Laboratorio #6

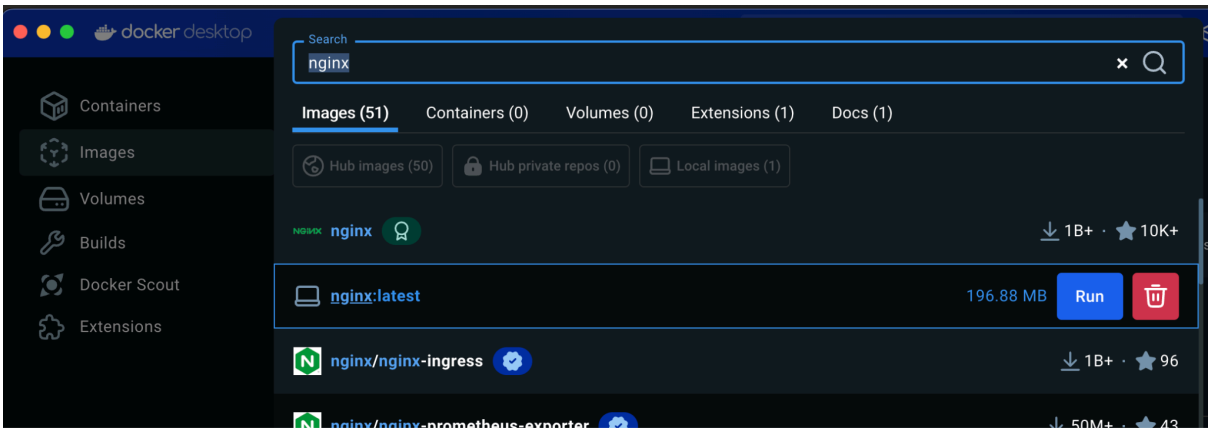
Estudiante:
Andrés Arias Medina

Curso
Seguridad en los Datos

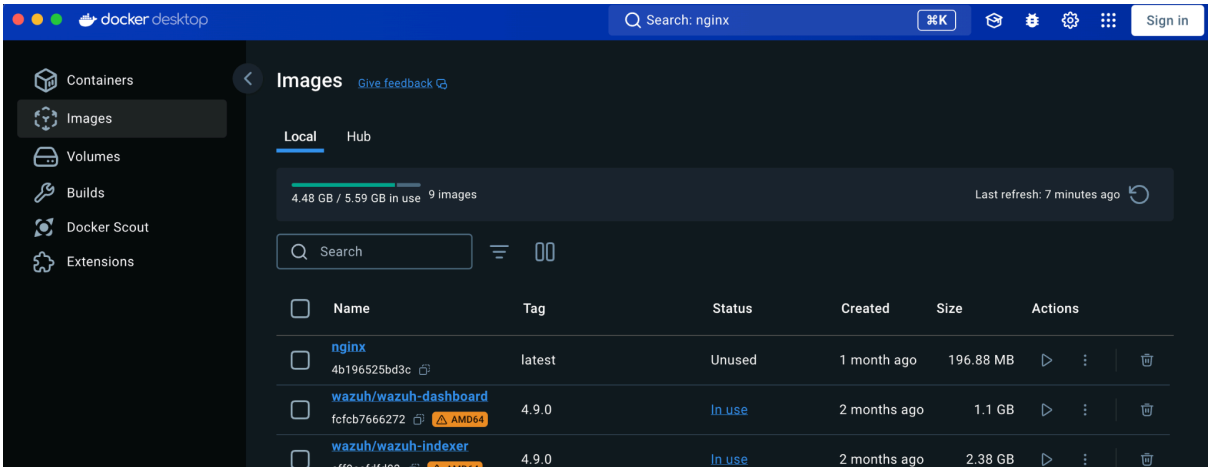
Profesor
Javier Omar Contreras Rodriguez

Universidad Pontificia Bolivariana
9 de noviembre de 2024
Medellín, Colombia

Se abre Docker Desktop y buscamos la imagen oficial de **nginx.** A través de un pull la descargamos en nuestro sistema.



