实验吧密码学writeup

转载

weixin_30419799 于 2017-10-12 19:39:00 发布 261 收藏
文章标签： 密码学 php
原文链接：http://www.cnblogs.com/Acewipe/p/7631300.html

传统知识+古典密码 分值：10

来源：霜羽 难度：易 参与人数：1507人 Get Flag：443人 答题人数：602人 解题通过率：74%

小明某一天收到一封密信，信中写了几个不同的年份
辛卯，癸巳，丙戌，辛未，庚辰，癸酉，己卯，癸巳。
信的背面还写有“+甲子”，请解出这段密文。
key值：CTF{XXX}

看密信内容知道需要查看天干地支表

干支表

01 甲子	11 甲戌	21 甲申	31 甲午	41 甲辰	51 甲寅
02 乙丑	12 乙亥	22 乙酉	32 乙未	42 乙巳	52 乙卯
03 丙寅	13 丙子	23 丙戌	33 丙申	43 丙午	53 丙辰
04 丁卯	14 丁丑	24 丁亥	34 丁酉	44 丁未	54 丁巳
05 戊辰	15 戊寅	25 戊子	35 戊戌	45 戊申	55 戊午
06 己巳	16 己卯	26 己丑	36 己亥	46 己酉	56 己未
07 庚午	17 庚辰	27 庚寅	37 庚子	47 庚戌	57 庚申
08 辛未	18 辛巳	28 辛卯	38 辛丑	48 辛亥	58 辛酉
09 壬申	19 壬午	29 壬辰	39 壬寅	49 壬子	59 壬戌
10 癸酉	20 癸未	30 癸巳	40 癸卯	50 癸丑	60 癸亥

找出迷信内容对应的数字+60（一甲子）得到一串数字。对应ASCII码表得到字符串

XZSDMFLZ

不像flag，在考虑题目中的古典加密，无非就是凯撒、栅栏等组合加密（一种的得不到密文），爆破之后发现栅栏2栏，再凯撒得到

SHUANGYU

2.The Flash -14

The Flash-14 分值：10

来源：山南水北 难度：易 参与人数：2670人 Get Flag：963人 答题人数：1236人 解题通过率：78%

这些数字都是什么呢~ 5443325222445534225152224434222311341 2
答案形式ctf{XXX}

观察密文，所有数字均不大于5，猜想可能是5*5矩阵字母表，百度题目发现闪电侠第二季14集里有个矩阵表

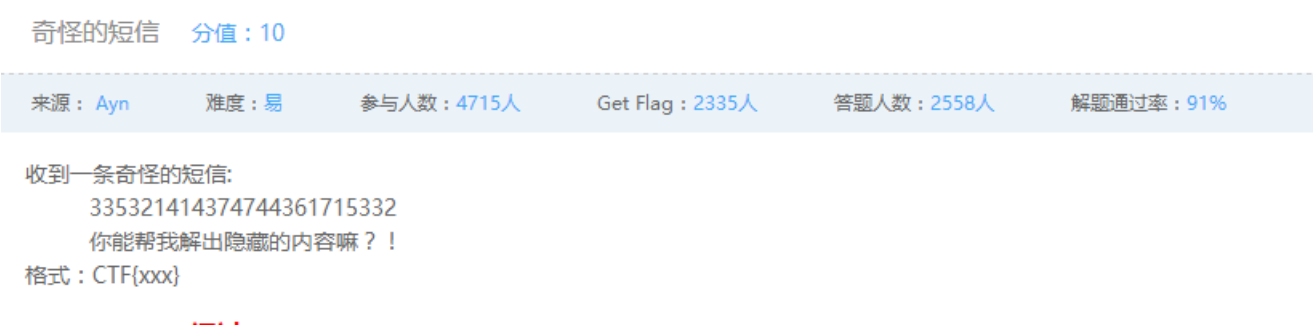
	1	2	3	4	5
1	A	B	C/K	D	E
2	F	G	H	I	J
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

