

# 전국청소년모의해킹대회

DIMI CTF 2019 예선 WriteUp

## **D3vle0**

# 목차

1. 순위
2. Mic Check
3. dimi-contract
4. gorev



# 순위

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

325점

중등부 15위 (D3vle0)

# Mic Check

## Mic Check

환영합니다.

한국디지털미디어고등학교 주최 2019년 전국청소년모의해킹대회 - DIMICTF에 참가하신 것에 대해 크나큰 감사의 인사를 드립니다.

Reversing / Pwnable / Web Hacking / Misc 로 분야가 나누어져있으며, 각 분야당 최대 5문제가 단계적으로 공개될 예정입니다.

문제 풀이와 관련없는 대회 웹사이트 / 서버에 대한 포트스캐닝/퍼징/공격 등은 법적 처벌을 받을 수 있습니다.

자세한 규칙은 <https://ctf.dimigo.hs.kr/rule> 을 참고해주시길 바랍니다.

IRC (디스코드) : <https://discord.gg/UGvmASa>

Welcome Flag : DIMI{A-A-A-A---Mic-Check!}

문제 풀이 인증

인증하기

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

# dimi-contract

## dimi-contract

요즘 코인이 유행이라면서요? 그래서 디미코인을 만들어 보았어요! 가즈아~~

nc ctf.dimigo.hs.kr 6713

hint1: -1000

파일

[binary.py](#)

문제 풀이 인증

인증하기

주어진 binary.py 코드를 보니

```
1 #!/usr/bin/python3
2
3 import sys
4 import random
5 import os
6 import time
7
8 def send(data, end='\n'):
9     sys.stdout.write(data + end)
10    sys.stdout.flush()
11
12 def read():
13     return input()
14
15 def checkCoin():
16     global dimicoin
17     if dimicoin > 1000000:
18         send("GoodJob!!!")
19         send('-'*50)
20         send(os.environ['flag'])
21         send('-'*50)
22         sys.exit(1)
23
24 def checkDebt():
25     global debt
26     global debtCount
27     if debt > 0:
28         if debtCount > 5:
```

CS

```

29         send("Hey! What are you doing?!?!?!")
30         sys.exit(-1)
31     else:
32         debtCount += 1
33     else:
34         debtCount = 0
35
36 def changeRate():
37     global rate
38     if random.randint(0,1) == 0:
39         rate = int(random.random() * -1 * 10) - random.randint(0, 10)
40     else:
41         rate = int(random.random() * 10) + random.randint(0, 10)
42
43 def changeByRate():
44     global rate
45     global dimicoin
46     global debt
47
48     dimicoin = dimicoin + dimicoin * (rate/100.0)
49     debt = debt + debt * (rate/100.0)
50
51 def banner():
52     global dimicoin
53     global rate
54     global debt
55
56     send('---- Rate ----')
57     if rate < 0:
58         send(str(rate) + '%')
59     else:
60         send(str(rate) + '%')
61     send('---- Coin ----')
62     send(str(dimicoin) + '@')
63
64     send('---- debt ----')
65     send(str(debt) + '@')
66
67     send("")
68
69 def menu():
70     send('1. pay back')
71     send('2. debt')
72
73 def payBack():
74     global dimicoin
75     global debt
76
77     if debt == 0:
78         send("You no have debt!")
79         return
80
81     send("How much you pay back?")

```

```

82     send(":> ", end='')
83
84     try:
85         payback = int(read())
86     except ValueError:
87         send("Plz input int")
88         return
89
90     if payback > debt or payback > dimicoi:
91         send("Too much :<")
92         return
93
94     debt -= payback
95     dimicoi -= payback
96
97 def getDebt():
98     global dimicoi
99     global debt
100
101     send("How much you loan?")
102     send(":> ", end='')
103
104     try:
105         loan = int(read())
106     except ValueError:
107         send("Plz input int")
108         return
109
110     if loan > 10:
111         send("Too much :<")
112         return
113
114     debt += loan
115     dimicoi += loan
116
117 if __name__ == '__main__':
118     global dimicoi
119     global rate
120     global debt
121     global debtCount
122
123     send("Welcome DIMI-Bank!")
124     send("Here 1@ dimi-coin")
125
126     dimicoi = 1
127     rate = 0
128     debt = 0
129     debtCount = 0
130
131     time.sleep(1)
132
133     for i in range(0,10):
134         send(chr(27) + "[2J")

