buu ctf wp（crypto）

原创

higher_sky 于 2020-12-08 20:28:23 发布 556 收藏 2

分类专栏： buu ctf wp

本文链接：https://blog.csdn.net/higher_sky/article/details/110881135

MD5

题目

e00cf25ad42683b3df678c61f42c6bda

解题过程

1、了解什么是MD5加密

2、粗略了解加密的过程及其特点

3、上百度搜索解密的网站

(https://www.cmd5.com/

flag{admin1}

url编码

题目

%66%6c%61%67%7b%61%6e%64%20%31%3d%31%7d

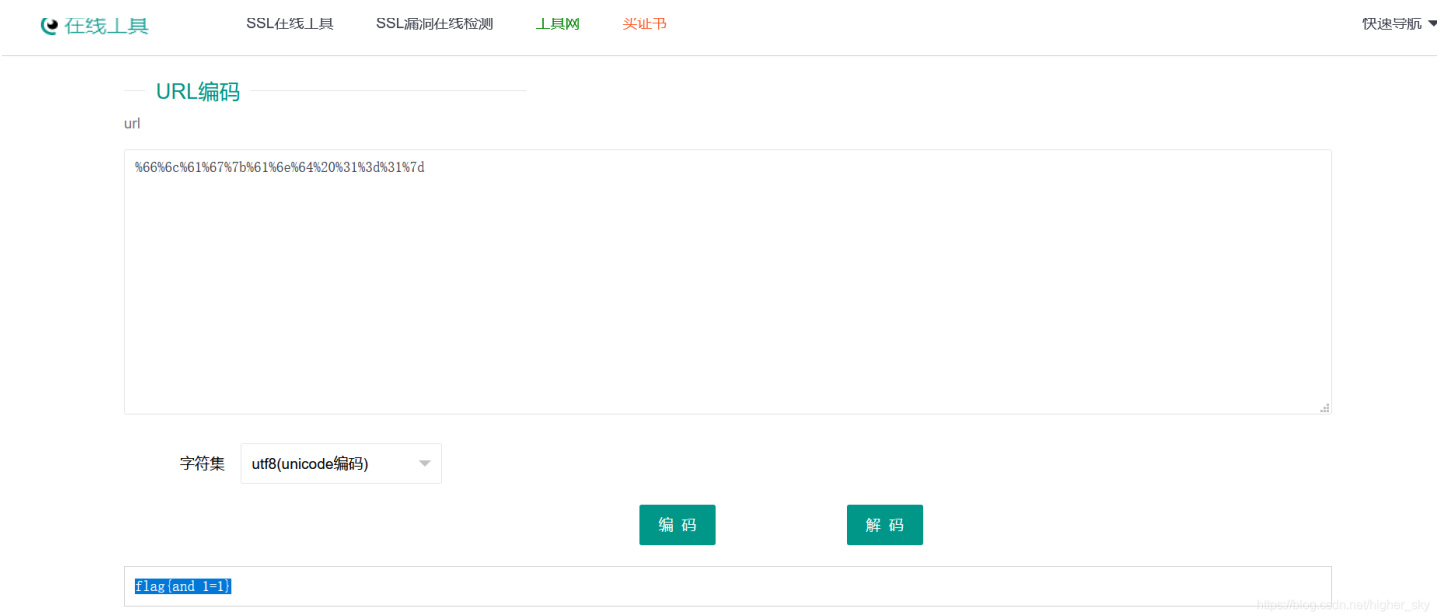
解题过程

1、url编码是将一个字符的assci码编码成16进制的方式然后在前面加一个%

2、url的编码的特点为十六进制数前面加上%

3、可以用C语言或python，写个脚本这里我就不写了，直接找度娘了，解码网站在下面

http://ctf.ssleye.com/url.html



flag{and 1=1}

一眼就解密

题目

ZmxhZ3tUSEVfRkxBR19PRl9USElTX1NUUklOR30=

解答过程

1、通过分析题目，发现题目中只有A-Z，0-9，还有一个明显的等于号

2、通过上述分析可以确定该代码运用了BASE64的加密方式

3、上度娘，找解密工具base

flag{THE_FLAG_OF_THIS_STRING}

看我回旋踢

题目

synt{5pq1004q-86n5-46q8-o720-oro5on0417r1}

解答过程

1、通过对常见密码的了解，可以猜测这是一个凯撒密码或者叫做移位密码

2、凯撒密码的介绍：

恺撒密码的替换方法是通过排列明文和密文字母表，密文字母表示通过将明文字母表向左或向右移动一个固定数目的位置。例如，当偏移量是左移3的时候（解密时的密钥就是3）：

明文字母表：ABCDEFGHIJKLMNOPQRSTUVWXYZ；

密文字母表：DEFGHIJKLMNOPQRSTUVWXYZABC。

使用时，加密者查找明文字母表中需要加密的消息中的每一个字母所在位置，并且写下密文字母表中对应的字母。需要解密的人则根据事先已知的密钥反过来操作，得到原来的明文。例如：