将密文两两为一对得到对应字符串 YSMWGTZOGVWGTOGHAOB

猜想可能还需要凯撒，于是尝试一下

发现+12之后就是flag

3.奇怪的短信



经过上一题试试两两拆分得到

33 53 21 41 43 74 74 43 61 71 53 32

想想短信联想到九宫格字母表前一个数字代表按键，后一个数字代表第几个字母，发现吻合这个规律

直接得到flag

3.RSAROLL

RSAROLL 分值：20

来源： hanyuhang 难度：中 参与人数：2571人 Get Flag：526人 答题人数：581人 解题通过率：91%

RSA roll ! roll ! roll !
flag格式：flag{xxx}

解题链接： http://ctf5.shiyanbar.com/crypto/RSAROLL.txt 通过

{920139713, 19}

```
704796792
752211152
274704164
18414022
368270835
483295235
263072905
459788476
483295235
459788476
663551792
475206804
459788476
428313374
475206804
459788476
425392137
704796792
458265677
341524652
483295235
534149509
425392137
428313374
425392137
341524652
458265677
263072905
483295235
828509797
341524652
425392137
475206804
428313374
483295235
475206804
459788476
306220148
```

暂时讲不清参考他人的解题思路

https://www.52pojie.cn/forum.php?mod=viewthread&tid=490769

5.困在栅栏中的爱

围在栅栏中的爱 分值：10

来源： Ayn 难度：易 参与人数：3639人 Get Flag：1919人 答题人数：2212人 解题通过率：87%

最近一直在好奇一个问题，QWE到底等不等于ABC？
-.- .. --.- .-.. .-- - ..-. -.-. --.- --. -. ... --- ---
flag格式：CTF{xxx}