```

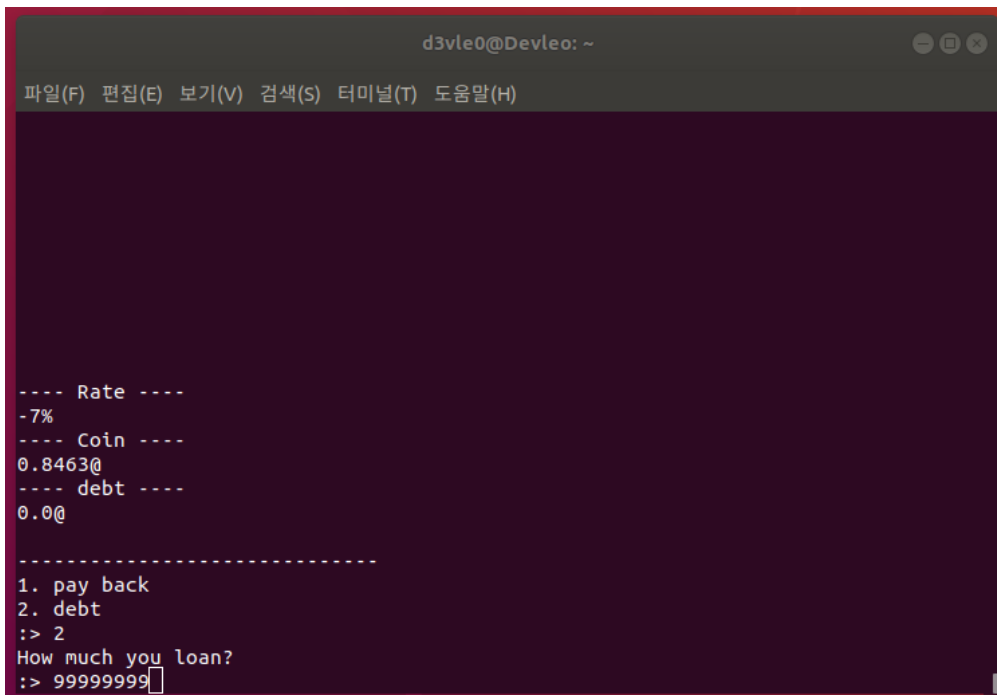
```

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 dimico인의 값이 100만이 넘으면 flag를 출력해준다.



```

d3vle0@Devleo: ~
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)

---- Rate ----
-7%
---- Coin ----
0.8463@
---- debt ----
0.0@

-----
1. pay back
2. debt
:> 2
How much you loan?
:> 9999999

```

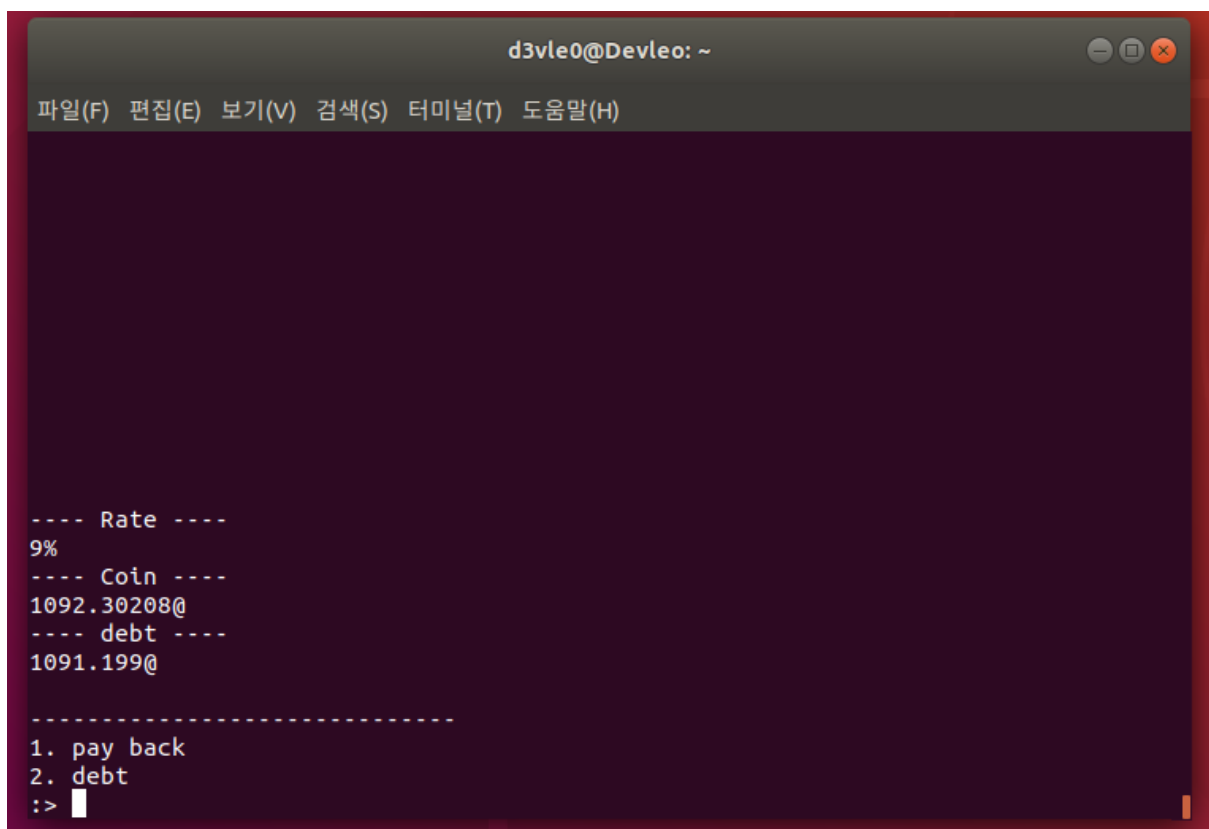


이렇게 입력하니 110번 줄의 조건 (loan이 10보다 작아야함) 에 걸려 Too much 가 출력되었다. 그럼 어떻게 해서 dimicoi n 값을 크게 늘일 수 있을까 생각하다가

