JarvisOJ basic部分WriteUp

原创

 Magic1an
 ● 于 2017-08-25 00:12:18 发布
 ● 2211 ☆ 收藏

 分类专栏:
 ctf 文章标签:
 ctf

 版权声明:
 本文为博主原创文章,遵循 CC 4.0 BY-SA 版权协议,转载请附上原文出处链接和本声明。

 本文链接:
 https://blog.csdn.net/Magic1an/article/details/77543978

 版权



ctf 专栏收录该内容

3 篇文章 0 订阅 订阅专栏

0x0 前言

由于开学后会有一个省赛,作为一个好久没做过除re以外ctf题的小白,不得不抽出时间来刷一刷题...通过做JarvisOJ的basic部 分确实学到了不少东西,感谢~

0x1 base64?

1.题目描述

 $GUYDIMZVGQ2DMN3CGRQTONJXGM3TINLGG42DGMZXGM3TINLGGY4DGNBXGYZTGNLGGY3DGNBWMU3W {\tt ==} \\$

2.解题过程

```
base64?应该是base家族的,写个脚本decode一下。
```

```
import base64
str1='GUYDIMZVGQ2DMN3CGRQTONJXGM3TINLGG42DGMZXGM3TINLGGY4DGNBXGYZTGNLGGY3DGNBWMU3WI==='
try:
    print base64.b64decode(str1)
except:
    print base64.b32decode(str1)
except:
    print base64.b16decode(str1)
```

得到结果504354467b4a7573745f743373745f683476335f66346e7d,很明显,十六进制转字符就可以了~

```
flag=''
key='504354467b4a7573745f743373745f683476335f66346e7d'
for i in range(0,len(key),2):
    flag+=chr(int(key[i:i+2],16))
print flag
```

得到flag:PCTF{Just_t3st_h4v3_f4n}

0x2 关于USS Lab.

题目描述

USS的英文全称是什么,请全部小写并使用下划线连接_,并在外面加上PCTF{}之后提交

解题过程

百度uss lab可以搜到

USS Lab. - Ubiquitous System Security Lab.

查看此网页的中文翻译,请点击 翻译此页

Ubiquitous System Security Lab. Welcome to USS(Ubiquitouse System Security) Lab. USL Lab. belongs to Electrical Engineering College in Zhejiang University... www.usslab.org/ マ - 百度快照 http://blog.csdn.net/Magiclan

OK,flag得到了。

0x3 veryeasy

题目描述

使用基本命令获取flag

解题过程

使用srings得到flag.

<pre>myubuntu@ubuntu:~/Desktop\$ strings veryeasy</pre>
PAGEZERO
text
TEXT
unwind_info
TEXT
DATA
data
DATA
LINKEDIT
/usr/lib/dyld
/usr/lib/libSystem.B.dylib
PCTF{strings_i5_3asy_isnt_i7}
_mh_execute_header
\$main
mh_execute_header
_main http://blog.csdp.pot/Magiclap
dyld_stub_binder ^{rrrrp.//brog.} csun.net/magician

0x4 段子

题目描述

程序猿圈子里有个非常著名的段子:

手持两把锟斤拷,口中疾呼烫烫烫。

请提交其中"锟斤拷"的十六进制编码。(大写)

FLAG: PCTF{你的答案}

Unicode和老编码体系的转化过程中,肯定有一些字,用Unicode是没法表示的,Unicode官方用了一个占位符来表示这些文字,这就是:U+FFFD REPLACEMENT CHARACTER。

那么U+FFFD的UTF-8编码出来,恰好是 "xefxbfxbd'。如果这个"xefxbfxbd',重复多次,例如 "xefxbfxbd\xefxbfxbd', 然后放到GBK/CP936/GB2312/GB18030的环境中显示的话,一个汉字2个字节,最终的结果就是: 锟斤拷——锟(0xEFBF),斤 (0xBDEF),拷(0xBFBD)^[1]。 http://] 編編編編

好了,将三个字拼起来就得到了flag:PCTF{EFBFBDEFBFBD}

0x5 手贱

题目描述

某天A君的网站被日,管理员密码被改,死活登不上,去数据库一看,啥,这密码md5不是和原来一样吗?为啥登不上咧?