看格式摩尔斯电码，解密得到

根据QWE=ABC？知道键盘加密

解密得到 rhasbenvaoylii

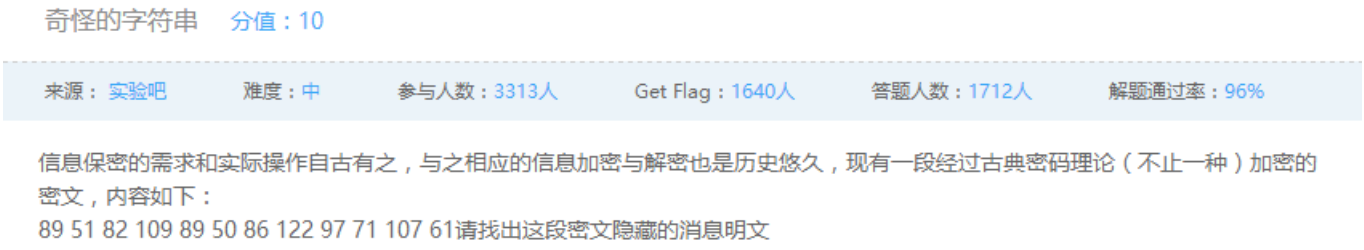
再结合题目栅栏解密和关键字爱（love），栅栏解密

6栏 rabnayosevol

7栏 rabnayiosevoli

倒序解密得到flag

6.奇怪的字符串



直接ASCII码解密得到字符串Y3RmY2UzaGk=

看格式知道base64解密得到flag

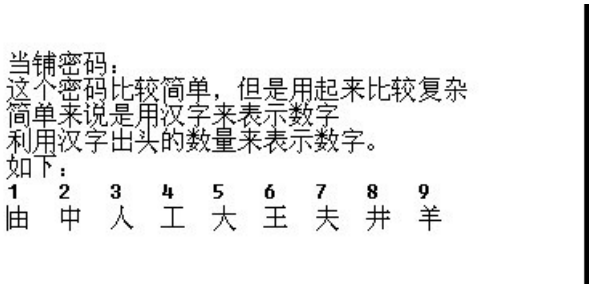
7.疑惑的汉字

疑惑的汉字　分值：10

来源：实验吧　难度：易　参与人数：3152人　Get Flag：1771人　答题人数：1844人　解题通过率：96%

现有一段经过加密的密文，内容如下：王夫 井工 夫口 由中人 井中 夫夫 由中大。请找出这段密文隐藏的消息明文。
格式：CTF{ }

当铺密码解密



得到数字67 84 70 123 82 77 125

ASCII码表解密得到flag

8.古典密码

古典密码　分值：10

来源：北邮天枢战队　难度：易　参与人数：4783人　Get Flag：1382人　答题人数：1595人　解题通过率：87%

密文内容如下{79 67 85 123 67 70 84 69 76 88 79 85 89 68 69 67 84 78 71 65 72 79 72 82 78 70 73 69 78 77 125 73 79 84 65}
请对其进行解密
提示：1.加解密方法就在谜面中
　　2.利用key值的固定结构
格式：CTF{ }

ASCII码表得到字符串OCU{CFTELXOUYDECTNGAHOHRNFIENM}IOTA

列置换参考 http://blog.sina.com.cn/s/blog_e23a215b0102wazq.html

最后根据flag的格式得到flag

9.困在栅栏里的凯撒

困在栅栏里的凯撒　分值：10

来源：北邮天枢战队　难度：易　参与人数：4166人　Get Flag：1885人　答题人数：2028人　解题通过率：93%

小白发现了一段很6的字符：NIEyQd{seft}

栅栏6栏 NEQ{etlydsf}，再凯撒解密即可得到flag

10.奇妙的音乐

奇妙的音乐　分值：10

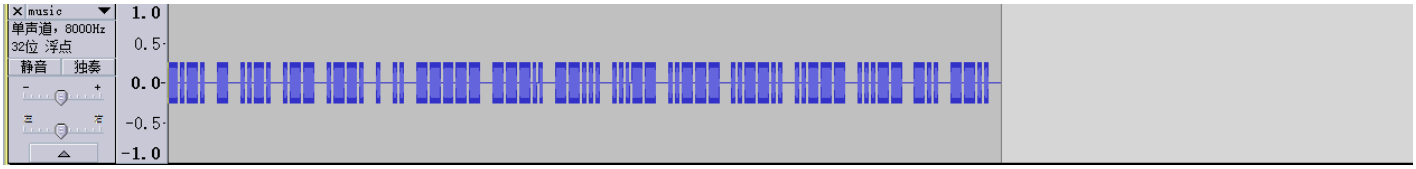
来源：北邮天枢战队　难度：易　参与人数：3611人　Get Flag：832人　答题人数：1004人　解题通过率：83%

据说flag就藏在这段音乐中，请仔细听。
格式：CTF{}

解压发现一张图片加一个压缩包，查看图片

盲文解密得到解压密码，解压得到一段音乐，听过之后应该是发电报的声音

在音乐编辑软件中打开



粗的条“-”，细的条“.”，没有条补空格

—.—. — ..—. .—— .——. . .. ———————— ————..———... ...—— ..——— ..——.. ..——— ... —— —.. ——..

摩尔斯电码解密得到flag

11.敌军情报

敌军情报　分值：10

来源：北邮天枢战队　难度：易　参与人数：3359人　Get Flag：1643人　答题人数：1771人　解题通过率：93%

知彼知己方能百战不殆。天枢战队成员截获了一条命令密文45 46 45 46 32 45 32 46 46 45 46 32 46 45 32，你能解密成明文，做到知己知彼吗？
格式：CTF{ }

