Nama : Farhan Dwi Septian
NIM : 105221036

Pretest Praktikum 1 Pemrograman Web

1. Apa itu HTTP (Hypertext Transfer Protocol) dan bagaimana cara kerjanya dalam komunikasi web?

   Jawab:

   "Hypertext Transfer Protocol" adalah protokol aplikasi untuk sistem informasi hipermedia terdistribusi, kolaboratif, dan memungkinkan pengguna untuk mengomunikasikan data di World Wide Web.

   HTTP diciptakan bersama HTML untuk membuat browser web interaktif berbasis teks pertama: World Wide Web yang asli. Saat ini, protokol ini tetap menjadi salah satu cara utama untuk menggunakan Internet.

   Sebagai protokol request-response, HTTP memberikan cara kepada pengguna untuk berinteraksi dengan sumber daya web seperti file HTML dengan mengirimkan pesan hiperteks antara klien dan server. Klien HTTP umumnya menggunakan koneksi Transmission Control Protocol (TCP) untuk berkomunikasi dengan server.

   HTTP menggunakan metode permintaan khusus untuk melakukan berbagai tugas. Semua server HTTP menggunakan metode GET dan HEAD, tetapi tidak semua mendukung metode permintaan lainnya:

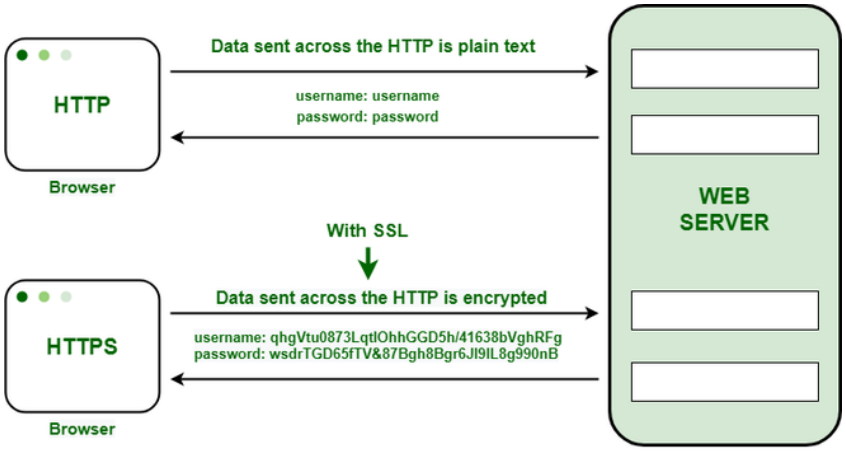
   - GET meminta sumber daya tertentu secara keseluruhan
   - HEAD meminta sumber daya tertentu tanpa konten tubuh
   - POST menambahkan konten, pesan, atau data ke halaman baru di bawah sumber daya web yang sudah ada
   - PUT secara langsung memodifikasi sumber daya web yang sudah ada atau membuat URI baru jika perlu
   - DELETE menghapus sumber daya tertentu
   - TRACE menunjukkan kepada pengguna setiap perubahan atau penambahan yang dilakukan pada sumber daya web
   - OPSI menunjukkan kepada pengguna metode HTTP mana yang tersedia untuk URL tertentu
   - CONNECT mengubah koneksi permintaan menjadi terowongan TCP/IP transparan
   - PATCH memodifikasi sebagian sumber daya web

   Referensi:
   https://www.extrahop.com/resources/protocols/http/

2. Apa perbedaan utama antara HTTP dan HTTPS (Hypertext Transfer Protocol Secure), dan mengapa HTTPS lebih aman?

Jawab:

Hypertext Transfer Protocol (HTTP) adalah protokol yang digunakan untuk mentransfer hypertext melalui Web. Karena kesederhanaannya, HTTP telah menjadi protokol yang paling banyak digunakan untuk transfer data melalui Web, tetapi data (yaitu hiperteks) yang dipertukarkan menggunakan HTTP tidak seaman yang kita inginkan. Protokol kriptografi seperti SSL dan/atau TLS mengubah HTTP menjadi HTTPS, yaitu HTTPS = HTTP + Protokol Kriptografi.



HTTP	HTTPS
HTTP stands for HyperText Transfer Protocol. In HTTP, the URL begins with “http://”.	HTTPS stands for HyperText Transfer Protocol Secure. In HTTPS, the URL starts with “https://”.
HTTP uses port number 80 for communication.	HTTPS uses port number 443 for communication.
Hyper-text exchanged using HTTP goes as plain text i.e. anyone between the browser and server can read it relatively easily if one intercepts this exchange of data and due to which it is Insecure.	HTTPS is considered to be secure but at the cost of processing time because Web Server and Web Browser need to exchange encryption keys using Certificates before actual data can be transferred.
HTTP Works at the Application Layer.	HTTPS works at Transport Layer.
HTTP does not use encryption, which results in low security in comparison to HTTPS.	HTTPS uses Encryption which results in better security than HTTP.

