جوملا، یک نرم افزار مدیریت محتوای وب‌سایت و پورتال است که به شما کمک می‌کند در سریع ترین زمان و بدون نیاز به داشتن تخصص فنی، یک وب سایت کاملا حرفه‌ای را ایجاد و مدیریت کنید. انعطاف‌پذیری فوق العاده و معماری منحصر به فرد آن به شما اجازه می‌دهد در هر زمانی که بخواهید، امکانات جدیدی را به وب سایت یا پورتال خود اضافه کرده و از آن استفاده کنید.

از مزایای جوملا، تغییر در ساختار، چینش ماژول‌ها و گرافیک است که می‌توانید آنها را سفارشی‌سازی کنید. شما با جوملا می‌توانید به دور از هر گونه وابستگی به برنامه نویسان و متخصصان وب، محتویات متنی و تصویری سایت خود را بصورت آنلاین، بدون محدودیت مکانی و زمانی بطور چندگانه مدیریت کنید.

از نقاط قوت سیستم مدیریت محتوای جوملا این است که هیچگونه محدودیتی در سفارشی‌سازی، توسعه، پشتیبانی و امنیت (که از دغدغه‌ها و خواسته‌های اکثر مشتریان است) ندارد و می‌تواند به عنوان بستری مناسب و مطمئن برای یک فعالیت بلند مدت مورد استفاده قرار گیرد.

امکانات زیاد جوملا، کاربردهای آن را در دنیای وب سایت‌های اینترنتی گسترش داده است. انواع وب سایت های تجاری کوچک، وب سایت های سازمانی بزرگ، کسب و کار آنلاین و تجارت الکترونیک، پورتال های خدمات الکترونیک، وب سایت های سازمان های دولتی، سایت های مذهبی، وب سایت های آموزشی و پورتال های آموزش الکترونیک، وب سایتهای خبری و حتی وب سایت های شخصی کوچک، را می‌توان بوسیله پیاده‌سازی کرد.

جوملا! می تواند به سادگی در کنترل تمامی قسمت های وب سایت شما، از اضافه کردن محتوا و تصویر تا به روز رسانی کاتالوگ محصولات و یا رزرواسیون آنلاین استفاده شود.

جوملا برای چه کسانی است؟

جوملا به دلیل قابلیت‌های ویژه‌ای که از لحاظ امکانات برنامه نویسی دارا می باشد، نه تنها کاربران عادی که متخصصان و برنامه نویسان وب را نیز به خود جلب کرده است. برنامه نویسان حرفه‌ای در کنار مجموعه عظیمی از افزونه‌های طراحی شده توسط دیگر برنامه نویسان، امکان تولید بسته های جدید را بر اساس بستر جوملا دارا می‌باشند. این موضوع جوملا را به عنوان گزینه مناسبی برای پیاده سازی انواع پروژه‌ها و نرم افزارهای کاربردی مطرح ساخته است.

چه کسانی از جوملا استفاده می کنند؟

جوملا! در سراسر دنیای اینترنت از یک صفحه شخصی ساده گرفته تا پیچیده ترین نرم افزارهای شرکتی تحت وب را پشتیبانی می کند. در ذیل تنها تعداد اندکی از روش هایی که کاربران برای استفاده از جوملا بکار می برند آمده است:

- وب سایت ها یا پورتال های شرکتی
- نرم افزارهای تجاری تحت وب
- برنامه های کاربردی دولتی
- شبکه های داخل و خارجی شرکتی
- پورتال های بر پایه انجمن
- صفحات وب شخصی یا خانوادگی
- روزنامه ها و مجلات
- وب سایت های کوچک خرید و فروش

جوملا برای چه کسانی است؟

جوملا خیلی بیشتر از یک سیستم مدیریت محتوای قدرتمند است. در این جا لیستی از ویژگی های جوملا برای شما گفته می شود، اما قدرت واقعی جوملا در قابلیت توسعه پذیری آن است.