ASCII码表得到一串摩尔斯电码，解密得到flag

12.我喜欢培根

我喜欢培根　分值：20

来源：Ph0enix　难度：中　参与人数：3327人　Get Flag：1336人　答题人数：1567人　解题通过率：85%

key: CTF{}

摩尔斯电码解密，注意/ 有三段，解密后发现很多dc字符，（附上培根加密图解）将d，c分别用b，a替换

参照图解解密即可得到flag

采用a和b，26个英文字母二进制表示法。

a	AAAAA	g	AABBA	n	ABBAA	t	BAABA
b	AAAAB	h	AABBB	o	ABBAB	u-v	BAABB
c	AAABA	i-j	ABAAA	p	ABBBA	w	BABAA
d	AAABB	k	ABAAB	q	ABBBB	x	BABAB
e	AABAA	l	ABABA	r	BAAAA	y	BABBA
f	AABAB	m	ABABB	s	BAAAB	z	BABBB

编写密码时，把密文每五个字母为一组，凡是其中的正体字母代表a，斜体字母代表b。随意选取句子或文章，就可以通过改变字母的写法来加密了。如：密文是LOVE，用“随意选取句子和文”加密，得到结果就是

“SuLyi XuanQ uJuZi HEwEN（随意选取句子和文）”

Ababb abbba babab aabaa （这里用小写代表斜体）

13.Decode

Decode 分值：10

来源： zusheng 难度：易 参与人数：3034人 Get Flag：1373人 答题人数：1463人 解题通过率：94%

flag格式:ctf{}

0x25346425353425343525333525343325366125343525373725346425353125366625373825346425343425363725346225346625353425366225346225346425353425343525373825343325366125343525373725346625353125366625373825346425343425343525346225346425353425343525333225343325366125343525373825346425353125366625373825346425353425353525346225346425353425343125333025343325366125343525373725346525353125366625373825346425366125343525346225346625353425363325346225346425353425343525373725343325366125366225333425343325366125366225333325343325366125343525373825346525343125336425336

0x开头，hex还原得到一串字符串

%4d%54%45%35%43%6a%45%77%4d%51%6f%78%4d%44%67%4b%4f%54%6b%4b%4d%54%45%78%4

URL解码得到一串数字，ASCII码表解密得到flag

14.RSA实践

RSA实践 分值：10

来源： Veneno 难度：易 参与人数：2519人 Get Flag：732人 答题人数：834人 解题通过率：88%

在一次RSA密钥对生成中，假设p=473398607161，q=4511491，e=17

求解出d

将得到的d提交

直接RSA算法解得d，提交即可

15.杯酒人生

杯酒人生 分值：10

来源： Veneno 难度：易 参与人数：2450人 Get Flag：696人 答题人数：854人 解题通过率：81%

使用古典密码

一喵星人要想喵星发送一段不知道干什么用的密码“BLOCKCIPHERDESIGNPRINCIPLE”，但是它忘记了密钥是什么，手头（爪头）只有它自己加密过的密钥“HTRUZYJW”，而且它还知道原密钥是一个单词，你可以帮助它传递信息，早日攻克蓝星，征服人类吗？

