تأمين وحماية مدونات الووردبريس الغير مجانية

إعداد وكتابة :
جريس عبدالعزيز الجريسي
(الرووت جريس)
www.jerais.com
الرياض ، المملكة العربية السعودية
الخميس ، 9 أكتوبر 2008

نسخة رقم : 1.0

محتويات الوثيقة :

المقدمة :

السلام عليكم ، وصباحكم خير ..
في البداية ، يمكن بعضكم يعرفني وبعضكم لا ، انا جريس الجريسي ولقبي زي ما تعرفه الناس (الرووت جريس) ، صاحب **مدونة الرووت جريس** المتخصصة بتعليم وإحتراف أنظمة لينكس ويونكس ونشر إستخدام المصادر المفتوحة ..

حبيت بالوثيقة هذي إني أشرح وأبين للناس كيفية تأمين وحماية مدوناتهم الغير مجانية (المستضافة عند أحد المستضيفين بمقابل مادي) المعتمدة على برنامج وورد بريس WordPress ..

أيش اللي دعاني أكتب هالوثيقة وهالشرح ؟
اللي دعاني الله يسلمكم إني لاحظت بأغلب المدونات اللي زرتها وأطلعت عليها إنها تفتقد أدنى مستويات الحماية والتأمين ، ويمكن بعضكم إستلم مني رسائل تنبيهيه على إيميلاتهم وعلى مدوناتهم أنبههم فيها إنو موجود عندهم في مدوناتهم الخطأ الأمني الفلاني ، أو عندهم الثغرة الفلانية ..
وبدل ما أزيد جهدي بتنويه كل صاحب أو صاحبة مدونة بشكل شخصي ، قلت أكتب الملاحظات في وثيقة وملف واحد ، وأنشرها للناس ، والناس من بعدي ينشرونها ، و يستفيدون منها المدونون بشكل أكبر ..

شرحي راح يكون بأسلوب مبسط وسهل وشبابي وبالصور ، و خالي من التعقيد والفلسفة والمصطلحات الكمبيوترية الغريبة ، جميع محتوياتها يستطيع أي مدون أو مدونة تطبيقها بدون وجع رأس :-) ..

ملاحظة على الوثيقة:

فيه طرق كثيرة لزيادة أمان مدونتك ، لكن ما راح أتطرق لها جميعها ، لأنو هذا بيأخذ وقت والوثيقة هذي بتطول ما راح تشوف النور ..
النسخة هذي زي ما كتبت في غلاف هذي الوثيقة تعتبر رقم 1.0 ، وراح يتم تحديثها بإستمرار مع تغيير رقم نسخة الوثيقة ..
راح أعرض هنا أشياء أمنية أساسية مهمة ، والنسخ القادمة من الوثيقة إن شاء الله راح تحتوي على طرق أمنية أخرى لزيادة أمن مدونتك .
تقدر تتابع آخر نسخ هذي الوثيقة عن طريق متابعة مدونتي ، على الرابط في الأسفل :

http://www.jerais.com

وإذا كانت عندك إستفسارات عن الوثيقة أو تعليق أو إضافة مفيدة ، تقدر ترسلها على إيميلي :

root@jerais.com

الترخيص:

الشرح :