- ✓ ذخیره شدن تمامی اطلاعات در پایگاه داده
- ✓ مدیریت و ویرایش اخبار، محصولات و سرویس ها
- ✓ افزودن عنوان به بخش ها به وسیله نویسنده
- ✓ سفارشی سازی منوها در قسمت چپ ، راست و وسط
- ✓ انجمن پویا/ نظرسنجی/ بازیدها و نتایج نقطه به نقطه
- ✓ قابل اجرا با Linux, FreeBSD, MacOSX server, Solaris, وAIX
- ✓ نصب و راه اندازی آن آسان است و پیش نیاز تکنولوژیک و یا نرم افزاری خاصی ندارد. (Windows/Linux)
- ✓ توسط گروه زیادی از جامعه کاربران جوملا پشتیبانی ، تست و رفع ایراد می شود
- ✓ بیش از ۱۰۰۰۰ ماژول و افزونه موجود (تا این لحظه)در تالارهای گفتگوی جوملا بیش از ۲ میلیون پست در موضوعات مختلف موجود است
- ✓ بطور مداوم هسته اصلی آن بروز می شود
- ✓ برای انطباق انواع قالب طراحی برروی آن ، بسیار انعطاف پذیر می باشد
- ✓ منطبق با استانداردهای موتورهای جستجو است(Search engine Friendly)
- ✓ براحتی می توان ماژول ها، کامپوننت ها و قالب های مورد نیاز را برای آن پیاده سازی کرد
- ✓ قابلیت سفارشی سازی آن بسیار بالاست. (Customization)
- ✓ با استفاده از مدیریت سطوح دسترسی ، مدیریت کاربران و مدیریت گردش کار می توان مدل های مختلف کاری ، بروزرسانی سایت و انتشار محتوا را برروی آن پیاده کرد
- ✓ قابلیت اتصال به سایر نرم افزار ها و بانک های اطلاعاتی
- ✓ انواع فرم ساز و گزارش ساز قوی موجودراحتی کار با پانل مدیریتی و مدیریت قوی محتوا (پشتیبانی از انواع زبانها ، انواع Editorها و ...)
- ✓ قابل استفاده برای انواع وب سایت و نرم افزار تحت وب برای منظورهای مختلف
- ✓ در دسترس بودن متخصصین ایرانی و خارجی زیاد برای پشتیبانیهای آتی
- ✓ براحتی امکان اتصال به سایر نرم افزارها در نقش یک پورتال را دارد.

مدیریت گسترده:

- پشتیبانی از ثبت APIهای غیر مجاز
- توابع JToolBarHelper برای دکمه های "ذخیره" ، "ذخیره و جدید" و "ذخیره به عنوان کپی"
- Mod_custom به همراه تصاویر زمینه
- اجازه انتخاب از پیش تعیین شده مجموعه ها در قسمت مدیریت مطالب com_content
- افزودن دستورالعمل های JFormRuleOptions برای ارزیابی type="list" در پارامترها
- امکان کپی/انتقال محتوای کامپوننت ها
- به روز رسانی ویرایشگر TinyMCE به نسخه ۳.۴
- پارامترهای جدیدی برای انتخاب گر زبان
- قابلیت تغییر فونت های سایت با گذاشتن یک فایل CSS در فایل های بخش مدیریت پکیج
- در قسمت مدیریت زبان زبان های نصب شده در چندین تب جداگانه نمایش داده می شوند
- بهینه سازی نصب امکانات
- نمایش مشخصات تماس با استفاده از فرم های پویا

