Incident Report

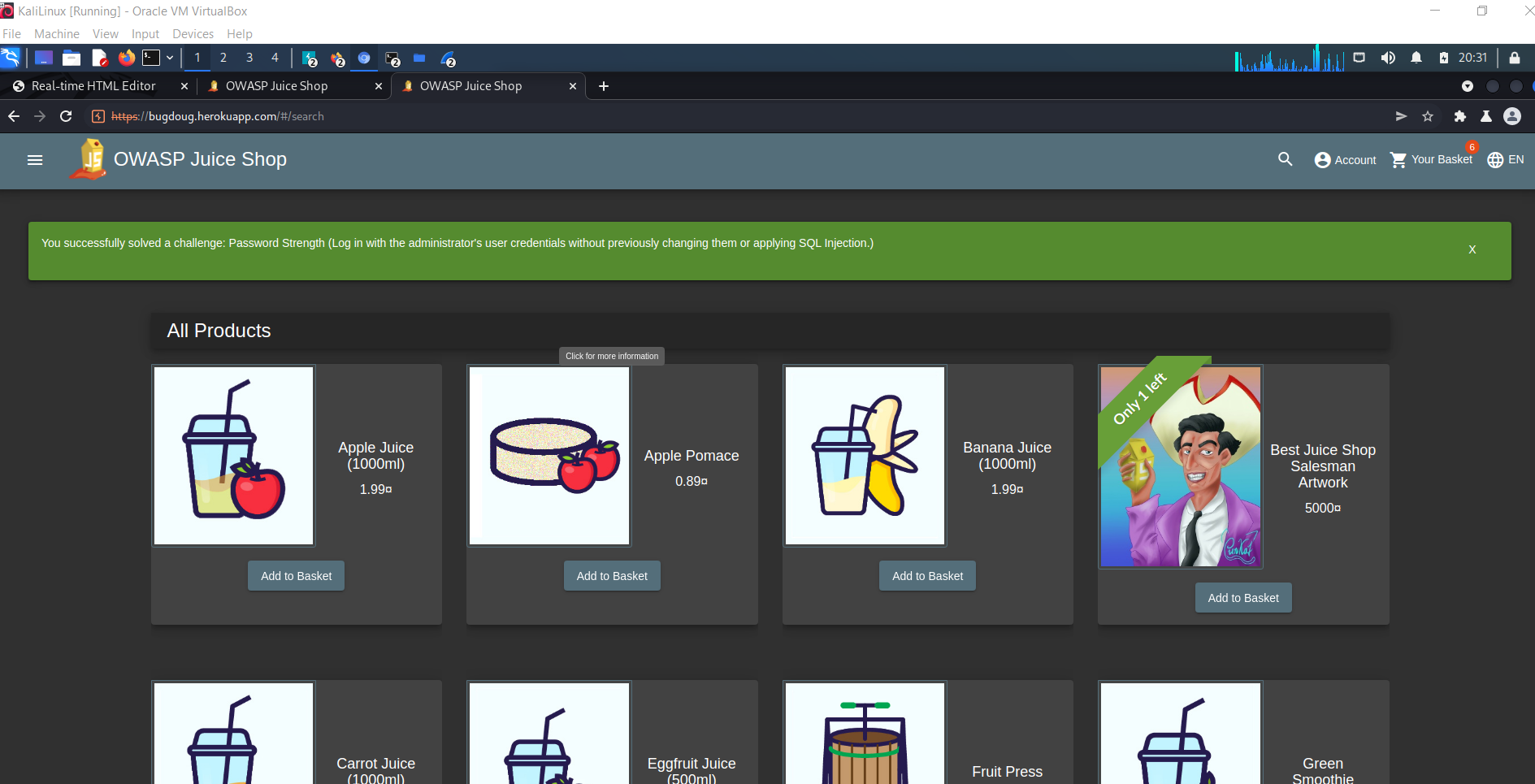
13147 Offensive: Reset Admin Password

Date: 5-27-2022 (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 the admin password could be accessed and reset using Brute Force with a payload.

**Results**:



**Application Details:**

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

User Account: admin@juice-sh.op

**Attack Narrative (Steps):**

* I first captured a login request from the proxy intercept in the Burp application.
* I then sent this request to the intruder tab.
* I then downloaded a list of commonly used passwords into the payload section of the intruder section.
* I then made sure that the parameter that the attack would be set in the “password” section and that the user would be the admins user account.
* I then started the attack and watched for a successful code, alerting me that the password led to a successful entry.
* After trying the password in the actual site to make sure it worked, I was able to successfully not only enter as admin but also change the password to whatever I liked.

After loading a list of simple passwords into Burp, I was able to set up a Brute Force attack using the most common passwords, which ended up finding **admin123**.

**Conclusion:**

ProsperSec was contracted to find vulnerabilities in the application, Juice store is unsafe due to a major breach in the admin account using a very simple brute force attack. The result was I was able to get into the admin account and actually reset the password, holding the account and therefore the site hostage.

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