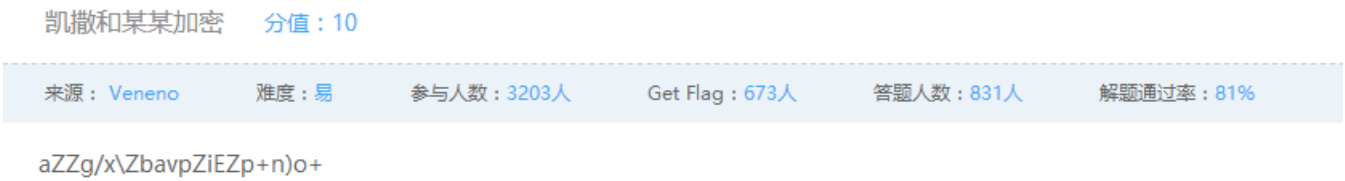
密钥HTRUZYJW,

凯撒一跑得到+21COMPUTER为加密密钥

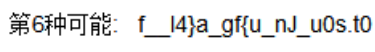
古典密码需要密钥加密的就只有那几种，最后试维吉尼亚密码发现可以得到flag

（不熟悉维吉尼亚加密的可以百度自行掌握，比较简单）

16.凯撒和某某加密



密文里面含有字母和符号，如果是凯撒加密的话，应该是整个ASCII码表的移动，列举全部结果发现最有可能是flag的



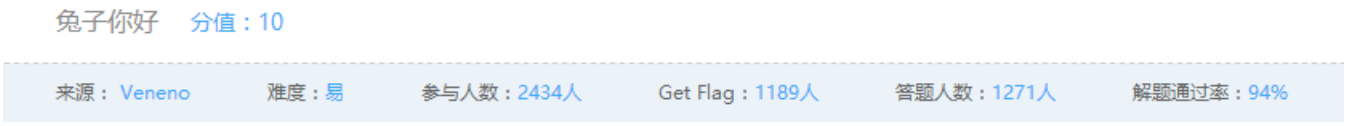
看这个密文结构应该是栅栏加密，不过这儿的是栅栏加密的一种变种

将字符串每三个一组顺序排列可以得到

f__ =>f _ _
l4} =>l 4 }
a_ =>a _
gf =>g f
{u =>{ u
_n =>_ n
J_ =>J _
u0 =>u 0
s. =>s .
t0 =>t 0

从上往下，从左往右一路看下来就得到flag

17.兔子你好



base64解密发现加了盐

百度发现有一种兔子算法加密的方式，在线解密即可得到flag

18.base？？

知道md5爆破就可以得到密文，发现其实密文全部大写就是YMFZZTY0D3RMD3RMMTIZ

将密文base64解密即可得到flag

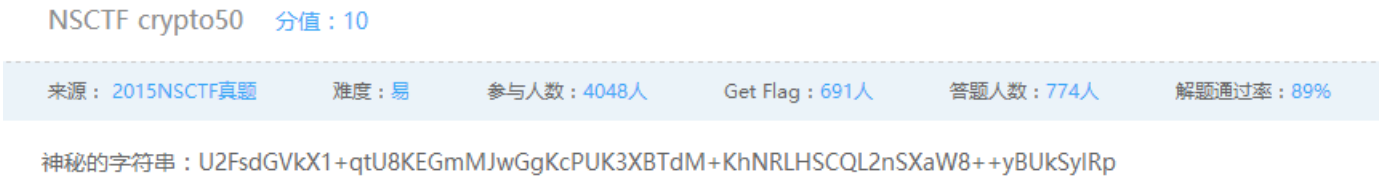
19.NSCTF crypto200

将图片保存后在stegsolve打开

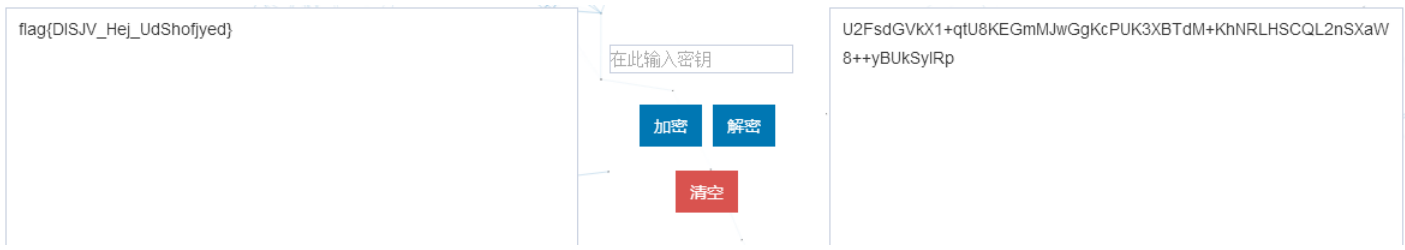
变换之后得到一张二维码图片

扫码没法应，颜色翻转后再扫得到flag

20.NSCTF crypto50



看格式知道AES加密，解密得到flag



提交不对，应该还有凯撒移位加密 ，flag头应该是NSCTF开头，解密得到flag

21.黑客叔叔（雨袭团）1.01

最简单的加密方式 by:p0tt1

dW1mcGJsamhhd3Jmcm14aHoxOXptZj1tZWducm13NDV4M2RvbmhxfDAxfDAzfDA3fCt8KzF8KzN8Kzd8MisxfDIrMnwyKzZ8Mis3fDIrOXwzKzB8MyszfDMrN3wzKzh8Mys5fD98