- JToolBar cleanup برای دکمه های "ذخیره و جدید" و "ذخیره به عنوان کپی"
- افزودن قابلیت ذخیره جستجو در گزینه های منو
- ایمیل گروهی - قابلیت عدم ارسال ایمیل به کاربران غیر فعال
- افزودن امکان نمایش کدهای PHP و HTML توسط پلاگین CodeMirror
- در نسخه های پیشین JModelList یک متغیر $ query را به صورت رشته شکل می دهد و به صورت غیر ضروری پیاده سازی Joomfish را غیر ممکن می سازد اما در نسخه جدید این مشکل برطرف شده است.
- افزودن قابلیت نمایش زمان و حافظه صرف شده به کامپوننت و ماژول ثبت اطلاعات خطایابی
- نمایش سطوح دسترسی در مدل های بخش مدیریت تست نمی شود.
- افزودن قابلیت پشتیبانی برای OpenSearch در کامپوننت جستجو (com_search)
- به روزرسانی پایگاه داده به صورت اتوماتیک
- افزودن WAI-ARIA (قابلیت هایی برای معلولین) و HTML5 که از progressbar.js پشتیبانی می کنند
- بهبود کارایی پلاگین loadmodule
- برای ویرایش نوع در بخش منوها یک صفحه lightbox باز می شود که توسط آن می توان "نوع منو" را تغییر داد.
- قابلیت تغییر زبان در گزینه های منو در تنظیمات چند زبانه سازی.
- افزودن ستون چینش به جدول jos_languages

- از PHP نسخه ۴.۳.۹ و ۴.۴.۲ و یا ۴.۰.۵ به هیچ عنوان استفاده نکنید. این نسخه ها دارای حفره های امنیتی زیادی هستند که نصب جوملای شما را با مشکل مواجه می کند. همچنین ZendOptimizer نسخه ۲.۵.۱۰ برای PHP نسخه ۴.۴ نیز دارای حفره های امنیتی بسیار خطرناکی است که باید از میزبان سایت خود بخواهید تا این نسخه را ارتقاء دهد. جوملا نسخه ۱.۵.۱۵ و بالاتر با PHP نسخه ۵.۳ کاملا سازگار است.
- جوملا هنوز با MySQL نسخه ۶ سازگاری ندارد.
- در صورتی که مایل به استفاده از آدرس های بهینه سازی شده (SEO URLs) می باشید، حتماً افزونه mod_rewrite باید بر روی آپاچی شما نصب شده باشد.
- برای مایکروسافت IIS (بسته به نوع تنظیمات آن) به موارد ذیل نیاز دارید :
- PHP نسخه ۵.۲ MySQL نسخه ۵.۱ ماژول Microsoft URL Rewrite (که فقط برای بهینه سازی آدرس های سایت)SEO (مورد نیاز است)FastCGI

جوملا یکی از محبوب ترین سامانه های مدیریت محتوای متن باز می باشد که تعداد بسیار زیاد کاربران و جوامع پویا و رو به رشد توسعه دهندگان آن گواه این مدعاست. هم اکنون بیش از ۲۰۰۰۰۰ جامعه مجازی شامل هزاران هزار کاربر و توسعه دهنده جوملا در حال فعالیت در جهت رشد و توسعه این نرم افزار قدرتمند می باشند. جوملا دو سال متوالی (یعنی در سال های ۲۰۰۶ و ۲۰۰۷) از جانب Packet Publishing به عنوان برترین نرم افزار متن باز مبتنی بر PHP معرفی شد.

اولین نسخه جوملا در سپتامبر ۲۰۰۵ منتشر شد و یکی از CMSهای متن بازی است که به کررات توسط کاربران از اینترنت دانلود شده است. هم چنین امنیت بالای این نرم افزار یکی از فاکتورهای شایان توجهی است که در اعطای این مقام به جوملا تاثیر بسزایی داشته است.جوملا به عنوان سامانه مدیریت محتوای برتر انتخاب شده و هم چنین به عنوان "نرم افزار پیشرو در بازار" گزارش شده است. به هر حال افتخارات کسب شده توسط این نرم افزار در حوزه های مختلف نرم افزاری دنیا کم نیست. جوملا مسلما کسب این افتخارات را نتیجه زحمات و مشارکت های کلیه افرادی می داند که در این پروژه عظیم به نوعی مشارکت داشته اند و به این افتخارات را با افتخار جشن می گیرد.

فهرست نکات امنیتی جوملا

با توجه به گسترش روزافزون هکرهای اینترنتی، افزایش امنیت سیستم مدیریت محتوای سایت شما بسیار مهم و حیاتی می باشد.

