدید و بدون هیچ نگرانی وارد بخش مدیریت شوید.

رمز عبور قوی انتخاب کنید

«حتما یک رمز عبور قوی انتخاب کنید.» این جمله ای است که خیلی وقت ها در فضای اینترنت، هنگام تعیین رمز عبور با آن مواجه می شویم. حالا قصد داریم بررسی کنیم که چگونه می توان یک رمز عبور مناسب انتخاب کرد و از آن مهم تر، اینکه چگونه این رمز عبور قوی را به خاطر بسپاریم؟

استفاده از یک نرم افزار مدیریت رمز عبور مثل LastPass که بتواند پسوردهای قوی ایجاد و آنها را به شما یادآوری کند، فکر خوبیست؛ اما حتی اگر از این نرم افزارها هم استفاده کنید، مجبورید که حداقل یک پسورد -یعنی رمز عبور برای همان برنامه- انتخاب کنید و آن را به خاطر بسپرید.

توصیه های رایج در مورد رمز عبور

از گذشته تا به حال توصیه هایی در مورد یک رمز عبور مناسب شنیده ایم؛ برخی از آنها همچنان هم کاربردی هستند. طبق این توصیه ها یک رمز عبور مناسب باید:

۱. حداقل دوازده کاراکتر داشته باشد

شما باید رمزی انتخاب کنید که به اندازه کافی طولانی باشد. هیچ مقدار حداقلی وجود ندارد که همه با آن موافق باشند، اما عموما بهتر است که پسوردهایتان حداقل ۱۲ تا ۱۴ کاراکتر باشند. اگر طول رمز عبور از این هم بیشتر شد، طبیعتا امنیت بالاتری را به همراه خواهد داشت.

۲. ترکیبی از اعداد، علائم، حروف بزرگ و حروف کوچک باشد

سعی کنید از ترکیبی از انواع کاراکترهای مختلف استفاده کنید تا هک کردن رمز عبور شما سخت تر شود.

۳. یک کلمه معنادار یا ترکیبی از چند کلمه معنادار نباشد

از به کار بردن کلمات معنی دار ساده و یا ترکیبی از چندتای آنها در ساخت رمز عبور خودداری کنید. استفاده از هر کلمه معناداری واقعا اشتباه است و ترکیب چندتای آنها که یک عبارت ساده را هم بسازد، اشتباهی دیگر. برای مثال "house" یک رمزعبور بسیار ضعیف است و به راحتی هک می شود؛ در عین حال "red house" هم بسیار نامناسب است.

۴. از کاراکترهای جایگزینی که واضح هستند در آن استفاده نشده باشد

برخی کاراکترها را به دلیل شباهت ظاهری به یکدیگر می توان جابجا کرد. مثلا ۰ (عدد صفر) و O (حرف الفبای انگلیسی) به هم بسیار شبیه هستند. پس بهتر است در انتخاب رمز عبور، عبارت هایی مثل "use۰h" هم خودداری کنید. چون اگر هکر احساس کند رمز شما چیزی

شبیه به کلمه house است، تمامی جایگزین های ممکن و شبیه به کاراکترهای موجود را تست می کند.

سعی کنید از تمامی توصیه های فوق استفاده کنید. مثلا در رمزعبور "۱۲۳$Bighouse" بسیاری از شرایط رعایت شده؛ ۱۲ کاراکتر دارد، دارای حروف بزرگ و کوچک است، یک علامت و چند عدد هم دارد. اما این عبارت تا حدودی معنادار بوده و نسبتا واضح است. زیرا ترکیبی است از یک کلمه معنی دار (که مثل نوشتار انگلیسی، فقط حرف اول آن بزرگ است)، فقط یک علامت و تعدادی عدد که همگی در انتها قرار داشته و حتی به ترتیب هم هستند.

یک ترفند برای ساخت رمز عبوری قوی (برای امنیت) و ساده (برای به خاطر سپردن)

اگر بخواهیم فقط از راهنمایی های قبلی استفاده کنیم، بسیار ساده می توانیم پسوردهای سخت ایجاد کنیم. کافی است که انگشتانتان را به صورت نامنظم روی کیبورد فشار دهید تا یک رمز عبور قوی مثل ۹t#۴hZ۳o(t&gSp&۳ ایجاد کنید. این رمز بسیار مناسب به نظر می رسد؛ چرا که ۱۶ کاراکتر دارد، ترکیبی از انواع مختلف کاراکتر است و به دلیل بی معنی بودن آن، حدس زدنش بسیار سخت است.

