

أفضل الإضافات لتأمين مدونات الورد برس من الاختراق

في البداية، يجب أن نعلم أنه لا توجد إضافة أو مجموعة إضافات تؤمن المدونة بنسبة (100%)، وذلك لأن شعبية وورد برس تزداد يوماً بعد يوم وكذلك يزداد معها عدد المخترقين الذين دائماً ما يبحثون عن الثغرات في المواقع التي تزداد شعبيتها بصورة كبيرة، لذا فإن هذه الإضافات إن لم تقم بحماية المدونة بصورة كاملة، فإنها سوف تقلل من مخاطر الاختراق التي يمكن أن تحدث لأي مدونة، خاصة إذا ازدادت شهرتها، وفيما يلي مجموعة من الإضافات:



[إضافة \(WP Security Scan\):](#)

تقوم بعمل مسح شامل لنسخة الورد برس التي تم إعدادها، وتقدم اقتراحات بالثغرات الامنية التي قد تكون موجودة بالمدونة، مثل كلمة مرور قاعدة البيانات، تصاريح الملفات، كذلك تقوم بإخفاء رقم اصدار الورد برس، بالإضافة إلى العديد من المهام الأخرى.

[إضافة \(Secure WordPress\):](#)

مهمتها الاساسية تقوم على حذف كل عناصر أو معلومات الخطأ التي نتجت بعد اعداد المدونة، قد ينظر البعض إليها على أنها محدودة التأثير، ورغم ذلك فهي هامة، حيث تقوم بحذف معلومات الاخطاء التي قد تظهر في صفحة الدخول، حذف أو تغيير معلومات اصدار المدونة، اخفاء معلومات التحديث للإضافات الموجودة في المدونة، إضافة صفحة فارغة (index.html) في جميع مجلدات الاضافات وذلك لمنع أي محاولة لمعاينة محتويات هذا المجلد، وغيرها من المهام والتي سوف تظهر عند تنصيب الاضافة.

[إضافة \(WordPress Database Backup\):](#)

لا غنى عنها لأي مدون يستخدم الورد برس، فهي تمثل صمام الامان إذا ما حدث اختراق لمدونته، وهذه الاداة تسمح بعمل نسخ احتياطي لمحتوى المدونة بالإضافة إلى عناصر أخرى يمكن تحديدها من خلال الاضافة، وتقوم بإرسال هذه النسخ إلى قرص صلب أو بريد إلكتروني أو خادم آخر يتم تحديده، وبالطبع في حالة وقوع أي مكروه للمدونة فسوف يكون من السهل إعادة المعلومات السابقة.

[إضافة \(Chap Secure Login\):](#)

تقوم بتأمين عملية الاتصال بين مالك المدونة وبين مدونته وذلك من خلال تشفير كلمة المرور الخاصة به، ولكنها لا تقوم بتشفير اسم المستخدم، وهي بذلك تقوم بعمل حماية أمنية كاملة وسد الطريق على المخترقين في هذه الجزئية التي لو تمكنوا منها لتحققت السيطرة الكاملة لهم على المدونة.

[إضافة \(Admin SSL\):](#)

هدفها هو تأمين عملية الاتصال بين المدونة والمدير (Admin)، حيث تشمل جميع الصفحات التي تستخدم فيها كلمة المرور مثل صفحة الدخول، صفحات الكتابة، صفحات التحكم في خيارات المدونة، وهكذا.

[إضافة \(AskApache Password Protect\):](#)

تمثل حائط دفاعي للمدونة، حيث تقوم بحماية مجلدات (includes) و (content)، وهي إضافة تستحق التثبيت، فلها العديد من الميزات يمكن الاطلاع على تفاصيلها من خلال صفحة الاضافة.

[إضافة \(TAC\):](#)



قد يعجب مالك المدونة أحد القوالب في موقع ما، فيقوم بتحميله وتركيبه على المدونة، ولكنك لا تقوم بفحصه عادة إما لنقص الخبرة وهذا الشائع أو للثقة الزائدة في الاضافات التي تم تركيبها، ورغم ذلك فهذه الاضافة والتي تقوم بفحص ملفات القالب واستخراج النصوص البرمجية (Codes) الخبيثة والتي قد ترسل معلومات عن المدونة للمخترقين، إضافة لا غنى عنها إذا كان قالم المدونة يتغير بشكل مستمر.

[إضافة \(Secure WordPress\):](#)

مهمتها الاساسية تقوم على حذف كل عناصر أو معلومات الخطأ التي نتجت بعد اعداد المدونة، قد ينظر البعض إليها على أنها محدودة التأثير، ورغم ذلك فهي هامة، حيث تقوم بحذف معلومات الاخطاء التي قد تظهر في صفحة الدخول، حذف أو تغيير معلومات اصدار المدونة، اخفاء معلومات التحديث للإضافات الموجودة في المدونة، إضافة صفحة فارغة (index.html) في جميع مجلدات الاضافات وذلك لمنع أي محاولة لمعاينة محتويات هذا المجلد، وغيرها من المهام والتي سوف تظهر عند تنصيب الاضافة.

[إضافة \(Hide Login\):](#)

هذه الاضافة تمكن مدير المدونة من انشاء عنوان (URL) خاص به فقط للدخول والخروج من المدونة، وذلك بدلاً من الدخول باستخدام الطريقة التقليدية عن طريق (wp-login.php).

[إضافة \(WP-DBManager\):](#)

مهمتها الاساسية هي صيانة قاعدة البيانات الخاصة بالمدونة مثل اصلاحها، عمل نسخ احتياطية تلقائية، إضافة أو حذف جداول، والعديد من الأمور الاخرى.

[إضافة \(Limit Login Attempts\):](#)

تقوم بتحديد عدد مرات محاولات الدخول المسموحة للمدونة من خلال صفحة الدخول وذلك اعتماداً على ملفات (Cookies) للشخص الذي يحاول الدخول للمدونة.

بالطبع هناك عشرات الإضافات الأخرى بخلاف تلك السابقة، ويمكن البحث عنها في موقع وورد برس الرسمي.