SEGURANÇA COM API

Envio de E-mail inválido por não ser o mesmo armazenado no banco, o token não foi gerado e foi apresentada uma mensagem de tratamento de erro (Figura 1).

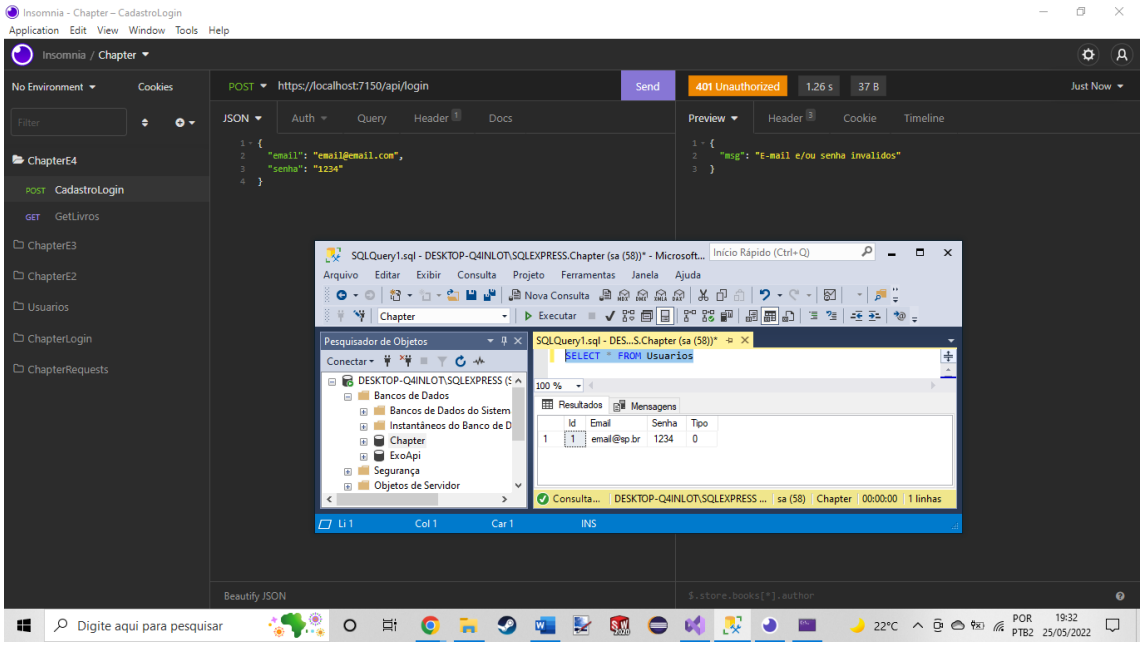

Figura 1 – envio de informações inválidas.

Envio de E-mail válido que condiz com o que está armazenado no banco. As informações foram validadas e o token foi gerado (Figura 2).

