راهنمای امنیت در وردپرس

تالیف: حامد تکمیل

WordPress Security

Version 1.0

مقاله پیش روی شما کوششی است برای گردآوری چندین ترفند امنیتی مختص سیستم مدیریت محتوی محبوب وردپرس که تقدیم جامعه وردپرس می شود. در این مقاله سعی شده تا به اختصار بهترین راهکارهای امنیتی و روش های پیشگرانه امنیتی برای کاربرانی که دغدغه امنیت سیستم های مبتنی بر وردپرس خود را دارند با بهره گیری از تجارب شخصی، توصیه های سایر حرفه ای های وردپرس گرداوری شود. لازم به ذکر است که این مقاله برای سطوح متوسط و پیشرفته تدارک دیده شده و افراد مبتدی نیازمند آشنایی با برخی از اصطلاحات مرسوم می باشند.در این مقاله عناوین زیر مورد بررسی قرار گرفته است:

- **سطح دسترسی به جدول ها**
- **تغییر پیشوند جدول در وردپرس**
- **تغییر نام کاربری admin**
- **ایجاد کاربران جدید به همراه اعطای مجوزهای لازم**
- **بستن رخنه های نفوذ ابتدایی**
- **جلوگیری از دسترسی موتورهای جستجو به پوشه های حیاتی سیستم**
- **برداشتن شماره نسخه وردپرس از قالب سایت**
- **ضرورت پشتیبان گیری از فایل های سایت**
- **بهره گیری از SSL**
- **ضرورت به هنگام سازی وردپرس و افزونه ها**
- **کد کردن محتویات فایل wp-config.php**
- **سطح دسترسی مطلوب برای پوشه های وردپرس**
- **انتقال wp-config.php به مکانی امن**
- **انتقال و تغییر نام پوشه wp-content**
- **استفاده از SFTP به جای FTP**
- **افزونه های مفید امنیتی برای وردپرس**

چنانچه در این مقاله نقص و کاستی ای مشاهده کرده و یا برای تکمیل آن پیشنهاداتی دارید می توانید آن ها را با ایمیل زیر برای بنده ارسال نمایید تا با مشارکت یکدیگر بتوانیم جامعه ی وردپرس مطلوب تری را پایه گذاری کنیم.

silvercover@gmail.com

http://silvercover.wordpress.com

نسخه ۱/۰ – حامد تکمیل – خرداد ۱۳۸۹

۱ – سطح دسترسی به جدول ها

یکی از نکات حائز اهمیت قبل از برپا کردن وردپرس توجه شایسته به سطح دسترسی کاربران تعریف شده برای بانک اطلاعاتی و اعطای سطح دسترسی مناسب به کاربران بانک اطلاعاتی می باشد. چنانچه این امر مهم و حیاتی مورد غفلت واقع شود دردسر های فراوانی برای صاحب سایت در پی خواهد داشت.

هرگز در برنامه های تحت وب خود از سطح دسترسی ریشه (root) استفاده نکنید. در غیر اینصورت با بی پروایی باید گفت که شما به دنبال دردسر می گردید!

بر اساس تجربه و روال های توصیه شده بهتر است که عموما کاربران بانک اطلاعاتی با مجوزهای دسترسی محدود تعریف شوند و هیچ یک از کاربران مد نظر به استثنا شرایط ضروری از مجوزهای سراسری بهره مند نباشند. بدین ترتیب در هنگام بروز حمله های احتمالی و نفوذ هکر ها، لایه های محافظتی بیشتری جهت عبور پیش رو خواهد بود و سایر بانک های اطلاعاتی مصون خواهند ماند.

