

Strncmp



strncmp를 다운받아서 ida에 넣고 f5를 눌러서 어셈블리어를 c코드로 변환하면 다음과 같다

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
    char v4[32]; // [rsp+20h] [rbp-50h] BYREF
    char v5[40]; // [rsp+40h] [rbp-30h] BYREF
    unsigned __int64 v6; // [rsp+68h] [rbp-8h]

    v6 = __readfsqword(0x28u);
    qmemcpy(v5, "0fdlDSA|3tXb32~X3tX@sX`4tXtz", 28);
    puts("Enter your input:");
    __isoc99_scanf("%s", v4);
    if ( !strcmp_(v4, v5) )
        puts("Good game");
    else
        puts("Always dig deeper");
    return 0;
}
```

main을 보면 미리 입력된 문자열(v5)와 내가 입력한 문자열(v4)를 strcmp_라는 함수에 인자로 주었을때 return 값으로 0이 나오면 풀리는 것 같다.

strcmp_함수를 살펴보자

```
int __fastcall strcmp_(const char *a1, const char *a2)
{
    int v3; // [rsp+14h] [rbp-1Ch]
    int i; // [rsp+18h] [rbp-18h]
    int j; // [rsp+1Ch] [rbp-14h]

    v3 = 0;
    for ( i = 0; i <= 21; ++i )
        v3 = (v3 + 1) ^ 0x17;
    for ( j = 0; j < strlen(a1); ++j )
        a1[j] ^= key;
    return strncmp(a1, a2, 0x1CuLL);
}
```

a1이 우리가 입력한 문자열 v4이고, a2가 미리 입력된 문자열 (v5)로 보인다.
a1의 각 문자를 key값이랑 xor한 값으로 바꿔주고 strncmp로 a1과 a2를 비교한다.
이때 우리가 0을 리턴하기 위해서는 `a1[j] ^= key` 한 문자열과 `a2` 가 같아야 한다.
key 값을 살펴보면 check 라는 함수에서 찾을 수 있다.

```
int __fastcall check(int a1, const char **a2)
{
    int v3; // [rsp+1Ch] [rbp-4h]

    v3 = atoi(a2[1]);
    if ( v3 * (v3 - 14) == -49 )
        key = v3;
    else
        key = 0;
    return main(a1, a2, a2);
}
```

key가 0이면 문자에 ^0을 아무리 해도 자기 자신이므로
"OfdIDSA|3tXb32~X3tX@sX`4tXtz"을 입력 값으로 넣으면 Good game이라고 나오긴 한
다. 하지만 우리가 원하는 flag값은 HackCTF{~~} 형식이므로 key = v3;일때를 생각해야할
것 같다.

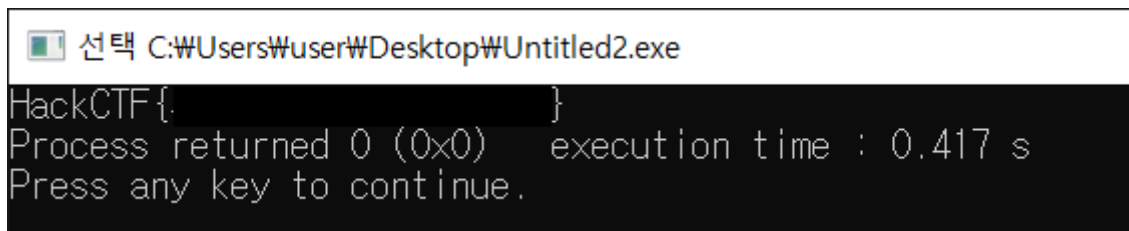
`v3 * (v3 - 14) == -49` 이려면 v3 = 7이어야 한다.

따라서 우리가 넣은 `a1 ^ key = a2("OfdIDSA|3tXb32~X3tX@sX`4tXtz")`이면 된다.

a1 = a2 ^ key로 구해보자!

```
#include <iostream>
#include <string>
using namespace std;
int main(){
    int key = 7;
    string a2 = "0fd1DSA|3tXb32~X3tX@sX`4tXtz";

    for(auto i : a2){
        char a = i^key;
        cout << a;
    }
}
```



```
선택 C:\Users\User\Desktop\Untitled2.exe
HackCTF{
}
Process returned 0 (0x0)   execution time : 0.417 s
Press any key to continue.
```

그럼 다음과 같이 flag를 알수있다!