

Module Lesson - HTTP & Browser

Hypertext Transfer Protocol (HTTP) vs Hypertext Transfer Protocol Secure (HTTPS)

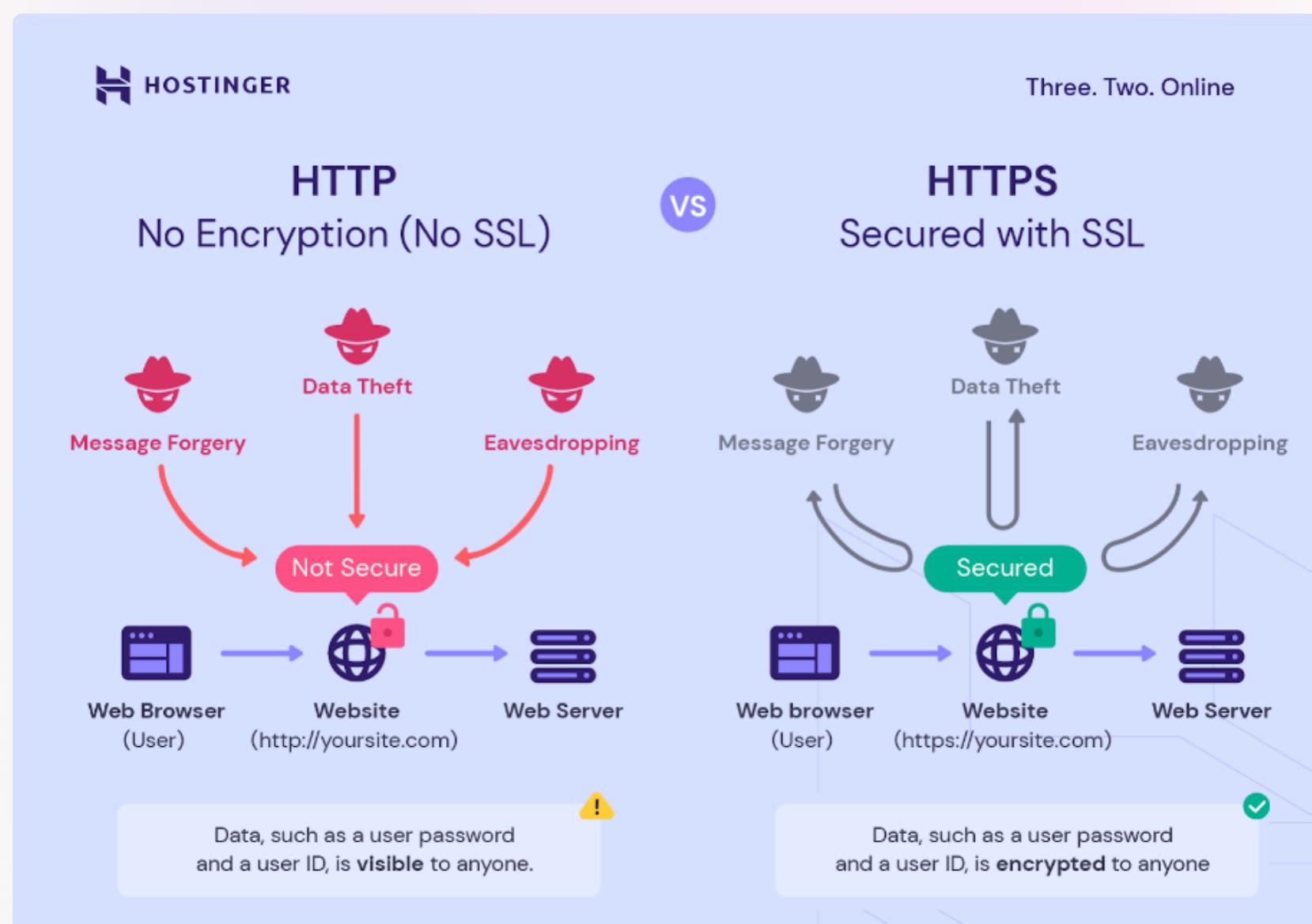
HTTP

HTTP adalah protokol aplikasi yang mentransfer data di web utamanya dalam bentuk teks biasa. Siapa pun dapat menguping atau mencegat data yang ditransfer melalui HTTP.

