|  |  |  |
| --- | --- | --- |
| **Security 1 Level Documents** | | |
|  | SSL / HTTPS |  |
|  | بکاپ |  |
|  | بروز رسانی |  |
|  | فعال کردن فایروال برنامه وب (WAF) |  |
|  | تغییر آدرس لاگین Admin | لازم است آدرس صفحه لاگین را از wp-admin یا wp-login.php به آدرس دیگری تغییر دهید. |
|  | ایمن سازی پوشه wp-admin | با اجرای این دستورالعمل، یک نام کاربری و رمز عبور از طریق سرور برای صفحه لاگین در نظر گرفته می شود. |
|  | غیر فعال کردن قابلیت ویرایش فایل از طریق وردپرس | هر کسی که به پنل ادمین وردپرس دسترسی داشته باشد براحتی می تواند بسیاری از فایل های قالب و پلاگین های وردپرس را تغییر داده، حذف کند یا حتی اطلاعات مخرب به آن ها تزریق کند.بنابراین توصیه می کنیم کد زیر را به آخر فایل wp-config.php اضافه کنید تا این امکان غیر فعال شود. در این صورت تنها راه ویرایش فایل، دسترسی به پنل هاست و FTP خواهد بود.  define('DISALLOW\_FILE\_EDIT', true); |
|  | غیر فعال کردن بخش Debug وردپرس | گاها اتفاق میفته که بخشی از وبسایت شما دچار مشکل میشه اما نمیدونید دلیل مشکل چیه. بنابراین بخش debug وردپرس رو فعال می کنید تا خطاها نمایان بشه و مشکل رو رفع کنید. اما خیلی مهم هست که بعد از رفع مشکل مجدد بخش debug یا در واقع خطایابی رو غیر فعال کنید.بنابراین مطمئن بشید که دو کد زیر در فایل wp-config.php وجود داشته باشند:  define('WP\_DEBUG', false);  define( 'WP\_DEBUG\_DISPLAY', false); |
|  | - XML-RPC را غیر فعال کنید | با استفاده از XML-RPC امکان انتقال اطلاعات از راه دور فراهم می شود. اما از طریق این تکنولوژی خیلی راحت به وبسایت حمله میشه به خصوص حملات DDOS. بنابراین از اونجایی که زیاد از این قابلیت استفاده نمیشه بهتره که از همین اول کار غیر فعالش کنیم.برای غیر فعال کردن XML-RPC، کافیه کد زیر رو به آخر فایل htaccess اضافه کنید:  <Files xmlrpc.php>  Order Deny,Allow  Deny from all  </Files>  از آنجاییکه اغلب کدها تا این مرحله در فایل htaccess. ذخیره میشوند بنابراین لازم است خود فایل htaccess. را از امکان ویرایش محافظت کنیم. به این منظور کد زیر را به این فایل اضافه کنید:  # Securing .htaccess file  <files ~ "^.\*\.([Hh][Tt][Aa])">  order allow,deny  deny from all  satisfy all  </files> |
|  | ایمن سازی wp-config.php | با اضافه کردن کد زیر به فایل htaccess.، دسترسی به فایل مهم wp-config.php غیر فعال می شود:  <Files wp-config.php>  order allow,deny  deny from all  </Files> |

|  |  |  |
| --- | --- | --- |
| **Security A2 Level Documents** | | |
|  | فعال سازی ورود 2 مرحله ای Two Factor Authentication | استفاده از پلاگین Google Authenticator  زمانی که از پلاگین Google Authenticator استفاده می کنید، هنگام ورود به وردپرس، علاوه بر نام کاربری و رمز عبور، یک کد امنیتی درخواست می شود که به صورت تصادفی ایجاد میشود و غیر قابل شناسایی توسط ربات هاست. این کد با استفاده از یک اپلیکیشن موبایلی مبتنی بر آندروید و آیفون تولید میشه و بعد از 1 دقیقه منقضی میشه. |
|  | تغییر پیشوند جداول دیتابیس (table\_prefix) | مدتیست که تغییر پیشوند جداول دیتابیس به عنوان راهی برای جلوگیری از حملات SQL Injection مطرح شده است. اما هر چند تغییر پیشوند کمی کار هکر را دچار مشکل می کند، اما هکر براحتی می تواند با اجرای یک کوئری ساده به شرح زیر، پیشوند جداول دیتابیس وردپرس را پیدا کند!  SELECT DISTINCT SUBSTRING(`TABLE\_NAME` FROM 1 FOR ( LENGTH(`TABLE\_NAME`)-8 ) )  FROM information\_schema.TABLES WHERE  `TABLE\_NAME` LIKE '%postmeta';  بنابراین لزوما تغییر پیشوند، از وقوع حمله SQL Injection جلوگیری نمی کند بلکه تنها یک مرحله کار را به تاخیر می اندازد. با این حال در صورت تمایل می توانید پیشوند جداول دیتابیس را در هنگام نصب وردپرس یا حتی پس از آن با استفاده از افزونه Change DB Prefix از wp به عبارت دیگر تغییر دهید. |
