

XCTF攻防世界 - Reverse - 666

原创

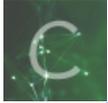
[Weird0](#) 于 2021-02-03 15:36:25 发布 183 收藏 1

分类专栏: [Reverse](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/Sanctuary1307/article/details/113608302>

版权



[Reverse](#) 专栏收录该内容

8 篇文章 0 订阅

订阅专栏

题目文件为ELF格式, 用IDA64打开, 反编译主函数:

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
    char s; // [rsp+0h] [rbp-1E0h]
    char v5; // [rsp+F0h] [rbp-F0h]

    memset(&s, 0, 0x1EuLL);
    printf("Please Input Key: ", 0LL);
    __isoc99_scanf("%s", &v5);
    encode(&v5, (__int64)&s); //对输入的flag字符串编码
    if ( strlen(&v5) == key ) //编码后长度为 key = 18
    {
        if ( !strcmp(&s, enflag) ) //比较编码后的flag是否正确
            puts("You are Right");
        else
            puts("flag{This_1s_f4cker_flag}");
    }
    return 0;
}
```

enflag字符串值如下 (IDA选中字符串, 快捷键Shift+E, 末尾0可去掉)

```
unsigned char ida_chars[] =
{
    105, 122, 119, 104, 114, 111, 122, 34, 34, 119,
    34, 118, 46, 75, 34, 46, 78, 105, 0
};
```

编码函数如下:

```

int __fastcall encode(const char *a1, __int64 a2)
{
    char v3[32]; // [rsp+10h] [rbp-70h]
    char v4[32]; // [rsp+30h] [rbp-50h]
    char v5[40]; // [rsp+50h] [rbp-30h]
    int v6; // [rsp+78h] [rbp-8h]
    int i; // [rsp+7Ch] [rbp-4h]

    i = 0;
    v6 = 0;
    if ( strlen(a1) != key ) //flag长度为18
        return puts("Your Length is Wrong");
    for ( i = 0; i < key; i += 3 ) //从0开始, 以三个字符为一组运算
    {
        v5[i] = key ^ (a1[i] + 6);
        v4[i + 1] = (a1[i + 1] - 6) ^ key;
        v3[i + 2] = a1[i + 2] ^ 6 ^ key;
        *(_BYTE *)(a2 + i) = v5[i];
        *(_BYTE *)(a2 + i + 1LL) = v4[i + 1];
        *(_BYTE *)(a2 + i + 2LL) = v3[i + 2];
    }
    return a2;
}

```

已知编码方式，编写python脚本解码：

```

#xctf-re-666
s = [105, 122, 119, 104, 114, 111, 122, 34, 34, 119,
     34, 118, 46, 75, 34, 46, 78, 105 ]
k = 18
i = 0
flag = ''

while(i < k):
    flag += chr((k^s[i] - 6)
    flag += chr((s[i+1]^k) + 6)
    flag += chr(s[i+2]^k^6)
    i += 3

print(flag)

```

运行脚本得到flag: `unctf{b66_6b6_66b}`