PROTOCOLLO HTTP

Il protocollo HTTP, acronimo di "Hypertext Transfer Protocol, è un protocollo di comunicazione utilizzato su Internet per il trasferimento di dati ipertestuali.

È il protocollo fondamentale utilizzato per la trasmissione di pagine web, immagini, video, file e altri contenuti su Internet, ed è supportato da diversi linguaggi di programmazione, framework e server web.

La prima versione dell'HTTP, la 0.9, risale alla fine degli anni 1980 e costituiva, insieme con il linguaggio HTML e gli URL, il nucleo base del World Wide Web.

Successivamente emersero le versioni: HTTP/1.0 - HTTP/1.1 - HTTP/2 - HTTP/3

Metaforicamente parlando, l'HTTP è la lingua che utilizza il browser per parlare al server web e comunicargli ciò che viene richiesto.

Questo protocollo funziona secondo un modello client-server:

il client chiede con il browser web le risorse, che può essere un servizio web o un server attraverso le richieste http, mentre il server o qualsivoglia servizio risponde con le risorse richieste che possono essere intestazioni, url e dati.

La richiesta (dal client) è composta da: GET, POST, HEAD, PUT, DELETE

Una volta che il server ha ricevuto la richiesta, conosce esattamente la risorsa di cui il client ha bisogno tramite l'URI (Uniform Resource Identifier) e ciò che il client vuole fare con quella risorsa, quindi in risposta fornisce la risorsa richiesta e altre informazioni, così come il codice di risposta, ad esempio:

200 > risorsa ok

301 > risorsa momentaneamente spostata ad un nuovo indirizzo

404 > risorsa non trovata

500 > errore interno del server

Ad oggi se un sito utilizza il protocollo http è più soggetto ad intercettazione e quindi a furto di identità, frodi e altri crimini.

Dall'anno 2000 si è diffuso man mano il protocollo HTTPS che utilizza TLS (Transport Layer Security) per la crittografia dei dati, che a differenza del precedente http funziona con connessioni più sicure.

TLS è stato approvato come standard di sicurezza, diventando il protocollo preferito per la sicurezza delle comunicazioni web, cosicché molte organizzazioni e aziende

hanno iniziato a implementare TLS (e di conseguenza HTTPS) sui loro server web per garantire la sicurezza delle comunicazioni tra i loro siti web e i loro utenti.

Essendo crittografata la connessione impedisce a terzi di intercettare la comunicazione tra il client e server.

A differenza del protocollo http, https servendosi di questo speciale protocollo di trasporto (SSL/TLS) come tipo di trasmissione, utilizza chiavi private e pubbliche a lungo termine per generare chiavi di sessione a breve termine.

Queste chiavi sono utilizzate successivamente per cifrare il flusso dei dati scambiati tra client e server.

La diffusione di HTTPS è stata un processo graduale che si è evoluto nel corso degli anni, con l'adozione crescente del protocollo a partire dagli anni 2000 fino a diventare uno standard di sicurezza comune per le comunicazioni web, come la maggior parte dei siti internet che utilizza questa sicurezza per impedire che le informazioni siano intercettate da terzi.

ESEMPIO HTTP:

trasmissione > non criptata

certificato > non presente

numero porta > 80

indirizzamento nell' url > http://

ESEMPIO HTTPS:

trasmissione > criptata

certificato > presente

numero di porta > 443

Indirizzamento nell' url > https://