DBC, Módulo de API (Postman)

QA, Rafael Linhares e Vitor Poeta

---

1. Documentação de Cenários de Teste (Gherkin)

Funcionalidade: Autenticação de Usuário (Login)

Endpoint: POST /login

- **Cenário 01: Login com credenciais válidas (Positivo)**
  - **Dado** que possuo um usuário cadastrado com email "rafael.postman@qa.com.br" e senha "1234".
  - **Quando** envio uma requisição POST para "/login" com essas credenciais.
  - **Então** o status da resposta deve ser **200 OK**.
  - **E** o corpo da resposta deve conter um token de autorização "Bearer".

- **Cenário 02: Login com senha incorreta (Negativo)**
  - **Dado** que possuo um usuário cadastrado com email "rafael.postman@qa.com.br".
  - **Quando** envio uma requisição POST para "/login" com a senha incorreta "senhaerrada".
  - **Então** o status da resposta deve ser **401 Unauthorized**.
  - **E** a mensagem de erro deve ser "Email e/ou senha inválidos".

- **Cenário 03: Login com formato de email inválido (Negativo)**
  - **Dado** que tento logar com um email sem formatação correta "https://www.google.com/search?q=emailsemarroba.com".
  - **Quando** envio uma requisição POST para "/login".
  - **Então** o status da resposta deve ser **400 Bad Request** (ou o erro de validação correspondente da API).

Funcionalidade: Cadastro de Usuários

Endpoint: POST /usuarios

- **Cenário 04: Cadastrar novo usuário administrador (Positivo)**
    - **Dado** que tenho dados de um novo usuário válido.
    - **Quando** envio uma requisição POST para "/usuarios" com "administrador": "true".
    - **Então** o status da resposta deve ser **201 Created**.
    - **E** a mensagem deve ser "Cadastro realizado com sucesso".

- **Cenário 05: Cadastro com email duplicado (Negativo)**
    - **Dado** que já existe um usuário cadastrado com o email "rafael.postman@qa.com.br".
    - **Quando** tento cadastrar outro usuário com o mesmo email.
    - **Então** o status da resposta deve ser **400 Bad Request**.
    - **E** a mensagem deve ser "Este email já está sendo usado".

- **Cenário 06: Cadastro com campo obrigatório vazio (Negativo)**
    - **Dado** que tento cadastrar um usuário sem preencher a "password".
    - **Quando** envio a requisição POST para "/usuarios".
    - **Então** o status da resposta deve ser **400 Bad Request**.
    - **E** a API deve informar que o campo é obrigatório..

Funcionalidade: Cadastro de Produtos

Endpoint: POST /produtos

Pré-requisito: Usuário deve estar logado e ser administrador

- **Cenário 07: Cadastrar produto com sucesso (Positivo)**
    - **Dado** que estou autenticado com um token de usuário administrador.
    - **Quando** envio um POST para "/produtos" com nome "Teclado Postman", preco 150, descricao "Teclado Gamer" e quantidade 10.
    - **Então** o status da resposta deve ser **201 Created**.
    - **E** a mensagem deve ser "Cadastro realizado com sucesso".

- **Cenário 08: Cadastrar produto com nome duplicado (Negativo)**
    - **Dado** que estou autenticado e já existe um produto "Teclado Postman".
    - **Quando** tento cadastrar novamente um produto com nome "Teclado Postman".
    - **Então** o status da resposta deve ser **400 Bad Request**.
    - **E** a mensagem deve ser "Já existe produto com esse nome"

.

- **Cenário 09: Cadastrar produto sem Token de acesso (Negativo)**
    - **Dado** que não realizei login (sem token no Header).
    - **Quando** tento enviar um POST para "/produtos".
    - **Então** o status da resposta deve ser **401 Unauthorized**.
    - **E** a mensagem deve ser "Token de acesso ausente, inválido, expirado...".

