LA SICUREZZA È IMPORTANTE:

21 suggerimenti per rendere sicuro il tuo sito WordPress

SiteGround

INTRODUZIONE

INTRO

Ti stai domandando se WordPress sia sicuro? La risposta è sì. WordPress si avvale delle più recenti tecnologie di sicurezza. Inoltre, viene aggiornato continuamente con nuove versioni, che includono patch contro le vulnerabilità. Infine, WordPress viene monitorato e gestito da una vasta community di sviluppatori a cui la sicurezza sta profondamente a cuore.

Se WordPress è così sicuro, perché abbiamo preparato una guida per prevenire le attività di hacking? Perché, in realtà, la protezione del tuo sito web dovrebbe essere un'attività continua, che implica, tra le altre attività, la creazione di barriere contro gli aggressori, la prevenzione di guasti, il monitoraggio dei cambiamenti, l'opposizione a accessi malevoli, l'occultamento di informazioni sensibili.

WordPress è utilizzato in più del 30% dei siti web: proprio a causa della sua popolarità è un bersaglio dei criminali informatici. È anche una piattaforma in continuo sviluppo, aperta a modifiche e integrazioni con terze parti.

A SiteGround siamo consapevoli del fatto che il tuo sito web possa subire attacchi in svariati modi e quindi ci impegniamo ad aiutarti a proteggerlo. Leggi questa guida per ampliare le tue conoscenze sulla sicurezza web in WordPress, per implementare nuove misure per proteggere il tuo sito web e per spargere la voce tra i tuoi amici affinché anch'essi proteggano i loro siti web.

1

PROTEGGI I FILE E I DATABASE

1. PRIMA DI INSTALLARE WORDPRESS

Quando crei una nuova installazione di WordPress, dovresti sempre scegliere l'ultima versione stabile. Prima di installare WordPress, segui queste due semplici procedure di sicurezza web da eseguire all'interno del file wp-config.php:

- *Cambia il prefisso del database;*
- *Utilizza chiavi di autenticazione.*

Per impostazione predefinita, tutte le installazioni di WordPress utilizzano il prefisso **wp_** nel loro database. Ti consiglio di cambiare il prefisso di ogni sito web per prevenire possibili attacchi al database.

Per cambiare il prefisso della tabella WordPress, modifica la seguente riga nel file di configurazione wp-config.php sostituendo il prefisso predefinito con quello che desideri:

```
$table_prefix  = 'wp_';
```

Ad esempio:

```
$table_prefix  = 'nuovosito_wp_';
```

Inoltre, grazie a questa modifica, potrai avere diverse installazioni di WordPress nello stesso database, a patto di non ripetere il prefisso.

Se hai già installato il tuo sito web e non hai modificato il prefisso predefinito durante il processo di installazione, non è troppo tardi. Utilizza un plugin come Change Table Prefix per realizzare la modifica. È possibile anche cambiare il prefisso manualmente, ma non lo consiglio se non hai familiarità con il database.

WordPress utilizza chiavi segrete, chiamate Keys e Salt, memorizzate nel file wp-config.php: proteggono le sessioni aperte crittografando i dati della sessione nel cookie del browser. Prima di avviare l'installazione, dovresti generare le chiavi segrete.

Come per il prefisso del database, puoi cambiare in qualsiasi momento le chiavi segrete di un sito web esistente: ti consiglio di eseguire regolarmente questa operazione per invalidare le sessioni attive e costringere tutti gli utenti a eseguire nuovamente l'accesso.

Sebbene sia possibile generare manualmente le chiavi, ti consiglio di utilizzare il servizio WordPress ufficiale alla pagina **https://api.wordpress.org/secret-key/1.1/salt/** e sostituire le chiavi con quelle presenti nel tuo file wp-config.php.