در بیشتر مواقع جهت انجام وظایف روزمره، مجوزهای دسترسی زیرکفایت می کند:

DATA	STRUCTURE
SELECT	CREATE
INSERT	ALTER
UPDATE	DROP
DELETE	

اما چنانچه بنا به شرایط تنها امکان استفاده از یک بانک اطلاعاتی منفرد بر روی فضای میزبان در کنار امکان تعریف چندین کاربر بانک اطلاعاتی فراهم است، سطوح دسترسی زیر کفایت می کند:

DATA	STRUCTURE
SELECT	ALTER
INSERT	
UPDATE	
DELETE	

۲– تغییر پیشوند جدول در وردپرس

در بیشتر برنامه های تحت وب از جمله وردپرس به منظور رفع محدودیت ها و شاخص سازی، از پیشوندهایی برای نامگذاری اسامی جدول ها استفاده می شود. در حالت پیشفرض پیشوند مورد استفاده وردپرس که در فایل wp-config.php درج شده عبارت "wp_" می باشد. از طرفی بی توجهی به چنین مقادیر پیشفرض احتمال موفقیت حملات از نوع SQL Injection را افزایش داده و نفوذگر را قادر می سازد تا از کدهای مخرب (Exploit) موجود که بر اساس همین مقادیر پیش فرض بنا شده اند با موفقیت بهره برداری کند. لذا به منظور ناکام گذاشتن نفوذگر در چنین مواردی می بایست تا این اسامی پیشفرض جداول از عبارتی همچون wp_ به عبارتی مطمئن تر و تصادفی همچون 5k91b_ تغییر یابد. با این حال جهت ایجاد سهولت در تمایز دادن جداول برنامه های مورد استفاده در فضای میزبانی بد نیست که پیشوندی دو حرفی به عنوان نماد برنامه ای که جدول بدان تعلق دارد را در ابتدای رشته تصادفی درج کنیم. به عنوان مثال wp_5k9b_. شایان ذکر است که فایل wp-config.php می بایست از مجوزهای لازم برای نوشتن در آن برخوردار باشد.

- قبل از فرآیند نصب وردپرس

چنانچه هنوز فرآیند نصب وردپرس را آغاز نکرده اید، تغییر پیشوند مورد بحث در بند قبل به سادگی قابل انجام می باشد. بدین منظور تنها کافیست تا از فایل wp-config.php واقع در پوشه ریشه وردپرس متغیر زیر را یافته و مقدار مناسب را جایگزین کنید:

$table_prefix='wp_'; ⇨ $table_prefix = 'wp_5k9b';

در نهایت و به هنگام پیگیری نصب وردپرس پیشوند تمامی جداول متعلق به وردپرس به عبارت مورد نظر شما تغییر خواهد کرد.

- تغییر دسترسی بعد از فرایند نصب

اعمال تغییرات بر روی نسخه ای از وردپرس که بر اساس تنظیمات پیشفرض برپا شده کمی خسته کننده می باشد. در حال حاضر ساده ترین راه حل موجود برای چیرگی بر این حالت یافتن و نصب افزونه ای موسوم به WP Prefix Table Changer می باشد که می توان با نصب آن و آگاه کردن آن از عبارت پیشوندی مد نظر

این بخش را پوشش داد. اما جهت تکمیل این مبحث و برای آندسته از افرادی که مایل به تغییر دستی مقادیر می باشند لازم است تا ابتدا همانند بند قبل مقدار متغیر مربوطه در فایل wp-config.php را تغییر داده و در ادامه با بهره گیری از واسط های کاربری MySQL همچون phpMyAdmin پیشوند جداول را تغییر داد. البته این انتهای راه نیست و می بایست همانند جدول زیر سایر تغییرات را اعمال نمود:

wp-usermeta	wp-options
meta-key	option_name
wp_user_level, wp_auto_save_draft_ids	wp_user_roles

مقادیر فیلدهای قید شده در جدول فوق ممکن است در هنگام مراجعه شما موجود نباشد. دلیل این امر ایجاد شدن آنها بر حسب نیاز می باشد. اما به هر حال با اعمال تغییرات و پیشدستی شما، خللی در ادامه پیش نخواهد آمد.

