**Incident Report 11896: Reset Admin Password**

**03/04/22**

**Flag:**

**Executive Summary:**

| For this two-part story we will be using Burp Suite to intercept HTTP requests.  Part 1: Gain access to another user's shopping basket.  Part 2: Leave a 0 star review on a product.  Take a screenshot of the HTTP request that you used for both attacks and write a report on your findings.  **Results**  User name: admin@tty.bookstore  Password: admin123  New password: asdfg  **Application Details:** https://ttabookstore.herokuapp.com/  **Attack Narrative:** Performed a cluster bomb, brute force attack using Burpsuite with a custom wordlist to figure out the admin password. I then logged in to the account. .  After that, I was able to change the passwords for this account.  **Conclusion:** To avoid attacks like this in the future, be sure to use passwords that are over 20 characters long that combine Uppercase and lowercase letters as well as numbers and symbols. It is also a good idea to incorporate two factor authentication.   |  | | --- | |  | |  | |
| --- | --- | --- | --- |

Screenshot