بسیاری از طراحان وب بیشترین زمان خود را صرف طراحی گرافیکی و بالا بردن رتبه سایت در گوگل می کنند و زمان نسبتا کمی را برای بالا بردن امنیت سایت صرف می کنند.

در مقاله اول نکات امنیتی جوملا سعی شده است تا با ارائه راه کارهای مختلف و مناسب شما را در افزایش ضریب امنیتی سیستم مدیریت محتوا جوملا یاری رسانیم.

توضیح ابتدایی:

امنیت همواره یک نگرانی است. بر روی اینترنت، امنیت همواره یک چالش همیشگی است. دو رهنمود بسیار ساده است که با رعایت آن گام بلندی را در امنیت هر وب‌سایتی برخواهید داشت. در زیر آن دو رهنمودی که سایت شما را تقریبا از هر بلایی مصنون می‌دارند، آمده‌اند.

تهیه نسخه پشتیبان :(backup) همواره از آخرین تغییرات سایت خود یک نسخه پشتیبان تهیه کنید. این‌گونه شما خواهید توانست در صورت بروز هرگونه مشکلی، داده‌های خود را بازیابی کنید.

به‌روز رسانی نرم افزار :(update) همواره پس از انتشار هر نسخه‌ی جوملا! توسط گروه، جوملای سایت خود را به روز کنید و همچنین هر یک از امکانات سایت خود را پس از انتشار نسخه‌های جدید، به‌روز کنید. این عمل باعث خواهد شد که سایت شما از هر نقص و مشکلی که در نسخه جدید برطرف شده در امان باشد و همچنین از تمامی شیوه‌های حملات جدید تا جایی که دفاع آن گسترش‌یافته وب‌سایت شما را محافظت خواهد کرد.چند نکته مهم دیگر درباره امنیت جوملا، در این چک لیست وجود دارد، که شایسته است آن‌ها را نیز مدنظر قرار دهید.

استفاده از یک میزبان فضای وب (Host) ایمن

امنیت به مسئله‌ی بزرگ میزبانی وب است. پس، یک میزبان فضای وب خوب پیـدا کنید! توجه داشته باشید که اگر هیچ تجربه یا دانشی در این ضمینه ندارید، از یک مشاور حرفه‌ای یاری بگیرید.

مراقب باشید که گول برنده شدن جایزه‌های استفاده ساده و آسان جوملا! را نخورید! برقرار نگهداشتن امنیت یک وب‌سایت پویا در محیط باز اینترنت کار آسانی نیست. امنیت کافی نیازمند فن و توانایی، دانش، مراقبت دائم، نسخه‌های پشتیبان خوب و تلاش و زحمت ادامه‌دار است. تنها یک راه درست وجود ندارد! با توجه به گوناگونی و پیچیدگی سیستم‌های مدرن وب، موضوعات امنیتی را نمی‌توان با یک راه حل ساده و قابل استفاده برای همه حل کرد. شما، یا کسی که شما به او اعتماد دارید، باید به اندازه کافی درباره شالوده‌ی سرور شما بیاموزد تا بتوانید تصمیمات امنیتی را اتخاذ کند. امنیت قوی، هدفی است که مدام در حال تغییر است. متخصصان امروز، ممکن است قربانیان فردا باشند. پس به بازی خوش آمدید... هیچ جانشینی برای تجربه وجود ندارد! برای برقراری امنیت سایت خود، شما باید تجربه واقعی را کسب کنید (که برخی از آنان تلخ خواهند بود) یا از تجربه‌ی دیگران استفاده کنید.

یک گام جلوتر از دیگران آغاز کنید

انجمن‌های امنیت جوملا! پُر است از مطالبی با عنوان "کمک! من هک شده‌ام" توسط کسانی که استانداردهای امنیتی را رعایت نکرده‌اند. اگر شما قصد مطالعه‌ی این چک لیست را پیش از آن که به سایت شما حمله شود را دارید، واقعا جای تبریک دارد، شما یک گام جلوتر از دیگران هستید!

