




CTF_MISC(习题)

原创

若比邻666  于 2021-12-13 22:57:10 发布  2373  收藏

分类专栏: [CTF_MISC](#) 文章标签: [安全 misc](#)

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/weixin_40614261/article/details/121916292

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

```
U3RlZ2Fub2dyYXBoeSBpcyB0aGUgYXJ0IGFuZCBzY2llbmNlIG9m
IHdyaXRpbmcgaGlkZGVuIG1lc3NhZ2VzIGlHNDY2ggYSB3YXkgdGhhdCBubyBvbmV=
LCBhcGFydCBmcm9tIHRoZSBzZW5kZXIgaW5kIGludGVuZGVkIHJlY2lwaWVudCwgc3VzcGU=
Y3RzIHRoZSBleGlzdGVuY2Ugb2YgdGhllIG1lc3M=
YWdlLCBhIGZvcml0b2Ygc2VjdXJpdHkgdGhyb3VnaCBvYnNjdXJpdHkuIFS=
aGUgd29yZCBzdGVnYW5vZ3JhcGh5IGlZlG9mlEdyZWVrIG9yaWdpbiBhbmQgbWVhbnMgImNvbmNIYW==
bGVkIHdyaXRpbmciIGZyb20gdGhllEdyZWVrIHdvcml0b2Y2ZGVuZGVkIHJlY2lwaWVudCwgc3VzcGU=
dmVyZWQgb3JlcHJvdGVjdGVkIiwgYW5kIGdyYXBoZWluIG1YW5pbmcgInRvIHc=
cm10ZSltIFRoZSBmaXJzdCBzZWVudGVuZGVkIGlHNDY2ggYSB3YXkgdGhhdCBubyBvbmV=
YW5uZXMgaW5kIGdyYXBoeSBpcyB0aGUgYXJ0IGFuZCBzY2llbmNlIG9m
dGlzZSBvbiBjcnlwdG9ncmFwaHkgYW5kIGlHNDY2ZGVuZGVkIHJlY2lwaWVudCwgc3VzcGU=
dWlzZWQgYXJ0IGFuZGVuZGVkIHJlY2lwaWVudCwgc3VzcGU=
YWdlcyB3aWxsIGFwcGVhcnR0byBiZSBzZW5kIGlHNDY2ZGVuZGVkIHJlY2lwaWVudCwgc3VzcGU=
Y2xlcwgc2hvcHBpbmcbG9ncmFwaHkgYW5kIGlHNDY2ZGVuZGVkIHJlY2lwaWVudCwgc3VzcGU=
```

CSDN @若比邻666

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						T						Q									
90						84						81									
0	1	0	1	1	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0
22						37						17									
W						I						R									

CSDN @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	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0
19						7						28									
T						H						c									

CSDN @若比邻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。

```

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
|<-

```

CSDN @若比邻666

aa=@eval.

```

(base64_decode($_POST[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwuMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ21jX3F1b3Rlc19ydW50aW1lKDAP
02Vj0C80Tj0%2Bf0T0000kZ7d1iVXNlNjBfZ0V0b0RlK0RfU0V0T0V0f00f0Y0kZ70M07500T1

```

0zVjag80110%2BtC1p0ZSKZJ11YXN1NJKTZGVJ0ZK1KCRTOE9IVFS1EJE1XSK7JGM9JF9Q11
NUWyJ6MiJdOyRjPXN0cl9yZXBsYWw1KCJcciIsIiIsJGMpOyRjPXN0cl9yZXBsYWw1KCJcbi
IsIiIsJGMpOyRidWY9IiI7Zm9yKCRpPTA7JGk8c3RybGVuKCRjKTskaSs9MikkYnVmLj11cm
xkZWNvZGUoIiUiLnN1YnN0cigkYywkaSwyKSk7ZWNobyhAZndyaXRlKGZvcGVuKCRmLCJ3Ii
ksJGJ1Zik%2FIjEiOiIwIik702VjaG8oInw8LSIp02RpZSgpOw%3D%3D&z1=RDpcd2FtcDY0
XHd3d1x1cGxvYWRCNjY2Ni5qcGc%3D&z2=FFD8FFE000104A464946000101010078007800
00FFDB00430001
01FFDB
004301
01FFC0001108
013001E202012200021101021101E5C4001E0000010501010101010100000000000000000000

