Come rendere sicuro WordPress

lunedì, 03 settembre 2018

Il tema della sicurezza di un sito web è un argomento sempre molto discusso e l'utilizzo di WordPress non fa eccezione, anzi spesso è proprio oggetto di critiche. Se da un lato l'utilizzo di un CMS open source mette a disposizione di tutti la possibilità di migliorarlo e correggerne bug ed errori, dall'altra lo espone all'analisi di malintenzionati che ricercano falle e possibilità di violarlo. Ma come ci si può difendere? Ecco qualche utile consiglio, qualcuno magari ai più potrebbe sembrare semplice e scontato, ma vale sempre la pena menzionarlo.

Sommario

Backup

Semplice e banale consiglio, ma può salvarti da disastri! È sempre bene avere a disposizione un **backup** del sito e soprattutto del database. Assicurati quindi di avere un hosting che offra il servizio di backup automatici (a meno che tu non voglia preoccuparti di farli manualmente).
SiteGround può essere un ottimo esempio:
Servizi di backup hosting

Aggiornamenti

WordPress, come accennato in precedenza, è un progetto open source che può avvalersi di una community davvero molto estesa. Lo scopo è proprio quello di migliorare il CMS, ma soprattutto di chiudere eventuali falle che possano essere sfruttate da **hacker**. Assicurati quindi di mantenere sempre aggiornato all'ultima versione il tuo WordPress.
Lo stesso discorso vale anche per gli eventuali plugin e temi che utilizzi.

Plugin e temi

Un consiglio molto spesso trascurato, è utilizzare temi e plugin **premium**. Questo non perché gli sviluppatori di risorse gratuite siano meno preparati, ma temi e plugin gratuiti spesso non hanno una frequenza di aggiornamento ed un supporto tale da correggere eventuali bug. Inoltre, proprio perché liberamente scaricabili, possono essere analizzati con più facilità da chi volesse carpirne eventuali falle.
Dai un'occhiata alla collezione di plugin e temi premium presenti su **Envato Market**:

Temi e plugin premium

Inoltre, elimina sempre plugins e temi non utilizzati, potrebbero essere sempre un eventuale porta di accesso. Ma perché rischiare se non sono utilizzati?
Infine, un consiglio perentorio: MAI utilizzare temi e plugin "crackati"! Chiunque abbia violato in qualche modo il codice per rimuovere i controlli di licenza, potrebbe benissimo aver aggiunto allo stesso modo codice malevolo per carpire informazioni ed accessi dal tuo sito.

Utenti e password

Non utilizzare "admin" come nome utente. Può sembrare banale e scontato, ma ti assicuro che non lo è, non sai quante volte mi sono imbattuto in siti in cui era presente un profilo utente "admin". Molti si staranno chiedendo: perché mai non dovrei usare "admin" come username? È presto detto: nel caso un malintenzionato volesse provare ad accedere al backend del tuo sito (in casi più evoluti magari attraverso un attacco **brute-force**), quale sarebbe uno dei primi nomi utenti che proverebbe? Utilizzare lo username "admin" sarebbe come regalare già il 50% di successo in un eventuale hackeraggio!
Altrettanto banale consiglio, utilizza sempre password non semplici da stanare e sebbene possa essere una seccatura riuscire poi a ricordarle, meglio adoperare password lunghe e generate casualmente.

Norton può fornirti uno strumento gratuito ed utile allo scopo:
Strong password generator

Login

Di default, quando qualcuno prova ad effettuare i login nel backend di WordPress, in caso di errore ci viene restituito un messaggio che indica con precisione se ad essere sbagliato è il nome utente o la password. Ma perché regalare questo tipo di informazione ad eventuali malintenzionati? Il consiglio è di utilizzare un messaggio di errore più generico che non dia precise indicazioni. Farlo è semplice, ti suggerisco di leggere l'articolo:

Personalizzare la pagina di login di WordPress

in particolare il paragrafo **"Personalizzare i messaggi di errore"**. Dai un'occhiata anche al paragrafo **"Forzare il login con email"**, che può fornirti uno strumento in più per proteggere il tuo WordPress.

