

ASSIGNMENT 3



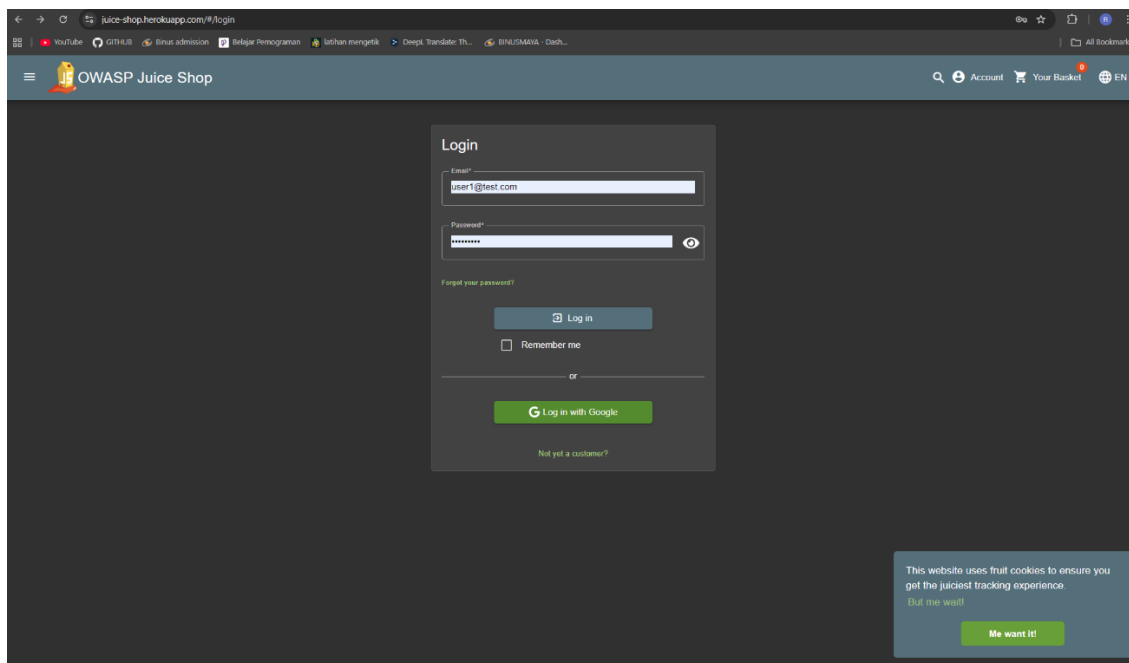
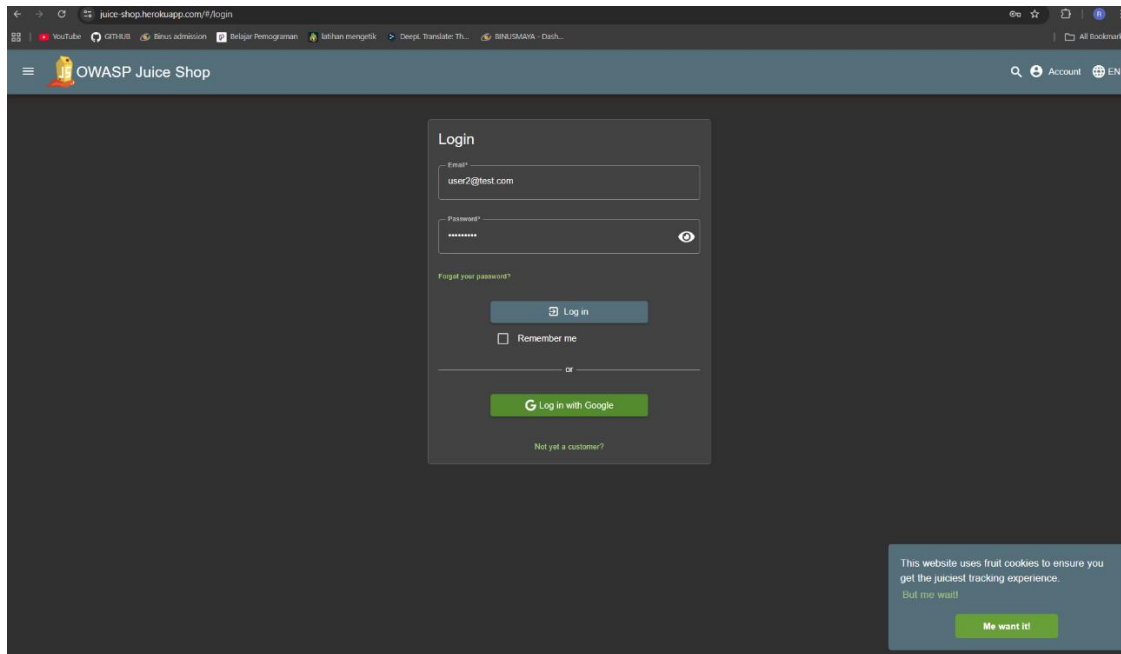
Ryan Hanif Dwihandoyo
Bootcamp CS Batch 3