HTTPS

HTTPS mengenkripsi dan mengirimkan data secara lebih aman melalui proses jabat tangan SSL/TLS, sehingga sulit bagi penyerang untuk mengintersepsi atau memanipulasi data pada HTTPS.

HTTP (Hypertext Transfer Protocol) dan HTTPS (Hypertext Transfer Protocol Secure) adalah protokol yang digunakan untuk mengirimkan data melalui internet. Keduanya berperan penting dalam menghubungkan pengguna dengan situs web dan memastikan keamanan komunikasi.



Mari kita bayangkan internet sebagai jaringan besar yang menghubungkan banyak komputer di seluruh dunia. Setiap komputer di internet memiliki alamat yang unik, seperti alamat rumah kita sendiri. Ketika kita ingin mengakses situs web, kita menggunakan protokol HTTP atau HTTPS untuk mengirim permintaan dari komputer kita ke server yang menyimpan situs web tersebut.

HTTP adalah protokol yang digunakan secara umum. Ia mengatur cara komunikasi antara browser (seperti Chrome, Firefox, atau Safari) yang kita gunakan dan server situs web. Ketika kita memasukkan URL (Uniform Resource Locator) ke dalam browser, contohnya <http://www.example.com>, browser kita akan mengirim permintaan HTTP ke server yang menyimpan situs web "example.com". Permintaan ini berisi informasi seperti tipe permintaan (GET, POST, PUT, DELETE), path atau alamat file yang diminta, dan informasi tambahan seperti cookie.

Saat server menerima permintaan HTTP, ia akan mengirimkan kembali respons yang berisi informasi yang diminta. Respons ini bisa berisi halaman web yang diminta, gambar, file teks, atau data lainnya. Respons ini juga dapat mencakup kode status HTTP yang memberikan informasi tentang apakah permintaan berhasil (kode 200), tidak ditemukan (kode 404), atau ada masalah lainnya.

Namun, meskipun HTTP sangat umum digunakan, ia memiliki kelemahan dari segi keamanan. Karena data yang dikirimkan melalui protokol HTTP tidak dienkripsi, data tersebut dapat dengan mudah diintersepsi oleh pihak yang tidak sah. Misalnya, jika kita mengisi formulir pribadi yang tidak dienkripsi dengan HTTP, data yang kita masukkan bisa diketahui oleh orang lain.

Inilah mengapa HTTPS hadir untuk mengatasi kelemahan tersebut. HTTPS menggunakan **SSL (Secure Sockets Layer)** atau **TLS (Transport Layer Security)** untuk mengenkripsi data yang dikirimkan antara browser dan server. Enkripsi ini menjaga kerahasiaan dan integritas data, sehingga pihak yang tidak sah sulit untuk mengakses atau mengubah informasi yang dikirimkan.

Understanding SSL/TLS

1 What is SSL/TLS?

SSL (Secure Socket Layer) dan TLS (Transport Layer Security) adalah protokol kriptografi yang bertujuan untuk menyediakan komunikasi yang aman di atas web.

2 How does SSL/TLS work?

Protokol SSL/TLS membentuk saluran komunikasi yang aman antara dua titik akhir yang terhubung dalam jaringan. Setelah saluran tersebut terbentuk, server dan klien dapat bertukar data dengan keyakinan bahwa data tersebut aman dan bersifat pribadi.

3 The difference between SSL and TLS

Perbedaan utama antara SSL dan TLS adalah versi dan evolusi protokol. TLS dirancang sebagai pengganti SSL dan telah mengalami pembaruan dan perbaikan berkelanjutan untuk mengatasi kelemahan yang ditemukan dalam SSL.

