Problemas de Segurança Detectados e Recomendações

SQL Injection no Endpoint de Login

Descrição: O endpoint /login é vulnerável a um ataque de injeção SQL devido à natureza direta do nome de usuário e da senha na consulta SQL.

Observação: Usar instruções preparadas ou criar funções para criar consultas SQL e evitar injeções maliciosas.

Exposição de Dados Sensíveis no Endpoint de Listagem de Usuários

Descrição: O endpoint /users retorna todos os usuários com id, nome de usuário e senha mostrando informações relevantes do usuário

Recomendação: Remova o campo password da resposta deste endpoint para garantir a segurança dos dados dos usuários.

Exposição de Senha no Endpoint de Detalhes do Usuário

Descrição: O nome de usuário refere-se ao seu nome de usuário completo, incluindo a senha da sua conta.

Recomendação: Remover a senha do último evento para garantir a segurança dos dados do usuário.