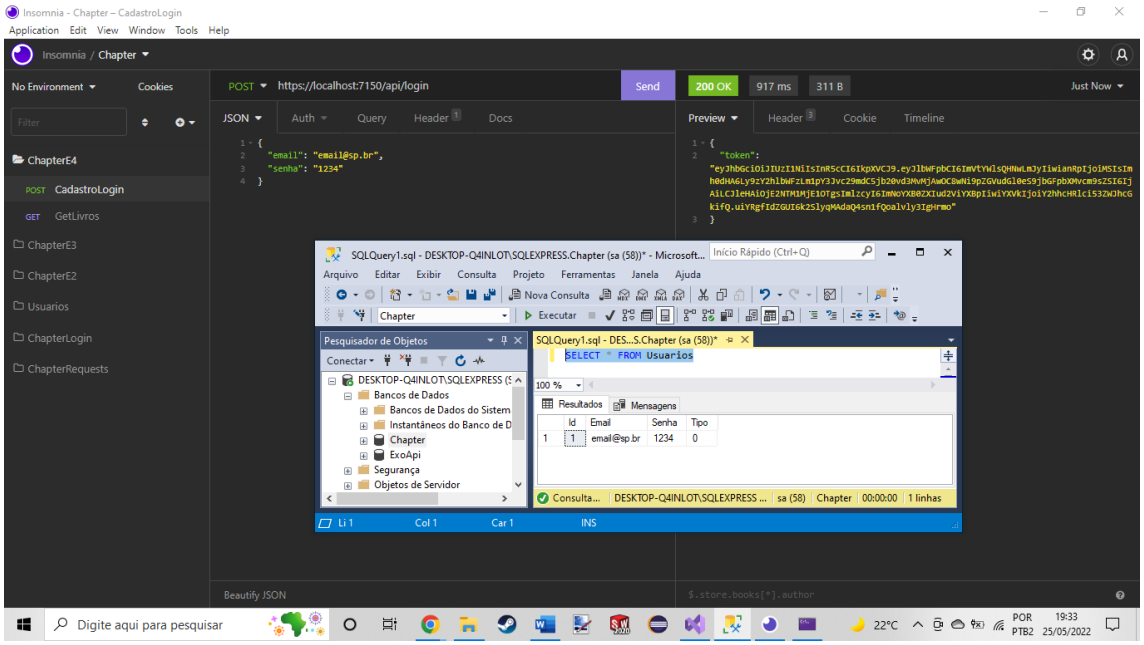

Figura 2 – Envio de informações válidas resultando na formação de token.

Tentativa de executar a requisição Get sem validar o usuário. Foi encaminhado um retorno 401 que indica que a ação não está autorizada para o requisitante (Figura 3).

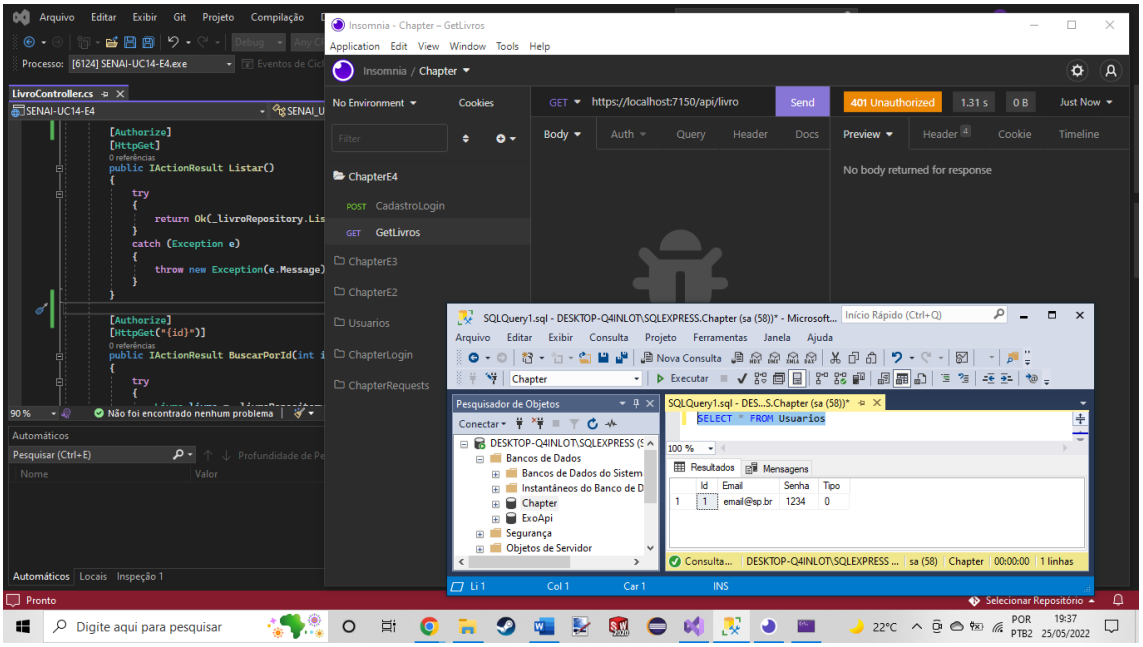

Figura 3 – requisição não autorizada.

