Introductie

In deze labo sessie kruipen we weer in de rol van white hat hacker die de Juice Shop die jullie vorige les hebben geïnstalleerd. Deze keer gaan we aan de hand van de tool BurpSuite het paswoord van de administrator brute force te hacken.

Wat ga je leren in dit labo?

- Installeren van BurpSuite.
- Brute force hacken van een paswoord.

Stappenplan

0. Als je gitpod gebruikt moet je er voor zorgen dat hij actief is en dat je er voor zorgt dat de web applicatie publiekelijk toegankelijk is. Dit kan je doen om op Ports te klikken en vervolgens op het slotje te klikken. Je zal dan zien dat de web applicatie nu publiekelijk toegankelijk is.

1. Open de registratie pagina van de juice shop web applicatie
2. Zijn alle paswoorden die je hier kan ingeven 'sterke paswoorden'? Zo niet, wat is er mis?

```
   (hoofdletters & kleiner letters)
3) Unieke characters (!,?,%) en cijfers (1,53,19)
```

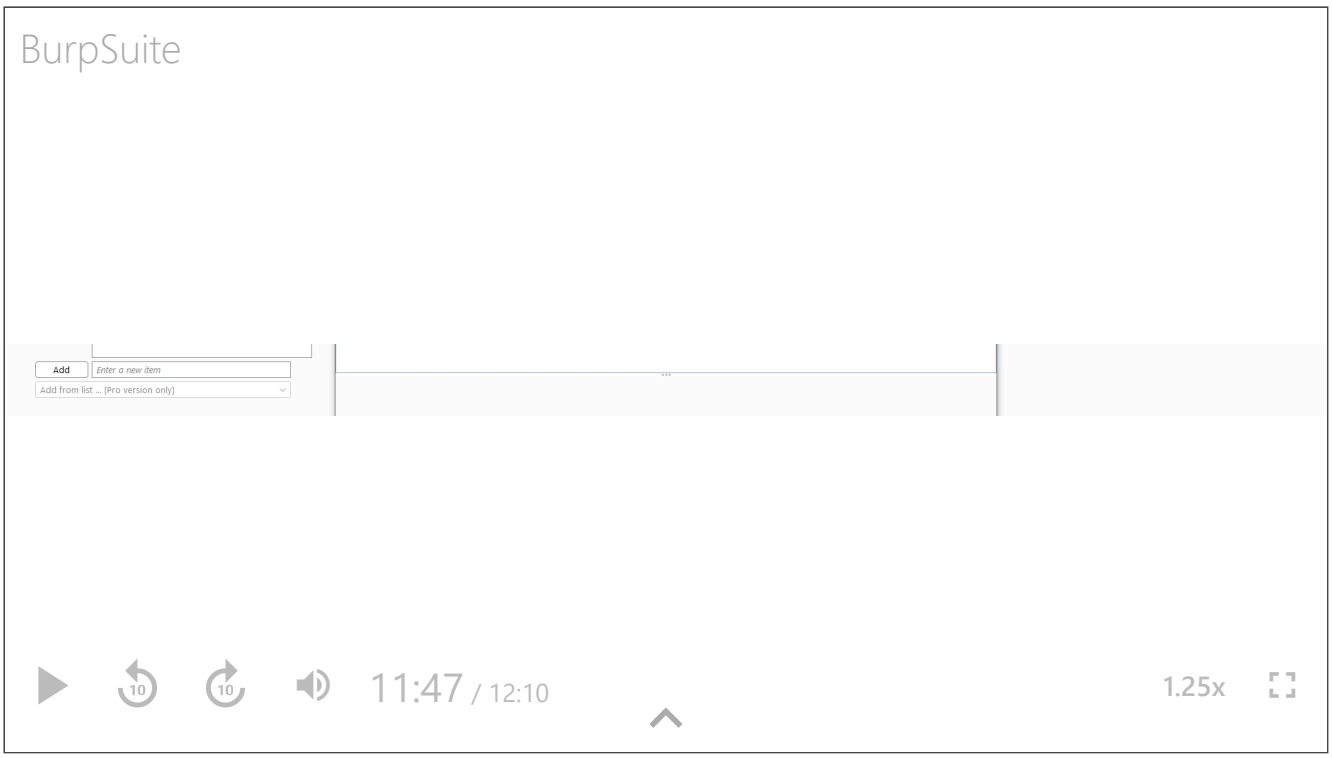
▶ Eerste tip

3. Open je browser en ga naar de volgende website

   BurpSuite

   en download de Community Edition van BurpSuite voor jouw platform.