تنها مشکلی که وجود دارد این است که این رمز عبور را چطور حفظ کنیم. اگر فرض کنیم که شما حافظه تصویری فوق العاده ای نداشته باشید، باید زمان بسیاری را صرف به خاطر سپردن این پسورد کنید. برنامه هایی وجود دارند که از این نوع رمزهای عبور قوی به صورت تصادفی (رندوم) درست می کنند و اگر از یک اپلیکیشن مدیریت رمز عبور استفاده می کنید، می توانند برای شما مناسب باشند.

برای ایجاد یک رمز عبور که بتوانید آن را به راحتی به خاطر بسپارید، نیاز است که کمی فکر کنید. شما نمی خواهید از عبارات ساده و واضح و یا کلمات معنی دار استفاده کنید. بنابراین روشی را بیان می کنیم که به کمک یک ترفند، بتوانید رمز عبور مناسب بسازید.

برای مثال ممکن است به خاطر سپردن این جمله برای شما بسیار ساده باشد :

“The first house I ever lived in was ۶۱۳Fake Street. Rent was ۴۰۰$ per month.”

(اولین خانه ای که من در آن زندگی کردم در خیابان ۶۱۳ Fake بود و مبلغ اجاره اش هم ماهی ۴۰۰ دلار بود)

حالا می توانید با استفاده از حرف اول هر کلمه آن را به یک پسورد تبدیل کنید و در نتیجه رمز عبور شما .pm۴$FS.Rw۶۱۳TfhIeliw خواهد بود. این یک رمز عبور قوی با ۲۱ کاراکتر است. قطعا یک رمز عبور تصادفی بهتر از این، می تواند شامل تعداد بیشتری عدد و علائم و حروف بزرگ، به صورت پراکنده باشد؛ اما این پسورد هم به هیچ وجه نامناسب نیست. حالا شما فقط نیاز دارید که دو جمله ساده را به خاطر بسپرید و در نتیجه به خاطر سپردن آن راحت خواهد بود.

شما می توانید این ترفند را با استفاده از فینگلیش نویسی هم پیاده کنید. مثلا جمله «رتبه من در کنکور سراسری ۴۳۸ بود. من درس ریاضی را ٪۵۴ زده بودم.» می تواند به صورت زیر دربیاید:

Rotbeye man dar konkoore sarasari ۴۳۸bood. Man darse riazi ra ٪۵۴zade boodam.

در نتیجه رمز عبور شما .zb٪۵۴b.Mdrr۴۳۸Rmdks خواهد بود.

آشنایی با روش Passphrase / Diceware

توصیه های رایج را در ابتدای مطلب بررسی کردیم، اما نمی توان گفت فقط این توصیه ها مناسب هستند. XKCD در مورد روند انتخاب پسورد از چندسال پیش تا الان -که روش ها جدیدتر شده- ، یک تصویر جالب درست کرده که آن را در ادامه مطلب می بینید. می توانید تمامی روش های گفته شده در بالا را فراموش کنید و این روش جالب را یاد بگیرید. در این روش شما چهار کلمه تصادفی و کاملا بی ربط به هم را پیدا می کنید و آنها را به هم می چسبانید تا یک رمز عبور درست شود. پسوردی که دارای چندین کلمه است. میزان تصادفی بودن کلمه ها و طول بیشتر آنها باعث قوی تر شدن این رمز عبور می شود.

مهم ترین نکته در این روش، تصادفی بودن کلمات است. مثلا "cat in the hat" (گربه در کلاه) اصلا رمز خوبی نیست؛ زیرا یک جمله رایج است و کلمات با هم تناسب دارند. یا " my beautiful red house" (خانه قرمز من) هم می تواند نامناسب باشد، چرا که کلمات از نظر معنایی و گرامری به درستی در کنار هم قرار گرفته اند. اما عبارت هایی مثل " correct horse battery staple" یا "seashell glaring molasses invisible" تصادفی هستند؛ چرا که این کلمات در کنار هم معنایی تولید نمی کنند و از نظر گرامر هم به درستی در کنار هم قرار ندارند که این دو نکته دلیل مناسب بودن دو عبارت گفته شده هستند. همچنین به خاطر سپردن رمزهایی که به کمک این روش ایجاد می شوند، باید ساده تر از پسوردهای تصادفی رایج باشد.