Com o envio do token, a requisição foi autorizada por ser um usuário autorizado. Tal ação foi feita devido a geração de uma chave simétrica que pode ser codificada na validação do usuário e decodificada na execução da requisição. No entanto, chaves simétricas são fáceis de serem atacadas pela técnica da força bruta (Figura 4).

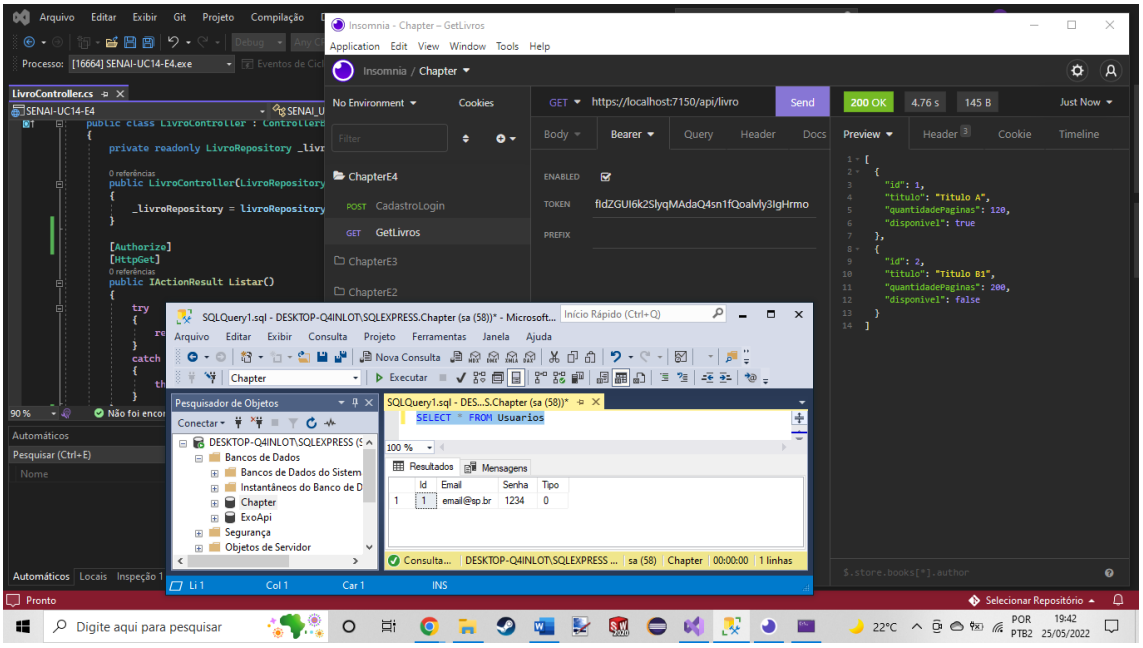

Figura 4 – requisição Get autorizada com a utilização do token.

Tentativa de utilizar a requisição delete para apagar a linha com o id 2 da entidade Livros do banco. Foi retornado um 401 pois o usuário não está autorizado (Figura 5).

