SKCTF Writeup



签到题

请打开微信关注,发送give me flag,即可获得。

Encode

1.ACSCLL

首先看到这类题,我们肯定是要使用ASCLL的(这么明显的提示大家肯定一眼就能看出来),我们可以对照 Ascii码表一一寻找,或者自己编写一段代码来实现,再或者简单地通过部分简单的解码网站来实现(如...这个就 不列举了) 这里放上自己写的吧

```
#include <stdio.h>
int main ()
{
    int n;
    while(scanf("%d",&n)!=000)
    {
        printf("%c",n);
    }
}
```



这个上面有小暗示(听说由十六位组成),这不是**16**位嘛,这就好办了,还是两种办法,一种自己写代码实现,另一种就是在线的转换

(https://www.bejson.com/convert/ox2str/)

第二种推荐实在编不出来在使用

flag{Hex_is_easy}

	CONCICII CI LIKHII II LIHIMA «
首页 JSON相关▼ 编码/加密▼ 格式化▼ 网络▼ 前端▼	∽ 后端♥ 转换▼ 其他▼
API→ 文档→ 平台工具→ 赞助商→ 更多→ <mark>●</mark>	
16进制到文本字符串的转换,在线实时转换	
16进制到又本子符甲的转换,在线实时转换(支持中又转换)	
加密或解密字符串长度不可以超过10M	
666c61677b4865785f69735f656173797d	
	24
16进制转字符 字符转16进制 清空结果	54
flag <mark>{Hex_is_easy}</mark>	
	https://blog.csdn.net/weixin_43848306

3.Escape

我们进来后会发现有一个txt文件在等着我们,我们就肯定开心的点开啊,但是发现有一个字符串在等着,仔细 观察发现这个是肯定是url解码啊,然后就解决了,这个不知道怎么写代码解决,就只推荐

(http://tool.chinaz.com/tools/urlencode.aspx) 这个网址来解决下吧, flag{do_not_Escape}

4.jsfuck

题目上写的很明显了,就是jsfuck,只需要点开,将内容复制下来,如果你使用的是google浏览器的话,打开 F12,点击console按下Ctrl+v加回车就完事了;如果没有的话,那就

http://discogscounter.getfreehosting.co.uk/js-noalnum.php?ckattempt=1&i=1,这个网址解决问题吧。 flag{it_is_js?}

		Misc	
z密码			
Challenge	33 Solves	×	
	Ez密码 30		
∿明喜欢用8位的 回的密码,你能	9日期当密码,他用了一个17 破解出来么?	7年以后的日子当做了压缩	
🛓 flag.zip			
Flag		Submit	

这个题是对考察zip文件解压的,上面题目里给出的信息有密码是**1.八位 2.是全数字.3.十七年后的日子** 我在这里使用的是暴力破解,借助了工具ziperello

7 Ziperello						
j ziperell	o sword recovery t	ool	帮	助	关于	退出
逝去时间: 00:00:03	当前密码长度 当前密码 当前速度 18%	8 信息 茶码: 20170328 通定	准备就绪,请 注意:搜索进 前的密码效验 耗时较长。	点击[开 度条(% 长度相)	步骤 4 始〕 按钮)及剩余时间字段 ^{美。} 破解 AES 算法	显示的信息与当 加密的密码可能
10:41:03: 201703	20 .μγμη: 55	步骤 4 / 4:			//esterementerementer////	

然后对文件进行解压,会发现:咦只有一个jpg文件,我的flag那?这是我们需要打开属性,查看详细信息,会 发现flag藏在这里,真皮

🔝 161026130024-9.jpg 属性 \times 详细信息 安全 以前的版本 常规 \land 属性 值 $\stackrel{}{\leftrightarrow} \stackrel{}{\leftrightarrow} \stackrel{}{\leftrightarrow} \stackrel{}{\leftrightarrow} \stackrel{}{\leftrightarrow} \stackrel{}{\leftrightarrow} \stackrel{}{\leftrightarrow}$ 分级 标记 flag{exif_is_easy} 备注 来源 作者 2016/3/10 7:49 拍摄日期 Adobe Photoshop CC 2014 (Windows) 程序名称 获取日期 版权 图像 图像 ID 分辨率 2560 x 1600 宽度 2560 像素 高度 1600 像素 水平分辨率 300 dpi 300 dpi 垂直分辨率 位深度 24 压缩 分辨率单位 2 颜色表示 sRGB V ______ 删除属性和个人信息 确定 取消 应用(A)

