**INCIDENT REPORT: TS-18954-Offensive: User Login**

**Date: 06/12/24**

**Executive summary:** The primary objective of this User Story is to gain a user’s login access to the OWASP Juice Shop Application without using the password input.

**Results**

**Application details:**

* Application URL: <http://localhost:3000>
* User Accounts: bender@juice-sh.op

**Attack Narrative:**

I conducted initial site reconnaissance and located the Login Page. I was also able to collect Bender’s email on product reviews on the site. I was able to conduct a SQL Injection attack by entering “bender@juice-sh.op‘–”, in the email input and I obtained Bender’s user access.

**Conclusion:**

This site is vulnerable to a basic SQL Injection Attack, which would allow an intruder to place product orders in Bender’s name and alter the User Profile, among other actions without the Bender’s consent.