明文：THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG；

密文：WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ。

恺撒密码的加密、解密方法还能够通过同余的数学方法进行计算。首先将字母用数字代替，A=0，B=1，...，Z=25。此时偏移量为n的加密方法即为：

$$E_n(x) = (x + n) \mod 26.$$

解密就是：

$$D_n(x) = (x - n) \mod 26.$$

3、通过解密工具进行尝试解密恺撒解密

摩丝

题目

... .-... — ...- . -.-- — ...-

解答过程

1、了解摩斯密码的加密方式

1、了解摩斯密码的加密方式

2、

摩尔斯电码表

字符	电码符号	字符	电码符号	字符	电码符号
A	• —	N	— •	1	• — — — —
B	— • • •	O	— — —	2	• • — — —
C	— • — •	P	• — — •	3	• • • — —
D	— • •	Q	— — • —	4	• • • • —
E	•	R	• — •	5	• • • • •
F	• • — •	S	• • •	6	— • • • •
G	— — •	T	—	7	— — • • •
H	• • • •	U	• • —	8	— — — • •
I	• •	V	• • • —	9	— — — — •
J	• — — —	W	• — —	0	— — — — —
K	— • —	X	— • • —	?	• • — — • •
L	• — • •	Y	— • — —	/	— • • — •
M	— —	Z	— — • •	( )	— • — — • —
				—	— • • • • —

3、摩斯转化器

莫斯密码(摩斯密码)转换器

07 02 2007

sunshine

so-so Mood at 11:54 AM

莫尔斯/摩尔斯电码(Morse code)是美国人莫尔斯于1844年发明的，由点（.）、划（-）两种符号组成：

1. 一点为一基本信号单位，一划的长度=3点的长度。
2. 在一个字母或数字内，各点、划之间的间隔应为两点的长度。
3. 字母（数字）与字母（数字）之间的间隔为7点的长度。

