| Juiceshop Walkthrough Diploma in CSF  Year 3 Apr 2022 (Semester 5) | 3 Stars |
| --- | --- |
| Practical |
| Payback Time | |

**OBJECTIVES**

* Learning how to exploit the insecure deserialization vulnerability and manipulate the check out and payment section.
* OWASP vulnerabilities:Insecure Deserialization, Software and Data Integrity(A08:2017, A08:2021)

**Prerequisite**

* Burp Suite

**Challenge – Payback Time**

* Place an order that makes you rich.
* Payback Time - Difficulty: 3/6 stars

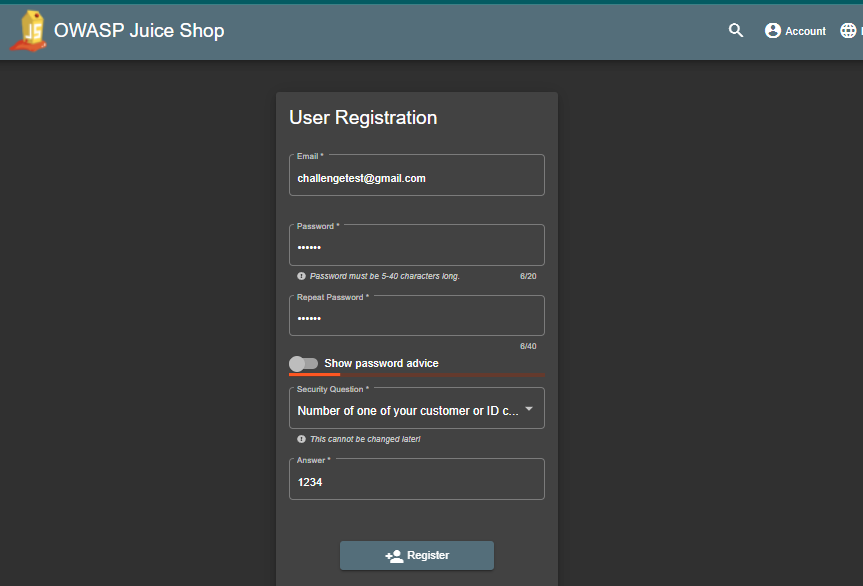
**Step 1**

Open Burp Suite and set Intercept to “Off” under Proxy tab. Click “Open browser” and head to your Juice Shop link

****

**~ Continue Practical below~**

**Step 2**

Create a new Juice Shop account and login

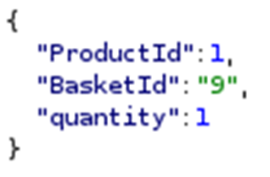
**Step 3**

Switch to Burp Suite and set intercept to “On”

**Step 4**



In Burp Suite click the button until you see these lines at the bottom



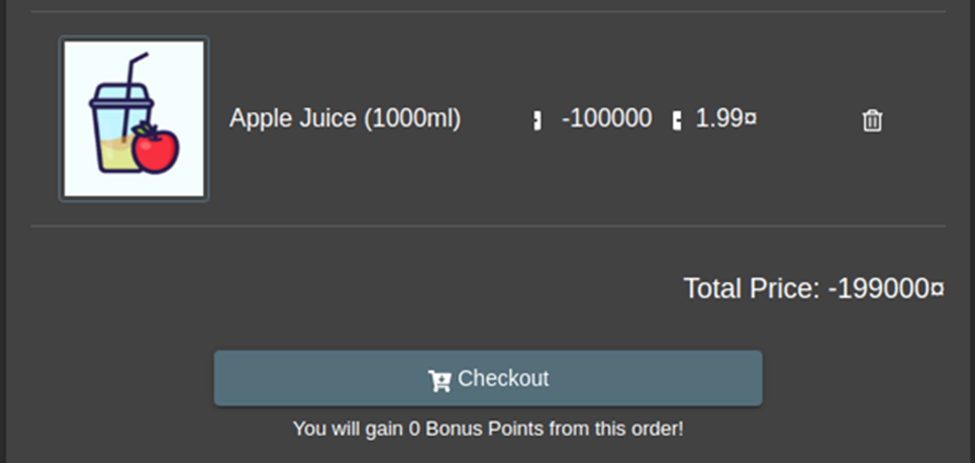
**Step 5**

Modify the “quantity” value to “-100000” and then turn intercept to “Off”



**Step 6**

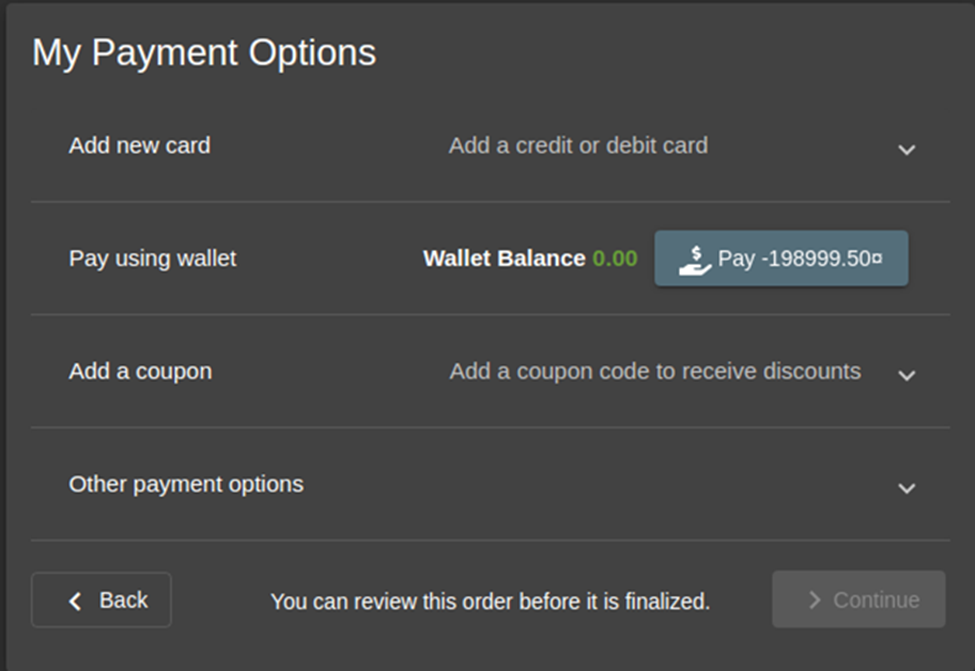
Return to the browser and check your basket



**Step 7**

Continue to Checkout – add a Delivery address and Delivery Speed

Click the blue “Pay” button



**Step 8**



Click and the challenge is complete



**~ End of Practical~**