Verificamos su instalación para asegurarnos de que esté la última versión.



Lo siguiente es abrir una terminal y verificar qué imágenes se tienen disponibles.

```
andresariasmedina@Andress-MacBook-Pro ~ % docker images
REPOSITORY                    TAG       IMAGE ID       CREATED         SIZE
nginx                         latest    4b196525bd3c   5 weeks ago     197MB
wazuh/wazuh-dashboard         4.9.0     fcfcb7666272   8 weeks ago     1.11GB
wazuh/wazuh-indexer           4.9.0     eff9cefdfd03   8 weeks ago     2.38GB
wazuh/wazuh-manager           4.9.0     8d4a758947bf   8 weeks ago     1.28GB
<none>                        <none>    2719e8857200   2 months ago    67.2MB
<none>                        <none>    53fd24a4423f   2 months ago    62.6MB
mariadb                       10        8fa1e38a7eae   2 months ago    388MB
ghcr.io/digininja/dvwa        latest    49fc0a3269e8   3 months ago    518MB
wazuh/wazuh-certs-generator   0.0.2     60d428874d3a   7 months ago    139MB
```

Ahora intentamos iniciar un contenedor exponiendo los puertos TCP 80 (HTTP) y TCP 443 (HTTPS).

```
andresariasmedina@Andress-MacBook-Pro ~ % docker run --name webserver -d -p 80:80 -p 443:443 nginx:latest
cce13535f6465e13c4c9de45d4cae6783ecccf6ec6f3b8fbc346a8ef4b705ab9
docker: Error response from daemon: driver failed programming external connectivity on endpoint webserver (3c9b3ef0827cbd1e5b7ae1
5f3b84f2dd6577e254975320d19460a69966fb2b96): Bind for 0.0.0.0:443 failed: port is already allocated.
andresariasmedina@Andress-MacBook-Pro ~ % sudo lsof -i :443
```

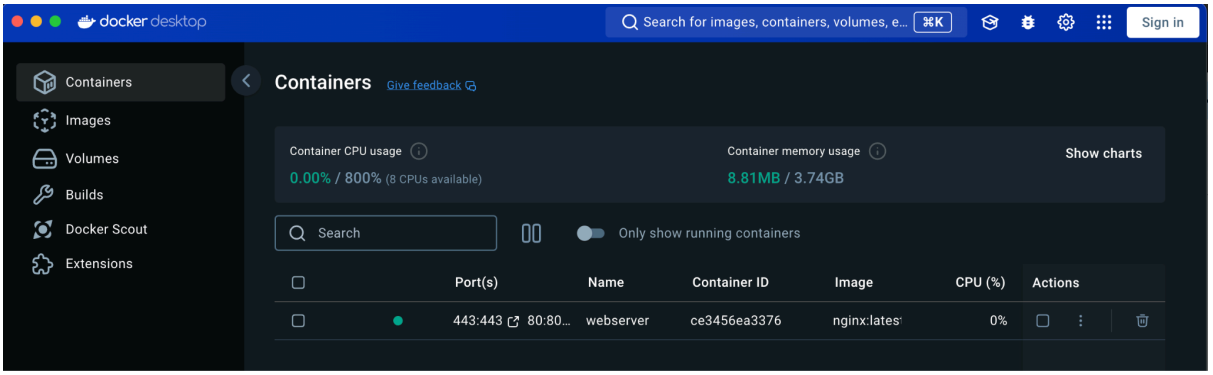
El error que salió indica que el puerto 443 no puede asignarse debido a que ya se encuentra en uso. Así que se procede a verificar cual contendor lo tiene en uso para suspenderlo o eliminarlo si este ya no se necesita.

En mi caso personal tenía algunos contenedores corriendo de forma innecesaria, entre ellos algunos usados para laboratorios anteriores entonces decidí eliminarlos. Además, suspendí varios procesos vinculados al localhost para liberar procesamiento, como Nessus.

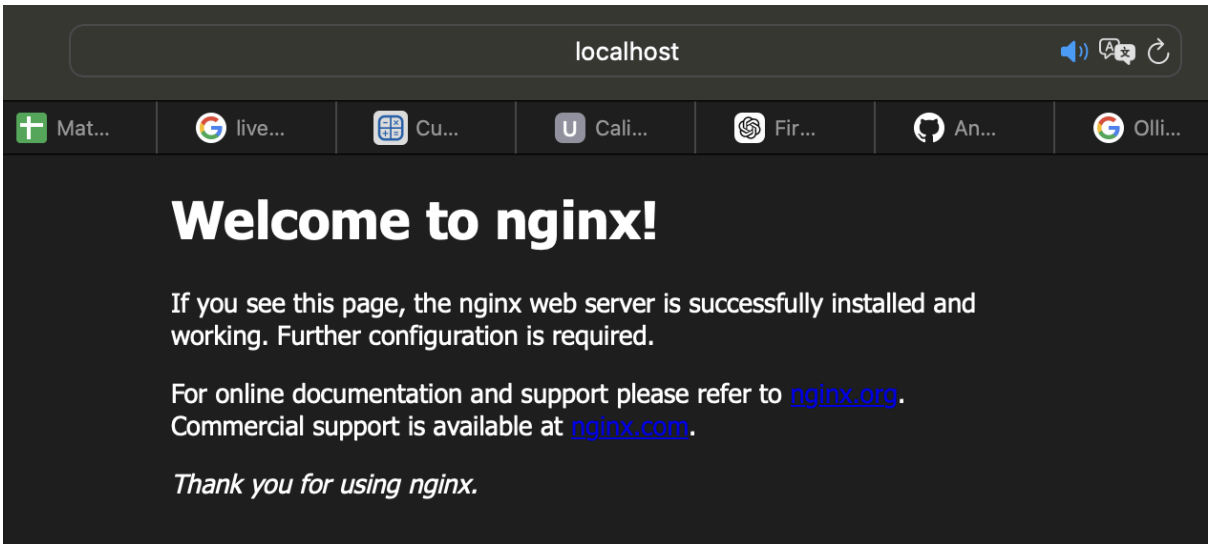
Luego de esto se vuelve a correr la línea para crear el contenedor de web server.

```
andresariasmedina@Andress-MacBook-Pro ~ % docker run --name webserver -d -p 80:80 -p 443:443 nginx:latest
ce3456ea3376d76c4586a4bbdf800ac4cc236e753f970234ca6db34636737674
```

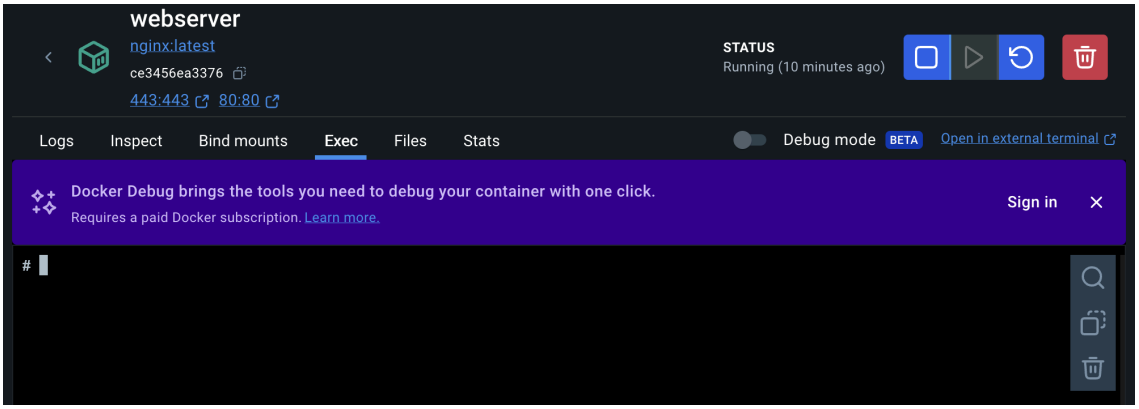
```
andresariasmedina@Andress-MacBook-Pro ~ % docker container ls -a
CONTAINER ID   IMAGE          COMMAND                  CREATED          STATUS          PORTS                                      NAMES
ce3456ea3376   nginx:latest   "/docker-entrypoint.…"   41 seconds ago   Up 40 seconds   0.0.0.0:80->80/tcp, 0.0.0.0:443->443/tcp   webserver
```



Para verificar la instalación y que todo haya quedado correctamente accedemos a un browser y nos dirigimos al localhost del puerto 80: http://localhost



Luego desde Docker Desktop nos dirigimos al contenedor y buscamos la consola de ejecución.
Nombre del contenedor >> Exec



En esta consola se ejecuta ***apt-get update*** & ***apt-get install vim*** para actualizar librerías e instalar un editor de texto que puede ser necesario.

```
# apt-get update
Hit:1 http://deb.debian.org/debian bookworm InRelease
Hit:2 http://deb.debian.org/debian bookworm-updates InRelease
Hit:3 http://deb.debian.org/debian-security bookworm-security InRelease
Reading package lists... Done
#apt-get install vim
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libgpm2 libsodium23 vim-common vim-runtime xxd
Suggested packages:
  gpm ctags vim-doc vim-scripts
The following NEW packages will be installed:
  libgpm2 libsodium23 vim vim-common vim-runtime xxd
0 upgraded, 6 newly installed, 0 to remove and 19 not upgraded.
```

Con el siguiente comando crearemos el certificado y la clave privada.
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/clave-privada.key -out /etc/ssl/certs/certificado-publico.crt

```
# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/clave-privada.key -out /etc/ssl/certs/certificado-publi
co.crt
...+..+....+.....+.............+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.................+..+....+..
+...+....++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.+.+...+..+.......+......+.....+.+...+...........+.....+..
..+..........+.+........+.+.................+..........+.......+..+.........+..........+.........+......+.+.....+.+.............
.+.....+...+.......+.........+...+...+...+..+...+.....+....+.........+..+...+.+.....+.........+.....+.......+........+.+.............
..+.+...+.....+.......+...+..+....+..+...+....+.....................+.......+...+..+.......+...+..+...+.......+.....+......+........
.+.+.........+...++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.+.......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*....+...+..++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++*.+.+......+..........+...+.+.....+......+...+..........+.....+....+...+................+.+......+...+...+..+.+....
.+.+.....+.................+...+....+......+..+...+....+......+.............+.+..+.+..........+......+...+.......+..+.+.........+..
+.+...+..............+..+...+.+.....+.+..+.......+.....+....+..............+......+...++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++
-----
```

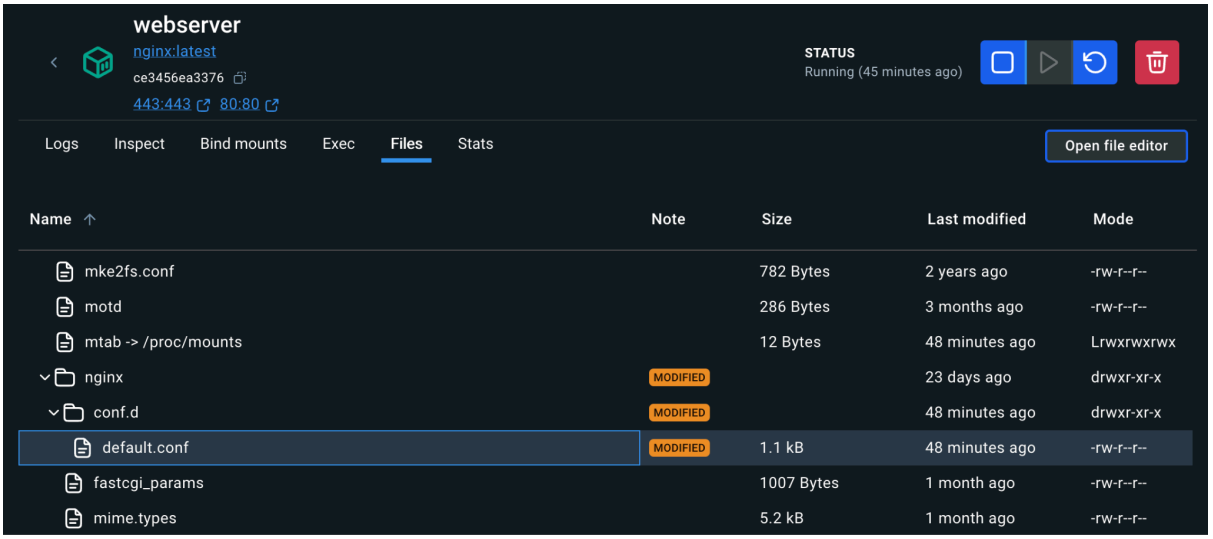
Se llenan los datos a continuación para el certificado.

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CO
State or Province Name (full name) [Some-State]:Antioquia
Locality Name (eg, city) []:Medellin
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UPB
Organizational Unit Name (eg, section) []:Seguridad Datos
Common Name (e.g. server FQDN or YOUR name) []:localhost
Email Address []:andres.ariasm@upb.edu.co
```

Lo que sigue es comprobar si el certificado y clave privada se crearon en los directorios correspondientes dentro de la misma consola.

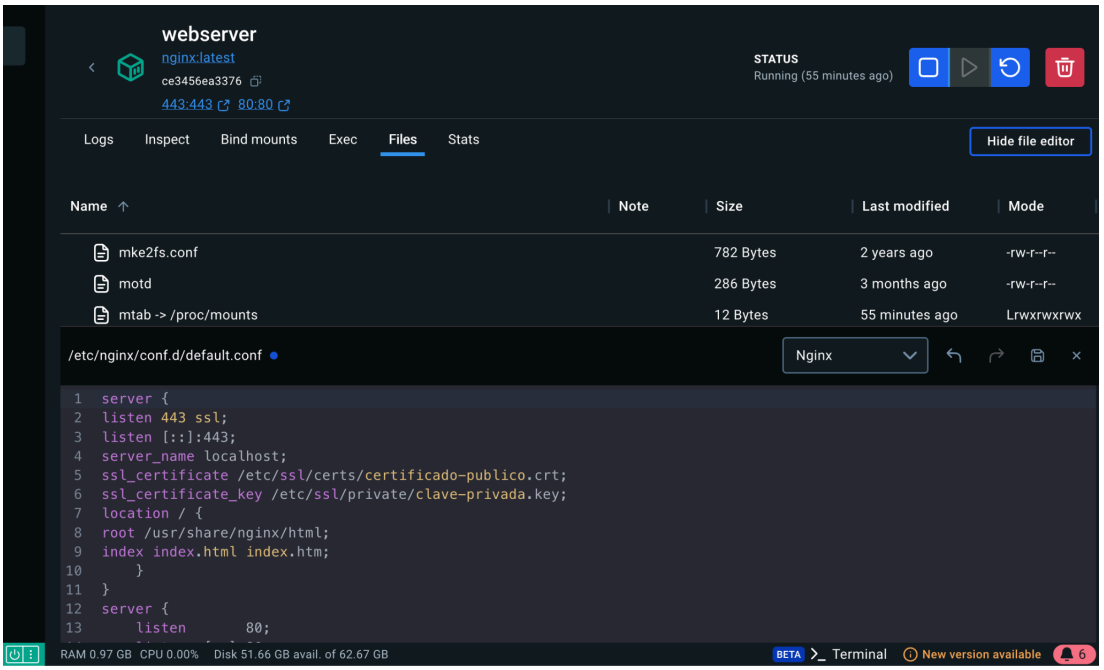
```
# ls /etc/ssl/certs | grep certificado-publico
certificado-publico.crt
# ls /etc/ssl/private | grep clave-privada
clave-privada.key
```

A continuación identificamos el archivo en la siguiente ruta: /etc/nginx/conf.d/default.conf y abrimos el editor de la parte superior derecha.

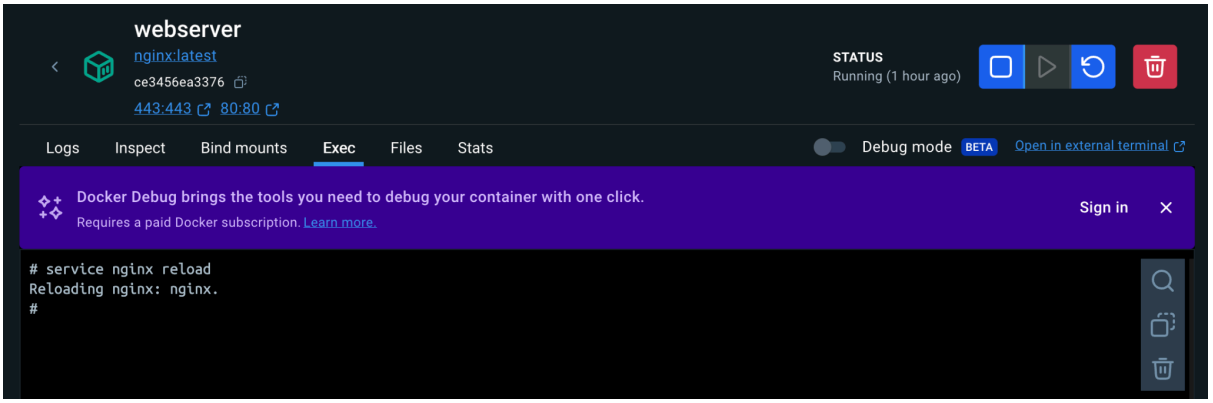


Con el editor abierto añadimos al comienzo las siguientes líneas para habilitar conexiones seguras por el puerto 443 (HTTPS) para el servicio de nginx.

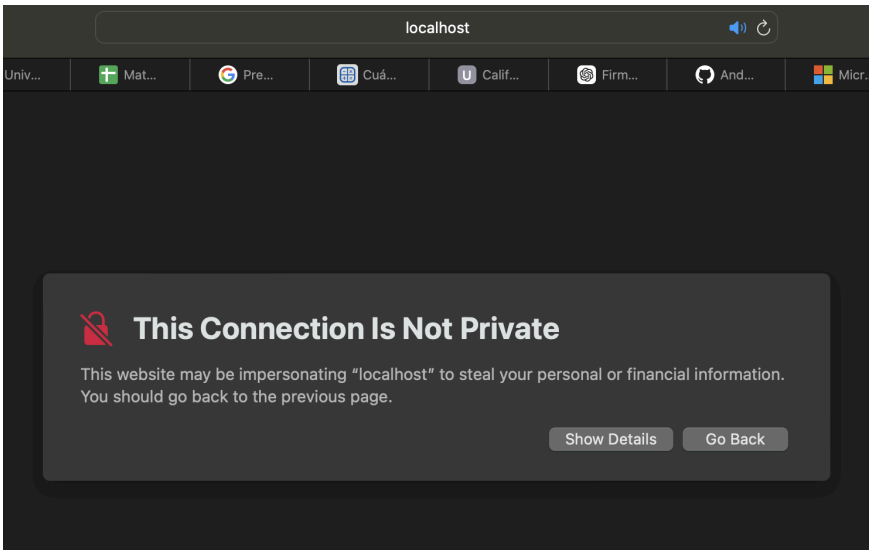
```
server {
listen 443 ssl;
listen [::]:443;
server_name localhost;
ssl_certificate /etc/ssl/certs/certificado-publico.crt;
ssl_certificate_key /etc/ssl/private/clave-privada.key;
location / {
root /usr/share/nginx/html;
index index.html index.htm;
        }
}
```



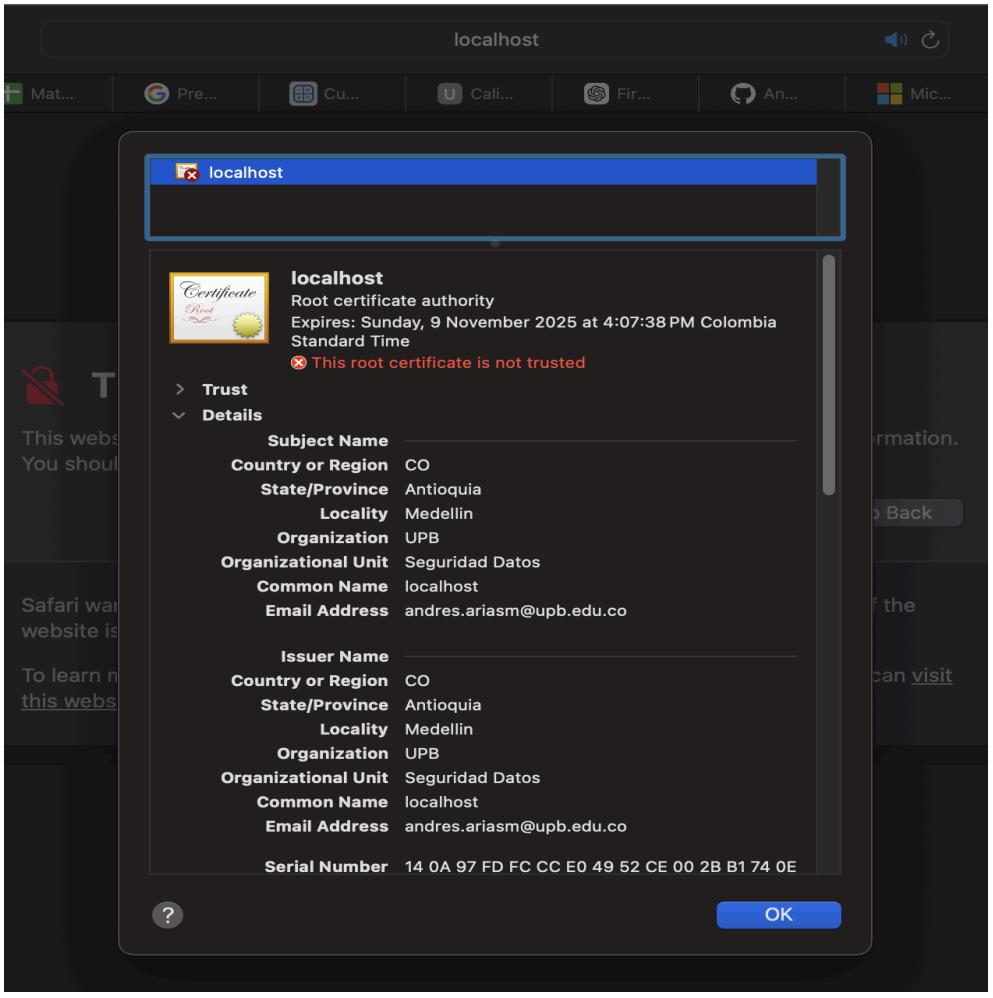
Guardamos cambios y cerramos esa pestaña. Volvemos a la consola Exec y reiniciamos al servicio para ver los cambios.



Ingresamos esta vez a https://localhost para ver los cambios usando el protocolo HTTPS por el puerto 443 de nuestro localhost.



Cuando intentamos visualizar el certificado marca que la conexión no es segura y que este certificado no es confiable.



El mensaje que indica que no es una conexión segura a pesar de tener un certificado se debe a que este certificado es auto-firmado. Esto significa que no fue emitido por una autoridad de certificación (CA) reconocida, por lo que los navegadores no confían automáticamente en él. Los certificados auto-firmados carecen de la cadena de confianza que los navegadores requieren para validar que una conexión es segura y auténtica. Para evitar esta advertencia se debe agregar el certificado a la lista de entidades de confianza de nuestro sistema o navegador, aunque esta medida es aceptable para entornos de desarrollo, no es recomendada para producción.