معمولا نمی توان کلمات را کاملا تصادفی انتخاب کرد. در نتیجه قصد داریم در اینجا یک ابزار مفید معرفی کنیم. وبسایت Diceware لیست مرتبی از کلمات را آماده کرده و به هرکدام یک شماره اختصاص داده. طرز کار این است که شما به کمک یک تاس ساده (که در بازی ها استفاده می شود) ۵ بار تاس می اندازید و اگر بعد از هر بار انداختن، عدد آن را یادداشت کنید، در پایان

یک عدد ۵ رقمی خواهید داشت که در لیست موجود در سایت Diceware نشان دهنده یک کلمه یا علامت تصادفی است. اگر این روند را ۴ بار انجام دهید، پسورد تصادفی شما با امنیت بالا آماده است. این روش، روش خوبی برای انتخاب یک رمز عبور تصادفی است، چرا که مطمئنید ترکیب این کلمات یک ترکیب کاملا تصادفی است. حتی ممکن است یکی از کلمات انتخاب شده، از واژگان روزمره مورد استفاده شما نباشد.

خالق Diceware پیشنهاد می دهد که در رمزهای عبور حداقل از ۶ کلمه استفاده شود؛ چرا که به دلیل پیشرفت در دنیای هک، کرک کردن پسوردها راحت تر شده.

مطالبی که گفته شد، تنها چیزهایی نیست که باید در مورد قوی بودن رمز عبورتان بدانید. مثلا یک نکته مهم این است که اگر شما از یک رمز عبور یکسان برای محل های متفاوت استفاده کنید، ممکن است از یکی از آنها پسورد شما لو برود و در نتیجه افراد به حساب های دیگر شما هم دسترسی پیدا کنند.

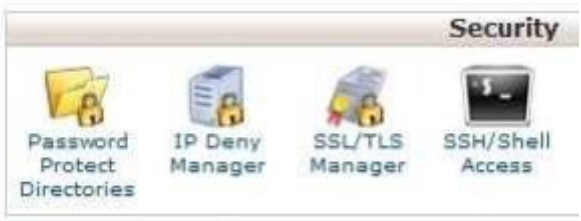
استفاده از رمزعبور منحصر به فرد، اجتناب از ورود به سایت های فیشینگ و محافظت کامپیوتر از نرم افزارهای مخربی که پسوردهای شما را کپچر می کنند نیز از دیگر نکته های مهم است.

درست است که باید یک رمز عبور قوی انتخاب کنید، اما انتخاب پسوردهای قوی تر منجر به محافظت بیشتر شما در مقابل همه تهدیدهای سایبری نخواهد شد؛ البته این کار یک قدم اول خوب محسوب می شود.

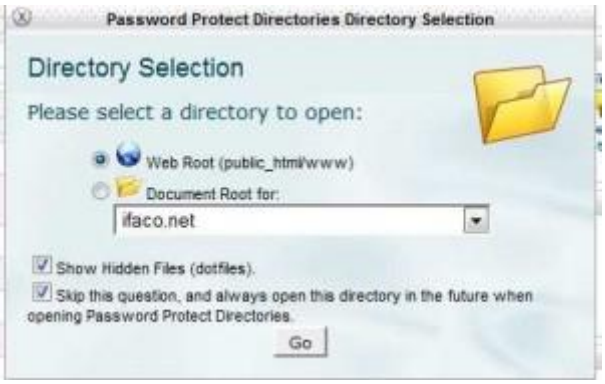
برروی پوشه ادمین خود رمز بگذارید

با توجه به اینکه اخیرا مشاهده شده است که اسکریپت معروف و پرطرفدار جوملا را از طریق باگهای موجود در قسمت مدیریت (Administrator) آن هک می کنند و در سایت ها خرابکاری می نمایند و باعث به هدر رفتن زحمات شما عزیزان میشوند، لذا سعی کنید در اولین فرصت ممکن روی شاخه آدمین جوملا در داخل سی پنل هاست به سبک آموزش تصویری ذیل پسورد گذاری مضاعف کنید تا حداقل نتوانند از طریق باگ مدیریت به قسمت مدیریت سایت تان وارد شوند.

