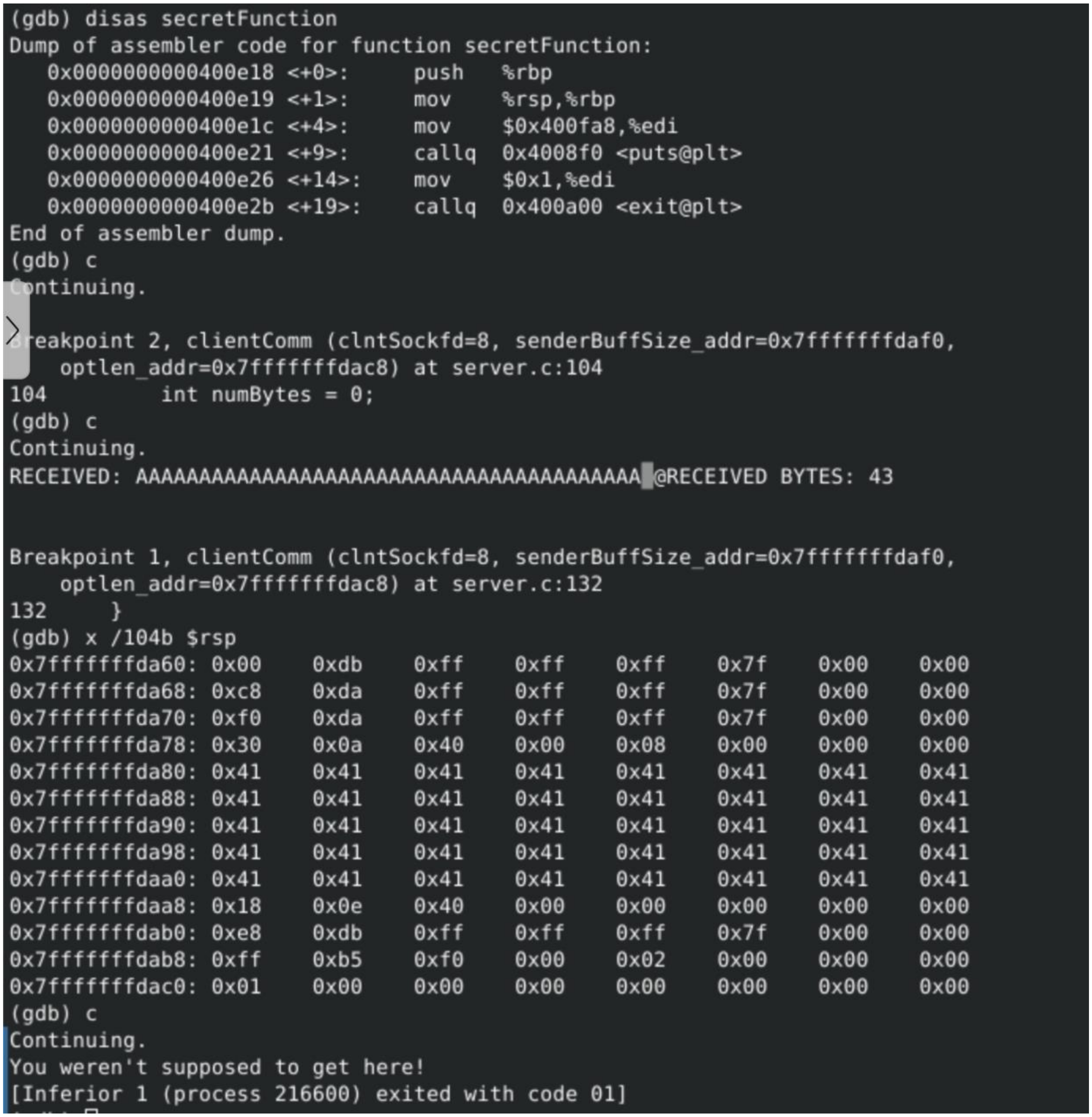
Chan Ng Cashin
ECE404
HW10

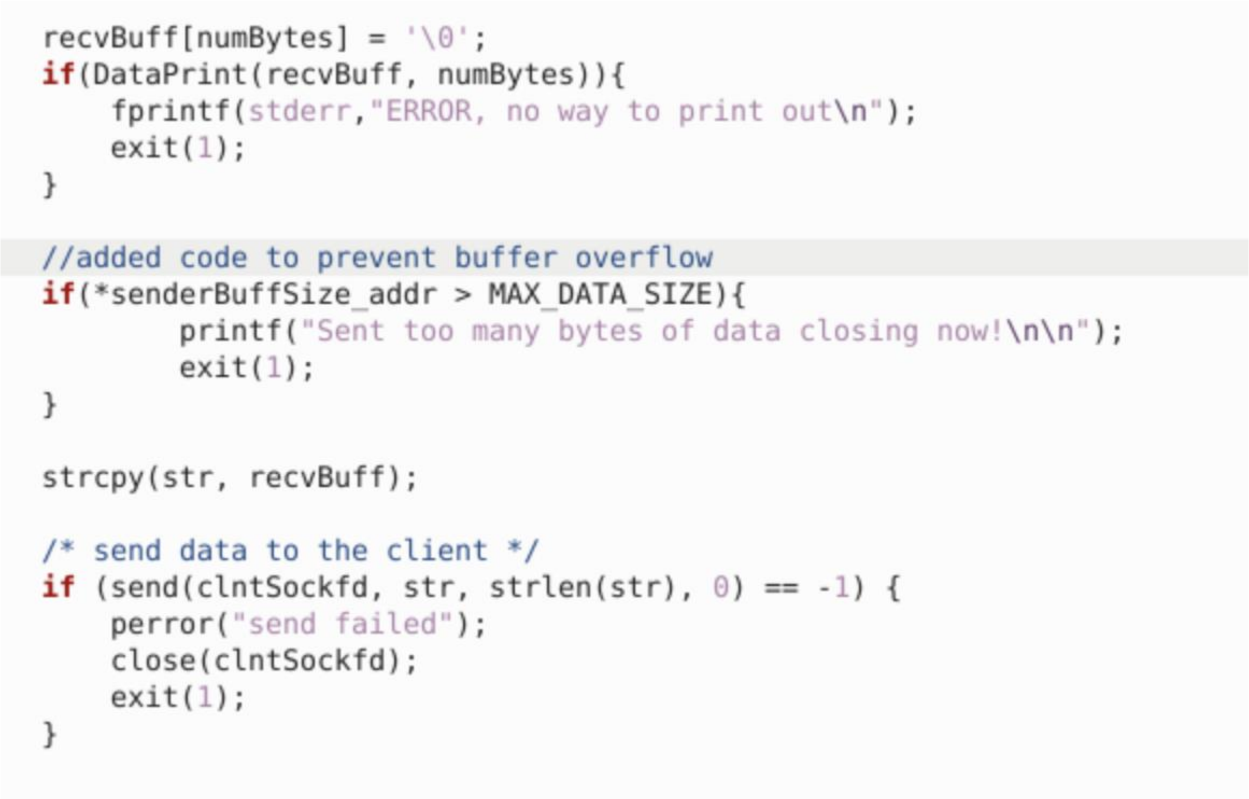


```
(gdb) disas secretFunction
Dump of assembler code for function secretFunction:
   0x0000000000400e18 <+0>:     push   %rbp
   0x0000000000400e19 <+1>:     mov    %rsp,%rbp
   0x0000000000400e1c <+4>:     mov    $0x400fa8,%edi
   0x0000000000400e21 <+9>:     callq  0x4008f0 <puts@plt>
   0x0000000000400e26 <+14>:    mov    $0x1,%edi
   0x0000000000400e2b <+19>:    callq  0x400a00 <exit@plt>
End of assembler dump.
(gdb) c
Continuing.

Breakpoint 2, clientComm (clntSockfd=8, senderBuffSize_addr=0x7fffffffdaf0,
    optlen_addr=0x7fffffffdac8) at server.c:104
104         int numBytes = 0;
(gdb) c
Continuing.