۳ – تغییر نام کاربری admin

به طور پیشفرض و در فرایند نصب مشهور وردپرس نام کاربری admin به همراه کلمه عبور تصادفی انتخاب و نمایش داده می شود و اکثر کاربران به همین نام کاربری و کلمه عبور بسنده کرده و ریسک امنیتی را افزایش می دهند. در زمان نگارش این مطلب آخرین نسخه عمومی عرضه شده وردپرس 2.9.2 می باشد که تمهیداتی برای این مورد اندیشیده است. (شایان ذکر است که در نسخه بعدی وردپرس یعنی نسخه 3.0 قابلیت انتخاب نام کاربری و کلمه عبور در فرایند نصب وردپرس گنجانده شده و بیش از پیش به بهبود امنیت کمک می نماید). از جمله آنکه به هنگام اولین ورود خود به پنل مدیریت پیامی شاخص و آشکار در بالای صفحه مبنی بر تعویض این کلمه عبور با مورد شخصی تر و البته امن تر مشاهده می شود که کاربر را صریحا به انجام این کار دعوت می نماید. بنابراین بهتر است اولین گام را با تغییر کلمه عبور به مواردی دیگر و البته امن برداشته تا در آینده مورد غفلت واقع نشود.

اما چنانچه در هر شرایطی، نسبت به تغییر نام کاربری admin غفلت ورزید به نفوذگر کمک شایانی کرده و دست وی را برای اعمال حملاتی موسوم به Brute Force (که در آن تعداد زیادی از عبارات و کلمات عبور

تصادفی تولید شده و به طور خودکار مورد ارزیابی قرار می گیرد) باز گذاشته اید. پس عقل سلیم حکم می کند که در اولین فرصت اقدام به تعویض و یا بر گزیدن نام کاربری دیگر نمایید.

۴ – ایجاد کاربران جدید به همراه اعطای مجوزهای لازم

همانطور که می دانید تعدادی از سایت ها نیازمند تعریف و یا ثبت نام کاربرانی با سطوح مختلف می باشند و نیاز به سیستمی جهت مدیریت سطوح دسترسی نقش های کاربران بسیار حائز اهمیت است. به صورت طبیعی وردپرس چند سطح کاربری[1] را معرفی و ارائه می کند که در جدول ذیل به شرح مختصر هر یک می پردازیم:

نقش (Role)	توضیح
Administrator	بالاترین سطح مدیریتی با امکان دسترسی به تمام ویژگی ها
Editor	شخص با دسترسی ارسال و ویرایش مطالب خود و دیگران
Author	شخص با دسترسی ارسال و ویرایش مطالب شخصی خود
Contributor	شخص با دسترسی نوشتن و مدیریت نوشته های خود بدون انتشار آن
Subscriber	عضو معمولی سایت و برخوردار از ویژگی مدیریت پروفایل شخصی خود

سطوح دسترسی فوق نیازهای موجود را تا حد قابل قبولی پاسخ می دهد، اما با این حال در برخی شرایط نیاز است تا امکانات در دسترس هر سطح بنا به شرایط خاص تغییر یافته و سفارشی سازی شود. در چنین حالتی می توان به سادگی از افزونه ای قدرتمند به نام Role Manager[2] سود جست. این افزونه مفید و کارا به شما امکان می دهد تا تمام جزئیات مورد نیاز برای پیکربندی سطوح دسترسی را در اختیار داشته باشید و کنترل کنید. این افزونه زوایای خوبی را برای مدیریت در اختیار مدیر سیستم گذاشته و وی را به خوبی تجهیز می کند.

همیشه به هنگام اعطای مجوزها به کاربران از اعطای مجوزهای آپلود فایل، دسترسی به افزونه ها، ویرایش صفحات و مطالب، درون ریزی و درج کدهای HTML فیلتر شده اطمینان حاصل کرده و بسیار هوشیار باشید. در غیر اینصورت رخنه های نفوذ خطرناکی را ناخواسته ایجاد خواهید کرد.

[1] - http://codex.wordpress.org/Roles_and_Capabilities
[2] - http://www.im-web-gefunden.de/wordpress-plugins/role-manager

۵ – بستن رخنه های نفوذ ابتدایی

در اکثر مواقع نفوذگران ابتدا به مطالعه سیستم مدنظر خود پرداخته تا با بدست آوردن اطلاعاتی اولیه مقدمات نفوذ را فراهم سازند. بر همین اساس توصیه می شود تا بلافاصله پس از نصب اولیه وردپرس اقداماتی که در ادامه بیان شده را مورد توجه و پیاده سازی قرار دهید تا اطلاعاتی که به بیرون درز می کند به حداقل برسد. لازم به ذکر است که توصیه های پیش رو بیشتر مناسب سایت ها و وبلاگ های منفرد بوده و برای محیط هایی همچون وردپرس چند کاربره (WordPress MU) نیاز به تمهیداتی پیشرفته تر خواهید داشت.