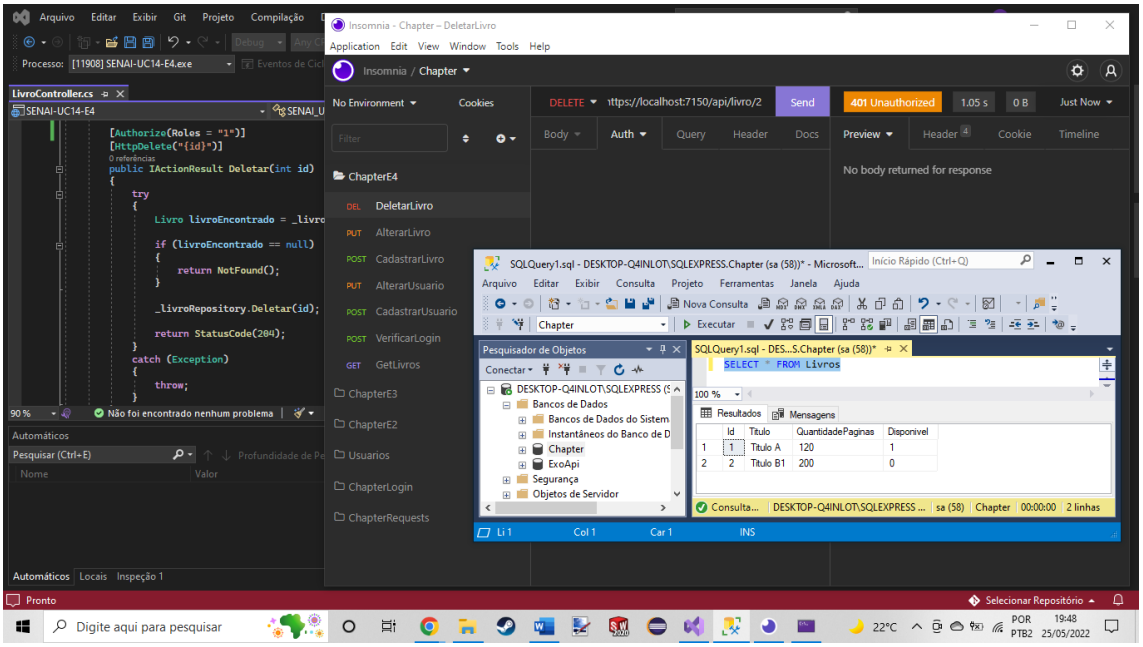

Figura 5 – requisição delete feita por usuário não autorizado.

Utilizando o token do usuário que foi validado a requisição delete não foi concluída. Isso ocorreu pois o usuário está com o tipo 0 armazenado no banco, apenas tipo 1 está autorizado, desta forma, a mensagem de erro foi a 403 que retorna um proibido para o requisitante (Figura 6).

