

# XJNU-CTF 2018 WP

## BASE

### 0x01 Base10

题目如下：

## Base10

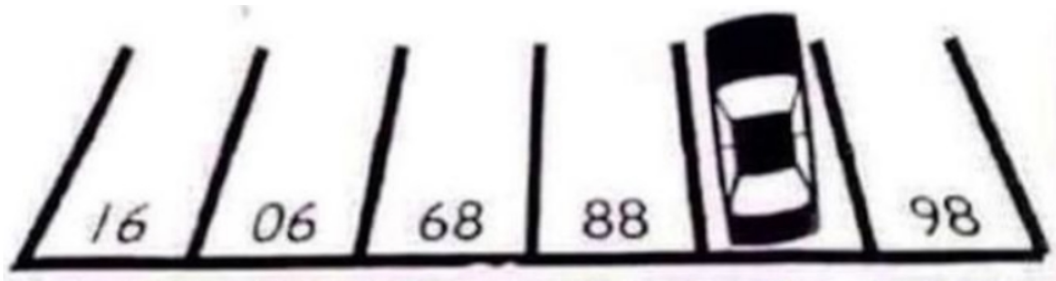
(solver: 61)

靠边停车

<http://ctf.xjnu.edu.cn:9900/base1/base1.html>

Auth

打开网页看到一张图片：



挡住的肯定是 87 啊，从右往左看就明白了，右键打开网页源代码：

```
</head>
<body>

<!-- flag{Math_is_Here_$num$!} 鏢板趾纒燐玊瑯圖確杞一濺鏹' 綈浜 ◆, num=md5(num)[:5]-->
</body>
</html>
```

将 87 进行 MD5 加密取前五位即可。

## 0x02 Base20

题目如下：

### Base20

(solver: 50)

Tom 和 Bob 共同的朋友Jack生日快到了，他两想知道Jack的生日，但是他俩都不知道，但是Jack给了他俩一个生日的列表,让他俩进行推算

May 15 May 16 May 19  
June 17 June 18  
July 14 July 16  
August 14 August 15 August 17

Jack分别告诉了Tom月份，Bob日期

Tom：我不知道Jack 的生日，我知道Bob也不知道。

Bob：首先我也不知道Jack的生日，但是我知道日期。

Tom：一开始我不知道，现在我知道Jack的生日了

Bob: 那我也知道了

flag{Th0\_Jack\_Birth\_Is\_月\_日}

Auth

我智商不够，答案是一个一个试出来的。

## 0x03 Base30

题目如下：

## Base30

(solver: 70)

:)内心有点小崩溃。  
请计算1000000000以内3或5的倍数之和。

如：10以内这样的数有3,5,6,9, 和是23

请提交flag{你的答案}

直接上脚本：

```
a=1000000000-1
```

```
sum=0
```

```
while(a):
```

```
    if a%3==0 or a%5==0:
```

```
        sum+=a
```

```
    a-=1
```

```
print sum
```

### 0x04 Base40

题目如下：

## Base40

(solver: 83)

给你一串16进制让你玩玩

666c61677b4a7573745f743373745f683476335f66346e5f686168615f36363636217d

直接 16 进制转字符串获得 flag

### 0x05 Base 50

题目如下：

## Base50

(solver: 46)

题目：小明常用密码是hash 是5bc76f3f319865431dcab801bbce47a1 现在 他只知道明文密码的  
前四位是xjnu  
中间是66\*\*\*\*88 后三位是ctf 请帮他算出 明文密码是啥  
flag{明文}

代码如下：

```
import string
```

```
import itertools
```

```
import hashlib
```

```
enc='5bc76f3f319865431dcab801bbce47a1'

code = ''

strlist = itertools.product(string.ascii_letters + string.digits, repeat=4)

for i in strlist:

    code = i[0] + i[1] + i[2] + i[3]

    key='xjnu66'+code+'88ctf'

    encinfo = hashlib.md5(key).hexdigest()

    if encinfo == enc:

        print key

        Break
```

