2018ustcCTF部分题目wp

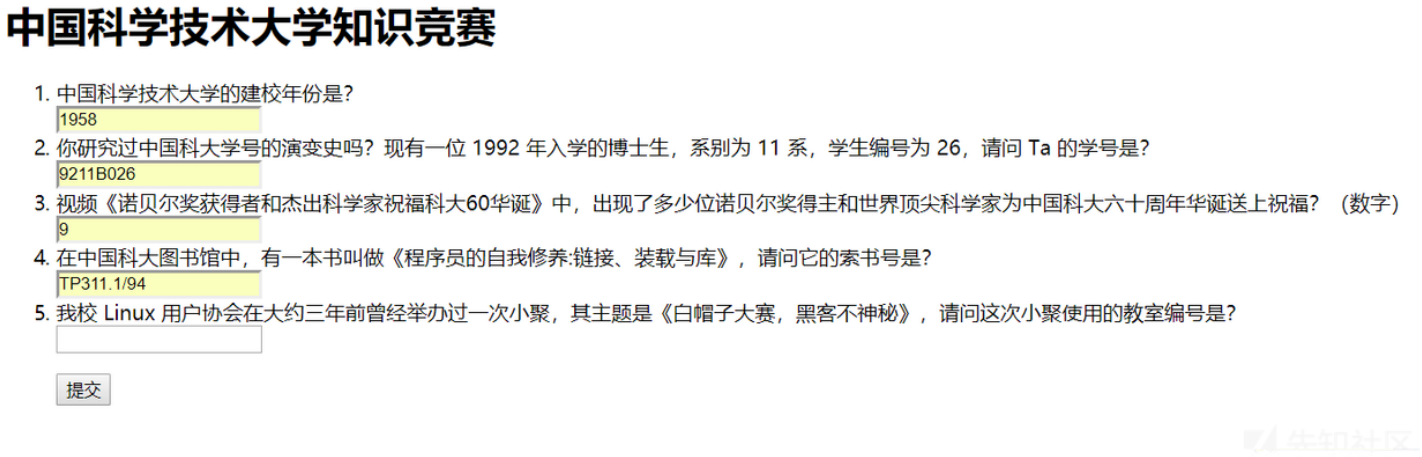
Bling1Dog / 2018-10-25 08:02:00 / 浏览数 3237 安全技术 CTF 顶(0) 踩(0)

签到题

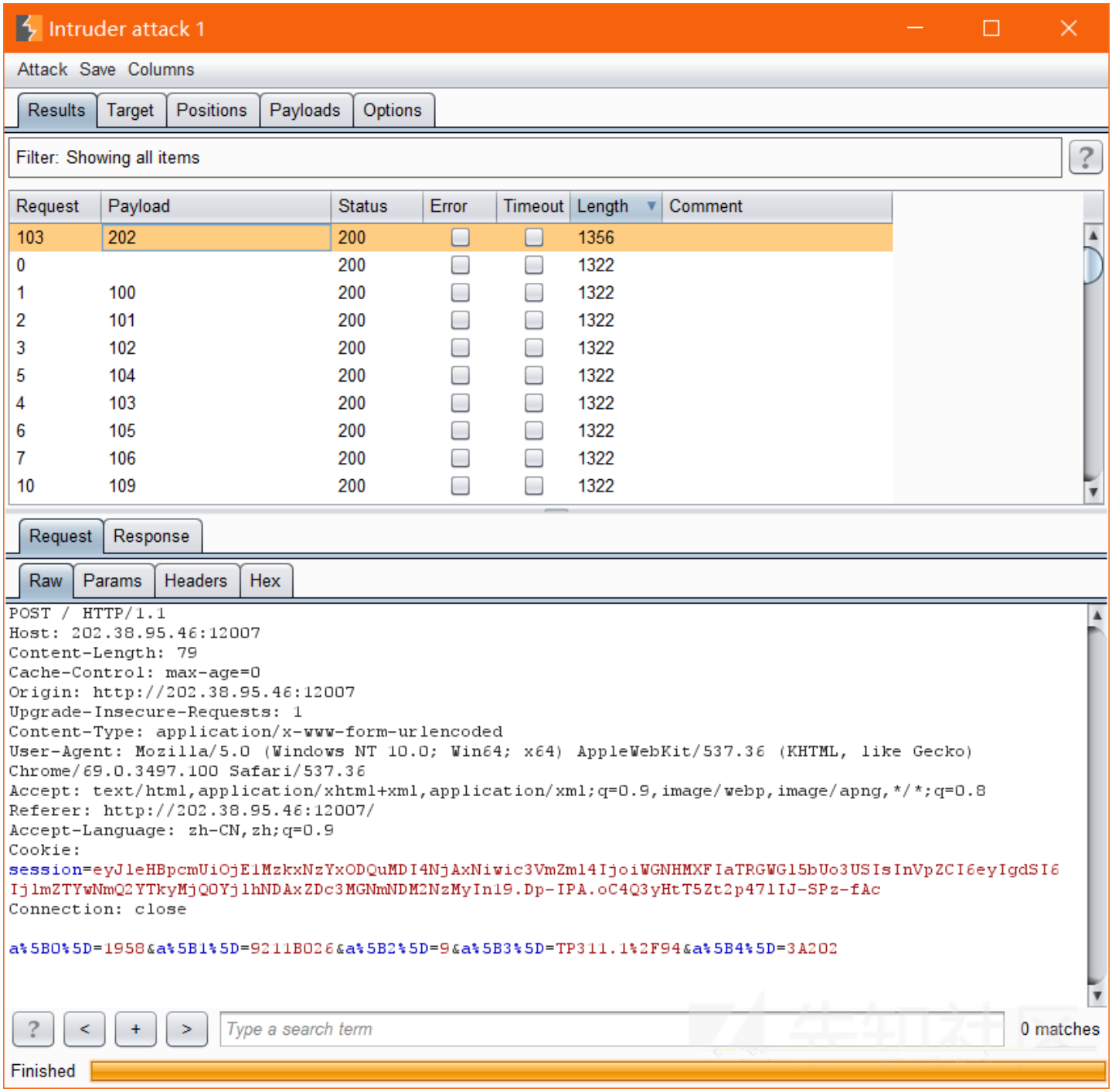
题目非常基础，chrome浏览器，F12打开控制台，将页面源码中的 maxlength 改为14即可完整输入hackergame2018，提交得到flag

