Input Validation 1

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 CSRF aanval
- het beschermen tegen een CSRF aanval

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 komt dan op een login pagina. Je kan eens proberen in te loggen met

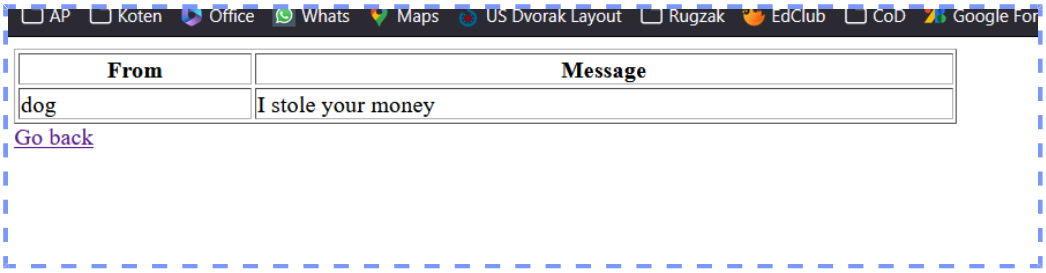
   ```
   username: dog
   password: hunter2
   ```

4. Pas de html file aan in de `public_cats` folder dat er naast het stelen van 100 euro ook automatisch een bericht wordt gestuurd naar dog waarin staat dat je het geld gestolen hebt. Je maakt hier gebruik van de `sendMessage` endpoint.

   Tip: Je gaat een extra iframe nodig hebben en een extra form. Deze moet je ook submitten a.d.v. javascript

code.

5. Start de `cats.js` server en voer de CSRF aanval uit. Neem een screenshot van het ontvangen bericht.



6. Gebruik net zoals de theorie de csurf library om een beveiliging in te bouwen tegen een CSRF aanval. Zorg ervoor dat alle forms een CSRF token hebben.

7. Probeer de CSRF aanval nog een tweede keer uit te voeren. Dit zou niet meer mogen werken.

8. Gebruik de chrome developer tools om de CSRF token aan te passen in het formulier. Welke error krijg je als je deze token aanpast en waarom?

```
 ForbiddenError: invalid csrf token

de token die nu in de post word meegegeven komt niet meer overeen met de token die voor die die pagina was meegegeven bij de get
```

9. 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_csrf.pdf
    - public_cats/index.html
    - views/login.ejs
    - views/main.ejs
    - index.js