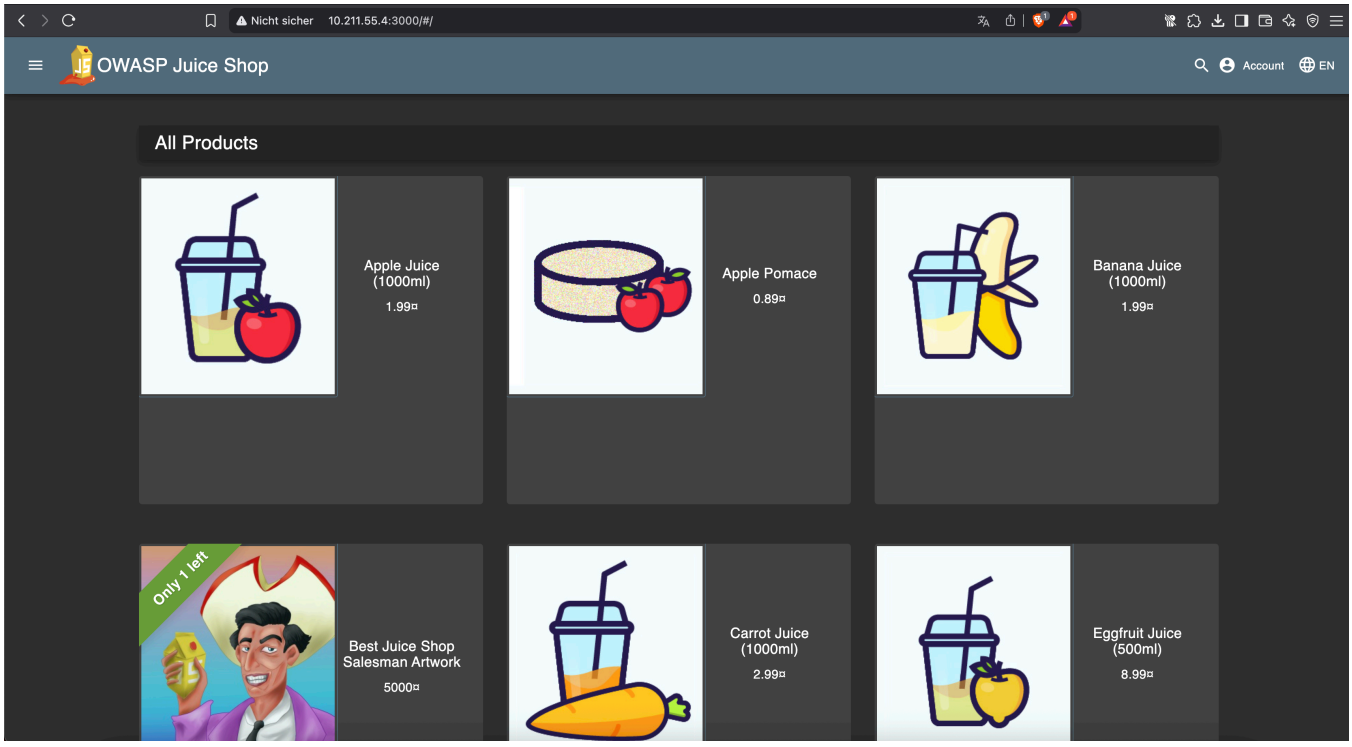
Netzwerksicherheit

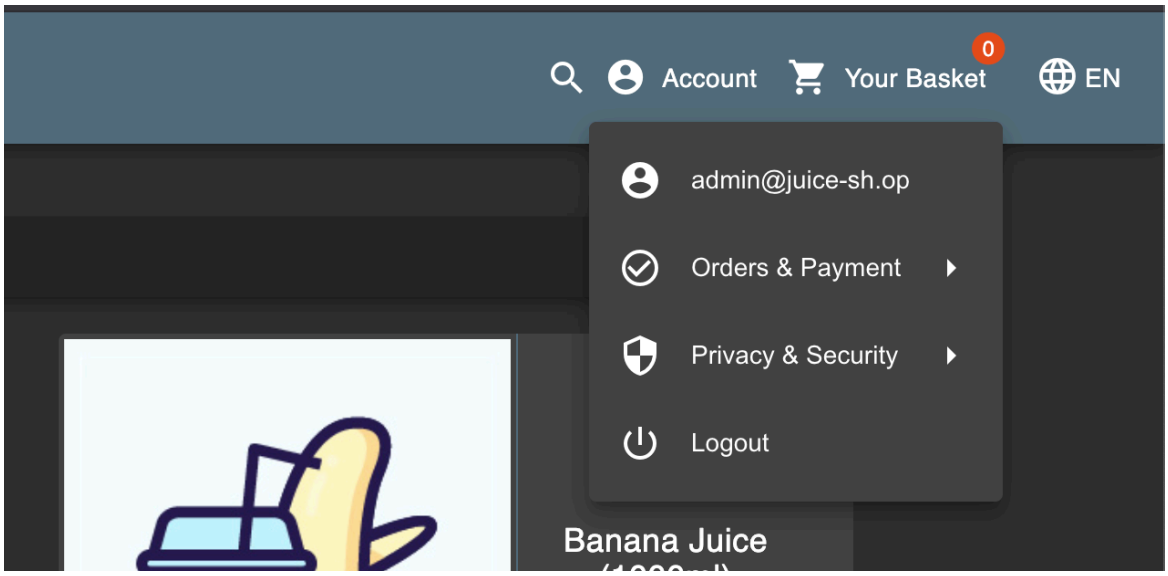
Task 6

Julian Bertol

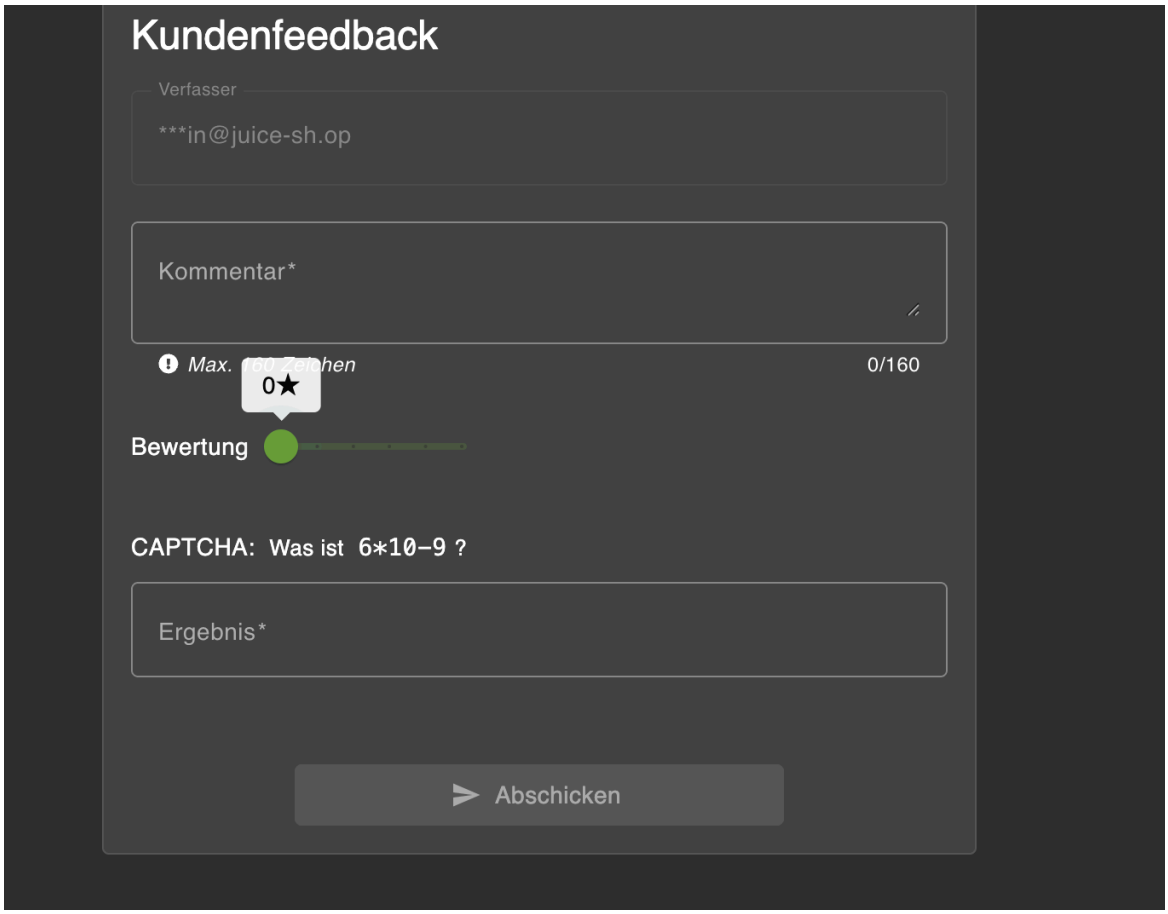
29. April 2025



Aufsetzen des Webshops. -> Docker Datei ausführen und Webseite aufrufen auf Port 3000



Mit Hilfe von SQL Injektion konnte ich mich als admin anmelden. Dafür muss man die Datenbankabfrage auf true setzten indem man 'or 1 – hinzufügt. So ist gibt die Abfrage immer true zurück.



Man muss den HTML Code etwas bearbeiten um 0 Sterne vergeben zu können.

Wie man in der Adminoberfläche sehen kann, wurden 0 Sterne vergeben.

Damit auch schon die nächste aufgabe

Adminbereich kommt man über die URL

http://10.211.55.4:3000/#/administration

Mit bender kann man sich auch über sql Injektion einloggen

User: bender@juice-sh.op'--

Password: egal

Funktioniert auch wieder durch das manipulieren der Datenbankabfrage

Die metriken kann man unter http://10.211.55.4:3000/metrics einsehen

Ich kann JS Code nicht direkt mit <script> ausführen. Eventuell gibt es da schon etwas was es verhindert. Aber mit diesem Trick <img src="x" onerror=„alert('test')"> funktioniert es. Da hier versucht wird ein Bild mit der quelle x die es nicht gibt einzubinden. Daher wird onerror aufgerufen und hier wurde dann javascript Code eingefügt.

Nun müssen die Konfigurationsdateien angepasst werden. Sobald NginX läuft, fungiert es als Reverse Proxy: Alle Anfragen gehen zuerst an NginX, das sie intern an den Webshop-Container weiterleitet. Dadurch ist der Webshop nicht mehr direkt von außen erreichbar.

NginX kann dabei einfache Sicherheitsprüfungen übernehmen, zum Beispiel bestimmte schädliche Zeichen in der URL oder im Anfragekörper blockieren. Auch der Zugriff auf interne Ports wird verhindert. Bekannte Sicherheitslücken der Webanwendung lassen sich dadurch schwerer ausnutzen.