به آن دشواری که به نظر می‌رسد نیست

اگر این یکی از نخستین وب‌سایت‌های شماست، ملاحظات امنیتی ممکن است هراسناک به نظر برسند، اما شما نباید با هر یک از آنان تنها یک بار مواجه شوید. هنگامی که شما با ابزارهای مدرن گسترش وب متن باز، نظیر TCP/IP, FTP, Subversion, GNU/Linux, Apache, MySQL, SQL, PHP, HTTP, CSS, XML, RSS, JavaScript, Joomla! آشنا شوید، خود تکنیک‌ها و تاکتیک‌ها تامین امنیت سایت را درخواهید یافت.

- جوملا به دلیل طراحی معماری بر مبنای تکنولوژی های روز دنیا و بهره گیری از مدل توسعه متن باز و وجود جامعه کاربری بزرگ و جامعه توسعه دهندگان توانا, این سیستم از امنیت بالایی برخوردار است.

یک میزبان فضای وب شایسته و واجد شرایط را انتخاب کنید - مهم‌ترین تصمیم

به طور حتم و یقین در خصوص امنیت سایت، هیچ تصمیمی مهم‌تر از انتخاب هاست و سرور نیست. به‌هرحال، با توجه به گوناگونی گزینه ها و پیکربندی‌های هاستیگ، ممکن نیست که بتوان یک فهرست کامل از تمامی راه‌حل‌ها را ارائه داد.

خطرات میزبانی اشتراکی (Shared Server)

اگر شما بودجه کافی برای هزینه در سایت خود ندارید، یا سایت شما دارای داده‌ها و محتوای بسیار سری و محرمانه نمی‌باشد، شما می‌توانید از میزبانی اشتراکی یا سرورهای اشتراکی استفاده کنید، اما حتما بدانید که شما در معرض خطرات غیرقابل اجتناب آن قرار دارید. بسیاری از نکته‌ها و توضیحاتی که در زیر می‌آیند در رابطه و مربوط با امنیت بر روی همین میزبانی‌های اشتراکی می‌باشند.

از پیکربندی و تنظیمات سرسری خودداری کنید

تنها برای این که چشم‌تان را باز کنید این گزارش را بخوانید، این گزارش درباره هزاران سایتی است که به گوگل اجازه ایندکس کردن نتایج phpinfo() را می‌دهد. شما چنین اشتباهی را در سایت خود مرتکب نشوید! این گزارش شامل آمار هشداردهنده‌ای درباره درصد سایت‌هایی است که از تنظیمات نادرست مانند روشن بودن register_globals یا نداشتن open_basedir استفاده کرده‌اند. درضمن اگر php.ini و register_globals برای شما کدهای ناآشنایی هستند، بدین معناست که شما آمادگی لازم برای مدیریت امنیت سایت خود را ندارید.

پیکربندی Apache (آپاچی)- استفاده از Apache .htaccess

اقدامات استفاده typical را با فایل‌های local Apache .htaccess بلوکه کنید. این گزینه بر روی همه سرورها فعال نیست. با میزبان خود بررسی کنید که آیا شما ممکن است دچار این مشکلات شوید یا خیر. با استفاده از . htaccess شما می‌توانید گذارواژه محافظی بر روی دایرکتوری‌های حساس، مانند مدیریت (administrator) قرار دهید، دسترسی دایرکتوری‌های حساس را بر اساس IP ببندید، و بسیاری پیکربندی‌های دیگر بر روی سرور خود در جهت افزایش امنیت با تغییر PHP4 به PHP5 اعمال کنید.

استفاده از Apache mod_security

Apache mod_security و فیلترهای mod_rewrite برای جلوگیری از حملات PHP با دقت تنظیم کنید. Google search for mod_security و Google search for mod_rewrite را مشاهده کنید. (توجه داشته باشید: این‌ها روش‌های پیشرفته‌ای هستند که نیازمند توافقنامه یا هماهنگی با پشتیبان فضای وب شما می‌باشد، چنین گزینه‌هایی به صورت جداگانه بر روی سرورهای اشتراکی قابل تنظیم نمی‌باشند.)

