



Codegate CTF 2018 == Junior ==

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

Your team			
#	Team	Score	Update
32	 FetchDEX	217	2 days ago

Rank - junior

General University **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 korean game caled 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
```

> 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
```

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

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 **0x**.

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

[illegible]