Referensi
https://www.geeksforgeeks.org/difference-between-http-and-https/

3. Bagaimana DNS (Domain Name System) berperan dalam penggunaan internet, dan mengapa penting untuk mengonfigurasi DNS dengan benar?

   Jawab:
   "The Domain Name System"(DNS) adalah buku telepon Internet. Manusia mengakses informasi secara online melalui nama domain, seperti nytimes.com atau espn.com. Peramban web berinteraksi melalui alamat Protokol Internet (IP). DNS menerjemahkan nama domain ke alamat IP sehingga browser dapat memuat sumber daya Internet.

   Setiap perangkat yang tersambung ke Internet memiliki alamat IP unik yang digunakan mesin lain untuk menemukan perangkat tersebut. Server DNS menghilangkan kebutuhan manusia untuk menghafal alamat IP seperti 192.168.1.1 (di IPv4), atau alamat IP alfanumerik yang lebih kompleks seperti 2400:cb00:2048:1::c629:d7a2 (di IPv6).

   Bagaimana cara kerja DNS?
   Proses resolusi DNS melibatkan pengubahan nama host (seperti www.example.com) menjadi alamat IP yang sesuai dengan komputer (seperti 192.168.1.1). Alamat IP diberikan kepada setiap perangkat di Internet, dan alamat tersebut diperlukan untuk menemukan perangkat Internet yang sesuai - seperti alamat jalan yang digunakan untuk menemukan rumah tertentu. Ketika pengguna ingin memuat sebuah halaman web, sebuah terjemahan harus dilakukan antara apa yang diketikkan pengguna ke dalam peramban web mereka (example.com) dan alamat yang sesuai dengan mesin yang diperlukan untuk menemukan halaman web example.com.

   Untuk memahami proses di balik resolusi DNS, penting untuk mempelajari berbagai komponen perangkat keras yang harus dilewati oleh kueri DNS. Untuk peramban web, pencarian DNS terjadi "di belakang layar" dan tidak memerlukan interaksi dari komputer pengguna selain dari permintaan awal.

   Referensi:
   https://www.cloudflare.com/learning/dns/what-is-dns/

4. Apa fungsi utama dari sebuah server dalam konteks teknologi informasi, dan bagaimana server

   Jawab:
   Server adalah program atau perangkat yang menyediakan fungsionalitas untuk klien yang disebut sebagai program atau perangkat lain. Arsitektur ini disebut model klien-server.

   Satu komputasi keseluruhan didistribusikan di beberapa proses atau perangkat. Server dapat menyediakan berbagai fungsi yang disebut layanan. Layanan ini termasuk berbagi data atau sumber daya di antara beberapa klien atau melakukan perhitungan untuk klien. Beberapa klien dapat dilayani oleh satu server, dan satu klien dapat menggunakan beberapa server.

   Bagaimana Cara Kerja Server?

Perangkat perlu diatur untuk mendengarkan permintaan klien melalui koneksi jaringan agar dapat menjalankan peran sebagai server. Sistem operasi dapat menyertakan fungsionalitas ini sebagai aplikasi yang terinstal, peran, atau kombinasi keduanya.

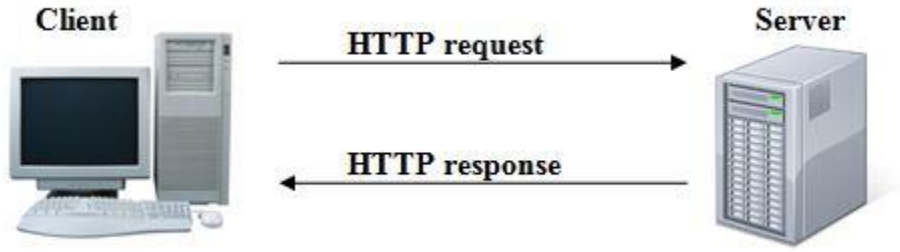
Sistem operasi windows server dari microsoft memiliki kemampuan untuk mendengar dan merespons permintaan klien. Jenis permintaan klien yang dapat ditangani server bertambah dengan adanya role atau layanan tambahan yang terinstal. Ilustrasi lain adalah ketika aplikasi tambahan yang disebut Apache diletakkan di atas sistem operasi untuk menangani permintaan dari browser web. Klien mengirimkan permintaan melalui jaringan setiap kali membutuhkan data atau fungsionalitas dari server. Server menerima permintaan ini dan memberikan informasi yang diperlukan sebagai tanggapan. Ini adalah model permintaan dan respons jaringan klien-server, yang biasa disebut sebagai model panggilan dan respons.

