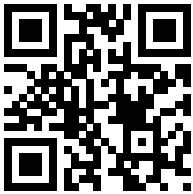
La Guida Definitiva alla Sicurezza dei Siti dei Clienti

KINSTA



Per la versione sempre aggiornata,
scansiona il codice QR qui sopra o vai su
kinsta.com/it/ebooks

Pubblicato da Kinsta

La Guida Definitiva alla Sicurezza dei Siti dei Clienti

Indice

La Guida Definitiva alla Sicurezza dei Siti dei Clienti

Secondo internet live stats, ogni giorno vengono hackerati oltre 100.000 siti web. 😲 Questo è il motivo per cui è così importante prendersi un po' di tempo per leggere le raccomandazioni che seguono in cui spieghiamo come rafforzare la sicurezza di WordPress.

E per quel che riguarda la sicurezza di WordPress, c'è molto di più della semplice chiusura dell'accesso al vostro sito, anche se di seguito vi daremo i nostri migliori consigli anche su questo argomento.

Investire in un Hosting WordPress Sicuro

Iniziamo con la sicurezza a livello di server, della quale è responsabile il vostro host WordPress. È molto importante che, quando spostate i siti dei vostri clienti, scegliate per la vostra azienda un host di cui potete fidarvi.

Se ospitate WordPress sul vostro VPS, allora dovete avere le conoscenze tecniche per fare queste cose da soli. Ma, ad essere onesti, cercare di essere un sysadmin per risparmiare 20 dollari al mese non è un modo efficace di gestire un business.

La messa in sicurezza del server è la chiave per mantenere un ambiente WordPress completamente al sicuro. Sono necessarie misure di sicurezza hardware e software a più livelli per garantire che l'infrastruttura IT che ospita i siti WordPress sia in grado di difendersi da sofisticate minacce, sia fisiche che virtuali.

Per questo motivo, i server che ospitano WordPress dovrebbero essere aggiornati con il sistema operativo e il software (di sicurezza) più recenti, nonché essere accuratamente testati e scansionati alla ricerca di vulnerabilità e malware.

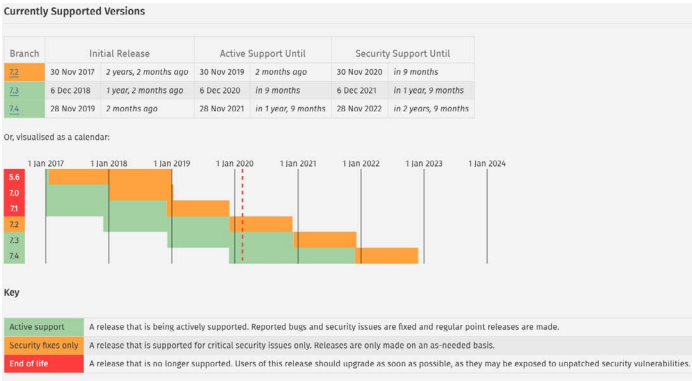
Dovrebbero essere presenti anche firewall e sistemi di rilevamento delle intrusioni a livello di server, per mantenere i siti dei vostri clienti ben protetti anche durante le fasi di installazione di WordPress e di costruzione dei siti web. Tuttavia, tutti i software installati sulla macchina destinati a proteggere i contenuti di WordPress dovrebbero essere compatibili con i più recenti sistemi di gestione dei database per mantenere prestazioni ottimali. Il server dovrebbe anche essere configurato in modo da utilizzare protocolli di rete sicuri e protocolli di crittografia per il trasferimento di file (come SFTP invece di FTP), per nascondere i contenuti sensibili ad intrusi malintenzionati.

Per garantire un hosting WordPress sicuro, qui da Kinsta utilizziamo Google Cloud Platform per tutti i nostri clienti. La sicurezza è integrata nella nostra architettura fin dall'inizio e questo garantisce maggiore sicurezza rispetto ad altre soluzioni oggi disponibili.

Utilizzare l'Ultima Versione di PHP

PHP è la spina dorsale di qualsiasi sito WordPress, quindi è molto importante assicurarsi che i siti dei vostri clienti utilizzino l'ultima versione presente sul vostro server. Dopo il suo rilascio, ogni major release di PHP è in genere pienamente supportata per due anni.

Durante questo periodo, i bug e i problemi di sicurezza vengono risolti e corretti regolarmente con delle patch. Oggi, chiunque abbia in esecuzione la versione di PHP 7.1 o inferiore non ha più supporto per la sicurezza ed è esposto a vulnerabilità non coperte da patch.



Currently Supported Versions

Branch	Initial Release		Active Support Until		Security Support Until	
7.2	30 Nov 2017	*2 years, 2 months ago*	30 Nov 2019	*2 months ago*	30 Nov 2020	*in 9 months*
7.3	6 Dec 2018	*1 year, 2 months ago*	6 Dec 2020	*in 9 months*	6 Dec 2021	*in 1 year, 9 months*
7.4	28 Nov 2019	*2 months ago*	28 Nov 2021	*in 1 year, 9 months*	28 Nov 2022	*in 2 years, 9 months*

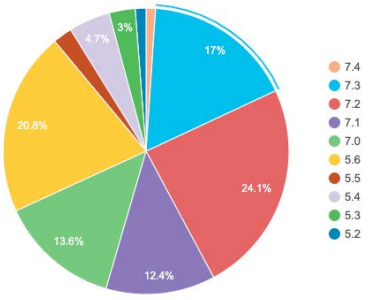
Or, visualised as a calendar:

Key

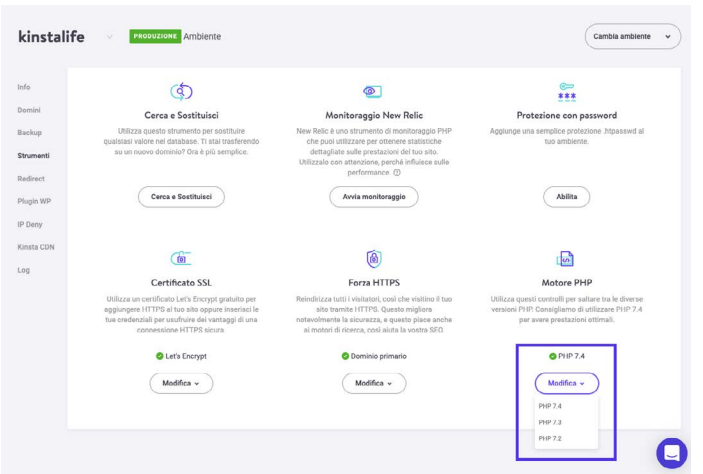
Active support	A release that is being actively supported. Reported bugs and security issues are fixed and regular point releases are made.
Security fixes only	A release that is supported for critical security issues only. Releases are only made on an as-needed basis.
End of life	A release that is no longer supported. Users of this release should upgrade as soon as possible, as they may be exposed to unpatched security vulnerabilities.

E indovinate un po'? Secondo la pagina ufficiale di WordPress Stats, circa il 34% degli utenti di WordPress è ancora su PHP 5.6 o inferiore, il che significa che più di un terzo degli utenti utilizza attualmente versioni di PHP non più supportate. È spaventoso!

Versioni di PHP



Qui da Kinsta consigliamo di utilizzare solo versioni stabili e supportate di PHP, tra cui 7.2, 7.3 e 7.4. Le versioni 5.6, 7.0 e 7.1 di PHP sono state gradualmente dismesse. È anche possibile passare da una versione di PHP all'altra con il clic di un pulsante, all'interno del cruscotto di MyKinsta.



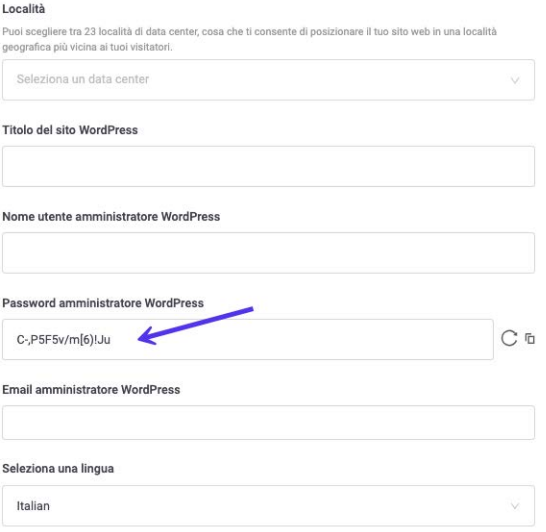
Se volete provarlo voi stessi, andate su demo.kinsta.com! 

Utilizzare Nome Utente e Password Intelligenti

Sorprendentemente, uno dei modi migliori per rafforzare la sicurezza di WordPress è semplicemente quello di utilizzare nomi utente e password intelligenti. Sembra abbastanza semplice, vero? Beh, date un'occhiata all'elenco annuale di SplashData delle password più popolari rubate nel corso del 2019 (ordinate in base alla popolarità).

- 123456
- 123456789
- qwerty
- password
- 1234567
- 12345678
- 12345
- iloveyou
- 111111
- 123123

La password più popolare è "123456". Questo è uno dei motivi per cui qui da Kinsta, sulle nuove installazioni di WordPress, forziamo l'utilizzo di una password complessa da utilizzare ad ogni accesso a wp-login da parte dei vostri clienti (come si vede qui sotto a proposito della nostra procedura di installazione ad solo clic). Questo non è facoltativo.



Date un'occhiata a questa funzionalità con la demo di MyKinsta.

La funzione wp_hash_password del core di WordPress utilizza il framework di hashing delle password phpass e otto passaggi di hashing basati su MD5. E, per quanto riguarda l'installazione di WordPress, non dovreste mai utilizzare il nome utente predefinito "admin" sui siti dei vostri clienti, ma piuttosto creare nomi utente WordPress unici per i loro account di amministratori.

È inoltre importante utilizzare password diverse per il sito di ogni cliente. Il modo migliore per memorizzarle è in locale, in un database criptato sul vostro computer.

Un ottimo strumento gratuito a questo scopo è KeePass. Se non volete seguire questa strada, ci sono anche gestori di password online come 1Password o LastPass.

Utilizzare Sempre l'Ultima Versione di WordPress, dei Temi e dei Plugin

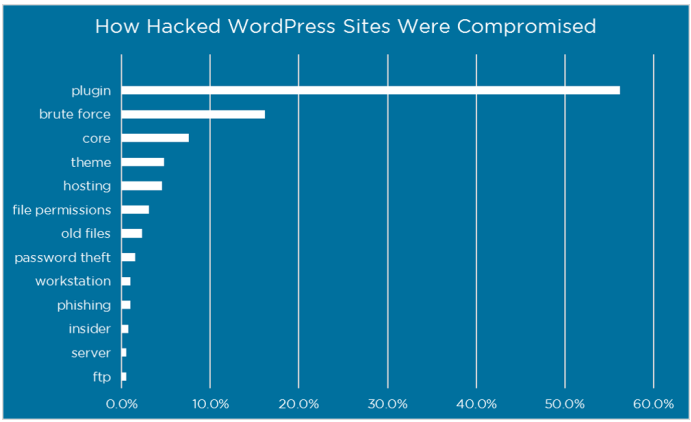
Un altro modo importante per rafforzare la sicurezza dei siti dei vostri clienti è tenerli sempre aggiornati. Questo riguarda sia il core di WordPress, che i plugin e i temi. Questi sono aggiornati per delle buone ragioni, e molte volte queste riguardano miglioramenti della sicurezza e correzioni di bug.