پیکربندی - MySQL پایگاه داده را ایمن کنید

از تنظیم حساب‌های MySQL در حالت دسترسی محدود اطمینان حاصل کنید. نصب اولیه MySQL ایمن نیست و نیازمند پیکربندی دقیق‌تری است. (راهنماهای MySQL http://dev.mysql.com/doc/را بخوانید) توجه داشته باشید که این گزینه تنها برای مدیریت سرورهایی که شما دارنده آن هستید، نظیر سرورهای Dedicated اعمال می‌گردد.

پیکربندی - PHP نحوه کار PHP را دریابید

نحوه کار با فایل php.ini و چگونگی تنظیمات کنترل شده PHP را بیاموزید. فهرست رسمی دستورالعمل‌های php.ini را در http://www.php.net مطالعه کنید.

استفاده از PHP5

در حال حاضر PHP5 و PHP4 هر دو پشتیبانی می‌گردند، و هر دو بر روی سرورها دردسترس می‌باشند. پیش از آن که PHP4 منسوخ شود، اسکریپ‌های دلخواه خود را به PHP5 ارتقا دهید. نگران کدهای هسته جوملا نباشید، تمامی نسخه‌های موجود با PHP5 سازگار می‌باشند. (مشاهده خبر PHP)

استفاده از فایل‌های محلی php.ini

در سرورهای اشتراکی شما نمی‌توانید فایل php.ini اصلی را ویرایش کنید، اما شما قادر به افزودن فایل‌های محلی php.ini دلخواه هستید. اگر چنین قصدی داشته باشید، شما باید رونوشت فایل‌های php.ini را در تمام زیردایرکتوری‌هایی که نیازمند تنظیمات سفارشی هست، ایجاد کنید. خوش‌بختانه تعدادی از اسکریپت‌ها موجودند که می‌توانند این کار دشوار را برای شما انجام دهند!

چند نکته مهم هست که باید به‌یاد داشته باشید.

فایل‌های محلی php.ini تنها در شرایطی که در سرور مورد استفاده آن‌ها تنظیم شود، قابل استفاده می‌باشند. این شامل یک فایل php.ini در دایرکتوری http_root شما می‌باشد. شما می‌توانید بررسی کنید که این فایل بر روی سایت شما توسط تنظیمات مستقیم فایل php.iniتاثیرگذار هست یا خیر. فایل‌های محلی php.ini تنها بر فایل‌های . php تاثیر می‌گذارند که در همان دایرکتوری قرار دارند. این به آن معناست که به صورت طبیعی تنها دو دایرکتوری جوملا هستند که شما می‌توانید فایل php.ini را در آن قرار دهید.

اگر شما در هر دایرکتوری یک فایل php.ini دارید، برخی از اسکریپت‌ها احتمالا این کار را برای شما انجام داده‌اند. اگر شما قصد آن را نداشته‌اید، شما باید آن‌ها را از شاخه اصلی خارج کنید، اما به طور منطقی شما باید نگران فایل‌های php.ini در دایرکتورهای http_root و administrator باشید.

استفاده از PHP disable_functions

از disable_functions برای غیر فعال‌کردن توابع خطرناک PHP که در سایت شما موردنیاز نیستند، استفاده کنید. در زیر یک نمونه تنظیم برای یک سایت جوملا! است:

```
disable_functions = show_source, system, shell_exec, passthru, exec, phpinfo, popen, proc_open
```

استفاده از PHP open_basedir

open_basedir باید فعال و به درستی تنظیم شده باشد. این تنظیمات فایل‌هایی را که می‌توانند توسط PHP در یک دایرکتوری درختی خاص باز شوند را محدود می‌کند. این تنظیمات از روشن یا خاموش بودن حالت امن هیچ تاثیری نمی‌پذیرد.

```
open_basedir = /home/users/you/public_html
```

دربرخی از پیکربندی‌های سیستم، حداقل با PHP 4.4.8 استفاده از slash برای محدود کردن دسترسی تنها به دایرکتوری مشخص شده ممکن است سبب اخطار JFolder::create: Infinite loop detected جوملا هنگام ذخیره پیکربندی کلی بخش مدیریت شود. این اخطار به سبب عدم موفقیت‌های PHP file_exists() function، به عنوان مثال هنگام بررسی وجود home/user/public_html/joomla_demo / و تنظیم open_basedirدر home/user/public_html/joomla_demo / شود.