|  | ایمن سازی wp-includes | ایمن کردن پوشه wp-includes به دلیل دسترسی به اسکریپت ها از اهمیت بالایی برخوردار است. بنابراین لازم است کد زیر را به آخر فایل htaccess. مسیر نصب وردپرس اضافه کنید.  # Block the include-only files  <IfModule mod\_rewrite.c>  RewriteEngine On  RewriteBase /  RewriteRule ^wp-admin/includes/ - [F,L]  RewriteRule !^wp-includes/ - [S=3]  RewriteRule ^wp-includes/[^/]+\.php$ - [F,L]  RewriteRule ^wp-includes/js/tinymce/langs/.+\.php - [F,L]  RewriteRule ^wp-includes/theme-compat/ - [F,L]  </IfModule>  جهت اطمینان از اینکه وردپرس کدها را جایگزین کدهای قبلی نکند مطمئن شوید کدهای بالا را در انتهای فایل بعد از End WordPress# وارد می کنید. |
|  | ایمن سازی مسیر wp-content/uploads | از دیگر مسیرهای آسیب پذیر وردپرس پوشه uploads است. در این پوشه فایل های وبسایت علی الخصوص فایل های مدیا نگهداری می شوند. بنابراین نیازی نیست فایل PHP در این مسیر اجرایی شود. برای جلوگیری از اجرای فایل های PHP در این مسیر یک فایل htaccess. در پوشه uploads ایجاد و کد زیر را در آن قرار دهید:  # Kill PHP Execution  <Files \*.php>  deny from all  </Files>  ممکن است قالب مورد استفاده شما، با استفاده از اجرای کد PHP پوشه upload را مدیریت می کند. بنابراین چنانچه پس از اعمال کد بالا وبسایت شما دچار مشکل شد ناچار به حذف کد بالا از فایل htaccess. هستید. |
|  | تغییر Security Key و Salt | اگر به محتویات فایل wp-config.php توجه کرده باشید، در انتهای فایل بعد از اطلاعات دیتابیس، 6 تا 8 خط کد می بینید که با کلمه define شروع شدند. این کدها که معمولا طولانی و غیر قابل فهم هستند یک الگوریتم برای ارتباطات وردپرس و عملکرد آن در بخش های مختلف ایجاد می کنند. اما توصیه می کنیم هر چند وقت یک بار (ماهیانه) این الگوریتم ها را تغییر بدید مخصوصا اگر قبلا وبسایت شما مورد نفوذ قرار گرفته باشه.  برای این کار به صفحه تولید الگوریتم های وردپرس مراجعه کنید. به محض مراجعه به صفحه مذکور، کدها به صورت تصادفی ایجاد میشن. کافیه اون ها رو جایگزین کدهای موجود در فایل wp-config.php کنید.  https://api.wordpress.org/secret-key/1.1/salt/ |
|  | فایروال و پلاگین امنیتی | با اجرای مراحل قبل، تا حد زیادی سیستم وردپرس شما ایمن میشود اما پلاگین های امنیتی هم می توانند راهگشا باشند. پلاگین های امنیتی با مانیتور مداوم وردپرس، فایل های مخرب را پیدا می کنند و به شما کمک می کنند تا وبسایت خود را در برابر حملات Brute-Force، ارسال اسپم، لاگین های مشکوک، SQL Injection و … محافظت کنید.البته خیلی مهمه که همواره از نسخه های اصلی و بروز این پلاگین ها استفاده کنید و تنظیمات درون آن ها را بدرستی انجام بدید.از جمله پلاگین های امنیتی ورپرس موارد زیر هستند:  Wordfence Security.BulletProof Security. iThemes Security  علاوه بر اینها در تمامی سرورهای HiSupport، فایروال تحت وب Mod\_Security به صورت مدیریت شده در دسترس شماست، ضمن اینکه با پیاده سازی سیستم های هوشمند و برنامه ریزی شده، همواره در حال مانیتور وبسایت های شما هستیم. |