猫咪问答

这道题前四个空都是可以Google出来的，第五个空因为无法查到具体教室，所以需要burpsuite进行爆破。



爆破的时候，找到了中科大官网上的查询教室网站教室网站链接
然后最终发现是西区三教的教室。



最终得到教室编号3A202，得到flag

中国科学技术大学知识竞赛

答对了 5 道题

flag{G00G1E-is-always-YOUR-FRIEND}

1. 中国科学技术大学的建校年份是?
2. 你研究过中国科大学号的演变史吗？现有一位 1992 年入学的博士生，系别为 11 系，学生编号为 26，请问 Ta 的学号是?
3. 视频《诺贝尔奖获得者和杰出科学家祝福科大60华诞》中，出现了多少位诺贝尔奖得主和世界顶尖科学家为中国科大六十周年华诞送上祝福？（数字）
4. 在中国科大图书馆中，有一本书叫做《程序员的自我修养:链接、装载与库》，请问它的索书号是?
5. 我校 Linux 用户协会在大约三年前曾经举办过一次小聚，其主题是《白帽子大赛，黑客不神秘》，请问这次小聚使用的教室编号是?

提交

游园会的集章卡片

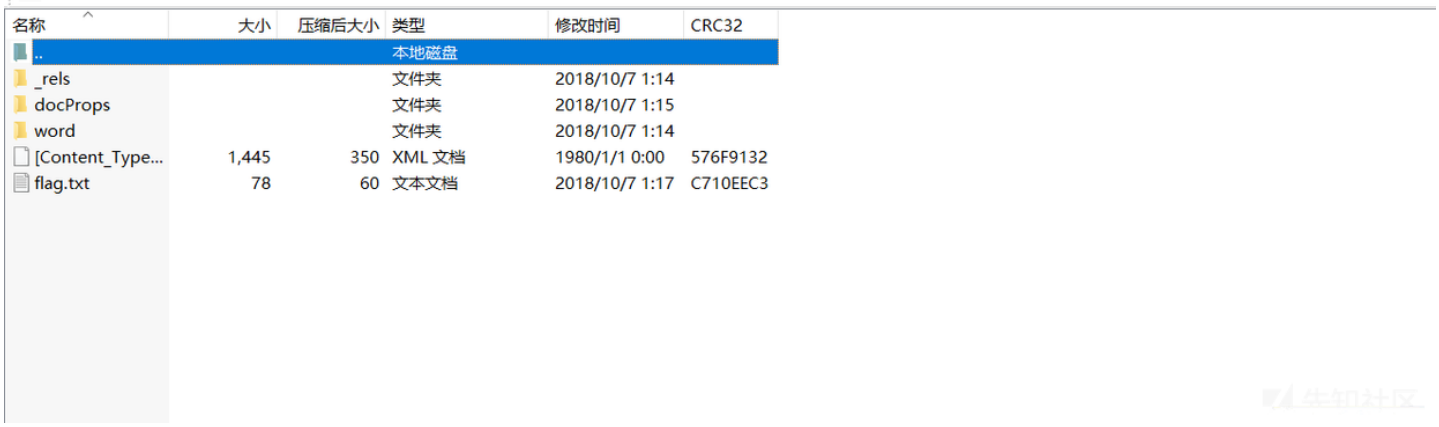
本题比较简单，下载题目压缩包，然后按照中科大给的标识，将图片拼起来即可(滑稽脸)

Word文档

本题为Misc基础题，直接winhex打开下载下来的word文档，查看文件的开头和结尾格式，发现是zip文件开头(50 4B 03 04)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
50	4B	03	04	14	00	00	00	08	00	00	00	21	00	32	91	PK ! 2'
6F	57	5E	01	00	00	A5	05	00	00	13	00	1C	00	5B	43	oW^ ¥ [C
6F	6E	74	65	6E	74	5F	54	79	70	65	73	5D	2E	78	6D	ontent_Types].xm
6C	55	54	09	00	03	80	35	CE	12	6B	EE	B8	5B	75	78	lUT €5Î kî¸[ux
0B	00	01	04	F5	01	00	00	04	14	00	00	00	B5	94	CB	õ µ"Ë
6A	C3	30	10	45	F7	85	FE	83	D1	36	D8	4A	BA	28	A5	jÃ0 E÷…þƒÑ6ØJº(¥
C4	C9	A2	8F	65	1B	68	FA	01	8A	34	4E	44	F5	42	9A	ÄÉ¢ e hú Š4NDõBš
BC	FE	BE	E3	38	35	A5	A4	31	E4	B1	31	C8	33	F7	DE	¼þ¾ã85¥¤1ä±1È3÷Þ
33	42	CC	70	BC	B1	26	5B	41	4C	DA	BB	92	0D	8A	3E	3BÌp¼±&[ALÚ»' Š>
CB	C0	49	AF	B4	9B	97	EC	73	FA	9A	3F	B0	2C	A1	70	ËÀI¯´›—ìsúš?°,¡p
4A	18	EF	A0	64	5B	48	6C	3C	BA	BD	19	4E	B7	01	52	J ï d[Hl<º½ N· R
46	6A	97	4A	B6	40	0C	8F	9C	27	B9	00	2B	52	E1	03	Fj—J¶@ œ'¹ +Rá
38	AA	54	3E	5A	81	74	8C	73	1E	84	FC	12	73	E0	77	8ªT>Z tŒs „ü sàw
FD	FE	3D	97	DE	21	38	CC	B1	F6	60	A3	E1	33	54	62	ýþ=—Þ!8Ì±ö`£á3Tb
69	30	7B	D9	D0	EF	86	24	82	49	2C	7B	6A	1A	EB	AC	i0{ÙÐï†$,I,{j ë¬
92	89	10	8C	96	02	A9	CE	57	4E	FD	49	C9	F7	09	05	'‰ Œ— ©ÎWNýIÉ÷
29	77	3D	69	A1	43	EA	51	03	E3	07	13	EA	CA	FF	01	)w=i¡CêQ ã êÊÿ
7B	DD	3B	5D	4D	D4	0A	B2	89	88	F8	26	2C	75	F1	B5	{Ý;]MÔ ²‰ˆø&,uñµ
8F	8A	2B	2F	97	96	94	C5	71	9B	03	9C	BE	AA	B4	84	Š+/—–”Åq› œ¾ª´„
56	5F	BB	85	E8	25	A4	44	77	6E	4D	D1	56	AC	D0	AE	V_»…è%¤DwnMÑV¬Ð®
D7	C5	E1	96	76	06	91	94	97	07	69	AD	3B	21	12	6E	×Åá–v '"— i-;! n
0D	A4	CB	13	34	BE	DD	F1	80	48	82	6B	00	EC	9D	3B	¤Ë 4¾Ýñ€H‚k ì ;
11	D6	30	FB	B8	1A	C5	2F	F3	4E	90	8A	72	A7	62	66	Ö0û¸ Å/óN Šr§bf
E0	F2	18	AD	75	27	04	D2	1A	80	E6	3B	38	9B	63	67	àò -u' Ò €æ;8›cg
73	2C	92	3A	27	D1	87	44	6B	25	9E	30	F6	CF	DE	A8	s,':'Ñ‡Dk%ž0öÏÞ¨
D5	39	0D	1C	20	A2	3E	FE	EA	DA	44	B2	3E	7B	3E	A8	Õ9 ¢>þêÚD²>{>¨