2.小猪佩奇





	00000880	50	54 (6C)	24	76 03 58 68) 5B	80	51	28	67 1	1F 9	5 UC	78	15 4E 76 7b	A Althornov - y N		C:\Users\Y\D
_	00000BD0	02	30 1	22 !	56 1E	96	FA	5E	CB	7A 1	BE 41	2 32	00	30 00	0 0âV -ú^ËzŽN2 0		File size:
Data	Interpreter		00 : 5D 0	32 (CF '	00 74 7E 10	5E 62	0C 3A	FF 4E	D1 86	53 ! 4E (55 50 00 41	C F3 E 2A	81 4E	CA 4E 09 67	E 1 2 t^ ÿÑsu\6 ÊN 7 ò]Ï~ b:N†N N*N g		
8 Bi	t (±): 0		5B 9	9в !	52 1Æ	59	86	98	DF	57	34 7	5 E2	56	1F 96	6 ž[>R Y†~ßW"vâv −		Default Edit I
16 Bi	t (±): 3,328		FF 1	14 '	78 76	5 7A	86	98	DF	57 (05 5	3 2B	54	17 6E	E ÿ xvz†~ßW S+T n		State:
32 Bi	t (±): 687,869,1	84	90 4	4B (6D D5	6 8B	01	30	06	90 :	11 5	4 E5	5D	0B 7A	A KmŐ< 0 Tå]z		vel:
	00000C30	01	30 3	BA (67 68	56	66	5B	60	4E (01 3	27	59	70 65	5 0:ghVf[`N 0'Ype	Position Manager (General)	×
	00000C40	6E	63 8	8C 5	54 C6	5 5 B	01	78	66	5B (02 3	0 O D	00	0D 00	0 nc@TE[xf[0		
	00000c50	0E	60 4	48 4	4E 65	51	E8	95	0D	00 4	41 5	3 00	4E	C7 8F	F `HNeQè• AS NÇ	Description of this and them	tim
	000000060	0E	54 :	lA 4	4F 09	67	70	65	ЗA	57	65 5	1 E8	95	11 54	4 T O gpe:WeQè• T	Description of this position.	
	00000070	80	62 3	2F (67 B2	8B	A7	5E	0C	FF 3	26 51	E 60	4 F	1D 52	2 €b/g°<§^ ÿ&^`O R	flag{Oh!_A_h1dd3n_mes5A9e}	e tin
	000000080	A2	63 8	39 !	5B 68	51	02	30	0D	00 (00 6	7 73	51	2E 95	5 ¢c%[hQ 0 gsQ.•	CD0	c un
	000000090	84	76 1	08 8	3F 2F	66	EA	81	F1	5D (34 7	5 AA	52	9B 52	2 "vø /fê ñ]"vªR>R		
	00000CA0	0C	FF '	7E (62 30	52	EA	81	F1	5D 1	F3 6) 81	89	66 5B	B ÿ~b0Rê ñ]ó`%f[Length (hexadec.):	es:
	00000CB0	60	4E (34 1	76 B9	65	11	54	0C	FF 3	29 53	2 28	75	EA 81	1 `N"v¹e T ÿ)R(uê	34	
	000000000	F1	5D 8	34 '	76 FE	8B	59	4F	F6	65 1	F4 9	5 02	30	0D 00	0 ñ]"vþ«YOöeô• 0		
	00000CD0	66	00 (6C (00 61	. 00	67	00	7B	00 4	4F 0	0 68	00	21 00	0 flag {Oh !		
	00000CE0	5F	00 4	41 (00 5E	00	68	00	31	00	64 0	0 64	00	33 00	0 _ A _ h 1 d d 3		
	00000CF0	6E	00 5	5F (00 GI	00	65	00	73	00 3	35 0) 41	00	39 00	0 n _ m e s 5 A 9		r þa
	000000000	65	00 '	7D (00 OI	00	29	52	28	75 4	43 0	54	00	46 00	0 e })R(uC T F		#:

00000D10 00000D20	73 5E F0 53 DB 8F 4C 88 65 67 C3 7E 60 4E 02 30 OD 00 66 4E 4D 7C 2F 00 51 7F FE 8B 2F 00 28 57	s^ðSÛ L^egĀ~`N 0 fNM/ Q bc/ (W
00000D30 00000D40	BF 7E 9E 5B 8C 9A 0D 00 66 5B 1A 4F D0 63 EE 95 20 00 13 00 20 00 48 00 59 00 50 00 45 00 52 00	دَخَلَقَةُ f[ODcî• H Y P E R QK Cancel @ Help der
00000D50 00000D60	4C 00 49 00 4E 00 4B 00 20 00 22 00 68 00 74 00 74 00 70 00 3A 00 2F 00 2F 00 77 00 77 00 77 00	LINK "ht Ap
00000D70 00000D80	2E 00 6A 00 69 00 61 00 6E 00 73 00 68 00 75 00 2E 00 63 00 6F 00 00 2F 00 70 00 2F 00 36 00	. jianshu . com/p/6
00000D90 00000DA0	30 00 64 00 64 00 38 00 65 00 39 00 63 00 64 00 31 00 32 00 66 00 22 00 20 00 14 00 3C 00 3C 00 20 00 20 00 20 00 20 00 20 00 3C 00 3C 00 3C 00	0 d d 8 e 9 c d 1 2 f " < <
00000DB0	20 00 D0 63 EE 95 84 76 7A 66 67 61 20 00 3E 00 3E 00 15 00 0D 00 84 55 28 75 47 00 6F 00 6F 00 67 00 66 00 66 00 16 64 22 7D PD 80 28 5F 60 4F	DCl•,VZZGa > ,U(uG o o) // a l o d'live ^) o
00000DE0 00000DF0	E3 89 B3 51 60 4F 47 90 30 52 84 76 27 59 E8 90 06 52 EE 95 98 98 0D 00 00 00 00 00 00 00 00	g t ∈ d /ye. 0 ãk*Q'OG 0R,,v'Yè Rŝ•*~
00000E00 00000E10	00 08 00 00 24 08 00 00 26 08 00 00 28 08 00 00 DA 08 00 00 E0 08 00 00 E2 08 00 00 FE 08 00 00	
00000E20 00000E30	02 09 00 00 08 09 00 00 4A 09 00 00 56 09 00 00 8A 09 00 00 94 09 00 00 50 0A 00 00 5A 0A 00 00	J V Š " P Z
00000E40 00000E50	D0 0A 00 0E C7 A8 8D A8 8D 72 59 3D 59 3D 59 72 59 72 59 70 00 </th <th>Ð &Ç " YYY YYY</th>	Ð &Ç " YYY YYY
00000E60 00000E70	00 00 00 00 00 00 00 00 00 00 00 00 00	7 h pI 🗸 https://blog.csdn.net/weix/n_43848306

点开就会得到flag

6.ZipWithCrypto

这个题目的话你会下载下来发现有个压缩包(好像听说这个有解压密码,但是貌似我的没有哎,可能是因为解 压工具原因),总之打开后会发现一个字符串

		↑ ■ Ξ	📕 flag.zip - 解包大小为 1 K	В					V				
	_ 🔨 🖱	名称			压缩前	压缩后	举刑	修改日日	A		1.00		14
	🥘 flag - 记事本									-		×	
字	文件(F) 编辑(E) 格式(O) 查看(V)	帮助(H)											网安
	fgsfr0}xsnraq@p{1_pr@											~	
													×
Т												14	作應ILX
													6
次件													
R													
												/eixin_4 <mark>38</mark> 4	
	•												

表示看到密码有点蒙,但是看到里面有"{}"类的,但是没有组合起来,自然就想到了栅栏,就用栅栏跑一下,考虑到密码是skctf开头的,{}位就要有5个字,因此就将移位码确定到3,将得到的密码再用凯撒跑下就得到flag了

