HCTF write-up

제갈지혜

- rev_equation

1. equation 바이너리 파일을 IDA로 분석해보니 입력 받은 숫자들을 계산하여 여러 개의 if 문들을 통과하면 되는 문제로 확인함.

2. symbolic execution 문제풀이에 주로 사용되는 라이브러리인 angr를 사용하여 rev_equation.py와 같이 코드를 작성함.

```
import angr


def main():
    p = angr.Project("./Downloads/equation", load_options={'auto_load_libs': False})
    ex = p.surveyors.Explorer(find=(0x400B65, ), avoid=(0x400B71,))
    ex.run()


    return ex.found[0].state.posix.dumps(0).strip('₩0₩n')


if __name__ == '__main__':
    print main()
```

3. flag는 42893724579049578813

- rev_DecompileME

1. ~~.apk 이므로 android 패키지 파일일 것이라 예상하고 web android decompiler를 찾아서 이용함. (http://www.javadecompilers.com)

2. sources/icewall/decompileme/MainActivity.java 에서 문제에서 제시한 형식에 맞는 flag를 발견함.

3. flag는 FLAG{Trust_th1s_5tr1ng}

- rev_script

1. script 바이너리 파일을 IDA로 분석해보니 A0 ~ A1101 함수가 존재하고 각 함수들은 해당 인덱스에 맞는 문자를 체크하는 것으로 확인함. (A0면 0번째 인덱스의 문자를 확인)

2. cmp hex값은 3c이므로 바이너리를 byte형식으로 읽어 3c를 찾고 다음 hex값을 저장한후, character 형식으로 변환하는 코드를 script.py와 같이 작성했다.

```
with open("script", "rb") as f:
        s = f.read()
idx = 0
flag = []
while idx < len(s):
        if s[idx] == 0x3c:
                flag.append(s[idx+1])
        idx += 1
flag_string = ""
```

3. 이 결과 다음과 같은 string이 나온다.

'DOLLAR DOLLARH₩nI used it all up in a dayC₩nRun run I earn and₩x0f I splurgeT₩nRun run run runF₩nRun run{₩nI want it, cruisin₩xe2₩x80₩x99 on the bayG₩nI want it, cruisin₩xe2₩x80₩x99 like NEMO0₩nI don₩xe2₩x80₩x99t have money but I wanna go somewhere far away_₩nI don₩xe2₩x80₩x99t have money but I want to destressM₩nI don₩xe2₩x80₩x99t have money but I wanna eat at Jiro Ono₩xe2₩x80₩x01₩x99s4₩nI worked so hard and earned my payC₩nAll of it, into my tummy4₩nI collect every drop and have fun wasting every drop, I spend it allU₩nLet me be, even though I overspend_₩nTomorrow morning, I may act crazyF₩nAnd withdraw installment savings0₩nWOO there₩xe2₩x80₩x99s n₩x02o tomorrowR₩nThere₩xe2₩x80₩x99s already a mortgage on my future_₩nWOO I spend more of my moneyT₩nFriends wussup4₩nDo you want some?N₩nDOLLAR DOLLARG₩nI spend it all in a dayJ₩nRun, run man i spend it like some partyI₩nDOLLAR DOLLARN₩nUntil every dog has his dayJ₩nUntil the s₩x03un risesA₩nYOLO YOLO YOLO YOM₩nYOLO YOLO YO_₩nSpend spend spendT₩nYOLO YOLO YOLO YO4₩nWhere my money yahN₩nSpend spend spendG₩nYOLO YOLO YOLO YOJ₩nYOLO YOLO YOI₩nSpend spend spendN₩nYOLO YOLO YOLO YOJ₩nWhere the party yahA₩nSpend spend spendM₩nWhere my money yah?!₩nWher₩x04e the party yah?}₩n%₩xff₩xff₩xff₩xff₩xffK₩x00₩x00₩x00₩x00₩x00₩x00₩x00₩x00~±₩xe4₩xad₩x0e!₩x00₩x00₩x00₩x00₩x00₩x00₩x00₩x004₩xff₩xff₩xff₩xff₩xff₩xff₩xff₩xff₩xff₩xff₩xff₩xff₩xff₩xffG@₩x03@₩x982₩xcb@@₩re₩x0f@₩x15₩x17'

4. 위 string에서 ₩n 앞에 있는 글자를 추리면 flag 형식의 문자열이 나온다

5. flag는 HCTF{G0_M4C4U_F0R_T4NGJINJAM_T4NGJINJAM!}