base64解密得到

umfpbljhawrfrmxhz19zmf9megnrmw45x3donhq|01|03|07|+|+1|+3|+7|2+1|2+2|2+6|2+7|2+9|3+0|3+3|3+7|3+8|
|

猜想应该是要部分字母变大写 规律是:

|01|03|07| 表示第1,3,7位

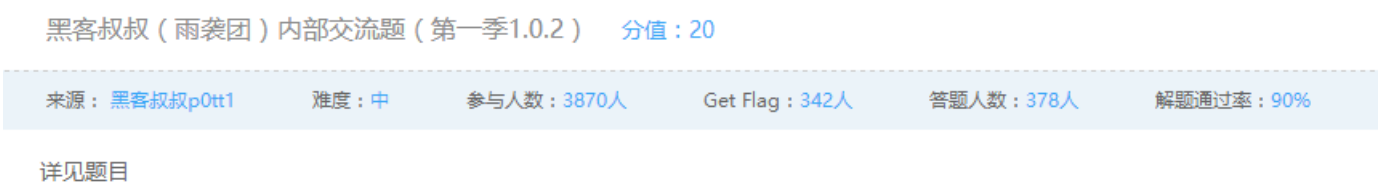
|+1|+3|+7|表示第11,13,17位

|2+1|2+2|2+6|2+7|2+9|表示第21,22,26,27,29位

|3+0|3+3|3+7|3+8|3+9|表示第30,33,37,39位

上面标记位数全部大写之后base64解密得到flag

22.黑客叔叔雨袭团（1.02）



U2FsdGVkX18vmjE0tvWk69T女B神u9inuiNnM3rBhsu6tXzLhu+

iofwuHNHq3YtDKs8Z1YLvSZuUY+

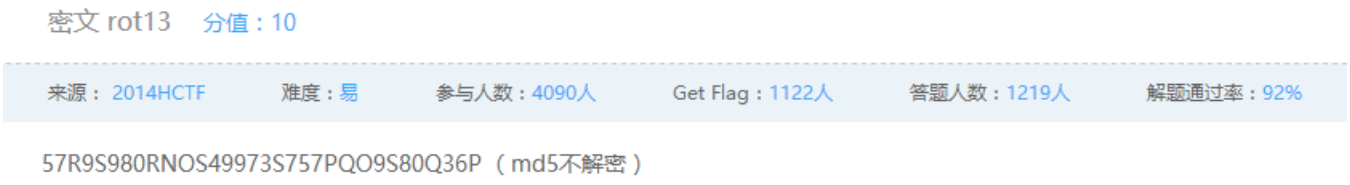
mxLRKO7+

m254R5YTCW8yzzgD+

mGwWfGRgqmPKdD你xA等等

看格式应该属于3des加密，不过里面有文字，将文字换成/，“等等“换成“==”，（别问我为什么，格式告诉我的）然后兔子解密（rabbit算法）即可

23.密文 rot-13



rot13解密即可得到flag

24.keyboard

BHUK,LP TGBNHGYT BHUK,LP UYGBN TGBNHGYT BHUK,LP BHUK,LP TGBNHGYT BHUK,LP TGBNHGYT UYGBN

键盘上画图得到字母，就是flag

25.古典密码的安全性不高，但仍然十分美妙，请破译下面的密文

古典密码的安全性不高，但仍然十分美妙，请破译下面的密文　分值：10

来源：强网杯CTF　难度：易　参与人数：4217人　Get Flag：864人　答题人数：1000人　解题通过率：86%

本题 flag 并非 flag{可见字符} 的形式

```
Os drnuzearyuwn, y jtkjzoztzoes douwlr oj y ilzwex eq lsdexosa kn pwodw tsozj eq ufyoszlbz yrl rlufydlx pozw douwlrzlbz, ydderxosa ze y rlatfyr jnjzli; mjy gfbmw vla xy
wbfnsy symmyew (mjy vrwm qrvvrf), hlbew rd symmyew, mebhsymw rd symmyew, vbomgeyw rd mjy lxrzy, lfk wr dremj. Mjy eyqybzye kyqbhjyew mjy myom xa hyedrevbfn lf bfzyewy
wgxwmbmgmbrf. Wr mjy dsln bw fl_2jyf-k3_jg1-vb-v1_1
```

字频分析得到

```
0     -2.814   ?l fog?vryoe?sg, e h?dhv?v?v?rl f??sao ?h e ?avsrb rc alfrb?ly dg ?s?fs ?l?vh rc ?ne?lvaiv eoa oa?nefab ??vs f??saovaiv, effrob?ly v
