**Incident Report:** CH-15100-Offensive-Admin-Access

**Date:** 10-22-2022

**Executive Summary:**

Test the OWASP Juice Shop application’s security by creating a new user account with admin privileges.

**Action Steps:**

To complete this task successfully, I took the following actions, in order:

1. Opened the OWASP app in browser with Burp Suite running in the background
2. Navigated to log-in page
   1. Clicked “Not yet a customer?” link
3. Completed and submitted User Registration form
4. In Burp Suite:
   1. Located the HTTP Request in the HTTP History list on the Proxy page
   2. Reviewed the details of the Response and Request
      1. Noted the presence of a “role” object with a corresponding “customer” variable
   3. Right-click → Send to Repeater
   4. Within Burp Repeater:
      1. Modified the Request details as follows:
         1. Changed the inputted username to create new account
         2. Added a “role” object with “admin” variable
      2. Clicked Send to create a new account with escalated privileges

**Consequences of Attack:**

This security test revealed the following exploitable vulnerabilities within this web application:

* Code injection
* Improper input validation
* End-point or API mass assignment

These vulnerabilities occur when an application automatically binds client-provided input to internal object properties, granting an attacker access to data items that are normally restricted.

The consequences of these vulnerabilities leave an application at-risk of an attacker:

* bypassing security measures
* escalating specific users’ privileges
* compromising data integrity
* accessing sensitive data, such as PII
* tampering with data

**Mitigation Strategies:**

Protection against these types of attacks include:

* Server-side validation (in addition to client-side)
* Avoiding input binding directly and using Data Transfer Objects instead
* Explicitly defining schemas for data payloads with allow lists