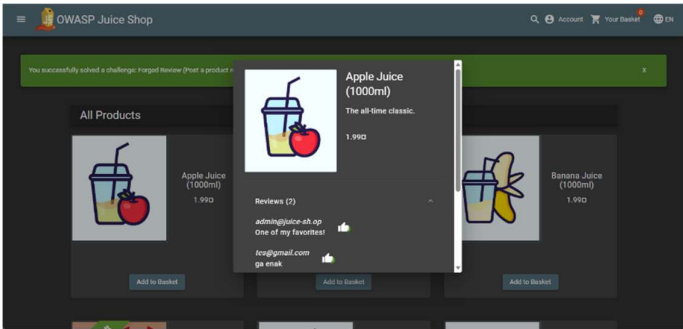
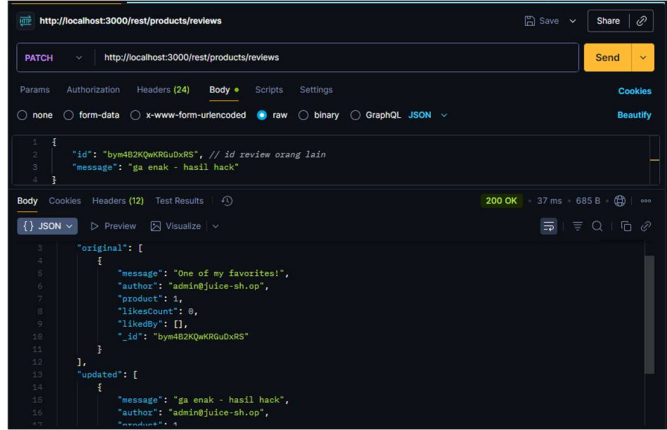
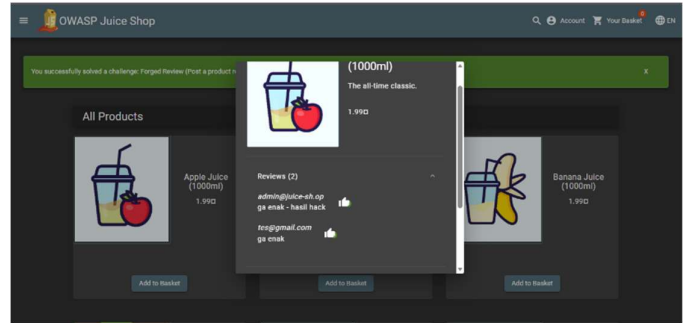
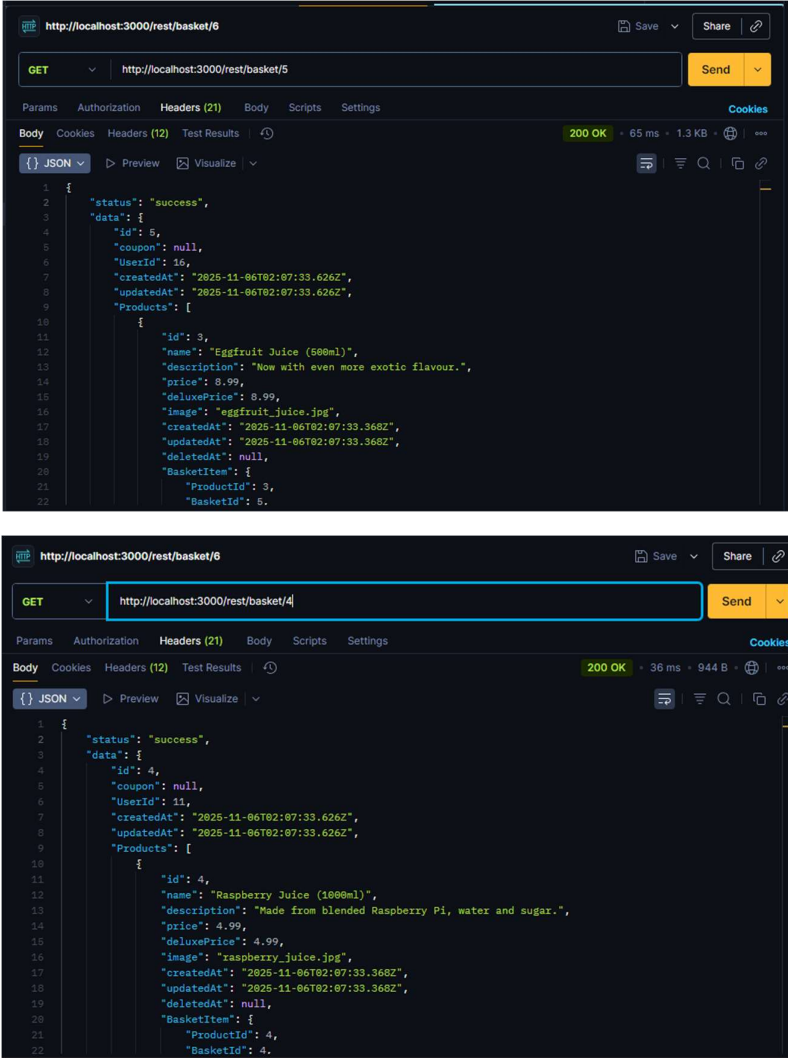


	Haryo Arief Wicaksono
1.	Ditemukan Broken Access Control (BAC). Dapat mengedit review orang lain, tanpa login dengan akun usernya.
	<p>Bukti screenshot:</p>   
	<p>Root Cause Analysis:</p> <p>Token yang digunakan hanya dites valid atau tidak. Namun tidak dicek apakah token tersebut pemiliknya atau bukan.</p> <p>Recommendation:</p> <p>Dilakukan validasi apakah yang mengedit memang pemiliknya atau bukan dengan token tersebut.</p> <p>Verification scenario:</p> <p>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>  <p>The first screenshot shows a GET request to <code>http://localhost:3000/rest/basket/5</code> returning a 200 OK status. The JSON response includes a <code>BasketItem</code> object with <code>BasketId</code> 6, indicating access to another user's basket.</p> <p>The second screenshot shows a GET request to <code>http://localhost:3000/rest/basket/4</code> returning a 200 OK status. The JSON response includes a <code>BasketItem</code> object with <code>BasketId</code> 4, indicating access to another user's basket.</p>
	<p>Root Cause Analysis:</p> <p>Token yang digunakan hanya dites valid atau tidak. Namun tidak dicek apakah token tersebut pemiliknya atau bukan.</p> <p>Recommendation:</p> <p>Dilakukan validasi apakah yang mengedit memang pemiliknya atau bukan dengan token tersebut.</p> <p>Verification Scenario:</p> <p>Saya tidak akan bisa melihat keranjang orang lain dengan mengubah id keranjang.</p>