

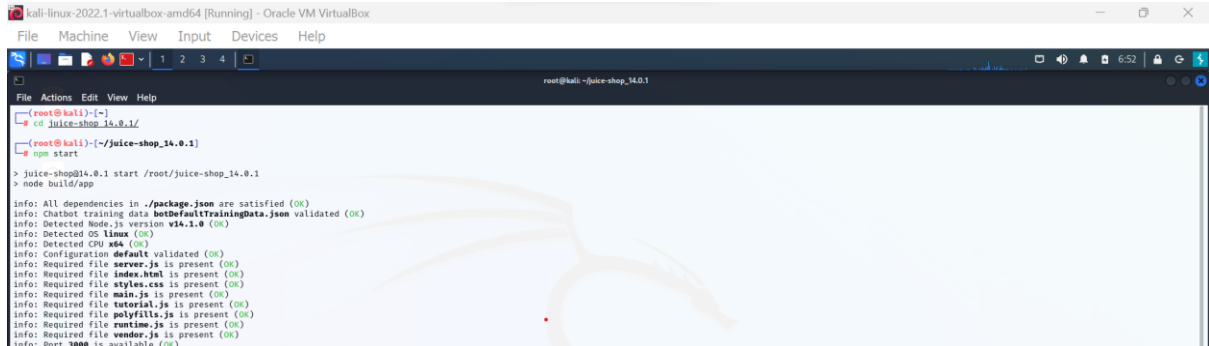
Percobaan Broken Access Control



Nama	: Choirun Annas
NRP	: 3122640032
Mata Kuliah	: Keamanan Jaringan
Dosen	: Bapak Fery Astika Saputra

Laporan

1. Ketik npm start pada direktori juice shop.

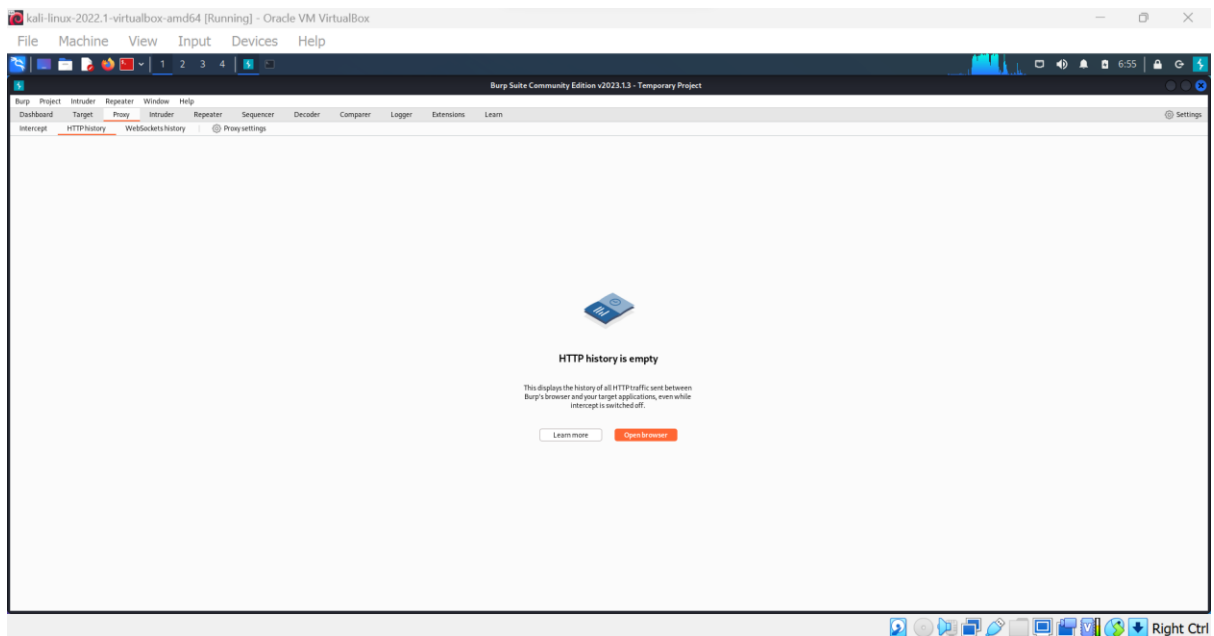


```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

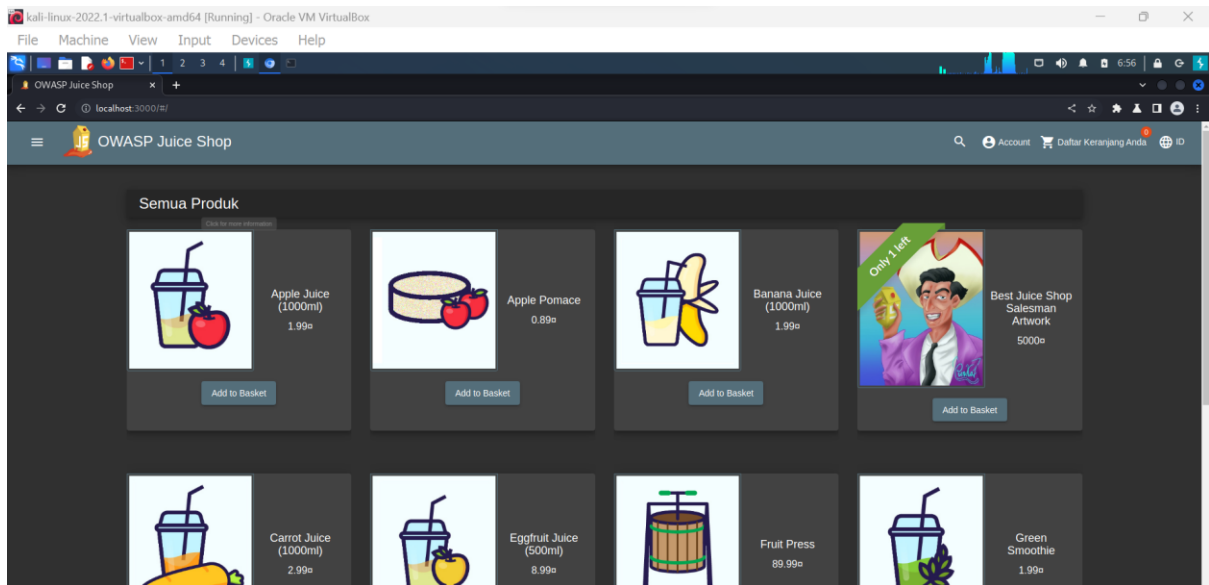
root@kali: ~/juice-shop_14.0.1
--(root@kali)--[~]
# cd juice-shop_14.0.1/
--(root@kali)--[~/juice-shop_14.0.1]
# npm start
> juice-shop@14.0.1 start /root/juice-shop_14.0.1
> node build/app

info: All dependencies in ./package.json are satisfied (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Detected Node.js version v14.1.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x86_64 (OK)
info: Configuration default validated (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file styles.css is present (OK)
info: Required file main.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
```

