

```
1 int __fastcall main(int argc, const char **argv, const char **envp)
2 {
3     char *v3; // rbx
4     char _0[72]; // [rsp+0h] [rbp+0h] BYREF
5     unsigned __int64 vars48; // [rsp+48h] [rbp+48h]
6
7     vars48 = __readfsqword(0x28u);
8     puts("Go ahead, guess the flag: ");
9     v3 = _0;
10    fgets(_0, 63, stdin);
11    while ( strlen(_0) > v3 - _0 )
12        *v3++ ^= 1u;
13    if ( !strcmp(_0, secretcode) )
14        puts("Correct! It was kinda obvious tbh.");
15    else
16        puts("Wrong. Not sure why you'd think it'd be that.");
17    return 0;
18 }
```

IDA로 디컴파일해서 보면 fgets 함수를 통해 사용자 입력을 받고, 1과 xor 연산한 결과와 secretcode와 비교해서 맞으면 Correct를 출력해준다.

```
gef> x/s $rsi
0x56426e331020 <secretcode>:    "bugzbnllhuude^un^uid^md`ru^rhfohghb`ou^chu|"
```

secretcode에는 다음과 같은 문자열이 저장되어 있는데, 위 값을 1과 xor하면 원본 문자열이 나온다.

**Recipe**

XOR

Key: 1      Scheme: Standard

Null preserving

**Input**

```
^ bugzbnllhuude^un^uid^md` ru^rhfohghb` ou^chu||
```

RBC 44    1    44

**Output**

```
actf{committed_to_the_least_significant_bit}
```