Prima di passare al seguente suggerimento, vorrei darti un altro consiglio sulle chiavi segrete di WordPress per i siti web attivi. Nell'eventualità remota in cui tu debba negare qualsiasi tipo di accesso al pannello di amministrazione, perfino tramite le credenziali di accesso, puoi configurare l'invalidazione delle chiavi ogni microsecondo inserendo nel file wp-config.php quanto segue:

```
define('AUTH_KEY',                microtime());
define(''SECURE_AUTH_KEY',        microtime());
define('LOGGED_IN_KEY',           microtime());
define('NONCE_KEY',               microtime());
define('AUTH_SALT',               microtime());
define('SECURE_AUTH_SALT',        microtime());
define('LOGGED_IN_SALT',          microtime());
define('NONCE_SALT',              microtime());
```

Ricordati di aggiornare periodicamente queste chiavi come misura preventiva o per terminare le sessioni attive.

2. IN SEGUITO ALL'INSTALLAZIONE DI WORDPRESS

Una volta terminata l'installazione del tuo nuovo sito WordPress, dovresti eliminare il profilo di amministratore utilizzato durante l'installazione, creare un nuovo utente con autorizzazioni di amministratore e tutti gli account utente di cui hai bisogno.

Evita i nomi utente deboli come “admin” o “amministratore” (comuni in tutte le installazioni di WordPress) e ricorda di utilizzare una password complessa.

Disattiva le notifiche di pingback e trackback sul tuo pannello di amministrazione (Impostazioni > Commenti), in quanto potrebbero costituire un accesso per possibili attacchi DDoS (Distributed Denial of Service) sul tuo sito web.

Proteggi i file da attacchi e intrusioni aggiungendo le seguenti righe di codice nel file .htaccess, idealmente all'inizio del file presente nella cartella principale del tuo sito web:

```
#Nega elenco cartelle
Options -Indexes
#Blocca file sensibili
<files .htaccess>
Order allow,deny
Deny from all
</files>
<files wp-config.php>
Order allow,deny
Deny from all
</files>
```

Dovresti bloccare l'accesso a tutti i file non necessari creando un nuovo file .htaccess nella cartella /wp-admin e aggiungendo le seguenti righe di codice:

```
#Blocca file di installazione
<files install.php>
Order allow,deny
Deny from all
</files>
<files setup-config.php>
Order allow,deny
Deny from all
</files>
```

Ti consiglio di analizzare il file robots.txt, che si trova nella cartella principale del tuo sito web. Questo file indica ai bot di ricerca cosa dovrebbe e cosa non dovrebbe essere analizzato sul tuo sito web, quindi controlla che non mostri informazioni sensibili relative alla tua installazione di WordPress, ad esempio la tua cartella wp-admin.

3. MODIFICA LE AUTORIZZAZIONI PER FILE E CARTELLE

Assicurati che i file e le cartelle nella tua installazione WordPress possiedano le autorizzazioni appropriate per impedire agli aggressori di assumere il controllo del tuo sito web.

Puoi modificare le autorizzazioni tramite un client FTP o tramite il pannello di amministrazione fornito dal tuo servizio di hosting web. Con SiteGround, è facile modificare le autorizzazioni per file e cartelle utilizzando il tuo cPanel.

Vai a Strumenti WordPress > Set Strumenti WordPress > Seleziona l'installazione > Correggi i permessi.

- *Dovresti impostare su 755 le autorizzazioni per tutte le cartelle.*
- *Dovresti impostare su 644 le autorizzazioni per tutti i file.*

Per limitare ulteriormente l'accesso, dovresti proteggere i seguenti due file nella configurazione di WordPress come indicato:

- *File wp-config.php: imposta le autorizzazioni su 600*
- *File .htaccess: imposta le autorizzazioni su 604*

Queste autorizzazioni sono indicate come Visualizza, Scrivi ed Esegui, come specificato nei sistemi operativi Unix.

4. BLOCCA PHP NELLE CARTELLE

Sebbene le installazioni di WordPress, per impostazione predefinita, blocchino i caricamenti di file PHP attraverso il pannello di amministrazione, dovresti anche bloccare la possibilità di eseguire il codice PHP nella cartella. Inoltre, dovresti limitare l'esecuzione non necessaria di codice PHP in altre cartelle utilizzate da WordPress a cui non si dovrebbe accedere direttamente.