*** إلغاء عرض جميع الملفات الموجودة في مجلد معين .**

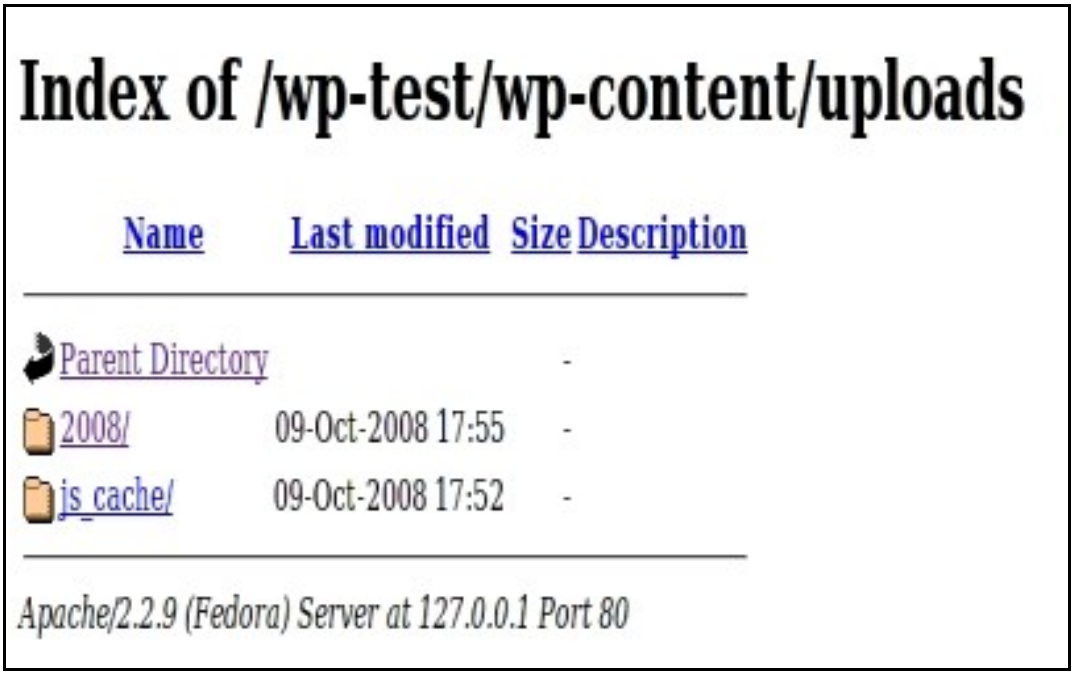
في مدونات الووردبريس ، تقدر إنك تعرف جميع محتويات مجلد معين عن طريق إستعراضه كاملاً ! ..
طبعاً هذا ماحد يبغاه ! ..
بشكل أوضح ، تعرفون المجلد wp-content/uploads الموجود في الووردبريس المخصص لرفع الملفات من جهازك إلى الإنترنت ؟
روح لرابط مدونتك على الإنترنت ، نفترض إنو رابطها كذا

http://jerais.com/plug

الحين روح لنهاية رابط مدونتك وأكتب إمتداد مجلد رفع الملفات من جهازك ، اللي هو زي ما ذكرته فوق wp-content/uploads
يعني بيصير رابط مدونتك كذا :

http://jerais.com/plug/wp-content/uploads

وشوف أيش بيطلع !



تصفح المجلدات اللي طلعت لك ، هل أحتاج أقول إنو جميع ملفاتك اللي رفعتها على مدونتك تم تصفحها ؟!

للمعلومية ، أي مجلد تنشئه على السيرفر الخاص فيك (إفتراضياً ، سوا كنت تستخدم وورد بريس ، عندك منتدى ، موقع خاص) يستطيع أي شخص وصل له إنو يستعرض محتوياته والملفات اللي بداخله :-) ..

طيب أيش الحل ؟

الحل سهل أسهل مما تتوقع :-) ..
إحنا راح نمنع إنو يتم عمل list أو سرد للملفات تبعك ، وهذي تتم عن أكثر من طريقة ، وأفضلها وأضمنها راح نستخدم ملفات يطلق عليها إسم .htaccess ، وهي مختصه بالتحكم بإعدادت سيرفر الويب ..