然后解压文件，发现flag.txt，打开之后即为flag



名称	大小	压缩后大小	类型	修改时间	CRC32
..			本地磁盘		
_rels			文件夹	2018/10/7 1:14	
docProps			文件夹	2018/10/7 1:15	
word			文件夹	2018/10/7 1:14	
[Content_Type...	1,445	350	XML 文档	1980/1/1 0:00	576F9132
flag.txt	78	60	文本文档	2018/10/7 1:17	C710EEC3

猫咪银行

本题目感觉是非预期解
按照正常的格式输入的话，肯定无法在规定的时间内得到足够的钱。于是测试大数溢出。

货币兑换

货币种类	我的余额	兑换 CTB	兑换 RMX	兑换 TDSU
CTB	9	1	57	6606
RMX	0	1/57	1	115
TDSU	5606	1/6606	1/115	1

理财产品

A1: 存入 TDSU，每分钟获得 4.3% 利息，最少一分钟。

已买入

买入份额：1000 TDSU

预计收益：-9223372036854775808 TDSU

取出时间：2018-10-15 10:48:32 后

取出

购买商品

商品类型	价格	购买
FLAG	20 CTB	Buy
FLAG 碎片(1/4)	5 CTB	Buy

发现预计收益变成了负数，说明大数字可能是后台的算法出现溢出，当存入时间输入为555555555555555555(可为别的数字，这里只是我随机选取的)，发现取出时间变为

货币种类	我的余额	兑换 CTB	兑换 RMX	兑换 TDSU
CTB	9	1	57	6606
RMX	0	1/57	1	115
TDSU	5606	1/6606	1/115	1

理财产品

A1: 存入 TDSU，每分钟获得 4.3% 利息，最少一分钟。

已买入

买入份额：1000 TDSU

预计收益：5442144815179337728 TDSU

取出时间：-112816812929-06-17 13:22:08 后

取出

flag兑换

恭喜！

The flag is: `flag{Evil_Integer._Evil_Overflow.}`

每个账号仅有十分钟的有效期，初始为 10 CTB。

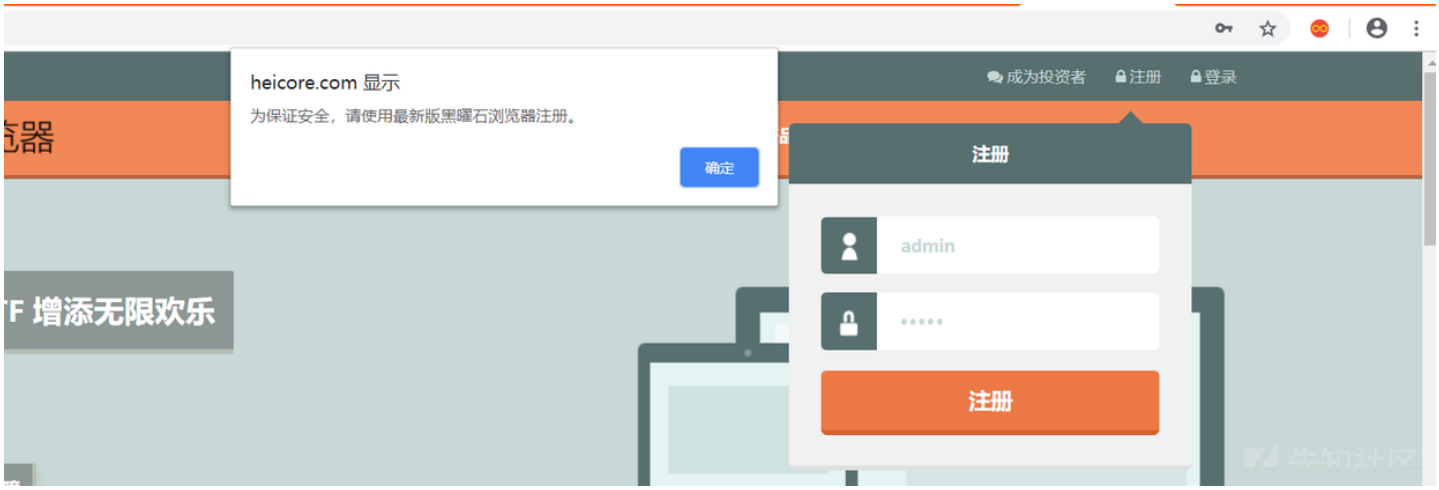
每个账号有三种货币：CTB，RMX，TDSU

货币兑换

货币种类	我的余额	兑换 CTB	兑换 RMX	兑换 TDSU
CTB	0	1	57	6606
RMX	0	1/57	1	115
TDSU	5442144815179271668	1/6606	1/115	1