莫尔斯/摩尔斯电码（Morse code)曾被用在间谍通信，电报，航海信号等各个领域。

ILOVEYOU

↓word2morse　↑morse2word

.. .-.. --- ...- . -.-- --- ..-

flag{lLOVEYOU}

[BJDCTF 2nd]签到-y1ng1

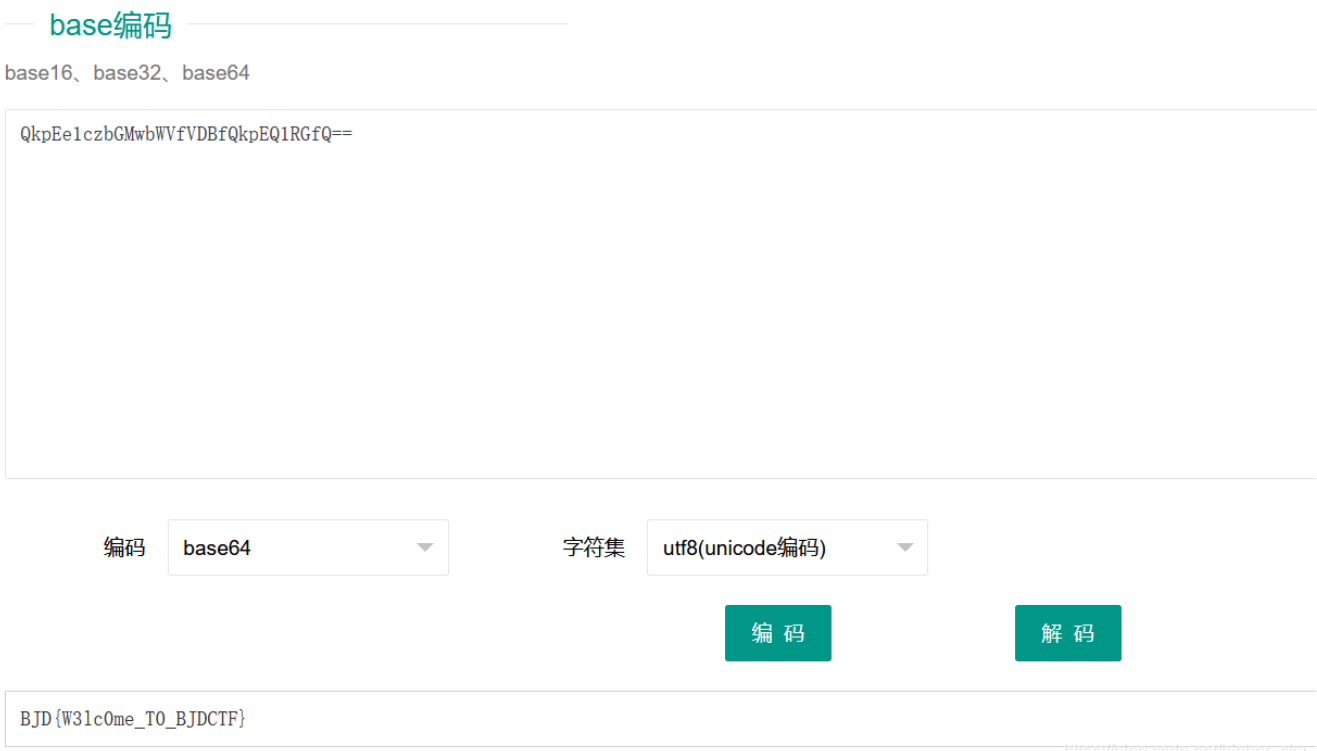
题目

QkpEe1czbGMwbWVfVDBfQkpEQ1RGfQ==

解答过程

1、一眼就能看出这是base加密

2、base



得到BJD{W31c0me_T0_BJDCTF}

flag{W31c0me_T0_BJDCTF}

password

题目

姓名：张三

生日：19900315

key格式为key{xxxxxxxxx}

解答过程

1、通过对题目的分析和尝试

2、key就是密钥，同理flag{}也是这样的格式

3、猜测flag{zs19900315},成功了

flag{zs19900315}

变异凯撒

题目

加密密文：afZ_r9VYfScOeO_UL^RWUc

格式：flag{ }

解答过程

1、

凯撒密码最早由古罗马军事统帅盖乌斯·尤利乌斯·凯撒在军队中用来传递加密信息，故称凯撒密码。此为一种位移加密手段，只对26个（大小写）字母进行位移加密，规则相当简单，容易被破解。下面是明文字母表移回3位的对比：

