[2023 JBUCTF] misc

baskin robbins 5001 ~ 20001

Write-Up

문제 개요

제공 파일 : baskin_robbins.py

```python
from random import randint

def run_game():
    wins = 0
    while wins != 5:
        mod = randint(50, 100)
        value = mod * randint(100, 200) + 1
        count = 0
        print(f'Baskin Robbins {value} !!!')

        while count != value:
            while True:
                try:
                    num = list(map(int, input(f'Input Numbers {count + 1} ~ {mod - 1} (ex {count + 1}, {count + 2}, {count + 3} .... {count + mod - 1}) : ').split(', ')))
                    if len(num) >= mod:
                        raise ValueError
                    for i in range(len(num)):
                        if num[i] != count + i + 1:
                            raise ValueError
                except (ValueError, IndexError):
                    print("Retry")
                    continue
                except Exception as e:
                    print(e)
                    exit()
                break

            count += len(num)
            if count == value:
                print("Lose :(")
                exit()

            if value - count < mod - 1:
                bot_num = [i + count + 1 for i in range(randint(1, value - count))]
            else:
                bot_num = [i + count + 1 for i in range(randint(1, mod - 1))]

            count += len(bot_num)

            print('YOU : ' + ', '.join(map(str, num)))
            print("BOT : " + ', '.join(map(str, bot_num)))

            if count == value:
                print("Win :)")
                wins += 1
                break
    print(f'flag : {flag}')

if __name__ == '__main__':
    flag = open('/flag', 'r').read()
    run_game()
```

mod : 50에서 100사이의 정수

value = mod * (100 ~ 200사의의 정수) + 1

baskin robbins 31게임의 변형으로

mod -1까지의 숫자를 입력할 수 있으며 value값을 봇이 총 5번 입력하게 해야 flag를 출력한다.

문제 풀이

value 값을 mod로 나눈 나머지는 1이 된다.

입력할 수 있는 숫자의 개수는 mod -1의 값이므로 먼저 1을 입력한 뒤, 봇이 입력한 개수를 센다.

봇이 입력한 개수를 n이라 하면 mod – (n+1)의 숫자를 부르고, 이후로는 계속 봇이 입력하는 숫자의 개수에 맞춰서 mod 값이 되도록 숫자를 입력하면 봇은 항상 value 값을 입력하게 된다.

이를 코드로 짜서 5연승 하면 flag를 얻을 수 있다.

exploit.py

```python
from pwn import *

p = remote('172.17.0.2', 10002)

wins = 0
while True:
    count = 0
    p.recvuntil(b'Baskin Robbins ')
    value = int(p.recvuntil(b' ')[:-1])
    p.recvuntil(f'Input Numbers {count + 1} ~ '.encode())
    mod = int(p.recvuntil(b' (ex')[:-4].decode())
    p.sendline(b'1')
    p.recvline()
    i = 0
    while count != value:
        p.recvuntil(b'BOT : ')
        bot_num = p.recvline().decode()
        bot_num = list(map(int, bot_num.split(', ')))
        count = bot_num[-1]
        if count == value:
            success(f'{p.recvline()=}')
            wins += 1
            break
        if i == 0:
            r = mod - (1 + len(bot_num))
            i += 1
            if r < 0:
                exit()
        else:
            r = mod - len(bot_num)
        if r == 0:
            r = mod

        if value < count + r:
            send_data = [i + count + 1 for i in range(value - count - 1)]
        else:
            send_data = [i + count + 1 for i in range(r)]
        send_data = ', '.join(map(str, send_data))
        p.sendline(send_data)
        p.recvline()
    if wins == 5:
        success(p.recvline())
        exit()
```

FLAG

scpCTF{c06826b54b56c16c0ffce5af59b6326a321b650f78d1}