黑曜石浏览器

本题有点坑，刚开始以为真的要用黑曜石浏览器打开网站，但是黑曜石浏览器下载不好，刚开始以为要绕过，后来发现自己想多了。
Google搜索到黑曜石浏览器，然后发现不能注册。

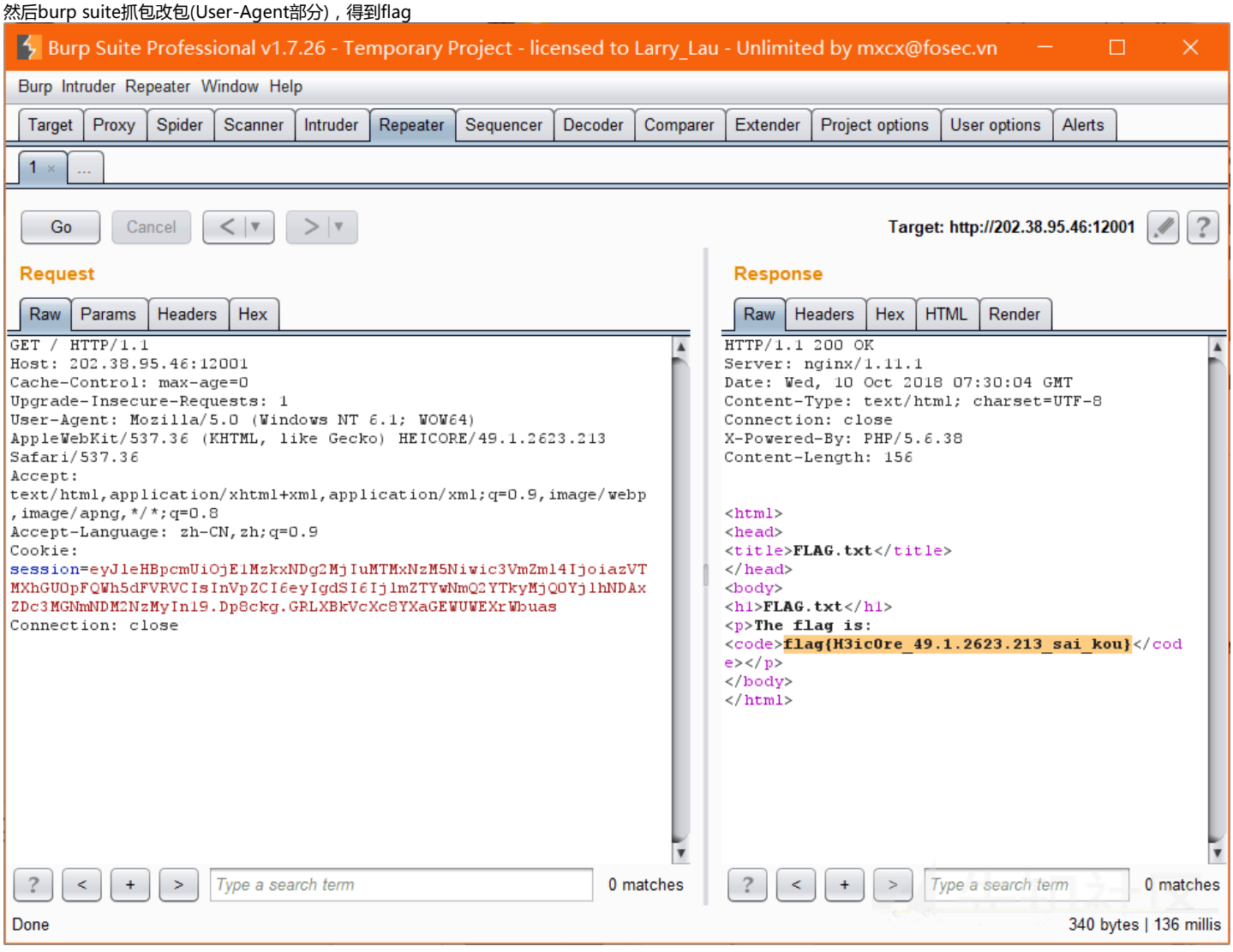


然后想到的是burpsuite修改浏览器标识，但是不知道具体的版本号，最终在黑曜石官网所谓官网查看源码，找到了版本号。

源码地址

```
            }
        });
    });
</script>
<script type="text/javascript">
    function isLatestHEICORE() {
        var ua = navigator.userAgent;
        var HEICORE_UA = "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) HEICORE/49.1.2623.213 Safari/537.36";
        return ua === HEICORE_UA;
    }
    // Login Form
    $(function () {
        var button = $('#loginButton');
        var box = $('#loginBox');
        var form = $('#loginForm');
        button.removeAttr('href');
        button.mouseup(function (login) {
            box.toggle();
```

