**Incident Report: KG-19106-Offensive: Reset Admin Password  
Date:** 09-10-2024

### **Executive Summary**

In this task, I used Burp Suite to perform a brute force attack on the admin account of the OWASP Juice Shop application. Using the **best1050.txt** wordlist, I successfully discovered the admin's password and then reset it to a new password of my choosing.

### **Methodology**

To complete this task, I followed these steps:

1. **Downloaded the Wordlist:**I downloaded the **best1050.txt** wordlist from GitHub and saved it locally on my machine.
2. **Set Up Burp Suite:**Opened Burp Suite and configured it to intercept HTTP requests by setting up a proxy in my browser. I navigated to the Juice Shop login page and submitted a login attempt with the admin's email (**admin@juice-sh.op**) and a random password to capture the request.
3. **Captured the Login Request:**Burp Suite intercepted the HTTP POST request. I then sent this request to Burp Suite's Intruder tool.
4. **Configured Intruder for Brute Force Attack:**I marked the password parameter in the request and loaded the **best1050.txt** wordlist in the Payloads tab. The attack type was set to "Sniper."
5. **Executed the Brute Force Attack:**I initiated the brute force attack, which tested all passwords in the wordlist. The correct password was identified based on the response length, which differed from the others.
6. **Reset Admin's Password:**After successfully logging into the admin account with the discovered password, I navigated to the Profile section and reset the admin’s password to a new one of my choice. The old password was **admin123**, and the new password I set was **admin1234**.
7. **Flag Confirmation:**After successfully resetting the password, a flag popped up confirming the task was completed.

### **Findings/Solutions**

The brute force attack was successful, and I was able to reset the admin password. This demonstrates the importance of protecting login forms with mechanisms like rate-limiting, multi-factor authentication, and strong password policies to prevent brute force attacks.

**Project Description**

You have gained access to two different accounts on OWASP Juice Shop now, but we do not know the passwords for them. Set up a brute force attack with Burp Suite to login as the admin using a list of common passwords, and then reset the admin’s password to your liking. Write a report including the steps taken, the old password, the new password you set, and a screenshot of the flag that pops up once you've successfully reset the admin's password.

Use the best1050.txt wordlist for your attack, the download link is below:

<https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/best1050.txt>