SHELLRENT

Il primo hosting italiano Security First

WordPress & Security: come difendersi dagli attacchi più frequenti

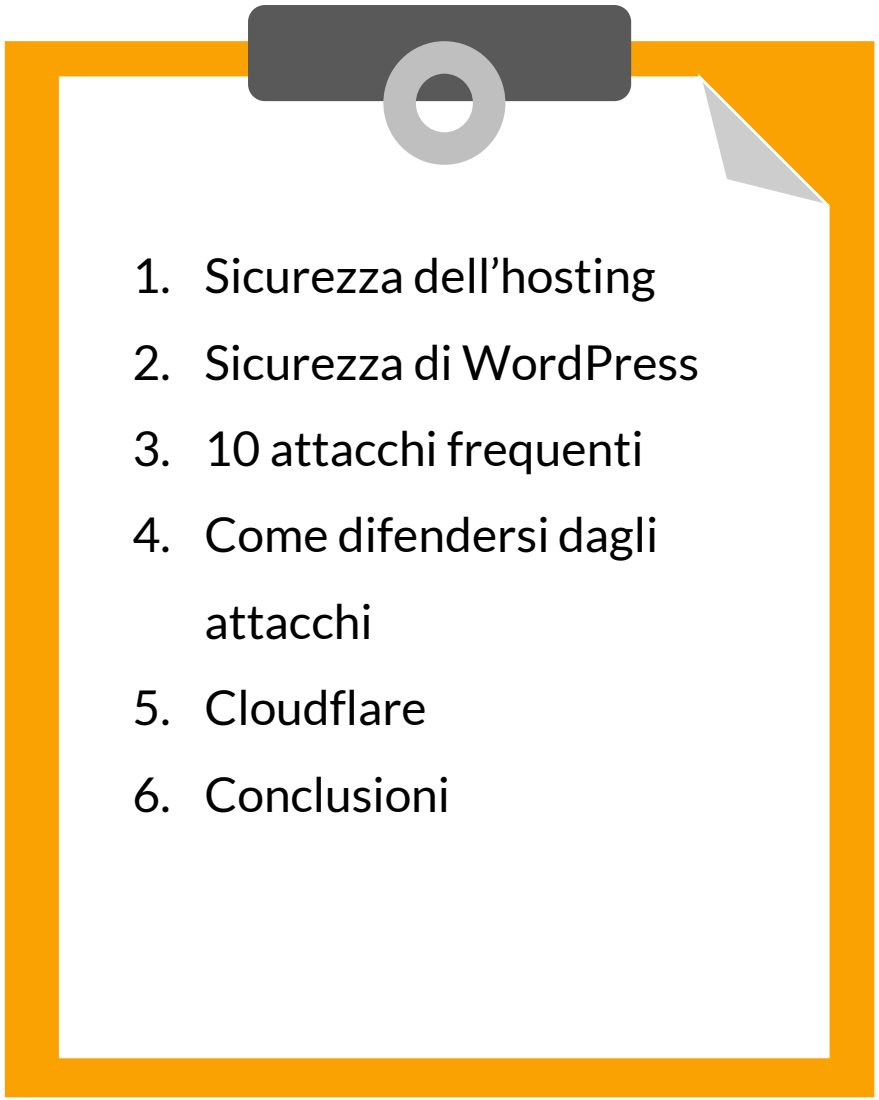
Ivo Lauro

Responsabile Consulenza e Supporto Tecnico – Shellrent

Da oltre 5 anni lavoro in Shellrent, hosting e cloud provider, come Responsabile della consulenza e del supporto tecnico.
Coordino il team che cura i progetti di consulenza e supporto i clienti nel realizzare soluzioni personalizzate per ogni progetto in materia di piattaforme web ed email, servizi cloud ed infrastrutture IT.

https://www.linkedin.com/in/ivolauro/

AGENDA



1. Sicurezza dell’hosting
2. Sicurezza di WordPress
3. 10 attacchi frequenti
4. Come difendersi dagli attacchi
5. Cloudflare
6. Conclusioni

LA SICUREZZA DELL'HOSTING

La sicurezza di WordPress ha inizio dall'hosting: prima di pensare all'applicativo bisogna ottimizzare la sicurezza a livello web-server.