كيف ؟

إفتح أي محرر نصوص ، على لينكس عندك مثلاً vi أو Gedit ، وفي الأخ الجميل الذكي ويندوز إستخدم برنامج notepad اللي هو المفكرة .
وأكتب العبارة هذي حرفياً:

```
Options -Indexes
```

وإحفظ الملف بالشكل هذا ، بدون زيادة أو نقصان :

```
.htaccess
```

ركز وفتح عويناتك ، بالشكل اللي ذكرته فوق ..
في ويندوز إذا بغيت تحفظ ملف عملته بالمفكرة بالأمتداد اللي تبغاه ، روح لـ حفظ بأسم Save As وبعدها بيطلع لك المربع الشاشة مكان الحفظ ، في خانة الإسم ، إكتب زي الإسم اللي فوق لكن بين علامتي تنصيص ، كذا يعني

```
".htaccess"
```

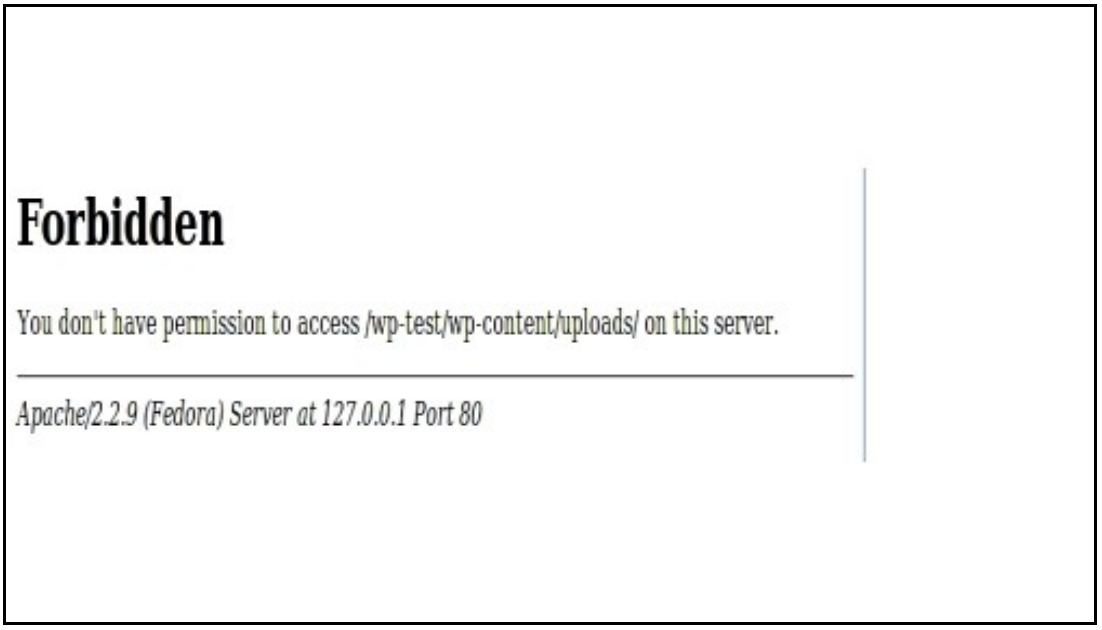
ثم إحفظه .

حلوين ، الحين أيش بنسوي ؟
إستخدم برنامجك الـ FTP لنقل ملفاتك إلى سيرفرك ، وبإعتقادي إنو أي شخص عنده موقع أكيد عنده خلفية عن طريقة نقل الملفات للموقع .

راح نرفع الملف اللي عملناه إلى مجلد public_html أو مجلد www الموجود على سيرفرك ..
إنقل الملف اللي عملته إلى المجلد public_html أو www زي ما ذكرت لك ..

الحين ، روح لموقعك وإطلب المجلد تبع رفع الملفات ، اللي هو wp-content/uploads ، وشوف أيش بيطلع لك :-) ..

http://jerais.com/plug/wp-content/uploads



سهل و حلو ، مو :-) ؟

***إيقاف دخول المستخدم Admin وإنشاء حساب خاص للكتابة :**

زي ماذكرت بالعنوان ، بعد ما تقراء هالصفحات ، لازم إنك توقف الدخول على الحساب اللي إسمه Admin ، اللي هو يعتبر مدير المدونة ..
ليه ؟
لأنو يا طويل العمر الحساب Admin إذا إنسرق منك ، عن طريق برنامج تجسس في جهازك ، أو عن طريق إلتقاط بيانات تصفحك للإنترنت وإنت تتصفح عن طريق الشبكة الاسلكية wireless ، أو غيرهم ، تقول مع السلامة مدونتي :-(!

