Incident Report: MR-10188-AdminLogin

Date: 10-6-2021

Executive summary:

I was tasked with logging into the admin account without using a password. There were not any special tools that were required for this attack. I chose to go without using any tools because I know SQL Injections are doable without the use of any tools.

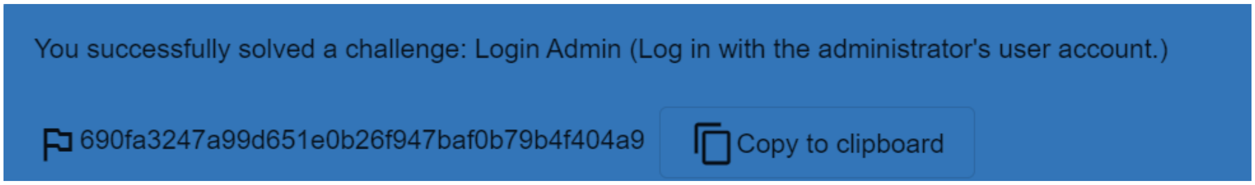
Results

Application Details:

- **Application URL:** https://mr-ttabookstore-104.herokuapp.com/#/login
- **User accounts:** admin@tta.bookstore

Conclusion:

As stated earlier, I was tasked with gaining access to the admin account without a password. The login page of the TTA Bookstore is not safe. I was able to log into the admin account by inputting *‘ OR 1=1 --* into the email field and whatever into the password field. The reason this is not safe is that this allows an attacker to log into the admin account without a password. This is a form of SQL Injection. This attack worked due to the webpage not sanitizing the inputted text before using it. Here is the flag I got: 690fa3247a99d651e0b26f947baf0b79b4f404a9. Below is a screenshot of the flag as well.



You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

690fa3247a99d651e0b26f947baf0b79b4f404a9