CSDN @若比邻666

1B407A4920E0FF170E0B5118751C7CD8D870126A758D780F2040FFA0B2078C1E49E5040
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

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	78JFIF.....x
00000010		00	78	00	00	FF	DB	00	43	00	01	01	01	01	01	01	01	.x.....C.....
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



三、bugku_misc:http://ctf.bugku.com/challenges/detail/id/310.html

名称	修改日期
你明白吗?	2021/6/9 14:46

1. zip文件，解压后得到
2. 放入TTheEdit，发现是jpg格式，于是修改后缀

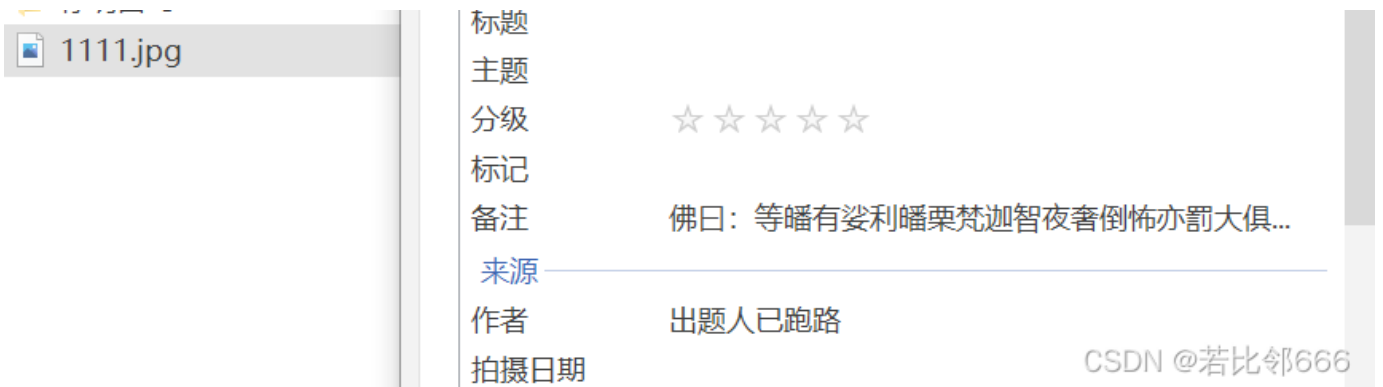
```
你明白吗?  
OFFSET H 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F ASCII  
00000000 FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60 .....JFIF.....`  
00000010 00 60 00 00 FF E1 11 3C 45 78 69 66 00 00 4D 4D ..<Exif..MM
```