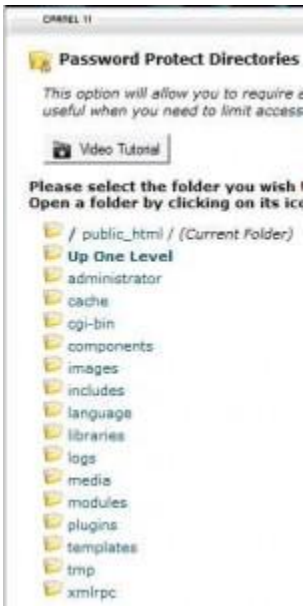
مرحله اول در صفحه اول سی پنل روی گزینه Password Protect Directories کلیک نمایید.



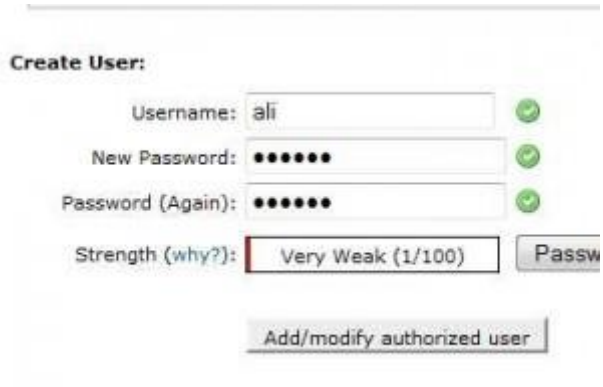
مرحله دوم چک باکس را به سبک زیر تیک بزنید.



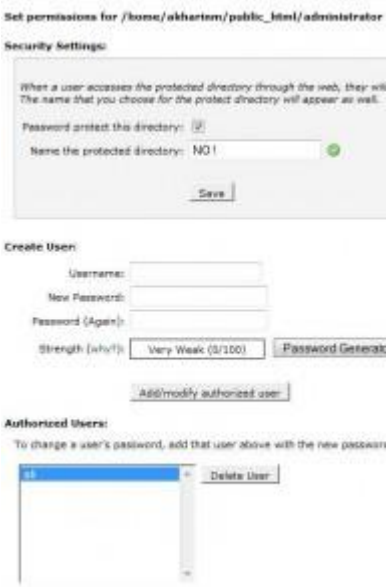
مرحله سوم روی نام شاخه Administrator کلیک کنید تا صفحه بعدی باز شود.



در مرحله چهارم باید یک یوزر و پسورد در کادرهای مربوطه درج کنید و دکمه Add را بزنید تا ساخته شود.



در مرحله آخر روی نام یوزر ساخته شده قبلی در کادر روبروی Authorized Users کلیک نمایید تا آبی رنگ شود سپس در بالای صفحه در قسمت Security Settings ، گزینه Password protect this directory را تیک بزنید و در کادر خالی Name the protected directory یک نام اختیاری مانند No Access ! و ... تایپ کنید و سپس دکمه Save را بزنید تا کار پسورد گذاری امنیتی تکمیل شود.



نکته : جهت تست موفقیت کار وارد Administrator جوملای سایت تان بشوید تا صفحه درخواست یوزر و پسورد ساخته شده در این قسمت نمایان شود و چنانچه یوزر و پسورد مورد نظر بیشتر از ۳ مرتبه اشتباه وارد شود، آی پی فرد وارد کننده پسورد اشتباهی توسط فایروال سرور مسدود خواهد گردید و دسترسی اش از سایت شما کوتاه خواهد شد !