Sebagai bagian dari satu permintaan dan respons, server sering kali menyelesaikan berbagai tugas tambahan, seperti mengonfirmasi identitas pemohon, memastikan klien memiliki izin untuk mengakses data atau sumber daya yang diminta, dan memformat dengan benar atau mengembalikan respons yang diperlukan dengan cara yang diharapkan.

Referensi:
https://www.geeksforgeeks.org/what-is-server/

5. Bagaimana protokol HTTP digunakan dalam konteks server? Jelaskan aliran komunikasi antara klien dan server ketika mengakses sebuah situs web.

   Jawab:
   Protokol HTTP menyediakan kumpulan perintah di dalam komunikasi antar jaringan. Komunikasi tersebut berlangsung antara web server dengan komputer client atau sebaliknya. Di dalam komunikasi ini, komputer client melakukan permintaan dengan mengakses alamat IP Address atau domain (URL). Kemudian web server mengelola permintaan tersebut sesuai dengan kode yang dimasukkan.



   Contoh yang paling sederhana penggunaan protokol HTTP adalah komunikasi antara komputer client dengan web server.

Komputer client melakukan permintaan menggunakan browser ke web server. Kemudian web server menanggapi permintaan tersebut dengan mengirimkan data/dokumen yang tersedia di dalam web server sesuai dengan permintaan komputer client.

Sebenarnya, ada protokol lain untuk bertukar data dan informasi seperti SMTP, FTP, IMAP atau POP3. Namun protokol HTTP yang paling banyak digunakan dibanding dengan yang lainnya. Alasannya karena HTTP pertama kali memang didesain untuk mengelola dokumen HTML dan mengirimkannya kepada client.

Selain itu, protokol HTTP cukup fleksibel dan sampai saat ini terus dikembangkan dengan penambahan beberapa fitur baru. Hal ini membuat protokol HTTP menjadi protokol yang paling dapat diandalkan dan paling cepat memproses pertukaran data.

Sedikit info tambahan, HTTP kini sudah berevolusi menjadi HTTP/3 yang pastinya lebih cepat dan aman. Simak artikel apa itu HTTP/3 untuk tahu lebih lanjut.

Referensi:
https://www.niagahoster.co.id/blog/pengertian-http/

6. Mengapa enkripsi data sangat penting dalam HTTPS dan bagaimana SSL/TLS (Secure Sockets Layer/Transport Layer Security) berperan dalam mengamankan koneksi web?

   Jawab:
   SSL adalah singkatan dari **Secure Sockets Layer**, yaitu protokol keamanan yang didesain untuk melindungi data di Internet. Sementara itu, **TLS adalah** pengganti SSL, sama-sama merupakan protokol keamanan yang berfungsi untuk mengamankan privasi data dan merupakan versi baru SSL.
   Secara umum, fungsi SSL adalah untuk mengamankan data pribadi, seperti nama, alamat, atau nomor kartu kredit dari para penjahat cyber.
   Jadi, penggunaan SSL adalah hal yang sangat penting bagi website Anda. Website atau blog yang memasang SSL/TLS biasanya memiliki simbol gembok di kolom URL browser saat Anda mengaksesnya, serta menggunakan **HTTPS dan bukan HTTP**.

   Secara digital, cara kerja SSL adalah dengan mengunci cryptographic key (kunci kriptografi) ke informasi perusahaan yang akan diidentifikasi. Data pun akan terenkripsi dengan baik selama proses transfer sehingga pihak ketiga tidak akan bisa masuk dan mencuri informasi sensitif.

   Tak hanya private key dan public key, SSL/TLS juga memiliki session key (kunci sesi) yang selalu berbeda untuk setiap secure session (sesi aman). Pada saat pengunjung mengetikkan alamat URL yang telah dilindungi SSL di kolom web browser atau membuka halaman yang sudah dilindungi, browser dan web server akan membuat koneksi. Selama koneksi awal, public key (kunci publik) dan private key (kunci privat) akan digunakan untuk membuat session key, yang kemudian mengenkripsi dan mendekripsi data yang sedang ditransfer. Session key ini akan tetap valid selama beberapa waktu dan hanya digunakan di sesi tersebut.

Seperti yang tadi kami jelaskan, Anda bisa melihat apakah suatu website menggunakan SSL/TLS atau tidak dari ikon gembok atau warna hijau yang muncul di kolom URL browser. Ikon tersebut bisa diklik untuk melihat siapa saja yang menyimpan informasi sertifikat dan juga untuk mengelola pengaturannya.

7.