نوشته شده توسط Administrator
شنبه ۱۶ آبان ۱۳۸۸ ساعت ۱۶:۳۹ - آخرین به روز رسانی شنبه ۱۶ آبان ۱۳۸۸ ساعت ۱۶:۴۴

پیکربندی جوملا!

نصب نسخههای رسمی جوملا!

برای جلوگیری از اختلال و خرابی (هک) در سایت خود، مستندات و آموزش ها، اخبار و اطلاعیهها و بخش های پشتیبانی تخصصی جوملا! را برای آگاهی از امکانات ناسازگار، پیش از بهروز رسانی به یک نسخه بالاتر مطالعه کنید.

در کوتاهترین زمان ممکن، سایت خود را با آخرین نسخه جوملا!به روز کنید.

جوملا! را تنها از سایتهای رسمی، مانند JoomlaCode.orgدانلود کنید و کددرهم MD5را بررسی کنید.

برای کسب اطمینان از نصب صحیح فایلها، از تشخیصهای جوملا!استفاده کنید. (توجه: تشخیصهای جوملا برای نسخههای ابتدایی 1.5 ساخته شده است و برای نسخههای جدیدتر در حال توسعه می باشد. شناسه (name user) پیش فرض مدیریت سایت را تغییر دهید

شناسه پیش فرض کاربر مدیر سایت (admin) را تغییر دهید. این تغییر ساده، تاثیر بسیار فراوانی در بالابردن امنیت سایت شما تا 50٪ دارد، زیرا با تغییر آن نفوذگران و خرابکاران باید برای دسترسی به آن، پیشتر از نام آن مطلع باشند. گذرواژه گزینه بعدی میباشد که اهمیت دارد، آن را همواره و به تناوب تغییر دهید.

فایلها و دایرکتوریها را محافظت کنید

با تغییر مکان فایل configuration.php (پیکربندی کلی) خارج از دایرکتوری public_html امنیت این فایل مهم و حیاتی را افزایش دهید. برای اطلاعات بیشتر به (FAQ) مراجعه کنید.
به یاد داشته باشید که تمامی مسیرهای تنظیمشده در حالت قابل ویرایش و قابلبارگذاری (مانند: حافظه نهانگاهی، گالریهای تصاویر، محل ذخیره اسناد و...) خارج از دایرکتوری public_html قرار دارند. همچنین امکانات اضافی و غیرهسته مانند

DOCMan و Gallery2 را برای مسیرهای قابلویرایش و قابلنوشتن بررسی کنید.

در پیکربندی کلی بخش مدیریت، مسیر ثبت وقایع را تغییر دهید. برخی از امکانات از ساختار JLog class استفاده میکنند. به صورت پیشفرض، ثبت وقایع در پوشه logs/yoursite//:http نوشته میشود. آنرا جایی قرار دهید که مرورگر نتواند آنرا بیابد. زیرا ما با یک نرم افزار متنباز سروکار داریم و نفوذگران میتوانند کدهای امکانات غیرهسته را بخوانند و ممکن است نام فایلهای ثبت وقایع را حدس بزنند.

در پیکربندی کلی بخش مدیریت، مسیر پوشه صفحات موقت (temp) را تغییر دهید.
اگر مسیر پوشههای صفحات موقت و ثبت وقایع تغییر داده شده باشند و PHP open_basedir به درستی تنظیم شده باشد، مطمئن شوید که مسیرهای جدید در حوزه open_basedir قرار میگیرند.
در حال حاضر هیچ راه آسانی برای انتقال دایرکتوریهای /image و /media جوملا! وجود ندارد. این به آن دلیل است که هزاران امکان غیرهسته باید این دایرکتوریهای مهم را در جایگاه فعلیشان بیابند. بهترین نقشه برای کسب اطمینان از open_basedir تنظیم صحیح آن برای تمامی حسابهای کاربری بر روی سرور اختصاصی است. آن را با پشتیبان فضای وب خود بررسی کنید، اگر مطمئن نیستید.

