**INCIDENT REPORT: TS-18969-Offensive: Admin Access**

**Date: 6/18/24**

**Executive summary:**

User Story instructions were to create a new user account, but set them up with Administrative-level access.

**Results:**

**Application Details:**

* **Application URL:** http://localhost:3000

**Attack Narrative:**

Using Burp Suite’s Intercept Mode, I was able to observe that the Admin profile is assigned the “Admin” role in associated JSON text while logging out of the profile. When sending the POST request for the User Registration page, I observed the new profile was assigned the “Customer” role in a subsequent response header. I created a new user profile, and added “role”:“admin” to the bottom of the POST request in the JSON text. I was then able to access the site with Admin-level access. A screenshot is included on the following page.

**Conclusion:**

I was able to successfully create a common user account and assign Admin-level access to the site. This allows me to access hidden files, remove User Reviews, among other potentially-malicious tasks. The Admin’s password information in the response header is obfuscated, and it’s recommended to take similar action with the user role, or hide the field altogether.