به علاوه اگر open_basedir تنظیم شده باشد، ممکن است نیاز به تنظیم پیکربندی PHP upload_tmp_dir در مسیری در حوزه open_basedir باشد یا به طور جایگزینی مسیر upload_tmp_dir را بیفزاید به open_basedir با استفاده از مسیر مربوطه جداکننده برای سیستم میزبان.

open_basedir = /home/users/you/public_html:/tmp

PHP از دایرکتوری موقت سیستم هنگامی که upload_tmp_dir تنظیم نشده باشد استفاده می‌کند یا هنگامی که تنظیم شده باشد اما دایرکتوری موجود نباشد. بنابراین الزامی است که آن را به open_basedir برای جلوگیری از بارگذاری خطا در جوملا بیفزایید.

تنظیم magic_quotes_gpc

magic_quotes_gpc را آن‌گونه که مورد نیاز سایت‌تان است، تنظیم کنید. این تنظیم برای جوملا! ۱.۰ پیشنهاد می‌شود که در وضعیت روشن تنظیم شود تا از ضعف امکانات اضافی محافظت شود. اما امن‌ترین روش این است که magic_quotes_gpc خاموش باشد تا در مقابل تمامی امکانات اضافی ضعیف و بی‌خاصیت محافظت شوید. جوملا! ۱.۵ به طور کل از این تنظیم صرف نظر می‌کند و به طریق دیگری عمل می‌کند.

magic_quotes_gpc = 1

از PHP safe_modeاستفاده نکنید

از استفاده‌ی PHP safe_mode اجتناب کنید. این کار در سیستم معتبر است، اما یک راه‌حل ناقص برای مشکلات بسیار پیچیده است که باعث بروز برخی مشکلات امنیتی می‌شود. برای اطلاعات بیشتر درباره این موضوع سایت رسمی PHP را بخوانید.

safe_mode = 0

از PHP register_globals استفاده نکنید

register_globals خودکار متغیرها به طور حتم یکی از اشتباه‌ترین تصمیمات برنامه‌نویسان و گسترش‌دهندگانِ PHP بود. این سند تعیین می‌کند که آیا EGPCS (Environment, GET, POST, Cookie, Server) به عنوان متغییرهای کلی ثبت شوند یا خیر و این‌که کجا باید سریعا برای تمام اسکریپت‌های PHP در دسترس باشند و همچنین کجا باید به سادگی بر روی متغییر شما مجددا نوشته شوند، هنگامی که شما بی‌دقت هستید. خوش‌بختانه گسترش‌دهندگان PHP مدتی است متوجه این اشتباه خود شده‌اند و این ویژگی را کم‌تر به کار می‌گیرند.

اگر سایت شما بر روی یک سرور اشتراکی با پشتیبان فضای وبی است که register_globals بر روی آن فعال است، شما واقعا باید نگران باشید. البته اگرچه شما می‌توانید register_globals را غیر فعال کنید، اما همچنان این امر شما را در معرض آسیب‌پذیری در برابر حملات به سایت شما از طریق سرور قرار می‌دهد.

register_globals = 0

از PHP allow_url_fopen استفاده نکنید

از PHP allow_url_fopen استفاده نکنید. این گزینه URL-aware fopen wrapperها را فعال می‌کند. Wrapperهای پیش‌فرض برای کنترل فایل‌ها با استفاده از ftp و یا پروتوکل http ایجاد شده اند، همچنین برخی از امکانات مانند zlib می‌توانند wrapperهای اضافی‌ای را ثبت کنند.

allow_url_fopen = 0