然后burp suite抓包改包(User-Agent部分)，得到flag



回到过去

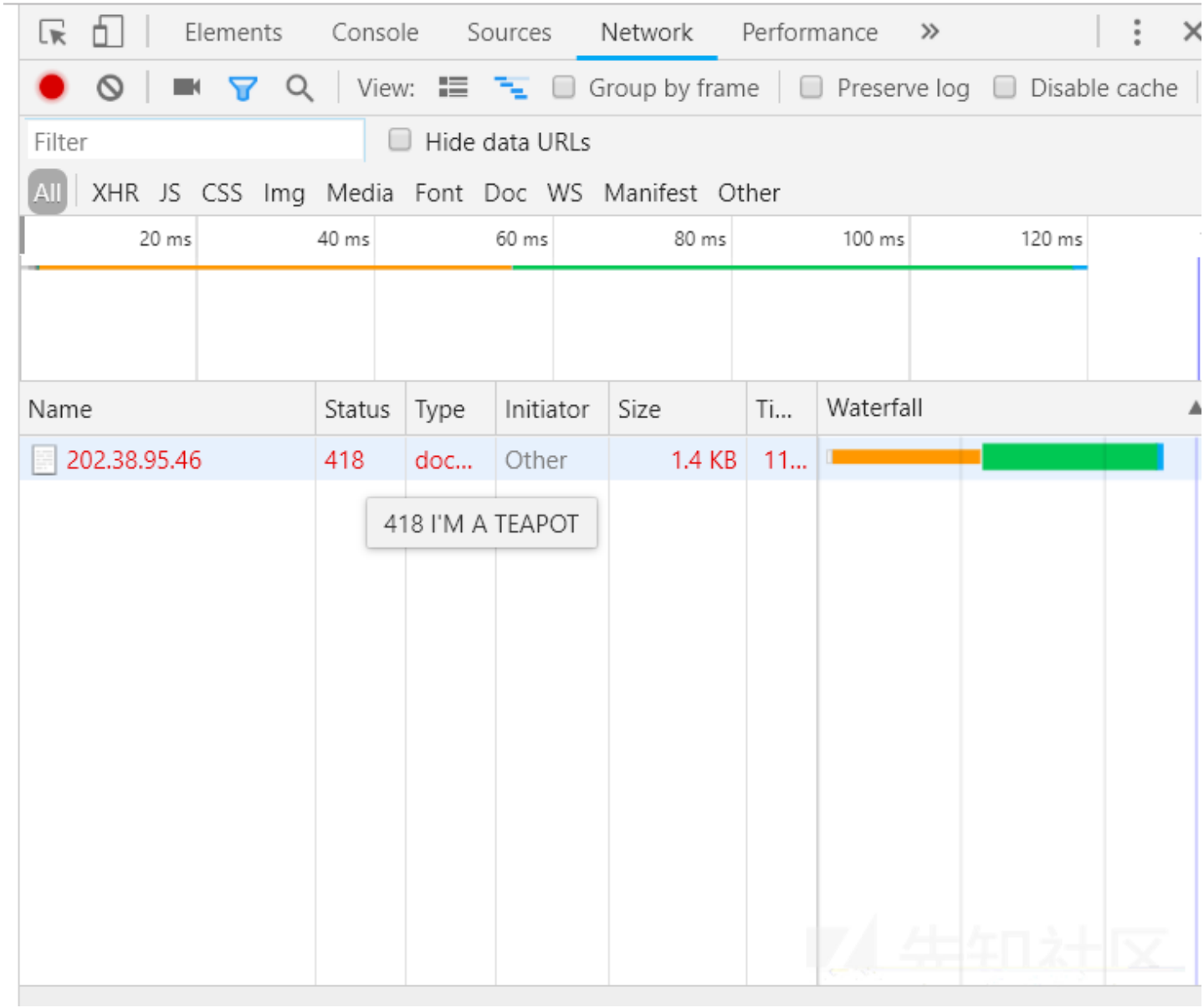
本题是一个Misc题目，没有难度，考了linux下的ed编辑器，本人之前也没用过，上网查找ed使用说明 linux系统输入之后，写入文件即可得到flag。

```
a
flag{
.
a
44a2b8
a3d9b2^[c
c44039
f93345
}
.
2m3
2m5
2m1
2
44a2b8
s/4/t
t4a2b8
w flag.txt
38
q
```

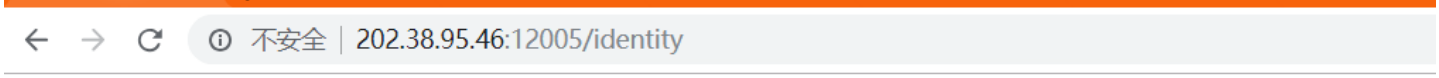

我是谁

哲学思考

这个题感觉脑洞比较大，之前卡了半天，然后朋友才告诉我，要看状态码.....



然后输入 taepot ，得到flag



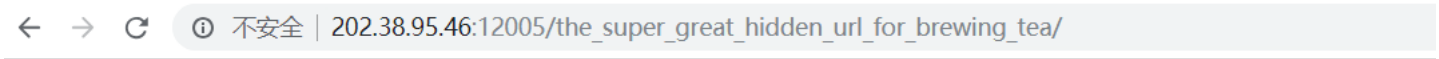
Yes, I finally realized that I am a teapot!

This is my gift for you:

flag{i_canN0t_BReW_c0ffEE!}

Come to This Link, help me brew some tea, and you can get the 2nd FLAG!

Can I help U?



Brewing tea is not so easy.

Try using other *methods* to request this page.

题目提示要换种方法请求页面，先burpsuite抓包，然后将本来的GET方法改为POST方法

```
POST /the_super_great_hidden_url_for_brewing_tea/ HTTP/1.1
Host: 202.38.95.46:12005
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,image/apng,*/*;q=0.8
Referer: http://202.38.95.46:12005/identity
Accept-Language: zh-CN,zh;q=0.9
Cookie:
session=eyJleHBpcmUiOjE1MzkxNzYxODQuMDI4NjAxNiwic3VmZml4IjoiWGNH
MXFIaTRGWG15bUo3USIsInVpZCI6eyIgdSI6IjlmZTYwNmQ2YTkyMjQ0YjlhNDAx
ZDc3MGNmNDM2NzMyIn19.Dp-IPA.oC4Q3yHtT5Zt2p471IJ-SPz-fAc;
PHPSESSID=b40888dfe05d80cdb85b7da361a9cff0
Connection: close
```

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 107
Server: Werkzeug/0.14.1 Python/3.6.6
Date: Mon, 15 Oct 2018 07:50:24 GMT


        <p>The method "POST" is deprecated.</p>
        <p>See RFC-7168 for more information.</p>
```

然后页面提示要看一个RFC-7168的东西，然后搜索找到它。https://www.rfc-editor.org/rfc/rfc7168.txt

2.1. BREW and POST Methods

Control of a TEA-capable pot is performed, as described in the base HTCPCP specification, through the sending of BREW requests. POST requests are treated equivalently, but they remain deprecated. Tea production differs from coffee, however, in that a choice of teas is often provided for client selection before the tea is brewed. To this end, a TEA-capable pot that receives a BREW message of content type "message/teapot" MUST respond in accordance with the URI requested, as below.

2.1.1. The "/" URI

For the URI "/", brewing will not commence. Instead, an Alternates header as defined in RFC 2295 [RFC2295] MUST be sent, with the available tea bags and/or leaf varieties as entries. An example of such a response is as follows:

```
Alternates: {"/darjeeling" {type message/teapot}},
            {"/earl-grey" {type message/teapot}},
            {"/peppermint" {type message/teapot}}
```

The following example demonstrates the possibility of interoperability of a TEA-capable pot that also complies with the base HTCPCP specification:

根据文档提示，应该是将POST方法改为BREW方法(虽然我开始也不知道是啥方法)，然后添加Content-Type: message/coffeepot

```
BREW /the_super_great_hidden_url_for_brewing_tea/ HTTP/1.1
Host: 202.38.95.46:12005
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,image/apng,*/*;q=0.8
Referer: http://202.38.95.46:12005/identity
Accept-Language: zh-CN,zh;q=0.9
Content-Type: message/coffeepot
Cookie:
session=eyJleHBpcmUiOjE1MzkxNzYxODQuMDI4NjAxNiwic3VmZml4IjoiWGNH
MXFIaTRGWGl5bUo3USIsInVpZCI6eyIgdSI6IjlmZTYwNmQ2YTkyMjQ0YjlhNDAx
ZDc3MGNmNDM2NzMyIn19.Dp-IPA.oC4Q3yHtT5Zt2p47lIJ-SPz-fAc;
PHPSESSID=b40888dfe05d80cdb85b7da361a9cff0
Connection: close
```

```
HTTP/1.0 418 I'M A TEAPOT
Content-Type: text/html; charset=utf-8
Content-Length: 75
Server: Werkzeug/0.14.1 Python/3.6.6
Date: Mon, 15 Oct 2018 08:30:52 GMT

        <p>Don't you remember what's in the 1st
FLAG?</p>
```

根据返回包提示，应该把coffeepot改为teapot，再GO一下

```
BREW /the_super_great_hidden_url_for_brewing_tea/ HTTP/1.1
Host: 202.38.95.46:12005
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,image/apng,*/*;q=0.8
Referer: http://202.38.95.46:12005/identity
Accept-Language: zh-CN,zh;q=0.9
Content-Type: message/teapot
Cookie:
session=eyJleHBpcmUiOjE1MzkxNzYxODQuMDI4NjAxNiwic3VmZml4IjoiWGNH
MXFIaTRGWGl5bUo3USIsInVpZCI6eyIgdSI6IjlmZTYwNmQ2YTkyMjQ0YjlhNDAx
ZDc3MGNmNDM2NzMyIn19.Dp-IPA.oC4Q3yHtT5Zt2p47lIJ-SPz-fAc;
PHPSESSID=b40888dfe05d80cdb85b7da361a9cff0
Connection: close
```

```
HTTP/1.0 300 MULTIPLE CHOICES
Content-Type: text/html; charset=utf-8
Content-Length: 19
Alternates:
{"/the_super_great_hidden_url_for_brewing_tea/black_tea
" {type message/teapot}}
Server: Werkzeug/0.14.1 Python/3.6.6
Date: Mon, 15 Oct 2018 08:32:37 GMT

Supported tea type:
```

发现返回包给了地址，然后将地址改为返回包的地址，GO一下，得到flag。

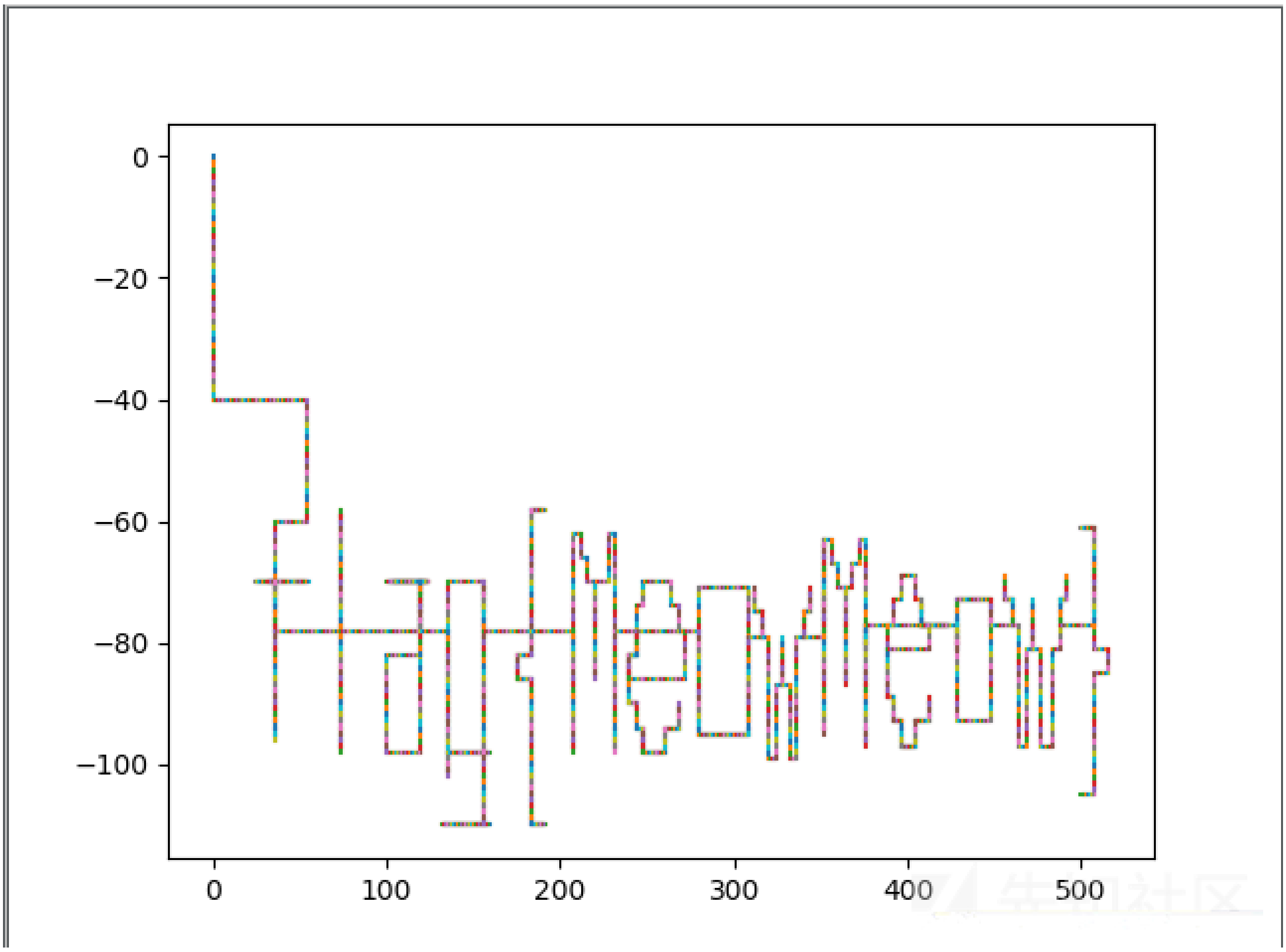
```
BREW /the_super_great_hidden_url_for_brewing_tea/black_tea
HTTP/1.1
Host: 202.38.95.46:12005
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,image/apng,*/*;q=0.8
Referer: http://202.38.95.46:12005/identity
Accept-Language: zh-CN,zh;q=0.9
Content-Type: message/teapot
Cookie:
session=eyJleHBpcmUiOjE1MzkxNzYxODQuMDI4NjAxNiwic3VmZml4IjoiWGNH
MXFIaTRGWGl5bUo3USIsInVpZCI6eyIgdSI6IjlmZTYwNmQ2YTkyMjQ0YjlhNDAx
ZDc3MGNmNDM2NzMyIn19.Dp-IPA.oC4Q3yHtT5Zt2p47lIJ-SPz-fAc;
PHPSESSID=b40888dfe05d80cdb85b7da361a9cff0
Connection: close
```

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 47
Server: Werkzeug/0.14.1 Python/3.6.6
Date: Mon, 15 Oct 2018 08:34:42 GMT

Here is your tea: flag{delivering_tea_to_DaLa0}
```

