**Incident Report: KG-19107-Offensive:-User-Log-In  
Date:** 09-11-2024

### **Executive Summary**

In this task, I successfully accessed the account of another user, "Bender," by exploiting an SQL injection vulnerability on the OWASP Juice Shop login page. The objective was to gain access to Bender's account without using a valid password and capture the flag for this challenge.

### **Methodology**

To complete this task, I followed these steps:

* Located Bender’s email address, **bender@juice-sh.op**, by reviewing the comments left on items in the Juice Shop (specifically the banana juice review).
* Used SQL injection to bypass the password requirement by entering the following payload in the email field: **bender@juice-sh.op'--**
* Entered a random password of my choosing and submitted the form, successfully gaining access to Bender's account.

The SQL injection attack worked by truncating the query with '--, which comments out the rest of the SQL statement, allowing me to bypass authentication with the provided email address.

### **Findings/Solutions**

The SQL injection successfully bypassed the login for Bender's account, triggering the flag: "You successfully solved a challenge." This highlights the importance of using proper input validation, sanitizing user inputs, and enforcing strong authentication measures to prevent unauthorized access through SQL injection vulnerabilities.

**Project Description**

***YOU WILL NEED TO COMPLETE THE ADMIN LOGIN STORY TO COMPLETE THIS STORY***

Now that we know we can get into the admins account, let’s try accessing another user's account from the same login form. Access Bender's account and take a screenshot of the flag that pops up. Then submit this to your instructor along with an accompanying report.

Something to consider, is that all members of this site are required to use the same email domain.

Hint: This can be done with an SQL Injection