전국청소년모의해킹대회

DIMI CTF 2019 예선 WriteUp

D3vle0

목차

순위

11	kongson	당동중학교	770	Sun Jul 07 2019 20:49:22 GMT+0900 (Korean Standard Time)
12	MI	용정중학교	702	Sun Jul 07 2019 20:44:59 GMT+0900 (Korean Standard Time)
13	Leejuhyup	상명중학교	435	Sun Jul 07 2019 18:38:05 GMT+0900 (Korean Standard Time)
14	선우	용인대덕중학교	325	Sun Jul 07 2019 19:20:40 GMT+0900 (Korean Standard Time)
15	D3vle0	시흥능곡중학교	325	Sun Jul 07 2019 19:59:49 GMT+0900 (Korean Standard Time)
16	Hacods	대송중학교	325	Sun Jul 07 2019 20:22:09 GMT+0900 (Korean Standard Time)
17	조주하	탄벌중학교	316	Sun Jul 07 2019 20:00:03 GMT+0900 (Korean Standard Time)
18	Dohun	조원중학교	219	Sun Jul 07 2019 16:56:43 GMT+0900 (Korean Standard Time)

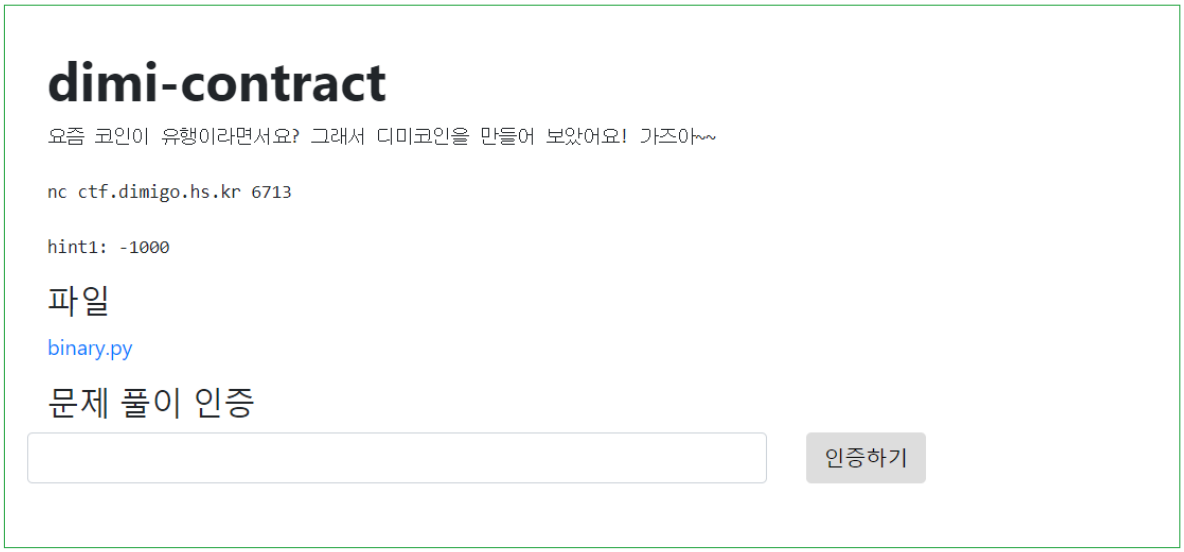
325점

중등부 15위 (D3vle0)

Mic Check

FLAG: `DIMI{A-A-A-A---Mic-Check!}`

dimi-contract



주어진 binary.py 코드를 보니

```cs
#!/usr/bin/python3

import sys
import random
import os
import time

def send(data, end='\n'):
    sys.stdout.write(data + end)
    sys.stdout.flush()

def read():
    return input()

def checkCoin():
    global dimicoin
    if dimicoin > 1000000:
        send("GoodJob!!!")
        send('-'*50)
        send(os.environ['flag'])
        send('-'*50)
        sys.exit(1)

def checkDebt():
    global debt
    global debtCount
    if debt > 0:
        if debtCount > 5:
```

