XCTF密码学（入门一）

原创

牛奶糖不甜 于 2020-10-15 21:40:05 发布 438 收藏 2

分类专栏： XCTF：crypto（入门） 文章标签： 密码学

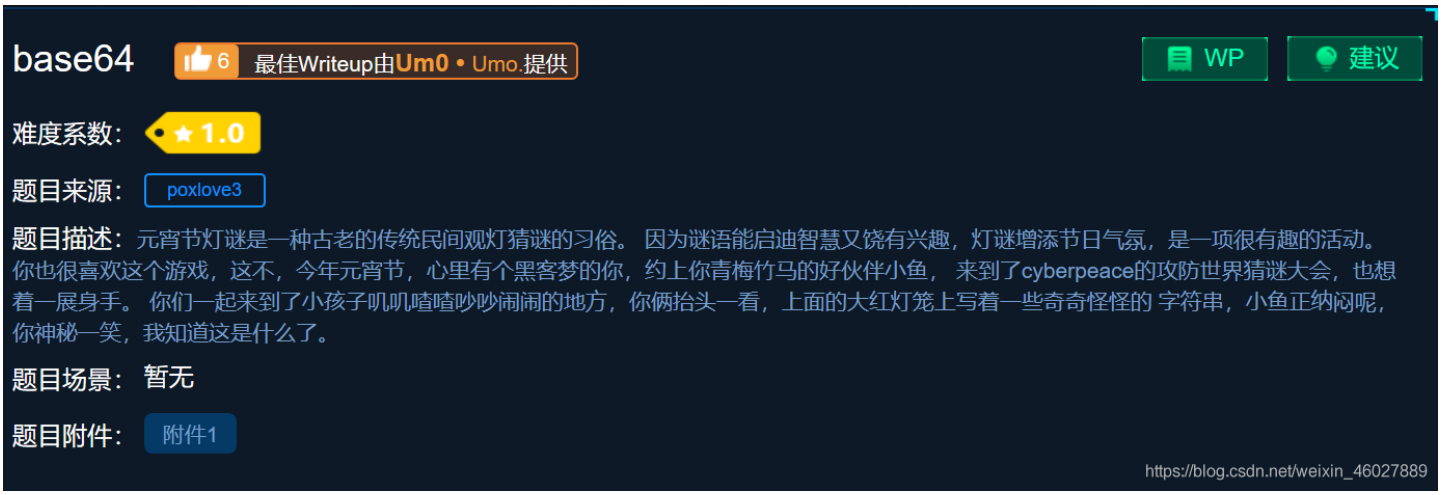
本文链接：https://blog.csdn.net/weixin_46027889/article/details/109104261

XCTF密码学（入门一）

1.1题目：base64

1.2描述：元宵节灯谜是一种古老的传统民间观灯猜谜的习俗。 因为谜语能启迪智慧又饶有兴趣，灯谜增添节日气氛，是一项很有趣的活动。 你也很喜欢这个游戏，这不，今年元宵节，心里有个黑客梦的你，约上你青梅竹马的好伙伴小鱼，来到了cyberpeace的攻防世界猜谜大会，也想着一展身手。 你们一起来到了小孩子叽叽喳喳吵吵闹闹的地方，你俩抬头一看，上面的大红灯笼上写着一些奇奇怪怪的 字符串，小鱼正纳闷呢，你神秘一笑，我知道这是什么了。

