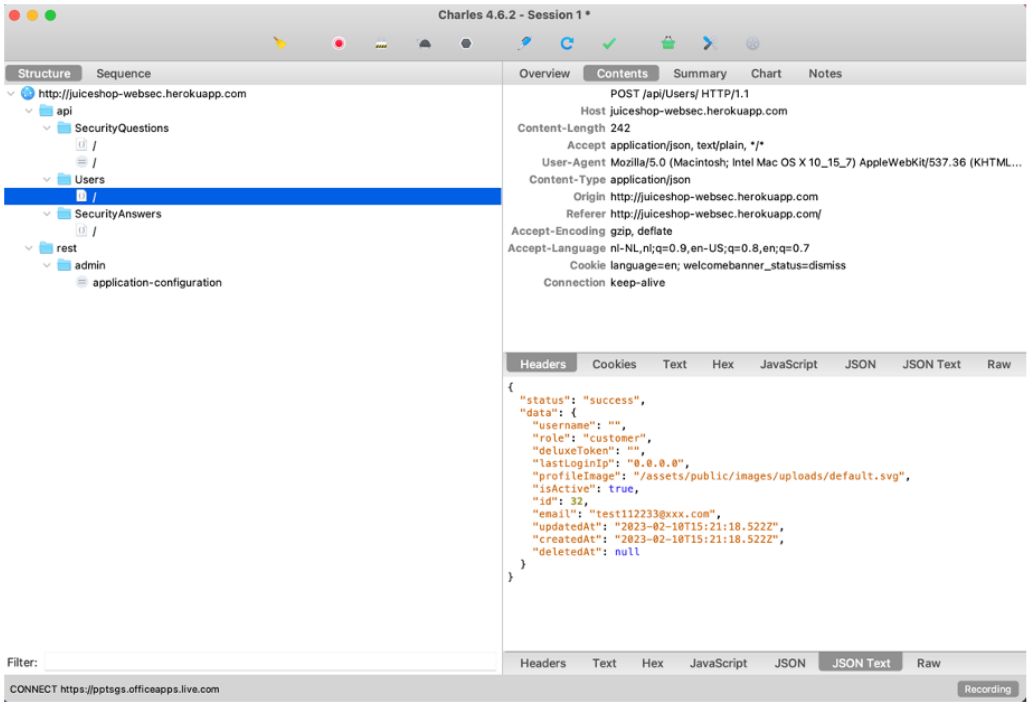
Oefening 1.3 Labo1

Gebruikte tool: CharlesProxy https://www.charlesproxy.com/
Target: http://juiceshop-websec.herokuapp.com/
Targeted Page: Register

Aanpak:

1. Ik open de tool Charles Proxy waar ik een sessie start.

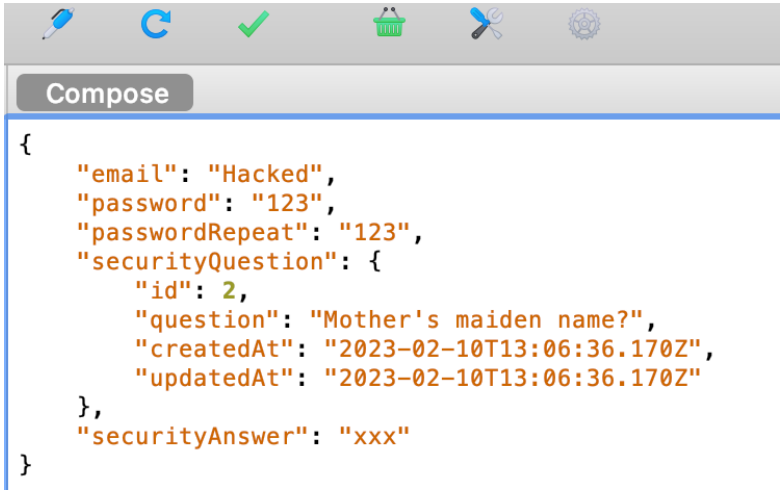
2. Op de register pagina van de target vul ik enkele test informatie in waarbij we na het drukken op registreren via de tool Charles de gemaakte request kunnen bekijken. (EXTRA: Ik zou eventueel enkel de request die gemaakt worden naar een specifieke server kunnen weergeven via een filter)



Afbeelding 1. Overzicht van onderschepte requests.

3. We zien dat er een post request is gemaakt naar http://juiceshop-websec.herokuapp.com/api/Users/ we merken op dat onze ingevulde gegevens ook zichtbaar zijn in de request content.

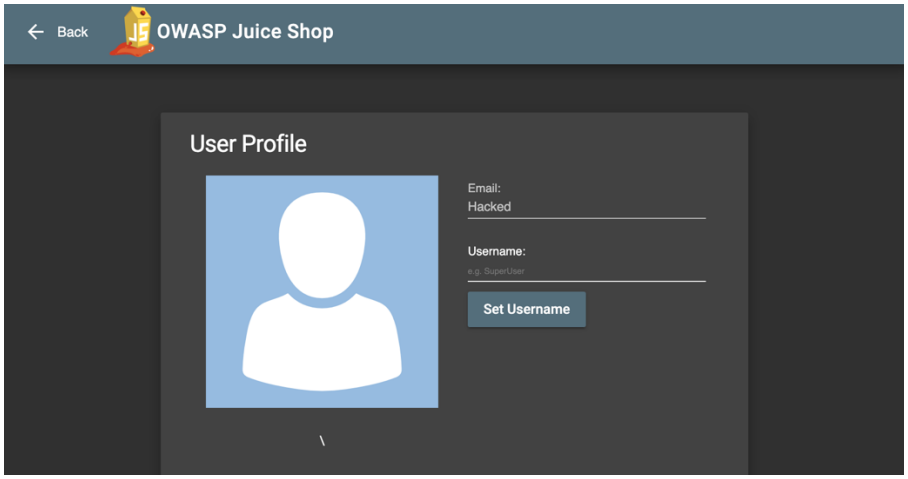
4. Vervolgens kunnen we op de (Pen knop) duwen om deze request te bewerken. Hier vullen we data in die we origineel via de borwser applicatie niet konden invoeren, en versturen we deze request door op execute te duwen.



5. We krijgen het volgende response. Met andere woorden, Het aanmaken van ons account met een nep e-mail is gelukt.


```
{
  "status": "success",
  "data": {
    "username": "",
    "role": "customer",
    "deluxeToken": "",
    "lastLoginIp": "0.0.0.0",
    "profileImage": "/assets/public/images/uploads/default.svg",
    "isActive": true,
    "id": 59,
    "email": "Hacked",
    "updatedAt": "2023-02-10T15:42:25.276Z",
    "createdAt": "2023-02-10T15:42:25.276Z",
    "deletedAt": null
  }
}
```


6. Resultaat is dat we vervolgens kunnen inloggen met ons bewerkt account



7. Conclusie: Er moet een serverside controle worden uitgevoerd. Een client side controle is enkel voor user experience