**Incident Report: KG-19105-Offensive:-Admin-Log-In  
Date:** 09-11-2024

### **Executive Summary**

In this task, I was required to gain access to the admin account of the OWASP Juice Shop application without using a password. I successfully bypassed the login authentication by leveraging an SQL Injection technique and obtained the admin login flag.

### **Methodology**

To achieve this, I used SQL Injection, a common attack technique that exploits vulnerabilities in the application's login page. I performed the following steps:

1. Navigated to the OWASP Juice Shop login page.
2. Entered an SQL Injection payload into the username and password fields.
   1. Username: ‘ OR 1=1–
   2. Password: 111 (Used Random Password)
3. Successfully logged into the admin account without providing a valid password, triggering a flag.

The SQL Injection method was chosen because it allows for the manipulation of queries sent to the database, making it possible to bypass authentication mechanisms.

### **Findings/Solutions**

The SQL injection worked, and I was able to log in as the admin. A flag popped up saying, "You successfully solved a challenge: Login Admin (Log in with the administrator's user account)." This really shows how important it is to have proper input validation and use query parameterization to keep web apps safe from SQL injection attacks.

**Project Description**

Using your Juice Shop application, log into the admin’s account without using a password from the login page.

Take a screenshot of the flag that pops up saying "You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)"

Be sure to write an incident report on your findings.

Hint: This can be done with an SQL Injection