غالباً إنت تدخل مدونتك عشان تشوف الردود وتكتب مواضيع جديدة صح ؟
بالتأكيد صح بدون شك !

ليه تدخل بحساب عنده صلاحيات أكبر من مجرد كتابة وإضافة وتعديل ردود ؟!
الحساب أدمن عنده صلاحيات كثيرة مره وحساسة ، زي التحكم بالمدونة بشكل كامل ، حذف المواضيع ، العبث وتغيير الشكل أو الـ Theme ، وبرضوا أزيدك بإمكانه المستخدم أدمن يقدر إنو يخلي مدونتك ماتشتغل بالمرة ، وبرضوا يقدر إنو يستغل قوة الحساب ويخلي مدونتك توجه زوارك لموقع ثاني !
الحساب أدمن أخطاره كثيرة ، وصعب حصرها ، وأيش راح نسوي احنا ؟

راح نوقف إستخدامنا للحساب Admin ، وراح ننشئ حساب مخصوص فقط للكتابة ..
مع العلم إنو يمكنك الدخول على الحساب Admin بأي وقت ، بس حاول قد ما تقدر إنك ما تدخل في الحساب Admin إلا في الحالات الضرورية مره اللي تطلب صلاحيات أكبر من مجرد كاتب ..

كيف ننشئ حساب له فقط صلاحيات الكتابة وتعديل ردود ، وبرضوا عنده صلاحيات إضافية ، كا إضافة روابط مثلاً ، يعني تقريباً مستخدم يؤدي شغلي اليومي في المدونة ؟

سهلة ، راح ننشيء حساب بصلاحية محرر Editor في النسخة العربية والإنقلش من الوورد بريس، تابع تحت .

نسخة وورد بريس الإنقلش :
لما تدخل على الوورد بريس ، راح تلاقي على يمينك كلمة **Users** ، إضغط عليها ..
في وسط الصفحة ، في موجود عندك عبارة Add New User ، الجزء اللي تحتها هو المخصص لإنشاء المستخدمين ..
في خانة User Name : أكتب إسم المستخدم اللي راح تدخل المدونة فيه ..
في خانة First Name وخانة Last Name تقدر تخليهم فارغات ، لأنهم إضافات .. هم يعبرون زي ما هو واضح لك عن الإسم الأول والثاني للمستخدم ..
خانة E-Mail : أكتب فيها إيميلك اللي تبغى توصلك فيه تحديثات مدونتك ..
خانة WebSite : موقعك ، تقدر تخليها فارغة ..
خانة الباسوورد Password، ما أحتاج أوصيك ، إكتب باسوورد قوية ، تحتوي على رموز وأرقام وحروف (لسلامتك) ..
الحقل الأخير ، وهو اللي يهمنا Role :إختار من القائمة Editor ..

وبس ، **إظغط Add User** ..

نسخة وورد بريس العربية :

لما تدخل على الووردبريس ، تلاقي على يسارك كلمة **الأعضاء** ، إظغط عليها ..

تلاقي في نصف الصفحة عبارة أضف عضواً جديداً ، وتحتها بعض الحقول ، تقريباً الحقول كلها واضحه ما يحتاج وكتبت عنها فوق ، لكن اللي يهمنا هو الحقل الأخير : **الوظيفة ، وهو المهم في هالشرح : إختار محرر ..**
وبعدها تظغط على زر **أضف المستخدم** الموجود بالأسفل .