7.Crack it

打开后会发现一个字符串:

root:\$6\$HRMJoyGA\$26Flgg6CU0bGUOfqFB0Qo9AE2LRZxG8N3H.3BK8t49wGlYbkFbxVFtGOZqVlq3qQ6k0or 仔细观察会发现这个是查看shadow的,打开kali使用john直接破解就行



然后就找到了, flag{hellokitty}

8.啊哒

这个题目中发现图中有隐藏文件,需要借助神器kali,打开kali,打开终端使用binwalk,发现有隐藏文件,使用 foremost将他分离,将会在out中发现隐藏文件flag是个被压缩的txt文件,呀比,这可怎么办?没有任何提示,发 现题目中也没有提示(so暴力破解也是不可能了),没办法就只好回头了,点开图片详细信息,发现里面有神

킨 ada.jpg 属性

7	常规 安全	详细信息 以前的版本
	属性 版权	值 ^
	图像 ———	
	图像 ID	
	分辨率	826 x 672
	宽度	826 像素
	高度	672 像素
	水平分辨率	96 dpi
	垂直分辨率	96 dpi
	位深度	24
	压缩	
	分辨率单位	
	颜色表示	
	昭相和	·
	照相机制造态	
		7264656072625522202120
	照相机空亏	/3040E09/3033F323U3138
	光闼但	
答	曝光时间	
1. 1	I ICA italia	

这不是base16嘛,解密后发现啊呀,好有规律的数字

```
sdnisc_2018
```

就这样得到了解压密码,打开后发现了flag flag{3XiF_iNf0rM@ti0n}

9.**basic**

打开后我们会发现是一个txt文件,打开后发现是一组组图像点,很容易就会想到python像素问题,讲到这里就 要敲敲小黑板了:好好学**python** 这里直接用**python**跑下 代码如下:

```
# coding=utf-8
from PIL import Image
import re
pic = Image.new("RGB",(150,900))
f = open('C:/Users/Y/Desktop/网安/0/basic.txt','r')
imlist = []
for i in f.readlines():
    i = re.sub('[( )\n]', '', i)
    imlist.append(i)
    i=0
    for x in range(0,150):
       for y in range(0,900):
            s = imlist[i].split(',')
            pic.putpixel([x, y], (int(s[0]), int(s[1]), int(s[2])))
            i += 1
            print(135000 - i)
            pic.show()
            pic.save("flag.png")
```

flag{RGB ZГ I 645

10.进制转换 这个题的话肯定还是代码直接跑吧,没发现什么辅助工具

```
import binascii
```

text = "d87 x65 x6c x63 o157 d109 o145 b100000 d116 b1101111 o40 x6b b1100101 b1101100 o141 d105 x62 d101 b
solution = ''
text2 = text.split(' ')
for x in text2:
 print(x)
 if x[0] == 'b': #binary
 solution += chr(int(x[1:],2))
 elif x[0] == 'x': # hexadecimal
 solution += x[1:].decode("hex")
 elif x[0] == 'd': # decimal
 solution += chr(int(x[1:]))
 elif x[0] =='o': # octal
 solution += chr(int(x[1:],8))

print(solution)

跑完就会在末尾找到flag

101110
20
1001000
97
18
105
*** 70
50 07
7/
40
103
11
111
54
32
164
1101001
64
145
7e
elcome to kelaibei. Give you a flag as a gift. flag{1e4bf81a6394de5abc005ac6 b3Fba287b iloc HaveAbga2d/Aim Myvin /22/22/6
Finished in 0.65]

Crypto

1.培根

培根烤肉可还行,直接打开找到aabaaaaaabaabbaaaabaabaaaaaaaaaaabaabbbaabbab 明显的培根啊,打开http://ctf.ssleye.com/baconian.html 直接破解

Baconian Cipher

.

aabaaaaaabaabbaaaabaabaaaaaaaaabaabbbaabbab

https://blog.csdn.net/weixin_43848306

2.Base64

直接打开辅助网站http://www.ssleye.com/,直接解码

flag{base_64_32_16}

3.Caesar来啦

凯撒密码了解下(其实就是一个偏移)

