Introductie

Zoals altijd kunnen de oefeningen binnengehaald worden door een git pull te doen.

```
git pull
```

of de git repository te clonen als je deze nog niet hebt.

```
git clone https://github.com/similonap/software_security_2021.git
```

Wat ga je leren in dit labo?

- Gebruik maken van Chrome Developer Tools
- Gebruik maken van tools zoals postman, curl,...
- De werking van JWT tokens begrijpen en gebruiken.
- Concepten als secret key en expiration van een token begrijpen.

Stappenplan

1. Ga naar jouw eigen juice shop die je hebt opgezet in het eerste labo. De url zou er als volgt moeten uitzien als je de instructies juist hebt gevolgd:

   `https://owasp-juice-shop-xxxxxx.herokuapp.com/#/` *(vervang xxxxxx met je studentenkaart nummer)*

   Opgelet: Dit kan een tijdje duren om deze pagina te laden omdat de server terug moet opstarten. Hou hier rekening mee.

2. Open de Chrome Developer Tools en zorg ervoor dat de Network tab open staat.

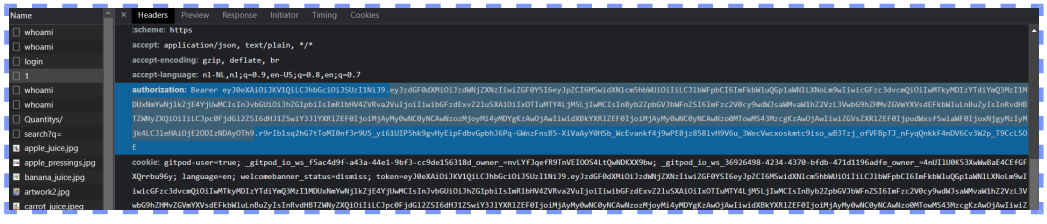
3. Log in als de administrator van de juice shop.

   Tip: Deze login gegevens heb je in vorige labo's gevonden.

4. Zoek nu de login request terug in de lijst van network calls in de Network tab.

   Open deze en ga op zoek naar de JWT token die wordt aangemaakt bij het inloggen.

   Neem een screenshot waar deze token duidelijk opstaat en sleep deze hieronder in



Vul ook hieronder de volledige JWT token in:

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWU
TdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiO
zL3VwbG9hZHMvZGVmYXVsdEFkbWluLnBuZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0Ijo
C0yNCAwNzo0MTowMS43MzcgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNjgyMzIyMjk4LCJleHAiOjE2ODIzN
GWnzFnsB5-XiVaAyY0HSb_WcEvankf4j9wPE8jz858lvH9V6u_3WecVwcxoskmtc9iso_wB3Tzj_ofVFBpTJ_nFyqQnkkF4n
```

5. Ga nu naar de Application tab en zoek in de `Local Storage` waar deze token wordt opgeslagen. Neem hiervan een screenshot en duid duidelijk aan waar het staat. Sleep deze hieronder in:

6. We gaan nu een aantal andere manieren bekijken om een request na te bootsen. We gaan eerst deze request leren uitvoeren via het curl commando.

   curl is een command line tool die toelaat http requests uit te voeren vanuit git bash.

7. Voer het commando

   `curl -i https://www.google.com/blabla`

   uit om te testen dat het bij jou werkt.

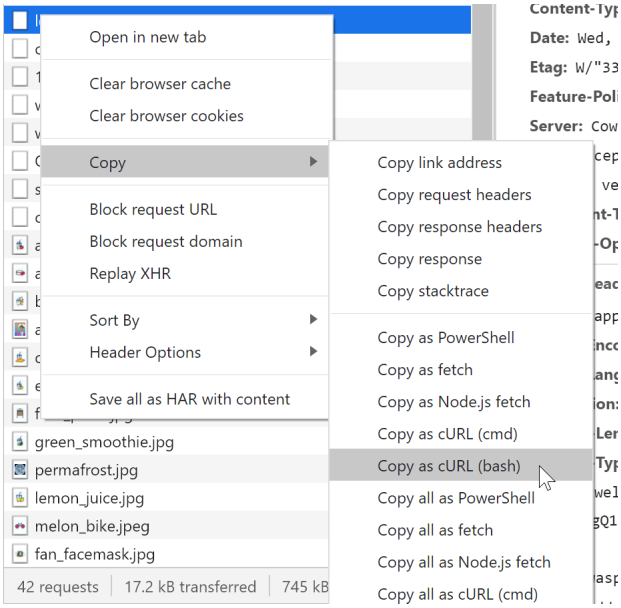
   De `-i` optie zorgt ervoor dat je ook de response headers en de http status code te zien krijgt.

   Welke status code geeft deze website terug en waarom?