LAPORAN ANALISIS KERENTANAN BROKEN ACCESS CONTROL

Aplikasi Target: OWASP Juice Shop

Nama Penguji: Ryan Hanif Dwihandoyo

Tanggal Pengujian: 10-04-2025



Temuan #1: Insecure Direct Object Reference (IDOR) Memungkinkan Pengguna Melihat Keranjang Belanja Pengguna Lain

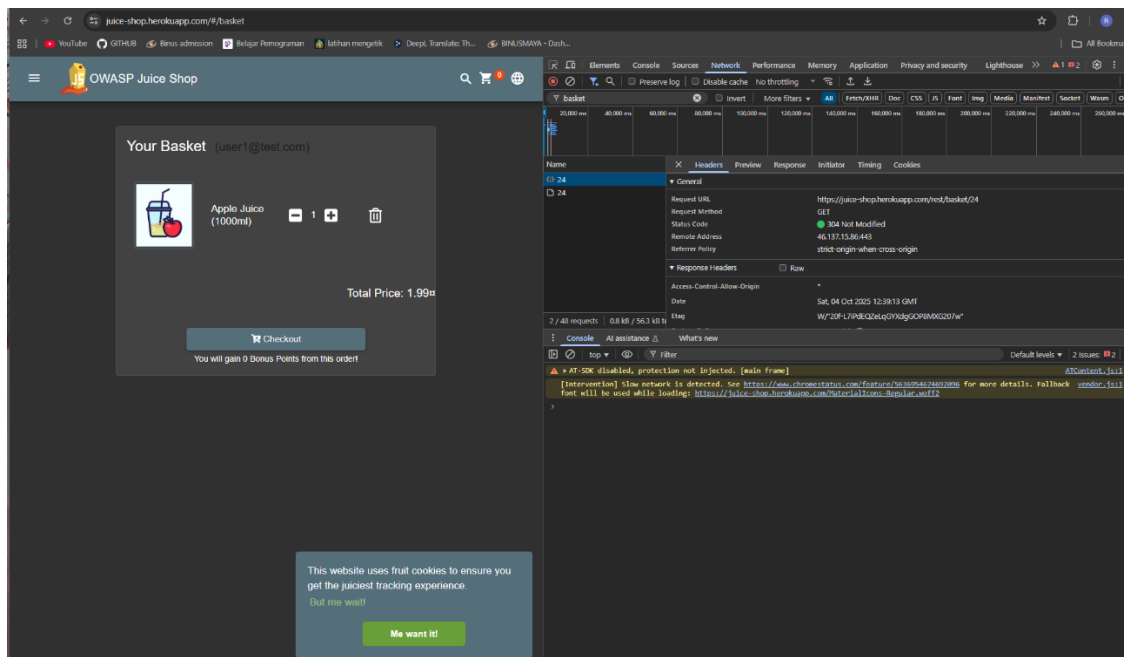
Peringkat Risiko: **Tinggi**

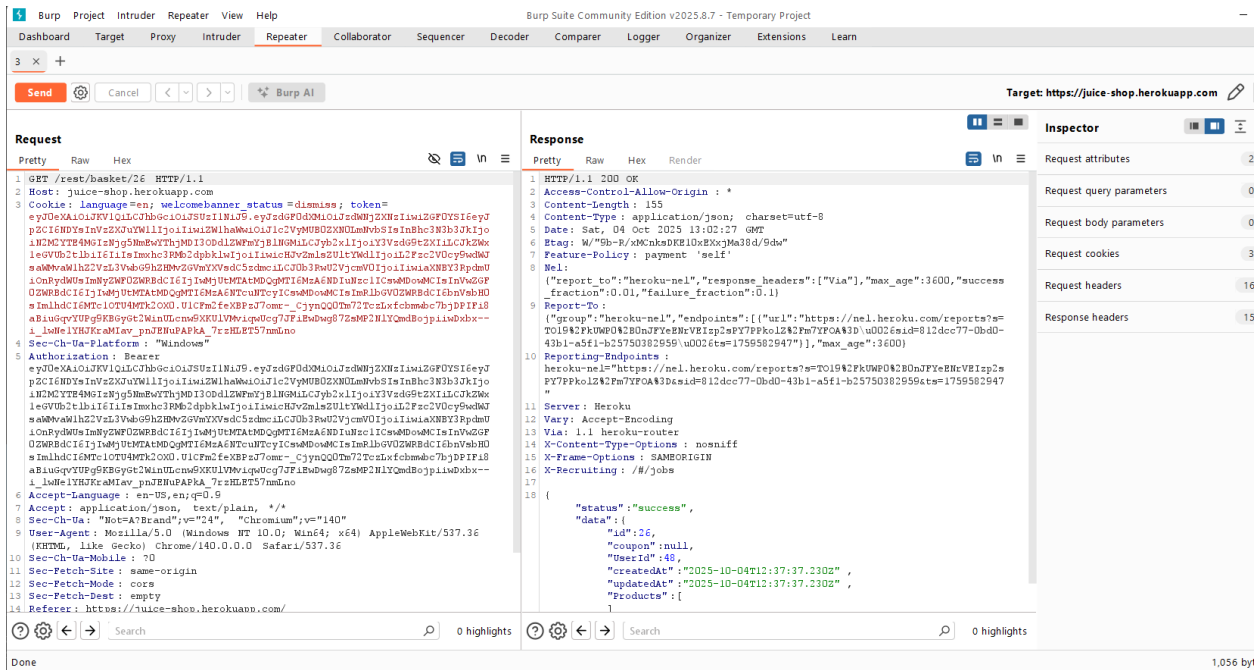
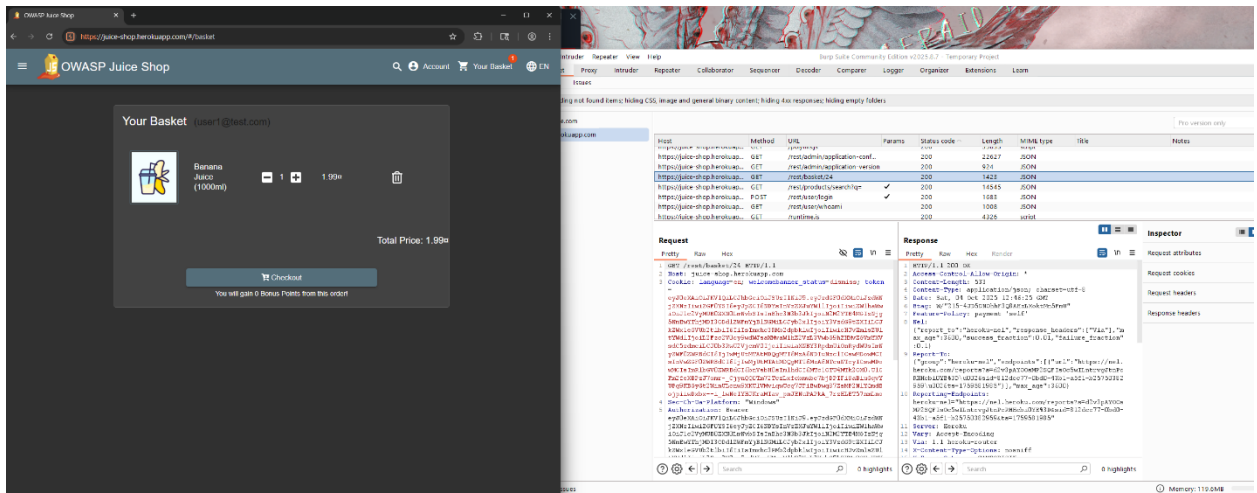
Deskripsi:

Aplikasi ini rentan terhadap IDOR pada fungsionalitas keranjang belanja. Endpoint API `/rest/basket/{basketId}` tidak melakukan validasi apakah keranjang yang diminta benar-benar milik pengguna yang sedang login. Akibatnya, penyerang yang telah terautentikasi dapat melihat isi keranjang belanja pengguna lain hanya dengan menebak atau mengganti nilai `'basketId'` di URL.

Bukti (Proof-of-Concept):

1. Pengguna A (user1@test.com) login dan memiliki `'basketId' = 24`.
2. Pengguna B (user2@test.com) login dan memiliki `'basketId' = 26`.
3. Saat login sebagai Pengguna A, saya mengirimkan request `'GET'` ke endpoint `'/rest/basket/26'`.
4. Server memberikan respons sukses (HTTP 200 OK) dan menampilkan seluruh isi keranjang belanja milik Pengguna B.





Dampak:

Kerentanan ini dapat menyebabkan pelanggaran privasi data pelanggan secara massal. Penyerang dapat memata-matai kebiasaan belanja pengguna lain, yang dapat disalahgunakan untuk tujuan pemasaran ilegal, penipuan, atau sekadar mengganggu pengguna. Ini secara signifikan merusak kepercayaan pelanggan terhadap platform.

Rekomendasi Mitigasi:

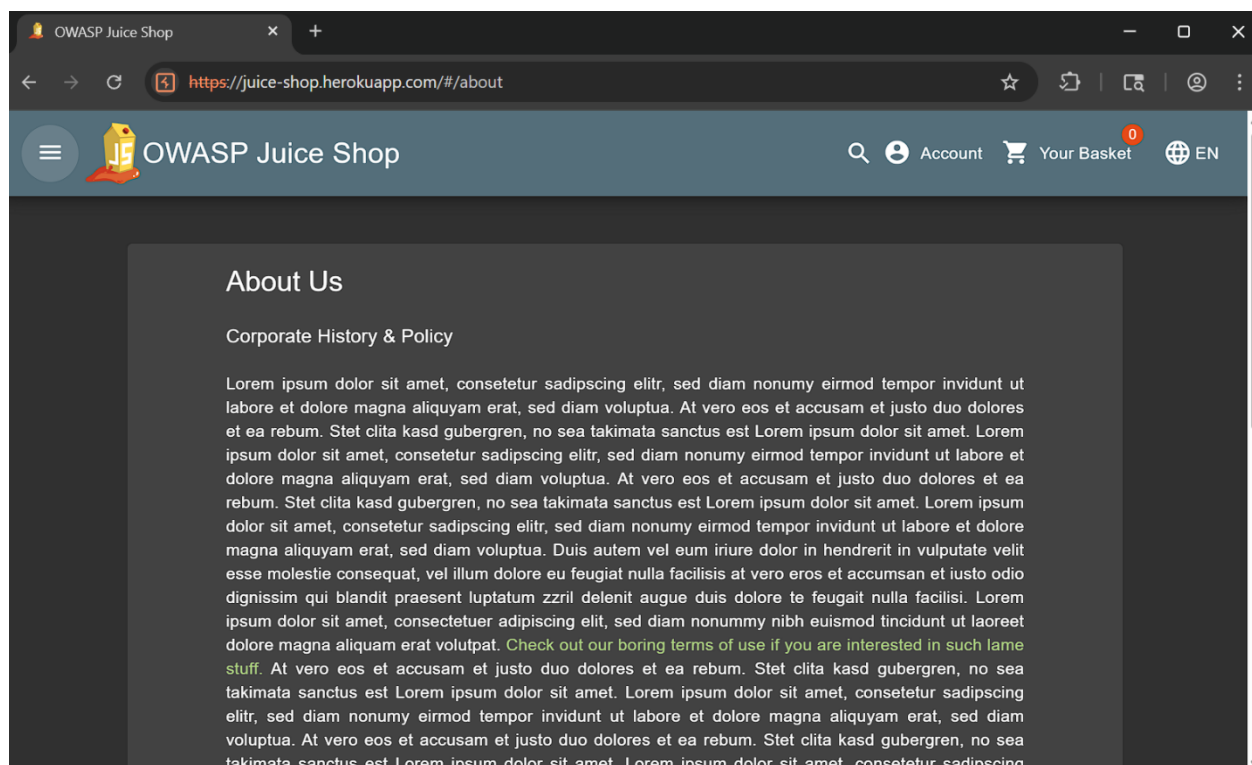
Terapkan validasi hak akses pada sisi server untuk setiap permintaan ke data sensitif. Sebelum menampilkan isi keranjang, server harus memverifikasi bahwa `basketId` yang diminta sesuai dengan `userId` dari pengguna yang sesi