Il prefisso delle tabelle

In fase di installazione, WordPress ci chiede quale prefisso desideriamo utilizzare per le tabelle del database

Il prefisso predefinito, che in tantissimi lasciano inalterato, è **wp**_. Ma se qualcuno volesse provare ad effettuare un attacco di tipo **SQL Injection**, avrebbe già un grosso vantaggio conoscendo non solo il nome standard delle tabelle del DB di WordPress, ma anche il prefisso utilizzato.
Assicurati quindi di utilizzare per le tabelle del tuo database un prefisso non comune.

Permessi file e cartelle

È sempre buona norma impostare i permessi di lettura e scrittura corretti per evitare accessi non autorizzati. Puoi approfondire l'argomento leggendo la guida:

Impostare i permessi delle cartelle e dei file di WordPress

Rimuovere i riferimenti a WordPress

È bene fare una piccola premessa: un occhio esperto può immediatamente riconoscere se un sito è stato realizzato utilizzando WordPress, ma evitare di esporre in chiaro la cosa può essere un ulteriore deterrente.
Ogni installazione di WordPress aggiunge nell'head del sito un meta tag che riporta in bella vista non solo il fatto che il sito sia realizzato con WordPress, ma anche la versione utilizzata!

Quindi, anche un semplice bot potrebbe carpire questa informazione, sfruttando i bug già noti di quella determinata versione. Ma niente paura, rimuovere il meta tag è semplicissimo. È sufficiente editare il file:

wp-content/themes/{nome_del_tema}/functions.php

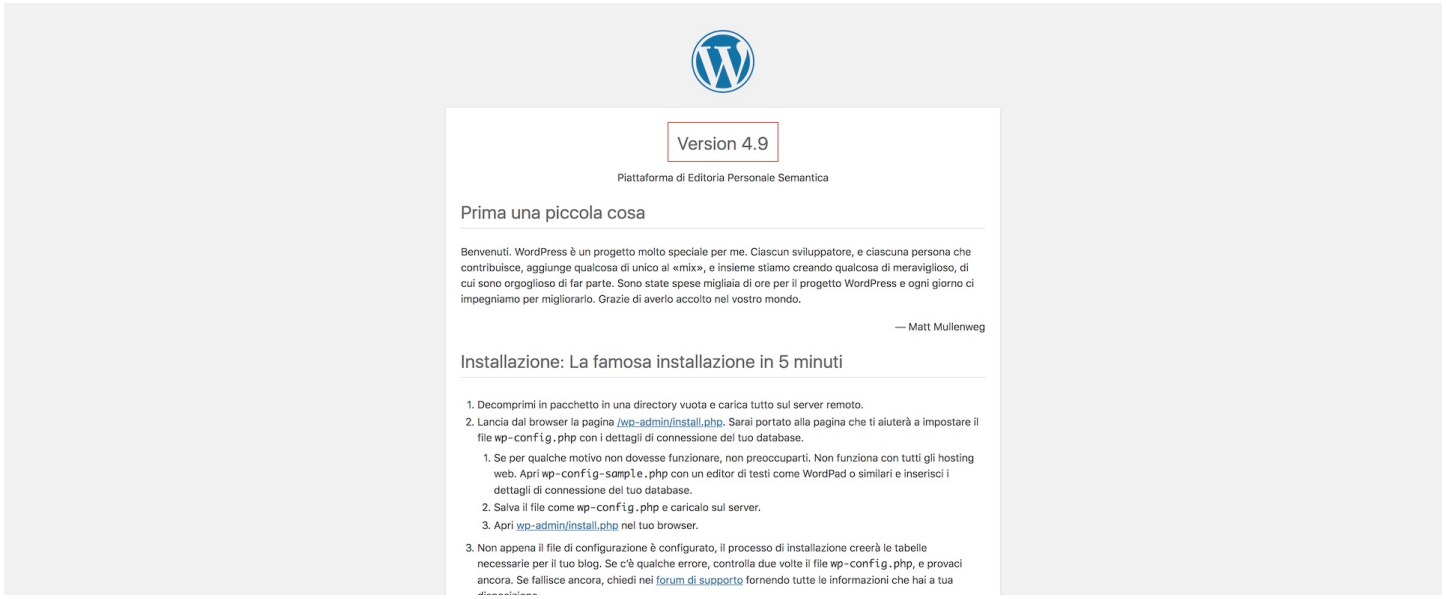
che trovi nello spazio FTP del tuo sito, nella cartella del tema attivo, ed inserire il codice:

```
// Rimuovo il tag XHTML generator
remove_action( 'wp_head', 'wp_generator' );

// Rimuovo il tag generator dai fedd RSS
add_filter( 'the_generator', '__return_false' );
```