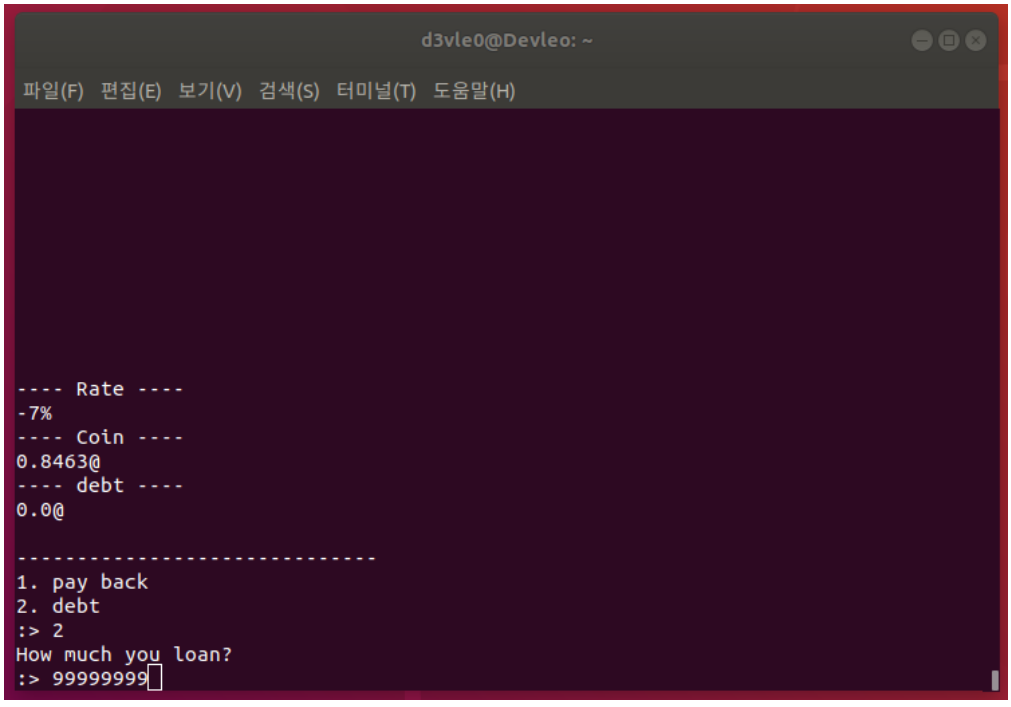
```
            send("Hey! What are you doing?!?!?!")
            sys.exit(-1)
        else:
            debtCount += 1
    else:
        debtCount = 0

def changeRate():
    global rate
    if random.randint(0,1) == 0:
        rate = int(random.random() * -1 * 10) - random.randint(0, 10)
    else:
        rate = int(random.random() * 10) + random.randint(0, 10)

def changeByRate():
    global rate
    global dimicoin
    global debt

    dimicoin = dimicoin + dimicoin * (rate/100.0)
    debt = debt + debt * (rate/100.0)

def banner():
    global dimicoin
    global rate
    global debt

    send('---- Rate ----')
    if rate < 0:
        send(str(rate) + '%')
    else:
        send(str(rate) + '%')
    send('---- Coin ----')
    send(str(dimicoin) + '@')

    send('---- debt ----')
    send(str(debt) + '@')

    send("")

def menu():
    send('1. pay back')
    send('2. debt')

def payBack():
    global dimicoin
    global debt

    if debt == 0:
        send("You no have debt!")
        return

    send("How much you pay back?")
```

```
    send(":> ", end='')

    try:
        payback = int(read())
    except ValueError:
        send("Plz input int")
        return

    if payback > debt or payback > dimicoin:
        send("Too much :<")
        return

    debt -= payback
    dimicoin -= payback

def getDebt():
    global dimicoin
    global debt

    send("How much you loan?")
    send(":> ", end='')

    try:
        loan = int(read())
    except ValueError:
        send("Plz input int")
        return

    if loan > 10:
        send("Too much :<")
        return

    debt += loan
    dimicoin += loan

if __name__ == '__main__':
    global dimicoin
    global rate
    global debt
    global debtCount

    send("Welcome DIMI-Bank!")
    send("Here 1@ dimi-coin")

    dimicoin = 1
    rate = 0
    debt = 0
    debtCount = 0

    time.sleep(1)

    for i in range(0,10):
        send(chr(27) + "[2J")
```

```
135
136         checkCoin()
137         checkDebt()
138         changeRate()
139         changeByRate()
140         banner()
141         send('-'*30)
142         menu()
143         send(':> ', end='')
144         try:
145             select = int(read())
146             if select == 1:
147                 payBack()
148             elif select == 2:
149                 getDebt()
150             else:
151                 send("No select!")
152 
153         except ValueError:
154             send("Plz input int")
155 
156 
157     send("You get Flag? XD")
158 
```