```
404
Geen idee
```

8. De chrome developer tools laten het ook toe om http requests te kopieren als curl commando zodat je dit niet elke keer zelf moet ingeven.

   Kopieer de login request door er met je rechter muisknop op te klikken en dan vervolgens te kopieren als curl commando.



9. Plak dit commando in je `git bash` terminal in visual studio code. Pas dit commando wel nog aan zodat je ook nog de http response headers te zien krijgt.

   Neem een screenshot van het resultaat en zorg er voor dat de headers en de response body goed te zien is. Sleep deze hieronder in:

10. Ga naar de administration page van de juice shop en probeer (op het pad `/#/administration`). En probeer via de chrome developer tools de `authentication-details` url te vinden.

    Je kan deze kopieren door er met je rechter muisknop op te klikken, `copy` en dan `copy link address` te doen. Geef de url hier onder in:

    ```
    https://3000-juiceshop-juiceshop-737kq78t0de.ws-eu95.gitpod.io/rest/user/authentication-details/
    ```

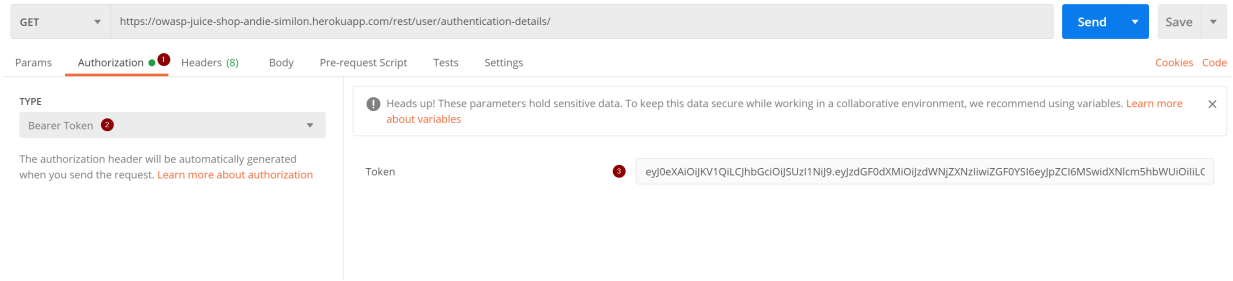
11. Installeer Postman door naar het adres https://www.postman.com te gaan en de installatie procedure te doorlopen.

12. Maak in postman een GET request naar de url die je in de vorige stap gevonden hebt (die van `authentication-details`)

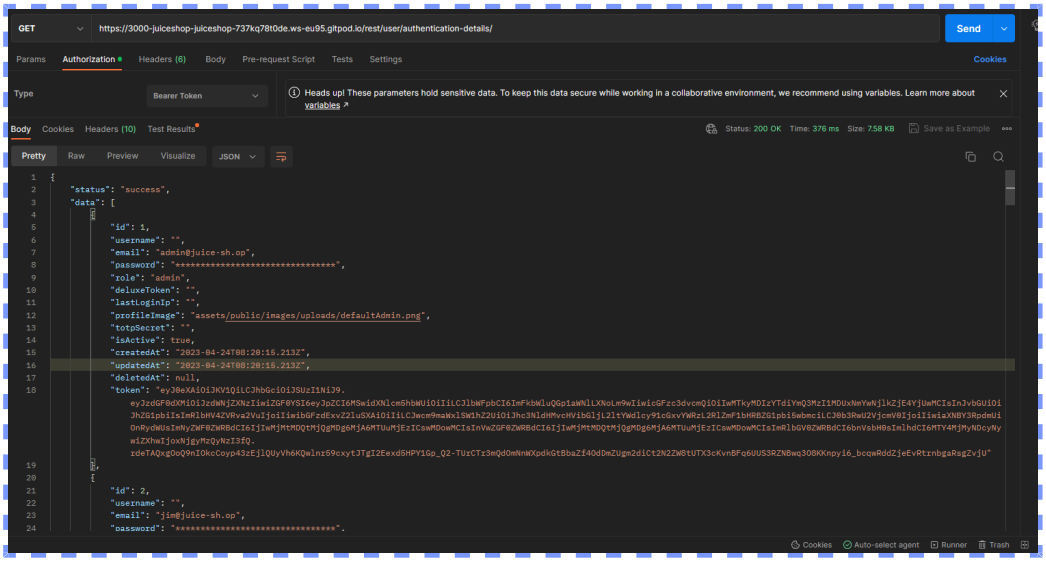
    Waarom werkt dit niet?