إنتهينا ، من الآن إستخدم الحساب اللي أنشئته للتو لكتابة المواضيع وتحرير الردود ، وإحرص على عدم إستخدامك للحساب Admin إلا في الحالات الضرورية ، وإذا إستخدمته فأحرص على إنك تخلص شغلك وتطلع ..

ودائماً إحرص في كل شغلك بالمواقع والإنظمة إنك تستخدم هالطريقة لضمان زيادة الحماية لك ..

*** أخذ نسخة إحتياطية من قاعدة البيانات بشكل دوري .**

ما راح أشرح هالنقطة في هالوثيقة ، لكن راح أدلك على رابط كتبته في وورد بريس العرب شرحت فيه كيفية أخذ نسخة إحتياطية من قاعدة بيانات مدونتك كل فترة إنت تحددها عن طريق سكريبت بطريقة سهلة وبسيطة ، وهي على هالرابط :

http://jerais.com/plug/?p=28

*** تعطيل إمكانية تسجيل مستخدمين وأعضاء جدد .**

في نسخة وورد بريس 2.6.1 ، أكتشفت فيه ثغرة خطيرة تسمح لأي شخص إنو يصير هو المستخدم أدمن Admin !
تعرف إيش معنى الكلام هذا ؟
معناه إنو أي شخص ثاني مجهول يقدر إنو يكون عنده حساب الأدمن Admin اللي هو مدير المدونة غيرك إنت !
أحتاج أقول إنو لاصار فيه شخص ثاني مجهول ومعه حساب الأدمن Admin تبع مدونتك أيش راح يصير في مدونتك ؟!
راجع النقطة اللي ذكرتها قبل " إيقاف دخول المستخدم Admin وإنشاء حساب خاص للكتابة " لتعرف بعض الأخطار ..

كيفية تقفيل الثغرة ..

تقفيل الثغرة سهل ، ألغي أمكانية تسجيل مستخدمين الجدد ..
كيف ؟
الووردبريس العربي :
لما تكون في الصفحة الرئيسية ، تلاقي على يسارك كلمة **الإعدادت** ، إظغط عليها ..
في وسط الصفحة ، فيه موجود كلمة **العضوية** ، وبجنبها مربعين مكتوب بجانبهم كذا :
- السماح بالتسجيل
- يجب على الزوار التسجيل ليتمكنوا من التعليق

إنت تلغي علامة (**الصح √**) من هالخيارين ، ثم تقول **حفظ التغييرات** ..

الووردبريس الإنقلش :
لما تكون في الصفحة الرئيسية ، تلاقي على يمينك كلمة **Settings** ، إظغط عليها ..
في وسط الصفحة ، موجود عندك عندك كلمة **Membership** ، وبجانبها هالخياران :
- Any one can Register
- Users must be registered and logged in to comment

إنت تلغي علامة (**الصح √**) من هالخيارين ، ثم تقول **Save Changes** ..

*** تأمين الدخول على مجلد wp-admin بكلمة مرور .**

بشكل واضح ، إنت لما تبغى تضيف موضوع جديد ، راح تروح للصفحة هذي :

http://jerais.com/plug/wp-admin

وتعمل تسجيل دخول صح ؟

إذا دخلت عليها ، راح تطلع لك صفحة وورد بريس اللي تطلب منك إسم المستخدم وكلمة المرور الخاص بالمدونة لتسجيل دخولك ..

هنا خلنا نوقف شوي ..

على أي أساس سمحت لأي شخص إنو يوصل إلى صفحة تسجيل الدخول لمدونتك ؟
قصدي ، على أي أساس سمحت لكل المتصفحين إنهم يوصولون لهالصفحة ؟
http://jerais.com/plug/wp-admin

مثلاً انا هاكر ، لما أوصل لصفحة تسجيل الدخول تبع مدونتك ، راح أجلس أحاول ليل نهار إني أخمن أو أحزر إسم المستخدم وكلمة المرور ، **ومصيري راح أوصلها** ..

