نوشته شده توسط Administrator
شنبه ۱۶ آبان ۱۳۸۸ ساعت ۱۵:۵۹ - آخرین به روز رسانی شنبه ۱۶ آبان ۱۳۸۸ ساعت ۱۶:۴۴

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 از امنیت بالایی برخوردار است.

در ادامه بررسی های موارد امنیتی و ارائه راهکارهای مناسب جهت ارتقاء بهره بری بهینه از جوملا 1.5 و پس از گذر از مرحله اول و انتشار "فهرست نکات امنیتی جوملا 1.5 - چگونه شروع کنیم - قسمت اول" حال زمان انتشار مرحله دوم سری مقالات تامین امنیت جوملا می باشد.

قسمت دوم را تحت عنوان "فهرست نکات امنیتی جوملا 1.5 - نصب، میزبانی وب و انجام تنظیمات سرور - قسمت دوم" منتشر می کنیم و در این مقاله بسیار مفید به بررسی نکات مهمی همچون : خطرات میزبانی وب اشتراکی، پیکربندی و تنظیمات اصلی سرور و دیگر موارد مرتبط می پردازیم.

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. بهرحال، با توجه به گوناگونی گزینه ها و پیکربندیهای هاستیگ، ممکن نیست که بتوان یک فهرست کامل از تمامی راهحلها را ارائه داد. برای اطلاع از میزبانان فضای وبی که حداقل موارد لازم امنیتی را رعایت کرده و با جوملا! سازگار هستند، میتوانید با مشاوران تخصصی جوملا! فارسی تماس بگیرید.

خطرات میزبانی اشتراکی (Server Shared)

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 globals_register یا نداشتن بدین ،هستند ناآشنایی کدهای شما برای register_globals و php.ini اگر درضمن .اندکردهاستفاده open_basedir معناست که شما آمادگی لازم برای مدیریت امنیت سایت خود را ندارید.

پیکربندی Apache (آپاچی)- استفاده از htaccess. Apache

اقدامات استفاده typical را با فایلهای htaccess. Apache local 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 .کنید اعمال PHP5

استفاده از security_mod Apache

Google .کنید تنظیم دقت با PHP حملات از جلوگیری برای mod_rewrite فیلترهای و Apache mod_security های‌روش‌هااینباشید داشته توجه) .کنید مشاهده را Google search for mod_rewrite و search for mod_security 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.

نوشته شده توسط Administrator
شنبه ۱۶ آبان ۱۳۸۸ ساعت ۱۵:۵۹ - آخرین به روز رسانی شنبه ۱۶ آبان ۱۳۸۸ ساعت ۱۶:۴۴

پیکربندی PHP - نحوه کار PHP را دریابید

نحوه کار با فایل ini.php و چگونگی تنظیمات کنترل شده PHP را بیاموزید. **فهرست رسمی دستورالعملهای ini.php 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 جوملا هسته کدهای نگران نباشید، دهید ارتقا PHP5 به را خود دلخواه های‌اسکریپ،شود منسوخ PHP4 موجود با PHP5 سازگار میباشند. (مشاهده خبر PHP)

استفاده از فایلهای محلی ini.php

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

چند نکته مهم هست که باید بهیاد داشته باشید.

1. **فایلهای محلی ini.php تنها در شرایطی که در سرور مورد استفاده آنها تنظیم شود، قابل استفاده میباشند. این شامل یک فایل ini.php در دایرکتوری root_http شما میباشد. شما میتوانید بررسی کنید که این فایل بر روی سایت شما توسط تنظیمات مستقیم فایل ini.php تاثیرگذار هست یا خیر.**
2. **فایلهای محلی ini.php 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 ini.php را در آن قرار دهید.**
3. **اگر شما در هر دایرکتوری یک فایل ini.php 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 باشید.administrator و http_root دایرکتورهای در php.ini**

استفاده از functions_disable PHP

از functions_disable **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 basedir_open PHP

یک در PHP **توسط توانندمی که را هاییفایل تنظیمات این .باشد شده تنظیم درستی به و فعال باید** open_basedir **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 4.4.8 PHP **استفاده از** slash **برای محدود کردن دسترسی تنها به دایرکتوری مشخص شده ممکن است سبب اخطار** create::JFolder: detected loop Infinite **جوملا هنگام ذخیره پیکربندی کلی بخش مدیریت شود. این اخطار به سبب عدم موفقیتهای** function ()exists_file PHP **، به عنوان مثال هنگام بررسی وجود** /home/user/public_html/joomla_demo/ **در** open_basedir **تنظیم و** /home/user/public_html/joomla_demo/ **شود.**

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

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

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

تنظیم gpc_quotes_magic **برای تنظیم این .کنید تنظیم ،است تانسایتنیاز مورد که گونهآنرا** magic_quotes_gpc

جوملا! 1.0 پیشنهاد میشود که در وضعیت روشن تنظیم شود تا از ضعف امکانات اضافی محافظت شود. اما امنترین روش این است که gpc_quotes_magic خاموش باشد تا در مقابل تمامی امکانات اضافی ضعیف و بیخاصیت محافظت شوید.

جوملا! 1.5 به طور کل از این تنظیم صرف نظر میکند و به طریق دیگری عمل میکند.

magic_quotes_gpc = 1

از mode_safe PHP استفاده نکنید

از استفادهی mode_safe PHP 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 globals_register PHP استفاده نکنید

.بود PHP دهندگان گسترش و نویسان برنامه تصمیمات ترین اشتباه از یکی حتم طور به متغیرها خودکار register_globals 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 globals_register بر روی آن فعال است، شما واقعا باید نگران باشید. البته اگرچه شما میتوانید globals_register 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 fopen_url_allow PHP استفاده نکنید

از fopen_url_allow PHP **استفاده نکنید. این گزینه** wrapper fopen aware-URL**ها را فعال میکند.** Wrapper**های پیشفرض برای کنترل فایلها با استفاده از** ftp **و یا پروتوکل** http **ایجاد شده اند، همچنین برخی از امکانات مانند** zlib **میتوانند** wrapper**های اضافیای را ثبت کنند.**

```
allow_url_fopen = 0
```

با مطالعه چک لیست های امنیتی جوملا در بالا و انجام دقیق تنظیمات، شما قادر به استفاده از یک سرور امن برای میزبانی جوملای سایت خود هستید، امیدواریم این مقاله نیز همانند دیگر مقالات جدید سایت جوملا فارسی (گروه نرم افزاری جوملا) بتواند به شما جهت استفاده لذت بخش از جوملا 1.5 **کمک و یاری رساند.**

در ضمن از تمامی دوستان خواهشمندیم نظرات خود را پیرامون این مقاله به صورت کامنت برای ما ارسال کنند تا تمامی کاربران سایت از نظرات یکدیگر آگاه شوند.