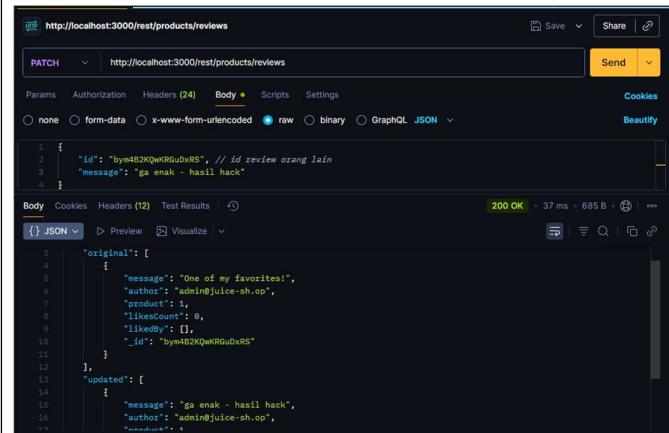
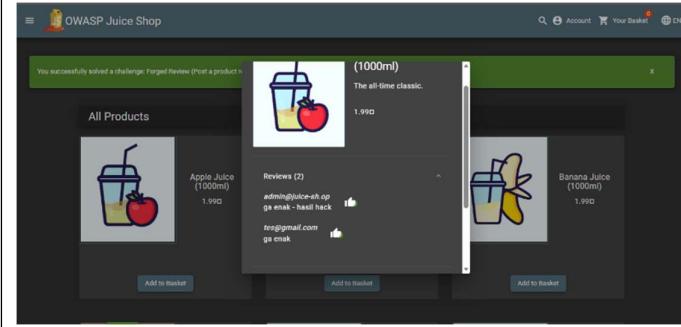
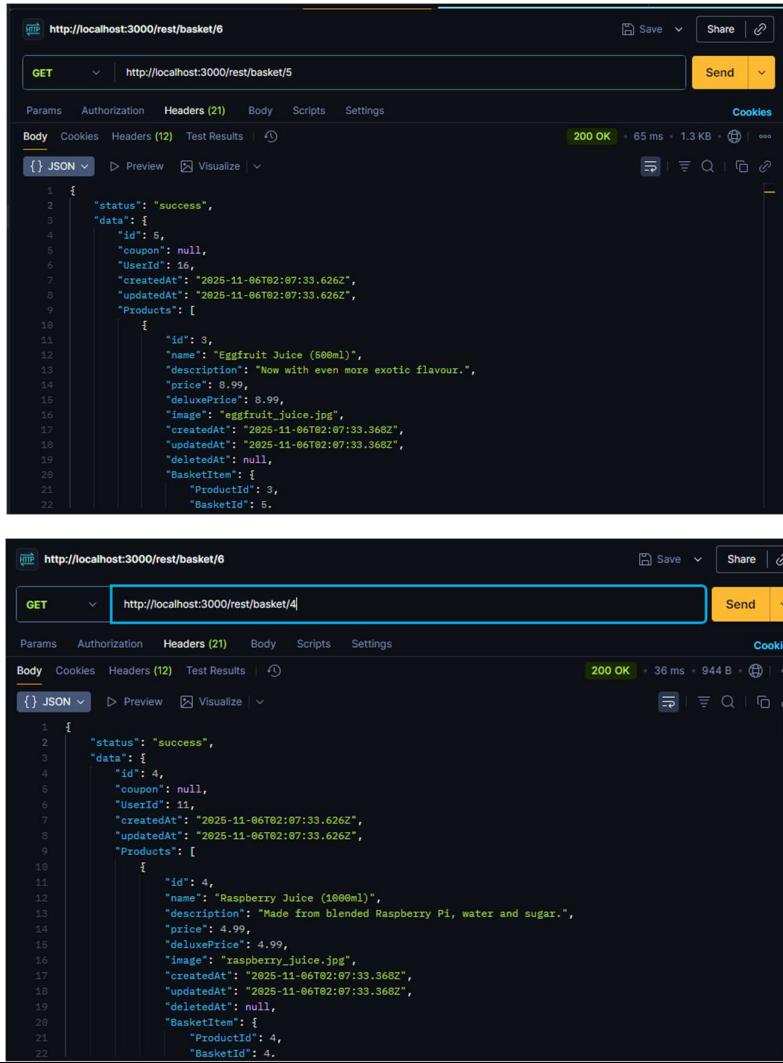


	Haryo Arief Wicaksono
1.	Ditemukan Broken Access Control (BAC). Dapat mengedit review orang lain, tanpa login dengan akun usernya.
	<p>Bukti screenshot:</p>   
	<p><b>Root Cause Analysis:</b>          Token yang digunakan hanya dites valid atau tidak. Namun tidak dicek apakah token tersebut pemiliknya atau bukan.</p> <p><b>Recommendation:</b>          Dilakukan validasi apakah yang mengedit memang pemiliknya atau bukan dengan token tersebut.</p> <p><b>Verification scenario:</b>          Tidak akan bisa mengedit data milik orang lain.</p>

2.	<p>Ditemukan BAC pada page “Basket”. Saya dapat melihat keranjang orang lain dengan mengubah id keranjang</p>
	<p>Bukti Screenshot (id keranjang saya 6, tapi bisa melihat id keranjang 5 dan 4)</p>  <pre> 1 { 2   "status": "success", 3   "data": { 4     "id": 5, 5     "coupon": null, 6     "userId": 16, 7     "createdAt": "2025-11-06T02:07:33.626Z", 8     "updatedAt": "2025-11-06T02:07:33.626Z", 9     "Products": [ 10       { 11         "id": 3, 12         "name": "Eggfruit Juice (500ml)", 13         "description": "Now with even more exotic flavour.", 14         "price": 8.99, 15         "deluxePrice": 8.99, 16         "image": "eggfruit_juice.jpg", 17         "createdAt": "2025-11-06T02:07:33.368Z", 18         "updatedAt": "2025-11-06T02:07:33.368Z", 19         "deletedAt": null, 20         "BasketItem": [ 21           { 22             "ProductId": 3, 23             "BasketId": 5. 24           } 25         ] 26       } 27     ] 28   } 29 } </pre> <pre> 1 { 2   "status": "success", 3   "data": { 4     "id": 4, 5     "coupon": null, 6     "userId": 11, 7     "createdAt": "2025-11-06T02:07:33.626Z", 8     "updatedAt": "2025-11-06T02:07:33.626Z", 9     "Products": [ 10       { 11         "id": 4, 12         "name": "Raspberry Juice (1000ml)", 13         "description": "Made from blended Raspberry Pi, water and sugar.", 14         "price": 4.99, 15         "deluxePrice": 4.99, 16         "image": "raspberry_juice.jpg", 17         "createdAt": "2025-11-06T02:07:33.368Z", 18         "updatedAt": "2025-11-06T02:07:33.368Z", 19         "deletedAt": null, 20         "BasketItem": [ 21           { 22             "ProductId": 4, 23             "BasketId": 4. 24           } 25         ] 26       } 27     ] 28   } 29 } </pre>
	<p><b>Root Cause Analysis:</b> Token yang digunakan hanya dites valid atau tidak. Namun tidak dicek apakah token tersebut pemiliknya atau bukan.</p> <p><b>Recommendation:</b> Dilakukan validasi apakah yang mengedit memang pemiliknya atau bukan dengan token tersebut.</p> <p><b>Verification Scenario:</b> Saya tidak akan bisa melihat keranjang orang lain dengan mengubah id keranjang.</p>