```
No Authorization header was found
```

13. Doe dezelfde GET request in postman maar geef deze keer de Authorization Header mee. Je doet dit op de volgende manier:



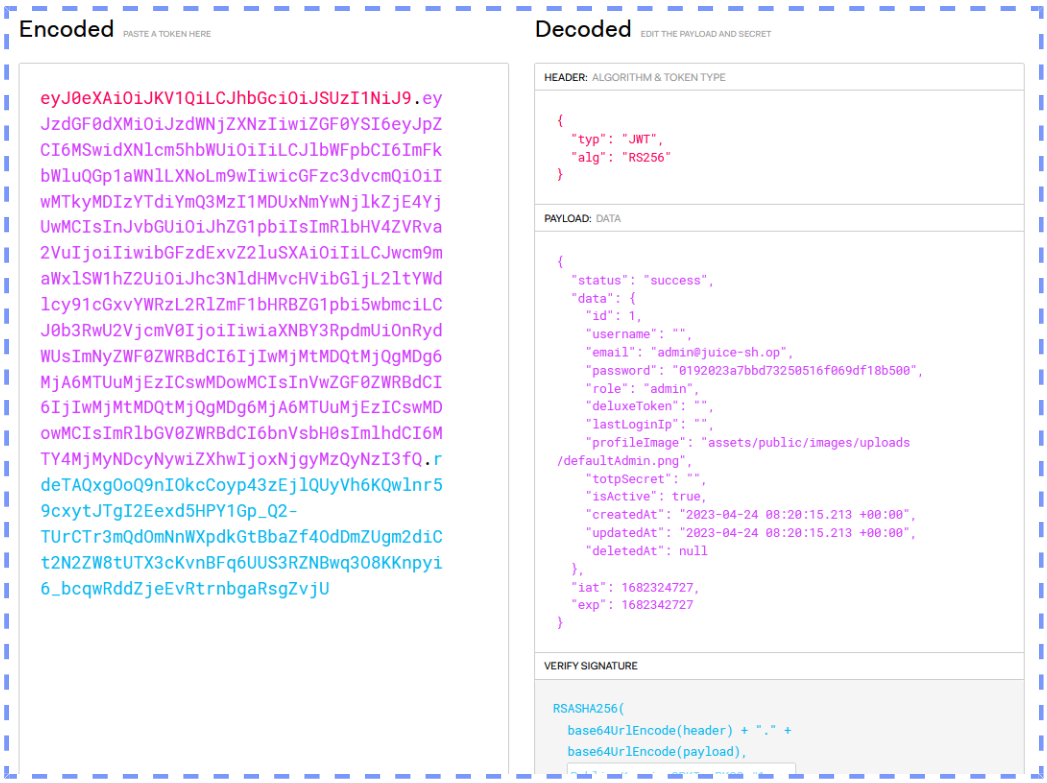
Neem een screenshot van het resultaat en plak dit hieronder in:



14. Je kan ook een volledige curl commando importeren in Postman. Kopieer het curl commando van de `authentication-details` en vervolgens doe je in postman: Import -> Raw Text en plak je de volledige curl commando van deze request hier in en druk je vervolgens op import.

15. Nu gaan we eens het token decoden zodat we kunnen kijken wat de inhoud ervan is. Ga naar jwt.io en ga naar debugger. Daar kan je het JWT token in plakken dat je hiervoor gevonden hebt.

    Maak een screenshot van deze website zodat het encoded gedeelte en decoded gedeelte duidelijk zichtbaar zijn. Sleep deze screenshot hieronder in:



16. Er zijn hier twee interessante velden. De expiration time (exp) en issued at time (iat). Op welke datum (en om hoe laat) vervalt deze token.

