**Incident Report 11897:Offensive HTTP requests**

**03/04/22**

**Executive Summary:**

There are two weaknesses in the shopping portion of the TTA bookstore app

1. Allowed me to view and a add a product to someone else's cart
2. Allowed me to write a review as another person

**Results**

**Application Details:**

**Attack Narrative:**

To view and edit another person’s cart:

Use the interceptor feature of Burpsuite.

Turn on the interceptor and add a product to the cart.

Go to the request in Burpsuite and add a second “basket number”. Made the 2nd basket number “3” instead of my own number(number 1).

Forward the edited request. Success!

To write a review as another person:

Write a review on TTA website.

Turn on Burpsuite interceptor.

Edit the review.

Look at http history. Find “Get” product reviews line

Copy id number of different review requests.(You will see it listed with your own edit)

Forward “edit” request

Edit the edit request and change id number to the one that you copied

Forward request.

Success

Go to intercepted edit request in Burpsuite and edit user ID

Forward to website; Success

**Conclusion:**

To Protect against attacks like this in future, it is recommended that login requests utilize secure headers., pre-login cookie, anti-CSRF(Cross Site Request Forgery) token, CAPTCHA, and even a second factor such as an RSA token. All user input fields should be sanitized and white lists should be used to limit character entry.

Here are screenshots from the hack.

