

Keygen



다운받은 파일을 ida에 넣고 디컴파일해서 메인을 보면 `check_key` 라는 함수로 입력한 문자열을 보낸다.

```

1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     FILE *stream; // [rsp+8h] [rbp-C8h]
4     char s[80]; // [rsp+10h] [rbp-C0h] BYREF
5     char v6[104]; // [rsp+60h] [rbp-70h] BYREF
6     unsigned __int64 v7; // [rsp+C8h] [rbp-8h]
7
8     v7 = __readfsqword(0x28u);
9     setvbuf(stdout, 0LL, 2, 0LL);
10    puts(::s);
11    fgets(s, 65, stdin);
12    if (check_key(s))
13    {
14        stream = fopen("flag", "r");
15        if ( !stream )
16        {
17            puts(&byte_400AC0);
18            return 0;
19        }
20        fgets(v6, 100, stream);
21        printf("%s", v6);
22    }
23    return 0;
24 }

```

그럼 `check_key` 라는 함수로 들어가보자!

```

1 bool __fastcall check_key(const char *a1)
2 {
3     char *s2; // [rsp+10h] [rbp-10h]
4
5     if ( strlen(a1) <= 9 || strlen(a1) > 0x40 )
6         return 0;
7     s2 = (char *)encoding(a1);
8     return strcmp("OO]oUU2U<sU2UsUsK", s2) == 0;
9 }

```

대게 간단하다. 입력받은 문자열을 `encoding` 함수에 넣고 돌려서 나오는 값이 "OO]oUU2U<sU2UsUsK" 이면 우리는 flag값을 볼 수 있을 것 같다.

그럼 이제 `encoding` 함수를 살펴보자

```

1  BYTE *__fastcall encoding(const char *a1)
2  {
3      unsigned __int8 v2; // [rsp+1Fh] [rbp-11h]
4      int i; // [rsp+20h] [rbp-10h]
5      int v4; // [rsp+24h] [rbp-Ch]
6      BYTE *v5; // [rsp+28h] [rbp-8h]
7
8      v5 = malloc(0x40uLL);
9      v4 = strlen(a1);
10     v2 = 72;
11     for ( i = 0; i < v4; ++i )
12     {
13         v5[i] = ((a1[i] + 12) * v2 + 17) % 70 + 48;
14         v2 = v5[i];
15     }
16     return v5;
17 }

```

엄 저렇게 생겼구나....

잘 생각해보면 $((a1 + 12) * v2 + 17) \% 70 + 48 == \text{"OO]oUU2U<sU2UsUsK"}$ 여야 한다
따라서 $a1 = (\text{"OO]oUU2U<sU2UsUsK"} - 48 + 70 * n - 17) / v2 - 12$ 이면 된다!

$a1 = (\text{"OO]oUU2U<sU2UsUsK"} - 48 + 70 * n - 17) / v2 - 12$

이제 이걸 바탕으로 코드를 만들자!

```

#include <stdio.h>
char* decoding(const char *a1);
int main(){
    char * result = "OO]oUU2U<sU2UsUsK";
    char* key = decoding(result);
    printf("%s", key);
    return 0;
}
char* decoding(const char *a1){
    int i;
    int v4;
    char* v5 = malloc(sizeof(char)*17);
    v4 = strlen(a1);
    int v2 = 72;
    for ( i = 0; i < v4; ++i ){
        int n = 0;
        int k;
        while(1) {
            k = a1[i] - 48 + 70 * n - 17;
            int h = k/v2 - 12;
            if(k%v2 == 0 && h > 32 && h < 127 ) break;
            n++;
        }
        v5[i] = k;
    }
    return v5;
}

```

```

    }

    v5[i] = k / v2 - 12;
    v2 = a1[i];
}
return v5;
}

```

실행시키면 key == "A,d<&\$+\$".+\$&.&&iJ IDEA?TL=q"라는 문자열을 받는데 "OO]oUU2U<sU2UsUsK"의 문자열이 17이므로 key = "A,d<&\$+\$".+\$&.&"라고 볼 수 있다.

이제 nc ctf.j0n9hyun.xyz 9004을 실행시켜서 입력칸에 key값을 입력하면 flag를 볼 수 있다.

```

leede@leede:~$ nc ctf.j0n9hyun.xyz 9004
키 입력 :
A,d<&$+$' ' .+$&.&
HackCTF{ }

```

여담) 아니 근데 "A,d<&\$+\$".+\$&.&"이게 키 값으로 보이는가???? 난 저 문자열이 나오고 당연히 내가 잘 못 했겠지 생각했는데 저게 맞다니... 좀 어이 없긴했다.. 내 시간ㅜㅜㅜ