Crea un nuovo file .htaccess all'interno delle tue cartelle "/wp-content/uploads", "/wp-content/plugins" e "/wp-content/themes" e aggiungi le seguenti righe di codice per bloccare le esecuzioni PHP:

```
<Files *.php>
deny from all
</Files>
```

Nota: ogni volta che modifichi un file .htaccess, dovresti controllarlo nella tua installazione. Svuota la cache per verificare il corretto funzionamento delle regole aggiunte.

5. DISABILITA L'EDITING DEI FILE IN WORDPRESS

Questo procedura mira ad aggiungere un livello di sicurezza al pannello di amministrazione, in modo da prevenire intrusioni indesiderate e limitare gli errori commessi dagli utenti autorizzati.

Per disabilitare l'opzione di editing dei file nel pannello di amministrazione di WordPress, utilizza la seguente riga di codice nel file di configurazione wp-config.php:

```
define( 'DISALLOW_FILE_EDIT', true );
```

Questo codice equivale alla rimozione delle autorizzazioni "edit_themes", "edit_plugins" e "edit_files" per qualsiasi utente registrato sul sito web.

Puoi aggiungere un ulteriore livello di controllo per i siti web attivi se non desideri che gli utenti installino temi e plugin autonomamente. Inserisci il seguente codice al file di configurazione wp-config.php:

```
define( 'DISALLOW_FILE_MODS', true );
```

Ricordati di disattivare il comando modificando la direttiva su 'false' se devi eseguire attività sull'installazione di WordPress.

Tutte le modifiche sul file wp-config.php devono essere inserite sopra la seguente riga di codice:

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

6. UTILIZZA UN CDN COME DNS

Sebbene conosciamo già i vantaggi di un servizio di Content Delivery Network (CDN) per migliorare le prestazioni del tuo sito web, l'utilizzo di un CDN di tipo DNS (prima del tuo web server) può migliorare la sicurezza del tuo sito web nei seguenti tre modi::

- *Abilita un Firewall attivo che viene aggiornato continuamente contro comportamenti malevoli come connessioni massicce, porte di tracciamento,*
- *Impedisce gli attacchi di forza bruta utilizzando la rete di server distribuiti del provider, che riducono al minimo l'impatto, e applica regole di blocco per rilevare questo tipo di attacchi, di solito DoS o DDoS;*
- *Nasconde il vero IP del tuo server, impedendo gli attacchi diretti contro il tuo sito web grazie alla mascheratura dell'IP reale in cui è ospitato il tuo sito web.*

Consiglio di utilizzare CloudFlare come CDN per migliorare la sicurezza e le prestazioni del tuo sito web in WordPress. Tutti i piani di hosting di SiteGround includono un account CloudFlare gratuito.

7. EFFETTUA IL BACKUP DEL TUO SITO WEB

Anche se mi auguro che tu non debba mai arrivare a utilizzare questo suggerimento, è meglio prevenire che curare: di conseguenza ti consiglio di eseguire un backup completo del tuo sito web.

Raramente è necessario ripristinare un backup completo del sito web, ma se dovessi farlo, SiteGround ha uno strumento sviluppato internamente per eseguire backup e ripristinare facilmente il tuo sito web, indipendente dall'infrastruttura dei servizi web. Puoi dormire sonni tranquilli: saprai di avere copie dei tuoi file in caso di incidenti e di poter ripristinare il tuo sito web facilmente e rapidamente.

Ti consiglio di seguire la regola 3-2-1 come strategia per i backup contenenti dati importanti:

- *Conserva 3 backup;*
- *In 2 formati diversi (minimo);*
- *1 dei backup dovrebbe essere in una differente posizione fisica.*

In caso di emergenza, è inutile avere tutti i backup nello stesso formato o nella stessa posizione. Ricordati di generare sempre un nuovo backup dopo aver realizzato cambiamenti importanti alla tua installazione WordPress.

2

PROTEGGI L'ACCESSO E LE SESSIONI

8. ATTIVA E FORZA HTTPS

Il protocollo HTTPS crea una connessione sicura tra gli utenti e il server, eliminando possibili attacchi **Man-in-the-Middle (MITM)**. Questi attacchi si verificano quando un servizio intermedio altera o acquisisce informazioni scambiate tra due parti. Ecco perché utilizziamo la crittografia HTTPS per tutte le informazioni sensibili.