Funcionalidade: Editar Produtos

Endpoint: PUT /produtos/ {_id}

Pré-requisito: Usuário deve estar logado e ser administrador

- **Cenário 10: Editar produto com sucesso (Positivo)**
    - **Dado** que estou autenticado com um token de usuário administrador.
    - **E** existe um produto cadastrado chamado “Logitech MX Vertical”.
    - **E** coloco o id do Logitech MX Vertical no campo “id do produto”.
    - **Quando** envio um PUT para "/produtos/{_id}", nome Logitech MX Vertical , preco 999, descricao "Mouse" e quantidade 381.
    - **Então** o status da resposta deve ser **200 OK.**
    - **E** a mensagem deve ser "Registro alterado com sucesso".

- **Cenário 11: Editar produto sem permissão de administrador (Negativo)**
    - **Dado** que estou autenticado com um token de usuário normal.
    - **E** existe um produto cadastrado chamado “Logitech MX Vertical”.
    - **E** coloco o id do Logitech MX Vertical no campo “id do produto”.
    - **Quando** envio um PUT para "/produtos/{_id}", nome Logitech MX Vertical , preco 1000, descricao "Mouse" e quantidade 199.
    - **Então** o status da resposta deve ser **403 Forbidden.**
    - **E** a mensagem deve ser "Rota exclusiva para administradores".

.

- **Cenário 12: Editar quantidade do produto para número negativo (Negativo)**
    - **Dado** que estou autenticado com um token de usuário administrador.
    - **E** existe um produto cadastrado chamado “Logitech MX Vertical”.
    - **E** coloco o id do Logitech MX Vertical no campo “id do produto”.
    - **Quando** envio um PUT para "/produtos/{_id}", nome Logitech MX Vertical , preco 999, descricao "Mouse" e quantidade -1.
    - **Então** o status da resposta deve ser **400 Bad Request.**
    - **E** a mensagem deve ser "Quantidade deve ser maior ou igual a 0".

Funcionalidade: Excluir Produtos

Endpoint: DELETE /produtos/ {_id}

Pré-requisito: Usuário deve estar logado e ser administrador

- **Cenário 13: Excluir produto com sucesso (Positivo)**
  - **Dado** que estou autenticado com um token de usuário administrador.
  - **E** existe um produto cadastrado chamado “Logitech MX Horizontal”.
  - **E** coloco o id do Logitech MX Horizontal no campo “id do produto”.
  - **Quando** envio um DELETE para "/produtos/{_id}"
  - **Então** o status da resposta deve ser **200 OK.**
  - **E** a mensagem deve ser "Registro excluído com sucesso".

- **Cenário 14: Excluir produto que não existe (Negativo)**
  - **Dado** que estou autenticado com um token de usuário normal.
  - **E** coloco o id de um produto inexistente no campo “id do produto”.
  - **Quando** envio um DELETE para "/produtos/{_id}"
  - **Então** o status da resposta deve ser **200 OK.**
  - **E** a mensagem deve ser "Nenhum registro excluído".

.

- **Cenário 15: Excluir produto sem Token de Acesso (Negativo)**
  - **Dado** que estou autenticado com um token de administrador inválido.
  - **E** existe um produto cadastrado chamado “Logitech MX Horizontal”.
  - **E** coloco o id do Logitech MX Horizontal no campo “id do produto”.
  - **Quando** envio um DELETE para "/produtos/{_id}"
  - **Então** o status da resposta deve ser **401 Unauthorized.**
  - **E** a mensagem deve ser "Token de acesso ausente, inválido, expirado...".

Funcionalidade: Excluir Usuários

Endpoint: DELETE /usuarios/ {_id}

- **Cenário 16: Excluir usuário com sucesso (Positivo)**
  - **Dado** que estou autenticado com um token de usuário.
  - **E** possuo o id de um usuário cadastrado
  - **Quando** envio um DELETE para "/usuarios/{_id}"

    - **Então** o status da resposta deve ser **200 OK.**
    - **E** a mensagem deve ser "Registro excluído com sucesso".

- **Cenário 17: Excluir usuário que não existe (Negativo)**
    - **Dado** que estou autenticado com um token de usuário normal.
    - **E** coloco no campo de id, um id inexistente
    - **Quando** envio um DELETE para "/usuarios/{_id}"
    - **Então** o status da resposta deve ser **200 OK.**
    - **E** a mensagem deve ser "Nenhum registro excluído".