– محدود کردن دسترسی به پوشه های wp-content و wp-includes

پوشه های فوق جز پوشه های سیستمی وردپرس بوده و فایل های حیاتی و هسته وردپرس در این دو پوشه بر حسب کارکرد خود قرارگرفته اند. در ادامه ما قصد داریم تا تمام دسترسی ها به جز خواندن فایل های تصویری، CSS و جاوا اسکریپت لازم را به این دو پوشه محدود کنیم. این کار را می توانیم با درج قطعه کد زیر در فایل htaccess. واقع در پوشه های فوق الذکر صورت دهیم:

```
Order Allow, Deny
Deny from all
<Files ~ ".(css|jpe?g|png|gif|js)$">
Allow from all
</Files>
```

توجه نمایید که ممکن است برخی از افزونه ها نیاز به دسترسی به فایل های مورد نیاز خود را داشته باشند و یا فایل های مورد نیاز دارای پسوند هایی متفاوت از آنچه در مثال قید شده باشند. بنابراین لازم است تا در هنگام پیکربندی این بخش از اطلاعات لازم برخوردار باشید.

- محدود کردن دسترسی به پوشه wp-admin

برای محدود کردن دسترسی به پوشه wp-admin که حکم شاهراه ورود به پنل مدیریت و هسته مدیریت وردپرس را دارد دو راه کلی پیشنهاد می شود. راه حل اول بر اساس IP ثابت است و راه حل دوم بر مبنای اختصاص کلمه عبور به پوشه ها.

محدود کردن با استفاده از IP ثابت

چنانچه از نوع اتصال خاص با IP ثابت و اختصاصی بهره مند هستید می توانید دسترسی به پوشه wp-admin را محدود به همان IP اختصاصی خود کرده و سایر IP ها را ممنوع کنید. برای این کار قطعه کد زیر را در فایل htaccess. واقع در پوشه wp-admin درج کنید. در این مثال فرض می کنیم که IP ثابت ما 240.120.11.180 می باشد.

Order allow, deny

Allow from 240.120.11.180

Deny from all

چنانچه قصد محدودکردن به چند IP را دارید می توانید به هر تعداد که نیاز است از عبارت "Allow from..." استفاده نمایید. از سوی دیگر اگر آدرس IP شما در محدوده ای خاص قرار دارد می توانید با حذف بخش مورد نظر از IP این کار را صورت دهید. به عنوان مثال چنانچه IP شما از 123.150.80.1 تا 123.150.80.200 متغیر است و در این محدوده جای می گیرد، کافیست از عبارت "Allow from 123.150.80" استفاده نمایید تا رنج مورد نظر را متذکر شوید.

محدود کردن با استفاده از کلمه عبور

این روش از عمومیت بیشتری در مقایسه با روش قبلی برخوردار است و به راحتی می توان از آن بهره جست. چنانچه بر روی فضای میزبانی خود از برنامه هایی همچون cPanel بهره می برید می توانید با بهره گیری از ویژگی تحت نام "Password Protect Directories" بر روی پوشه wp-admin و یا سایر پوشه ها کلمه عبوری قرار دهید. روش دیگر برای گذاشتن کلمه عبور درج قطعه کد زیر در فایل htaccess. واقع در پوشه wp-admin می باشد.

AuthType Basic

AuthName "My Protected Area"

AuthUserFile /path/to/.htpasswd

Require valid-user

برای ایجاد فایل رمز شده htpasswd. می توانید از ابزارهایی که برای این کار به صورت آنلاین موجود است استفاده نمایید. بدین منظور کافیست تا عبارت "htpasswd generator." را در موتور جستجو وارد کرده و لیستی از این قبیل ابزارها را مشاهده نمایید.

همان طور که در قطعه کد بالا مشخص است کلمه عبور در فایلی تحت عنوان htpasswd. ذخیره می شود که بهتر است این فایل در خارج از پوشه ریشه فضای میزبان شما (عمدتا public_html) قرار داده شود تا دسترسی نا خواسته به آن محدود شود. در قطعه کد بالا عنوانی که پس از AuthName درج شده دلخواه بود و همان عنوانی است که در بالای کادر ورود پسورد درخ خواهد شد.