Per utilizzare il protocollo HTTPS sul tuo sito web, installa un certificato SSL sul tuo server web e modifica l'URL nel pannello di amministrazione.

Con SiteGround, tutti i piani di hosting includono i certificati SSL gratuiti Let's Encrypt che possono essere installati e configurati con uno strumento semplice all'interno del pannello di controllo nella sezione Sicurezza > Let's Encrypt.

Esistono diversi plugin di WordPress che forzano una connessione HTTPS su tutte le risorse del tuo sito web, per evitare avvisi o errori durante la visualizzazione di contenuti HTTP e HTTPS sulla stessa pagina.

Infine, dovrai forzare ogni nuova sessione nel pannello di amministrazione del tuo sito web affinché utilizzi il protocollo SSL. Dovrai inserire il seguente codice al file wp-config.php:

```
define('FORCE_SSL_LOGIN', true);
define('FORCE_SSL_ADMIN', true);
```

Nota: ricorda che è necessario disporre di un SSL attivo nell'installazione come, ad esempio, quello fornito da Let's Encrypt.

9. DISABILITA SUGGERIMENTI DI SESSIONE

Come accennato in precedenza, ma vale la pena ripeterlo, come tua prima priorità dovresti "regalare" meno informazioni possibili agli aggressori. Questo suggerimento ti aiuterà a ridurre al minimo i possibili accessi al tuo sito web disabilitando i suggerimenti dalla

pagina di login, che appaiono in maniera predefinita se il nome utente o la password non sono corretti:.

```
function no_wordpress_login_errors(){
return 'Grazie per il tentativo, ma questo sito web è protetto';
}
add_filter( 'login_errors', no_wordpress_login_errors );
```

Nota: è possibile personalizzare il messaggio.

10. SPOSTA L'ACCESSO AMMINISTRATORE DEL TUO SITO WEB

Non è di certo una sorpresa: molti attacchi a siti web si concentrano sulla pagina di accesso. Questo perché i bot sono programmati per riconoscere un'installazione di WordPress, aggiungere il percorso /wp-admin ed accedere così alla pagina di accesso, quindi modificandolo aggiungerai un ulteriore livello di difficoltà per gli aggressori.

Nel repository di WordPress sono presenti diversi plugin che consentono di modificare il percorso e la posizione della tua pagina di accesso, ad esempio **www.ilmiodominio.com/nuovopannelloadmin.**

Consiglio il plugin WPS Hide Login. Tuttavia, esistono altri plugin per questo scopo e perfino anche molti plugin di sicurezza includono questa funzionalità.

11. LIMITA I TENTATIVI DI ACCESSO

Puoi configurare il tuo sito web affinché blocchi l'accesso alla pagina di login per qualche minuto, qualche ora o per sempre nel caso un utente inserisse credenziali di accesso errate un determinato numero di volte. In questo modo i bot avranno vita più difficile per ottenere l'accesso tramite attacchi di forza bruta.

Generalmente, i plugin di sicurezza come Wordfence includono questa funzionalità, così come i seguenti plugin:

- *Limit Login Attempts (miniorange)*
- *Limit Login Attempts Reloaded*
- *Loginizer*

Anche alcuni plugin firewall includono questa funzionalità.

12. USA I PLUGIN FIREWALL

Un firewall è un software che fornisce un ulteriore livello di sicurezza ed è in grado di proteggere le connessioni web o l'installazione di WordPress rilevando e analizzando le connessioni in entrata. I plugin firewall sono molto efficaci e facili da gestire, poiché la configurazione avviene da un unico plugin.

Generalmente includono un firewall WAF (Web Application Firewall), uno strumento che analizza e blocca gli attacchi al sito web in tempo reale. SiteGround offre questo servizio di default per impostazione predefinita: analizziamo i tipi di connessione e blocchiamo i tentativi di attacco in modo completamente trasparente per i nostri clienti.