4. Bekijk het filmpje over het installeren en de werking van BurpSuite proxy.



5. Vooraleer we kunnen beginnen met het kraken van het admin paswoord, moeten we op zoek gaan naar het email adres van de administrator.

   ▼ Eerste tip

   De email adressen van de gebruikers kan je gewoon uitlezen in de reviews van producten.

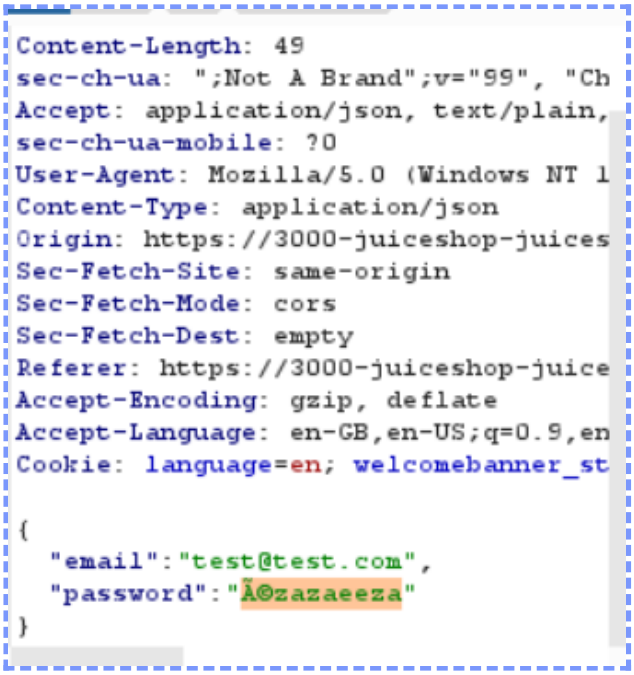
6. We gaan uiteraard niet zelf alle mogelijkheden proberen. We gaan hier gebruik maken van een paswoord list. Ga naar de website

   https://github.com/danielmiessler/SecLists/tree/master/Passwords/Common-Credentials

   Dit is een grote collectie aan text bestanden die allemaal onveilige paswoorden bevatten. Voor deze beperkte opgave hoef je alleen `best1050.txt` te downloaden.

7. Start Burp Suite op en gebruik de proxy om de request op te vangen waarmee je probeert mee in te loggen (Zie filmpje hierboven).

   Neem een screenshot van deze request en sleep deze hier onder in:



8. Gebruik deze request in de Intruder tool door op actions te klikken en vervolgens op 'send to intruder' te klikken. Ga vervolgens naar de intruder tab.

9. Zorg ervoor dat alleen het paswoord variabel is.

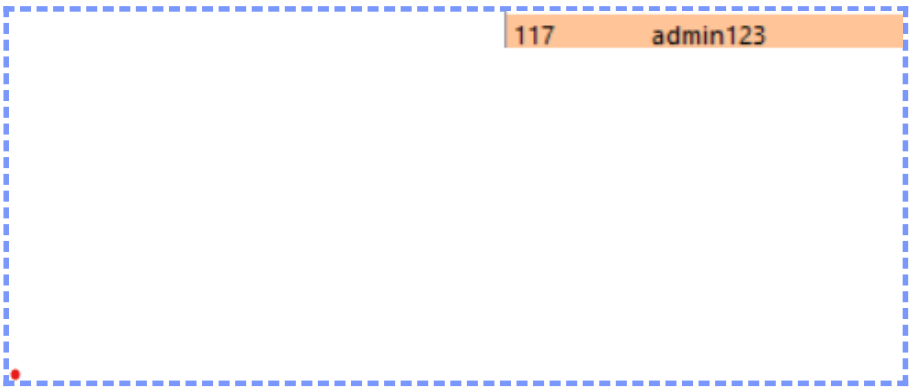
   ▼ Eerste tip

   Zorg ervoor dat er alleen bij het paswoord een § symbool staat.