会得到skctf{veni_vidi_vici.}

4.栅栏里的爱

栅栏密码了解下,解码后会得到

flag{jursytp_taon}_old_c

5.base一家

base一家嘛,那肯定有64、32、16啦,首先观察得到的字符是64的,那就肯定先64,解完发现是32的再解就是 16,最后得到了flag

flag{fl4g_1_B4se_i3_V3ry_9ood}

6.仿射密码

放射密码的话可以了解下工具http://ctf.ssleye.com/affine.html

们别名响				
Affine Cipher				
vtusdjdgulyjudgh				
				1
14	7		2014年ま(Demous Dunstruction)	
п	-1		参称你不 (Remove Punctuation)	
	to sta	47 ats		
	<u>лн с</u>	— <i>I</i> IFF 124		
mathisintersting				

mathisintersting,最后再加上flag{}。

7.RivestShamirAdleman

下载 页	え后就 [。] 共享	会) E	压缩包,解压后会发现三个文件 查看		~ (
\uparrow		用	户 〉 Y 〉 桌面 〉 0 〉 fujian	✓ ひ 搜索"fujian"	م		
	*	^		修改日期	类型		
			encrypted.message1	2017/6/7 12:48	MESSAGE1 文件		
			🗋 encrypted.message2	2017/6/7 12:48	MESSAGE2 文件		
'es			encrypted.message3	2017/6/7 12:48	MESSAGE3 文件		
			Dublic.key	2017/6/7 11:08	KEY 文件		
ve -	Persc						
盘							

https://blog.csdn.net/weixin_43848306

看到是这个,就肯定得打开kali linux的openssl

Public-Key: (256 bit) Modulus: 00:d9:9e:95:22:96:a6:d9:60:df:c2:50:4a:ba:54: 5b:94:42:d6:0a:7b:9e:93:0a:ff:45:1c:78:ec:55: d5:55:eb Exponent: 65537 (0x10001) Modulus=D99E952296A6D960DFC2504ABA545B9442D60A7B9E930AFF451C78EC55D555EB writing RSA key -----BEGIN PUBLIC KEY-----MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhANmelSKWptlg38JQSrpUW5RC1gp7npMK /0Uce0xV1VXrAgMBAAE= https://blog.csdn.net/weixin_43848306 -----END PUBLIC KEY-----

然后就看到e是Exponentialent的值,将Modulus转成10进制就得到n=,接着将n因式分解得到p、q。(此过程可以自己编程实现或者引用一下工具http://www.atool.org/quality_factor.php);然后将得到的m,n,接着用python 跑一下

#coding:utf-8 import gmpy import rsa p = 302825536744096741518546212761194311477q = 325045504186436346209877301320131277983 n = 98432079271513130981267919056149161631892822707167177858831841699521774310891e = 65537 d = int(gmpy.invert(e , (p-1) * (q-1))) privatekey = rsa.PrivateKey(n , e , d , p , q) #根据已知参数,计算私钥 with open("encrypted.message1" , "rb") as f: print(rsa.decrypt(f.read(), privatekey).decode()) #使用私钥对密文进行解密,并打印 with open("encrypted.message2" , "rb") as f: print(rsa.decrypt(f.read(), privatekey).decode()) #使用私钥对密文进行解密,并打印 with open("encrypted.message3" , "rb") as f: #使用私钥对密文进行解密,并打印 print(rsa.decrypt(f.read(), privatekey).decode())

得出flag



Web

1.你能看见flag吗

那可不肯定能看见啊,不过需要小技巧,这个不就是在眼皮下面吗,首先我们查看下源代码,按下**F12**,调出开 发人员工具,就能看到了

		•							~
DOM 资源管理器	控制台	调试程序	网络 🖻	性能	内存	₹	⊑ 17 ▼ 11	▶ ?	۹.

