**INCIDENT REPORT: BN-18976-Admin-Login**

**Date: 6/19/2024**

**Executive Summary:** I was tasked with logging into the Juice Shop web application's administrator account by exploiting a SQL injection vulnerability in the login form.

**Results**

* **Exploit Successful:** Gained unauthorized access to the admin account.
* **Vulnerability:** SQL Injection in login form.

**Application Details:**

* OWASP Juice Shop: Latest version
* Burp Suite Community Edition: v2024.4.4.5

**Attack Narrative:**

1. **Intercepted Login Request:** Used Burp Suite to capture the HTTP POST request sent when attempting to log in.
2. **Configured Intruder Attack:**
   * **Attack Type:** Sniper
   * **Payload Positions:** Email and password fields
   * **Payload List:** SQL injection login bypass payloads
   * **Launched Attack:** Initiated the Intruder attack to test various SQL injection payloads.
   * **Identified Successful Payload:** Observed a successful login attempt with a 200 OK status code when the following payload was used: ' OR 1=1--
   * **Bypassed Login:** Inserted the successful payload into the intercepted login request and forwarded it. Successfully logged in as the administrator without a password.

**Conclusion:**

This exercise emphasized the critical importance of sanitizing user input to prevent SQL injection attacks. It also showcased the effectiveness of Burp Suite's Intruder tool for automating the testing process. The vulnerability exploited here demonstrates the potential impact of SQL injection, as it allowed unauthorized access to a privileged account. Mitigating this type of vulnerability requires implementing input validation and parameterized queries on the server-side.