

[IEM-4] **US003-BUG01: É permitido listar produtos e buscar produtos por id sem autenticação** Created: 09/May/25

Updated: 09/May/25 Resolved: 09/May/25

Status:	Done
Project:	Issues e Melhorias
Components:	None
Affects versions:	None
Fix versions:	None

Type:	Tarefa	Priority:	Medium
Reporter:	Raique Alfredo Pereira de Ramos	Assignee:	Unassigned
Resolution:	Done	Votes:	0
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original estimate:	Not Specified		

Attachments:	EvidênciaListarProdutos.png  EvidênciaBuscarProdutoPorId.png
Rank:	0 i0002v:

Description

1 - Descrição Detalhada:

Ao tentar realizar a ação de listar produtos e buscar produtos por id sem ter autenticação, consigo acessar a lista de produtos e buscar o produto por id.

2 - Passo a Passo:

1. Acessar o grupo Produtos sem autenticação
2. Acessar a rota GET /produtos ou GET /produtos/\_id
3. Na rota GET /produtos enviar os seguintes parâmetros:
  1. \_id
  2. nome
  3. preco
  4. descricao
  5. quantidade
4. Na rota GET /produtos/\_id enviar o id do produto
5. Executar os requests.

3 - Resultado Esperado:

Como o usuário está sem autenticação, independente da rota, o que ele tentar fazer deve dar erro e o sistema deve informar "Token de acesso ausente, inválido, expirado ou usuário do token não existe mais"

4 - Resultado Atual:

Sem ter autenticação, o usuário consegue acessar a rota de GET /produtos e executar o request, então consegue visualizar a lista de produtos. Ou acessar a rota GET /produtos/\_id e ao executar o request informando o id válido do produto, visualizar ele.

5 - Gravidade:

Alta - Viola uma regra de segurança crítica, expondo informações sensíveis a usuários não autenticados.

6 - Prioridade:

Imediato - A questão envolve segurança e proteção de dados, que devem ser tratados com prioridade máxima

7 - Ambiente onde ocorre:

- API ServeRest

- Rota: POST /produto & /produtos/\_id
- Sistema Operacional: Windows 10 Pro, versão 22H2

## 8 - Responsável:

A ser decidido pela equipe de desenvolvimento

## 9 - Anexos:

API ServerRest / ... / Lista de produtos cadastrados / **Listar produtos cadastrados**

GET

{{url}} /produtos

Send

Params

Auth

Headers (6)

Body

Scripts

Settings

Cookies

Auth Type

Inherit auth from parent

The authorization header will be automatically generated when you send the request.  
[Learn more about authorization](#)

Bearer Token

Sem token de autenticação

Edit Auth in Collection

Token

{{Authorization}}

200 OK

175 ms

2.67 KB

Save Response

JSON

Preview

Visualize

Permitiu listar produtos sem autenticação

1

2

3

4

5

6

7

8

9

10

11

{

"quantidade": 11,

"produtos": [

{

"nome": "Logitech MX Vertical",

"preco": 470,

"descricao": "Mouse",

"quantidade": 382,

"\_id": "BeeJh5Iz3k6kSIzA"

}

,

}

Variables in request

url

https://compassuol.serverest....

Authorization

Enter value

Sem valor de token

produto-ID

BeeJh5Iz3k6kSIzA

All variables

API ServerRest / Produtos / Buscar produto por ID / **Buscar produto por ID**

GET

{{url}} /produtos/ {{produto-ID}}

Send

Params

Auth

Headers (6)

Body

Scripts

Settings

Cookies

Auth Type

Inherit auth from parent

The authorization header will be automatically generated when you send the request.  
[Learn more about authorization](#)

Bearer Token

Sem token de autenticação

Edit Auth in Collection

Token

{{Authorization}}

200 OK

190 ms

594 B

Save Response

JSON

Preview

Visualize

Permitiu "buscar produto por ID" sem ter autenticação

1

2

3

4

5

6

7

{

"nome": "Logitech MX Vertical",

"preco": 470,

"descricao": "Mouse",

"quantidade": 382,

"\_id": "BeeJh5Iz3k6kSIzA"

}

Variables in request

url

https://compassuol.serverest....

Authorization

Enter value

Sem valor

produto-ID

BeeJh5Iz3k6kSIzA

All variables

## 10 - Relação com outros defeitos ou requisitos:

Não foi identificado

## 11 - Melhorias Sugeridas:

- Implementação de Validação de Autenticação em Todas as Rotas Protegidas:
  - Verifique, em cada requisição, a presença de um token válido antes de permitir acesso a rotas protegidas, como GET /produtos e GET /produtos/\_id.

- Certifique-se de que as rotas rejeitem requisições não autenticadas com uma mensagem de erro adequada.

- **Mensagens de Erro Consistentes e Informativas:**

- Padronize as mensagens de erro relacionadas à autenticação em todo o sistema.
- Evite fornecer informações excessivas ao usuário em caso de falhas de autenticação, para não expor detalhes sobre a implementação.

- **Revisão de Logs de Auditoria:**

- Certifique-se de que todas as tentativas de acesso não autenticado ou inválido sejam registradas para monitoramento e análise posterior.
- Configure alertas para padrões suspeitos de acessos não autorizados.

---

Generated at Mon May 12 18:01:09 UTC 2025 by Raique Alfredo Pereira de Ramos using Jira 1001.0.0-SNAPSHOT#100283-rev:ae90960f6ce4b93d8be8d846e57df479663fa457.