Incident Report

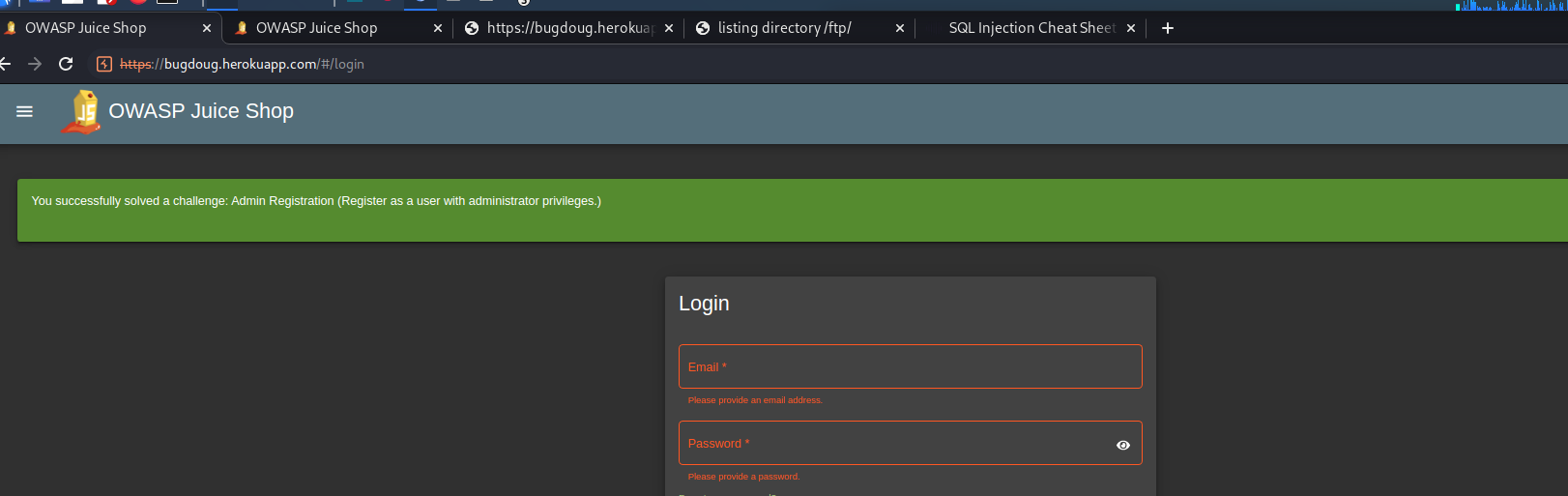
13183 Offensive: Admin Access

Date: 6/2/2022 (DS)

# Executive Summary:

ProsperSec was contacted by The Tech Academy to conduct penetration testing on a new Juice Shop application. The main goal was to see if there was a way to upgrade a regular user account to an admin account.

**Results**:



**Application Details:**

Application URL: bugdoug.herokuapp.com/#/login

User Account: bobb@gmail.com

**Attack Narrative (Steps):**

* Using burp, I tracked what the HTTP history looked like when I registered as a new user.
* When I was looking at the In the post response to the API, it shows that there is a “role” section that is filled as a “customer”.
* This API request was then sent to the repeater tab.
* This role was then replicated by placing the “role” line in the request section and trying out admin to see if it works.
* The request was sent and it successfully made a user with an admin role.

**Conclusion:**

ProsperSec was contracted to find vulnerabilities in the application, Juice store is unsafe due to an API that allows attacks allowing *any* new user to upgrade to an admin role.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_