d78b6f302l25cdc811adfe8d4e7c9fd34

请提交PCTF{原来的管理员密码}

解题过程

在上面不容易看出,复制到别的地方还是可以轻松的发现上面md5比正确的值多了一位I。去掉I后得到 d78b6f30225cdc811adfe8d4e7c9fd34,进行md5解密后即可。

0x6美丽的实验室logo

题目描述

出题人丢下个logo就走了,大家自己看着办吧

ri	S	_		×
	Frame : 2 of 2			
É				
ų				
				t
				619
5)				
'n				
	PCTF{You_are_R3ally_Car3ful}			
				, 1
				4)
-				
				4
-				
	Save			
	http://blog.csdn.	net/	Mag10	an mu tank

0x7 veryeasyRSA

题目描述

已知RSA公钥生成参数:

 $\mathsf{p} = 3487583947589437589237958723892346254777 \ \mathsf{q} = 8767867843568934765983476584376578389$

e = 65537

求d =

请提交PCTF{d}

Hint1: 有好多小伙伴问d提交什么格式的,现在明确一下,提交十进制的d

运用RSA Tool计算出d.

📽 RSA-Tool 2 by tE! —	\times
VI.7 Keysize (Bits)	Base
Random data generation Public Exponent (E) [HEX] Start Seedfile loaded. 10001	
1st Prime (P)	
3487583947589437589237958723892346254777	$\hat{}$
2nd Prime (Q)	
8767867843568934765983476584376578389	$\hat{}$
Modulus (N) R Exact size:	0 Bits
30578675145816634962204467309994126955968568987449100734690153203822106214253	< \ \
Private Exponent (D)	
19178568796155560423675975774142829153827883709027717723363077606260717434369	^
	\sim
Generate Test Factoring info (Prime factors):	0
Calc. D Factor N	^
Help Exit Use MROS method only I No time chacks	~
Ready. To create RSA Keys, press >Start< now to generate some random data	cla n

0x8 神秘的文件

题目描述

出题人太懒,还是就丢了个文件就走了,你能发现里面的秘密吗?

解题过程

利用linux的file得知所给文件为磁盘文件。 将磁盘文件挂载

mkdir ffffile &&sudo mount haha ffffile

挂载后可以查看文件中的内容 我们发现里面是253个只包含一个字符的文件 猜测可以把这些字符拼接起来得到flag.

```
flag=''
for i in range(254):
    file=open('ffffile/'+str(i))
    flag+=file.read()
    file.close()
print flag
```

myubuntu@ubuntu:~/Desktop\$ python kkkkk.py
Haha ext2 file system is easy, and I know you can easily decompress of it and fi
nd the content in it.But the content is spilted in pieces can you make the piece
s together. Now this is the flag PCTF{P13c3_7oghter i7}. The rest is up to you.
Cheer up, boy.

0x9公倍数

题目描述

请计算100000000以内3或5的倍数之和。

如: 10以内这样的数有3,5,6,9, 和是23

请提交PCTF{你的答案}

解题过程

```
sum=0
for i in xrange(100000000):
    if i%3==0 or i%5==0:
        sum+=i
print sum
```

一个简单的小脚本得到flag,这里注意一定要用xrange,不要用range!

0x10

题目描述

都说逆向挺难的,但是这题挺容易的,反正我不会,大家来挑战一下吧~~:)

解题过程

载入IDA, 很容易就能找到关键代码

```
*( WORD *)v5 = 0xDDABu;
 v5[2] = 0x33;
 v5[3] = 0x54;
 v5[4] = 0x35;
 v5[5] = 0xEFu;
 printf((unsigned __int64)"Input your password:");
 _isoc99_scanf((__int64)"%s", v6, *(_QWORD *)v5);
 if ( strlen(v6) == 26 )
 {
   v3 = 0LL;
   if ( (v6[0] ^ 0xAB) == list1 )
   {
     while ( ((unsigned __int8)v6[v3 + 1] ^ (unsigned __int8)v5[(signed __int64)(((signed int)v3 + 1)
      {
       if ( ++v3 == 25 )
        {
          printf((unsigned __int64)"Congratulations!");
          return 0;
       }
     }
   }
 }
 printf((unsigned __int64)"Password Wrong!! Please try again.");
 return 0;
}
```

逆一下代码写脚本得到flag.

得到flag: PCTF{r3v3Rse_i5_v3ry_eAsy}

0x11 Secret

题目描述

传说中的签到题

题目入口: http://web.jarvisoj.com:32776/

Hint1: 提交格式PCTF{你发现的秘密}

查看响应头,可以找到疑似flag的字符串..