- 3.
- 4. foremost后得到zip, 需要密码



- 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



- 6. 解压密码如图



- 7. 得到zip文件, 需要密码解压, passwd.txt有提示



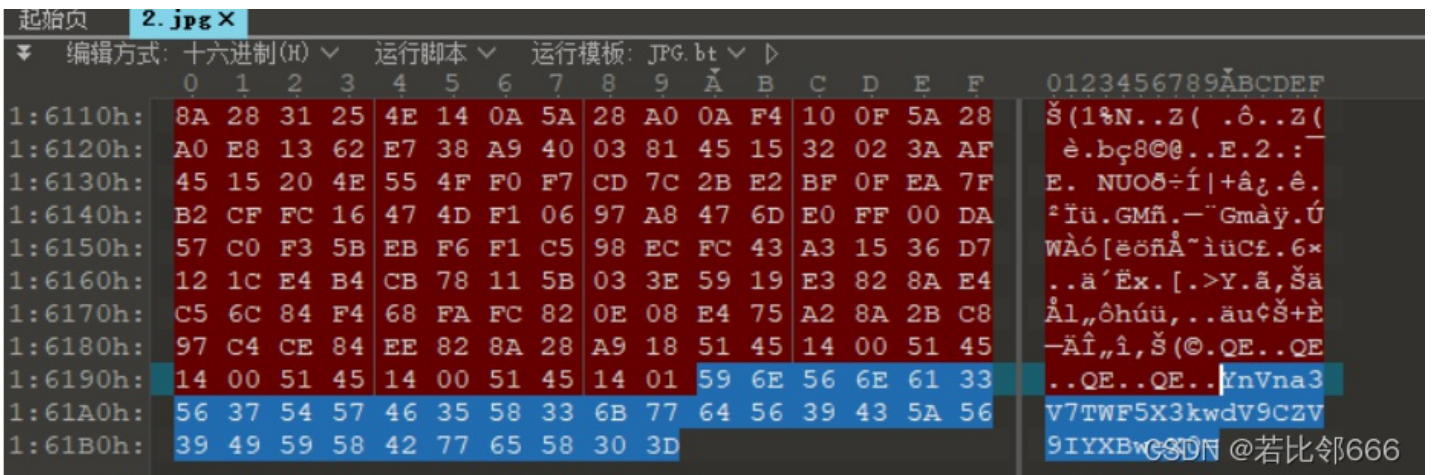
40 5
42 7
44 9

tip:

###你听过《青花》吗?###
#####

CSDN @若比邻666

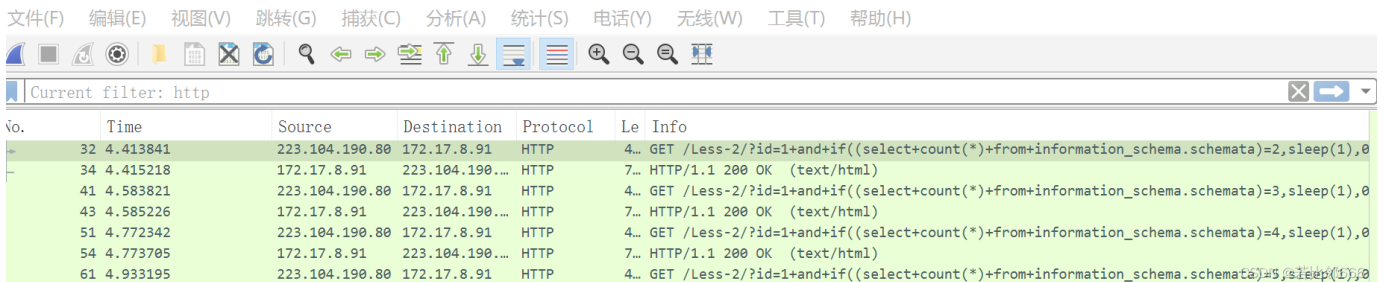
- 8. 按照歌词每一行每一列，依次得到密码 三勿爱温蒙惚心信承失记愈的逢过濡善着记回寞神梦
- 9. 解压后得到图片，仿佛010中，发现最后有base64密码，解密后得到flag