				查找	(Ctrl+F)	
itml>		样式	已计算	布局	事件	更改
<head></head> <body windowc_onresizez="true"> 你你美国口口口口口口口口口口口口口口口口口口口口口口口口口口口口口口口口口口口</body>		⊿内联样	式 {			a:
小和名加于1ag+日; flag{this is comment}		}				
'html>						
flag{this_is_comment}						
2.GET						
只需要在地址栏输入?get=flag即可						
~く > C 合 ◎ http://47.105.148.65:49189/?get=flag						
🞖 收藏 🗸 📮 手机收藏夹 🗅 课程成绩 🔥 首页 - 园 📴 Track 安 🚾 HTML 🕿	⊗ CodePe	en 🝎 【极客	学 🗋 【i春秋	CTF	中常 🗋 代码	在线 🖬 账号管
_GET['get']; echo \$get; if(\$get == 'flag') echo 'flag{***************	·}'; flag{is	s_get_request	_23333}			

https://blog.csdn.net/weixin 43848306

3.POST

这个只是考察对hackbar的使用,在hackbar里输入post=flag就能得到flag了

47.105.148.65:49190/	× +	- 🗆 X
$\left(\boldsymbol{\leftarrow} ightarrow \boldsymbol{C} \boldsymbol{\hat{\omega}} $	 ④ 47.105.148.65:49190 圖 ··· ☆ 	III\ 🗓 🛱 🦘 🌐 🗾 📀 🗏
📄 火狐官方站点 🗘 最常访问 📄 >	《狐官方站点 🔞 新手上路 🗘 最常访问 📄 常用网址 🞵 京东商城 💹 淘宝12.12 💮 天猫 💮 淘宝 💮 天猫双11	■ 移动版书签
⑦ 您的火狐主页已被篡改,需要立即	灰复。	是(<u>R</u>) 否(<u>N</u>) 不再提示(<u>D</u>) X
<pre>\$post=\$_POST['post']; echo</pre>	<pre>\$post; if(\$post == 'flag') echo 'flag{************************************</pre>	
日本 古香器 日 控制台 日 う	職業 職業 職業 職業 職業 職業 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	⊡ ··· ×
Encryption - Encoding - C	ther -	HackBar v1
Load URL http://47.105.14	8.65:49190/	
● Execute Post data □	Referrer 🗌 User Agent 🔲 Cookies	

Post	Data

https://blog.csdn.net/weixin_43848306

走(広) 一つ(山) 小舟旋小(山)

4.找一找flag

我的做法是直接给他禁止创建更多页面,打开源码就直接找到了类似flag的东西



这个题只是需要更改下地址,从本地访问就行

Please access the server from the local

							_			
	□ 查看器	□ 控制台 (⊃ 调试器 { } #	样式编辑器	◎ 性能	🕸 内存 🗦 网络	8 存储	↑ 无障碍环	境	HackBar
Ŵ	♡ 过滤 UF	RL					II 所	所有 HTML	CSS	SS JS XHR 字体 图像 媒体 WS 其他 □ 持续日志 □ 禁用缓存 不节流 :
状	초	方法文化	域名	触发	类型	传输	大小	0 室秒	10.2	0.2 🖸 消息头 Cookie 参数 响应 耗时 堆栈跟踪
200	GET	index	🔏 119.23.8.18.	document	html	413 字节	181 字节	→ 141 ms		▽预览
404	GET	favico	🔏 119.23.8.18.	img	html	503 字节	288 字节	→ 50 ms		flag{JUST REMOTE ADDR is S4fy}
200	GET	index	💋 119.23.8.18.	other	html	406 字节	133 字节			
										▼响应载荷 (payload)
										1 <html></html>
										2 <head> 3 <meta charset="utf-8"/></head>
										<pre>4 <title>Where are you from</title> 5</pre>
										6
										7 (body) 8 flog(TUST REMOTE ADDR is SAfe() (body)
										9
Q	3 个请求	已传输 602 字节	/ 1.29 KB 完成	35.60 秒	DOMCon	tentLoaded: 109 毫種	🤌 🕴 load: 127	毫秒		10 https://blog.csdn.net/weixin_4384830

6.这个题目应该是挺清楚的打开源代码后,发现需要输出a,(可以在控制台直接写a或者在那里执行js代码)就可以得到上交的密码

听说浏览器的控制台可以执行JavaScri

submit

flag{860811cce93639b9701db88dd06183e5}

Elements	Console Sour	ces Network	Performance	Memory	Application	Security	Audits
🕩 🛇 top	• •	Filter				Default leve	els 🔻
> print(a)							
v undefined							
> a							
< 2087267							

https://blog.csdn.net/weixin_43848306

转载于:https://www.cnblogs.com/ftc7/p/10731542.html