Explanation:

* specially-crafted buffer overflow string: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa\x18\x0e\x40\x00
* I followed the instructions in Lecture 21 step by step, and first construct server client connection, and run disas clientComm to set the break point for leaving the function. Then I examine the contents of stackframe for clientComm function. Which print out the what is stored in frame pointer and return address and stored in stack pointer. And after done several procedures to check out I ran ffffffffff at the client side and then run x /100b $rsp at the server terminal, this time it examine 100 bytes on the stack starting at the location pointed to by stack pointer.

A black background with white text

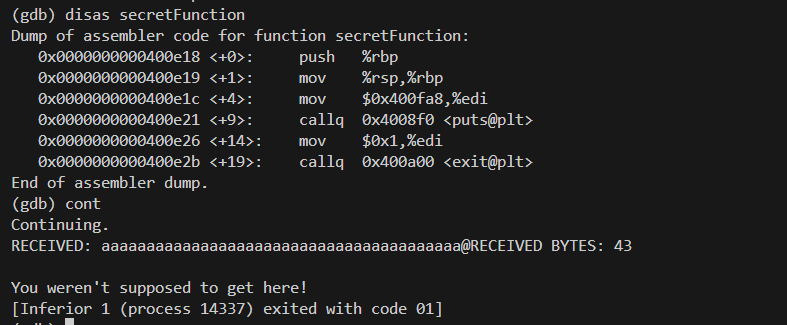
Description automatically generated

As the screenshot shown there’s 10 0x66 starting at the line 0x7fffffffdd30, which is the pattern that I sent from client side. And then I print out the ending position which is dd58, so there’s 40 random characters in front of the last 4 hex.

A black background with white letters

Description automatically generated

After knowing this, I ran disas secretFunction to have the following, for the first line which I see it has 00400e18 which should locate at the end of 40 a’s to construct the string. Below is the screenshot that I sent the string and then reach the secret function.



Modification for server.c

* I have modified the line with strcpy function (strcpy(str, recvBuff);) that cause the buffer overflow vulnerability. This is because the strcpy function doesn’t take the variable size as input so it doesn’t know how long space it should reserve. I change it strncpy (strncpy(str, recvBuff, MAX\_DATA\_SIZE);) which take in the MAX\_DATA\_SIZE as variable length and it solves the buffer overflow vulnerability problem. Below is the output when I send the same string and it didn’t reach the secret function this time.

A screen shot of a computer

Description automatically generated

A black screen with white text

Description automatically generated

Logfile contents from Mail directory

A screenshot of a computer screen

Description automatically generatedA screenshot of a computer screen

Description automatically generated