请求网址: http://web.jarvisoj.com:32776/	
请求方法: GET	
远程地址: 120.26.131.152:32776	
状态码:● 200 OK [详细了解]	编辑和重发 原始头
版本: HTTP/1.1	
♡ 过滤消息头	
▼ <u>响应头 (321 字节)</u>	
Date: "Wed, 23 Aug 2017 11:24:34 GMT"	[详细了解]
Server: "Apache/2.4.18 (Unix) OpenSSL/perl/2.0.8-dev Perl/v5.1	6.3" [详细了解]
X-Powered-By: "PHP/5.6.21"	
Secret: "Welcome_to_phrackCTF_2016"	
Content-Length: "26"	[详细了解]
Keep-Alive: "timeout=5, max=100"	[详细了解]
Connection: "Keep-Alive"	[详细了解]
Content-Type: "text/html; charset=UTF-8"	[详细了解]
▶请求头(432字节) http://blog.csdn.	net/Magiclan

提交上去没想到竟然是对的。

0x12 爱吃培根的出题人

题目描述

听说你也喜欢吃培根?那我们一起来欣赏一段培根的介绍吧:

bacoN is one of aMerICa'S sWEethEartS. it's A dARlinG, SuCCulEnt fOoD tHAt PaIRs FlawLE

什么,不知道要干什么?上面这段巨丑无比的文字,为什么会有大小写呢?你能发现其中的玄机吗?

提交格式: PCTF{你发现的玄机}

解题过程

提示培根加密,直接用脚本,不过脚本得到的flag多了一个字母...不知道哪儿出了问题。

```
#coding:utf-8
import string
letters=string.uppercase
a="bacoN is one of aMerICa'S sWEethEartS. it's A dARlinG, SuCCulEnt fOoD tHAt PaIRs FlawLE"
str1=''
str2=''
key1={"A":"aaaaa","B":"aaaab","C":"aaaba","D":"aaabb","E":"aabaa","F":"aabab","G":"aabba","H": "aabbb",
"T":"baabb",
"U":'babaa',
'V':'babab',
'W':'babba',
'X':'babbb',
'Y':'bbaaa',
'Z':'bbaab'}
key2={'a':'AAAAA','g':'AABBA','n':'ABBAA','t':'BAABA',
'b':'AAAAB','h':'AABBB','o':'ABBAB','u':'BAABB','v':'BAABB',
'c':'AAABA','i':'ABAAA','j':'ABAAA','p':'ABBBA','w':'BABAA',
'd':'AAABB','k':'ABAAB','q':'ABBBB','x':'BABAB',
'e':'AABAA','l':'ABABA','r':'BAAAA','y':'BABBA',
'f':'AABAB','m':'ABABB','s':'BAAAB','z':'BABBBB'}
list1=[]
list2=[]
temp1=''
temp2=''
num=0
for i in a:
    if i.isupper():
        temp1+='b'
        temp2+='B'
        num+=1
        if num%5==0:
            list1.append(temp1)
            list2.append(temp2)
            temp1=''
            temp2=''
    elif i.islower():
        temp1+='a'
        temp2+='A'
        num+=1
        if num%5==0:
            list1.append(temp1)
            list2.append(temp2)
            temp1=''
            temp2=''
#
for i in list1:
    for j,k in key1.items():
        if i==k:
            str1+=j
print "第一种:"
print str1+'\n'
for i in list2:
    for j,k in key2.items():
        if i==k:
            str2+=j
print "第二种:"
print str2
```

0x13 Easy RSA

题目描述

还记得veryeasy RSA吗?是不是不难?那继续来看看这题吧,这题也不难。

已知一段RSA加密的信息为: 0xdc2eeeb2782c且已知加密所用的公钥:

(N=322831561921859 e = 23)

请解密出明文,提交时请将数字转化为ascii码提交

比如你解出的明文是0x6162,那么请提交字符串ab

提交格式:PCTF{明文字符串}

已知N、e可以计算出d,这里仍然可以用RSA Tool。

SA-Tool 2 by tE!	_	×
TOOL 2 v1.7	Numi 10	ber Base ▼
Random data generation Public Exponent (E) [HEX] -		
1st Prime (P)		
13574881		$\hat{}$
2nd Prime (Q)		
23781539		$\hat{\mathbf{C}}$
Modulus (N) R	Exact size:	255 Bits
322831561921859		A
		~
Private Exponent (D)		
42108459725927		~
		~
Generate Test Factoring info (Prime factors):		0
PRIME FACTOR: 13574881		^
Calc. D Factor N From From From From From From From From		
		U
Help Exit		
Help Exit Use MPQS method only No time checks	n. net./Ma	ricla n

