[DreamHack] rev-basic-2

```
__int64 sub_140001120()
{
  char v1; // [rsp+20h] [rbp-118h]

  memset(&v1, 0, 0x100ui64);
  sub_1400011B0("Input : ");
  sub_140001210("%256s", &v1);
  if ( (unsigned int)sub_140001000((__int64)&v1) )
    puts("Correct");
  else
    puts("Wrong");
  return 0i64;
}
```

아이다로 분석해봤을 때 여러 함수 목록들을 살피다 보면 이런 함수를 발견할 수 있다.

If 조건부 내부의 함수에서 입력값에 대해 검증을 하고 리턴하는 값에 따라 결과를 출력한다.

저 함수를 확인해보면

```
signed __int64 __fastcall sub_140001000(__int64 a1)
{
  int i; // [rsp+0h] [rbp-18h]

  for ( i = 0; (unsigned __int64)i < 0x12; ++i )
  {
    if ( *(_DWORD *)&aC[4 * i] != *(unsigned __int8 *)(a1 + i) )
      return 0i64;
  }
  return 1i64;
}
```

이렇게 구성되어 있다.

aC라는 놈이 가르키는 주소에서 값들을 가져오며 입력 값과 비교를 한다.

4바이트마다 글자가 있는 것 같다.

```
.data:0000000140003000 aC              db 'C',0
.data:0000000140003002                 align 4
.data:0000000140003004 aO              db 'o',0
.data:0000000140003006                 align 8
.data:0000000140003008 aM              db 'm',0
.data:000000014000300A                 align 4
.data:000000014000300C aP              db 'p',0
.data:000000014000300E                 align 10h
.data:0000000140003010 a4              db '4',0
.data:0000000140003012                 align 4
.data:0000000140003014 aR              db 'r',0
.data:0000000140003016                 align 8
.data:0000000140003018 aE              db 'e',0
.data:000000014000301A                 align 4
.data:000000014000301C                 db '_',0
.data:000000014000301E                 align 20h
.data:0000000140003020 aT              db 't',0
.data:0000000140003022                 align 4
.data:0000000140003024                 db 'h',0
.data:0000000140003026                 align 8
.data:0000000140003028 aE_0            db 'e',0
.data:000000014000302A                 align 4
.data:000000014000302C                 db '_',0
.data:000000014000302E                 align 10h
.data:0000000140003030 aA              db 'a',0
.data:0000000140003032                 align 4
.data:0000000140003034 aR_0            db 'r',0
.data:0000000140003036                 align 8
.data:0000000140003038 aR_1            db 'r',0
.data:000000014000303A                 align 4
.data:000000014000303C a4_0            db '4',0
.data:000000014000303E                 align 20h
.data:0000000140003040 aY              db 'y',0
.data:0000000140003042                 align 10h
```

aC라는 놈을 따라 가보니 이렇게 flag가 뭔지 나온다.

Comp4re_the_arr4y