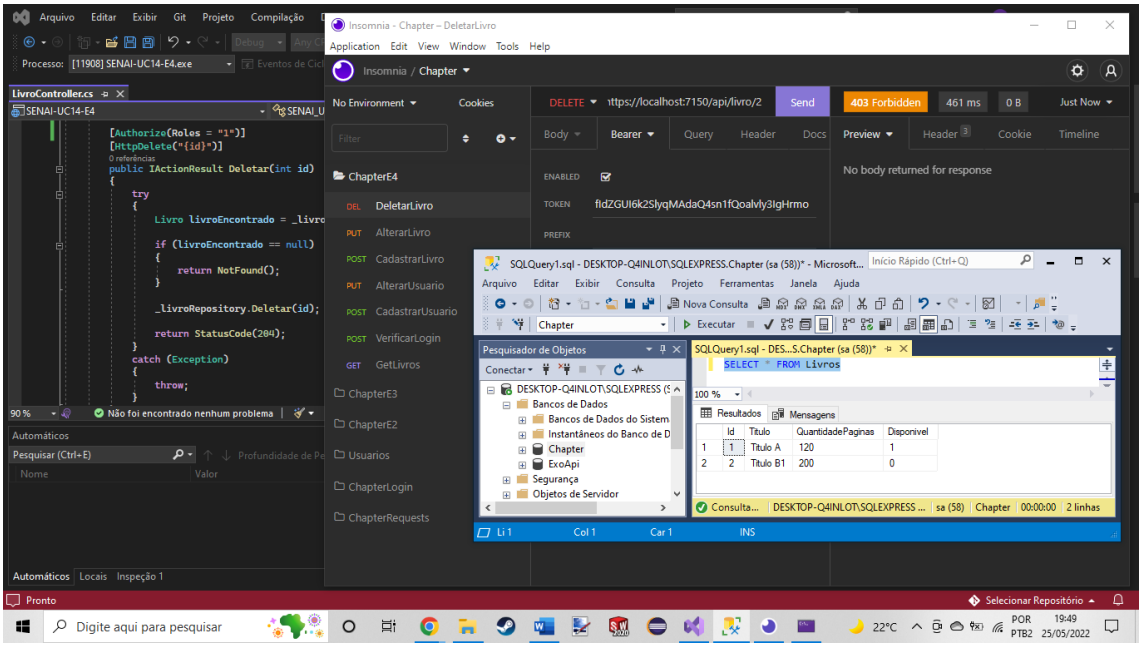

Figura 6 – usuário validado porém não permitido a fazer a requisição delete.

Foi criado um novo usuário através da requisição post em api/usuarios, foi passado a informação tipo 1 no corpo da requisição JSON (Figura 7).

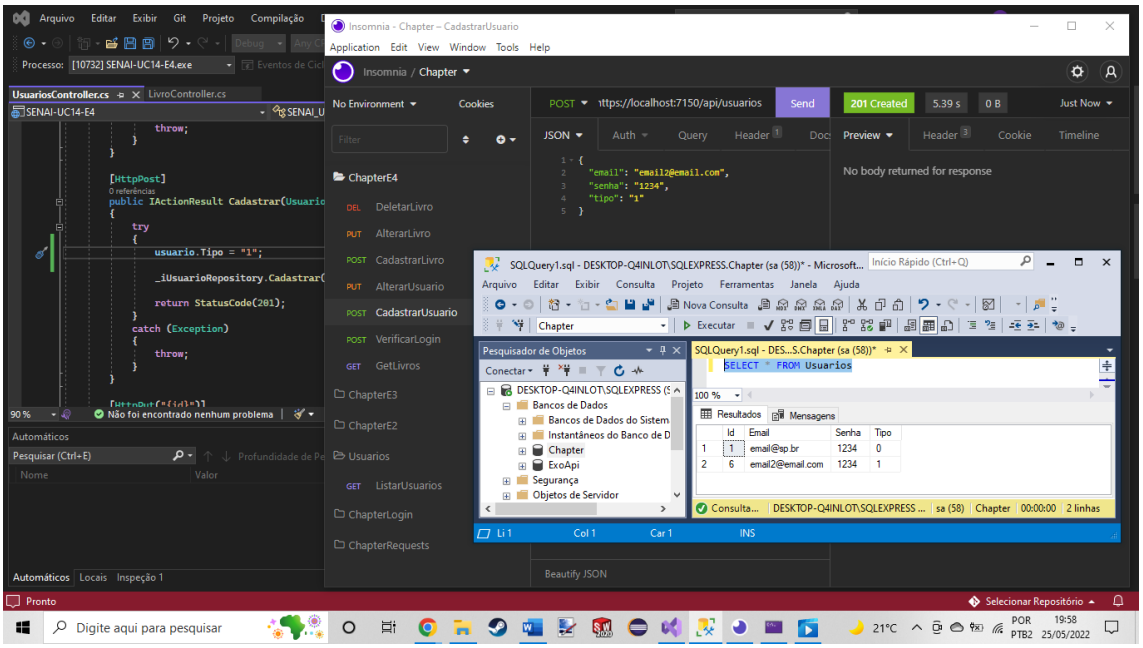

Figura 7 – requisição post em api/usuarios.

Foi criado um novo usuário através da requisição post em api/usuarios, desta vez, não foi passada a informação tipo, pois isto está configurado no método Cadastrar, como pode ser verificado na Figura 8.

