Vulnerability Mapping, Burp Suite

I this project I loaded up burp suite in a virtual machine and set up a proxy between OWASP juice shop in sort of man in the middle fashion. This website was made to intentionally be extremely vulnerable and susceptible to attacks. I am using this website to intentionally find these vulnerability and gain access to any (fake) sensitive data that might be in their systems.

A screenshot of a menu

Description automatically generated

OWASP juice shop. Simple e-commerce site. Users can buy, review/rate and view many different juices.

Regular users that are not authenticated can:

* View the products and reviews
* Fill out a customer feedback form
* View a photo wall
* Visit about us page
* Register/Login

I began my search in the customer feedback form. The first vulnerability I found was upon filling out this customer feedback form was that the CAPTCHA provides the answer in the GET request. It also fills in the customer feedback with the name anonymous. Immediately I am thinking if this request can be replayed, if the name given can be forged into something and if we can automate this task to exploit this system.

After clicking the photo wall tab I found GET request to ‘application configuration’. This could be nothing but it doesn’t need to be seen by users of the website. Upon further investigation, there was another GET request for all of the posted images. In the response, the user object was returned. This contained user enumeration including usernames and even their hashed password.

On their about us page I noticed that the legal information was located on an FTP server. Curious to look into this a little more.

When Logging in/ Signing up, in response to the POST request there is different user object than before returned which includes “deluxe token” and “role”. Potentially these can be changed in the exploitation phase. Can I grant myself administrative privileges or give myself a deluxe token?