إحنا أيش راح نسوي ؟
راح نركب لنا حاجز ، مصد ، أو جدار ناري (فايروول Firewall) على مجلد wp-admin يطلب من المشخص إنو يكتب إسم مستخدم وكلمة مرور صحيحين (خاصين فقط بهالجدار الناري ، ولا لهم أي علاقة بالوورد بريس) ، وإذا كانوا صحيحين ، راح يدخله على صفحة تسجيل الدخول ..

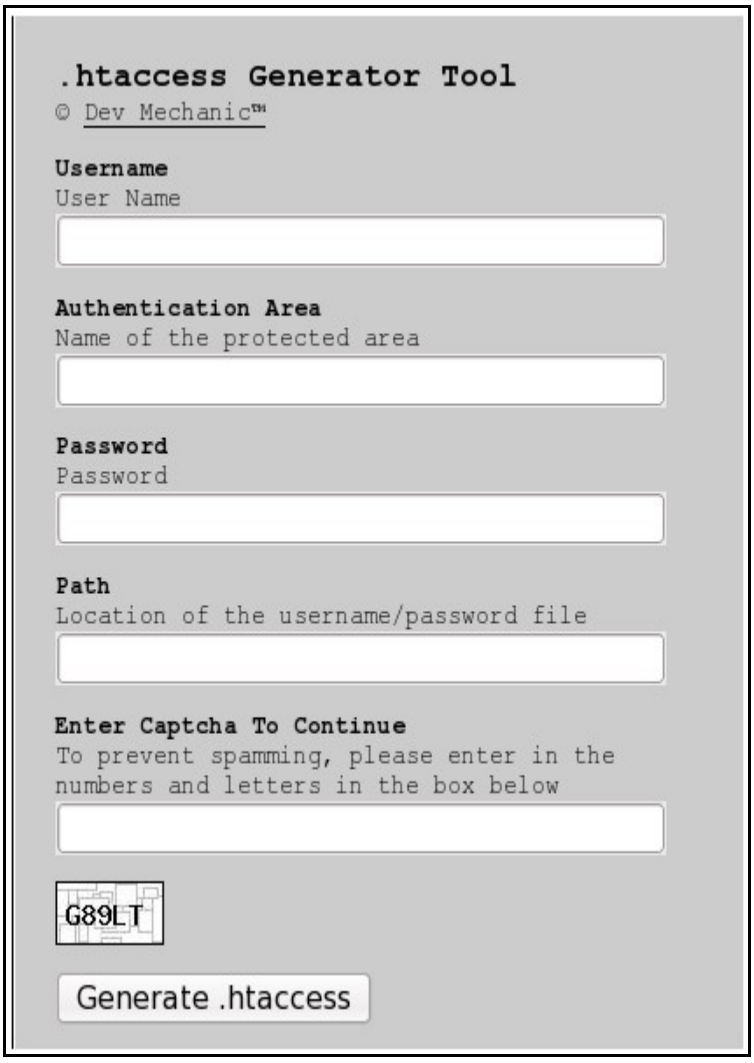
أيش الفائدة ؟
لما أجي انا يالهاكر لمدونتك ، وأشوفك مركب جدار ناري على الدخول إلى مجلد wp-admin ، بيكون عندي حاجزين لازم أجتازهم عشان أدخل على مدونتك وأعبث بمحتوياتها ، الأول حاجز الجدار الناري اللي تطرق له فوق ، والثاني حاجز صفحة تسجيل الدخول الخاصة بمدونتك ..

طيب كيف نطبق الطريقة هذي ؟
سهلة لأبعد الحدود ، وبشكل بيخليك تستغرب من السهولة :-) ..

ذكرت فوق بأحد النقاط نو تقدر تتحكم بإعدادت سيرفر الويب عن طريق ملفات صغيرة تسمى .htaccess ، وهذي هي اللي بنستخدمها إن شاء الله ..