然后再利用 密文=明文^d mod N的公式计算出密文,最后将密文转化为ascii就好了。

8	Big	Integer Calculator v1.00	Jul.2007		_		\times
X	(242094131279916					Ŷ
Y n		42108459725927					0
2	Z	322831561921859					0
A Q B A M R	ns uo cd od em	0 862008665					~ ~ ~
B	md						~
	X+Y	X-Y X*Y X/Y	X n X !	X (1/n) CD(X, Y)	X Y M	MOD Z	
В	ase	C 2 C 8 🖲 10	C 16 C	36 🔿 60	C 64	C 256	
Bit	ts: :	x-48 y-46 z-49 A+0 B-30	blog.c	sdn.ab	but / M	Brit	lan

最后得到flag为PCTF{3a5Y}

0x14 ROPGadget

题目描述

都说学好汇编是学习PWN的基础,以下有一段ROPGadget的汇编指令序列,请提交其十六进制机器码(大写,不要有空格)

XCHG EAX,ESP

RET

MOV ECX,[EAX]

MOV [EDX],ECX

POP EBX

RET

提交格式: PCTF{你的答案}

解题过程

一开始我试图用pwntools的asm函数去求flag,不过不幸的是失败了。然后又想到利用od去求,幸好这次成功了。

94	xchg eax,esp
C3	retn
8B 08	mov ecx,dword ptr ds:[eax]
890A	mov dword ptr ds:[edx],ecx
5B	Rep rep /hlog ordn not /Mogiolon
63	reti

将十六进制拼接起来既是flag。

0x15取证

题目描述

有一款取证神器如下图所示,可以从内存dump里分析出TureCrypt的密钥,你能找出这款软件的名字吗?名称请全部小写。



解题过程

以前没接触过只好百度了,不过得到好多结果,最后试出flag为PCTF{volatility}

0x16 熟悉的声音

题目描述

两种不同的元素,如果是声音的话,听起来是不是很熟悉呢,据说前不久神盾局某位特工领便当了大家都很惋惜哦

XYYY YXXX XYXX XXY XYY X XYY YX YYXX

请提交PCTF{你的答案}

先将上面字符串转化为-.组成的字符串

```
def getMorse(s):
    morse=''
    for i in range(len(s)):
        if s[i]=='X':
            morse+='.'
        elif s[i]=='Y':
            morse+='-'
        else:
            morse+=s[i]
        return morse
s='XYYY YXXX XYXX XXY XYY X XYY YX YYXX'
print getMorse(s)
```


然后找一个摩斯密码解密的网站得到JBLUWEWNZ。本来以为到这就完了,结果提交上去并不对..需要凯撒解密才可以得到flag~

```
s="JBLUWEWNZ"
for j in xrange(26):
   flag=''
    print str(j)+':',
    for i in s:
        if(i \ge A' and i \le Z'):
            temp = ord(i) + j
            if temp>ord('Z'):
               temp = temp - 26
            flag +=chr(temp)
        elif i>='a' and i<='z':
           temp = ord(i) + j
            if temp>ord('z'):
                temp = temp - 26
            flag +=chr(temp)
        else:
            flag +=i
    print flag
```

#http://rot13.de/index.php

0x16 Baby's Crack

题目描述

既然是逆向题,我废话就不多说了,自己看着办吧。

```
while ( feof(*(_QWORD *)&argc, argv, v8, v16) == 0 )
{
 v17 = fgetc(*(_QWORD *)&argc, argv, v9, v16);
 if ( v17 != -1 && v17 )
  {
   if ( u17 > 47 && u17 <= 96 )
    {
     v17 += 53;
    }
    else if ( v17 <= 46 )
    {
     u17 += u17 % 11;
                           Т
    }
    else
    {
     v17 -= v17 % 61;
    fputc(*(_QWORD *)&argc, argv, v15, (unsigned int)v17);
 }
}
```

我这采用了爆破的方法解密文件. 最后将解密的十六进制转为字符即可得到flag.

```
file=open('flag.enc','r')
s=file.read()
flag=''
for i in range(len(s)):
    for j in range(128):
        if j>47 and j<=96:
            k=j+53
            if k==ord(s[i]):
                flag+=chr(j)
                break
        elif j<=46:
            k=j+j%11
            if k==ord(s[i]):
                flag+=chr(j)
                break
        else:
            k=j-j%61
            if k==ord(s[i]):
                flag+=chr(j)
                break
print flag
file.close()
key=''
for i in range(0,len(flag),2):
    key+=chr(int(flag[i:i+2],16))
print key
```

0x17 Help!!