Ti consiglio anche vivamente di cancellare il file **readme.html** presente nella cartella principale del tuo sito, perché anche lì è chiaramente visibile la versione di WordPress utilizzata. Inoltre, accedere a questa informazione è semplicissimo per chiunque, basta digitare nel browser l'indirizzo (dove *www.example.com* è il dominio del tuo sito):

https://www.example.com/readme.html



Version 4.9

Piattaforma di Editoria Personale Semantica

Prima una piccola cosa

Benvenuti. WordPress è un progetto molto speciale per me. Ciascun sviluppatore, e ciascuna persona che contribuisce, aggiunge qualcosa di unico al «mix», e insieme stiamo creando qualcosa di meraviglioso, di cui sono orgoglioso di far parte. Sono state spese migliaia di ore per il progetto WordPress e ogni giorno ci impegniamo per migliorarlo. Grazie di averlo accolto nel vostro mondo.

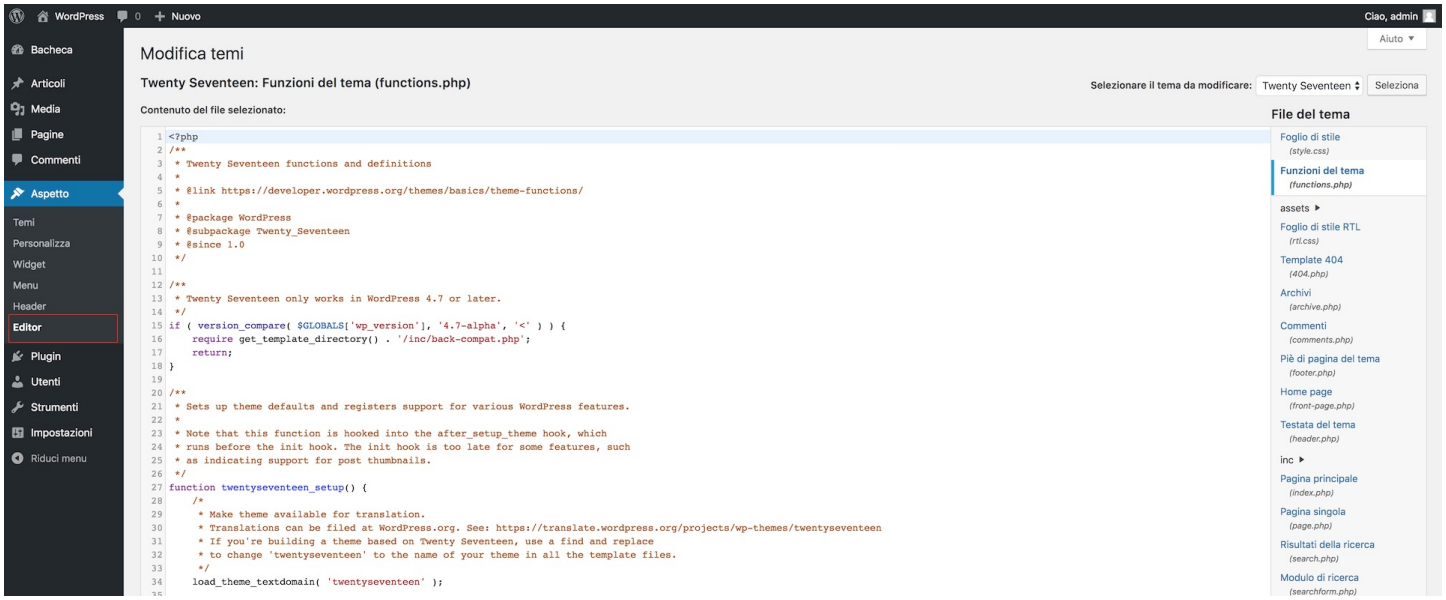
— Matt Mullenweg

Installazione: La famosa installazione in 5 minuti

1. Decomprimi in pacchetto in una directory vuota e carica tutto sul server remoto.
2. Lancia dal browser la pagina /wp-admin/install.php. Sarai portato alla pagina che ti aiuterà a impostare il file `wp-config.php` con i dettagli di connessione del tuo database.
    1. Se per qualche motivo non dovesse funzionare, non preoccuparti. Non funziona con tutti gli hosting web. Apri `wp-config-sample.php` con un editor di testi come WordPad o similari e inserisci i dettagli di connessione del tuo database.
    2. Salva il file come `wp-config.php` e caricalo sul server.
    3. Apri wp-admin/install.php nel tuo browser.
3. Non appena il file di configurazione è configurato, il processo di installazione creerà le tabelle necessarie per il tuo blog. Se c'è qualche errore, controlla due volte il file `wp-config.php`, e provaci ancora. Se fallisce ancora, chiedi nei forum di supporto fornendo tutte le informazioni che hai a tua

La modifica dei file da admin

WordPress attiva di default una funzione molto utile in fase di sviluppo, ovvero la possibilità di modificare al volo un file .PHP direttamente dall'area admin (backend)