Colored by Color Scripter

15번줄 checkCoin 함수를 보아 dimicoin의 값이 100만이 넘으면 flag를 출력해준다.



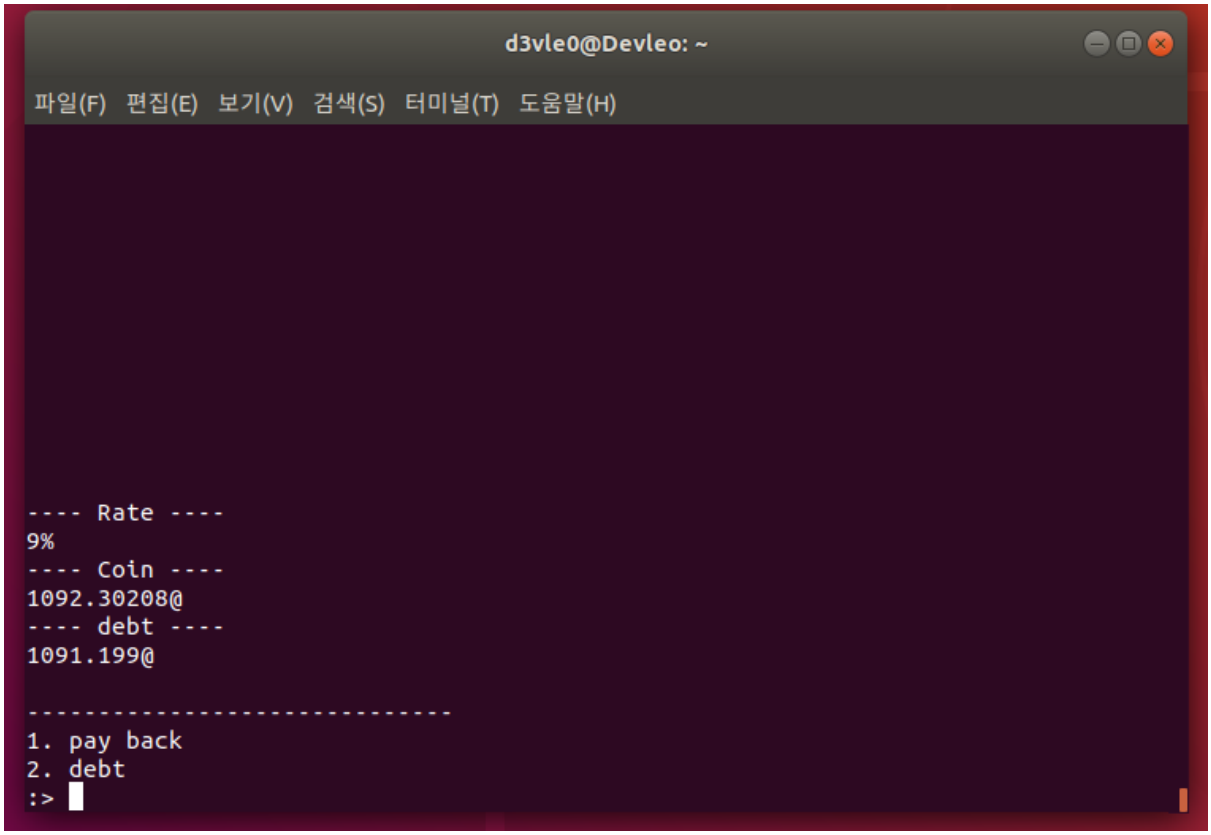
이렇게 입력하니 110번 줄의 조건 (loan이 10보다 작아야함) 에 걸려 Too much 가 출력되었다. 그럼 어떻게 해서 dimicoin 값을 크게 늘일 수 있을까 생각하다가

```cs
94 debt -= payback
95 dimicoin -= payback
```