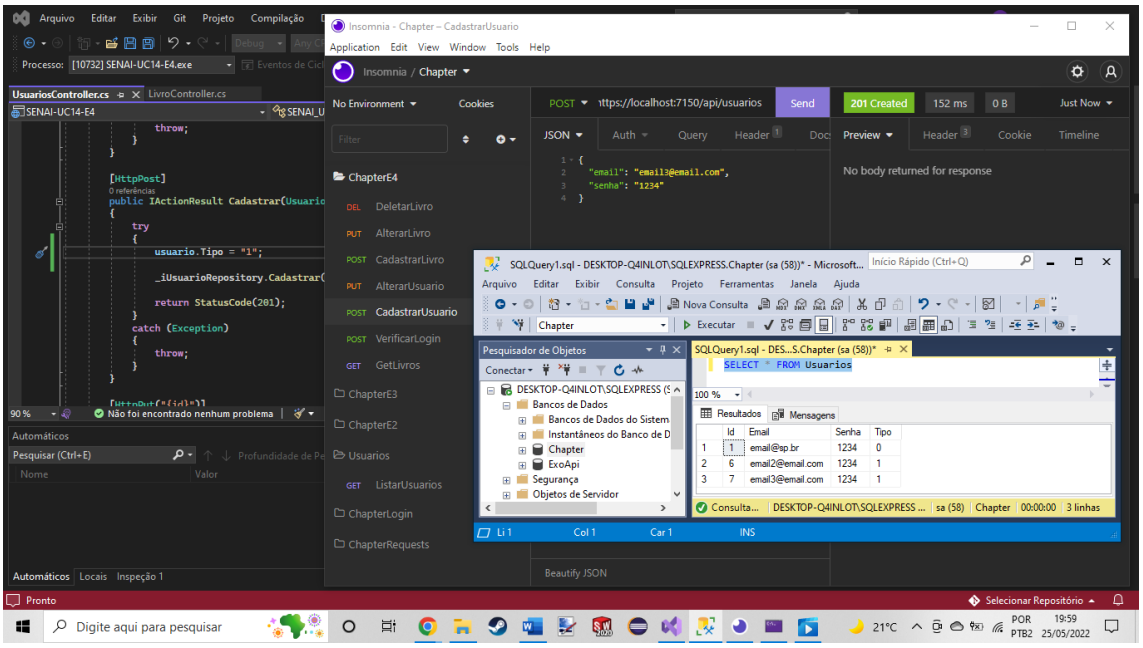

Figura 8 – usuário criado em api/usuarios, o tipo foi atribuído de acordo com a configuração.

O novo usuário com o tipo 1 foi validado e o token foi gerado (Figura 9).