الحين راح ننشئ هالملف ، فيه مواقع تساعدنا بإنشائها وإعدادتها بسهولة ، وبنستخدم حنا هالموقع :
http://tools.devshed.com/webmaster-tools/htaccess-generator/

طلعت لك صفحة ، وفي وسطها مستطيل رمادي بداخله الحقول هذي :



الجدول هذا هو اللي بيساعدنا على إنشاء ملف .htaccess يحمي لنا مجلد wp-dmin ، نشوفه سوا ..

User name : إكتب فيها إسم المستخدم اللي راح يكون له صلاحية الدخول على صفحة تسجيل الدخول الخاصة بمدونتك ..
تنبيه ، إستخدم إسم مستخدم مختلف عن إسم لمستخدم الخاص بمدونتك لزيادة الأمان .
يعني ، إذا كنت دائماً تدخل مدونتك بالأسم Fahad ، هنا أكتب إسم مختلف ، وليكن على سبيل المثال Fahad_1243 .

Authentication Area : هذي معناها " أيش الرسالة اللي تبغاها تظهر للشخص اللي يحاول الدخول " ، أكتب أي شيء ، وليكن مثلاً " This is my secret folder " .
Password : أكتب كلمة المرور الخاصة للمستخدم اللي أنشئته بالخطوة الأولى ، يفضل تكون خليط بين أرقام وحروف ورموز .

تنبيه ثاني ، لاتكتب كلمة مرور نفس كلمة مرورك اللي تستخدمها في تسجيل دخولك للمدونة ، لمصلحتك ، ولزيادة الأمان .
Path : هذا معناه " وين تبغاني أخزن ملف إسم المستخدم و كلمة المرور المشفرة على السيرفر ؟ "
يفضل وينصح إنك تكتب إمتداد خارج عن المجلدات هذي www , public_html, public_ftp ، ليه ينصح إنك ما تضع ملف معلومات الدخول هنا ؟
لأنو المجلدات هذي أي شيء ينوضع فيها ، راح ينشر على الإنترنت ، وطبعاً خطر إنو معلومات دخولك تنشر على الإنترنت ..

طيب وين نخزن الملف ؟
راح ننضم نفسنا شوي ، راح ننشئ لنا مجلد بنخليه للشيء هذا عشان ترجع له إنت بعدين ..
في برنامج الإف تي بي FTP الخاص فيك ، إدخل إلى سيرفرك وأنشئ مجلد تحت "/" وخارج عن هالثلاث مجلدات www , public_html, public_ftp ..
انا مثلاً أنشئت لي مجلد وسميته security ..
حلوين ، الحين روح لموقعنا اللي جالسين نشرح عليه ، وأكتب في الـ Path إمتداد مجلدك ، في حالتي أبتكتب

/security
بعد ما نملي الحقول ، نملئ حقل الـ Captcha باللي مكتوب تحته بالصورة ، ثم نظغط على الزر Generate .htaccess ..

راح تطلع لنا صفحة تحتوي على مربعين ، والمربعين يحتوون على الكلام هذا :
المربع الأول اللي طالع لك يحتوي على كلام مثل هذا :

```
AuthUserFile /security/.htpasswd
AuthGroupFile /dev/null
AuthName "Secret Folder"
AuthType Basic

<limit GET POST>
   require valid-user
</limit>
```

لمحتويات اللي ظاهرة لك ، إنسخها بالكامل وإفتح محرر النصوص الخاص فيك والصقها فيه ، ثم إحفظها بالظبط بالإسم والشكل هذا

.htaccess

وشرحت فوق بأحد النقاط كيف تحفظها ..

وفي المربع الثاني في الموقع ، تلاقيه يحتوي على كلام مثل هذا :

```
jj:110110001010
```

هذي إسم المستخدم وكلمة المرور المشفرة ، إنسخهم حرفياً وروح لمحرر النصوص وإلصقهم فيه وإحفظ الملف بالإسم والشكل هذا :

.htpasswd

وشرحت برضوا فوق كيف تحفظ بإسم أو إمتداد معين ..

