

# atividade SAN

## 1. Como funciona SAN

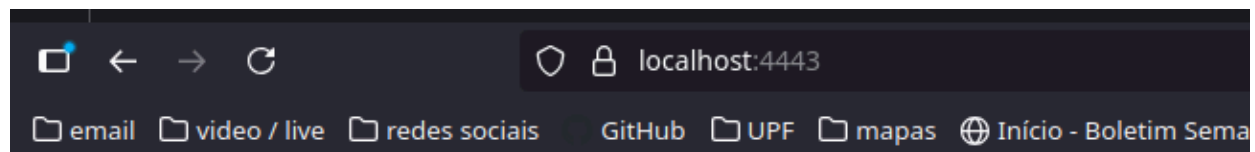
- O campo Subject Alternative Name (SAN) do certificado lista nomes alternativos válidos para o certificado (DNS names e IPs).
- Browsers e clientes HTTPS verificam SAN e ignoram o CN (Common Name) para checagem de host: o nome do host (ou IP) que você usa na URL deve estar presente em SAN.
- Para resolver o problema: o certificado do servidor precisa conter DNS:localhost e IP:127.0.0.1 no SAN. Assim conexões por localhost e por 127.0.0.1 serão aceitas.

## 2. Evidências:

```
:calling stat(server.key)
(.venv) enzo@enzo-Inspiron-15-3520:~/repos/CA-2025-2/aula3$ openssl req -new -key ACRaiz.key
-out 186665.csr -config san.cnf
```

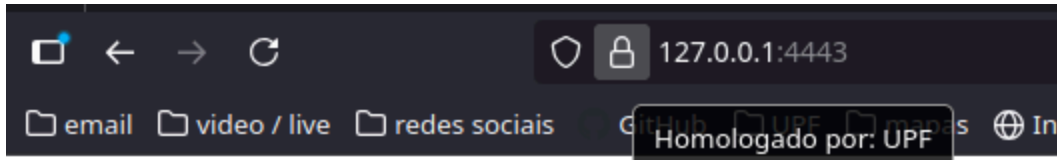
```
(.venv) enzo@enzo-Inspiron-15-3520:~/repos/CA-2025-2/aula3$ openssl x509 -req \
-in 186665.csr \
-CA ACRaiz.crt \
-CAkey ACRaiz.key \
-CAcreateserial \
-out server.crt \
-days 365 \
-sha256 \
-extfile san.cnf \
-extensions req_ext
Certificate request self-signature ok
subject=C = BR, ST = SP, L = Sao Paulo, O = MinhaOrg, OU = MinhaUnidade, CN = localhost
(.venv) enzo@enzo-Inspiron-15-3520:~/repos/CA-2025-2/aula3$ openssl x509 -in server.crt -noout -text
```

```
001:00E1:0017: [X509: KEY_VALUES_INFORMATION] Key Values Information ([001:0.0.0.0])
(.venv) enzo@enzo-Inspiron-15-3520:~/repos/CA-2025-2/aula3$ python servidor.py
Servidor HTTPS rodando em https://localhost:4443
127.0.0.1 - - [31/Oct/2025 14:16:52] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [31/Oct/2025 14:16:52] code 404, message File not found
127.0.0.1 - - [31/Oct/2025 14:16:52] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [31/Oct/2025 14:17:00] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [31/Oct/2025 14:17:00] code 404, message File not found
127.0.0.1 - - [31/Oct/2025 14:17:00] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [31/Oct/2025 14:17:24] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [31/Oct/2025 14:17:25] code 404, message File not found
127.0.0.1 - - [31/Oct/2025 14:17:25] "GET /favicon.ico HTTP/1.1" 404 -
```



## Directory listing for /

- [186665.crt](#)
- [186665.csr](#)
- [ACRaiz.crt](#)
- [ACRaiz.key](#)
- [ACRaiz.srl](#)
- [desafios\\_certificados/](#)
- [meu-servidor.crt](#)
- [private.key](#)
- [san.cnf](#)
- [server.crt](#)
- [servidor.py](#)



# Directory listing for /

---

- [186665.crt](#)
  - [186665.csr](#)
  - [ACRaiz.crt](#)
  - [ACRaiz.key](#)
  - [ACRaiz.srl](#)
  - [desafios\\_certificados/](#)
  - [meu-servidor.crt](#)
  - [private.key](#)
  - [san.cnf](#)
  - [server.crt](#)
  - [servidor.py](#)
-