RECEIVED: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA▮@RECEIVED BYTES: 43


Breakpoint 1, clientComm (clntSockfd=8, senderBuffSize_addr=0x7fffffffdaf0,
    optlen_addr=0x7fffffffdac8) at server.c:132
132     }
(gdb) x /104b $rsp
0x7fffffffda60: 0x00    0xdb    0xff    0xff    0xff    0x7f    0x00    0x00
0x7fffffffda68: 0xc8    0xda    0xff    0xff    0xff    0x7f    0x00    0x00
0x7fffffffda70: 0xf0    0xda    0xff    0xff    0xff    0x7f    0x00    0x00
0x7fffffffda78: 0x30    0x0a    0x40    0x00    0x08    0x00    0x00    0x00
0x7fffffffda80: 0x41    0x41    0x41    0x41    0x41    0x41    0x41    0x41
0x7fffffffda88: 0x41    0x41    0x41    0x41    0x41    0x41    0x41    0x41
0x7fffffffda90: 0x41    0x41    0x41    0x41    0x41    0x41    0x41    0x41
0x7fffffffda98: 0x41    0x41    0x41    0x41    0x41    0x41    0x41    0x41
0x7fffffffdaa0: 0x41    0x41    0x41    0x41    0x41    0x41    0x41    0x41
0x7fffffffdaa8: 0x18    0x0e    0x40    0x00    0x00    0x00    0x00    0x00
0x7fffffffdab0: 0xe8    0xdb    0xff    0xff    0xff    0x7f    0x00    0x00
0x7fffffffdab8: 0xff    0xb5    0xf0    0x00    0x02    0x00    0x00    0x00
0x7fffffffdac0: 0x01    0x00    0x00    0x00    0x00    0x00    0x00    0x00
(gdb) c
Continuing.
You weren't supposed to get here!
[Inferior 1 (process 216600) exited with code 01]
```

Here is the string that caused a buffer overflow. I found this by setting a breakpoint at the end of clientComm and then continuing past that address until I found where multiple A's were being printed. Once that was found I determined through further investigation that 40 leading A's were needed before the address of the start of secret function was inputted. After inputting these A's followed by the start address of secretFunction the string caused a buffer overflow.