돈을 pay back 하는 과정에서 dimicoin= dimicoin - payback 이므로

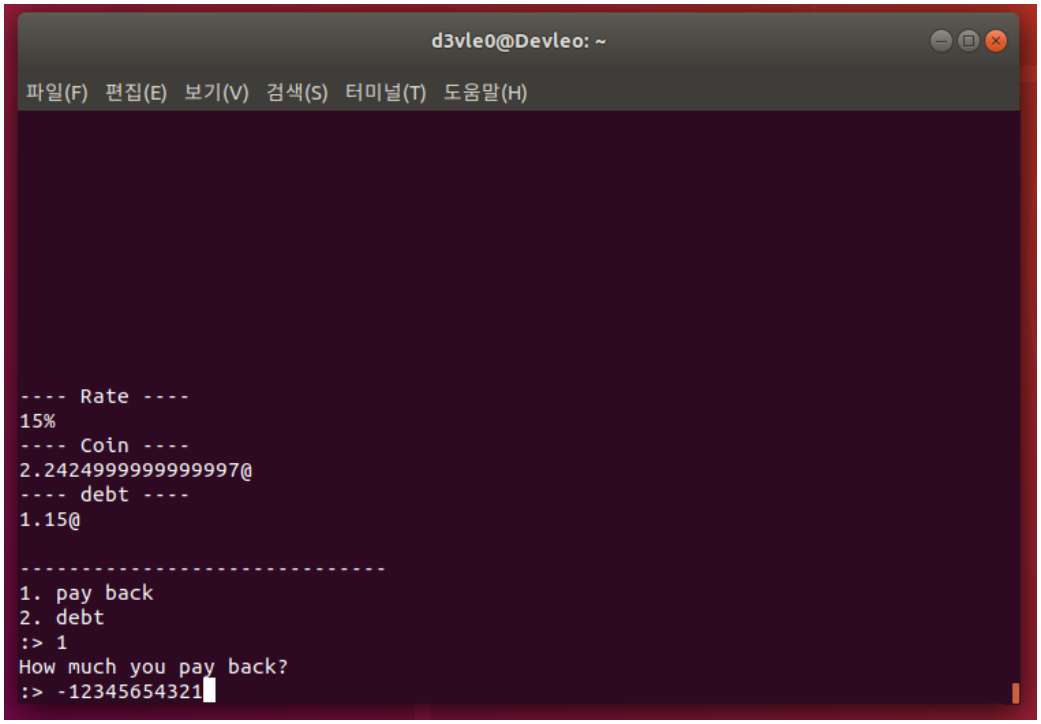
0보다 작은 값을 입력하면 dimicoin이 증가할 것이다.