Cosa deve offrire un hosting provider in termini di sicurezza?

Server hardening con aggiornamenti costanti alla struttura e al sistema operativo.

Politica di backup automatica e preventiva.

Presenza di un firewall centralizzato con blocco automatico sia degli attacchi brute force sia degli attacchi DOS.

Scansioni malware automatiche.

Protezione DDoS grazie all'utilizzo di una CDN come Cloudflare.

LA SICUREZZA DI WORDPRESS

Installazione di WordPress: 10 elementi a cui fare attenzione

1. **Aggiorna WordPress, PHP, plugin e temi**: gli aggiornamenti vengono fatti per migliorare la sicurezza o correggere alcuni bug. Noi consigliamo sempre di aggiornare alle versioni recenti WordPress, PHP, temi e plugin.
2. **Blocca l'area admin**: puoi modificare l'URL di login di wp-admin e limitare i tentativi di accesso seguendo il concetto di *security by obscurity*.
3. **Sfrutta l'autenticazione a 2 fattori**: puoi integrare la password con l'autenticazione via SMS o OTP per una maggiore protezione dagli attacchi brute-force.
4. **Usa il protocollo HTTPS e installa il certificato SSL**: assicura una connessione protetta, un migliore ranking SEO e maggiore credibilità nei confronti degli utenti.
5. **Proteggi il file wp-config.php**: puoi spostare il file in una directory non accessibile da browser, modificare le chiavi di sicurezza all'interno del file o controllare i permessi in modo che solo tu possa leggerlo (permesso 440 o 400).

Installazione di WordPress: 10 elementi a cui fare attenzione

6. **Disabilita XML-RPC**: questo protocollo viene spesso usato per condurre attacchi brute-force per questo si consiglia di disabilitarlo. Extra: prima di procedere controlla se qualche plugin necessita del protocollo per funzionare correttamente
7. **Rafforza la sicurezza del database**: solitamente il nome del database è impostato su wp_nomesito ma per renderlo più sicuro ti consigliamo di personalizzarlo.
8. **Controlla i permessi di file e directory**: questi possono essere di lettura, scrittura o esecuzione. Di norma, tutti i file dovrebbero essere 640, ad esclusione di wp-config.php impostato su 400. Le directory invece dovrebbero essere 750.
9. **Sfrutta .htaccess**: puoi inserire del codice nel file che limiti l'accesso a wp-config.php e a wp-admin.php. Extra: ricorda di inserirlo fuori dai tag # BEGIN WordPress e # END WordPress per evitare che venga sovrascritto dagli aggiornamenti.
10. **Usa un firewall**: potrai monitorare il traffico di rete, bloccare gli utenti e gli IP spammosi e proteggere il sito dagli attacchi DDoS (Cloudflare).

WordPress Toolkit - Plesk

Se usi Plesk come pannello di gestione, potrai installare e gestire da un'unica interfaccia tutti i siti WordPress grazie al WordPress Toolkit.

Quali sono i vantaggi di WordPress Toolkit?

- Dashboard unica per gestire e controllare tutti i siti dei clienti e le relative istanze WordPress.
- Ambiente di staging per eseguire test e verificare il corretto funzionamento di aggiornamenti.
- Gestione intuitiva di temi e plugin su una singola istanza WordPress o su multiple istanze contemporaneamente.
- 1-click hardening.
- Gestire in modo diretto i debug di tutti i siti.
- Clonare un'istanza WordPress.
- Migliorare la sicurezza dei siti WordPress semplicemente cliccando su *Secure*.

10 ATTACCHI FREQUENTI

Backdoor: spesso appare come file legittimo di sistema o sfrutta qualche bug di versioni obsolete di WordPress; viene utilizzata accedere al back-end o caricare file corrotti.

Pharma Hacks: inserisce codice malevolo in versioni obsolete della piattaforma in modo che i motori di ricerca restituiscano annunci di prodotti farmaceutici.

