Attivare HTTPS con Altervista e WordPress

Filippo Rigotto*

Sommario

Il protocollo HTTPS consente la cifratura della comunicazione tra il server che ospita un sito web e il browser che lo sta visitando. Altervista ha reso gratuita la possibilità di abilitarlo per il proprio sito. Oltre ad essere necessario se si scambiano dati sensibili con l'utente, l'indicizzazione Google è migliore se il sito supporta HTTPS. Questa è una sintetica guida passo-passo per l'attivazione della cifratura su un'installazione WordPress in un dominio Altervista.

I primi passi si eseguono dal pannello di controllo di Altervista[1]:

- Attivare CloudFlare, dal pannello Risorse cliccando sull'apposito tasto; in seguito accettare i termini del contratto con una spunta sul relativo controllo.
- Attivare HTTPS, sempre dal pannello Risorse: occorre verificare l'identità inviando un SMS al numero che appare.
- Nella stessa schermata, attivare la riscrittura dei link; questo consentirà una traduzione automatica dei collegamenti HTTP in HTTPS.

Tenere sotto controllo l'indirizzo email associato all'account Altervista per le email di conferma degli account, per i punti precedenti.

La procedura prosegue dal pannello di amministrazione WordPress[2]:

- Dalla schermata Plugin, cliccare su Aggiungi nuovo e installare Really Simple SSL[3], un efficace plugin di Rogier Lankhorst.
- Dopo aver attivato il plugin, dal banner che compare in alto cliccare Ricarica in SSL: l'adeguamento di WordPress avviene in automatico se tutto è corretto.

Ora un ultimo passo per controllare che tutto funzioni correttamente: utilizzando varvy.com/tools/redirects, inserire l'indirizzo del sito e controllare che i vari *redirect* per tutte le versioni dell'URL funzionino, con al massimo 2 "salti".

In CloudFlare, nel pannello Crypto è possibile impostare alcune scelte aggiuntive: per il corretto funzionamento del sito è *necessario* mantenere l'impostazione SSL su Flexible, mentre si può abilitare Always use HTTPS e Automatic HTTPS rewrites per avere la riscrittura automatica dei link anche da qui. Require modern TLS è utile in caso si voglia sicurezza aggiuntiva, consente di utilizzare soltanto le ultime versioni di TLS, il protocollo specifico per la cifratura della connessione.

— Procedura corretta e funzionante al 10 marzo 2018.

Quest'opera è distribuita con licenza "CC BY-NC-ND 4.0".

* http://rigottofilippo.altervista.org – rigottofilippo AT altervista.org

[1] https://altervista.org/cplogin.php

[2] http://<account>.altervista.org/wp-admin generalmente

[3] https://it.wordpress.org/plugins/really-simple-ssl