Perché non sottovalutare la sicurezza del tuo sito Wordpress

Utilizzo Wordpress da almeno 5 anni e ho realizzato e gestito svariati siti internet. Una cosa che ho imparato è che questa piattaforma gratuita è estremamente potente e flessibile ma, allo stesso tempo, come tutti i software open source, tristemente vulnerabile. Il fatto che il codice sorgente con cui è scritto sia alla portata di tutti ne aumenta notevolmente la qualità (in quanto tutti possono contribuire al suo sviluppo), ma al contempo espone anche a occhi malevoli “tutti i segreti che stanno sotto al cofano”.Negli anni sono stati fatti passi da gigante per migliorare la sicurezza di Wordpress e i continui aggiornamenti ne seguono la strada, ecco perché è importantissimo mantenere sempre aggiornato Wordpress quando si utilizza per i propri progetti web.

Personalmente non mi sono mai preoccupato più di tanto di questo aspetto. Nella mia mente mi giustificavo con frasi come “è un sito amatoriale (o piccolo), a chi vuoi che importi hackerarlo?”, ma ho dovuto ricredermi quando mi sono trovato i primi siti bucati.

Esempi di attacchi Hacker personalmente subiti su siti Wordpress

Gli attacchi che ho potuto vedere e curare “con le mie mani” sono stati:

1. **Defacement della homepage del sito**: gli hacker hanno sostituito l’index.php del sito con un loro index.php che riportava il logo della Crew e simpatici messaggi per sfottere il webmaster del sito (io! :))

2. **Cancellazione totale di tutti i file nello spazio web del dominio**: sì, avete letto bene e per ben due volte. Fortuna che tengo sempre un backup locale dei file del sito. Peccato che nel primo caso non avessi una copia dei file caricati dagli utenti del sito (immagini e pdf) e sono andati irrimediabilmente persi. Nel secondo avevo invece attivato il backup automatico su Dropbox e tutto si è risolto per il meglio.

3. **Inserimento di iframe in tutte le pagine del sito**: questo è stato davvero difficile da identificare. In pratica l’hacker era riuscito ad entrare nel *file system* dell’hosting che usavo iniettando una *shell php* tramite un bug noto di un plugin che usavo ed ha inserito nel file *footer.php* del mio tema due *iframe* che caricavano due siti di casino online (penso per aumentare le visite ai fini statistici). Essendo nel *footer.php*, tutte le pagine del sito caricavano i contenuti dei due *iframe* provocando un sensibile rallentamento del sito. Me ne sono accorto controllando i tempi di *crawling* dello spider di Google da Webmaster Tools.

4.

Cambio delle password di amministrazione: un vero scherzone! Ti cambiano la password e la mail di tutti gli utenti Wordpress che trovano nel database e non puoi più entrare nel backend di Wordpress. Simpatico, no?

```
<html>

<body bgcolor="#000000" text="white" link="pink" vlink="pink">
<center>
<center>
<br><br>
<img src="https://fbcdn-sphotos-a-a.akamaihd.net/hphotos-ak-frc3/p480x480/992918_146533875551187_1925443845_n.jpg" title="Indonesian Hacker" />

<br>
<br>

<p> <font face="courier new"><font size="4" color=yellow>

<blink><font color=cyan></font>You Have </blink> been Hacked by </font><font color="#00ff00">Dowoh</font>
<br><br>
<font color="orange">be secure, your security get Down</font>
<br><br>

<font color=#c0c0c0 size=2>
<i><b>ubeliung96@yahoo.com</b></i>
</font></font>
<br>
<br>
<font color="darkred">Greet: God | maniak k4sur | sultan haikal | Agendosa | Sandal | Rio | sumaryanto<br> | Dias | Mheezand | All Indonesian Hacker
<font color=yellow size=2><br>
<a href="/index.php">Enter Site</a>
</font></font>


</p></center>

</body></html>
```

Cosa ho imparato?

Dagli attacchi sopra citati ho imparato che:

- preoccuparsi della sicurezza di Wordpress è buona (vitale) cosa (vedremo in seguito qualche consiglio)
- è necessario avere un backup (aggiornato) di tutti i file che compongono il sito
- è necessario avere un backup (aggiornato) dei dati nel database
- è necessario usare password sicure
- è consigliato controllare di tanto in tanto che i siti che realizzate siano “in salute”

Come rendere più sicuro Wordpress

Nell’ottimo articolo scritto da Maurizio Tarchini proprio su YIW un anno fa avevamo visto alcune caratteristiche e best practices per rendere sicuro Wordpress che sono ancora **valide** e attuali.