تغییر پیشوند جداول پیشفرض جوملا

همانطور که میدانیم زمانی جوملا خود را نصب می کنید در پایگاه داده جداول مرتبط با جوملا با پیشوند jos_ ساخته میشود از آنجایی این پیشوند در تمامی سایت های جوملایی به صورت پیش فرض ایجاد میشود لذا یک هکر میداند در صورتی که یک سایت بر پایه مدیریت محتوا جوملا باشد جداول پایگاه داده آن سایت با jos_ شروع میشود لذا راحت تر به برخی از جداول دست پیدا مینماید از طرفی برنامه اسکن سایت های جوملایی نیز به صورت پیش فرض با این پیشوند کار میکنند البته این مشکل در جوملا ۱,۶ و ۱,۷ مرتفع شده است اما جوملا نگارش ۱,۵ از این قائده مستثنی نیست . لذا در یک گام جهت ارتقا امنیت سایت میباید این پیشوند ها را تغییر داد.

افزونه ای که پیش رو دارید برای جوملا ۱ به نگارش در آمده است اما با جوملا ۱,۵ هم همخوانی دارد . ابتدا پلاگین ارث بری را فعال و افزونه را نصب کنید. (برای دانلود پلاگین اینجا کلیک کنید.)

در جعبه اولی پیشوند فعلی جداول پایگاه داده نوشته شده است که معمولا jos_ میباشد . در جعبه دوم پیشوند دلخواه را وارد نمایید به عنوان مثال joomina_

حال بر روی Update Tabel Prefixes کلیک کنید.

نگران نباشید ! وارد روت جوملا خود شده و فایل configuration.php را ویرایش کنید در این فایل به دنبال عبارت زیر گشته و آن را با پیشوند جداولی که انتخاب نموده اید جایگزین نمایید.

var $dbprefix = 'joomina_'; ← var $dbprefix = 'jos_';

کار تمام است.

بروز نگه داشتن جوملا

باور کنید یکی از مهمترین نکات در هک نشدن سایت های جوملایی بروز نگه داشتن نشخه جوملا است بارها شده از من سئوال شده که چگونه نسخه بروز رسانی جوملا را نصب کنیم (با توجه به اینکه سایت های پشتیبان جوملا معمولا با تاخیر نشخه های بروز رسانی فارسی را منتشر میکنند) بهترین کار این است که به خود سایت joomla.org رفته و بسته بروز رسانی را دانلود نمایید . از طرفی سایت های وزین ایرانی هم هستند که گرچه با تاخیر یکی دو روزه اما این نسخه ها را منتشر میکنند که معتبر ترین آن ها جومفا ، گروه مامبو و جوملا دات ای ار است هر سه گروه نسخه های ترجمه شده خوبی از جوملا ۱,۵ دارند و الالخصوص که جومفا هم توزیع کننده زبان منطقه ای جوملا جهانی برای جوملا ۱,۵ در این بوده است.

SEF سایت خود را فعال کنید

نمیدونم تا حالا فکر که میشه با سئو هم امنیت سایتُ ارتقاع داد !؟

برای بهینه سازی وبسایت برای موتورهای جستجو مباحثی مثل سئو (seo) و سِف (sef) وجود داره. بطور خلاصه؛ sef اصلاح کننده یا به اصطلاح کوتاه کننده لینک های یک سایت هست.

اهمیت این نکته زمانی حس میشه که شما توی سایتتون از افزونه ها و پلاگین های مختلفی استفاده کنید. ممکنه برخی از افزونه ها دارای حفره های امنیتی باشند و اگه sef در سایت شما فعال نشده باشه، هکرها میتونن با استفاده از موتور جستجو گوگل نام افزونه و پلاگینی که شما برای سایتتون نصب کردین جستجو کنن و به راحتی سایت شما رو مورد حمله قرار بدن. برای فعال کردن sef در جوملا کافیه به روت سایت خودتون برید (میتونید از فایل منیجر هاست یا نرم افزارهای مدیریت فایل استفاده کنید) و فایل htaccess.txt تغییر نام بدید. بطوریکه txt. را از انتهای htaccess.txt پاک کنید و در ابتدای اون یک "." (نقطه) بذارید.

توجه کنید، زمانی که وارد فایل منیجر میشید از شما پرسیده میشه که فایل های مخفی نمایش داده بشه یا خیر

htaccess. برای سرور ها فایل مخفی شناخته میشه، به همین دلیل ممکنه بعد از تغییر نام این فایل، دیگه نتونید اونُ ببینید. و این نشون دهنده اینه که شما کارتونُ درست انجام دادید.