明文字母表 X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

密文字母表 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

然后A变成D，B变成E，Z变成C。

字母最多可移动25位（按字母表）。通常为向后移动，如果您想向前移动1位，则相当于向后移动25位，位移选择为25位。

2、显然这里不是简单的凯撒加密，因为凯撒加密的对象为二十六个英文字母，看到_、^我们可以想到ASCII码

ASCII值	控制字符	ASCII值	控制字符	ASCII值	控制字符	ASCII值	控制字符
0	NUT	32	(space)	64	@	96	、
1	SOH	33	!	65	A	97	a
2	STX	34	"	66	B	98	b
3	ETX	35	#	67	C	99	c
4	EOT	36	$	68	D	100	d
5	ENQ	37	%	69	E	101	e
6	ACK	38	&	70	F	102	f
7	BEL	39	,	71	G	103	g
8	BS	40	(	72	H	104	h
9	HT	41	)	73	I	105	I
10	LF	42	^	74	J	106	j
11	VT	43	+	75	K	107	k
12	FF	44	,	76	L	108	l
13	CR	45	-	77	M	109	m
14	SO	46	.	78	N	110	n
15	SI	47	/	79	O	111	o
16	DLE	48	0	80	P	112	p
17	DCI	49	1	81	Q	113	q
18	DC2	50	2	82	R	114	r
19	DC3	51	3	83	S	115	s
20	DC4	52	4	84	T	116	t
21	NAK	53	5	85	U	117	u
22	SYN	54	6	86	V	118	v
23	TB	55	7	87	W	119	w
24	CAN	56	8	88	X	120	x
25	EM	57	9	89	Y	121	y
26	SUB	58	:	90	Z	122	z
27	ESC	59	;	91	[	123	{
28	FS	60	<	92	/	124	|
29	GS	61	=	93	]	125	}
30	RS	62	>	94	^	126	~
31	US	63	?	95	_	127	DEL

3、通过对照知道该字符串移位了5

```
m='afZ_r9VYfScOeO_UL^RWUc'
j=5
for i in m:
    print(chr(ord(i)+j), end='')
    j += 1
```

flag{Caesar_variation}

Quoted-printable

题目

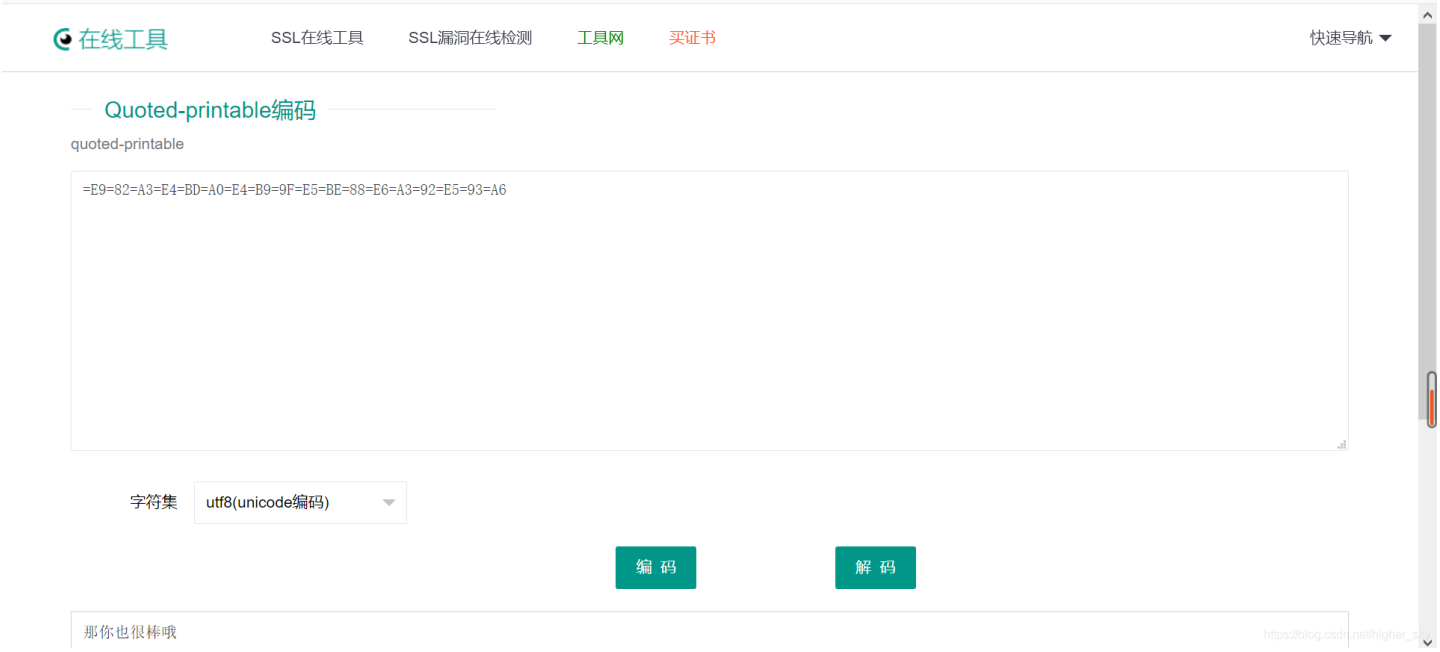
=E9=82=A3=E4=BD=A0=E4=B9=9F=E5=BE=88=E6=A3=92=E5=93=A6