bugku{May_y0u_Be_Happy}

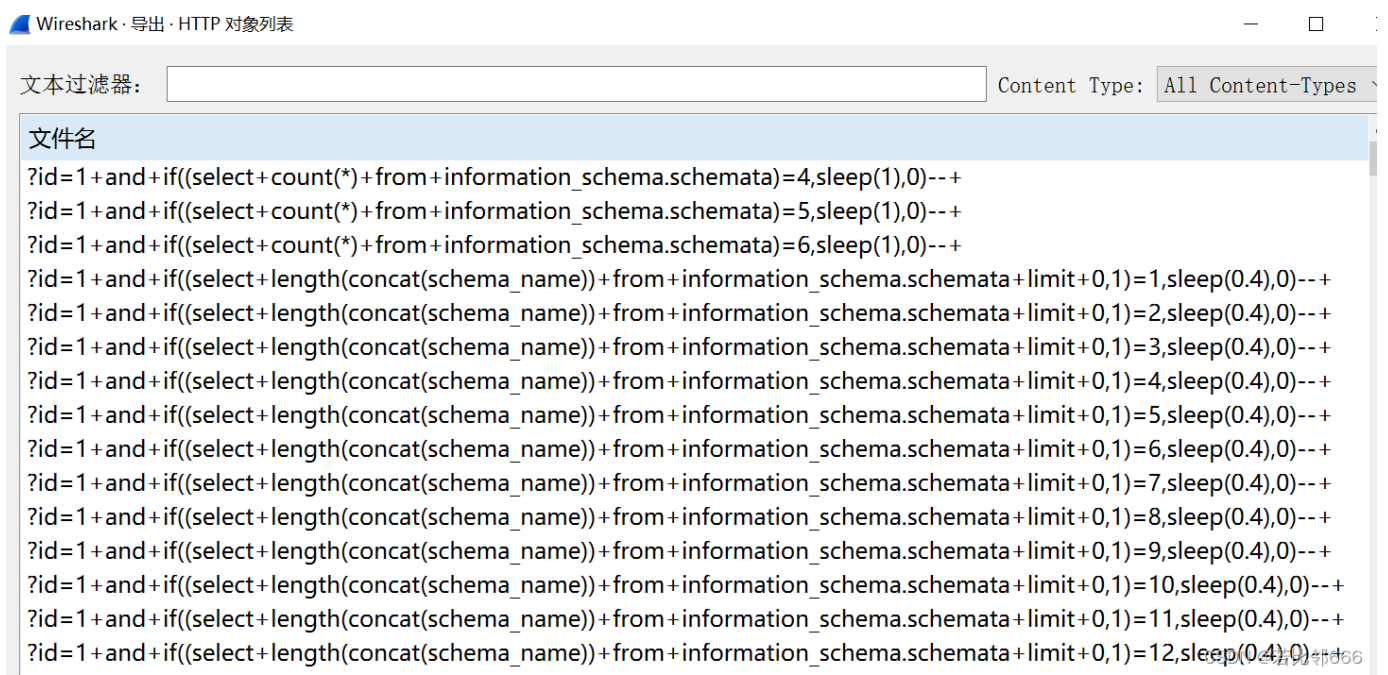
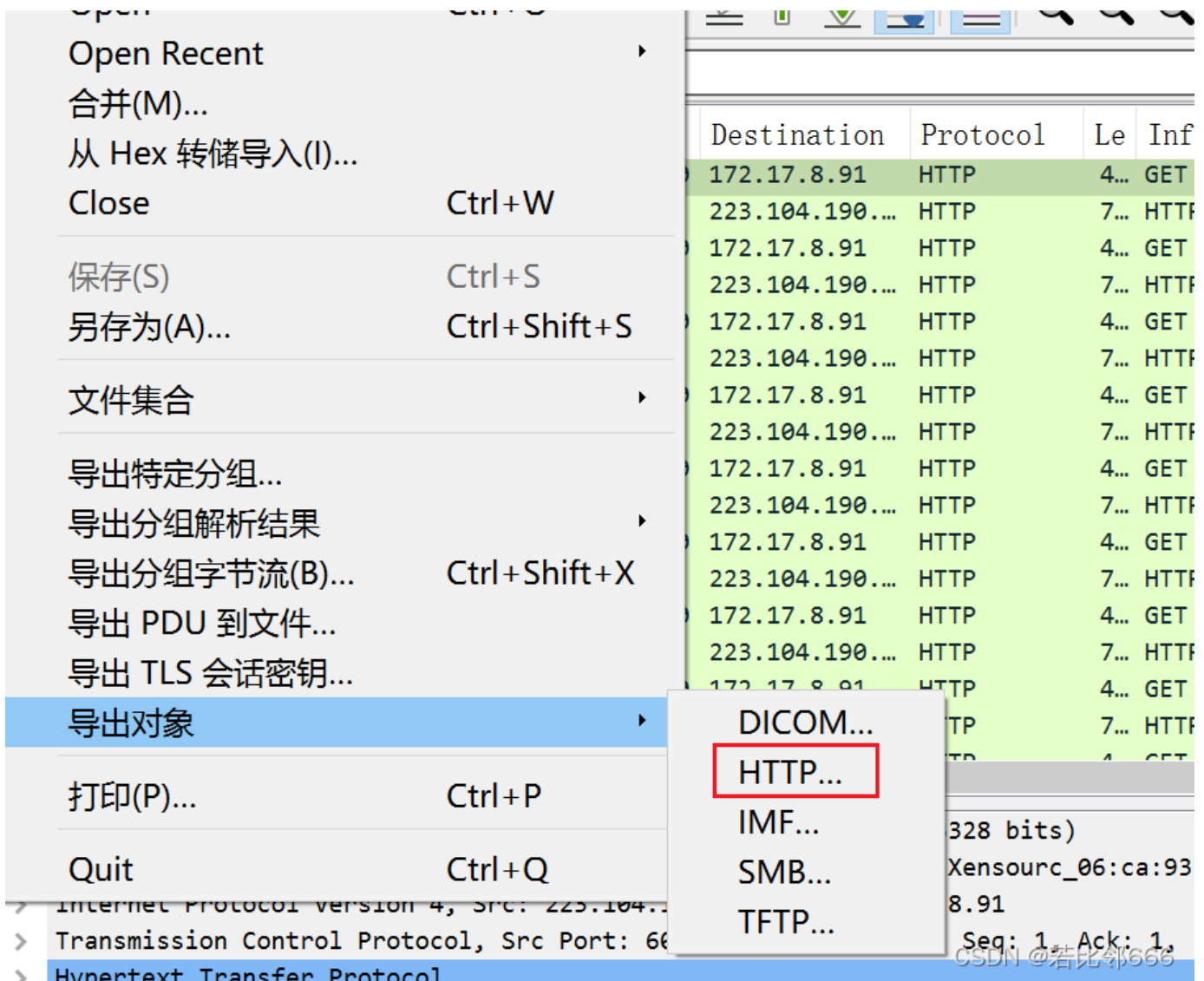
四、bugku_blind_injection2:http://ctf.bugku.com/challenges/detail/id/212.html

