Rafforza la sicurezza su WordPress: come proteggo il mio sito da attacchi amplificati XML-RPC?

Christian Cantinelli - 2023-11-15 - Applicazione CMS

Come proteggo il mio sito da attacchi amplificati XML-RPC

Sei il fortunato proprietario di un sito WordPress e sappiamo quanto sia fondamentale comprendere le insidie legate alle funzionalità del tuo spazio online.

XML-RPC, acronimo di "XML Remote Procedure Call", rappresenta un meccanismo di pubblicazione remota all'interno di WordPress. Consente a client come Windows Live Writer di effettuare chiamate da remoto per la pubblicazione di contenuti.

Tuttavia, questa funzionalità, se non gestita adeguatamente, potrebbe diventare una **potenziale vulnerabilità**, aprendo la strada ad attacchi amplificati verso altri siti web.

In questo articolo, vogliamo condividere con te questo rischio e come puoi affrontarlo: disabilitando in modo sicuro XML-RPC attraverso .htaccess.

Vediamo cosa comporta avere la funzione aperta:

1. **Rischio di attacchi amplificati**: È importante che tu sappia che il tuo sito WordPress potrebbe involontariamente diventare un punto di partenza per attacchi amplificati tramite XML-RPC. Un BOT malevolo, puntando al tuo sito, potrebbe sfruttare chiamate massicce a XML-RPC per intensificare gli attacchi verso altri obiettivi.
2. **Evitiamo il sottoutilizzo**: Se noti che XML-RPC è poco utilizzata sul tuo sito, è sensato disabilitarla. Questo evita sprechi di risorse e protegge il tuo sito da essere coinvolto in attacchi amplificati. Molti siti non hanno necessità di avere xmlrpc attivo

Quindi come proteggiamo il tuo sito web?

Per proteggere il tuo sito WordPress e prevenire attacchi amplificati attraverso XML-RPC, ti consigliamo di **disabilitare la funzionalità.**

Per farlo, aggiungi le seguenti righe al tuo file .htaccess principale per garantire una difesa efficace:

```
# Blocca le richieste a WordPress xmlrpc.php
<Files xmlrpc.php>
order deny,allow
deny from all
</Files>
```

Questo garantisce che nessun possa utilizzare questo modulo.

Se vuoi attivarlo solo per un indirizzo IP (es. un servizio esterno), modifica l'.htaccess aggiungendo "allow from IP" (con l'indirizzo ip da abilitare):

```
# Blocca le richieste a WordPress xmlrpc.php
<Files xmlrpc.php>
order deny,allow
deny from all
allow from 123.123.123.123
</Files>
```

La sicurezza del tuo sito WordPress è una priorità. Disabilitando XML-RPC tramite .htaccess, stai compiendo un passo fondamentale nel rafforzamento della sicurezza del tuo spazio online.

Questa azione non solo mitiga il rischio di abusi, ma assicura anche una presenza online più sicura e affidabile per te e i tuoi visitatori.