Sfortunatamente, milioni di aziende in rete utilizzano versioni obsolete del software e dei plugin di WordPress e credono comunque di essere sulla strada giusta per il successo del loro business. Hanno sempre una buona ragione per non aggiornare, come "il sito si romperà" o "le modifiche al core saranno sovrascritte" o "il plugin X non funzionerà" oppure, semplicemente, "non hanno bisogno delle nuove funzionalità".

In realtà, i siti web si rompono soprattutto a causa di bug nelle vecchie versioni di WordPress. Le modifiche dirette al Core non sono mai consigliate dal team di WordPress e da sviluppatori esperti che ne comprendono i rischi. E gli aggiornamenti di WordPress

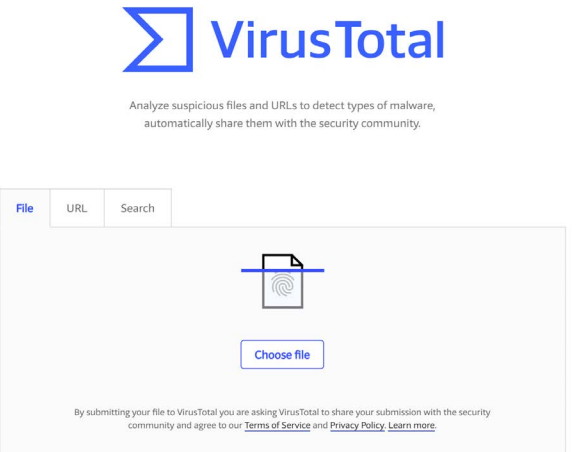
riguardano per lo più patch di sicurezza indispensabili, oltre alle funzionalità aggiuntive necessarie per eseguire gli ultimi plugin.

Sapevate che è stato segnalato che le vulnerabilità dei plugin rappresentano il 55,9% dei punti di ingresso noti per gli hacker? Questo è quanto ha scoperto WordFence in uno studio in cui ha intervistato oltre 1.000 proprietari di siti WordPress che sono stati vittime di attacchi. Aggiornando i plugin è possibile garantire al meglio di non essere tra queste vittime.



Raccomandiamo anche di installare solo plugin affidabili per i vostri clienti. Le categorie “featured” e “popular” della repository di WordPress possono essere un buon punto di partenza. Oppure scaricateli direttamente dal sito web dello sviluppatore. Sconsigliamo vivamente di utilizzare plugin e temi di WordPress annullati.

Potete utilizzare uno strumento online come VirusTotal per effettuare la scansione dei file di un plugin o di un tema, per vedere se viene rilevato un qualsiasi tipo di malware.



In giro ci sono anche molte risorse che possono aiutarvi a stare al passo con gli ultimi aggiornamenti per la sicurezza di WordPress e con le vulnerabilità rilevate. Qui sotto ne segnaliamo alcune:

- WP Security Blogger: Una fantastica risorsa che aggrega oltre 20 feed sulla sicurezza.
- WPScan Vulnerability Database: Cataloga oltre 10.000 vulnerabilità del Core, dei Temi e dei Plugin di WordPress.
- ThreatPress: Database aggiornato quotidianamente di vulnerabilità dei temi, dei plugin e del core di WordPress.
- Official WordPress Security Archive

Bloccare l'Accesso al Pannello di Amministrazione di WordPress

A volte, la popolare strategia di security by obscurity di WordPress è adeguatamente efficace per un business online e per un sito WordPress nella media. Se si rende più difficile per gli hacker trovare determinate backdoor, allora è meno probabile che si venga attaccati. Bloccare l 'accesso all'area di amministrazione dei siti WordPress e alla pagina di login dei vostri clienti è un buon modo per rafforzare la sicurezza. Per farlo, ci sono due ottimi metodi: prima di tutto cambiando l'URL di login predefinito di wp-admin, poi limitando anche i tentativi di accesso.

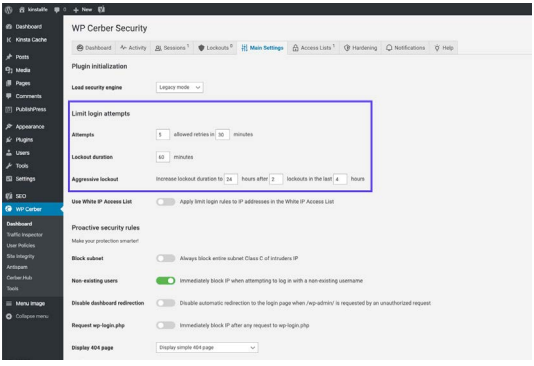
Come Cambiare l'URL di Accesso a WordPress

Di default, l'URL di accesso del vostro sito WordPress è domain.com/wp-admin. Uno dei problemi qui è che tutti i bot, gli hacker e gli script in circolazione lo sanno. Cambiando l'URL potete esporvi di meno e proteggervi meglio contro gli attacchi brute force. Questa non è una soluzione per tutto, è semplicemente un piccolo trucco che può sicuramente contribuire a proteggervi.

