

Introductie

In deze labo sessie gaan we ons bezig houden met het installeren van een onveilige web applicatie die we bij bepaalde labo's gaan gebruiken. Het is dus de bedoeling dat ieder van jullie een eigen versie van deze web applicatie gaan installeren.

Wat ga je leren in dit labo?

- Installeren van een web applicatie op heroku
- Onderzoeken van kleine security problemen in deze web applicatie.

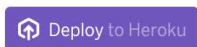
Stappenplan

1. Open je browser en ga naar de volgende website

<https://signup.heroku.com/>

en maak een account aan. Indien je al een heroku account hebt mag je deze stap overslaan.

2. Zorg ervoor dat je de volledige registratieproces hebt doorlopen en ingelogd bent in heroku.
3. We gaan nu de web applicatie installeren op heroku. Je kan dit doen door op de onderstaande knop te klikken:



4. Geef je applicatie een naam met de volgende structuur:

`owasp-juice-shop-xxxxxx` (vervang xxxxxx met je studentenkaart nummer)

Zorg er ook voor dat je 'Europe' als region kiest.



Deploy your own

[OWASP Juice Shop](#)

Probably the most modern and sophisticated insecure web application



[similonap/juice-shop#master](#)

App name

owasp-juice-shop-117852



owasp-juice-shop-117852 is available

Choose a region



Europe



Add to pipeline...

Deploy app

5. Als je op **Deploy app** klikt dan zal je web applicatie worden gedeployed. Dit kan tot 10-15 minuten duren. Dus wees geduldig en sluit je browser niet af.

Create app



Configure environment



Build app [Hide build log](#)



```
engines.npm (package.json): unspecified (use default)
```

```
Resolving node version 10 - 14...
```

```
Downloading and installing node 14.15.4...
```

```
Using default npm version: 6.14.10
```

```
-----> Installing dependencies
```

```
Installing node modules (package.json)
```

☒ Autoscroll with output

Run scripts & scale dynos

Deploy to Heroku

6. Als de applicatie gedeployed is dan zal je hiervan een melding krijgen in het groen:

Deploy app

Create app

Configure environment

Build app [Show build log](#)

Run scripts & scale dynos

Deploy to Heroku

✓

✓


✓

✓

✓

Your app was successfully deployed.

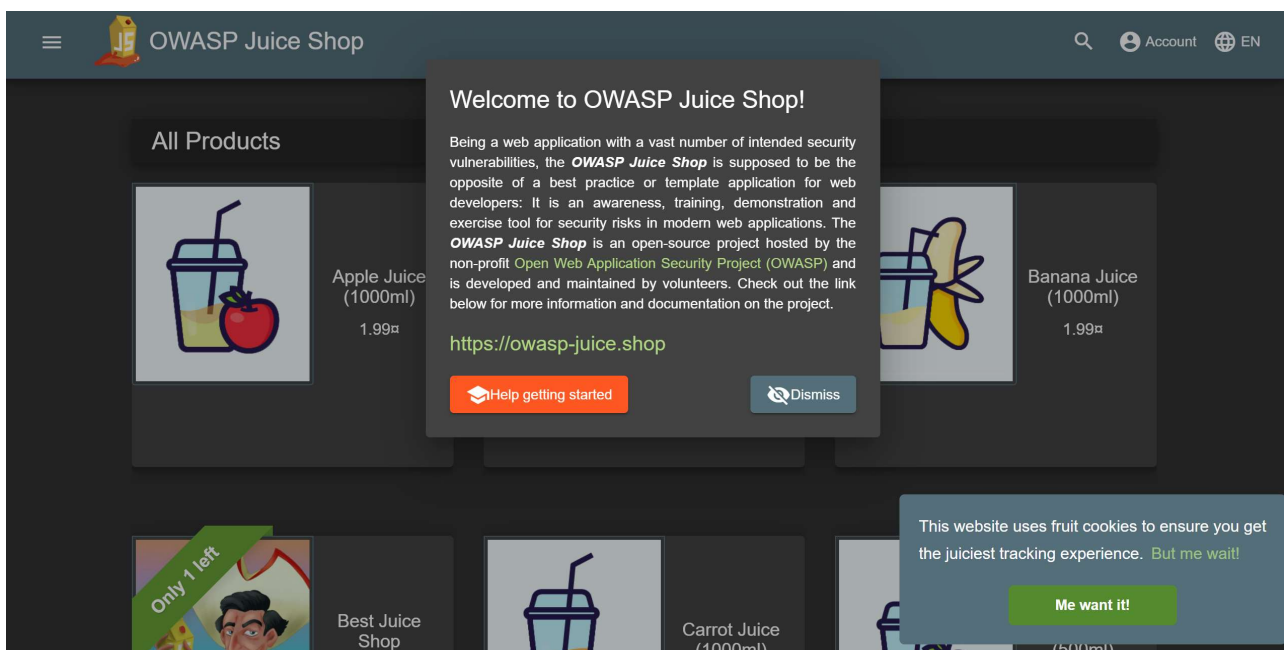
Manage App

 View

7. Als de deployment gelukt is kan je de web applicatie aanspreken via:

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

Je krijgt dan de volgende pagina te zien:



8. Je eerste opdracht is op zoek te gaan naar het score bord. Daar kan je jouw vooruitgang volgen. Je moet deze echter zelf proberen te vinden.

- Eerste tip
- Tweede tip

9. Op het score bord kan je je vooruitgang volgen. Let op deze vooruitgang wordt gewist als de webserver heropgestart wordt. Dit gebeurt op heroku vrij vaak.

10. Vul hier de url in die je hebt gevonden:

```
https://owasp-juice-shop-andie-similon.herokuapp.com/#/score-board
```

11. Een onoplettende werknemer heeft een directory niet goed beveiligd en iedereen kan zonder problemen aan de bestanden. Deze directory is genaamd 'ftp' en staat dus volledig publiek. Ga hier naartoe.
12. Vul hier de url in die je hebt gevonden:

```
https://owasp-juice-shop-andie-similon.herokuapp.com/ftp
```

13. Probeer een aantal files te openen. Waarom kan je sommige files niet openen?

```
Omdat je alleen .md en .pdf files kan openene
```

14. We gaan nu proberen het bestand `package.json.bak` te openen.

Dit gaat jammer genoeg niet zomaar.

Je moet gebruik maken van een `poison null byte` (%2500). Als je dit achteraan de url van het bestand plaatst, gevolgd door een van de bestandstypes die wel werken kan je wel het bestand openen.

▼ Een tip

```
package.json.bak%2500.md
```

15. Probeer nu zelf het eastere.gg bestand te openen en kopieer hier de inhoud:

```
"Congratulations, you found the easter egg!"  
- The incredibly funny developers  
  
...  
  
...  
  
...  
  
Oh' wait, this isn't an easter egg at all! It's just a boring text file! The real  
easter egg can be found here:  
  
L2d1ci9xcmlmL25lci9mYi9zaGFhbc9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndXIvcn5mZ3JlL3  
J0dA==  
  
Good luck, egg hunter!
```

16. Print deze pagina af als PDF en zend deze via digitap in.

Opmerking: Als dit niet lukt maak dan een zip file en stuur deze door.