.

- **Cenário 18: Excluir usuário sem Token de Acesso (Negativo)**
    - **Dado** que estou autenticado com um token de usuário inválido.
    - **Quando** envio um DELETE para "/usuarios/{_id}"
    - **Então** o status da resposta deve ser **401 Unauthorized.**
    - **E** a mensagem deve ser "Token de acesso ausente, inválido, expirado...".

Funcionalidade: Editar Usuários

Endpoint: PUT /usuarios/ {_id}

- **Cenário 19: Editar usuário com sucesso (Positivo)**
    - **Dado** que estou autenticado com um token de usuário.
    - **E** possuo o id de um usuário cadastrado
    - **Quando** envio um PUT para "/usuarios/{_id}" nome Vitor QATeste , email vitorqa@gmail.com, password “teste” e administrador false.
    - **Então** o status da resposta deve ser **200 OK.**
    - **E** a mensagem deve ser "Registro alterado com sucesso".

- **Cenário 20: Editar usuário com formato de e-mail inválido (Negativo)**
    - **Dado** que estou autenticado com um token de usuário.
    - **E** possuo o id de um usuário cadastrado
    - **Quando** envio um PUT para "/usuarios/{_id}" nome Vitor QATeste , email vitorqagmail.com, password “teste” e administrador false.
    - **Então** o status da resposta deve ser **400 Bad request.**
    - **E** a mensagem deve ser "Email deve ser um email válido".

.

- **Cenário 21: Editar usuário com um e-mail já cadastrado (Negativo)**
    - **Dado** que estou autenticado com um token de usuário.

- **E** possuo o id de um usuário cadastrado
- **E** que já existe outro email vitorqa@gmail.com cadastrado
- **Quando** envio um PUT para "/usuarios/{_id}" nome Vitor QATeste , email vitorqa@gmail.com, password “teste” e administrador false.
- **Então** o status da resposta deve ser **400 Bad request.**
- **E** a mensagem deve ser "Este email já está sendo usado".

2. Relatório de Bugs

BUG-01: Exclusão de usuário permitida, sem autenticação (Falha de Segurança)