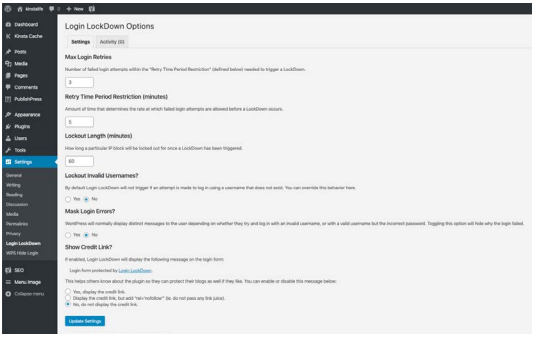
Per modificare l'URL di login di WordPress, consigliamo di utilizzare il plugin gratuito WPS Hide login. Ricordatevi solo di scegliere qualcosa di unico, che non sia già presente in una lista che potrebbe essere scansionata da un bot o uno script.

Come Limitare i Tentativi di Accesso

Sebbene la soluzione descritta di cambiare l'URL di accesso al pannello di amministrazione può aiutarvi ad eliminare la maggior parte dei tentativi di login non autorizzati, anche l'impostazione di un limite può essere una misura molto efficace. Il plugin gratuito Cerber Limit Login Attempts è un'ottima soluzione per impostare facilmente la durata del blocco, il numero de tentativi di login, le whitelist e le blacklist degli IP.



Se siete alla ricerca di una soluzione più semplice per la sicurezza di WordPress, un'ottima alternativa è il plugin gratuito Login Lockdown.

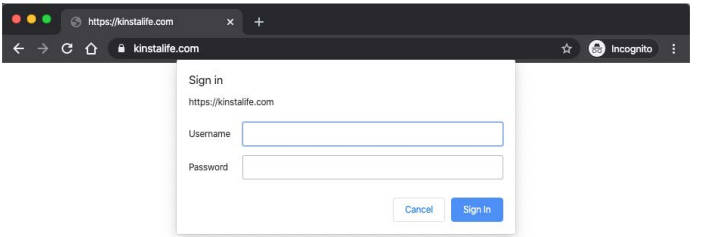


Login LockDown registra l'indirizzo IP e il timestamp di ogni tentativo di accesso fallito. Se viene rilevato più di un certo numero di tentativi in un breve periodo di tempo dallo stesso intervallo di IP, allora la funzione di login viene disabilitata per tutte le richieste successive provenienti dallo stesso intervallo. Ed è totalmente compatibile con il plugin WPS Hide login di cui abbiamo parlato in precedenza.

Se spostate il sito dei vostri clienti su Kinsta, non sarà necessario installare alcun plugin aggiuntivo, in quanto la nostra piattaforma limita e blocca automaticamente i tentativi di accesso malevoli.

Come Aggiungere l'Autenticazione HTTP di Base (protezione htpasswd)

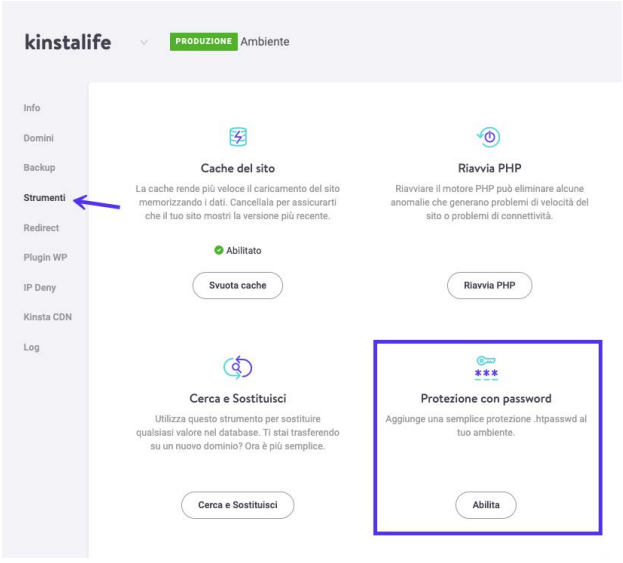
Un altro modo per bloccare l'accesso al pannello di amministrazione è aggiungere l'autenticazione HTTP. Questa richiede l'inserimento di uno username e una password prima di poter accedere alla pagina di login di WordPress.



Date un'occhiata a questa funzionalità con la demo di MyKinsta.

Importante: in genere questa soluzione non dovrebbe essere utilizzata sui siti di eCommerce o sui siti di affiliazione. Ma può offrire un modo molto efficace per evitare che i bot raggiungano il vostro sito.

Se i siti dei vostri clienti sono ospitati su Kinsta, potete utilizzare il nostro semplice strumento di protezione con password (htpasswd) presente nel cruscotto di MyKinsta (potete vederlo in azione sull'account demo gratuito di MyKinsta). Potete trovarlo nella sezione "Strumenti" del vostro sito. Basta cliccare su "Abilita", scegliere un nome utente e una password e il gioco è fatto!



Date un'occhiata a questa funzionalità con la demo di MyKinsta.

Una volta attivata la protezione con password, per accedere ad ognuno dei siti WordPress sarà richiesta autenticazione. Potete modificare le credenziali in qualsiasi momento o disabilitare la protezione quando non ne avete più bisogno.

Sfruttare l'Autenticazione a Due Fattori (2FA)

L'autenticazione a due fattori comporta una procedura in due fasi in cui non solo è necessaria la password per effettuare il login, ma è anche previsto un secondo metodo di autenticazione. Nella maggior parte dei casi, questa soluzione è efficace al 100% nel prevenire attacchi di forza bruta ai siti WordPress dei vostri clienti.

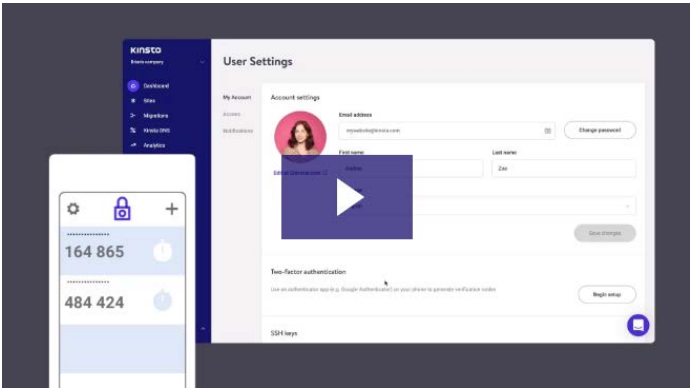
L'autenticazione a due fattori per i siti dei clienti si divide in due parti.

