# Incident Report: MR-10241-ResetAdminPassword

**Date:** 10-8-2021

## Executive summary:

I was tasked with doing a brute force attack on the admin account and changing the current password to one of my own. The tool I used was Burp Suite because this is a reliable brute-force attacking tool.

## Results

## Application Details:

- **Application URL:** https://mr-ttabookstore-104.herokuapp.com/#/login
- **User accounts:** bender@tta.bookstore

**Conclusion:**

Like I stated earlier in this report, I was tasked with brute force attacking my way into the admin account and changing the password to my liking. To do this, I used Burp Suite. The first step I took was to open Burp Suite and make sure that I was intercepting my traffic. Once I got Burp Suite to intercept my traffic, took that POST request and sent it to the Intruder. After opening the intruder tab, this is where I inserted my payload. The payload I used was given to me. Here is the URL to that payload: https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/best1050.txt. Now that the payload is uploaded into Burp Suite, I pressed the attack button and waited for Burp Suite to work its magic. I was able to determine which attack was successful by looking at the length column. I found an attack with a larger length than the rest. I went back to the browser and entered in this password and it worked. The majority of the password attempts had a length of 394 and the successful one had a length of 1205. Now that I know the password of the admin account(admin123), I was able to log into the account and change the password. The password that I chose was

something simple: hacked. The flag that I got was:

ff4aebffe31b0ffdea9bdd0207a16a3c01ac6c56. Below is a screenshot of the flag as well.

You successfully solved a challenge: Password Strength (Log in with the administrator's user credentials without previously changing them or applying SQL Injection.)

X

🏳 ff4aebffe31b0ffdea9bdd0207a16a3c01ac6c56     📋 Copy to clipboard