Ma questa funzione va assolutamente disattivata una volta che il sito è in fase di produzione. Qualora un malintenzionato riuscisse ad accedere al backend di WordPress (scovando username e password ad esempio), potrebbe sicuramente fare danni, ma nulla in confronto a cosa potrebbe succedere se riuscisse ad avere accesso e addirittura modificare i file del sito!
Evitare questa spiacevole quanto dannosa evenienza è semplice. È sufficiente editare il file:

wp-config.php

che trovi nello spazio FTP del tuo sito ed inserire il codice:

```
// Disabilita l'editor dei files di WordPress
define( 'DISALLOW_FILE_EDIT', true );
```

esattamente prima della riga:

/ Finito, interrompere le modifiche! Buon blogging. */*

Per i più esperti: il file .htaccess

Ecco infine qualche consiglio più avanzato per mettere in sicurezza e rendere sicuro il tuo WordPress utilizzando poche righe da inserire nel file **.htaccess**:

```
# Previene lâ€™accesso ai file dellâ€™installer di WordPress
RedirectMatch Permanent wp-admin/install(-helper)?\.php /

# Disabilita la navigazione delle cartelle
Options All -Indexes

# Blocca lâ€™accesso diretto alle cartelle ed ai file presenti in wp-includes
<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>

#  Blocca lâ€™accesso diretto a file di sistema
<FilesMatch "^.*(error_log|debug\.log|wp-config\.php|php.ini|\.[hH][tT][aApP].*)$">
 Order deny,allow
 Deny from all
</FilesMatch>

# Protegge da tentativi di attacchi di tipo â€œscript injectionsâ€•
Options +FollowSymLinks
RewriteEngine On
RewriteCond %{QUERY_STRING} (<|%3C).*script.*(>|%3E) [NC,OR]
RewriteCond %{QUERY_STRING} GLOBALS(=|[|%[0-9A-Z]{0,2}) [OR]
RewriteCond %{QUERY_STRING} _REQUEST(=|[|%[0-9A-Z]{0,2})
RewriteRule ^(.*)$ index.php [F,L]

# Protegge da tentativi di attacchi di tipo â€œbrute forceâ€•
<IfModule mod_rewrite.c>
    RewriteEngine On
    RewriteCond %{REQUEST_METHOD} POST
    RewriteCond %{REQUEST_URI} ((wp-comments-post)|(wp-login)|(xmlrpc))\.php$
    RewriteCond %{HTTP_REFERER} ^$
    RewriteRule (.*) - [F,L]
</ifModule>

# Previene lâ€™enumerazione dei nome utente
RewriteCond %{QUERY_STRING} author=d
RewriteRule ^ /? [L,R=301]
```