Report de bug - Ana - ID: 240

Título

[Place an order] API aceita quantidade negativa no `POST /store/order`. Compromete estoque e abre margem para ataques maliciosos.

Descrição

A API do endpoint `POST /store/order` aceita valores negativos no campo `quantity`. Assim, ao clicar em “Send” no Postman, a API responde com o código `200 OK`, que indica que a operação foi completada com sucesso, e com as informações enviadas no “Body”, confirmando a ação incorreta.

Esse tipo de comportamento é prejudicial para o sistema de estoque pois pode diminuir itens indevidamente da lista de inventário. Com isso, faz com que ele seja vulnerável a ataques maliciosos, já que qualquer pessoa pode reduzir itens do estoque facilmente, o que pode gerar inconsistências nos dados e bloquear vendas de outros clientes.

Passos para reprodução

1. Utilizar a ferramenta Postman
2. Criar uma nova requisição `POST`
3. Adicionar a URL `{{url}}/store/order`, considerando que url = https://petstore3.swagger.io/api/v3
4. Adicionar o seguinte código JSON (ou qualquer um que tenha valor `quantity` negativo) no “Body”:

```
{
  "id": 10,
  "petId": 198772,
  "quantity": -11,
  "shipDate": "2025-05-02T03:50:43.627Z",
  "status": "approved",
  "complete": true
}
```

5. Clicar em “Send”

Comportamento Esperado

A API deveria validar que o valor de `quantity` é um número positivo ou igual a 0. Caso contrário, deveria retornar um erro `400 Bad Request` para deixar claro que o input inserido é inválido.

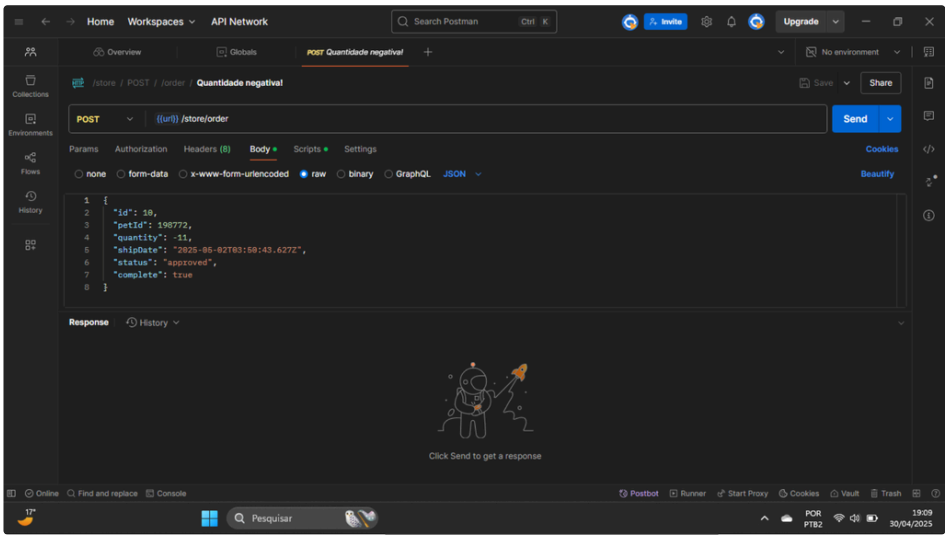
Comportamento Atual

A API permite que o valor de `quantity` seja um número negativo, retornando `200 OK` e aceitando o erro.

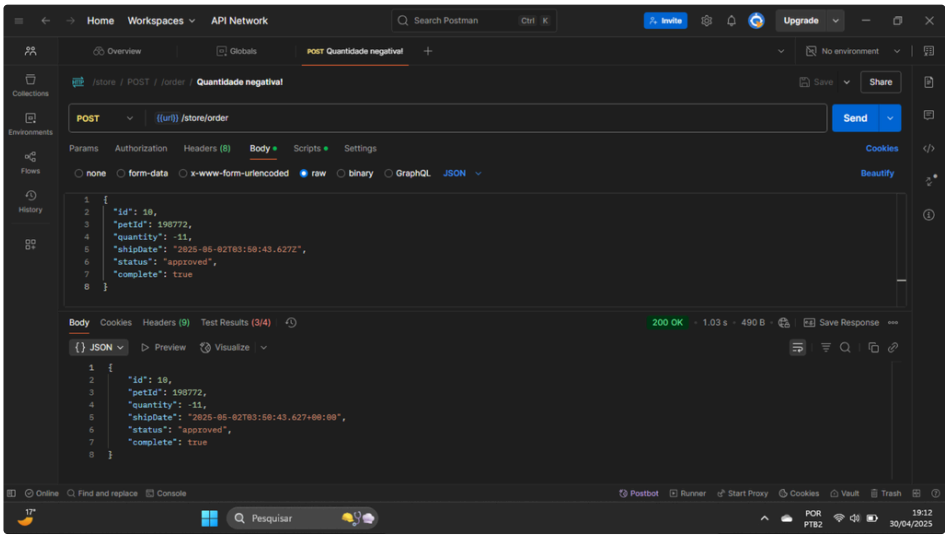
Ambiente

- API: https://petstore3.swagger.io/api/v3
- Documentação da API: https://petstore3.swagger.io/
- Ferramenta: Postman
- Ambiente: Produção
- Navegador: Microsoft Edge
- Sistema Operacional: Windows 11

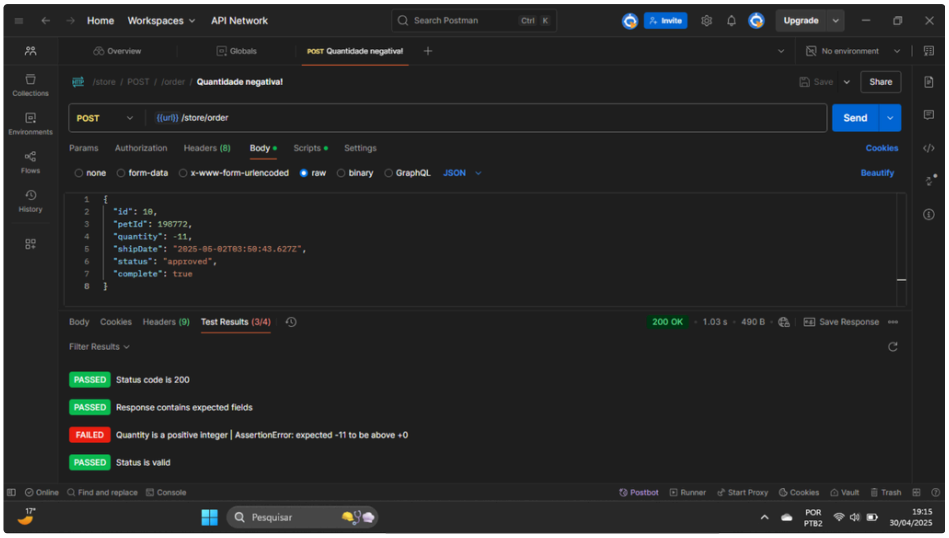
Evidências



“Body” com código JSON adicionado na requisição `POST` com a URL `{{url}}/store/order`



Resposta da API após clicar no “Send”



Resultado dos testes realizados mostrando que a quantidade adicionada é negativa

Notas

- A API precisa de uma validação no valor de `quantity` para ter certeza que é um número positivo ou igual a 0, já que representa um número de itens.
- Os valores adicionados no campo `quantity` alteram os valores das quantidades dos status em `GET /store/inventory`.