Reverse Engineering CTF Final Project

Lu Cao, Joey Mathis, Rong Wang

Our group create a multi-part CTF project. The script that was written revolves around a game service where the user interacts with a robot called BALA BOT.

Part 1

The first part to the exploit is to realize that there is an error within the change description function. The way the program deals with negative lengths is incorrect. When a negative length is entered, the function will simply multiply the length by the negative number and not bounds check the result. The next thing to note is how the user objects are stored. We have an array that stores 5 user objects and this memory is contiguous. So, combining these