La prima riguarda il vostro account e/o cruscotto fornito dal vostro provider di web hosting. Se qualcuno riesce ad accedervi, potrebbe cambiare tutte le password dei siti dei vostri clienti, cancellare i loro siti web, modificare i record DNS, e fare ogni sorta di orribili cose. Noi di Kinsta utilizziamo la 2 FA basata su Authenticator per il vostro cruscotto MyKinsta perché:

- La 2FA basata su Authenticator è più sicura della 2FA basata su SMS, dato che non è legata al vostro numero di cellulare e non si affida alla tradizionale tecnologia degli SMS. Questo rende la 2FA basata su Authenticator resistente alle tecniche di scambio SIM.

- La 2FA basata su Authenticator può essere utilizzata, per maggiore comodità, con le applicazioni di gestione delle password come 1Password. Aggiungendo i dati della 2FA a un gestore di password, non sarà necessario affidarsi a un dispositivo esterno per accedere a MyKinsta.

Ecco quanto è semplice abilitare la 2FA:



La seconda parte dell'autenticazione a due fattori riguarda le installazioni WordPress dei vostri clienti. Per queste ultime ci sono alcuni plugin che potreste provare e consigliare ai vostri clienti:

- Duo Two-Factor Authentication
- Google Authenticator
- Two Factor Authentication

Dopo aver installato e configurato uno di questi plugin sul sito di un cliente, normalmente verrà aggiunto un nuovo campo sulla loro pagina di login di WordPress per inserire il codice di sicurezza. Oppure, con il plugin Duo, prima di tutto effettueranno il login

con le loro credenziali e poi dovranno scegliere un metodo di autenticazione, come Duo Push, chiamata, o passcode.

Utilizzare HTTPS per le Connessioni Criptate - Certificato SSL

Un modo per rafforzare la sicurezza di WordPress spesso trascurato è l'installazione di un certificato SSL e l'esecuzione dei siti su HTTPS. HTTPS (Hypertext Transfer Protocol Secure) è un meccanismo che permette a qualsiasi browser o applicazione web di connettersi in modo sicuro a un sito web. Un grosso equivoco è che, se i siti dei clienti non accettano carte di credito, allora non hanno bisogno di SSL.

Bene, lasciateci esporre alcune ragioni per cui HTTPS è importante al di là del solo eCommerce. Molti host, tra cui Kinsta, offrono certificati SSL gratuiti con Let's Encrypt.

6 Ragioni Determinanti per cui HTTPS è Importante al di là del Solo eCommerce

1. Sicurezza Aggiuntiva
Quanto sono importanti i dati di login dei vostri clienti? Beh, dovreste sapere che, ogni volta che un utente effettua il login, queste informazioni vengono trasmesse al server in chiaro. HTTPS è assolutamente vitale per mantenere una connessione sicura tra un sito web e un browser. In questo modo si può evitare che gli hacker e/o un soggetto intermedio possano accedere ai siti dei vostri clienti.

2. SEO
Google ha annunciato ufficialmente che HTTPS è un fattore di ranking. Dato che la maggior parte dei vostri clienti probabilmente sfrutterebbe ogni possibile vantaggio della SEO e delle SERP per battere i propri concorrenti, non c'è da stupirsi.

3. Fiducia e Credibilità
Secondo un sondaggio di GlobalSign, il 28,9% dei visitatori cerca il lucchetto verde nella barra degli indirizzi del proprio browser. E il 77% è preoccupato che i propri dati possano essere intercettati online o utilizzati in modo improprio. Vedendo quel lucchetto verde, i clienti saranno immediatamente più tranquilli sapendo che i loro dati sono più sicuri.

4. Dati di Referral
Molti non si rendono conto che i dati di referral da HTTPS a HTTP sono bloccati in Google Analytics. Quindi cosa succede ai dati? Beh, la maggior parte è concentrata solo nella sezione "traffico diretto". Se qualcuno passa da HTTP a HTTPS, il referrer viene comunque passato.

5. Avvertenze su Chrome
A partire dal 24 luglio 2018, le versioni di Chrome 68 e superiori hanno iniziato a contrassegnare tutti i siti non HTTPS come "Not Secure" e, a partire dal 2020, il popolare browser ha iniziato a considerare deprecato il supporto delle versioni TLS legacy. Google sta rendendo molto più chiaro ai visitatori che un sito WordPress potrebbe non essere accessibile su una connessione sicura. Ecco perché HTTPS è assolutamente importante!

6. Prestazioni
Grazie ad un protocollo chiamato HTTP/2, molte volte, coloro che hanno siti ottimizzati su HTTPS possono anche registrare miglioramenti della velocità. Per avere il supporto dei browser, HTTP/2 richiede HTTPS. Il miglioramento delle prestazioni è dovuto a diverse ragioni, come il fatto che HTTP/2 è in grado di supportare meglio il multiplexing, il parallelismo, la compressione HPACK con la codifica Huffman, l'estensione ALPN e il server push.

E con TLS 1.3, le connessioni HTTPS sono ancora più veloci. Kinsta supporta TLS 1.3 su tutti i server e sul CDN di Kinsta.

Leggete la nostra guida approfondita alla migrazione di WordPress su HTTPS per cominciare subito e scoprite ancora di più nel nostro confronto tra TLS e SSL.

