Aufgabenstellung: Der OWASP Juice Shop ist eine interaktive, realistische Lernplattform für Sicherheitslücken in Web-Anwendungen. Eine Instanz für diesen Kurs ist unter `https://saftladen.css.net.in.tum.de` zu finden. Hier wird nur ein kleiner Teil der Möglichen Challenges, welche unter `https://saftladen.css.net.in.tum.de/#/score-board` zu finden sind, besprochen. Zuerst soll eine sogenannte *XSS* (Cross-Site-Scripting) Attacke durchgeführt werden. Wie kann das Suchfeld oben benutzt werden, um JavaScript-Code auszuführen? Testen Sie verschiedene Eingaben, u.a. von HTML-Code um zu verstehen, was passiert. Schauen sie im Entwickler-Tab ihres Browsers (F12 oder Rechtsklick → Inspect) an welcher Stelle im Code Ihre Eingabe eingefügt wird. Außerdem soll der Login überlistet werden. Hierfür soll eine *SQL-Injection* genutzt werden. Wie kann man sich als Admin anmelden, ohne sein Passwort zu wissen?

Hintergrundinformationen: XSS ist eine *Injection*-Attacke, d.h. wir nutzen aus, dass unsere Eingabe auf unvorhergesehene Weise verarbeitet wird. Wir nutzen hier aus, dass wir HTML-Code eingeben können, welcher dann direkt so in die neu geladene Website eingesetzt wird. Oft wird dies genutzt, um innerhalb des HTML-Codes JavaScript-Code auszuführen.

Eine SQL-Injection nutzt aus, dass wir SQL-Code an einem bestimmten Teil der SQL-Abfrage einfügen können. Eine typische SQL-Abfrage bei der Anmeldung auf einer Website, die Nutzername und Passwort abfragt, sieht wie folgt aus:

```
SELECT * FROM users WHERE username='x' AND password='y';
```

Hierbei sind x und y die Werte, die der Nutzer eingibt. Falls diese Abfrage ein Ergebnis zurückgibt (es also einen Nutzer mit Username x und Passwort y gibt), ist die Anmeldung erfolgreich. Wenn die Eingabe des Nutzernamen oder Passworts auch die Eingabe von SQL-Code ermöglicht, spricht man von einer SQL-Injection. Hierbei können Strings terminiert eingefügt werden, die Bedigungen für die Abfrage-Logik verändert oder Zeichen eingefügt werden, sodass alle nachfolgenden Zeichen ignoriert werden (–).