题目描述

出题人硬盘上找到一个神秘的压缩包,里面有个word文档,可是好像加密了呢~让我们一起分析一下吧!

下载下来后发现是个被加密的压缩包,这里是伪加密,用ZipCenOp轻松去掉伪加密后获得一个word文件。 关于word我至今只做过解压和利用word软件的隐藏字符功能两类题目,这儿是解压。 解压后得到flag:PCTF{You_Know_moR3_4boUt_woRd}。

0x18 Shellcode

题目描述

作为一个黑客,怎么能不会使用shellcode?

这里给你一段shellcode,你能正确使用并最后得到flag吗?

解题过程

一个shellcode当然是要执行啊!

编译运行即可得到flag:PCTF{Begin_4_good_pwnn3r}.

0x19 A Piece Of Cake

题目描述

nit yqmg mqrqn bxw mtjtm nq rqni fiklvbxu mqrqnl xwg dvmnzxu lqjnyxmt xatwnl, rzn nit uxnntm xmt zlzxuuk mtjtmmtg nq xl rqnl. nitmt vl wq bqwltwlzl qw yivbi exbivwtl pzxuvjk xl mqrqnl rzn nitmt vl atwtmxu xamttetwn xeqwa tsftmnl, xwg nit fzruvb, nixn mqrqnl ntwg nq gq lqet qm xuu qj nit jquuqyvwa: xbbtfn tutbnmqwvb fmqamxeevwa, fmqbtll gxnx qm fiklvbxu ftmbtfnvqwl tutbnmqwvbxuuk, qftmxnt xznqwqeqzluk nq lqet gtamtt, eqdt xmqzwg, qftmxnt fiklvbxu fxmnl qj vnltuj qm fiklvbxu fmqbtlltl, ltwlt xwg exwvfzuxnt nitvm twdvmqwetwn, xwg tsivrvn vwntuuvatwn rtixdvqm - tlftbvxuuk rtixdvqm yivbi evevbl izexwl qm qnitm xwvexul. juxa vl lzrlnvnzntfxllvldtmktxlkkqzaqnvn. buqltuk mtuxntg nq nit bqwbtfn qj x mqrqn vl nit jvtug qj lkwnitnvb rvquqak, yivbi lnzgvtl twnvnvtl yiqlt wxnzmt vl eqmt bqefxmxrut nq rtwal nixw nq exbivwtl.

解题过程

加密方式为字母频率破解替换加密,可在http://quipqiup.com/上进行在线解密。 解密后得到

the word robot can refer to both physical robots and virtual software agents, but the latter are usuall

0x20 -.-字符串

题目描述

请选手观察以下密文并转换成flag形式

flag形式为32位大写md5

解题过程

啥也不说,直接摩斯密码解密得到flag.

0x21德军的密码

题目描述

解题过程

一种名为费纳姆密码的加密方式, 解密脚本如下

```
# coding=utf-8
#--author:Magician--
passdict={'A':'1000001','B':'1000010','C':'1000011', 'D': '1000100','E':'1000101', 'F' :'1000110', 'G':
password='WELCOMETOCFF'
li=[]
for i in password:
   li.append(passdict[i])
flag=''
for i in range(0,len(miwen),7):
   test=miwen[i:i+7]
   test=int(test,2)
   test^=int(li[i/7],2)
   for i,j in passdict.items():
      if test==int(j,2):
         flag+=i
print '解密/加密结果为:%s'%flag
```

0x22 握手包

题目描述

给你握手包,flag是Flag_is_here这个AP的密码,自己看着办吧。

解题过程

以前没接触过,百度得知可以用linux自带的aircrack-ng进行暴力破解。

```
aircrack-ng -a2 -w password.txt wifi.cap
```