Alcuni di questi plugin sono:

- *Wordfence Security (attenzione alla funzionalità Live Traffic, che può causare il sovraccarico del server e lasciarti così senza servizio)*
- *All in one security and firewall*
- *iThemes Security (in precedenza Better WP Security)*

Le funzionalità di sicurezza variano in base al plugin, ma generalmente sono presenti:

- *Scansione di file per cercare modifiche, errori e virus*
- *Firewall WAF che rileva e blocca le visite dannose*
- *Visualizzazione del traffico in tempo reale*
- *Uno strumento per bloccare l'accesso al sito web tramite IP*
- *Captcha per la pagina di accesso di WordPress e una funzionalità che limita i tentativi di accesso*
- *Verifica della password*
- *Verifica a due fattori per accedere al pannello di amministrazione di WordPress*
- *Possibilità di bloccare Paesi specifici*
- *Uno strumento per verificare le autorizzazioni di file e cartelle*

13. UTILIZZA INTESTAZIONI DI SICUREZZA

Migliora la sicurezza del tuo sito web implementando una serie di intestazioni integrate nel server web e inviate al browser.

Inizia con l'intestazione X-Frame-Options, che impedisce l'apertura delle pagine in un frame esterno o iframe, impedendo così gli attacchi clickjacking (letteralmente "furto di clic") sul tuo sito web, una tecnica che induce gli utenti a rivelare informazioni riservate su un sito web apparentemente normale.

Aggiungendo la seguente riga di codice al tuo file .htaccess, comunichi al browser che i frame possono essere aperti solo dallo stesso dominio o dalla stessa origine:

```
Header set X-Frame-Options SAMEORIGIN
```

Se il tuo sito web integra servizi di terze parti, puoi specificare i domini consentiti e negare l'accesso ai rimanenti. Ad esempio:

```
Header set X-Frame-Options "ALLOW-FROM https://esempio.com/"
```

Aumenta la protezione del tuo sito web dagli attacchi XSS (cross-site scripting) sui browser meno recenti aggiungendo la seguente riga di codice al tuo file .htaccess:

```
Header set X-XSS-Protection "1; mode=block"
```

Per ridurre il rischio di XSS, utilizza l'intestazione content-security-policy o politica di sicurezza del contenuto del browser, che specifica quali contenuti del sito web o di terze parti possono caricarsi in maniera dinamica.

Ad esempio, se desideri che il tuo sito web accetti solo contenuti provenienti dallo stesso dominio, aggiungi la seguente riga di codice al tuo file .htaccess:

```
Header set Content-Security-Policy "default-src 'self';"
```

In questo modo bloccherai il caricamento di script da fonti esterne.

Ad esempio, per modificare le variabili per il tuo specifico progetto, utilizza la seguente riga di codice per consentire script di terze parti come Google Analytics:

```
header set Content-Security-Policy "script-src 'self' www.google-analytics.com;"
```

Dovresti prestare attenzione quando implementi questa intestazione perché è facile bloccare risorse senza accorgersene. Consiglio di eseguire vari test con questa intestazione in una scheda del browser separata per verificare eventuali errori sul terminale.

Nota: se in precedenza hai incluso l'intestazione x-content-security-policy nel tuo server ed è diventata obsoleta, dovrai eliminarla perché se utilizzi entrambe le intestazioni contemporaneamente potresti avere problemi.

La quarta intestazione che puoi utilizzare per aumentare la sicurezza è X-content-type-options, che protegge il tuo sito web dal caricamento di stili e script indesiderati quando i tipi MIME previsti non corrispondono a quelli dichiarati nella pagina. Per aggiungere questa protezione, aggiungi questa riga di codice al tuo file .htaccess:

```
Header set X-Content-Type-Options "nosniff"
```

14. PREVIENI GLI ATTACCHI XML-RPC

Il file xmlrpc.php è impiegato da alcune applicazioni e software per comunicare con WordPress; tra questi, l'app WordPress o i client di posta come Outlook e Thunderbird che consentono la funzionalità "Pubblica articoli via email". Anche plugin come Jetpack o JSON Api utilizzano il file XMLRPC per alcune delle loro funzionalità.