tokennya aktif saat itu. Jika tidak cocok, server harus menolak permintaan tersebut dengan respons **`403 Forbidden`** atau **`404 Not Found`**.

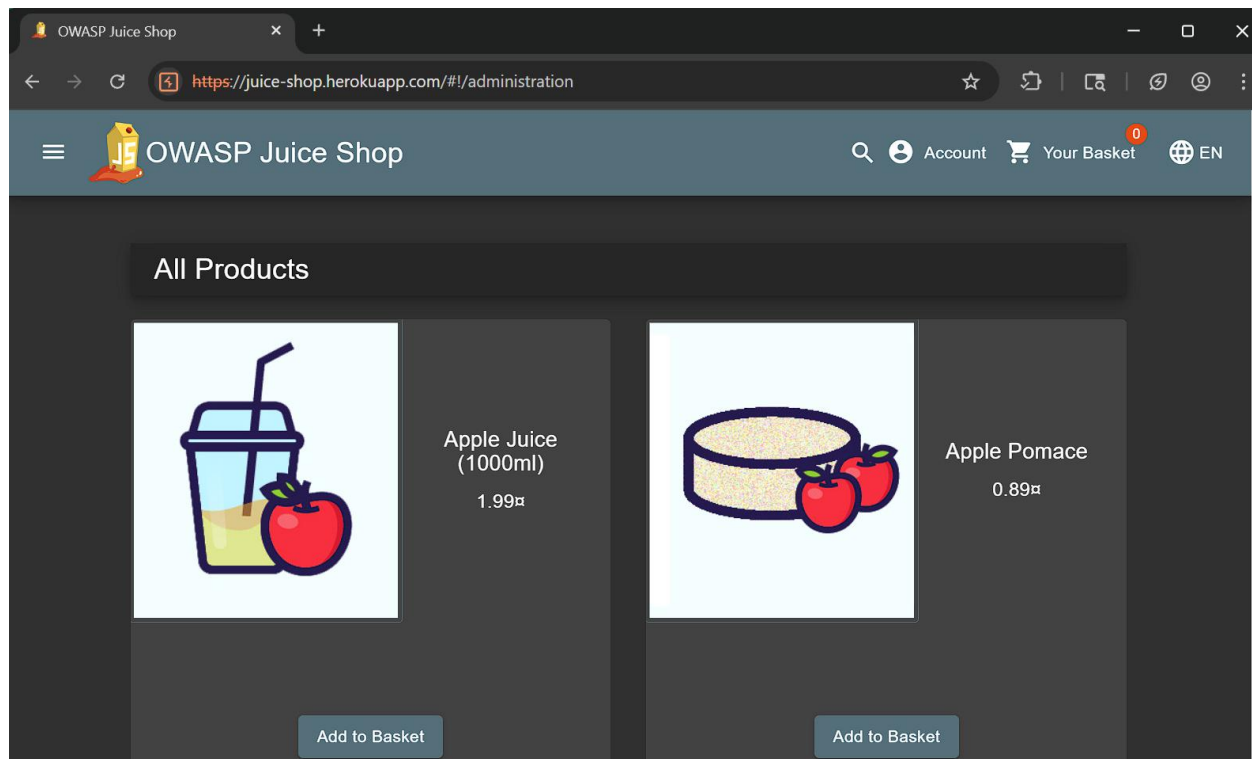
Temuan #2: Eskalasi Hak Akses ke Halaman Administrasi melalui Bypass control Sisi Klien