تنظیم (سطح دسترسی) مجوزهای فایل و دایرکتوری (Permissions)

هنگامی که پیکربندی سایت شما کامل و پایدار شد، پوشههای مهم را از نوشتن محافظت کنید (write-protect). برای این کار مجوزهای پوشه را به 755 تغییر دهید و مجوزهای فایل را به 644. ویژگی و امکانی در پیکربندی کلی سایت هست که سرور تمامی مجوزهای فایل و پوشه را یک جا تنظیم میکند. پس از آن امکانات غیرهسته را امتحان کنید و کدهای آنها را بادقت بررسی نمایید تا مشکلی با تنظیمات آن نداشته باشید.

فایلهای غیرضروری را پاک کنید

تمامی قالبهای طراحی شده در سایت را که از آنها استفاده نمیکنید و به آنها نیاز ندارید را پاک کنید.

XML-RPC سرور را اگر به آن نیاز ندارید، حذف کنید.
پس از نصب، پاک کنید! پردازش نصب نیامند حذف دایرکتوری نصب و تمامی محتویات آن خواهد بود. حتما آن را حذف کنید و به سادگی تنها آن را تغییرنام ندهید. اگر فایلها را به صورت فشرده بارگذاری کردید، پس از نصب فایل فشرده را حذف کنید. پوشه /temp/ را بررسی کنید، شاید فایلهای موقت نصب در آن باقی مانده باشند. به صورت کلی، هیچ فایل غیرضروری (فشرده یا غیره) را در یک سرور عمومی رها نکنید. هر فایل استفاده نشدهای پتانسیل تبدیل به یک حفره امنیتی را دارد.

نوشته شده توسط Administrator
شنبه ۱۶ آبان ۱۳۸۸ ساعت ۱۶:۳۹ - آخرین به روز رسانی شنبه ۱۶ آبان ۱۳۸۸ ساعت ۱۶:۴۴

کنید خاموش را Register Globals Emulation

Register Globals Emulation **جوملا را خاموش کنید. اگر چه این تنظیم پاری اوقات ایمنتر از** PHP register_globals **است، اما بسیار بهتر است که همهی این تنظیمات را خاموش کنید. در نسخههای پیش از** 1.0.13 **جوملا، این تنظیم در فایل** globals.php **قرار دارد. اگر شما از نسخه** 1.0.13 **استفاده میکنید، میتوانید آن را در پیکربندی کلی بخش مدیریت خاموش کنید.**

جوملا 1.5 **از** register globals **استفاده نمیکند و در حقیقت کدهایی هوشمند برای مقابله با این تنظیم در صورتی که در سطح** PHP **روشن باشد دارد. توجه داشته باشید باوجود اینکه این تنظیم جوملا را ایمنتر میکند، اما هر سروری که** register globals **آن روشن باشد، پتانسیل آسیبپذیری را دارد. هر سرور اشتراکی که** register globals **آن روشن باشد مانند کشتی به گِل نشسته است.**

نصب امکانات جوملا!

پیش از نصب نسخه پشتیبان (backup) **تهیه کنید**

پیش از نصب امکانات، همیشه از فایلها و پایگاه داده خود نسخه پشتیبان تهیه کنید. یک اصل پایهای موجود است:

تو باید در هر زمانی که خواستی، بتوانی به سایت پایدار قبلیت که کار میکرد از طریق یک نسخه پشتیبان قوی و پردازش بازیافت، بازگردی.

بنابراین، هوشیارانه خواهد بود نوشتن یک اسکریپت کوچک برای تهیه آسان و سریع نسخه پشتیبان به صورت خودکار. اگر شما این پروسه آسان را انجام ندهید و بدون تهیه نسخه پشتیبان اقدام به بهروز رسانی و ارتقای سایت خود کنید، ممکن است با عواقب سنگینی روبهرو شوید.