Puoi negare completamente l'accesso al file xmlrpc.php modificandone le regole nel file .htaccess o eliminandolo direttamente se sei sicuro di non averne bisogno.

Per negare l'accesso tramite .htaccess, aggiungi le seguenti righe di codice al file:

```
# nega l'accesso a xmlrpc.php
<Files xmlrpc.php>
Order Deny,Allow
Deny from all
</Files>
```

Inoltre è possibile negare l'accesso a XMLRPC utilizzando plugin come Disable XML-RPC o iThemes Security, menzionati nel suggerimento 14.

Per coloro che hanno assolutamente bisogno di questa funzionalità API, la soluzione migliore è abilitarla solo dall'IP in cui è necessario accedere e negare gli altri. In questo caso specifico, aggiungi le seguenti righe di codice al file .htaccess, sostituendo l'IP con quello da cui desideri ottenere l'accesso:

```
<Files xmlrpc.php>
order deny, allow
deny from all
allow from X.X.X.X
</Files>
```

15. DISABILITA LE JSON REST API

Dalla versione 4.4 di WordPress, le REST API sono incluse nel software centrale, consentendo a qualsiasi sviluppatore di interagire con il sito web. Ciò ha consentito a WordPress di raggiungere un numero maggiore di sviluppatori che non hanno familiarità con WordPress, ma allo stesso tempo ha lasciato una porta aperta a possibili attacchi al tuo sito web, in particolare gli attacchi DDoS.

Se nessuno dei tuoi plugin utilizza le REST API, puoi disattivarle con facilità per la tua installazione WordPress. È sufficiente aggiungere le seguenti linee di codice al file functions.php del tuo tema attivo o utilizzare un plugin:

```
add_filter('json_enabled', '__return_false');
add_filter('json_jsonp_enabled', '__return_false');
```

Se preferisci non armeggiare con il codice, puoi utilizzare il plugin Disable REST API. Puoi anche utilizzare il plugin iThemes Security, menzionato nel suggerimento 12 sui plugin firewall, che manterrà attive le REST API ma consentirà l'accesso solo agli utenti con autorizzazioni esclusive.

3

MANTIENI AL SICURO LA TUA INSTALLAZIONE DI WORDPRESS

16. SCEGLI PLUGIN E TEMI AFFIDABILI

Plugin e temi sono potenti risorse esterne che possono aiutarti ad aumentare le funzionalità del tuo sito WordPress. Ce ne sono centinaia di migliaia disponibili nel repository ufficiale di WordPress e su altri siti web. Purtroppo non tutti sono esaminati, costituendo così un serio problema di sicurezza. Spesso, non svolgiamo controlli approfonditi delle funzionalità e dei codici prima di installare un plugin, ma un plugin non verificato può provocare violazioni di sicurezza e conflitti.

Scarica solo plugin e temi dal repository di WordPress e da siti web affidabili. Prima di scegliere il tuo prossimo plugin o tema, vorrei darti qualche consiglio:

- *dai un'occhiata alle recensioni, al numero di download e ai commenti;*
- *controlla la data dell'ultimo aggiornamento per scoprire se il software è attivo;*
- *cerca l'autore e controlla ogni altro suo tema presente nel repository;*
- *verifica la presenza di problemi di compatibilità con il software e la tua installazione attuale.*

Esegui sempre un backup completo del tuo sito web prima di installare un nuovo plugin o un tema.

17. ELIMINA LE INFORMAZIONI SULLA VERSIONE DI WORDPRESS

Questo suggerimento di sicurezza nasconderà le informazioni relative alla tua versione di WordPress dal codice HTML del tuo sito web. In questo modo, gli aggressori non potranno sfruttare eventuali vulnerabilità note associate a una specifica versione di WordPress.