Disabilitare XML-RPC

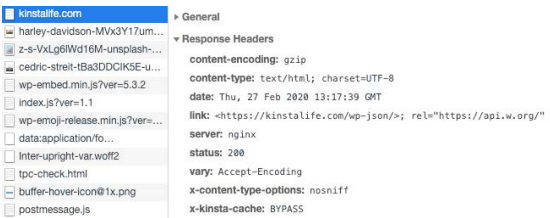
Negli ultimi anni, XML-RPC è diventato un bersaglio sempre più grande per gli attacchi di forza bruta. Alcuni plugin di WordPress come Jetpack si affidano a XML-RPC, ma la maggior parte di noi non ne avrà bisogno e potrebbe essere utile disabilitarne l'accesso.

Se siete clienti di Kinsta, non dovete preoccuparvi di questo, perché abbiamo implementato misure attive e passive per fermare gli attacchi e le azioni malevoli nel loro corso. In particolare, quando viene rilevato un attacco tramite XML-RPC, viene aggiunto un piccolo frammento di codice nel file di configurazione di Nginx per impedire che generi un errore 403.

Aggiungere i Più Recenti Header HTTP di Sicurezza

Un altro passo da compiere per aumentare la sicurezza dei siti WordPress dei vostri clienti è sfruttare gli header HTTP di sicurezza. Questi sono di solito configurati a livello di server e dicono al browser come comportarsi quando gestisce il contenuto dei siti dei vostri clienti. Ci sono molte intestazioni HTTP di sicurezza, ma quelle riportate di seguito sono solitamente le più rilevanti.

- Content-Security Policy
- X-XSS-Protection
- Strict-Transport-Security
- X-Frame-Options
- Public-Key-Pins
- X-Content-Type



Potete verificare le intestazioni attive su una qualsiasi installazione di WordPress avviando i devtools di Chrome e guardando gli header della risposta iniziale del sito.

Ecco un esempio da kinstalife.com (un sito demo). Potete vedere che utilizziamo l'intestazione x- Per i siti dei clienti, come nell'esempio mostrato, x-content-type-options è sempre aggiunto

di default, mentre x-frame-options e strict-transport-security sono impostati solo se è necessario.

Se avete bisogno di effettuare una scansione dei siti dei vostri clienti, potete farlo con lo strumento gratuito securityheaders.io di Scott Helme.

È anche importante ricordare che, quando si implementano gli header HTTP di sicurezza, questi potrebbero influenzare i sottodomini di WordPress. Ad esempio, se aggiungete l'intestazione Content Security Policy e limitate l'accesso per dominio, dovrete aggiungere anche i vostri sottodomini. Se non siete sicuri del modo in cui vanno implementati, potete sempre chiedere aiuto al vostro host.

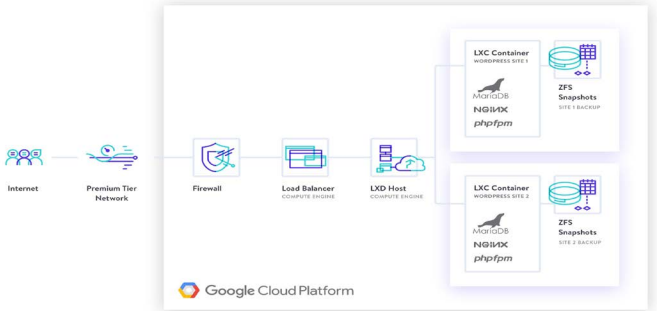
Utilizzare i Plugin per la Sicurezza di WordPress

In giro ci sono un sacco di sviluppatori in gamba e aziende di livello che forniscono ottime soluzioni per aiutarvi a proteggere meglio il vostro sito WordPress. Tra quelle maggiormente degne di nota ricordiamo:

- Sucuri Security
- iThemes Security
- Wordfence Security
- WP Security Audit Log
- WP fail2ban
- All In One WP Security & Firewall
- SecuPress
- BulletProof Security
- VaultPress
- Google Authenticator – Two Factor Authentication

- Security Ninja
- Defender
- Astra Web Security
- Shield Security
- Hide my WP
- WebARX

Kinsta dispone di firewall hardware, sicurezza attiva e passiva, controlli di uptime al minuto e decine di altre funzionalità avanzate per impedire agli aggressori di accedere ai vostri dati. Se, nonostante i nostri sforzi, il vostro sito dovesse essere compromesso, allora lo ripareremo gratuitamente.

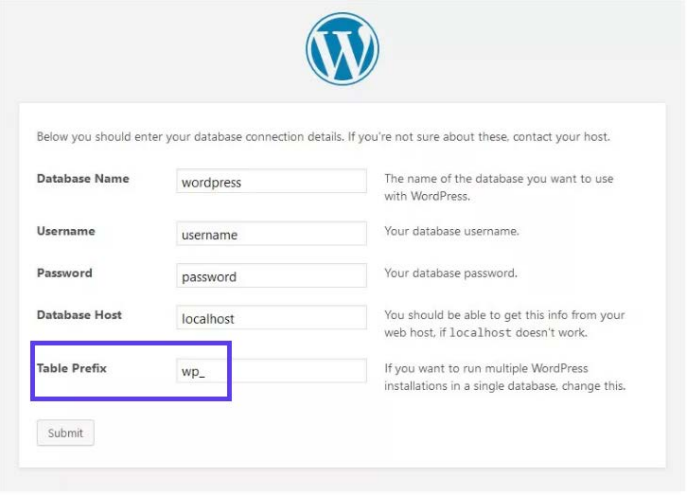


Una funzionalità molto importante offerta da molti plugin di sicurezza è una utility di checksum (“somma di controllo”). Significa che ogni installazione WordPress dei vostri clienti viene ispezionata alla ricerca di modifiche sui file del core forniti da WordPress.org (tramite l’API). Qualsiasi cambiamento o modifica a questi file potrebbe indicare la presenza di un hack.