1.3附件：Y3liZXJwZWFjZXtXZWxjb21lX3RvX25ld19Xb3JsZCF9



作为xctf新手区的第一道题，极其基础，各位应该都会，我就简单写写。

拿到附件的内容，大佬们应该一眼就能看出这是什么加码了，但萌新可能就有点懵逼了，再回头看看题目，base64，好知道是什么加密了。

百度一下base64，大概知道是一种通过将8位转化为6位来实现3字变4字的移位加密这里推荐线上解密。

地址：http://ctf.ssleye.com/base64.html

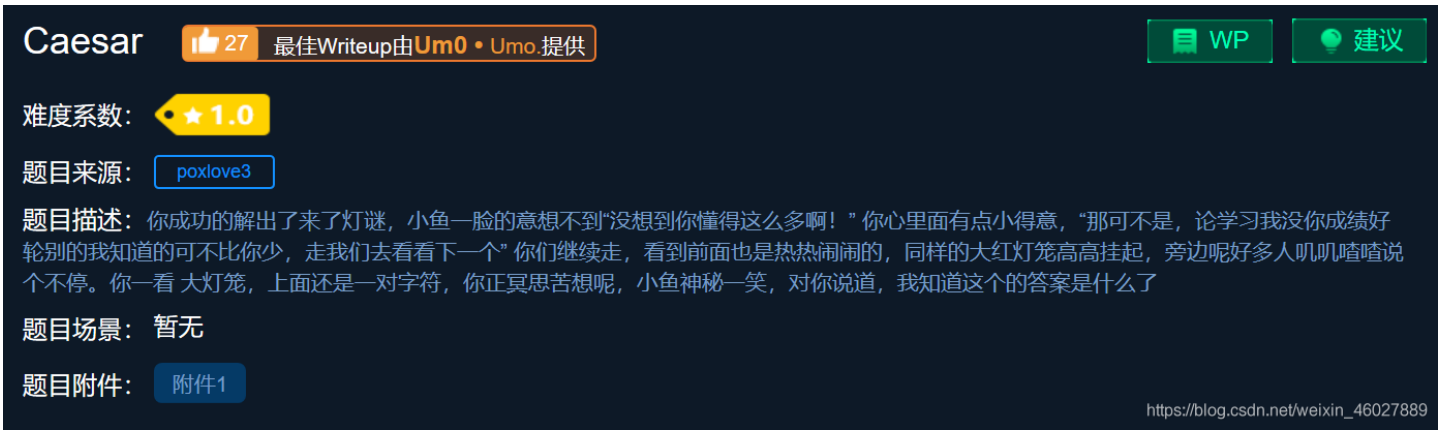
直接copy进去得到flag。

flag：cyberpeace{Welcome_to_new_World!}

2.1题目：Caesar

2.2描述：你成功的解出了来了灯谜，小鱼一脸的意想不到“没想到你懂得这么多啊！”你心里面有点小得意，“那可不是，论学习我没你成绩好轮别的我知道的可不比你少，走我们去看看下一个”你们继续走，看到前面也是热热闹闹的，同样的大红灯笼高高挂起，旁边呢好多人叽叽喳喳说个不停。你一看 大灯笼，上面还是一对字符，你正冥思苦想呢，小鱼神秘一笑，对你说道，我知道这个的答案是什么了

2.3附件：oknqdbqmoq{kag_tmhq_xqmdzqp_omqemd_qzodkbfuaz}



吸取上一次的经验，可以看出，题目翻译过来叫凯撒，再看看附件的内容全部是字母，大小写一致，尾部的字符为'}'可以很明显的猜到这是个简单的字母替换加密，再加上提示可以知道是凯撒密码。同样代入在线工具。

地址：http://ctf.ssleye.com/caesar.html

我们再来看key（0~25），我们可以一个一个试试，当key为12时，得到cyberpeace{you_have_learned_caesar_encryption}很明显这就是flag。

我自己也随便写了个c++放在下面。

```
#include <stdio.h>
void main()
{
 char a[100],b[100];
 int i,n;
 printf("输入密文：");
 gets(a);
 printf("若key为0则穷举：");
 scanf("%d",&n);
 if(n!=0)
 {
  for(i=0;a[i]!='\0';i++)
  {
   if(a[i]>='a'&&a[i]<='z')
   {
    if(a[i]+n>'z')
    {
     a[i]-=26;
     a[i]+=n;
    }
    else
    {
     a[i]+=n;
    }
   }

   if(a[i]>='A'&&a[i]<='Z')
   {
    if(a[i]+n>'Z')
    {
     a[i]-=26;
```