Puoi eliminare le informazioni dall'intestazione HTML e dai file statici aggiungendo il seguente codice al file functions.php del tuo tema o alle utility del tuo plugin:

```
/*
Nascondi la versione di script e stili
*/
function SG_remove_wp_version_strings( $src ) {
        global $wp_version;
        parse_str(parse_url($src, PHP_URL_QUERY), $query);
        if ( !empty($query['ver'])  &&  $query['ver'] === $wp_version ) {
                $src = remove_query_arg('ver', $src);
        }
        return $src;
}
add_filter( 'script_loader_src', 'SG_remove_wp_version_strings' );
add_filter( 'style_loader_src', 'SG_remove_wp_version_strings' );
/*
Nascondi il tag generator dall'intestazione
*/
function SG_remove_wp_generator() {
        return '';
}
add_filter('the_generator', 'SG_remove_wp_generator');
```

Puoi anche nascondere le informazioni sulla versione attuale di WordPress aggiungendo la seguente riga di codice al file .htaccess all'interno della cartella principale di WordPress:

```
#Blocca info su WP
<files readme.html>
Order allow,deny
Deny from all
</Files>
<files license.txt>
Order allow,deny
Deny from all
</files>
```

Nota: sebbene alcune guide di sicurezza di WordPress consigliano di eliminare del tutto questi file, il mio consiglio è di bloccarne accesso poiché un nuovo aggiornamento o la reinstallazione di WordPress potrebbe generarne di nuovi.

18. NASCONDI AVVISI E NOTIFICHE PHP

Insieme ad altre strategie per limitare le informazioni fornite agli aggressori, è una buona idea nascondere le segnalazioni di errori. Le segnalazioni di errori possono fornire informazioni preziose agli aggressori, come le versioni PHP e WordPress del tuo sito web, l'albero delle cartelle o le informazioni del server.

Negli ambienti di sviluppo, le segnalazioni di errori sono utili per convalidare il tuo lavoro e trovare potenziali errori; tuttavia, su un sito web attivo, dovresti disattivare questi registri per nascondere informazioni come percorsi, nomi, versioni e altro.

Per disabilitare le segnalazioni di errori in WordPress, è sufficiente aggiungere le seguenti righe di codice al file wp-config.php:

```
error_reporting( 0 );
ini_set( 'display_errors', 0 );
```

19. NASCONDI LE INFORMAZIONI SU APACHE E PHP

L'ultimo suggerimento per nascondere le informazioni è quello di configurare le intestazioni inviate dai server: spesso contengono informazioni relative al software installato sul server e alla versione di PHP in esecuzione.

A seconda dell'installazione, è necessario nascondere o limitare le informazioni condivise sul server web aggiungendo la seguente riga di codice al file .htaccess nella cartella principale:

```
ServerSignature Off
```

Esistono due modi per nascondere le informazioni sulla versione PHP del tuo sito web che alcuni server inviano nell'intestazione HTTP. Innanzitutto, aggiungi il seguente codice al file .htaccess:

```
Header unset X-Powered-By
```

Oppure usa la seguente direttiva nel file php.ini:

```
expose_php = Off
```

Nota: generalmente è possibile aggiungere questa linea di codice al file php.ini attivo utilizzando il pannello di amministrazione del server, ma la procedura potrebbe variare in base al tuo servizio di hosting.

20. MANTIENI WORDPRESS AGGIORNATO

Per proteggere il tuo sito web dalle vulnerabilità di sicurezza conosciute, dovresti utilizzare l'ultima versione del software centrale di WordPress, mantenere aggiornati i plugin installati e aggiornare i tuoi temi.

Personalmente preferisco mantenere aggiornato il mio sito web manualmente, anche se richiede più attenzione e tempo, perché mi consente di verificare le funzionalità incluse in ogni aggiornamento e il loro scopo. Per quanto riguarda l'ordine degli aggiornamenti, consiglio sempre di aggiornare prima il software centrale di WordPress e poi aggiornare plugin e temi senza preoccuparsi dell'ordine.

Se, tuttavia, desideri che il core di WordPress sia aggiornato automaticamente, è sufficiente aggiungere la seguente riga di codice al tuo file wp-config.php:

```
define( 'WP_AUTO_UPDATE_CORE', true );
```

Nota: l'aggiornamento automatico non verrà eseguito se hai disabilitato il cron di WordPress.

