Broken Access Control 1 : Mengakses tracking order user lain

Kenapa berhasil?

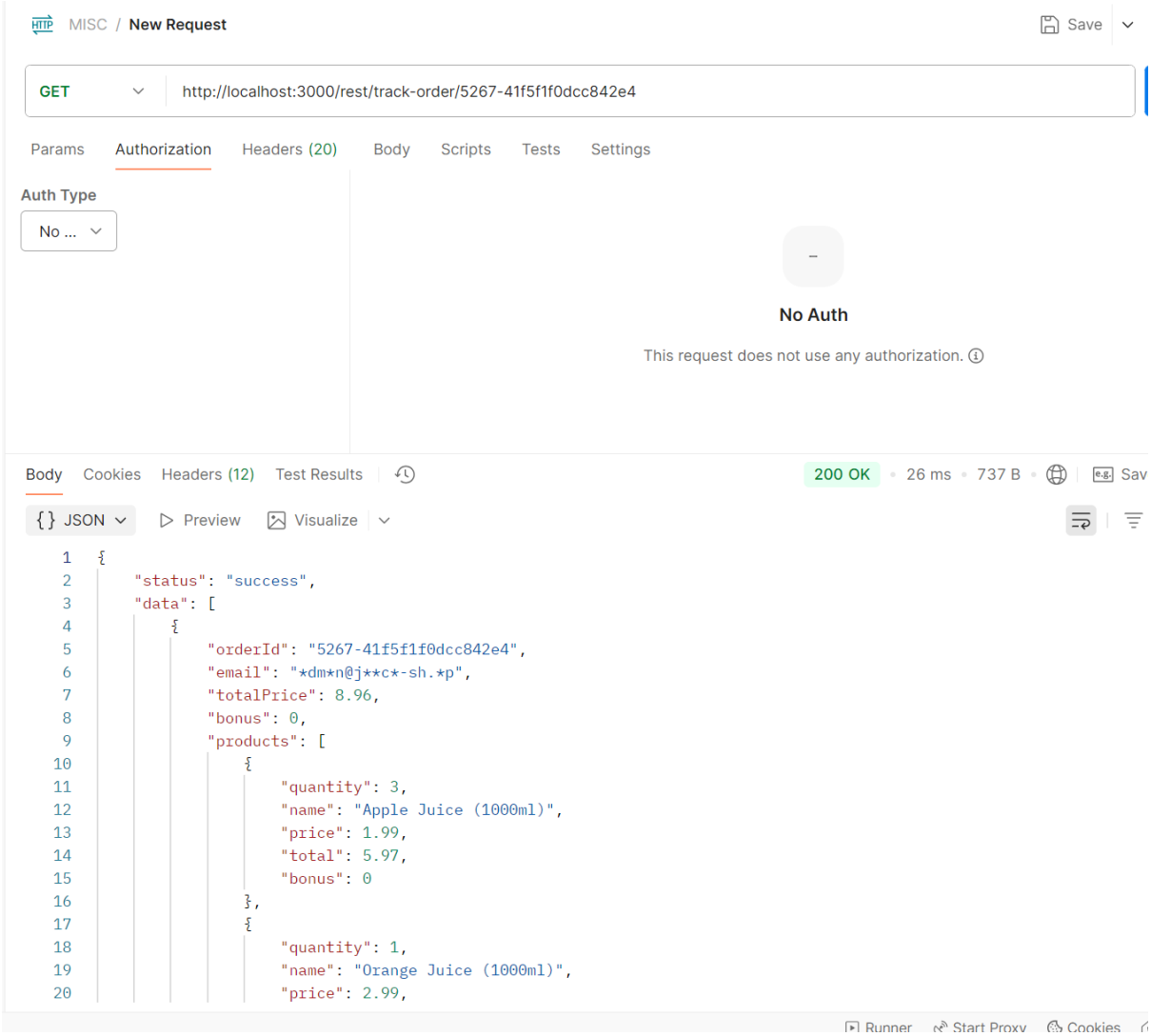
1. Tidak ada mekanisme authorization untuk service track-order.

Risiko dampak

1. Pencurian informasi.

Rekomendasi perbaikan

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



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.