Secara konseptual, keduanya berfungsi sama, yaitu menyediakan enkripsi dan keamanan dalam komunikasi internet. Namun, karena perkembangan yang lebih lanjut dan peningkatan keamanan, disarankan untuk menggunakan TLS daripada SSL.

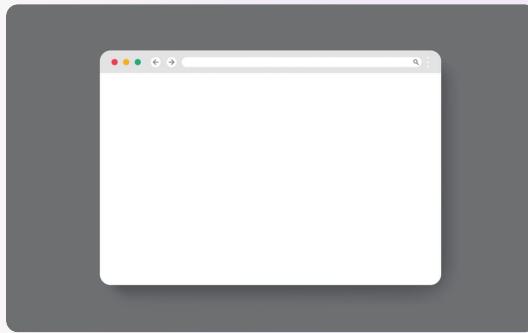
Dalam prakteknya, ketika kita berbicara tentang HTTPS (Hypertext Transfer Protocol Secure), protokol yang digunakan adalah TLS, bukan SSL. Sebagai pengguna, kita sering mendengar istilah HTTPS karena itu adalah implementasi keamanan yang umum digunakan dalam browsing web modern.

Jadi, secara ringkas, SSL dan TLS adalah protokol keamanan yang digunakan untuk menyediakan enkripsi dan keamanan dalam komunikasi internet. TLS adalah pengganti SSL yang lebih aman dan cenderung digunakan secara luas saat ini.

The Wonders of Browser's Main Functionality

"Fungsi utama dari peramban adalah untuk memuat dan mengartikan HTML, CSS, dan JavaScript, yang membentuk dasar dari web modern. Ini memberikan kemampuan kepada pengguna untuk mengubah konten web statis ini menjadi dinamis dengan memanggil skrip JavaScript."

The Browser Structure – Comprehend Its Anatomy



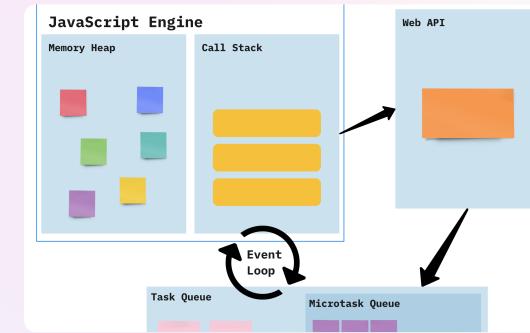
Browser Window

Peramban mencakup semua elemen di dalamnya, termasuk bilah judul, bilah alamat, tab, konten halaman saat ini, bilah status, dan ikon ekstensi apa pun.



Browser Engine

Mengelola tampilan halaman yang diminta setelah melakukan permintaan ke server, mengartikan kode HTML/CSS/JS, dan memformatnya di jendela peramban.



JavaScript Engine

Ini menerjemahkan kode JavaScript ke dalam kode mesin. Secara umum, mesin V8 menjalankan sebagian besar peramban.

HTTP Status Codes: Meaning and Usage

Code	Title	Description
200	OK	Request succeeded
204	No Content	Request successful, but no data is returned to the client
301	Moved Permanently	Resource has been moved
404	Not Found	Resource requested cannot be found
500	Internal Server Error	Server error

Client-Side vs Server-Side Rendering

1

Client-Side Rendering

Ini melibatkan memuat HTML dan DOM kerangka untuk menampilkan pengisi (loader) sementara backend mengambil data dari API di latar belakang. Data diambil dari server dan konten dirender langsung di peramban klien.

2

Server-Side Rendering

Ini terjadi ketika konten pertama kali dirender di sisi server sebelum disajikan ke peramban klien. Server mengirimkan berkas HTML yang sudah sepenuhnya diisi dengan data yang diambil di sisi server.



Made with Gamma

Error Handling in Browser

"Peramban mengatasi sumber daya yang diminta yang menghasilkan kesalahan secara tangguh. Jika sumber daya halaman web mengalami kesalahan, peramban akan kembali ke versi yang sebelumnya di-cache atau halaman kesalahan yang relevan."