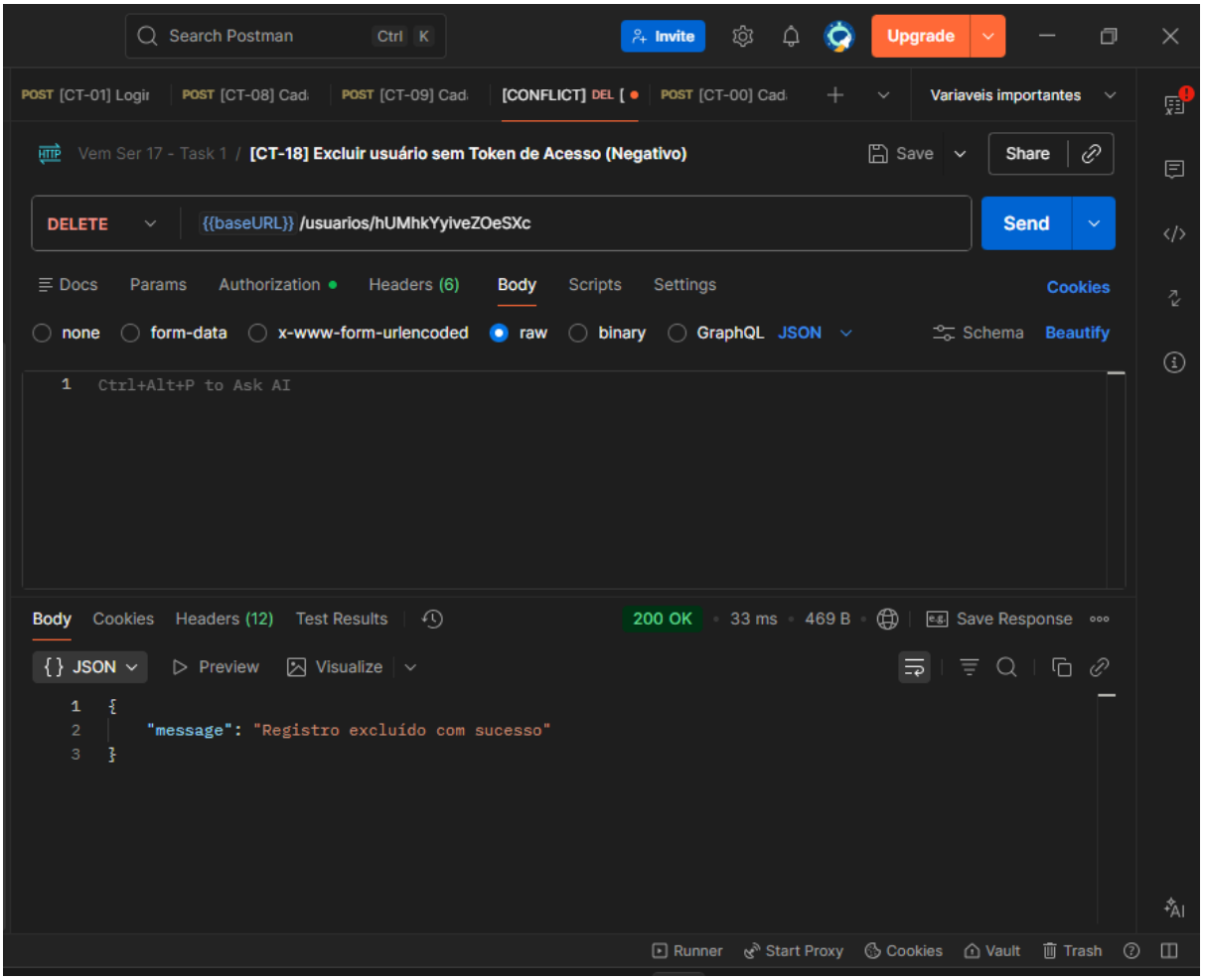
- **Severidade:** 🔴 Crítica (Blocker)
- **Endpoint:** `DELETE /usuarios/{_id}`
- **Descrição:** O endpoint de exclusão não está validando a presença ou validade do Token JWT. Isso permite que usuários não autenticados (anônimos) excluam os registros do banco.

- **Passo a Passo (Reprodução):**
  - Abrir o Postman.
  - Criar uma requisição `DELETE` para `http://localhost:3000/usuarios/[ID-DE-UM-USUARIO]`.
  - Na aba "Authorization", selecionar "No Auth" (garantindo que nenhum token está sendo enviado).
  - Clicar em "Send".

- **Resultado Esperado:**
  - Status HTTP: `401 Unauthorized`
  - Body: Mensagem de erro informando falta de token.

- **Resultado Obtido:**
  - Status HTTP: `200 OK`
  - Body: `Request Body: { "message": "Registro excluído com sucesso" }`

- **Evidência:**


Search Postman
Ctrl K
Invite
Upgrade
POST [CT-01] Logir
POST [CT-08] Cad
POST [CT-09] Cad
[CONFLICT] DEL [
POST [CT-00] Cad
Variaveis importantes
Vem Ser 17 - Task 1 / [CT-18] Excluir usuário sem Token de Acesso (Negativo)
Save
Share
DELETE
{{baseURL}} /usuarios/hUMhkYyiveZOeSXc
Send
Docs
Params
Authorization
Headers (6)
Body
Scripts
Settings
Cookies
none
form-data
x-www-form-urlencoded
raw
binary
GraphQL
JSON
Schema
Beautify
1 Ctrl+Alt+P to Ask AI
Body
Cookies
Headers (12)
Test Results
200 OK
33 ms
469 B
Save Response
{} JSON
Preview
Visualize
1 {
2 "message": "Registro excluído com sucesso"
3 }
Runner
Start Proxy
Cookies
Vault
Trash