Attacchi brute-force: utilizzano script automatici per identificare password deboli e accedere al sito web.

Redirect malevoli: sfruttando delle backdoor in WordPress come utente admin è possibile iniettare codici di reindirizzamento malevoli nel sito web. Spesso i redirect vengono inseriti nel file .htaccess o direttamente nel database modificando la siteurl.

Cross-site Scripting (XSS): consiste nell'inserimento di uno script dannoso in un sito web autorevole per appropriarsi dei dati di cookie o di sessione fino a riscrivere l'HTML di una pagina.

Denial of Service: sovraccarica la memoria dei sistemi operativi dei siti web, sfruttando versioni obsolete del software di WordPress o errori e bug nel codice.

Phishing: l'obiettivo è rubare le informazioni sensibili degli utenti come dati di accesso o carta di credito spacciandosi per un noto sito affidabile, invitando gli utenti a condividere le proprie informazioni.

Mailbombing: sfruttando form di contatto non protetti da recaptcha, si generano automaticamente email destinate ad una casella bersaglio, per saturarla e bloccarla.

Defacement: utilizzato per modificare l'aspetto visivo di un sito web per renderlo inutilizzabile e promuovere messaggi non correlati, spesso di natura politica/sociale.

Php.mailers: sono strumenti che utilizzano comandi php per inviare e-mail di spam o phishing direttamente dal sito web infetto.

COME DIFENDERSI DAGLI ATTACCHI

Come difendersi dagli attacchi?

Effettua sempre i backup, diversificando la destinazione e l'orario.

Esegui dei check regolari per verificare l’integrità dei file.

Ricorda di mantenere tutto aggiornato.

Scansiona il sito per verificare il livello di sicurezza, individuare malware o altre vulnerabilità e risolverle preventivamente.

Quando non devi fare modifiche, rendi i file immutabili (File Protection).

Monitora i log di accesso e di attività.

Verifica se Google ha indicizzato il sito in modo incongruo.

Come difendersi dagli attacchi?

Utilizza dei plugin per migliorare la sicurezza:

Sucuri Security

WP fail2ban

Jetpack

iThemes Security

All in One WP Security & Firewall

Wordfence Security


CLOUDFLARE

La CDN Cloudflare offre un sistema di **cache dei contenuti**, la quale viene distribuita in un insieme di server sparsi nel mondo che li ridistribuiscono localmente, **aumentando la velocità** e distribuendo il carico.
Integra inoltre un raffinato sistema **anti-DDOS** e varie strategie di evasione dagli attacchi.

Cloudflare deve essere attivato a livello di dominio in quanto si basa sulla gestione dei nameserver per proteggere i web server, anche mascherando il reale indirizzo IP (*security by obscurity*).

Vantaggi:

- Ridurre i **tempi di caricamento del sito web**: le richieste di contenuti degli utenti saranno elaborate con la stessa velocità in ogni parte del mondo.
- **Ridurre il carico sul server**: a parità di risorse si potranno gestire molti più utenti contemporanei.
- **Migliorare la sicurezza**: sistema di identificazione delle minacce, bot e malware per bloccare gli attacchi prima che raggiungano il server.
- **Protezione dagli attacchi DDoS**: la CDN offre un'enorme banda disponibile per resistere anche ad attacchi massicci.

CONCLUSIONI

Cosa abbiamo imparato

1. Sicurezza dell’hosting: server hardening, backup, firewall, scansioni, CDN.
2. Sicurezza di WordPress: aggiornamenti costanti, 2FA, HTTPS, protezione del database, file, directory, area admin e file wp-config.php.
3. 10 attacchi frequenti: backdoor, pharma hacks, brute-force, redirect malevoli, XSS, DoS, phishing, mailbombing, defacement, php.mailers.
4. Come difendersi dagli attacchi: backup, check regolari, aggiornamenti, scansioni, file protection, monitoraggio, indicizzazione.
5. Cloudflare: sito più veloce, server meno carico, protezione attacchi DDoS.

DOMANDE?


THANK YOU

Visita il nostro sito:
www.shellrent.com