Per eseguire un vostro checksum, potete utilizzare anche WP-CLI. Date un'occhiata a questi ulteriori plugin di sicurezza di WordPress che possono aiutarvi a bloccare i malintenzionati.

Rafforzare la Sicurezza del Database

Ci sono diversi modi per aumentare la sicurezza del database di WordPress. Il primo è quello di utilizzare per il database un nome intelligente. Cambiare il nome del database, scegliendo un nome più oscuro, ci aiuta a proteggere il sito, rendendo più difficile per gli hacker identificare il database e accedere ai dati.



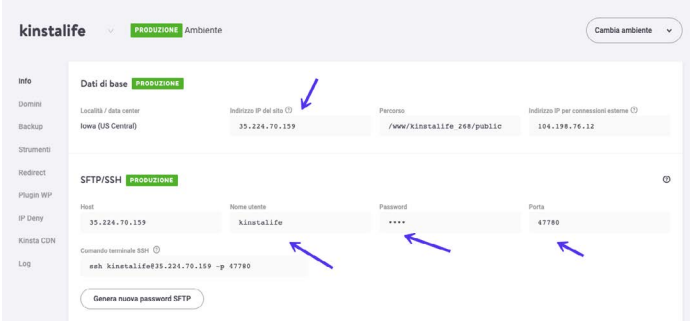
Una seconda raccomandazione è quella di utilizzare un diverso prefisso per le tabelle del database. Quando installate WordPress, vi viene richiesto di specificare un prefisso per le tabelle. Di default, WordPress utilizza wp_. Cambiare il valore predefinito, scegliendo

qualcosa come 39xw_, può essere molto più sicuro.

Se siete clienti di Kinsta e avete da noi tutti i siti dei vostri clienti, questo passaggio non è necessario. Gli accessi al sito e al database sono già messi in sicurezza!

Utilizzare Sempre Connessioni Sicure

Non potremo mai sottolineare abbastanza quanto sia importante utilizzare connessioni sicure! Assicuratevi che il vostro host WordPress stia prendendo precauzioni, ad esempio offrendo SFTP o SSH. SFTP, o Secure File Transfer Protocol (noto anche come protocollo di trasferimento file SSH), è un protocollo di rete utilizzato per il trasferimento di file. Si tratta di un metodo più sicuro rispetto all'FTP standard.



Date un'occhiata a questa funzionalità con la demo di MyKinsta.

Da Kinsta supportiamo solo connessioni SFTP per garantire che i vostri dati rimangano sicuri e criptati. Inoltre, la maggior parte degli host WordPress utilizza per SFTP la porta 22. Qui da Kinsta siamo un passo avanti e assegniamo ad ogni sito una porta randomizzata che potete trovare nella vostra dashboard di MyKinsta.

Controllare i Permessi dei File e del Server

I permessi sui file, sia sulle installazioni dei vostri clienti che sui server web, sono cruciali per rafforzare la sicurezza di questi ambienti. Se i permessi sono troppo generici, qualcuno potrebbe facilmente avere accesso al sito e creare scompiglio. D'altra parte, se i vostri permessi sono troppo rigidi, questo potrebbe compromettere la funzionalità del sito. Quindi è importante avere i permessi corretti su tutta la linea.

Per effettuare la scansione dei permessi sui siti WordPress dei vostri clienti potete utilizzare un plugin gratuito come iThemes Security.

File Permissions

Reload File Permissions Details

Relative Path	Suggestion	Value	Result	Status
/	755	755	OK	
wp-includes	755	755	OK	
wp-admin	755	755	OK	
wp-admin/js	755	755	OK	
wp-content	755	755	OK	
wp-content/themes	755	755	OK	
wp-content/plugins	755	755	OK	
wp-content/uploads	755	755	OK	
wp-config.php	444	644	WARNING	
nginx.conf	444	644	WARNING	
Relative Path	Suggestion	Value	Result	Status

Ecco alcune comuni raccomandazioni relative ai permessi sui file e sulle cartelle di WordPress:

- Tutti i file dovrebbero essere su 644 o 640. Eccezione: wp-config.php dovrebbe essere su 440 o 400 per evitare che possa essere letto da altri utenti sul server.
- Tutte le directory dovrebbero essere su 755 o 750.
- Nessuna directory dovrebbe mai essere su 777, neanche le directory di upload.

Per una spiegazione più approfondita di questo argomento, si legga l'articolo del Codex di WordPress sulla modifica delle autorizzazioni dei file.

Protezione DDoS

Il DDoS è un tipo di attacco DOS in cui vengono utilizzati più sistemi per colpire un singolo sistema con un attacco Denial of Service (DoS). Gli attacchi DDoS non sono una novità - secondo Britannica il primo caso documentato risale all'inizio del 2000. Diversamente da quando qualcuno porta un attacco al vostro sito, gli attacchi di questo tipo normalmente non danneggiano il sito, semplicemente lo mandano giù per qualche ora o per qualche giorno.

Cosa potete fare per proteggervi? Uno dei migliori consigli è quello di utilizzare un servizio di sicurezza di terze parti affidabile come Cloudflare o Sucuri.

I loro sistemi di protezione avanzata DDoS possono mitigare gli attacchi DDoS di qualsiasi tipo e volume, compresi gli attacchi che prendono di mira i protocolli UDP e ICMP, nonché gli attacchi SYN/ACK, l'amplificazione del DNS e gli attacchi Layer 7. Altri vantaggi includono l'inserimento di un proxy che aiuta a nascondere l'indirizzo IP di origine, anche se questo non è a prova di proiettile.

