Incident Report: MR-10242-AdminRegistration

Date: 10-12-2021

Executive summary:

I was tasked with creating a new user account with admin privileges. The tool I used was Burp Suite because it allows me to see what the requests and responses are.

Results

Application Details:

- **Application URL:** https://mr-ttabookstore-104.herokuapp.com/#/login
- **User accounts:** asdf@mailmail.co

Conclusion:

As stated earlier, I was tasked with creating a user account that had administrative privileges. In order to do this, I used Burp Suite. The first step I took was intercepting an account creation with Burp Suite. Intercepting the creation of an account showed me some useful information. To find this information, I first had to forward the request to the repeater. Here I was able to see the useful information I was talking about. The info showed me the username, role, deluxeToken, lastLoginIp, profileImage, isActive, and more. The information that I found useful was the role. The role said that the account created was a customer account. I took that information and doctored up the HTTP request. I inputted a role section and instead of customer, I switched it to admin. For example, the original HTTP request said role: “customer”. I took that and changed it to role: “admin”. Once doctored, I pressed send and it came back as successful. This could be very detrimental if performed by an attacker because it would allow the attacker to have administrative privileges. With that much power, the attacker could also get user credentials and sell them or make actions on another user’s behalf without the victim knowing about it. To prevent a Mass Assignment from happening is by block-listing sensitive information. So in this case you would want to block-list the role of

the account. The flag that I got was: adf858a9828123061257cba29e3f34da87b23962. Below is a screenshot of the tag as well.