۶ – جلوگیری از دسترسی موتورهای جستجو به پوشه های حیاتی سیستم

پوشه های حیاتی سیستم می بایست از دسترسی و پیمایش خزنده های موتورهای جستجو دور نگه داشته شوند. زیرا بی توجهی به چنین امری می تواند سبب ذخیره شدن ساختار فایل ها و پوشه های شما در موتورهای جستجو شود و اطلاعات جالب توجهی را در اختیار نفوذگران قرار دهد و به نفوذگر در رخنه به سیستم شما کمک کند.

جهت جلوگیری از رخ دادن چنین موردی می توانید قطعه کد زیر را در فایل robot.txt خود درج کنید:

*Disallow /wp-**

از طرفی مجاز گذاشتن دیگران به گشت و گذار در بین پوشه های حیاتی سیستم و علی الخصوص پوشه افزونه های وردپرس می تواند بسیار خطرناک باشد. از این دست می توان به انتشار کدی مخرب برای نسخه های خاص از افزونه ها اشاره داشت که چنانچه نفوذگر بتواند از نسخه افزونه ای که در حال حاضر استفاده می شود به سادگی آگاهی یابد، فرایند نفوذ برایش دو چندان ساده گشته است. بنابراین توصیه می شود که بعد از نصب افزونه ها ابتدا فایل های Readme.txt که حاوی اطلاعاتی در مورد شماره نسخه پلاگین مورد استفاده است را

از داخل پوشه های هر افزونه پاک کنید. در ادامه جهت جلوگیری از نمایش فهرست فایل های داخل پوشه ها کد زیر را داخل فایل htaccess. خود واقع در ریشه سایت درج کنید:

Options All -indexes

چنانچه دسترسی به فایل htaccess. برای شما میسر نیست می توانید به عنوان راه حلی جایگزین یک فایل خالی با اسم index.html در هر یک از پوشه هایی که مستعد بروز اطلاعات ارزشمند برای نفوذگر می باشد قرار دهید. همان طور که می دانید سرورهای وب به صورت پیش فرض ابتدا در هر پوشه به دنبال فایل های با اسم index گشته و چنانچه این فایل یافت نشود اقدام به نمایش فهرست فایل ها و پوشه های پوشه مد نظر می نماید. لذا برای جلوگیری از این امر می توان با چنین ترفندی مانع از نمایش فهرست فایل ها و پوشه ها شد.

۷ – برداشتن شماره نسخه وردپرس از قالب سایت

طراحان قالب وردپرس اغلب بنا به عادت و یا ایجاد امکان جهت کاربردهای آماری، از تابعی تحت نام bloginfo('version') در فایل header.php استفاده می کنند که در زمان اجرا این تابع شماره نسخه ورد پرس را در محلی که از آن استفاده شده درج می کند. این کار می تواند به راحتی سبب شود تا نفوذگر از شماره نسخه مورد استفاده شما آگاهی یافته و برنامه نفوذ خود را بر اساس رخنه ها و حفره های کشف شده برای آن نسخه پایه ریزی کند. بنابراین بهتر است تا با برداشتن خطی که حاوی شماره نسخه می باشد ریسک امنیتی را کاهش دهیم. اما خط مورد نظر که حاوی تابع مذکور است شبیه به کد زیر است:

<meta content="WordPress <?php bloginfo('version'); ?>" name="generator" />

یک راه دیگر برای مسئله بالا، درج کد زیر در فایل functions.php همراه بسته قالب شما می باشد:

<?php remove_action('wp_head','wp_generator'); ?>

۸ – ضرورت پشتیبان گیری از فایل های سایت

راهکار پشتیبان گیری به صورت منظم و در فواصل خاص از فایل ها و بانک اطلاعاتی سایت یک امر بدیهی و انکارنشدنی است که در بلند مدت در حل مشکلات امنیتی و غیر امنیتی پیش رو بسیار گره گشا خواهد بود. از