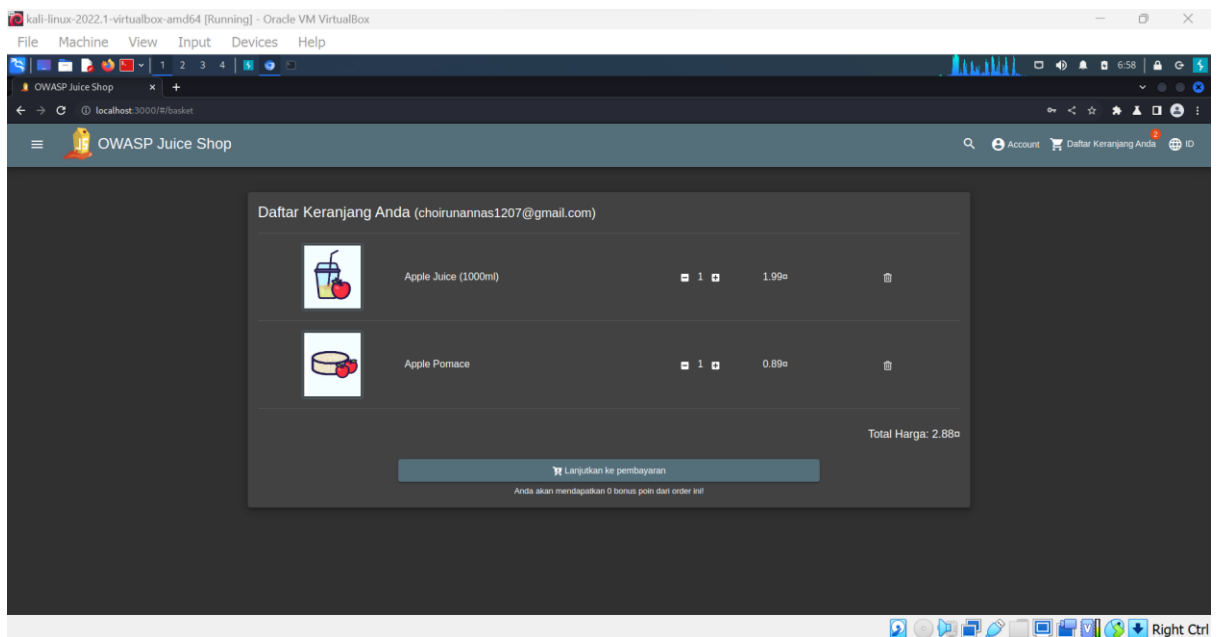
2. Buka browser di burp suite



3. Buka web juice shop menggunakan alamat localhost:3000



4. Tambahkan ke keranjang 2 product



5. Lihat data basket di history proxy pada burp suite

The screenshot shows the Burp Suite interface with the HTTP history tab selected. The table displays the following request:

#	Host	Method	URL	Params	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
84	http://localhost:3000	GET	/rest/user/whami		200	253						127.0.0.1		06:57:49.11M	8080
85	http://localhost:3000	GET	/rest/basket/6		200	254	JSON					127.0.0.1		06:57:51.11M	8080
86	http://localhost:3000	GET	/api/basketitem/9		200	488	JSON					127.0.0.1		06:57:51.11M	8080
87	http://localhost:3000	PUT	/api/basketitem/9		200	488	JSON					127.0.0.1		06:57:51.11M	8080
88	http://localhost:3000	GET	/api/product/164646/204646/201716		200	560	JSON					127.0.0.1		06:57:52.11M	8080
89	http://localhost:3000	GET	/rest/basket/6		200	1349	JSON					127.0.0.1		06:57:52.11M	8080
90	http://localhost:3000	GET	/rest/user/whami		200	253						127.0.0.1		06:57:54.11M	8080
91	http://localhost:3000	GET	/rest/basket/6		200	254						127.0.0.1		06:57:54.11M	8080
92	http://localhost:3000	GET	/api/basketitem/9		200	488	JSON					127.0.0.1		06:57:57.11M	8080
93	http://localhost:3000	PUT	/api/basketitem/9		200	488	JSON					127.0.0.1		06:57:57.11M	8080
94	http://localhost:3000	GET	/rest/basket/6		200	1349	JSON					127.0.0.1		06:57:58.11M	8080
95	http://localhost:3000	GET	/rest/basket/6		200	254						127.0.0.1		06:57:58.11M	8080

The selected request (89) is a GET request to /rest/basket/6. The response is a JSON object:

```
{
  "status": "success",
  "data": {
    "id": 6,
    "coupon": null,
    "userId": 21,
    "createdAt": "2023-03-07T09:01:36.000Z",
    "updatedAt": "2023-03-07T09:01:36.000Z",
    "Products": [
      {
        "id": 1,
        "name": "Apple Juice (1000ml)",
        "description": "The all-time classic.",
        "price": 1.99,
        "deluxePrice": 4.99,
        "image": "apple_juice.jpg",
        "createdAt": "2023-03-07T08:56:18.811Z",
        "updatedAt": "2023-03-07T08:56:18.811Z"
      }
    ]
  }
}
```

6. Ubah api 6 ke 2 maka item akan berubah

The screenshot shows the Burp Suite interface with the HTTP history tab selected. The selected request is a GET request to /rest/basket/2. The response is a JSON object:

```
{
  "status": "success",
  "data": {
    "id": 2,
    "coupon": null,
    "userId": 2,
    "createdAt": "2023-03-07T08:56:19.659Z",
    "updatedAt": "2023-03-07T08:56:19.659Z",
    "Products": [
      {
        "id": 4,
        "name": "Raspberry Juice (1000ml)",
        "description": "Made from blended Raspberry Pl., water and sugar.",
        "price": 4.99,
        "deluxePrice": 14.99,
        "image": "raspberry_juice.jpg",
        "createdAt": "2023-03-07T08:56:18.811Z",
        "updatedAt": "2023-03-07T08:56:18.811Z",
        "BasketItem": {
          "productId": 4,
          "basketId": 2,
          "id": 4,
          "quantity": 2,
          "createdAt": "2023-03-07T08:56:19.900Z",
          "updatedAt": "2023-03-07T08:56:19.900Z"
        }
      }
    ]
  }
}
```