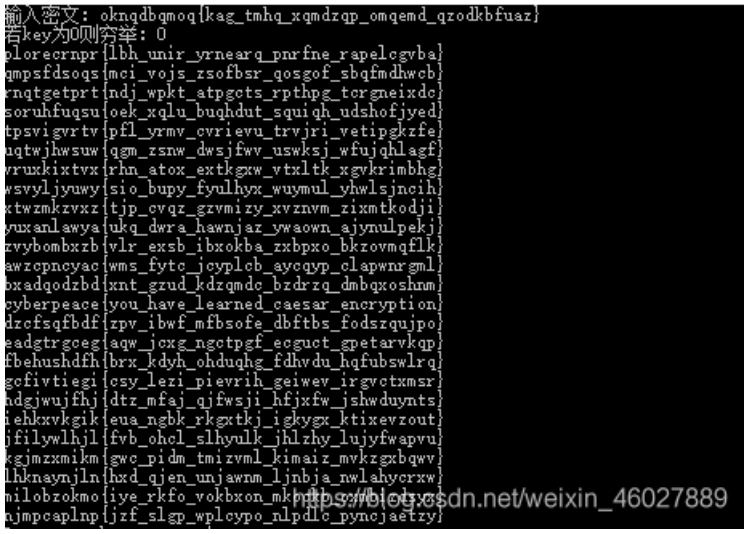
```
    a[i]+=n;
   }
   else
   {
    a[i]+=n;
   }
  }
 }
 puts(a);
}
if(n==0)
{
 for(n=1;n<26;n++)
 {
  for(i=0;a[i]!='\0';i++)
  {
   if(a[i]>='a'&&a[i]<='z')
   {
    if(a[i]+1>'z')
    {

     a[i]-=26;
     a[i]+=1;
    }
    else
    {
     a[i]+=1;
    }
   }

   if(a[i]>='A'&&a[i]<='Z')
   {
    if(a[i]+n>'Z')
    {
     a[i]-=26;
     a[i]+=1;
    }
    else
    {
     a[i]+=1;
    }
   }
  }
  puts(a);

 }
}


}
```

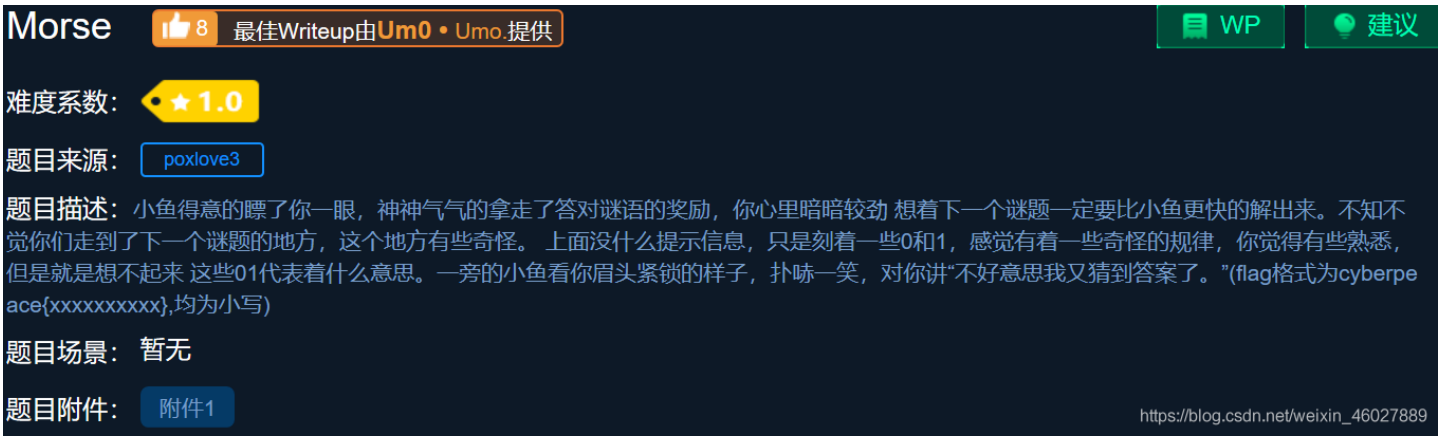


这里教一个小技巧，‘｛’前是oknqdbqmoq刚好10个字母，对照往常经常出现的flag，ctf，xctf…这样的开头，恰好与cyberpeace对应，再将字母o与c联系起来，刚好相差12。

3.1题目： Morse

3.2描述：小鱼得意的瞟了你一眼，神神气气的拿走了答对谜语的奖励，你心里暗暗较劲 想着下一个谜题一定要比小鱼更快的解出来。不知不觉你们走到了下一个谜题的地方，这个地方有些奇怪。 上面没什么提示信息，只是刻着一些0和1，感觉有着一些奇怪的规律，你觉得有些熟悉，但是就是想不起来 这些01代表着什么意思。一旁的小鱼看你眉头紧锁的样子，扑哧一笑，对你讲“不好意思我又猜到答案了。”(flag格式为cyberpeace{xxxxxxxxxx},均为小写)