این رو توصیه اکید می شود که با انتخاب روش پشتیبان گیری مناسب خود، سایت خود را در برابر برخی از حملات مخرب احتمالی مصون نگه داشته و بیمه کنید. جهت تهیه پشتیبان شما می توانید یکی از روش های پیشنهادی زیر را که به اختصار بیان می شود مورد استفاده قرار دهید:

- استفاده از پنل مدیریت فضای میزبانی (همچون cPanel) و تهیه نسخه های پشتیبان
- استفاده از FTP و تهیه نسخه پشتیبان از فایل های خود.
- استفاده از افزونه های موجود و اختصاصی وردپرس جهت امر پشتیبان گیری همچون افزونه WordPress Database Backup Plug-In.
- پرداخت هزینه جهت بهره گیری از سرویس های اختصاصی پشتیبان گیری که توسط شرکت های میزبانی وب صورت می پذیرد.

۹ – بهره گیری از SSL[۳]

اگر شما قصد افزایش سطح امنیت سایت خود را داری و یا نوعی از خدمات را ارائه می دهید که مستلزم بهره گیری از SSL می باشد باید بدون تردید از آن استفاده کنید. بدین منظور پس از تهیه گواهی معتبر SSL و نصب آن بر روی سرور خود از قطعه کد زیر در فایل wp-config.php اطمینان حاصل نمایید:

Define('FORCE_SSL_ADMIN', true);

در ادامه و در بخش معرفی افزونه ها یک افزونه دیگر در این باره معرفی خواهد شد.

۱۰ – ضرورت به هنگام سازی وردپرس و افزونه ها

بر خلاف برنامه های نرم افزاری همچون سیستم عامل ویندوز که شرکت های تولید کننده آنها به هنگام رخ دادن موارد امنیتی و کشف حفره های امنیتی به اصلاح و ارائه وصله امنیتی جداگانه می پردازند، ماهیت وردپرس به گونه ای است که روزآمدهای امنیتی و وصله ها در قالب نسخه های جدید وردپرس ارائه می شوند. پس این عامل ضرورت به هنگام سازی و روزآمد کردن وردپرس را به خوبی آشکار می نماید. همواره باید در کنار

[3] - Secure Socket Layer

سایر راهکارهای امنیتی خود و حتی قبل از اعمال هر سیاست امنیتی، جدیدترین نسخه وردپرس را نصب و مورد بهره برداری قرار دهید. خوشبختانه از نسخه 2.7 وردپرس به بعد امکان به هنگام سازی خودکار و سریع فراهم شده و این امر باعث می شود تا شما بیشتر به روزآمد کردن وردپرس خود ترغیب شوید.

از سوی دیگر در پنل مدیریت وردپرس چنانچه روز آمد جدیدی برای افزونه های موجود ارائه شود با نمایش پیام های مرتبط این امر به اطلاع شما می رسد که این بار نیز، لازم است با بذل توجه به موقع سلامت و امنیت هر چه بیشتر وردپرس خود را تضمین کنید. همچنین همواره سعی کنید از مخزن رسمی افزونه های وردپرس استفاده کنید و از دانلود سایر افزونه ها در سایر سایت ها پرهیز کنید. مگر اینکه افزونه مورد نظر بسیار معروف و مشهور باشد. همانند افزونه Role Manager.

۱۱ – کد کردن محتویات فایل wp-config.php

در زبان PHP و با بهره گیری از نرم افزارهایی همچون ZendGaurd یا ionCube می توانید سرس کد فایل های PHP خود را به صورت رمز شده[۴] در آورده و از کنجکاوی های نا به جای افراد تا حد امکان ممانعت به عمل آورید.

حال برای افزایش امنیت می توانید محتوی فایل های حیاطی وردپرس خود همچون wp-config.php را به وسیله ابزارهای فوق به صورت رمز شده در آورده و بر روی سروری که از چنین برنامه هایی پشتیبانی می کند قرار داده و مورد استفاده قرار دهید. برای حصول اطمینان از اجرا شدن فایل های کد شده بهتر است با شرکت میزبان خود ارتباط برقرار نمایید و یا محتویات فایل php.ini خود را با استفاده از تابع phpinfo()[۵] مورد بررسی قرار دهید.

