

Broken Access Control 1 : Mengakses tracking order user lain

Kenapa berhasil?

1. Tidak ada mekanisme authorization untuk service track-order.

Risiko dampak

1. Pencurian informasi.

Rekomendasi perbaikan

1. Tambahkan mekanisme authorization service-service yang mungkin mengembalikan data dan/atau informasi sensitive.

The screenshot shows a Postman interface with the following details:

- Method:** GET
- URL:** http://localhost:3000/rest/track-order/5267-41f5f1f0dcc842e4
- Authorization:** No Auth (highlighted in red)
- Body:** JSON response (highlighted in red)
- Headers:** (12) (highlighted in red)
- Test Results:** (highlighted in red)
- Status:** 200 OK
- Time:** 26 ms
- Size:** 737 B

The JSON response body is as follows:

```
1 {  
2   "status": "success",  
3   "data": [  
4     {  
5       "orderId": "5267-41f5f1f0dcc842e4",  
6       "email": "*dm*n@j**c*-sh.*p",  
7       "totalPrice": 8.96,  
8       "bonus": 0,  
9       "products": [  
10          {  
11            "quantity": 3,  
12            "name": "Apple Juice (1000ml)",  
13            "price": 1.99,  
14            "total": 5.97,  
15            "bonus": 0  
16          },  
17          {  
18            "quantity": 1,  
19            "name": "Orange Juice (1000ml)",  
20            "price": 2.99,  
21          }  
22        ]  
23      }  
24    ]  
25  ]  
26}  
27 }
```

Broken Access Control 2 : Men-submit data atas nama orang lain

Kenapa berhasil?

1. Tidak ada mekanisme authorization untuk service PUT product/1/reviews.

Risiko dampak

1. Social engineering.
2. Integritas data yang questionable.

Rekomendasi perbaikan

1. Tambahkan mekanisme authorization pada service yang meng-insert data ke database agar data yang diinput lebih akurat.

The screenshot shows a POST request in Postman to `http://localhost:3000/rest/products/1/reviews`. The request method is `PUT`. The `Body` tab is selected, showing the following JSON payload:

```
1 {  
2   "message": "aaa",  
3   "author": "tom.cruise@google.com"  
4 }
```

The response status is `201 Created`, with a response time of `28 ms` and a response size of `409 B`. The response body is:

```
1 {  
2   "status": "success"  
3 }
```

The screenshot shows the OWASP Juice Shop application. On the left, there's a sidebar with a drink icon and the text "All Products". In the center, there's a product card for "Apple Juice (1000ml)" with a price of 1.99. To the right of the product card, a modal window titled "Reviews (3)" is open, showing three reviews:

- 1. **admin@juice-sh.op** - One of my favorites!
- 2. **a@b.c** - aaa
- 3. **tom.cruise@google.com** - aaa