در مرحله بعد؛

وارد پنل مدیریت سایت جوملای خودتون بشید و از تب سایت به قسمت تنظیمات اصلی یا پیکربندی برید و در قسمت تنظیمات سئو (seo)، همه گزینه ها رو با قرار دادن روی " بله " فعال کنید.

توجه کنید، بعضی از سرورها با فعال کردن تمام موارد مشکل دارن، برای همین میتونید گزینه هارو بصورت تک تک فعال کنید و تنظیمات مربوط به اونُ ذخیره کنید.

بعضی وقت ها هم فایروالی که روی سایت جوملا نصب کردید اجازه این تغییرات به شما نمیده، برای این کار بطور موقت فایروال سایتُ غیرفعال کنید و بعد از انجام این تغییرات اونُ مجددا فعال کنید.

استفاده از htaccess. جهت ارتقا امنیت

فایل htaccess در حقیقت روشهای پردازش وب سرور را برروی وب سایت شما مشخص میکند. چند دستور وجود دارد که شما امکان اضافه کردن آنها را به انتهای فایل htaccess تان دارید و با این کار میتوانید انتظار افزایش کارایی از وب سایت تان را داشته باشید.

دستور ETag : این دستور به مرورگرها میگوید اگر یک تصویر از قبل دانلود شده بود مرورگر میتواند آنرا از کش داخلی مربوط به خود فراخوانی کند به جای آنکه آن تصویر را از وب سرور فراخوانی کند.

دستور Expires headers : عملکرد این دستور همانند ETag است اما با این تفاوت که میتواند برای مجموعه از انواع فایلها زمان انقضا تعریف کند تا در آن زمان از کش داخلی مرورگر استفاده شود.

دستور AddOutputFilterByType DEFLATE : این دستور باعث می شود فضاهای خالی و خطوط فاصله هنگام انتقال صفحات HTML به صورت کد شده منتقل شوند.

```
########## Begin - ETag Optimization
## This rule will create an ETag for files based only on the modification
## timestamp and their size.
## Note: It may cause problems on your server and you may need to remove
it
FileETag MTime Size
# AddOutputFilterByType is now deprecated by Apache. Use mod_filter in
the future.
AddOutputFilterByType DEFLATE text/plain text/html text/xml text/css
application/xml application/xhtml+xml application/rss+xml
application/javascript application/x-javascript
# Enable expiration control
ExpiresActive On
# Default expiration: ۱ hour after request
ExpiresDefault "now plus ۱ hour"
# CSS and JS expiration: ۱ week after request
ExpiresByType text/css "now plus ۱ week"
ExpiresByType application/javascript "now plus ۱ week"
ExpiresByType application/x-javascript "now plus ۱ week"

# Image files expiration: ۱ month after request
ExpiresByType image/bmp "now plus ۱ month"
ExpiresByType image/gif "now plus ۱ month"
ExpiresByType image/jpeg "now plus ۱ month"
ExpiresByType image/jp۲ "now plus ۱ month"
ExpiresByType image/pipeg "now plus ۱ month"
ExpiresByType image/png "now plus ۱ month"
ExpiresByType image/svg+xml "now plus ۱ month"
ExpiresByType image/tiff "now plus ۱ month"
ExpiresByType image/vnd.microsoft.icon "now plus ۱ month"
ExpiresByType image/x-icon "now plus ۱ month"
ExpiresByType image/ico "now plus ۱ month"
ExpiresByType image/icon "now plus ۱ month"
ExpiresByType text/ico "now plus ۱ month"
ExpiresByType application/ico "now plus ۱ month"
ExpiresByType image/vnd.wap.wbmp "now plus ۱ month"
ExpiresByType application/vnd.wap.wbxml "now plus ۱ month"

ExpiresByType application/smil "now plus ۱ month"
# Audio files expiration: ۱ month after request
ExpiresByType audio/basic "now plus ۱ month"
ExpiresByType audio/mid "now plus ۱ month"
ExpiresByType audio/midi "now plus ۱ month"
```

```
ExpiresByType audio/mpeg "now plus ١ month"
ExpiresByType audio/x-aiff "now plus ١ month"
ExpiresByType audio/x-mpegurl "now plus ١ month"
ExpiresByType audio/x-pn-realaudio "now plus ١ month"
ExpiresByType audio/x-wav "now plus ١ month"

# Movie files expiration: ١ month after request
ExpiresByType application/x-shockwave-flash "now plus ١ month"
ExpiresByType x-world/x-vrml "now plus ١ month"
ExpiresByType video/x-msvideo "now plus ١ month"
ExpiresByType video/mpeg "now plus ١ month"
ExpiresByType video/mp٤ "now plus ١ month"
ExpiresByType video/quicktime "now plus ١ month"
ExpiresByType video/x-la-asf "now plus ١ month"
ExpiresByType video/x-ms-asf "now plus ١ month"
```

