Telkom University	**Tugas 7** **Pemrograman Jaringan (CSH4V3)** **----------** **Semester Ganjil 2019 - 2020** **Dosen: Aulia Arif Wardana, S.Kom., M.T. (UIW)**

Berdo'alah sebelum mengerjakan. Dilarang berbuat curang.
Tugas ini untuk mengukur kemampuan anda, jadi kerjakan dengan sepenuh hati.
Selamat belajar, semoga sukses !

Nama Mahasiswa: **Lukman Budiman** ……	**NIM:** **1301164725** ……	**Nilai:** ……
Nama Mahasiswa: **Yuwantoro Mukhlisin** ……	**NIM:** **1301150042** ……	**Nilai:** ……
Nama Mahasiswa: **Salma Fauzia Susan** ……	**NIM:** **1301164442** ……	**Nilai:** ……

Siapkan tools berikut sebelum mengerjakan:

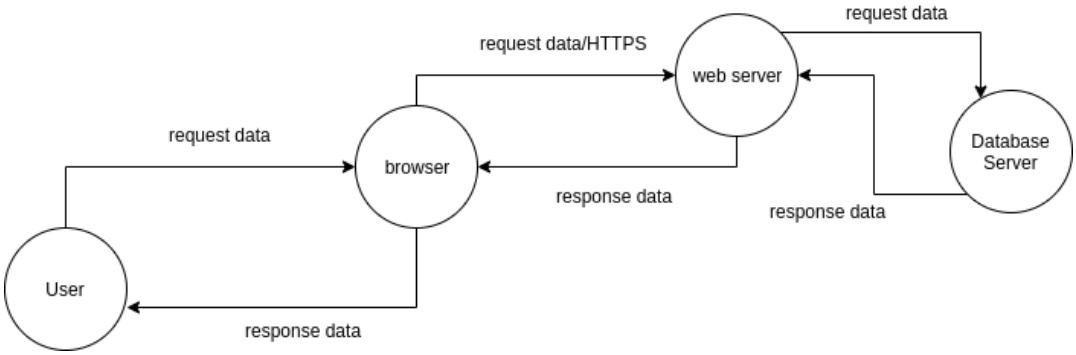
1. Go Programming Language (https://golang.org/dl/).
2. Visual Studio Code (https://code.visualstudio.com/) atau LiteIDE (https://github.com/visualfc/liteide).
3. Harus menggunakan linux dengan distro fedora (https://getfedora.org/id/workstation/).
4. Gunakan openssl (https://www.openssl.org/) untuk mengerjakan salah satu tugas pada modul ini.
5. Buatlah git repository pada https://github.com/ kemudian push semua kode dan hasil laporan anda ke dalam repository github yang sudah anda buat.
6. Kumpulkan link repository github tersebut sebagai tanda bahwa anda mengerjakan tugas modul ini.
7. Link repository harus berbeda untuk setiap tugasnya. Buatlah markdown yang rapi disetiap repository tugas yang anda kumpulkan.
8. Printscreen program harus dari desktop kelompok anda sendiri, dan harus dari linux yang sudah diinstall. Jika tidak, maka harus mengulang pengerjaan tugasnya.
9. Jangan lupa untuk menuliskan NAMA dan NIM pada laporan.
10. Laporan berbentuk PDF dan dikumpulkan pada link repository github beserta kodenya.
11. Walaupun tugas berkelompok tapi pengumpulan link github harus individu, jika tidak mengumpulkan maka dianggap tidak mengerjakan.

Nama:	NIM:	Nilai:

Soal No 1 (Secure Web Server Design)

Buatlah perancangan aplikasi Web Server yang dapat melakukan serve koneksi HTTPS menggunakan diagram FSM serta jelaskan cara kerjanya!

Jawaban:



Cara kerja FSM diatas adalah :

- user atau HTTPS klien akan membuat sambungan dan mengirimkan permintaan dokumen kepada web server melalui browser.
- Selanjutnya HTTPS server akan memproses permintaan tersebut dan HTTPS klien menunggu respon.
- Terakhir, setelah data ditemukan maka web server akan mengirimkan data melalui HTTPS dan menampilkannya di browser. Setelah perminataan data selesai web server akan menutup sambungan. Pada protokol HTTPS, jalur komunikasi menggunakan port 443 sehingga melalui tahap secure connection.