## MISC

### 0x01 Misc10

题目如下：

**Misc10**  
(solver: 40)

微博关注 <https://weibo.com/2218910835/profile?topnav=1&wvr=6>

Auth

关注微博后，私信发送 flag

## 0x02 Misc15

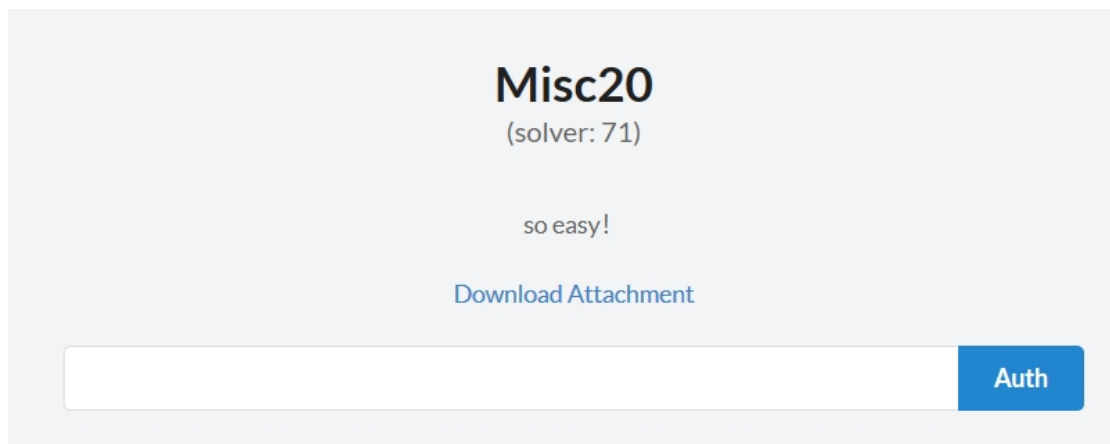
题目如下：



将图片直接右键记事本打开，看到了 flag

## 0x03 Misc20

题目如下：



将下载的 misc10 直接 foremost，分离的图片即为 flag

## 0x04 Misc40

题目如下：

# Misc40

(solver: 69)

想入门 ctf 吗？学 ctf 要仔细。

[Download Attachment](#)

Auth

将下载好的 docx 文件，后缀名改为 zip，解压缩后即可看到以 flag 作为名字的文件夹。

## Crypto

### 0x01 Crypto30

题目如下：

# Crypto30

(solver: 13)

mix?  
http://ctf.xjnu.edu.cn:9900/  
提示：  
确定要登陆吗？

Auth

是一道简单的 rsa：

```
</div>
</body>
<!-- hint m=58768105316148841999777370412186936018625486668532134194761549884510599390592 -->
</html>
```

n 在图片里，e 为图片名，e=3:

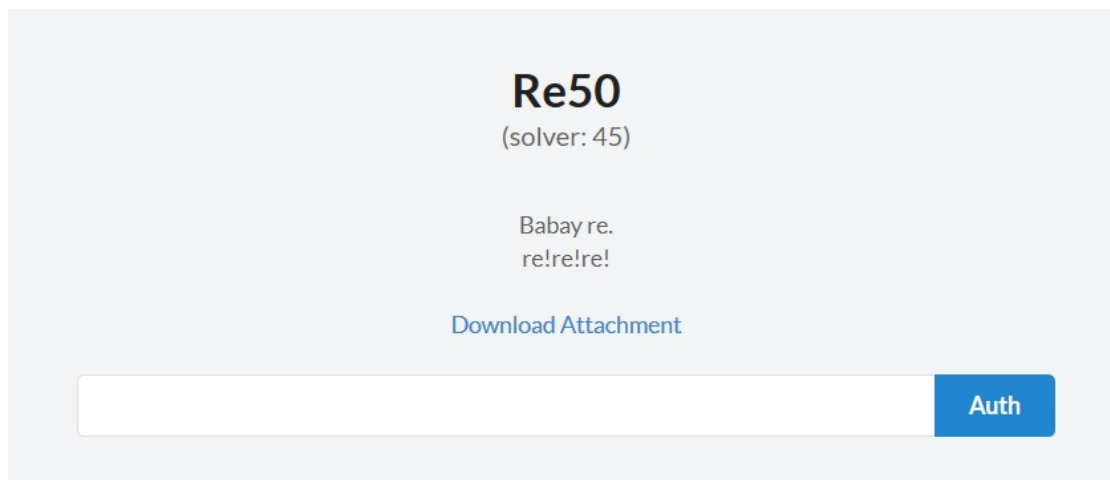
[illegible]

有了  $n, e, c$ , 直接分解  $n$ , 之后求出  $d$ , 最后解出明文

## RE

## 0x01 Re50

题目如下：



直接扔进 IDA，看下字符串：



```

461      mov     ebp, esp
463      and     esp, 0FFFFFF0h
466      sub     esp, 30h
469      call    __main
46E      mov     dword ptr [esp], offset aHiThisIsABabyr ; "Hi~ this is a babyre"
475      call    _printf
47A      mov     byte ptr [esp+2Fh], 66h
47F      mov     byte ptr [esp+2Eh], 6Ch
484      mov     byte ptr [esp+2Dh], 61h
489      mov     byte ptr [esp+2Ch], 67h
48E      mov     byte ptr [esp+2Bh], 78h
493      mov     byte ptr [esp+2Ah], 52h
498      mov     byte ptr [esp+29h], 65h
49D      mov     byte ptr [esp+28h], 5Fh
4A2      mov     byte ptr [esp+27h], 31h
4A7      mov     byte ptr [esp+26h], 73h
4AC      mov     byte ptr [esp+25h], 5Fh
4B1      mov     byte ptr [esp+24h], 53h
4B6      mov     byte ptr [esp+23h], 30h
4BB      mov     byte ptr [esp+22h], 5Fh
4C0      mov     byte ptr [esp+21h], 43h
4C5      mov     byte ptr [esp+20h], 30h
4CA      mov     byte ptr [esp+1Fh], 4Fh
4CF      mov     byte ptr [esp+1Eh], 4Ch
4D4      mov     byte ptr [esp+1Dh], 7Dh
4D9      mov     eax, 0
4DE      leave

```

这个就是 flag