Non trascurate il provider utilizzato dal vostro web host, perché anche questo è molto importante.

Da Kinsta abbiamo in funzione il firewall hardware di Google Cloud Platform, con restrizioni software molto severe per proteggere i siti dei vostri clienti. Google Cloud Platform Firewall dispone anche di un software per r ilevare gli attacchi DDoS nel momento in cui si verificano.

Ciò significa che voi e i vostri clienti potrete beneficiare di un modello di sicurezza che è stato sviluppato nel corso di 15 anni e che attualmente protegge prodotti e servizi come Gmail, Search, ecc. Google attualmente impiega più di 500 professionisti della sicurezza a tempo pieno.

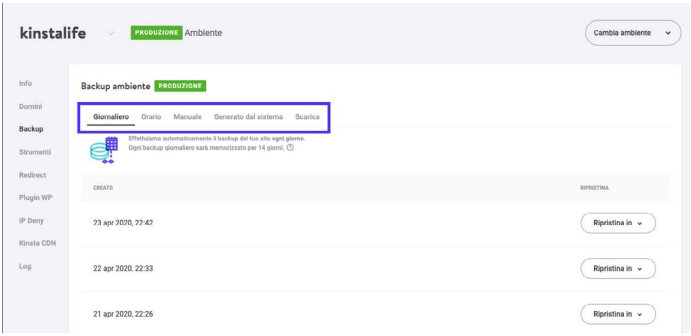
Al top di Google Cloud Platform, utilizziamo anche container Linux (LXC e LXD per orchestrarli), il che ci permette di isolare completamente non solo ogni account, ma anche ogni singolo sito WordPress.

Le cose vanno male lo stesso? Kinsta fornisce la riparazione gratuita degli hack e la rimozione del malware. Se uno dei siti dei vostri clienti è infetto, il nostro team di supporto farà tutto il necessario per ripulirlo.

Leggete più approfonditamente quanto prendiamo sul serio la sicurezza da Kinsta!

Fare Sempre dei Backup

Non importa quanto sia sicuro il vostro sito, non sarà mai sicuro al 100%. Ecco perché dovete avere dei backup nel caso succeda il peggio. I backup sono l'unica cosa di cui tutti sanno di aver bisogno, ma che non sempre prendono. La maggior parte delle raccomandazioni qui delineate sono misure di sicurezza che potete adottare per proteggere meglio i siti dei vostri clienti e la vostra attività.



Date un'occhiata a questa funzionalità con la demo di MyKinsta.

La maggior parte dei provider di hosting WordPress gestito adesso fornisce backup. Kinsta ha cinque diversi tipi di backup:

- Giornaliero: Kinsta crea backup automatici di tutti i siti dei vostri clienti ogni 24 ore, in modo che possiate dormire sonno tranquilli.
- Orario: Se avete bisogno di un programma di backup più frequente, potete attivare backup automatici di 6 ore o orari per qualsiasi sito target lo richieda (questo servizio va ad aggiungersi al vostro piano mensile).
- Manuale: se i backup automatici non sono sufficienti, è possibile creare backup manuali per ogni sito che si ha in gestione e avere questa copia aggiuntiva a disposizione per 14 giorni o più, in base al vostro piano corrente.

- Generati dal sistema: Kinsta attiverà i backup generati dal sistema prima dell'esecuzione di azioni critiche come l'utilizzo dello strumento di ricerca e sostituzione in MyKinsta, il passaggio da ambiente di staging ad ambiente live e il ripristino di un backup nel vostro ambiente live.
- Archivio scaricabile: se tutto questo non bastasse, una volta alla settimana potreste scaricare un file zip di ogni sito con i file del sito web e un file SQL con il contenuto del database.

Le opzioni di backup non vengono da sole, in quanto Kinsta consente di ripristinare facilmente qualsiasi sito con un solo clic. È comodo, vero?

Provate gratuitamente quanto sia facile creare backup con MyKinsta! 

Se il vostro host non dispone di backup, ci sono diversi plugin di WordPress molto popolari che potete utilizzare per automatizzare la procedura di backup.

Plugin per il Backup di WordPress

I plugin per il backup di WordPress consentono di prelevare i backup via FTP, oppure si integrano con un'origine di archiviazione esterna come Amazon S3, Google Cloud Storage, Google Drive o Dropbox. Consigliamo vivamente di optare per una soluzione incrementale in modo da utilizzare meno risorse:

- Duplicator
- WP Time Capsule
- BackupBuddy

- UpdraftPlus
- BackUpWordPress
- BackWPup
- WP BackItUp

Kinsta non consente di installare plugin di backup non incrementale, dato che questi ultimi generano problemi di performance: gestiamo tutto questo per voi a livello di server, in modo da non rallentare i siti dei vostri clienti.

Riepilogo

La sicurezza è un gioco a livelli. Più riuscirete a sovrapporre nuovi livelli di sicurezza uno sull'altro, più i siti dei vostri clienti diventeranno sicuri. Si inizia utilizzando password intelligenti, e si continua mantenendo il core e i plugin aggiornati e seguendo le altre best practice relative alla sicurezza di cui abbiamo parlato.

Ma non è tutto quello che c'è da fare per ridurre le possibilità di trovarvi con i siti dei vostri clienti hackerati. Scegliendo un host WordPress gestito come Kinsta, la maggior parte delle misure di sicurezza sono curate al posto vostro, e questo vi permette di costruire una base solida, sicura e scalabile per garantire il futuro dei siti dei vostri clienti. E quello del vostro business.

Volete provare quanto sia facile gestire i siti dei vostri clienti su Kinsta?

Date un'occhiata a demo.mykinsta.com!


KINSTA