Soal No 2 (Secure Web Server Implementation)

Implementasikan aplikasi secure web server dari design yang sudah anda buat, aplikasi harus mempunyai config file untuk melakukan konfigurasi aplikasi!
Anda bisa mengembangkan dari code berikut https://github.com/aulwardana/simpe-web-server

Jawaban:

Pertama untuk membuat aplikasi secure web server harus menyiapkan private key dan public key terlebih dahulu

Gunakan openssl untuk generate private key

$ openssl genrsa -out server.key 2048

```
$ openssl ecparam -genkey -name secp384r1 -out server.key
```

Dua command di atas menghasilkan server.key yang merupakan private key. Setelah itu, generate *self-signed* certificate (yang berisikan public key) dari private key yang telah dibuat.

$ openssl req -new -x509 -sha256 -key server.key -out server.crt -days 3650

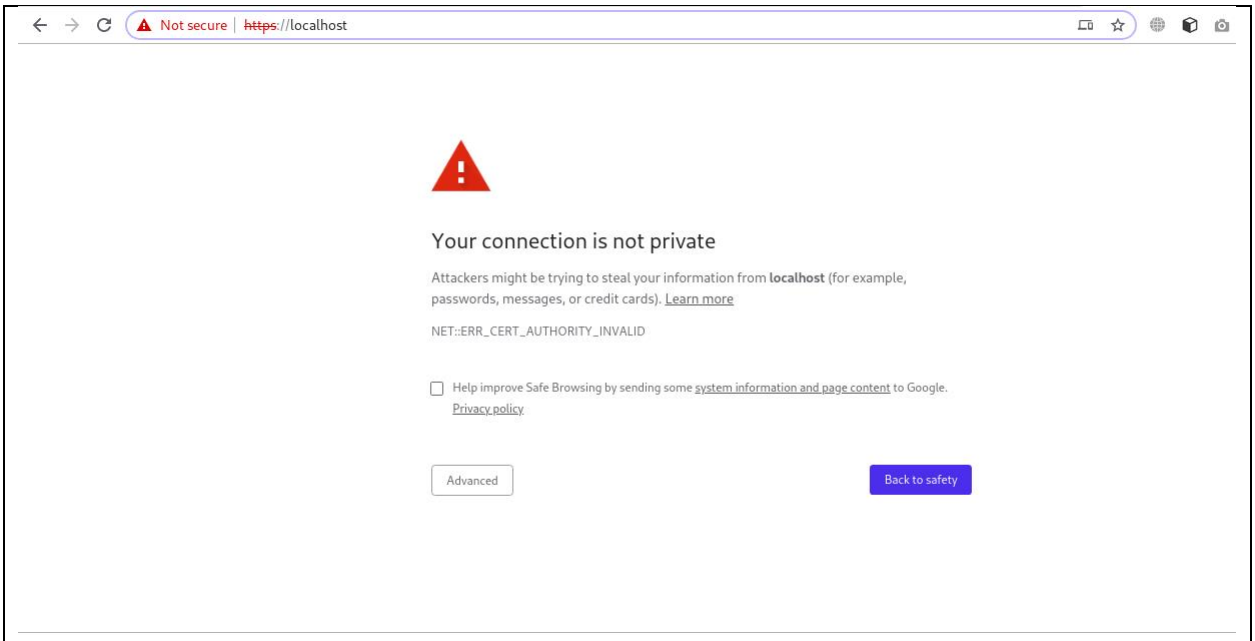
Command untuk generate certificate di atas akan memunculkan form. Informasi seperti alamat, email, host diminta untuk di-isi, pastikan isi dengan benar, terutama di bagian **"Common Name"** dan **Email Address**.

- Pada bagian common name isi dengan **localhost**.
- Untuk email isi dengan alamat email yang valid.

Setelah selesai, running go run main.go

```
root@localhost tugas7]# go run main.go
2019/10/07 00:19:32 Server started at :443
2019/10/07 00:21:41 http: TLS handshake error from [::1]:53052: remote error: tls: unknown cert
ficate
```

Lalu bukalah browser dengan mengetikan https://localhost maka hal pertama yang akan tampil adalah



Browser akan melakukan validasi dari sertifikat ssl dan memastikan website tersebut benar-benar valid. Selama proses SSL handshake, untuk public key dan private key akan melakukan enkripsi dan dekripsi. Apabila sertifikat valid, session key akan dibuat oleh klien dan server. Agar bisa ke halaman selanjutnya klik advanced lalu klik procees to localhost (unsafe), maka tampilannya seperti berikut.