- 1. 下载附件，pcap文件，题目提示盲注



- 2. 导出http对象





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%201,13,1)%20%3E%2096,sleep(0.4),0)--+
(select%20schema_name%20from%20information_schema.schemata%20limit%201,13,1)%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%3E%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%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%2044,sleep(0.4),0)--+
(select%20schema_name%20from%20information_schema.schemata%20limit%202,1,14,1))%20%3E%2044,sleep(0.4),0)--+
(select%20schema_name%20from%20information_schema.schemata%20limit%202,1,14,1))%20%3C%2050,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,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%201,1),1,1))%20=%2099,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%201,1),2,1))%20=%20104,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%201,1),3,1))%20=%2097,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%201,1),4,1))%20=%20108,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%201,1),5,1))%20=%20108,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%201,1),6,1))%20=%20101,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%201,1),7,1))%20=%20110,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%201,1),8,1))%20=%20103,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%201,1),9,1))%20=%20101,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%201,1),10,1))%20=%20115,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%202,1),1,1))%20=%20102,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%202,1),2,1))%20=%20108,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%202,1),3,1))%20=%2097,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%202,1),4,1))%20=%20103,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%202,1),5,1))%20=%2095,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%202,1),6,1))%20=%2056,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%202,1),7,1))%20=%2097,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%202,1),8,1))%20=%20102,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%202,1),9,1))%20=%2056,sleep(0.4),0)--+
0 bytes	?id=1+and+if(ascii(substr((select%20schema_name%20from%20information_schema.schemata%20limit%202,1),10,1))%20=%20101,sleep(0.4),0)--+

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)
```