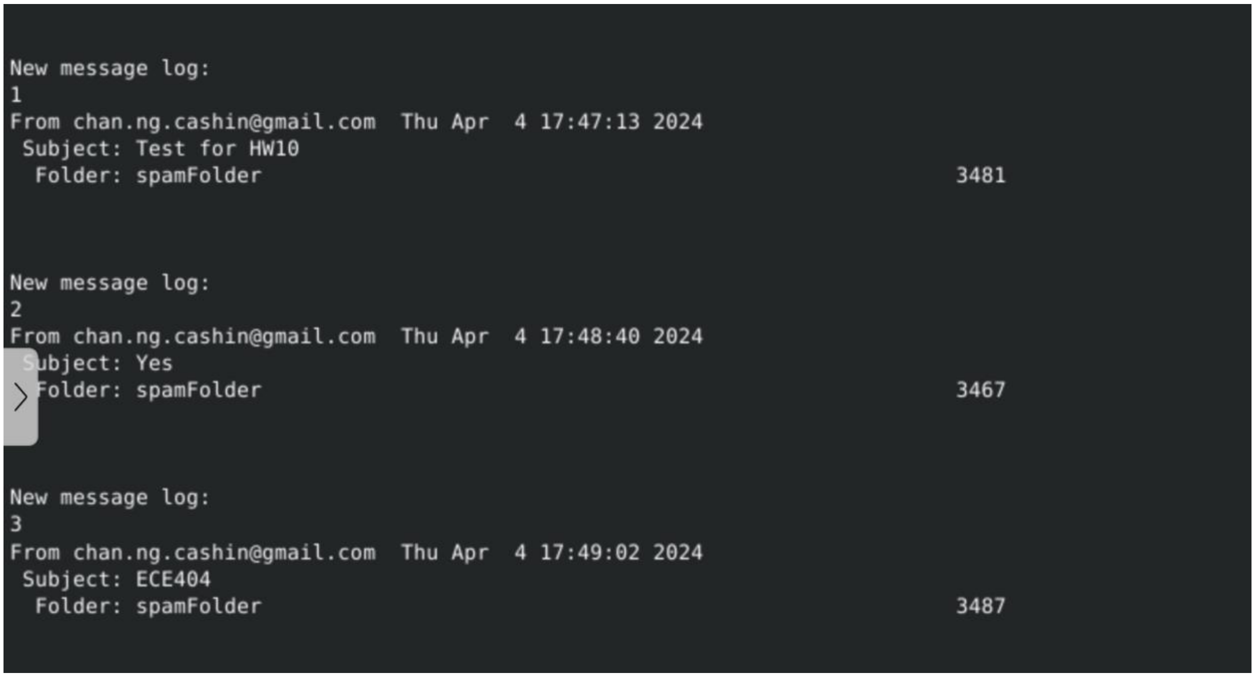
```c
recvBuff[numBytes] = '\0';
if(DataPrint(recvBuff, numBytes)){
    fprintf(stderr,"ERROR, no way to print out\n");
    exit(1);
}

//added code to prevent buffer overflow
if(*senderBuffSize_addr > MAX_DATA_SIZE){
        printf("Sent too many bytes of data closing now!\n\n");
        exit(1);
}

strcpy(str, recvBuff);

/* send data to the client */
if (send(clntSockfd, str, strlen(str), 0) == -1) {
    perror("send failed");
    close(clntSockfd);
    exit(1);
}
```

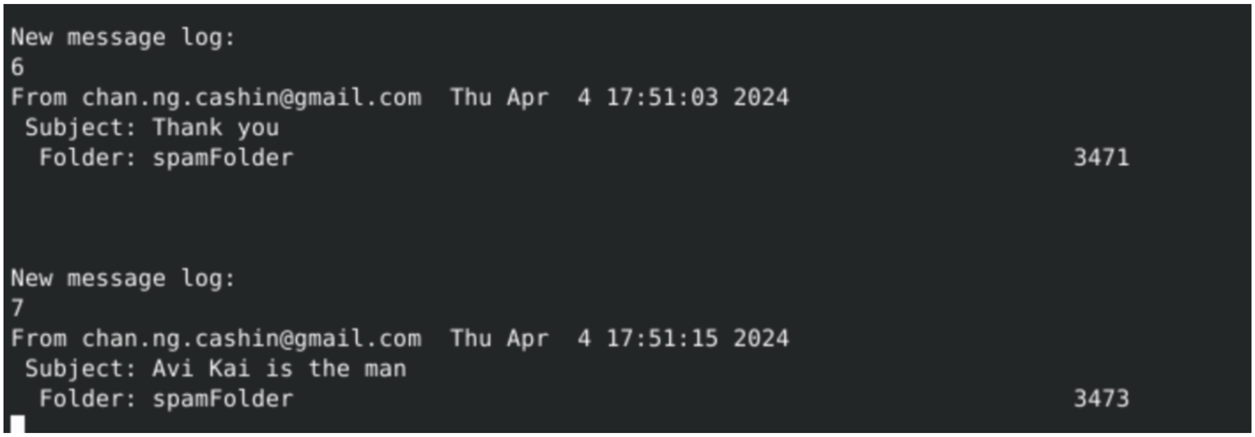
This was the few lines of code I added to server.c that prevented the buffer overflow. This way the sender buffer size address that the client sends will never exceed the data size of the server and a buffer overflow won’t occur.



```
New message log:
1
From chan.ng.cashin@gmail.com  Thu Apr  4 17:47:13 2024
 Subject: Test for HW10
  Folder: spamFolder                                                       3481


New message log:
2
From chan.ng.cashin@gmail.com  Thu Apr  4 17:48:40 2024
 Subject: Yes
  Folder: spamFolder                                                       3467


New message log:
3
From chan.ng.cashin@gmail.com  Thu Apr  4 17:49:02 2024
 Subject: ECE404
  Folder: spamFolder                                                       3487
```



```
New message log:
6
From chan.ng.cashin@gmail.com  Thu Apr  4 17:51:03 2024
 Subject: Thank you
  Folder: spamFolder                                                        3471



New message log:
7
From chan.ng.cashin@gmail.com  Thu Apr  4 17:51:15 2024
 Subject: Avi Kai is the man
  Folder: spamFolder                                                        3473
```

Here are some email logs from my mail spam mail account.