解题过程

1、通过百度查询题目知道这是一种编码方式

2、我这里提供一个网址在线解码方式添加链接描述

3、



flag{那你也很棒哦}

Rabbit

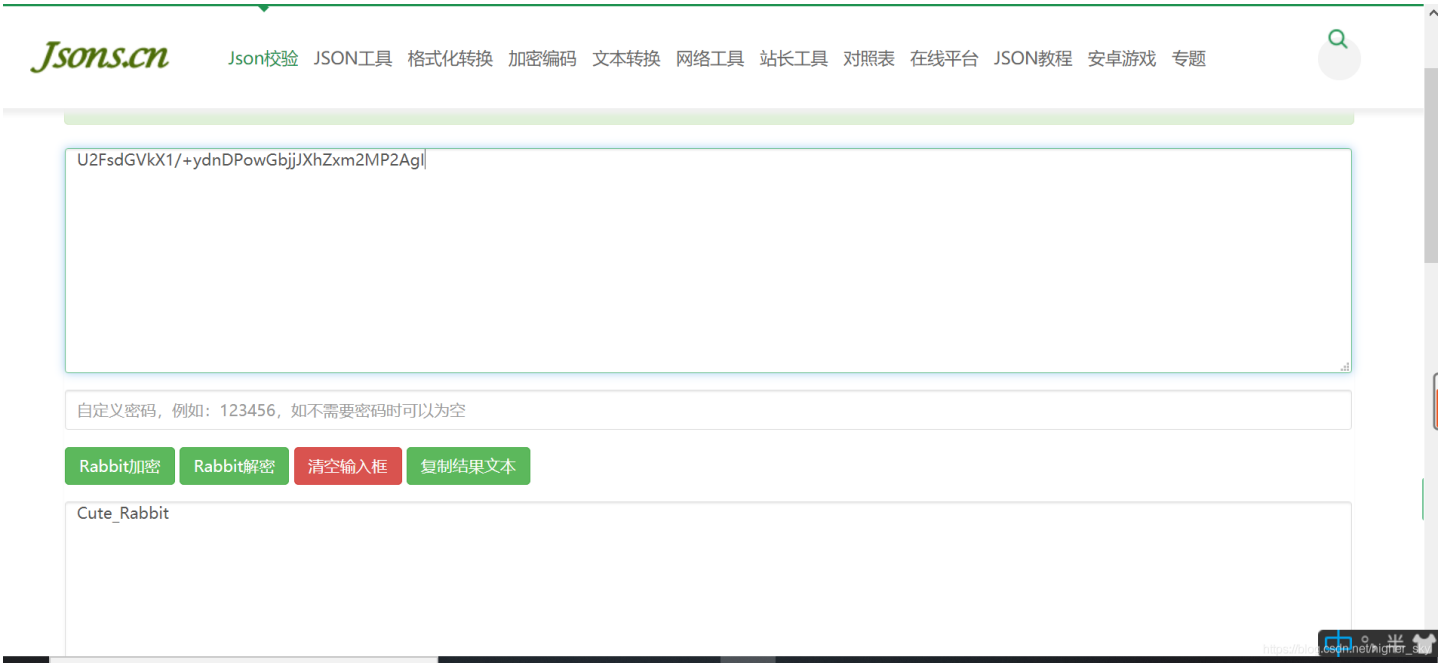
题目

U2FsdGVkX1/+ydnDPowGbjjJXhZxm2MP2AgI

解答过程

1、分析题目，通过度娘搜索得到Rabbit这是一种密码

2、然后我这里提供一个网址，在线解析得添加链接描述



flag{Cute_Rabbit}

篱笆墙的影子

题目

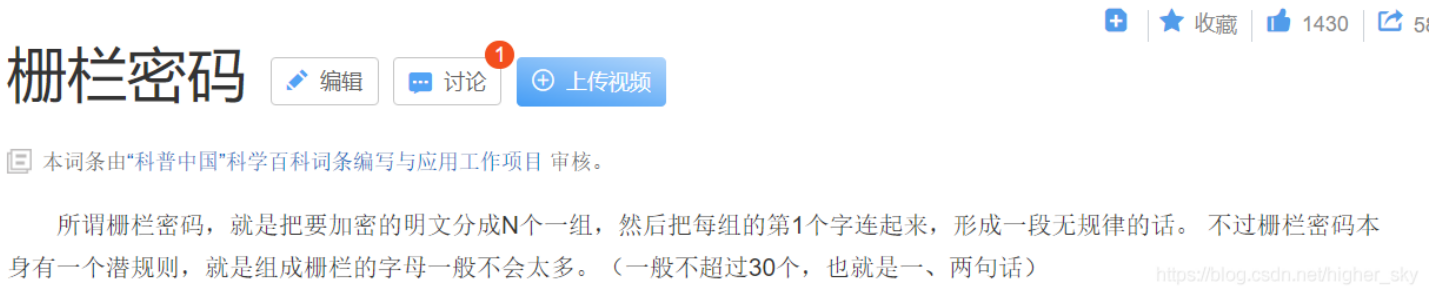
felhaagv{ewtehtehfilnakgw}

解答

1、有题目形式可以看出这是一个栅栏密码

2、在线加密添加链接描述

3、尝试解答

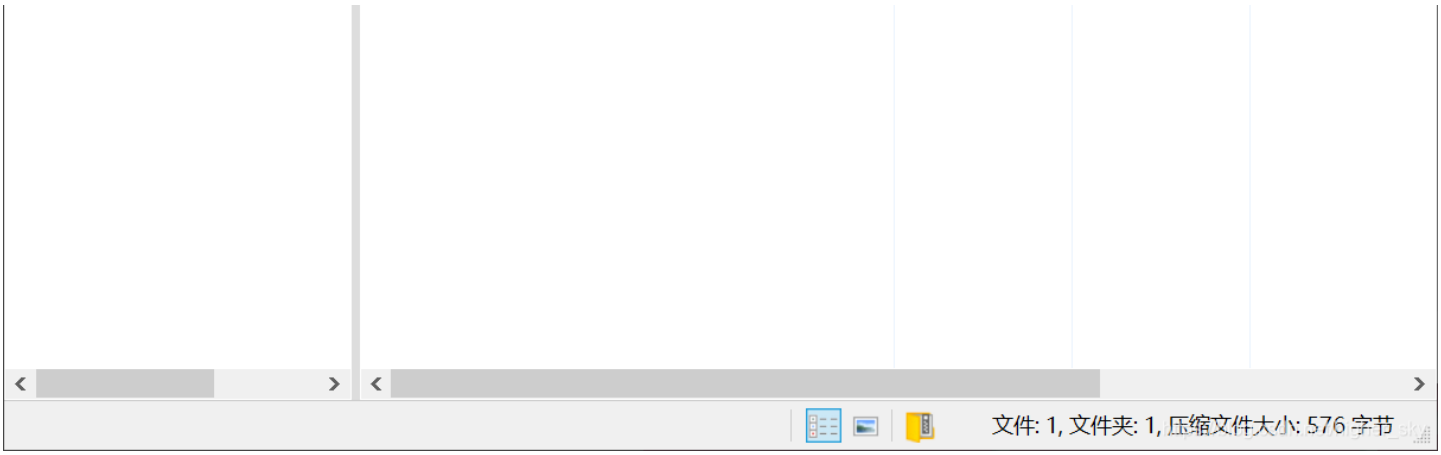


题目共有26个字母把26分解成因素1,2,13,26排除掉1和字符串长度，

flag{wethinkwehavetheflag}

丢失的MD5

题目



用python IDLE打开得到

```
import hashlib
