Come difendersi da un attacco brute force su WordPress?

Dario Lombardi - 2025-12-02 - Applicazione CMS

Sono oggetto di **attacco brute force su WordPress**. Quali sono le contromisure? Come difendere il tuo sito web da questa minaccia? Il primo punto è una conoscenza minima del tipo di cyberattacco. Devi scoprire cos'è e come si articola un attacco del genere.

Poi passiamo alla miglior difesa possibile: quella che ti permette di proteggere il tuo sito web WordPress. Anche aggiungendo **un livello di autenticazione HTTP Basic** prima che qualcuno o qualcosa possa raggiungere il form di login standard.

Cos'è un attacco brute force su un sito web?

L'attacco brute force - letteralmente forza bruta, prepotenza - è un metodo utilizzato dai cybercriminali per **entrare in una proprietà digitale** ottenendo in modo illecito le password. Questo avviene attraverso il tentativo di tutte le possibili combinazioni di caratteri.

Tutto si basa su software automatizzati che generano migliaia di tentativi al secondo. L'attacco consiste nel **provare tutte le possibili combinazioni** di lettere, caratteri speciali e numeri finché non individua quella corretta. Il tempo necessario per completare l'attacco dipende da due fattori che fanno da base alla nostra difesa:

- Creazione di ostacoli efficaci.
- Complessità della password.

WordPress è particolarmente soggetto ad attacchi del genere per diversi motivi. In primo luogo, ha una pagina login raggiungibile da tutti. E **ha sempre lo stesso indirizzo** di default, quindi nella maggior parte dei siti si raggiunge facilmente. (qui ti spieghiamo come accedere al pannello di controllo WordPress).

Poi è un CMS super diffuso: **un attaccante può lanciare lo stesso script** automatizzato su milioni di siti sapendo che funzionerà su una percentuale significativa. Ma al tempo stesso non offre nessuna protezione nativa. Nessun problema, ci pensiamo noi a spiegarti come difendersi da un attacco brute force su WordPress.

Scegli una password sicura

Il primo consiglio per rallentare un attacco brute force: usa una password sicura, tipo quella che ti viene suggerita dal CMS quando fai il tuo primo login per entrare nella dashboard di WordPress. Utilizzare parole e combinazioni tipo admin, 12345, qwerty o la squadra di calcio è una pessima idea, i **programmi di brute force** la indovinano in un decimo di secondo.

Ma basta poco per risolvere: come ci ricorda Security.org, una password di dodici caratteri con una lettera maiuscola, un numero e un simbolo **è quasi inviolabile**, per decifrarla un computer dovrebbe impiegare 34.000 anni.

Cambia indirizzo di login

Certo, se posso raggiungere subito la pagina di riferimento per accedere nel tuo sito web ho già superato un ostacolo importante per entrare nel portale. Di default, la pagina di login è sempre a `/wp-admin` o `/wp-login.php`. Non serve un lavoro approfondito per indovinare: basta utilizzare l'indirizzo `www.esempiodominio.it/wp-admin` per arrivare direttamente alla porta d'ingresso. Per risolvere questo problema puoi utilizzare il plugin WPS Hide Login:

- Lo installi.
- Vai nelle impostazioni.
- Scegli il nuovo login URL.
- Salvi.

Fatto. Sarà il plugin a gestire **redirect e aggiornamenti**. Si tratta di un’estensione leggera, puoi utilizzarla tranquillamente. Ma ricorda che se l’attacco di brute force raggiunge questa pagina sei al punto di partenza. Meglio pensare a un’operazione più articolata.

Aggiungi un livello di autenticazione HTTP

Ecco una soluzione per tutelare il tuo account WordPress da attacchi brute force: creare una barriera protetta da login prima di arrivare all'accesso ufficiale. In questo modo, chi tenta di scassinare il tuo sito web si trova di fronte a due passaggi da affrontare.

Questa guida spiega come aggiungere un livello di sicurezza aggiuntivo alla pagina di login di WordPress utilizzando l'autenticazione HTTP Basic tramite file .htaccess e .htpasswd.

Client FTP (come FileZilla)
Accesso FTP al server WordPress
Editor di testo
Generatore htpasswd online (es. www.web2generators.com)

Modificare il file .htaccess

Accedi via FTP al tuo dominio con WordPress installato e naviga nella cartella /home/utente/public_html/

Apri il file .htaccess e inserisci le stringhe in testa al file:

```
<FilesMatch "wp-login.php$">
    AuthName "Protezione WordPress"
    AuthType Basic
    AuthUserFile /home/utente/wordpress.htpasswd
    Require valid-user
    ErrorDocument 401 /e.html
</FilesMatch>
```

Sostituisci "utente" con il tuo nome utente di accesso FTP nel percorso AuthUserFile.

Generare le credenziali con formato htpasswd

Visita un generatore htpasswd online come www.web2generators.com

Inserisci lo username e la password che desideri per la protezione (ad esempio, username: "wordpress" e password: "aesoni8OR4aeXa").

Il generatore produrrà una riga nel formato htpasswd, ad esempio:

```
wordpress:$apr1$xocb54k8$sBzP/m2ngCCTA/70wpjAI0
```

Copia questa riga generata per utilizzarla nel prossimo passaggio.

Creare il file wordpress.htpasswd

Nel client FTP, naviga nella cartella /home/utente/ (quindi fuori dalla cartella public_html, un livello superiore).

Crea un nuovo file chiamato wordpress.htpasswd

Apri il file e incolla la riga generata nel passaggio precedente.

Salva e chiudi il file.

Generare la pagina di errore personalizzata

Torna nella cartella /home/utente/public_html/ tramite il client FTP.

Crea un nuovo file chiamato e.html (può essere anche vuoto o contenere un messaggio di errore personalizzato).

Salva il file.

Verificare il funzionamento

Visita la pagina www.tuodominio.ext/wp-admin o www.tuodominio.ext/wp-login.php

Ti verrà presentato un popup del browser che richiede username e password (quelle create con il generatore htpasswd).

Dopo aver inserito le credenziali corrette, vedrai la normale pagina di login di WordPress.

Al termine della procedura, la pagina di login di WordPress sarà protetta da un doppio livello di autenticazione: prima l'autenticazione HTTP Basic, poi quella standard di WordPress.