CYBERSECURITY

VULNERABILIDADES

1. COMUNICAÇÃO NÃO SEGURA
2. FALTA DE AUTENTICAÇÃO E CONTROLE DE ACESSO
3. BANCO DE DADOS SEM SEGURANÇA

COMUNICAÇÃO NÃO SEGURA

- MQTT E HTTP SEM CRIPTOGRAFIA, VULNERÁVEIS A INTERCEPTAÇÕES (MAN-IN-THE-MIDDLE)

- A COMUNICAÇÃO MQTT NÃO UTILIZA TLS/SSL, EXPONDO AS MENSASGENS A ATAQUES DE INTERCEPTAÇÃO

FALTA DE AUTENTICAÇÃO E CONTROLE DE ACESSO

- O dashboard não tem verificação de login ou autenticação de usuário, permitindo que qualquer pessoa acesse os dados sem controle de acesso.
- A falta de autenticação também possibilita que um atacante manipule os dados ou envie comandos falsificados ao sistema.
- Ausência de controle de acesso granular: Todos os usuários podem acessar os mesmos níveis de dados e comandos, aumentando o risco de uso indevido ou acesso não autorizado.

BANCO DE DADOS SEM PROTEÇÃO

injeção de SQL: Um atacante pode manipular consultas ao banco de dados para obter informações ou alterar registros.

-**Roubo de Dados:** Sem criptografia, um invasor pode acessar dados diretamente do banco em caso de acesso não autorizado.

COMO MITIGAR?

HTTP ---> HTTPS

Implementar HTTPS para toda a comunicação entre o ESP32 e o servidor

MQTT ---> TLS/SSL

Configurar o protocolo MQTT com TLS/SSL para proteger as mensagens transmitidas.

Injeção SQL ---> Autenticação

Extração de dados --> criptografia do banco de dados

Força bruta --> ataques múltiplos de tentativas de credenciais

JÁ TÁ PODENDO?