Homework Number: hw10
Name: Shu Hwai Teoh
ECN Login: teoh0
Due Date: Thursday 4/09/2020 at 4:29PM

1. specially crafted buffer overflow string:
   AAAAAAAAAAAAAAAAAAAAAAAAAAAA\xc8\x0d\x40\x00\x00\x00\x00\x00
2. explanation of why you chose the string:
   - address of variable str in clientComm(): 0x7fffffffe42b
   - return address of clientComm(): 0x7fffffffe448
   - entry to the object code for the secretFunction() function: 0x0000000000400dc8
   - difference between address of variable str and return address of clientComm(): 0x7fffffffe448 - 0x7fffffffe42b = 29
   - Therefore, the specially crafted buffer overflow string is 29*A concatenated with the entry to the object code for the secretFunction() function.
3. explanation of your fixes to the code: when the number of characters inputted by client is larger than MAX_DATA_SIZE, let the server send string “less” to client and prevent the server from using strcpy().
4. the modified parts of the server code by highlighting or underlining them: as the following page, the modified part is highlighted in pink.