|  | در برخی از دایرکتوری های وردپرس اجرای فایل PHP را غیرفعال کنید. | روش دیگر برای سخت کردن امنیت وردپرس شما غیرفعال کردن اجرای فایل PHP در فهرست هایی است که نیازی به آن نیست مانند / wp-content / uploads /.می توانید این کار را با باز کردن یک ویرایشگر متن مانند Notepad انجام دهید و این کد را جای گذاری کنید:  <Files \*.php>  deny from all  </Files>  در مرحله بعدی، باید این فایل را به صورت .htaccess ذخیره کرده و با استفاده از سرویس گیرنده FTP آن را در / wp-content / uploads / پوشه ها در وب سایت خود بارگذاری کنید . |
|  | تلاش های ورود به سیستم را محدود کنید. |  |
|  | با رمز عبور از مدیریت وردپرس محافظت کنید. | به طور معمول، هکرها می توانند پوشه wp-admin و صفحه ورود شما را بدون هیچ محدودیتی درخواست کنند. این به آنها امکان می دهد ترفندهای هک شده خود را امتحان کنند یا حملات DDoS را انجام دهند. می توانید اقدامات محافظتی اضافی با رمز عبور را در سطح سمت سرور اضافه کنید، که به طور موثر این درخواست ها را مسدود می کند. |
|  | نمایه سازی فهرست را غیرفعال کنید. | هکرها می توانند از فهرست دایرکتوری استفاده کنند تا بفهمند آیا پرونده ای با آسیب پذیری های شناخته شده دارید یا خیر، بنابراین آن ها می توانند با استفاده از این پرونده ها به سایت شما دسترسی پیدا کنند. افراد دیگر می توانند از فهرست دایرکتوری برای جستجوی پرونده ها و فایل های شما، کپی کردن تصاویر، یافتن ساختار دایرکتوری و سایر اطلاعات استفاده کنند. به همین دلیل توصیه می شود فهرست بندی ها را خاموش کنید.  شما باید با استفاده از مدیر پرونده FTP یا cPanel به وب سایت خود متصل شوید. سپس، فایل .htaccess را در دایرکتوری ریشه وب سایت خود قرار دهید. پس از آن، باید خط زیر را در انتهای پرونده .htaccess اضافه کنید:  Options -Indexes  فراموش نکنید که فایل htaccess را ذخیره کرده و بارگذاری کنید. |

|  |  |  |
| --- | --- | --- |
| **Security A3 Level Documents** | | |
|  | به طور خودکار کاربران غیر فعال را از سایت وردپرسی خود خارج کنید. | به سادگی مدت زمان را تنظیم کنید و یک پیام خروج اضافه کنید. فراموش نکنید که برای ذخیره تنظیمات خود بر روی دکمه ذخیره تغییرات کلیک کنید |
|  | سوالات امنیتی را به صفحه ورود به وردپرس اضافه کنید. | افزودن سوالات امنیتی به صفحه ورود به وردپرس دسترسی به غیر مجاز را برای افراد دشوارتر می کند. با نصب افزونه WP Security Questions می توانید سوالات امنیتی را اضافه کنید. پس از فعال سازی، برای پیکربندی تنظیمات افزونه باید به صفحه تنظیمات »سوالات امنیتی بروید. |
|  | سطح دسترسی فایل ها و پوشه ها | سطح دسترسی استاندارد برای فایل ها 644 و پوشه ها 755 است. بنابراین چنانچه دسترسی فایل یا پوشه از مسیر نصب وردپرس، بیش از این مقادیر بود حتما آن ها را تغییر دهید.  های ساپورت با پیاده سازی رول های امنیتی این کار را به صورت خودکار انجام می دهد اما بهتر است شما نیز همواره این نکته را مد نظر قرار دهید. |
|  | اسکن انلاین وردپرس برای بدافزارها و آسیب پذیری ها |  |
|  | استفاده از آدرس Email برای ورود؟ محدودیت در ورود با ایمیل در وردپرس؟! |  |
|  | مخفی کردن نام کاربری نویسنده |  |
|  | **استفاده از کپچا وردپرس** |  |
|  | **غیرفعال کردن مشاهده پوشه‌های هاست** |  |
|  | **غیرفعال کردن اجرای فایل PHP در وردپرس** |  |
|  | تغییر دوره‌ای رمز کلیه کاربران در وردپرس |  |
|  | گزینه گزارش دهی خطاهای PHP(PHP Error Reporting) را حذف کنید. |  |
|  | فعالیت داشبورد را پیگیری کنید WP Security Audit Log |  |
|  | Keeppass |  |
|  | تنظیمات اپ درفت |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |