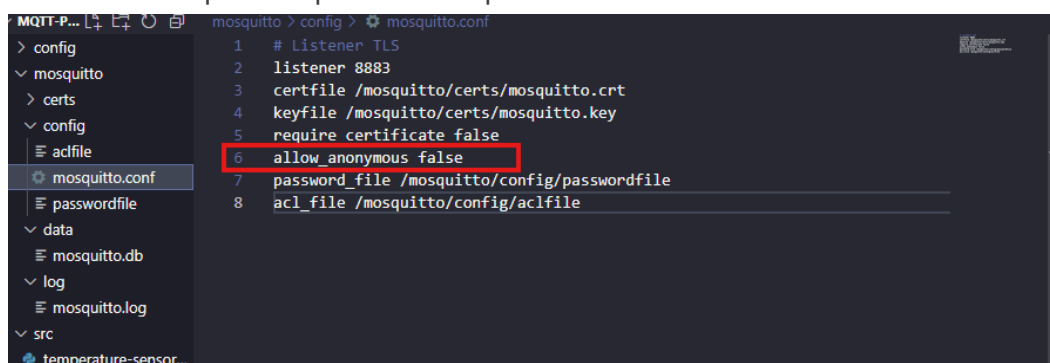


Atividade - Exploração e correção de vulnerabilidades MQTT Broker

Victor Djalma

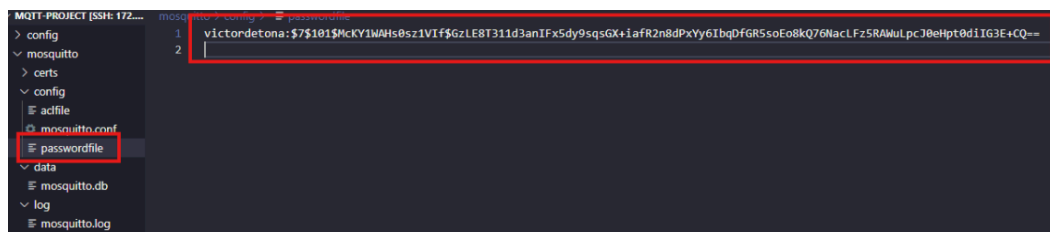
Identifique três vulnerabilidades principais presentes no projeto (exemplos possíveis: uso de comunicação não criptografada, autenticação fraca, tópicos abertos/vulneráveis, falhas de parsing, DoS, etc.).

Foi identificado 3 vulnerabilidades, a configuração do Broker estava acessível para qualquer usuário então o primeiro passo foi bloquear essa variável



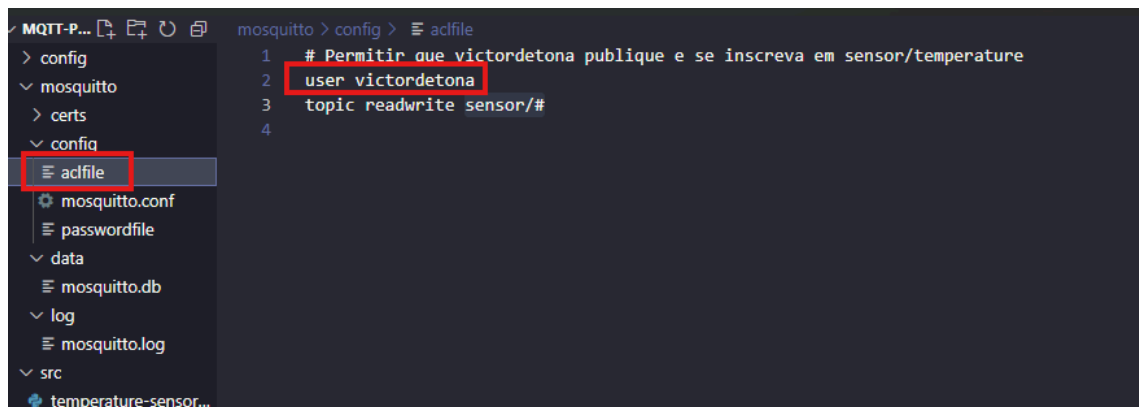
```
mosquitto > config > mosquitto.conf
1 # Listener TLS
2 listener 8883
3 certfile /mosquitto/certs/mosquitto.crt
4 keyfile /mosquitto/certs/mosquitto.key
5 require_certificate false
6 allow_anonymous false
7 password_file /mosquitto/config/passwordfile
8 acl_file /mosquitto/config/aclfile
```

A próxima configuração foi configurar um user para acessar o BROKER, criando um arquivo chamado passwordfile onde nele está o USER criado (victordetona) e a senha configurada em HASH



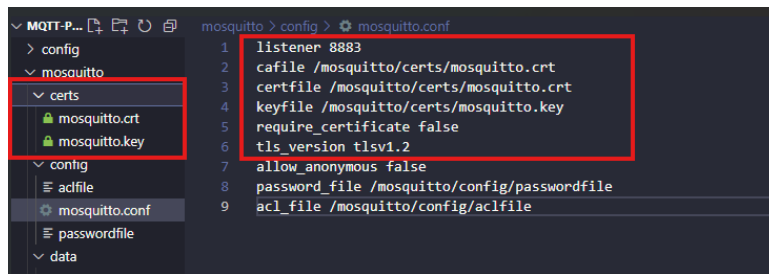
```
mosquitto > config > passwordfile
1 victordetona:$7$101$McKY1WAHs0sz1VIf$GzLE8T311d3anIfx5dy9sqSGX+1afR2n8dPxYy6TbqDFGR5soEo8kQ76NaCLFz5RAWuLpcJ8eHpt0diIG3E+CQ==
2
```

Próxima configuração vai ser criar a ACL, uma lista de controle que permite que somente o USER (victordetona) faça publisher

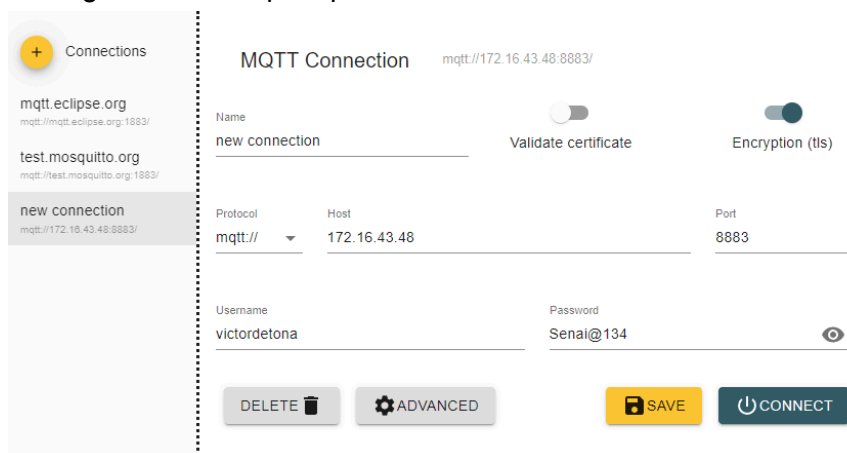


```
mosquitto > config > aclfile
1 # Permitir que victordetona publique e se inscreva em sensor/temperature
2 user victordetona
3 topic readwrite sensor/#
4
```

Depois de configurar todos esses parâmetros precisamos realizar a ultima configuração para ficar seguro, que seria a criptografia com TLS, criamos um novo diretório e dentro criei a key e o certificado de criptografia, e no mosquitto.conf você configura os certificados .crt e .key



Depois o BROKER vai estar configurado apenas para o USER (victordetona) e só conseguirá acessar pela porta 8883



Com o erro que estava dando no TLS NOT FOUND, resolvi trocar a conexão externa para a porta 8883, e a conexão do subscriber para a 1883, então como não necessitava desse TLS

