Dreamhack CTF Season 5 Round #10

[REV] instrs

31기 육은서

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  int v4; // [rsp+1Ch] [rbp-24h]
  char *lineptr; // [rsp+20h] [rbp-20h] BYREF
  size_t n; // [rsp+28h] [rbp-18h] BYREF
  FILE *stream; // [rsp+30h] [rbp-10h]
  unsigned __int64 v8; // [rsp+38h] [rbp-8h]

  v8 = __readfsqword(0x28u);
  sub_12EA(a1, a2, a3);
  memset(&unk_4050, 0, 8uLL);
  memset(&unk_4060, 0, 8uLL);
  dword_4070 = 0;
  dword_406C = 0;
  puts("Enter Your Program");
  read(0, &unk_4050, 8uLL);
  byte_4058 = 0;
  v4 = sub_136D();
  printf("Result: %d₩n", (unsigned int)v4);
  if ( v4 > 99999 )
  {
    lineptr = 0LL;
    n = 0LL;
    stream = fopen("./flag", "r");
    getline(&lineptr, &n, stream);
    printf("Good, get the flag: %s", lineptr);
    free(lineptr);
    fclose(stream);
  }
  return 0LL;
}
```

main은 여기

1. v4>99999 해야함

```
void makev4()
{
  unsigned int v0; // eax
  unsigned int v1; // eax
  int v2; // [rsp+8h] [rbp-8h]

  v2 = 0;
  while ( 1 )
  {
    ++v2;
    v0 = byte_4050[dword_406C];
    if ( v0 > 0x72 )
      goto LABEL_11;
    if ( byte_4050[dword_406C] >= 0x61u )
      break;
    if ( v0 == 43 )
    {
      ++byte_4060[dword_4070];
    }
    else
    {
      if ( v0 != 45 )
        goto LABEL_11;
      --byte_4060[dword_4070];
    }
    if ( ++dword_406C > 7 )
      dword_406C = 7;
  }
  v1 = v0 - 97;
  if ( v1 <= 0x11 )
    __asm { jmp         rax }
LABEL_11:
  puts("No Hack!");
  exit(-1);
}
```

```
12    if ( v0 > 0x72 )
13      goto LABEL_11;
```

v0<=0x72 해야함

```
14    if ( byte_4050[dword_406C] >= 0x61u )
15      break;
```

```
29  v1 = v0 - 97;
30  if ( v1 <= 0x11 )
31    __asm { jmp     rax }
```

v1이 분기의 조건이 되는 거 같은데.. 일단 함수 의도를 모르겠으니 pass

```
3   unsigned int unsigned100000; // eax
4   int signed100000; // [rsp+1Ch] [rbp-24h]
5   char *lineptr; // [rsp+20h] [rbp-20h] BYREF
6   size_t n; // [rsp+28h] [rbp-18h] BYREF
7   FILE *stream; // [rsp+30h] [rbp-10h]
8   unsigned __int64 v9; // [rsp+38h] [rbp-8h]
9
10  v9 = __readfsqword(0x28u);
11  sub_12EA(a1, a2, a3);
12  memset(input, 0, sizeof(input));
13  memset(byte_4060, 0, 8uLL);
14  dword_4070 = 0;
15  param1inmakev4 = 0;
16  puts("Enter Your Program");
17  read(0, input, 8uLL);
18  byte_4058 = 0;
19  makev4();
20  signed100000 = unsigned100000;
21  printf("Result: %d\n", unsigned100000);
```

main 다시 뜯어보니까 unsigned100000 초기화 해주는 게 없는데...

내가 rename 하다가 디컴파일 코드가 좀 바뀐 거 같다. 동적 분석으로 넘어가서 봐야할 거 같다.