10. Ga naar de payloads tab en zorg ervoor dat je de file `best1050.txt` gebruikt als paswoord lijst.

11. Start de aanval en maak een screenshot als het paswoord gevonden is.

    Sleep de screenshot hier onder in:

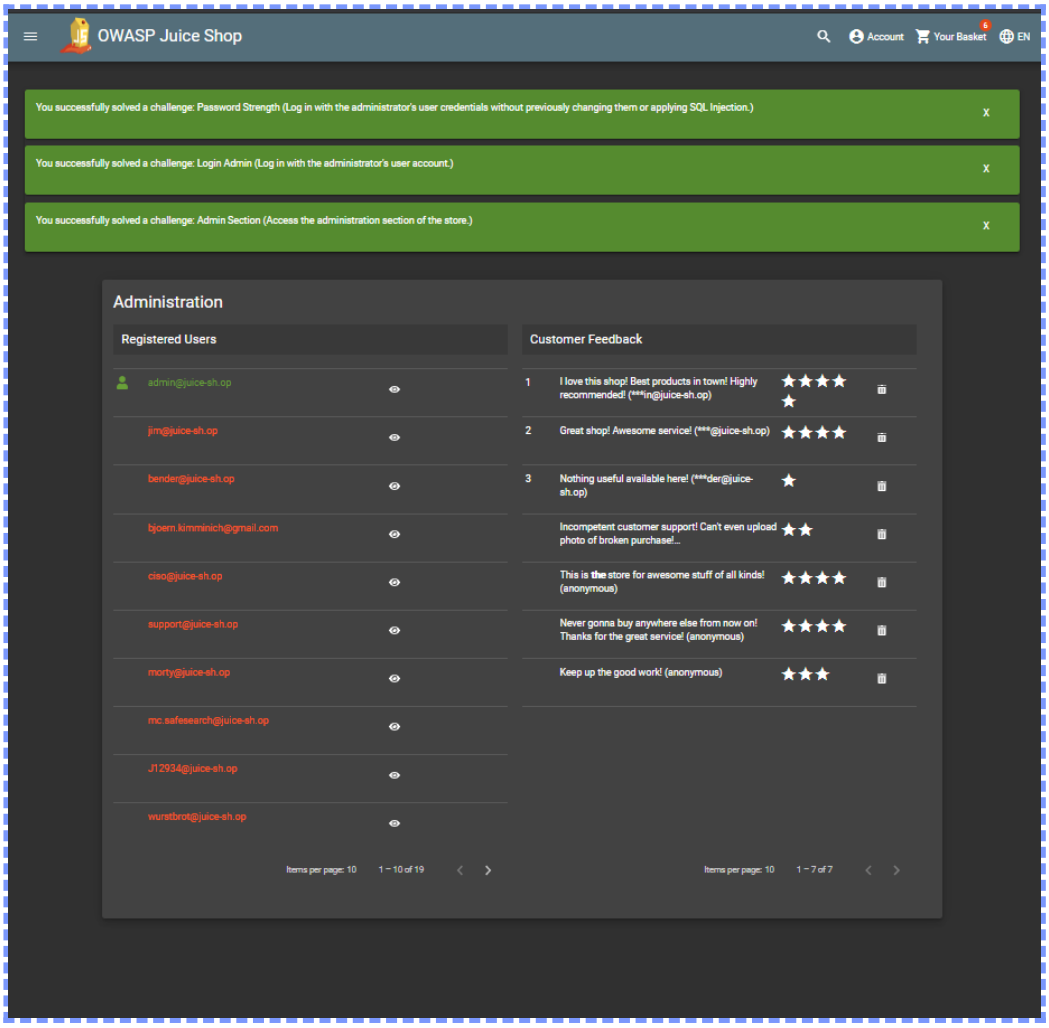


    Opmerking: Na maximum 200 pogingen zou het paswoord gevonden moeten zijn. Duurt dit langer, dan ben je op het foute spoor.

12. Vindt je dit een goed paswoord? Waarom wel/niet?

```
 vreselijk: Voorspelbaar, simpel, geen hoofdletters, opeenvolgende cijfers, geen speciale
characters
```

13. Spoor net zoals in vorig labo de 'administration' pagina op en log in met de admin email en paswoord. Neem hier een screenshot van en sleep deze hier onder in:



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.