آسیبپذیری امکانات را بررسی کنید

اکثر آسیبپذیریهای امنیتی به سبب امکانات غیرهسته میباشد. پیش از نصب امکانات، حتما فهرست رسمی امکانات غیرهستهای را مطالعه کنید.

تنها از سایتهای قابل اطمینان دانلود کنید

تعریف، معنای و منظور کامل و صحیح از واژه قابل اطمینان، سایتهایی هستند که شما به آنها اطمینان دارید!

آزمایش، آزمایش، آزمایش...

تمام امکانات غیرهسته را پیش از نصب بر روی سایت اصلی خوب بر روی یک سایت محلی (localhost) آزمایش کنید. فراموش نکنید که گزارشهای خطای زمان اجرا و هشدارها را بررسی کنید.

فایلهای بیمصرف را حذف کنید

تمامی امکاناتی که از آنها استفاده نمی کنید و پوشه و فایلهای مربوط به آنها را حذف کنید. توجه داشته باشید که در هنگام حذف (uninstall) امکانات غیرهسته برخی از فایلهای مرتبط با آنها بر روی سایت شما و جداول پایگاه داده شما باقی میمانند. هر فایلی که بر جا بماند، بر روی سرور شما باقی میمانند و از طریق نشانی اینترنتی مستقیم وب مانند: http://yousite.com/modules/bad_module. قابل دسترسی میباشند.

از کدهای رمز شده جلوگیری کنید

جوملا! یک پروژه GNU GPL است. این به آن معناست که تمام امکانات جوملا! هم باید آزاد و باز (به معنای خواندن کدها) باشند. کدهای رمزشده ممکن است ایمن باشند، اما شما نمیتوانید تصمیم بگیرید که باید به برنامهنویس و گسترشدهنده آن اعتماد کنید یا خیر.

شما اغلب اجازه ویرایش، بهبود و یا به اشتراک گذاشتن کدهای رمزشده را ندارید. این محدودیت کدهای رمز شده را در نزد اجتماع کاربران کم ارزشتر کرده است و گرایش کاربران را به پروژه جوملا که مبنی بر اشتراک آزاد و باز منابع (open source) برای تمامی استفاده کنندگان است را افزایش داده است.

نکتهها و ترفندهای دیگر جوملا!

از سرورهای اشتراکی (Hosting Share) تا جایی که ممکن است اجتناب کنید

برای بیشترین حد امنیت، از سرورهای اشتراکی اجتناب کنید، مخصوصا آنهایی که شما از همسایگان و دیگر کاربرانی که از آن استفاده میکنند، اطلاع ندارید.

از یک سرور دارای SSL استفاده کنید

سرورهای SSL درحال حاضر تنها راهِ پردازش تراکنشهای محرمانه و ایمن بین کاربران است. SSL با رمزگذاری تمامی ارتباطات HTTP بین وب سرورها و کاربران بیشترین میزان امنیت را تامین میکند.

متاسفانه جوملا! 1.0 به شما اجازه اختصاص یک سرور SSL را به یک زیردایرکتوری خاص و شخصی نمیدهد. اما جوملا 1.5 به نحو شگفتانگیزی دررابطه با SSL و امکانات و گزینههای آن پیشرفت کرده است.

از htacces. s'Apache استفاده کنید

به عنوان یک لایه اضافی در امنیت و حفاظت گذرواژه، شما میتوانید از htaccess. برای محافظت گذرواژه دایرکتوریهای مهم استفاده کنید. این کار معمولا برای جلوگیری از اسکریپتهای مخرب معمولی کافی است اما آگاه باشید که .htaccess به تنها برای تامین امنیت کافی نیست. این باید با یک سرور SSL ترکیب شود. سرور SSL نیاز امنیت سایت شما در برابر حملات قدرتمند و خطرناک است.

از جوملا! 1.5 استفاده کنید

ارتقا جوملا! به نسخه 1.5 تضمینکننده امنیت بالا و افزایش کارکرد و عملکرد سایت شما میباشد.