SQL Injection no Endpoint de Login

Descrição: O endpoint /login está suscetível a ataques de SQL Injection devido à forma direta como os campos de nome de usuário e senha são utilizados na consulta SQL.

Recomendação: Utilize instruções preparadas ou funções de construção de consultas para mitigar a possibilidade de injeção de código malicioso.

Exposição de Dados Sensíveis no Endpoint de Listagem de Usuários

Descrição: O endpoint /users expõe informações sensíveis ao retornar todos os usuários com seus respectivos id, nome de usuário e senha.

Recomendação: Remova o campo de senha da resposta deste endpoint para assegurar a proteção dos dados dos usuários.

Exposição de Senha no Endpoint de Detalhes do Usuário

Descrição: O endpoint /profile expõe a senha do usuário ao retornar todas as informações, incluindo o nome de usuário.

Recomendação: Remova a exposição da senha nesse endpoint para garantir a segurança dos dados dos usuários.