rev-basic-1 문제 write-up

강승민

```
C:\Users\tmdal>C:\Users\tmdal\Desktop\File\dreamhack\Reversing\rev-basic-1\chall1.exe
Input : asdf
Wrong
```

[그림 1]

문제파일을 실행시키면 [그림 1]과 같고 리버싱을 위해 ida를 이용해서 열고 haxray기능을 사용하면

```
1  int __cdecl main(int argc, const char **argv, const char **envp)
2  {
3    char v4[256]; // [rsp+20h] [rbp-118h] BYREF
4
5    memset(v4, 0, sizeof(v4));
6    sub_1400013E0("Input : ", argv, envp);
7    sub_140001440("%256s", v4);
8    if ( (unsigned int)sub_140001000(v4) )
9      puts("Correct");
10   else
11     puts("Wrong");
12   return 0;
13 }
```

[그림 2]

[그림 2] 같은 메인함수가 나타나게 된다. Correct를 띄우는게 목표이기 때문에 sub_140001000함수를 ture로 만들기 위해 함수를 보면

```
_BOOL8 __fastcall sub_140001000(_BYTE *a1)
{
  if ( *a1 != 67 )
    return 0i64;
  if ( a1[1] != 111 )
    return 0i64;
  if ( a1[2] != 109 )
    return 0i64;
  if ( a1[3] != 112 )
    return 0i64;
  if ( a1[4] != 97 )
    return 0i64;
  if ( a1[5] != 114 )
    return 0i64;
  if ( a1[6] != 51 )
    return 0i64;
  if ( a1[7] != 95 )
    return 0i64;
```

[그림 3]

[그림 3]과 같이 문자열을 한자리씩 비교한다.

이를 전부 모아보면

```
3   if ( *a1 != 'C' )
4     return 0i64;
5   if ( a1[1] != '[redacted]' )
6     return 0i64;
7   if ( a1[2] != '[redacted]' )
8     return 0i64;
9   if ( a1[3] != '[redacted]' )
10    return 0i64;
11  if ( a1[4] != '[redacted]' )
12    return 0i64;
13  if ( a1[5] != '[redacted]' )
14    return 0i64;
15  if ( a1[6] != '[redacted]' )
16    return 0i64;
17  if ( a1[7] != '[redacted]' )
18    return 0i64;
19  if ( a1[8] != '[redacted]' )
20    return 0i64;
21  if ( a1[9] != '[redacted]' )
22    return 0i64;
23  if ( a1[10] != 'e' )
24    return 0i64;
25  if ( a1[11] != '[redacted]' )
26    return 0i64;
27  if ( a1[12] != '[redacted]' )
28    return 0i64;
29  if ( a1[13] != '[redacted]' )
30    return 0i64;
31  if ( a1[14] != '[redacted]' )
32    return 0i64;
33  if ( a1[15] != '[redacted]' )
34    return 0i64;
35  if ( a1[16] != '[redacted]' )
36    return 0i64;
37  if ( a1[17] != '[redacted]' )
38    return 0i64;
39  if ( a1[18] != '[redacted]' )
40    return 0i64;
41  if ( a1[19] != '[redacted]' )
42    return 0i64;
43  if ( a1[20] == '[redacted]' )
44    return a1[21] == 0;
45  return 0i64;
```

[그림 4]

[그림 4]에서 전부 모으면 C*********e********** 라는 flag를 얻을 수 있다.

(정확한 flag값은 *로 가렸습니다.)