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 gitpod.
- Onderzoeken van kleine security problemen in deze web applicatie.

Stappenplan

1. Open je browser en ga naar de volgende website

   https://gitpod.io/

   en log in met je github account. Heb je nog geen github account, maak er dan eentje aan.

2. Zorg ervoor dat je de volledige registratieproces hebt doorlopen en ingelogd bent in gitpod.

3. We gaan nu de web applicatie installeren op gitpod. Je kan dit doen door naar de volgende url te surfen:

   https://gitpod.io/#https://github.com/juice-shop/juice-shop/

4. Je zal zien dat er een aantal taken worden uitgevoerd. Dit kan even duren. Wacht tot dat de Open Preview Window (Internal Browser) verschijnt als de taken klaar zijn. Hoewel je de juice shop kan gebruiken vanuit de gitpod, is het handiger om de juice shop in een aparte browser te openen.

5. Let op dat de gitpod niet eeuwig blijft draaien. Als je de gitpod een tijdje niet gebruikt zal deze stoppen met draaien. Je kan dan gewoon terug je gitpod openen (https://gitpod.io/workspaces) en verder gaan waar je gebleven was.

6. 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

7. Op het score bord kan je je vooruitgang volgen. Let op deze vooruitgang wordt gewist als de webserver heropgestart wordt. Dit gebeurd op gitpod vrij vaak.

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

   ```
   https://3000-juiceshop-juiceshop-xp3nu7iw2ao.ws-eu86.gitpod.io/#/score-board
   ```

9. 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.

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

```
https://3000-juiceshop-juiceshop-xp3nu7iw2ao.ws-eu86.gitpod.io/ftp/
```

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

```
omdat; "Only .md and .pdf files are allowed!"
```

12. 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

13. 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:

L2d1ci9xcmlmL25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndXIvcm5mZ3JlL3J0dA==

Good luck, egg hunter!


https://3000-juiceshop-juiceshop-xp3nu7iw2ao.ws-eu86.gitpod.io/the/devs/are/so/funny/they/hid
/an/easter/egg/within/the/easter/egg
```

14. 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.