3.3附件：11 111 010 000 0 1010 111 100 0 00 000 000 111 00 10 1 0 010 0 000 1 00 10 110



老样子，题目是摩斯，猜测是摩斯密码。

丢进解密工具。

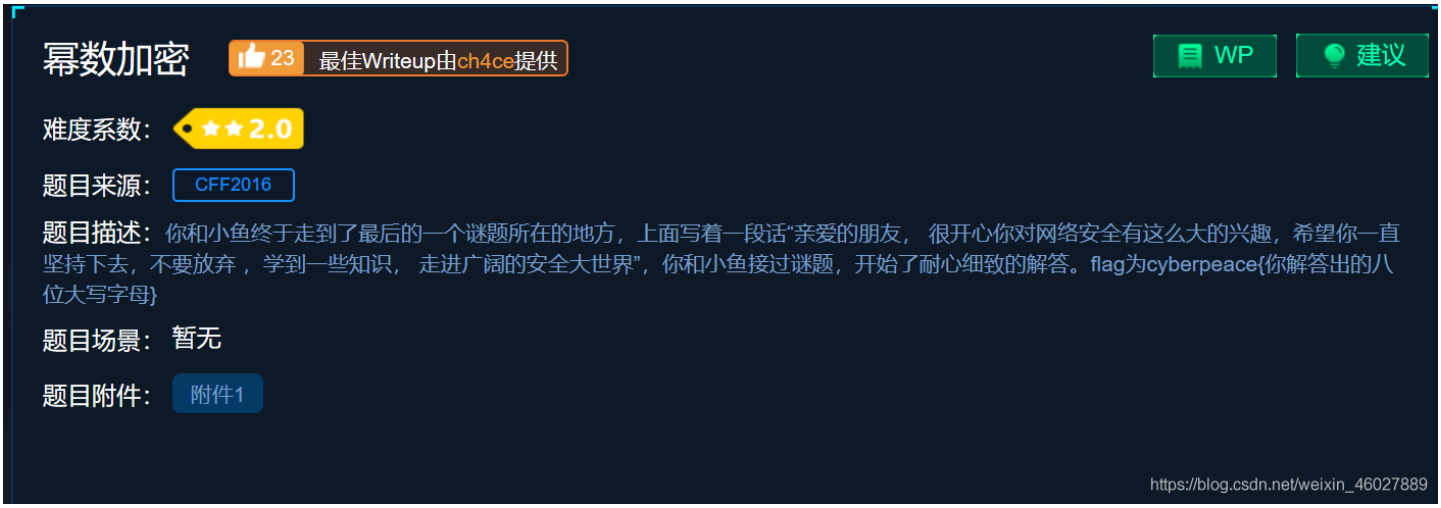
地址：http://ctf.ssleye.com/morse.html

得到morsecodeissointeresting，加上描述的提示上交flag：cyberpeace{morsecodeissointeresting}

4.1题目：幂数加密

4.2描述：你和小鱼终于走到了最后的一个谜题所在的地方，上面写着一段话“亲爱的朋友， 很开心你对网络安全有这么大的兴趣，希望你一直坚持下去，不要放弃 ，学到一些知识， 走进广阔的安全大世界”，你和小鱼接过谜题，开始了耐心细致的解答。flag为cyberpeace{你解答出的八位大写字母}

4.3附件：884210122048022440401422420248012 2



做题之前先百度了解一下什么是二进制幂数加密，经过学习，知道是每个字母以二进制指数形式表现，也就是a是1，b是2，c是3…以此类推，由于大于9的数字不好表示，就将其分解，以W为例子，W是第23位，将23分解为两个8，一个4，一个2，一个1，以0结尾表现为884210.

由此分析附件的内容为WELLDONNE，加上描述的提示，得到flag：cyberpeace{WELLDONE}

下面还有一个大佬写的py脚本，附上blog地址。

```
#! /usr/bin/env python
#coding=utf-8
a="884210122048022440401422420248012 2"
a=a.split("0")
flag=''
for i in range(0,len(a)):
     str = a[i]
     list=[]
     sum=0
     for j in str:
        list.append(j)
        length = len(list)
     for k in range(0,length):
        sum+=int(list[k])
     flag+=chr(sum+64)
print flag
```

博客地址：https://blog.csdn.net/An_Mei_Ying/article/details/89460565

先就写四题，之后的再继续。