**INCIDENT REPORT: TS-18963-Offensive: Admin Page**

**Date: 06/14/24**

**Executive summary:**

User Story instructions were to access another user’s shopping basket, as well as delete five-star reviews in the Customer Feedback section

**Results:**

**Application Details:**

* **Application URL:** http://localhost:3000/#/administration

**Attack Narrative:**

Burp Suite was used to intercept GET traffic from my system. One of the intercepts included the user’s Basket number in the GET header. This was altered from “1”, which is the Administrator’s, to “2”, which allowed me to see another user’s basket.

The administrator page was located using the Chrome Console in the /main.js file, where the code lists various URL paths. This included the /administration directory.

Once the directory was added to the URL path in the address bar, I was able to access the stored Customer Feedback comments and a list of Registered Users. I was then able to remove the five-star review.

**Conclusion:**

The OWASP Juice Shop App is vulnerable to allowing the Administrator to access the shopping baskets of other users, in addition to having an exposed list of Registered Users and being able to alter Customer Feedback comments. Screenshots are included on the following page.