[4] - Encoded

[۵] - تابعی است که تمام تنظیمات مربوطه به زبان پی اچ پی را نمایش می دهد

۱۲ – سطح دسترسی مطلوب برای پوشه های وردپرس

همان طور که می دانید در سرورهای مبتنی بر یونیکس و لینوکس می توان مجوز دسترسی به فایل ها و پوشه ها را با دستور CHMOD [۶] معین کرد. از سوی دیگر برنامه های FTP و یا برنامه مدیریت فضای میزبانی همچون cPanel قادرند با بهره گیری از این دستور مجوز های لازم برای دسترسی را اعمال نمایند. در جدول زیر مجوزهای مناسب برای پوشه های حیاتی و مهم وردپرس آورده شده است:

نام پوشه یا فایل	مجوز
root	0755
wp-includes	0755
wp-admin/index.php	0644
wp-admin/js	0755
wp-content/themes	0755
wp-content/plugins	0755
wp-admin	0755
wp-content	0755

۱۳ – انتقال wp-config.php به مکانی امن

با وجود اینکه از نسخه 2.6 وردپرس به بعد این امکان فراهم است تا فایل حیاتی wp-config.php را به مکانی امن و خارج از پوشه ریشه وردپرس منتقل کرد، اما کماکان این امر مورد غفلت واقع می شود. همان طور که اشاره شد، وردپرس چنانچه فایل wp-config.php را در پوشه ریشه خود نیابد، به صورت خودکار به یک پوشه بالاتر سر زده و به دنبال فایل مذبور می گردد. بنابراین به سادگی می توانیم با انتقال فایل wp-config به یک پله بالاتر از پوشه ریشه وردپرس (که معمولا ریشه سایت ماست) سطح امنیت را بالاتر ببریم.

[6] - **CH**ange **MODE** عبارتی مخفف برگرفته شده از

۱۴ – انتقال و تغییر نام پوشه wp-content

در فایل wp-settings.php [۷] امکان تعریف دو ثابت همانند کدهای زیر وجود دارد تا به توسط آنها قادر باشیم نام و محل قرار گیری پوشه wp-content را تغییر دهیم.

بدین منظور کافیست تا در ابتدای فایل wp-settings.php دو خط کد زیر را با مقادیر دلخواه ما مقدار دهی شده اند قرار دهیم:

define('WP_CONTENT_DIR', '/full/path/to/content/dir');

define('WP_CONTENT_URL','http://www.examplesite.com/'/full/path/to/content');

در خط اول کد بالا می بایست مسیر مطلق منتهی به پوشه wp-content جدید را بدون نوشتن اسلش (/) در انتها درج کرده و در خط دوم آدرس URL همان پوشه جدید را بنویسیم.

۱۵ – استفاده از SFTP به جای FTP

پروتکل FTP یک پروتکل قدیمی است که از آن جهت انتقال فایل ها به سرور و بالعکس استفاده می شود و سال هاست که برنامه هایی دیداری جهت کار با این پروتکل همچون FileZilla، CuteFTP، WSFTP و... عرضه و مورد استفاده قرار می گیرد. اما در بطن این پروتکل دو ضعف عمده نهفته است که باعث می شود پیشنهاد کنیم تا شما از جایگزین آن یعنی SFTP استفاده کنید.

مورد اول امنیت پایین FTP می باشد که در هنگام تبادل داده ها آنها را بدون رمز نگاری روانه مقصد می کند و احتمال سرقت اطلاعات توسط تکنیک های استراغ سمع را افزایش می دهد.

مورد دوم که لزوما امنیتی نیست ولی یکی از ضعف های FTP است، عدم توانایی پروتکل FTP جهت از سر گیری فرایند تبادل پس از قطع شدن های ناگهانی[۸] است.

مشابه چنین حالتی را مسلما در حین دانلود فایل از اینترنت و با برنامه های مدیریت دانلود تجربه کرده اید و به ارزش این ویژگی واقف هستید.

---

[۷] - واقع در پوشه ریشه وردپرس و در کنار فایل wp-config.php

[۸] - به این ویژگی Stateless گویند.