猫咪遥控器

本题为Misc方向题目，查看题目给的文档，里面只出现了四个字母，U D L R
应该是表示方向所以本题应该是作图。然后就用到了python的matplotlib库和numpy库。将题目给的文档作图，得到flag



python代码(py2.7)

```
#!/usr/bin/env python2
# -*- coding: UTF-8 -*-
import numpy as np
import matplotlib.pyplot as plt

xxx="DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRDDDDDDDDDDDDDDDDDDDDLLLLLLL
# print xxx.__len__()
xxxx=0
yyyy=0
for i in range(2813):
   if xxx[i]=='D':
       x=np.linspace(xxxx,xxxx,100)
       yyyy=yyyy-1
       y=np.linspace(yyyy,yyyy+1,100)
       print y
       plt.plot(x,y)
       continue
   if xxx[i]=='U':
       x = np.linspace(xxxx, xxxx, 100)
       yyyy = yyyy + 1
       y = np.linspace(yyyy-1, yyyy, 100)
       plt.plot(x, y)
       continue
   if xxx[i]=='R':
       y=np.linspace(yyyy,yyyy,100)
       xxxx=xxxx+1
       x=np.linspace(xxxx-1,xxxx,100)
       plt.plot(x,y)
       continue
   if xxx[i]=='L':
       y = np.linspace(yyyy, yyyy, 100)
       xxxx = xxxx - 1
       x = np.linspace(xxxx, xxxx+1, 100)
       plt.plot(x, y)
       continue
plt.show()
```

她的诗

原题关键代码为

```
for i in fin:
   data = "begin 666 <data>\n" + i + " \nend\n"
   decode_data = decode(data.encode("ascii"), "uu")
   print(decode_data)
   fout.write(decode_data.decode("ascii") + "\n")
```

但是根据官方给出的代码，只能解出一首诗

```
a despairingly large difference in skill.
---------
A joke only lasts for a moment,
if it leaves a misunderstanding,
it becomes a lie.
---------
If someone didn't have any pride,
wouldn't they also be lacking
in self-confidence?
If someone was free of greed,
wouldn't they have trouble
supporting their family?
And if people didn't envy one another,
wouldn't they stop inventing new things?
---------
If I don't have to do it, I won't.
If I have to do it, I'll make it.
---------
/* Here is the end of my poem.
Have you ever found my FLAG? :) */
```


所以我们需要自己解析官方给的文档,google搜索begin 666，发现这是UUencode编码，找到uuencode解码网站，解码。
发现解码出来的东西和用官方python代码解出的东西有一些不同，然后上python代码，调用difflib库
解得flag