Dopo ogni aggiornamento, riceverai un'email all'indirizzo di posta elettronica utilizzato per l'account amministratore della piattaforma.

L'aggiornamento del core di WordPress è solo una parte dell'equazione: secondo un rapporto di wpscan.org, il 52% delle vulnerabilità riscontrate nelle installazioni di WordPress sono dovute a plugin, l'11% a temi e il 37% al software centrale di WordPress.

Se desideri aggiornare automaticamente i plugin, aggiungi la seguente riga di codice al file functions.php del tuo tema attivo o nel tuo plugin di funzionalità:

```
add_filter( 'auto_update_plugin', '__return_true' );
```

Prima di aggiungere questo codice, elimina tutti i plugin non utilizzati sul tuo sito web. La semplice disattivazione non è sufficiente per rimuovere potenziali vulnerabilità: eliminali!

Aggiungendo la seguente riga di codice aggiornerai automaticamente i temi:

```
add_filter( 'auto_update_theme', '__return_true' );
```

Infine, ricorda che va benissimo mantenere al sicuro il tuo sito WordPress, ma non dovresti dimenticarti che anche il tuo computer dovrebbe essere protetto da virus e software dannosi. Assicurati di utilizzare un antivirus affidabile e di mantenere aggiornato il tuo sistema operativo.

21. SCEGLI UNA SOCIETÀ DI HOSTING AFFIDABILE

L'ultimo consiglio relativo alla sicurezza, sebbene dovrebbe essere il primo in termini di importanza, è quello di scegliere un server sicuro per ospitare il tuo progetto web.

Il tuo fornitore di hosting dovrebbe offrirti una piattaforma sicura e mantenere attivamente la sicurezza della propria infrastruttura. Diffida di servizi di hosting che fanno uso di software obsoleto, che non proteggono l'accesso e che impiegano supporto tecnico con una scarsa conoscenza di WordPress.

La scelta di un buon fornitore di hosting è un fattore importantissimo per la riuscita e la sicurezza del tuo progetto WordPress.

CONCLUSIONE

RIEPILOGO

In termini di sicurezza, il buon senso è il tuo miglior alleato: utilizza password complesse, elimina utenti inattivi, assegna i ruoli corretti a ciascun utente, non salvare sessioni attive su computer pubblici, mantieni aggiornato l'orario del server, consenti solo l'accesso protetto e monitora attivamente il tuo sito web.

Naturalmente, è impossibile raggiungere la totale sicurezza, ma mi auguro che questa guida possa aiutarti a proteggere a lungo il tuo sito web. Ragiona sempre con la tua testa e applica soltanto i suggerimenti che ti servono e che sono compatibili con il tuo progetto. Sicuramente non ti farà male aggiornarti sulle ultime notizie e tendenze relative a WordPress e alla sua sicurezza.

Questa guida si basa sulla mia esperienza pluridecennale con WordPress. La maggior parte delle informazioni raccolte e condivise in questa guida non potrebbero esistere senza i professionisti della community, a cui va il mio riconoscimento. I miei suggerimenti si basano anche sulle svariate risorse online relative alla sicurezza web di WordPress, contenuti che vengono generati quasi ogni giorno: nel momento in cui leggi la presente guida, molto probabilmente alcuni suggerimenti saranno già superati, mentre altri non saranno più necessari grazie agli aggiornamenti del core di WordPress.

Scegli l'hosting SiteGround per la sicurezza del tuo sito WordPress
https://it.siteground.com/hosting-wordpress

4

INFORMAZIONI SULL'AUTORE

FERNANDO PUENTE

Fernando è un esperto IT: l'informatica è il suo lavoro, nonché la sua passione. Insegna saltuariamente e si definisce un appassionato di enogastronomia. Lavora nel settore IT da più di 21 anni, 12 dei quali per i mass media. Ha iniziato a lavorare con WordPress nel 2007, ma la scintilla si è accesa solo alla versione 3.0. Si è specializzato nell'ottimizzazione delle prestazioni dei siti web di notizie e degli e-commerce. Attualmente lavora come consulente aziendale e fornisce assistenza tecnica per varie piattaforme online.

fpuenteonline


SiteGround