**Incident Report:** CH-15080-Offensive-Reset-Admin-Password

**Date:** 10-20-2022

**Executive Summary:**

Using OWASP Juice Shop application and Burp Suite, perform a brute force attack in order to discover the admin account password. After logging in successfully, change the password to something different.

**Methodology:**

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

1. Downloaded the best1050.txt file by accessing the GitHub link provided
   1. Saved file to local drive
2. Navigated to the OWASP Juice Shop account login page
3. Opened Burp Suite
   1. Turned Intercept ON in Proxy tab
4. Back in OWASP app:
   1. Made initial login attempt
      1. Used known admin username ([admin@juice-sh.op](mailto:admin@juice-sh.op)) and random password (“password”)
      2. Clicked “Login”
5. In Burp Suite:
   1. Selected the POST Login Request from the HTTP History list in Proxy tab
   2. Right-click → Send to Repeater
6. In Repeater tab:
   1. Reviewed details of login Request and Response
   2. Right-click → Send to Intruder
7. In Intruder tab:
   1. Under Positions:
      1. Set Attack type to “Sniper”
      2. In Payload Positions section:
         1. Removed all highlighted payloads using the “clear” button
         2. Highlighted the payload value in the password identifier of the Request (“password”) and clicked “add” button
   2. Under Payloads:
      1. In Payload Options [Simple List] section:
         1. Clicked “load”
         2. Uploaded best1050.txt file from local drive
   3. Clicked “Start attack”
      1. Scanned results window for status code 200 OK (successful HTTP Response)
         1. **Request 117, Payload admin123**
         2. HTTP Request details for this payload revealed the auth token and password for this user account (**old password = admin123**)
8. Back in browser:
   1. Login credentials confirmed
      1. Account homepage displayed
   2. Under Account menu in upper-right corner:
      1. Privacy & Security → Change Password
      2. Account password updated:
         1. **New password =** **!36JtkB**

**Findings/Solutions:**