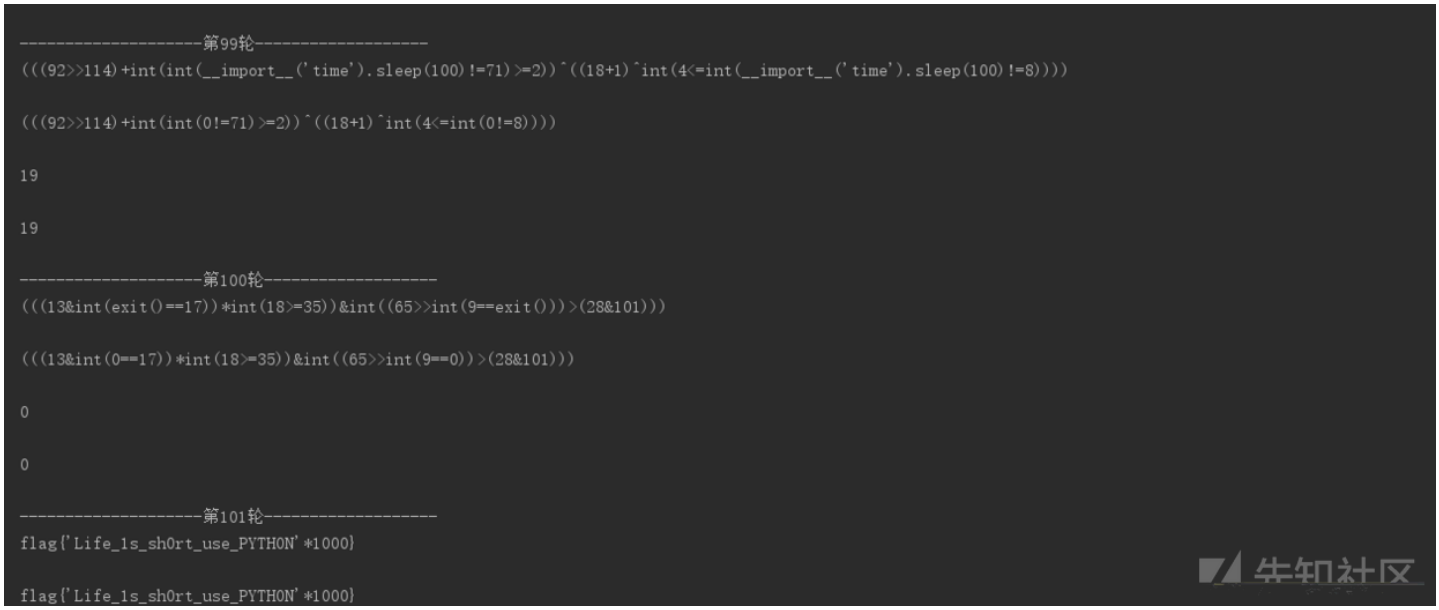
python代码(py2.7)

```
# coding:utf-8
import re
import string
import difflib
flag=""
a='''
---------
There is something in this world
that no one has ever seen before.
It is gentle and sweet.
Maybe if it could be seen,
everyone would fight over it.
That is why the world hid it,
so that no one could get their hands
on it so easily.
```

```
However, someday, someone will find it.
The person who deserves it the most
will definitely find it.
---------
Do you like this school?
I really, really love it.
But nothing can stay unchanged.
Fun things... Happy things...
They can't all possibly stay unchanged.
Even so,
can you go on loving this place?
---------
Sometimes I wonder,
what if this town was alive?
What if it had thoughts and feelings
like one of us?
If it did,
I think it would want to make the people
who live here happy.
---------
Expectations are what you have
when you have given up.
Expectations are born from
a despairingly large difference in skill.
---------
A joke only lasts for a moment,
if it leaves a misunderstanding,
it becomes a lie.
---------
If someone didn't have any pride,
wouldn't they also be lacking
in self-confidence?
If someone was free of greed,
wouldn't they have trouble
supporting their family?
And if people didn't envy one another,
wouldn't they stop inventing new things?
---------
If I don't have to do it, I won't.
If I have to do it, I'll make it.
---------
/* Here is the end of my poem.
'''
a=a.replace("\n","")
b="---------There is something in this worldfthat no one has ever seen before.It is gentle and sweet.lMaybe if it could be see
d = difflib.Differ()
diff = list(d.compare(a,b))
for line in diff:
   if line[0]=='+':
       flag+=line
flag=flag.replace("+","").replace(" ","")
print flag
```

猫咪克星

本题为python脚本编写题目，nc对面的端口，对面发来一些表达式，需要再规定时间内计算出这些表达式，并且将计算结果返回到对面。解出来之后发现是30s内算100道表
结果：



python代码：

```
#!/usr/bin/env python2
# -*- coding: UTF-8 -*-
from socket import*
import socket
import re
HOST = '202.38.95.46'    # The remote host
PORT = 12009                # The same port as used by the server
s = None

def RRR(shizi):
   xxxx=str(shizi)
   xxxx = xxxx.replace(r"__import__('time').sleep(100)",'0')
   xxxx = xxxx.replace(r"__import__('os').system('find ~')", '0')
   xxxx = xxxx.replace(r"exit()",'0')
   xxxx = xxxx.replace(r"print('\x1b\x5b\x33\x3b\x4a\x1b\x5b\x48\x1b\x5b\x32\x4a')",'0')
   print(xxxx)
   t = str(eval(xxxx)) + '\n'
   print(t)
   b1 = t.encode(encoding='utf-8')
   print(b1)
   return b1

sock = socket.socket()
sock.connect((HOST,PORT))
szBuf = sock.recv(1024)
print(szBuf)
x=0
while 1:
   x=x+1
   print('--------------------■'+str(x)+'■-------------------')
   szBuf = sock.recv(1024)
   print(szBuf)
   b1=RRR(szBuf)
   sock.send(b1)
```

Z同学的RSA

本题比赛的时候没有解出来，后期看官方wp，发现是低位爆破。刚开始学crypto,还不咋会，解题代码：

```
#!/usr/bin/env python2
#coding=utf-8
import gmpy2
import codecs
a=201776502865533190486565724314268646839723226165375287286448369509076541671449619384295097789265059381471632591473288721788
b=-201776502865533190486565724314268646839723226165375287286448369509076541671449619384295097789265059381471632591473288721788
c=133669037177951734291877613815676340480639848151331984089285031236028726473180970727139146395329801235376738280801364430967
```

```
f1 = lambda p, q: (p * q) ^ (p + q)
f2 = lambda p, q: (p * q) ^ (p - q)
candidates = {(0, 0)}

def run(m):#b2s
   m=hex(m)[2:]
   if len(m)%2==1:
       m='0'+m
   print(codecs.decode(m,'hex_codec'))

for m in range(1025):
   print(m, len(candidates))
   candidates_ = set()
   mask = (2 << m) - 1
   for x, y in candidates:
       if f1(x, y) == a and f2(x, y) == b:
           p, q = x, y
           d = gmpy2.invert(65537, (p - 1) * (q - 1))#■■■■
           m = pow(c, d, p * q)#■■■■
           run(m)
           exit()
       for bx in range(2):
           for by in range(2):
               xx = x + (bx << m)
               yy = y + (by << m)
               if f1(xx, yy) & mask != a & mask:
                   continue
               if f2(xx, yy) & mask != b & mask:
                   continue
               candidates_.add((xx, yy))
   candidates = candidates_

print libnum.b2s(int(463274022977499715904238458095255392124044273974527763262012433395686452421 22))
```


上一篇：PHP反序列化的一些例子 下一篇：http-header安全总结

1. 0 条回复

- 动动手指，沙发就是你的了！