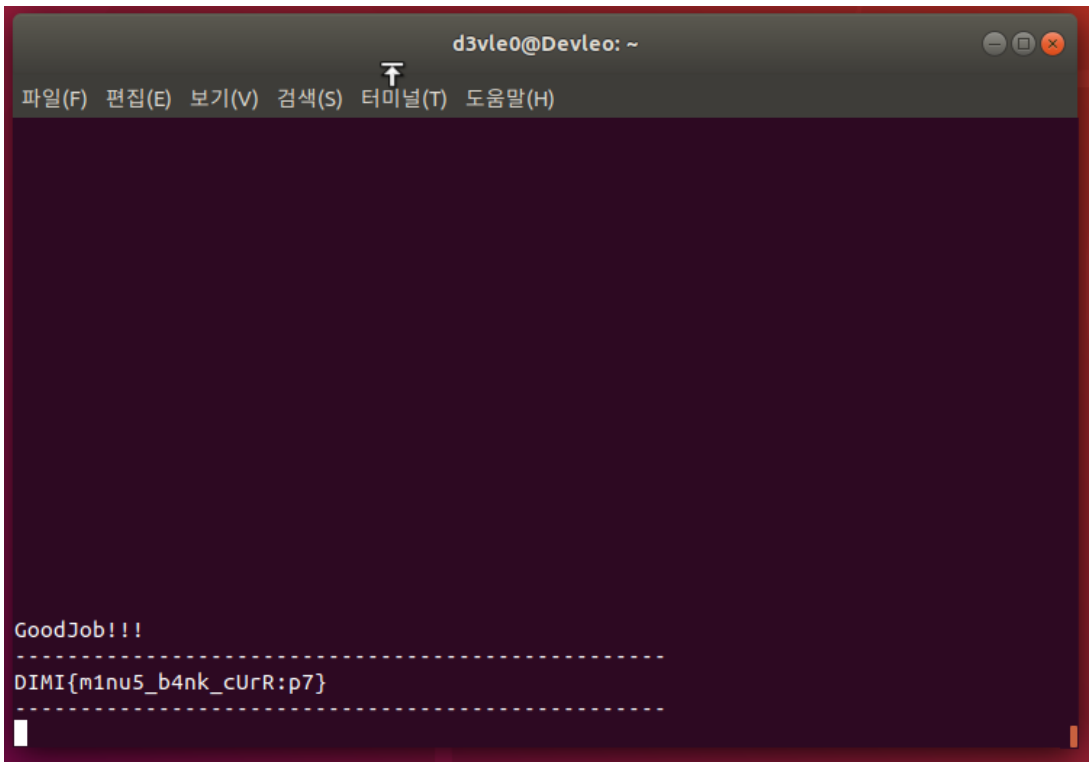
마침 hint1에 -1000이 적혀있길래 -1000만큼 pay back을 한 결과



dimicoin이 크게 증가하였다.

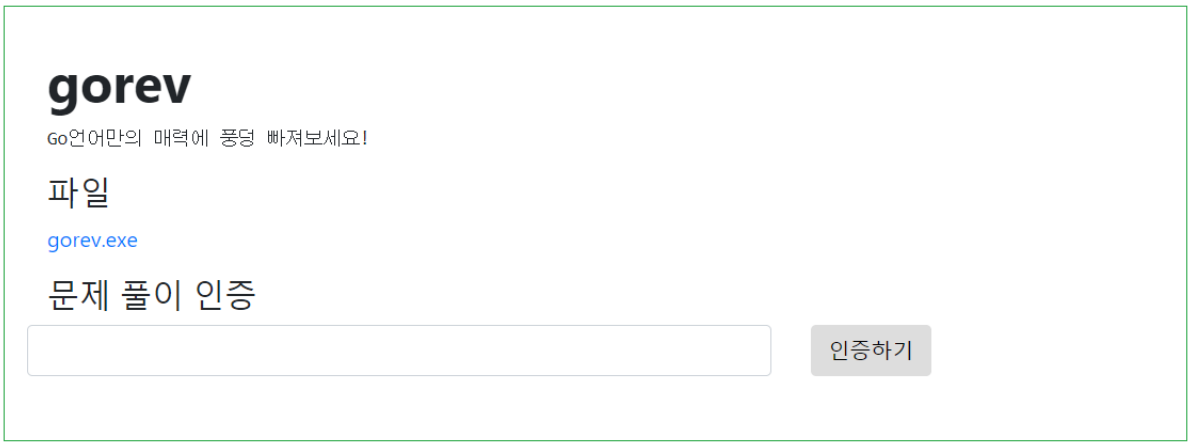
pay back 시 -1000000 이하의 값을 입력하면 플래그를 주는 것을 알 수 있다.



