**Incident Report:** CH-15060-Offensive-User-Login

**Date:** 10-19-2022

**Executive Summary:**

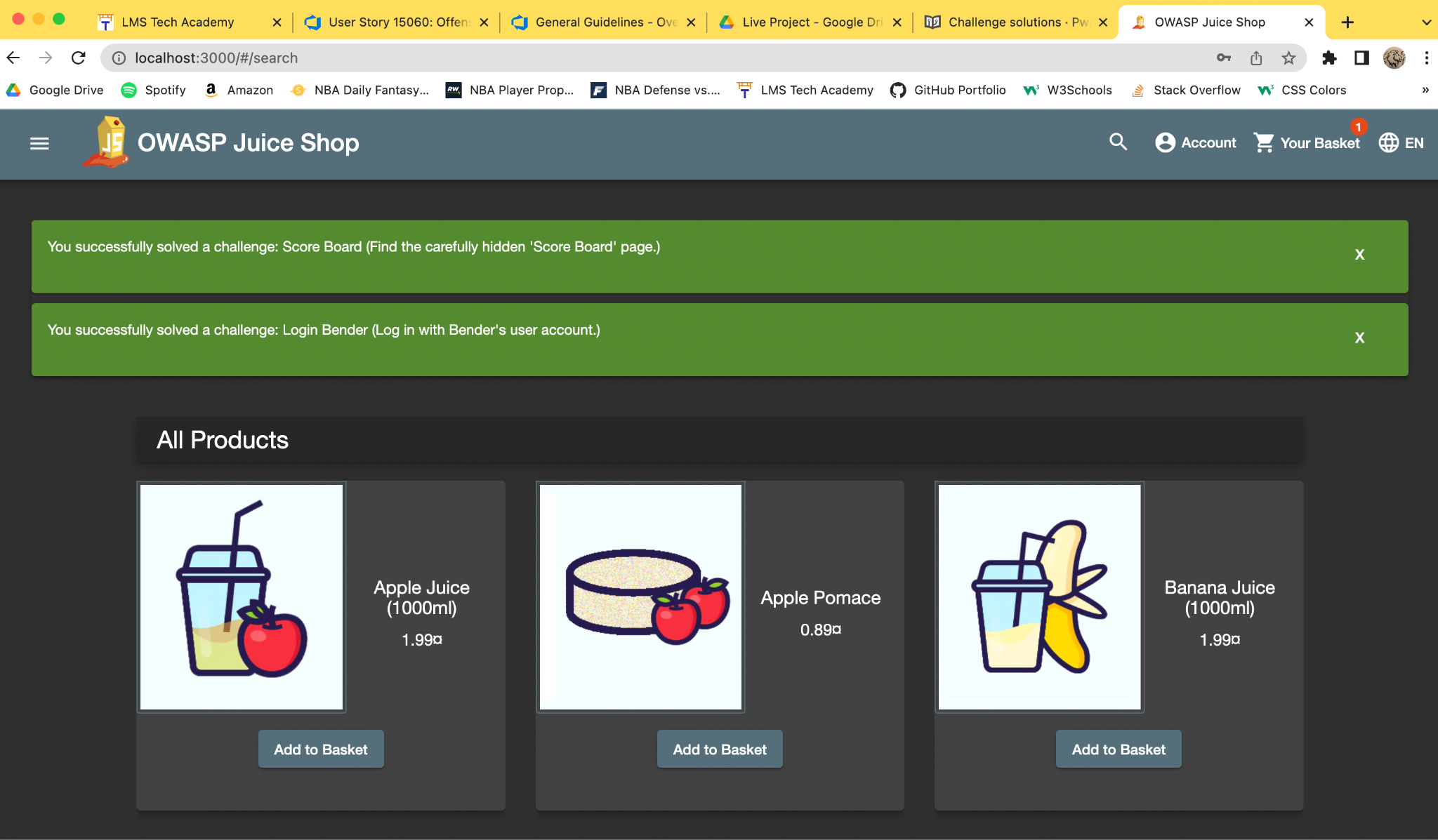
Using OWASP Juice Shop application, successfully log into Bender’s user account.

**Methodology:**

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

1. Reviewed notes from last challenge:
   1. Learned from the Admin Login Story that the email domain for this app’s users is **@juice-sh.op**
      1. Using Burp Suite to intercept the POST Login request in the last challenge → admin user email was listed in the Response box ([admin@juice-sh.op](mailto:admin@juice-sh.op))
   2. Based on the hint provided in the task requirements for this Story, it was safe to assume that Bender’s email login was his name @juice-sh.op
2. With OWASP app still running:
   1. Browser navigated to <http://localhost:3000/#/login>
   2. In the email input field: **bender@juice-sh.op –**
   3. In the password input field: **password**
3. Login was successful:
   1. During the last challenge, I successfully determined how to bypass the need for passwords to be entered into the login form
   2. Changed query to SELECT \* FROM USERS WHERE email = ‘[bender@juice-sh.op](mailto:bender@juice-sh.op)’
      1. Adding -- to the end of my input value means that the rest of the query will be ignored; no password is required

**Findings/Solutions:**

****