Peringkat Risiko: **KRITIS**

Deskripsi:

Aplikasi gagal menerapkan control akses untuk halaman administrasi di sisi klien namun tidak di sisi server. Seorang penyerang dapat melewati mekanisme pertahanan ini dengan melakukan serangan *race condition*, yaitu membuat sebuah halaman / administration dan segera menghentikan eksekusi sebelum divalidasi dan dialihkan.





Dampak:

Penyerang dapat melihat dan memanipulasi data sensitif seluruh system, seperti menghapus semua ulasan, mengubah harga produk, atau yang paling parah mengakses dan menghapus akun pengguna lain secara massal. Hal ini dapat merusak integritas dan kerahasiaan seluruh aplikasi.

Rekomendasi Mitigasi:

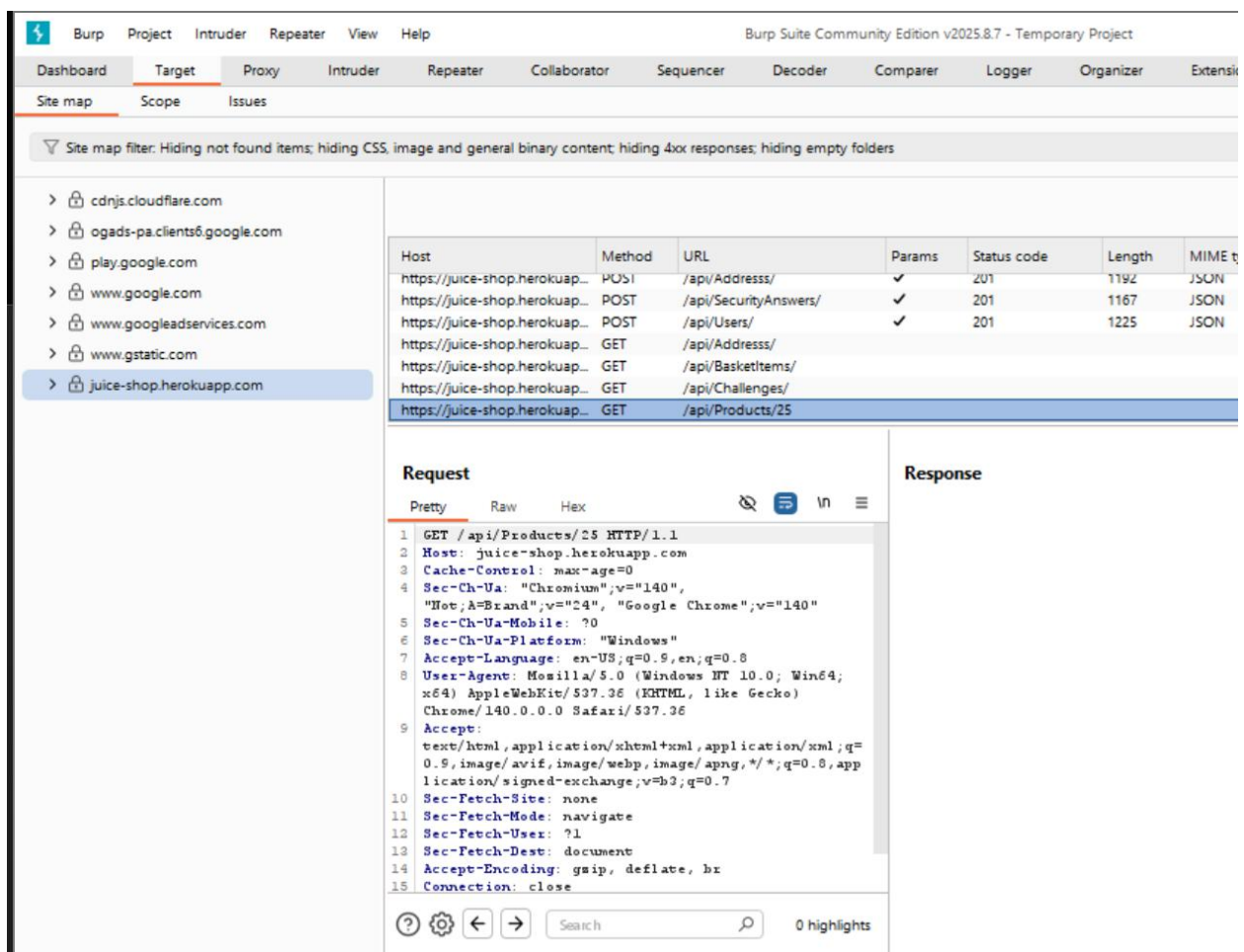
Terapkan **Role-Based Access Control** (RBAC) di sisi server pada endpoint yang melindungi panel administrasi. Server harus secara eksplisit memverifikasi peran pengguna sebelum mengizinkan akses ke endpoint, jika peran tidak sesuai kembalikan respon *403 forbidden*.

Temuan #:3 Insecure Direct Object Reference (IDOR) Memungkinkan Akses Detail Produk Non-Publik

Peringkat Risiko: **TINGGI**

Deskripsi:

Aplikasi rentan terhadap *IDOR* pada fungsionalitas detail produk. Endpoint detail produk. Tidak melakukan validasi otoritas yang memadai untuk memastikan informasi produk yang diminta Adalah data yang sah untuk dilihat oleh pengguna yang sedang login. Penyerang dapat melihat detail produk lain, termasuk produk yang mungkin belum dipublikasi atau memiliki detail internal, hanya dengan memanipulasi nilai *produkId*



Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

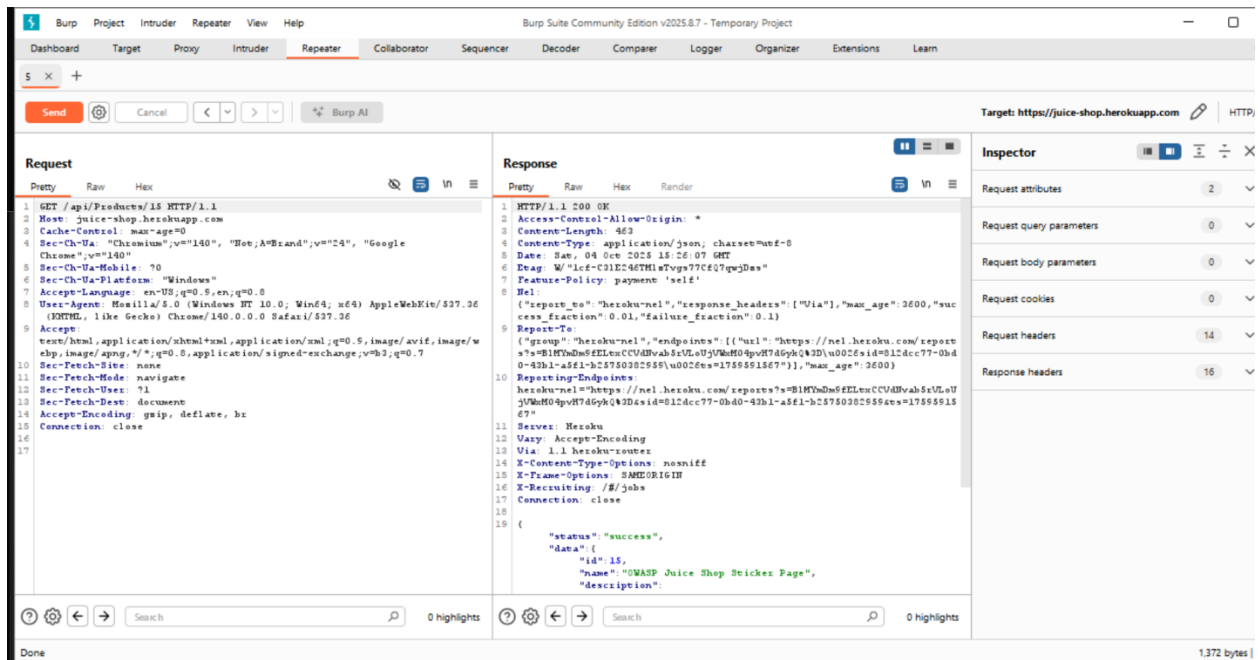
Host	Method	URL	Params	Status code	Length	MIME t
https://juice-shop.herokuapp...	POST	/api/Address/	✓	201	1192	JSON
https://juice-shop.herokuapp...	POST	/api/SecurityAnswers/	✓	201	1167	JSON
https://juice-shop.herokuapp...	POST	/api/Users/	✓	201	1225	JSON
https://juice-shop.herokuapp...	GET	/api/Address/				
https://juice-shop.herokuapp...	GET	/api/BasketItems/				
https://juice-shop.herokuapp...	GET	/api/Challenges/				
https://juice-shop.herokuapp...	GET	/api/Products/25				

Request

Pretty Raw Hex

```
1 GET /api/Products/25 HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cache-Control: max-age=0
4 Sec-Ch-Ua: "Chromium";v="140",
5 "Not;A=Brand";v="24", "Google Chrome";v="140"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept-Language: en-US;q=0.9,en;q=0.8
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
10 x64) AppleWebKit/537.36 (KHTML, like Gecko)
11 Chrome/140.0.0.0 Safari/537.36
12 Accept:
13 text/html,application/xhtml+xml,application/xml;q=
14 0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
15 lication/signed-exchange;v=b3;q=0.7
16 Sec-Fetch-Site: none
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-User: ?1
19 Sec-Fetch-Dest: document
20 Accept-Encoding: gzip, deflate, br
21 Connection: close
```

Response



Dampak:

Pelanggaran kerahasiaan informasi bisnis. Kerentanan ini dapat mengekspos detail produk yang belum dirilis, strategi harga, atau metadata internal yang berharga bagi pesaing atau public.

Rekomendasi Mitigasi:

Terapkan validasi otoritas di sisi server products. Server harus memverifikasi bahwa produk yang diminta bertatus public atau bahwa pengguna yang mengakses memiliki peran yang diizinkan untuk melihat deail non-publik. Jika produk ID 15 adalah produk rahasia, server harus mengembalikan respons **403 forbidden**.