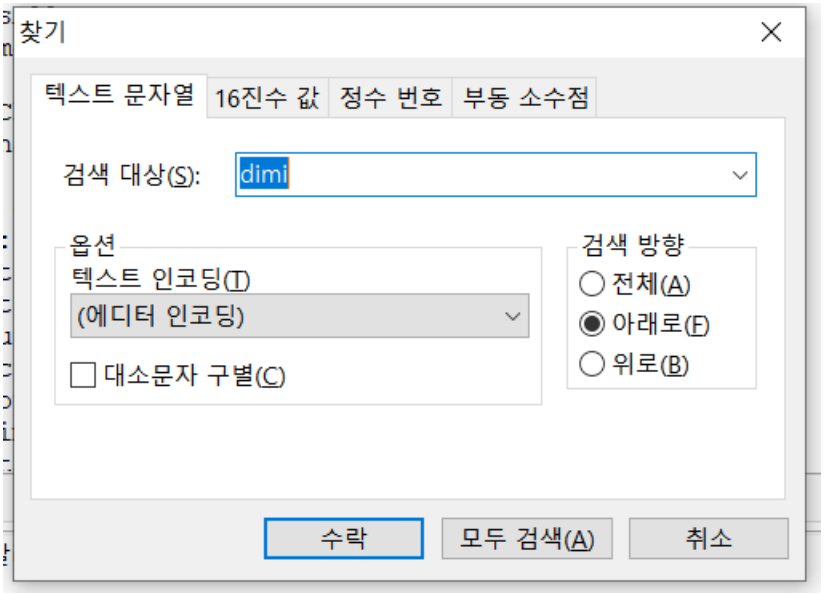


FLAG: DIMI{m1nu5_b4nk_cUrR:p7}

gorev



gorev.exe 파일을 다운받고 HxD로 열어보았다.



'dimi' 문자열을 검색해본 결과

```
000C38C0  73 75 70 70 6F 72 74 65 64 20 66 69 6C 65 20 74  supported file t
000C38D0  79 70 65 33 35 35 32 37 31 33 36 37 38 38 30 30  ype3552713678800
000C38E0  35 30 30 39 32 39 33 35 35 36 32 31 33 33 37 38  5009293556213378
000C38F0  39 30 36 32 35 44 49 4D 49 7B 47 6F 5F 47 30 5F  90625DIMI{Go_G0_
000C3900  47 4F 5F 67 6F 5F 67 30 5F 67 4F 5F 72 33 76 65  GO_go_g0_gO_r3ve
000C3910  72 73 69 6E 67 21 7D 4D 48 65 61 70 5F 41 6C 6C  rsing!}MHeap_All
000C3920  6F 63 4C 6F 63 6B 65 64 20 2D 20 4D 53 70 61 6E  ocLocked - MSpan
000C3930  20 6E 6F 74 20 66 72 65 65 4D 53 70 61 6E 5F 45   not freeMSpan_E
000C3940  6E 73 75 72 65 53 77 65 70 74 3A 20 6D 20 69 73  nsureSwept: m is
```

플래그를 바로 찾을 수 있었다.

FLAG: `DIMI{Go_G0_GO_go_g0_gO_r3versing!}`