افزونه های مورد استفاده خود را بروز نگه داریدافزونه هایی که در سایت خود استفاده می‌نمایید را همواره بروز نگه دارید

به عنوان مدیر یک سایت این وظیفه شما است که از بروز بودن افزونه های سایت خود مطمئن باشید برای این کار میتوانید دائما به سایت های انتشار دهنده این افزونه ها سر بزنید و از بروز بودن آن ها اطمینان حاصل کنید .و البته بسیاری از افزونه در قسمت مدیریتشان نسخه افزونه را اعلام می کنند.

حذف افزونه و فایل های غیر ضروری

هر افزونه ای که در وب سایت شما نصب و اجرا میشود نیاز به یک سری منابع نظیر فضا در سرور و پایگاه داده و ... دارد اگر چندین افزونه دارید که از آنها استفاده نمیشود باعث هدر رفتن منابع میشود.

در بسیاری از موارد مدیران سایت ها پلاگین ها و ماژول ها و کامپوننت هایی را در سایت نصب و تست می کنند اما فراموش میکنند که آنها را پاک کنند لذا پاک کردن افزونه های بلااستفاده بسیار حایز اهمیت است.

طول عمر کش را زیاد نکنید

این گزینه در پیکربندی سایت قرار داد و برخی موارد دیده ام که طول عمر کش را برخی از سایت زیاد میکنند تا تعداد میهمانان را زیاد نشان دهد . ببینید در پوشه کش جوملا نام کاربری و رمز ورود شما تا زمانی که جلسه کاری به پایان نرسد وجود خواهد داشت و سیستم شما را وارد شده فرض میکند کافی است هکر به این پوشه و پوشه لاگ دسترسی پیدا کند و .... (راه استخراج را به دلایل امنیتی ذکر نمیکنیم)

فایل های index.html موجود در پوشه ها را پاک نکنید

این فایل یک صفحه سفید را نمایش میدهد یعنی اگر کسی مستقیما آدرس یک پوشه را وارد نماید با یک صفحه سفید روبرو میشود . این مورد مخصوصا در پوشه tmp , logs خیلی مهم است

از سایت هایی که سایت شما را به صورت رایگان اسکن میکنند استفاده نمایید نمونه این سایت ها را میتوانید از اینجا ببینید.

به غیر مواقع لازم از FTP استفاده نکنید

در صورتیکه از سروری که از su_php استفاده مینماید بهره می برید نیازی به فعال سازی ftp نیست. حال فرض کنید که اینطور نباشد . در صورتی که ftp را فعال نمایید مشخصات ان در فایل config شما ثبت می شود حال اگر هکر به این فایل دسترسی پیدا کند کل سایت شما در دستان وی خواهد بود ! به همین دلیل اگر هم مجبور شدید ftp را فعال کنید پس از استفاده ان را غیر فعال (نام کاربری و رمز عبور آن را عوض کنید) نمایید . گرچه فعال بودن ftp باعث بهبود سرعت سایت شما می شود.

فایل config خود را کد کنید

شما میتوانید این فایل را که تمامی مشخصات شما در آن قرار دارد کد نمایید گرچه کد شکن همه نرم افزار ها موجود است اما باز هم کار را کمی برای هکر سخت میکند در این مورد بهتر است با سرپرست سرور صحبت نمایید.

این موارد تنها خلاصه ای از مواردی است که باید در سایت های خود بکار ببرید . موارد دیگری از جمله تغییر مکان فایل config و تغییر شناسه admin از ۶۲ به عددی دیگر و ... وجود دارد.

منابع :

جومینا

دانشنامه جوملا فارسی