```
Mon Apr 24 2023 15:25:27 GMT+0200
```

Tip: De tijd is uitgedrukt in iets dat de unix timestamp heet. Dit zijn het aantal milliseconden sinds 1 januari 1970. Zoek zelf op het internet hoe je dit moet omzetten naar een leesbare datum.

17. Wat staat er in de payload van de jwt token dat er absoluut niet mag instaan?

```
"password": "0192023a7bbd73250516f069df18b500"
```

18. Gebruik het onderstaande token om de `authentication-details` endpoint aan te spreken (in postman).

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI
6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTk
yMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjo
iIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWF
nZXMvdXBsb2Fkcy9kZWZhdWx0QWRtaW4ucG5nIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnV
lLCJjcmVhdGVkQXQiOiIyMDIxLTAzLTMxIDEzOjMyOjU1LjQ1MiArMDA6MDAiLCJ1cGRhdGVkQXQiOiI
yMDIxLTAzLTMxIDEzOjMyOjU1LjQ1MiArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE2MTc
xOTc2NTksImV4cCI6MTYxNzIxNTY1OX0.Byi9R76JFCkYm4qIIMNrbfpymqGssIp7jSuQACkzme9Qrgo
qqjgndsFdEkjei74tPRr9gtepettgd5-
LCW6GEqrtAn47pNFrn98aBaDHz7lnJ6E5F8Vm7ZoiTHDOODHszqy4oDRORpME9CYyJMcII6mSauA6MJt
J5WIa6UmQolk
```

Wat geeft deze terug als response:

```
  "error": {
      "message": "jwt expired",
      "name": "UnauthorizedError",
      "code": "invalid_token",
      "status": 401,
      "inner": {}
  }
```

Waarom is dit?

```
de jwt token blijkt vervallen te zijn
```

19. We gaan nu eens een token proberen aan te passen. Kopieer het tweede deel (de payload) van de JWT token (na het eerste puntje) en decodeer dit deel met een base64 decoder (base64decode.org of burpsuite)

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.ey
JzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZ
CI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFk
bWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiI
wMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4Yj
UwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva
2VuIjoiIiwibGFzdExvZ2luSXAiOiJ1bmRlZmlu
ZWQiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHV
ibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG
1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY
3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjEt
MDQtMTcgMDk6Mzc6NDcuNzUyICswMDowMCIsInV
wZGF0ZWRBdCI6IjIwMjEtMDQtMTcgMTA6Mzk6ND
AuODU3ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsb
H0sImlhdCI6MTYxODY2MTgzMiwiZXhwIjoxNjE4
Njc5ODMyfQ.XJCdfnGI2idgdi3FlgLlCVjJfbrF
2J1Fe4fwJ2yY5yMB32x9M-CGYfiaT45qeQ-
MUIf0AmMV_CF_C2L3JdUk-
5RnbxBErlNMB5b3s6n6yy4ETk18CD7Xszth-
yROsXjRzRvO1xAdLlAHo7lAuuWM8yy7Ge__iOO_
izrqX19ICxY
```

20. Vervolgens pas je hier het email adres en de id aan naar iets anders en encodeer je vervolgens dit terug naar base64 (base64encode.org of burpsuite).

21. Kopieer nu dit stukje terug op dezelfde plaats in de JWT token waar het vandaan komt en gebruik nu deze token om de `authentication-details` endpoint aan te spreken (in postman)

    Wat geeft deze terug als response:

    ```
    "error": {
        "message": "invalid signature",
        "name": "UnauthorizedError",
        "code": "invalid_token",
        "status": 401,
        "inner": {}
    }
    ```

    Waarom is dit?

    ```
    de token in niet authentiek
    ```

22. Print deze pagina af als PDF en slaag deze op als `naam_voornaam_labo_tokens.pdf` en stuur deze door via digitap.