الحين صار عندك ملفين ، الملف الأول إسمه

.htaccess

هذا إرفعه إلى مجلد wp-admin في مدونتك ..

والملف الثاني اللي إسمه

.htpasswd

هذا إرفعه إلى المجلد اللي أنشئته لأجل تخزن فيه ملف معلومات الدخول ، وفي حالتي انا راح أرفع هالملف إلى المجلد

/security

اللي أنشئته من شوي ..

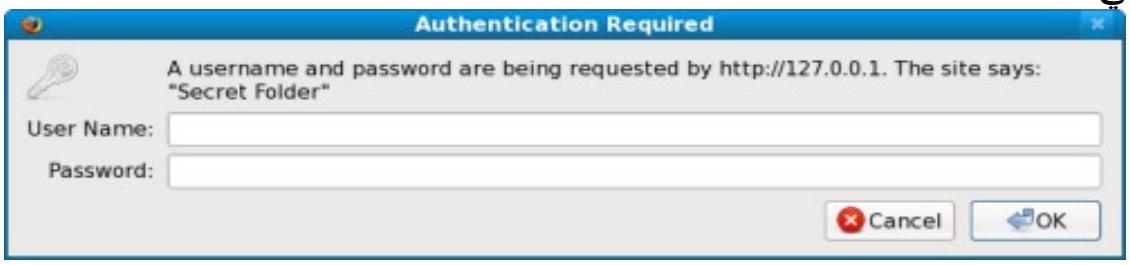
حلوين ، الحين روح وأطلب مجلد wp-admin في مدونتك ، وشوف أيش بيطلع لك :-)

..

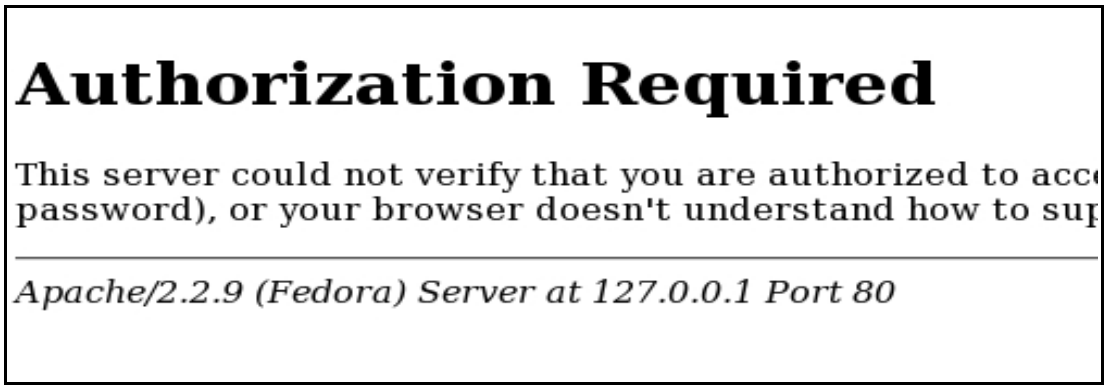
مثال :

http://jerais.com/plug/wp-admin/

وطلع لي هالشاشة :



ولو كتبت المعلومات خطأ أو ظغطت Cancel كانسل ، راح يقولي " باي باي " ، شوف تحت :



الخاتمة:

أتمنى من الله سبحانه إنو أكون توفقت بالشرح ، وإنو فيه أحد إستفاد منه ..
إذا إستفدت من هالوثيقة ، ما أطلب منك إلا إنك تدعي لي (دعوة صادقة) إن الله يشفيني ويسهل علي ..
وبرضوا أتمنى نشر هالوثيقة لإصحابك المدونين لزيادة الوعي ونشر الأمن التدويني في مدوناتنا العربية ..

كل التوفيق للجميع ..
الرووت جريس ..