                e oay?neo hghva?; the units may be single letters (the most common), pairs of letters, triplets of letters, mi?tures of the above,
                and so forth. The receiver deciphers the te?t by performing an inverse substitution. So the flag is n1_2hen-d3_hu1-mi-ma_a
```

26.凯撒是罗马共和国杰出的军事统帅

凯撒是罗马共和国杰出的军事统帅　分值：10

来源：西普学院　难度：中　参与人数：4748人　Get Flag：1631人　答题人数：1786人　解题通过率：91%

MGAKUZKRWZWGAWCP

凯撒解密得到flag

27.摩擦摩擦

摩擦摩擦　分值：10

来源：西普学院　难度：易　参与人数：4368人　Get Flag：1522人　答题人数：1608人　解题通过率：95%

".-- . .-.. -.-. --- -- . - --- -..- .. .--. ..- -..- ..- . -.-- ..- .- -."

解题链接：http://ctf5.shiyanbar.com/crypto/1/beiai.html　通过

摩尔斯电码解密得到flag

28.最近听说刘翔离婚了

最近听说刘翔离婚了　分值：10

来源：西普学院　难度：易　参与人数：4652人　Get Flag：1518人　答题人数：1636人　解题通过率：93%

kyssmlxeei{ipeu}

栅栏解密得到flag

29.最近在论证一个问题，到底是先有鸡还是先有蛋

最近在论证一个问题，到底是先有鸡还是先有蛋　分值：10

来源：西普学院　难度：易　参与人数：4046人　Get Flag：1198人　答题人数：1288人　解题通过率：93%

ljm,lo 3wsdr4 6tghu7

解题链接：http://ctf5.shiyanbar.com/crypto/1/dan.html　通过

简单键盘加密，键盘画画

30.一段奇怪的代码

一段奇怪的代码　分值：30

来源：西普学院　难度：难　参与人数：4501人　Get Flag：1472人　答题人数：1495人　解题通过率：98%

哎！怎么出题的，都提示到家门口了

Tips　asp, encode

一段奇怪的代码

#@~^EQAAAA==VXlj4UmkaYAUmKN3bAYAAA==^#~@

这段代码解密之后就是key

百度asp encode，网站在线解密即可得到flag

31.这里没有key

这里没有key　分值：10

来源：西普学院　难度：易　参与人数：5500人　Get Flag：1909人　答题人数：2018人　解题通过率：95%

你说没有就没有啊，俺为啥要听你的啊

点开有提示框大家好，不管直接看源代码，发现

<!-- #@~^TgAAAA==’[6*liLa6++p’aXvfiLaa6i[[avWi[[a*p[[6*!I’[6cp’aXvXILa6fp[:6+Wp[:XvWi[[6+XivRIAAA==^#~@ -->

明显的vbscript encode

丢控制台解密即可得到flag

转载于:https://www.cnblogs.com/Acewipe/p/7631300.html