Oggi vorrei aggiungere qualche buon consiglio. Non voglio fare una carrellata di tutte le cose da fare per aumentare la sicurezza di Wordpress ma darvi qualche **utile suggerimento** (direttamente

dalla mia personale esperienza) da applicare velocemente ed avere da subito ottimi risultati.

Utilizza temi e plugin da fonti autorevoli e fidate

Sembrerà un consiglio scontato, ma ho visto più di qualche tema con codici sospetti per evitare di citarlo. A volte “solamente” semplici link inseriti in pagina tramite hook o filtri Wordpress che non sono direttamente visibili dal “normale utilizzatore”, ma che di fatto aggiungono al vostro sito un link esterno non desiderato (ad esempio ad un sito di spam o di pornografia) e che vi mettono in cattiva luce agli occhi dei vostri visitatori più attenti e (non da meno) un visitatore particolare chiamato Google (che potrebbe decidere di penalizzarvi).

Il mio consiglio è quindi di utilizzare **Temi Premium** (come gli ottimi creati dal team di YIThemes ed acquistati su marketplace autorevoli), **temi gratuiti** e **plugin** scaricati da **Wordpress**.**org** (sottoposti a controlli dal loro team).

Se non siete pienamente convinti di un **plugin** o **tema** che avete scaricato da una fonte poco attendibile potete fare una scansione direttamente nel vostro spazio web con il plugin chiamato Antivirus (che potete attivare alla bisogna o lasciare sempre attivo) o Exploit Scanner. Forse non scoveranno tutto, ma è una sicurezza in più.

Nascondi le informazioni sensibili

Come giustamente consigliava Maurizio nel precedente articolo nascondere le informazioni sulla versione di Wordpress che utilizzate è una buona pratica per non dare agli hacker un solido punto di partenza da cui partire per cercare eventuali vulnerabilità legate alla versione in uso.

Pertanto oltre a rimuovere la versione di Wordpress nella sezione della pagina (meta generator) e il paramentro di versionamento dei files (javascript e css) dovreste impedire l’accesso a questi particolari files presenti su un’installazione standard di Wordpress. Per farlo potete aggiungere nel file *.htaccess* del vostro sito quanto segue:

Sinceramente preferisco questa soluzione a quella suggerita da Maurizio (cancellare i files *readme* e *license*) perché dovreste farlo ad ogni aggiornamento di Wordpress (rischiando di dimenticarvene). Con questa regola invece potete dormire sonni tranquilli.

Limita l’accesso al backend di Wordpress

Una cosa che spesso si sottovaluta è l’errore umano. Supponete che per qualche ragione un hacker venga in possesso del vostro account di amministrazione (intercetta una vostra mail, legge il post-it che avete attaccato proprio sotto lo schermo del computer, ecc).

Per limitare i danni possiamo fare due cose. La prima agendo nel file *.htaccess* per restringere l'accesso all'amministrazione di Wordpress ad una lista nota di IP:

Io stesso uso un **IP dinamico** e questa soluzione diventa laboriosa (richiederebbe l'aggiornamento del file *htaccess* ogni volta che dovete fare login), ma in ambito aziendale non è così strano avere un **IP statico**. In caso potreste voler proteggere la cartella wp-admin realizzando un'area riservata con accesso controllato da *htaccess*.

Un'altra cosa che potere fare per limitare i danni è **impedire** l'editing dei file direttamente da Wordpress. Si può fare semplicemente aggiungendo questa riga al vostro file wp-config.php (anche se i corretti permessi sui files dovrebbero già dare questo tipo di protezione):

Non usare l'utente di default: admin

Nelle ultime versioni di Wordpress l'installazione permette di scegliere il nome utente per l'account principale, ma fino a poco tempo fa era preimpostato su: **admin**.

Questo esponeva (ed espone tutt'ora) il vostro sito Wordpress ad attacchi di tipo **brute force**. Gli hacker conoscono già il nome utente e devono "solo" indovinare la vostra password per poter entrare.

Per prima cosa consiglio di rimuovere l'utente admin.

Ecco due modi per farlo.

Il primo utilizza una query SQL che potete lanciare direttamente dal pannello di controllo del vostro database (penso a phpMyAdmin) o da qualsiasi client MySql:

Il secondo, più semplice e laborioso, consiste nel creare un altro utente con ruolo di amministrazione e di eliminare il precedente.