۱۶ – افزونه های مفید امنیتی برای وردپرس

در جدول زیر سعی شده تا اسامی افزونه های شاخص امنیتی وردپرس به همراه شرحی مختصر از کاربرد آنها ارائه شود. افزونه های زیر را می توانید از بخش مخزن[9] افزونه های وردپرس و یا با جستجو در گوگل بیابید.

نام افزونه	شرح افزونه
WP Security Scan	این افزونه دارای یک پویشگر جهت یافتن رخنه های امنیتی وردپرس می باشد که می توان با استفاده از آن از سطح امنیتی وردپرس خود آگاه شده و یا در صورت بروز مشکل به راهکارهایی که این افزونه ارائه می دهد توجه نمود.
WPIDS	یک افزونه ارزشمند جهت بررسی حملاتی از انواع مختلف اعم از XSS ، SQL Injection و... در یک کلام این افزونه یک لایه تدافعی برای محافظت از وردپرس شما ایجاد می کند.
Login Lockdown	افزونه ای جهت ثبت ورودهای مشکوک و یا نا موفق به سیستم جهت بازرسی های احتمالی بعدی و تعیین سیاست ها بر اساس نرخ آمار ورود افراد به سایت.
WP-Admin Protection	افزونه ای جهت محافظت از پوشه wp-admin
WP Prefix Table Changer	افزونه ای جهت تغییر پیشوند جداول بانک اطلاعاتی در وردپرس
WordPress Antivirus	همانطور که از نامش پیداست این افزونه قادر است تا وردپرس شما را از برخی کدهای مخرب و حملات در امان نگه دارد.
Admin SSL	چنانچه قصد استفاده از گواهی SSL در سایت مبتنی بر وردپرس خود را دارید این افزونه می تواند به کمک شما آید.
TAC (Theme Authenticity Checker)	این افزونه به پویش قالب شما می پردازد تا شما را از وجود کدهای مخرب احتمالی در آنها آگاه سازد. با توجه به وفور قالب های رایگان و احتمال آلوده بودن آنها این افزونه می تواند بسیار مفید باشد.
Stealth Login	این افزونه کارا می تواند با تغییر و ایجاد ساختاری جدید برای آدرس ورود و خروج صفحات وردپرس از افشا شدن آدرس های پیش فرض جلوگیری کند.
Safer Cookies	با اعمال خصوصیاتی بر روی کوکی های ایجاد شده از سو استفاده ها و

[9] - http://wordpress.org/extend/plugins

	دسترسی های غیر مجاز که مبنی بر ربودن کوکی هاست ممانعت به عمل می آورد.
Inspector WordPress	این افزونه همانند نگهبانی هوشیار عمده درخواست های ارسالی به سمت سایت شما را ثبت و نگهداری می کند تا در هنگام بروز مشکل بتوانید مشکل را به سهولت بیابید.
Akismet	یک افزونه بسیار مفید که محصول تولیدکنندگان وردپرس است و کارش جلوگیری از ارسال پیام های ناخواسته و به طور کلی ممانعت از هرزه نگاری (Spamming) است.
Invisible Defender	این افزونه با اضاف کردن چند فیلد مخفی به بخش نظر دهی، سایت شما را از شر ربات های هرزنامه فرست (Spam Bot) خلاص می کند.
Monitor Hakd Files	در هنگام نصب خود به پایش کردن فایل های سایت شما می پردازد و به هنگام مواجه با تغییراتی در فایل های شما، شما را توسط یک ایمیل آگاه می کند. این افزونه می تواند به این ترتیب شما را از تغییرات ناخواسته و پنهانی نفوذگران آگاه سازد.

منابع

- http://codex.wordpress.org/Hardening_WordPress
- http://blogsecurity.net/wordpress/wordpress-security-whitepaper
- http://www.noupe.com/how-tos/wordpress-security-tips-and-hacks.html
- http://speckyboy.com/2009/09/22/20-powerful-wordpress-security-plugins-and-some-tips-and-tricks
- http://www.shahvar.net/1387/06/03/%D8%A7%D9%85%D9%86%D9%8A%D8%AA-%D8%AF%D8%B1-%D9%88%D8%B1%D8%AF%D9%BE%D8%B1%D8%B3/
- http://zangoole.com/1387/10/30/15steps-to-maximum-wordpress-security