```
94 | debt -= payback
95 | dimicoi n -= payback
```

돈을 pay back 하는 과정에서 dimicoi n= dimicoi n - payback 이므로 0보다 작은 값을 입력하면 dimicoi n이 증가할 것이다.

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

A terminal window titled 'd3vle0@Devleo: ~' with a menu bar containing '파일(F)', '편집(E)', '보기(V)', '검색(S)', '터미널(T)', and '도움말(H)'. The terminal output shows: '---- Rate ----', '9%', '---- Coin ----', '1092.30208@', '---- debt ----', '1091.199@', followed by a dashed line and a menu: '1. pay back', '2. debt', and a prompt ':>'.

```
d3vle0@Devleo: ~
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)

---- Rate ----
9%
---- Coin ----
1092.30208@
---- debt ----
1091.199@

-----
1. pay back
2. debt
:> 
```

dimicoi n이 크게 증가하였다.

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

```
d3vle0@Devleo: ~
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)

---- Rate ----
15%
---- Coin ----
2.2424999999999997@
---- debt ----
1.15@

-----
1. pay back
2. debt
:> 1
How much you pay back?
:> -12345654321
```

```
d3vle0@Devleo: ~
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)

GoodJob!!!
-----
DIMI{m1nu5_b4nk_cUrR:p7}
-----
```

FLAG: DIMI{m1nu5\_b4nk\_cUrR:p7}

# gorev

## gorev

Go언어만의 매력에 푹 빠져보세요!

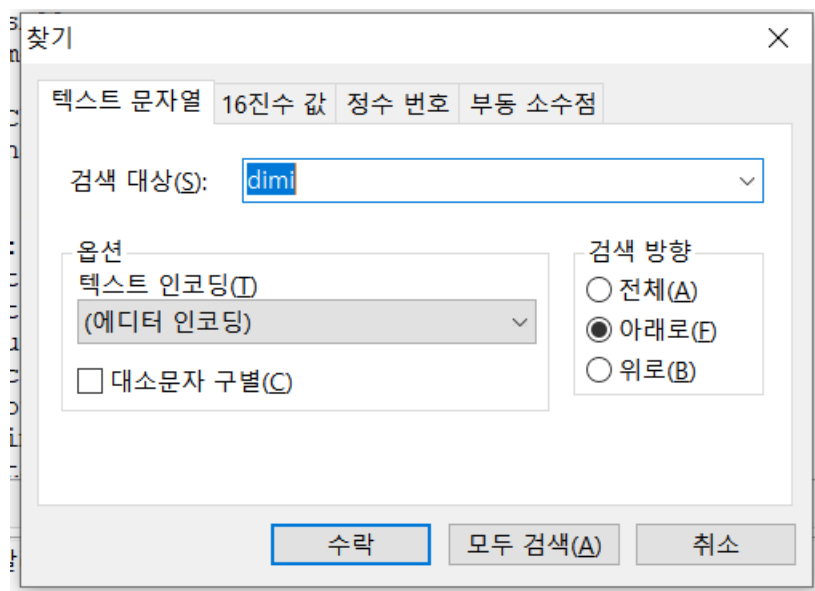
파일

[gorev.exe](#)

문제 풀이 인증

인증하기

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_g0_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\_G0\_go\_g0\_g0\_r3versing!}