Vediamo velocemente i passi da seguire:

1. Entra su Wordpress con il tuo account **admin**
2. Crea un nuovo utente con ruolo di **Amministratore**
3. Esci e rientra su **Wordpress** con il nuovo utente
4. **Cancella** l'utente **admin** ed attribuisci pagine ed articoli al tuo nuovo amministratore

Sempre nell'ottica di tamponare gli attacchi di tipo **brute-force** potete evitare di visualizzare gli

errori relativi al login in quanto danno importanti informazioni agli hacker. Per farlo aggiungete al vostro file *functions.php* questo codice:

Al posto del "*return null;*" potete inserire una funzione di **callback** per inviarvi una mail a ogni tentativo fallito. Il plugin Limit Login Attemps fa egregiamente questo sporco lavoro per voi, limitando l'accesso ad un IP che abbia fallito il login per più di un numero da voi impostato di tentativi.

Monitorare i cambiamenti sui files

La cosa che mi avrebbe salvato in tutti i casi di attacco che ho descritto sopra sarebbe stato un **alert via email** ogni volta che fosse avvenuto un **cambiamento** nel **file system** dello spazio web (es. modifica di un file, creazione di un nuovo file, ecc).

In passato ho usato a tale scopo il plugin File Monitor, ma sembra essere un progetto abbandonato. Qualcuno ha voglia di riesumarlo assieme a me?

Sono poi passato a **Website Defender**, un servizio online che monitorava (tramite un loro file php da inserire in root del dominio) i cambiamenti sui file. Oggi hanno cambiato modello di business diventando un plugin per Wordpress che offre varie configurazioni per aumentare la sicurezza del sistema. Non l'ho provato.

Voi conoscete qualche altro servizio online che dia questa possibilità? È sufficiente una mail di alert quando cambia qualcosa all'interno dello spazio web. Penso sia un buon metodo per poter intervenire in tempi brevi a seguito di un attacco, quando le nostre contromisure sono state già superate.

Monitorare i gli errori 404

Oltre ad aiutarvi a correggere potenziali errori nel vostro sito, il monitoraggio degli **errori 404** (pagina non trovata) può aiutarvi ad individuare potenziali richieste malevole, che hanno l'intento di:

- entrare nel vostro sito cercando la **login page** o la **pagina di registrazione**
- entrare nel vostro sito sfruttando **vulnerabilità** note di **plugin Wordpress**

Ecco un'esempio di richieste che hanno causato errori 404 in alcuni dei miei siti WordPress (se riconoscete uno dei plugin che usate, forse è il caso di preoccuparsi :)):

```
/wp-content/plugins/tell-a-friend/tell-a-friend.php  /wp-content/themes/O
ptimizePress/lib/admin/media-upload.php  /wp-login.php?action=register  /
```

```
member/index_do.php?fmdo=user&dopost=regnew  /wp-content/plugins/wp-maili
nglist/vendors/uploadify/upload.php  /wp-content/plugins/mini-mail-dashbo
ard-widget/wp-mini-mail.php  /wp-content/plugins/thecartpress/checkout/Ch
eckoutEditor.php  /wp-content/plugins/wpstorecart/php/upload.php  /wp-con
tent/plugins/wp-property/third-party/uploadify/uploadify.php  /wp-content
/plugins/advanced-custom-fields/core/actions/export.php  /wp-content/plug
ins/tell-a-friend/tell-a-friend.php  /wp-content/plugins/mm-forms-
community/includes/doajaxfileupload.php
```

Conclusioni

Mi auguro di avervi raccontato una bella storia, tratta dalla mia personale esperienza, che spero possa mettervi una pulce nell'orecchio e farvi, se già non lo fate, apprezzare e curare maggiormente la **sicurezza** dei vostri siti.

Penso che il **miglior plugin** in circolazione per aumentare la sicurezza di Wordpress sia Better WP Security. Alcuni dicono che è un po' affamato di risorse, ma nelle installazioni in cui l'ho usato non ha creato particolari rallentamenti. Sono in contatto con lo sviluppatore e so che a breve uscirà un nuova versione potenziata… speriamo abbiano curato anche le performance.

Se invece siete dei puristi, consiglio di crearvi il vostro file *.htaccess* e *functions*.php (meglio se un file separato da includere in esso) con le regole di base e di includerli in ogni sito che realizzate.

Ricordate inoltre che, potete prendere tutte le misure di sicurezza possibili, ma se il vostro vicino di casa (un sito ospitato sullo stesso server del vostro) o l'hosting in generale non mantiene standard elevati per la sicurezza siete sempre a rischio. Pertanto backup regolari e monitoraggio dei siti web sono due cose da mettere sempre in piano.

Nel mio prossimo articolo vorrei parlare delle soluzioni e procedure da adottare quando un vostro sito Wordpress viene hackerato. Che dite? Potrebbe interessarvi?

Le vostre esperienze

Quali sono le vostre esperienze in merito? Un vostro sito è mai stato "bucato" da un hacker? Quali accorgimenti adottate per rendere sicuro Wordpress?

Aspetto i vostri commenti. :)