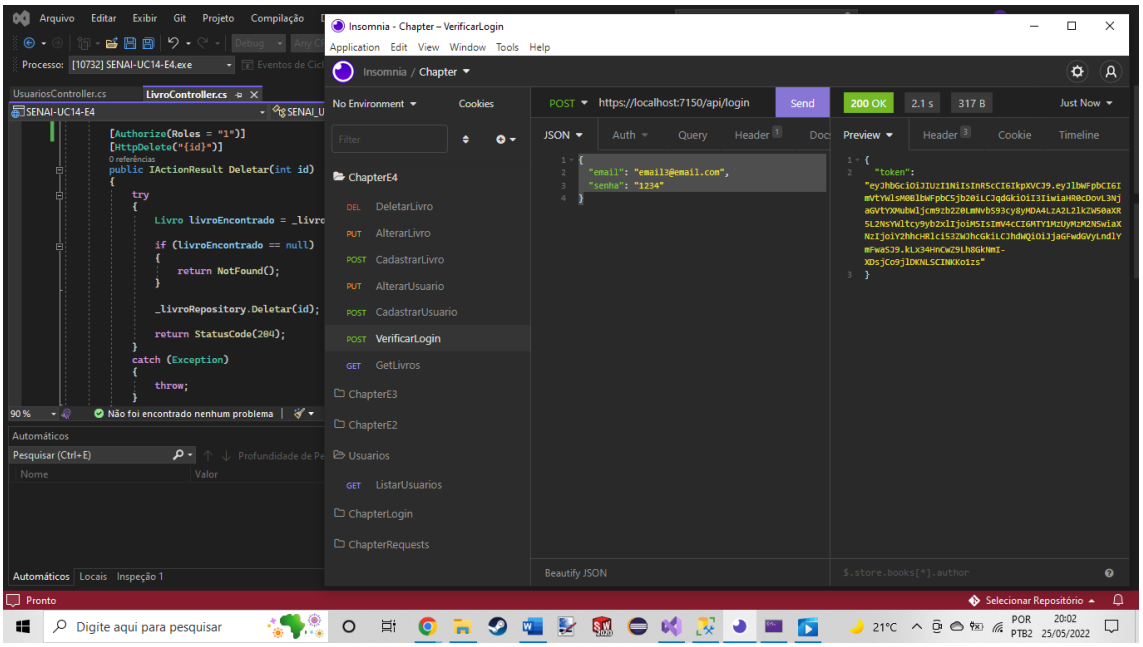

Figura 9 – token gerado para o novo usuário tipo 1.

Desta vez, o token foi passado no corpo da requisição, ao ser decodificado, o usuário foi reconhecido, por ser um usuário tipo 1, a requisição delete em api/livro/2 foi autorizada e a linha com o id 2 da entidade Livros foi excluída (Figura 10).

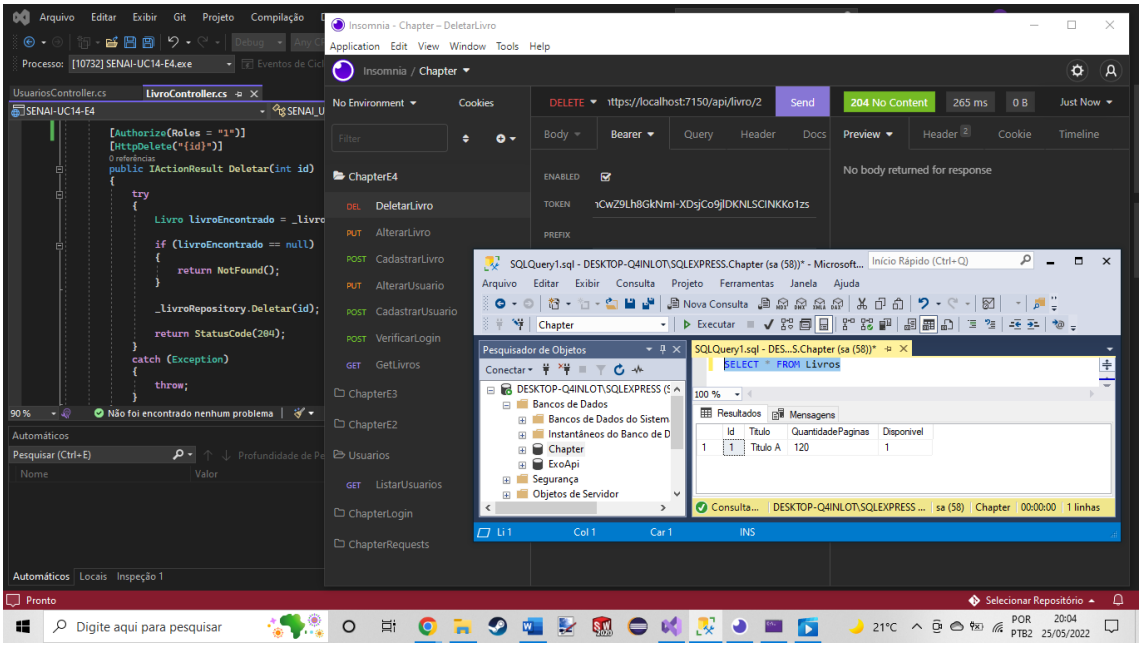

Figura 10 – requisição delete autorizada para usuário tipo 1.