for i in range(32,127):
    for j in range(32,127):
        for k in range(32,127):
            m=hashlib.md5()
            m.update('TASC'+chr(i)+'O3RJMV'+chr(j)+'WDJKX'+chr(k)+'ZM')
            des=m.hexdigest()
            if 'e9032' in des and 'da' in des and '911513' in des:
                print des
```


直接改下脚本运行一下就出来了

```
import hashlib
for i in range(32,127):
    for j in range(32,127):
        for k in range(32,127):
            m = hashlib.md5()
            s = 'TASC'+chr(i)+'O3RJMV'+chr(j)+'WDJKX'+chr(k)+'ZM'
            m.update(s.encode("utf8"))
            des=m.hexdigest()
            if 'e9032' in des and 'da' in des and '911513' in des:
                print(des)
                break
```

flag{e9032994dabac08080091151380478a2}

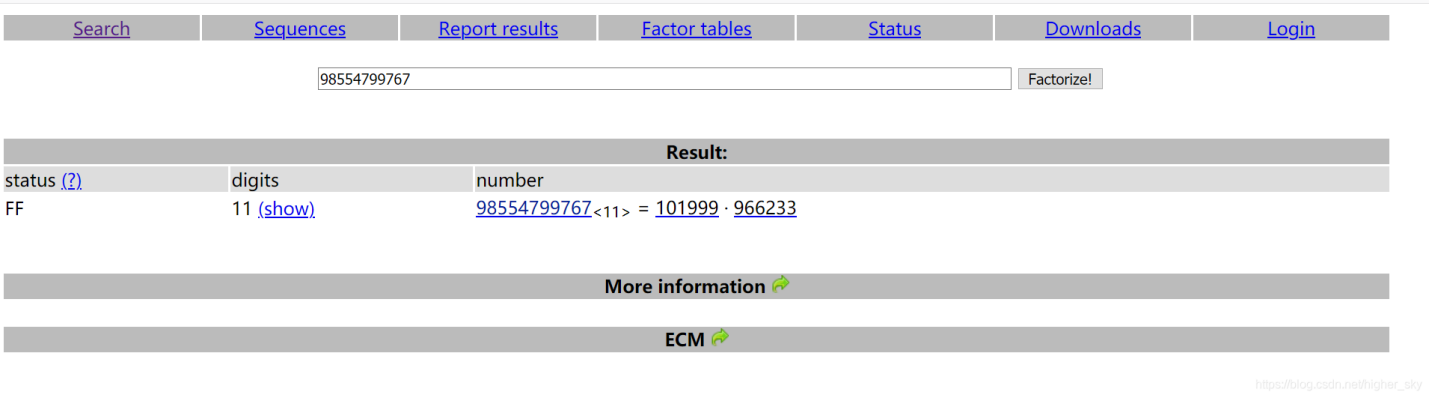
Alice与Bob

题目

密码学历史中，有两位知名的杰出人物，Alice和Bob。他们的爱情经过置换和轮加密也难以混淆，即使是没有身份认证也可以知根知底。就像在数学王国中的素数一样，孤傲又热情。下面是一个大整数:98554799767,请分解为两个素数，分解后，小的放前面，大的放后面，合成一个新的数字，进行md5的32位小写哈希，提交答案。 注意：得到的 flag 请包上 flag{} 提交

解答过程

1、在线分解素数添加链接描述



2、101999966233添加链接描述

flag{ d450209323a847c8d01c6be47c81811a}