Crypto日记之利用CyberChef解png图片xor难题

原创

Sm0ry 已于 2022-03-10 00:25:51 修改 1349 收藏 2
分类专栏： Crypto日记 文章标签： 安全 算法
于 2022-03-10 00:24:25 首次发布

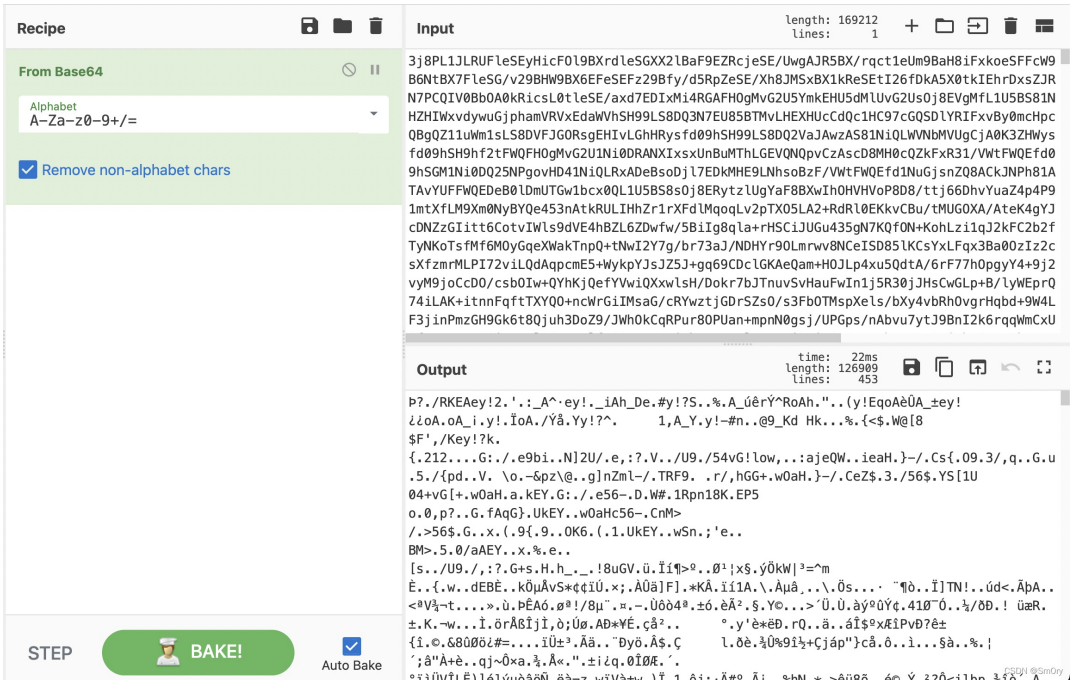
今天晚上在刷题时发现了两道png图片加密的题目，都是xor，发现用CyberChef都能秒出，下面把解题过程整理下。

第一题：攻防世界Crypto sleeping-guard

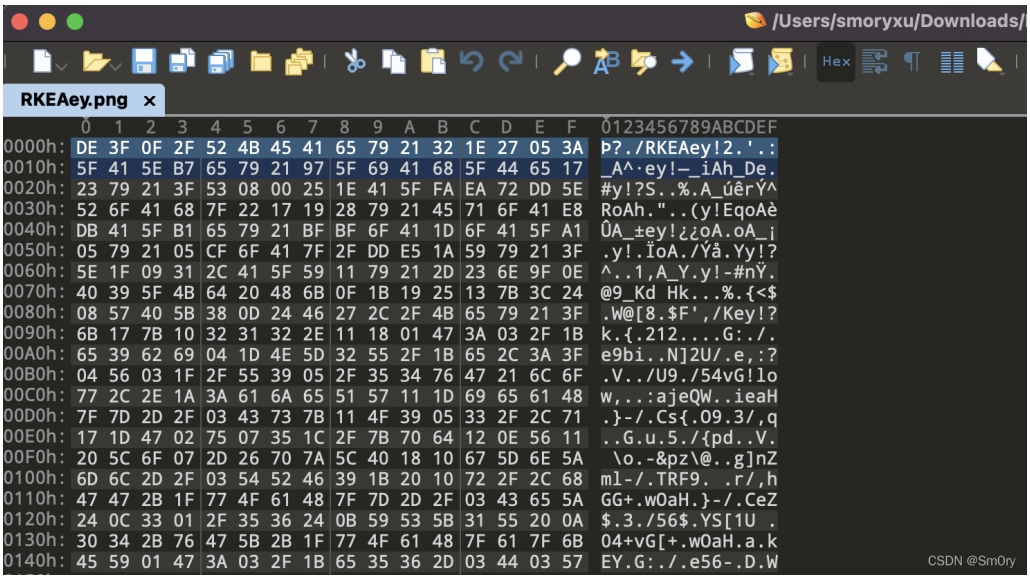
题目来源： csaw-ctf-2016-quals

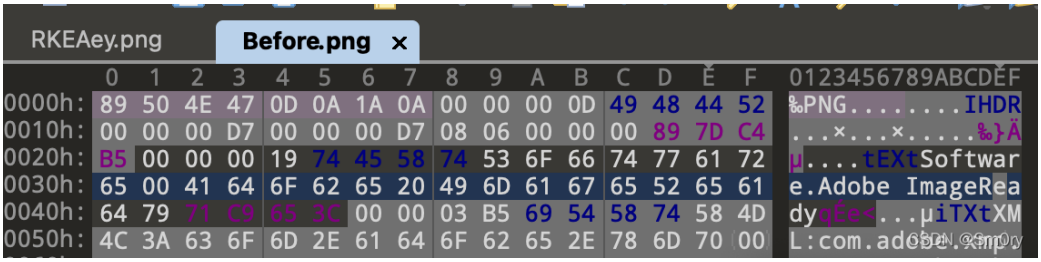
题目描述：只有真正的hacker才能看到这张图片。（据说原题是有个py的代码，包含key的长度。）

题目场景给了ip和端口，直接用nc连接发现一长串编码，这么长串的编码，先from base64一波：



output是一段乱码，不过好像看到了RKEAey连续的字符，就像是%PNG这样的字符，不管怎样先保存成png后缀的图片，就保存为RKEAey.png吧。010打开看一下，并对比一下png的文件头：



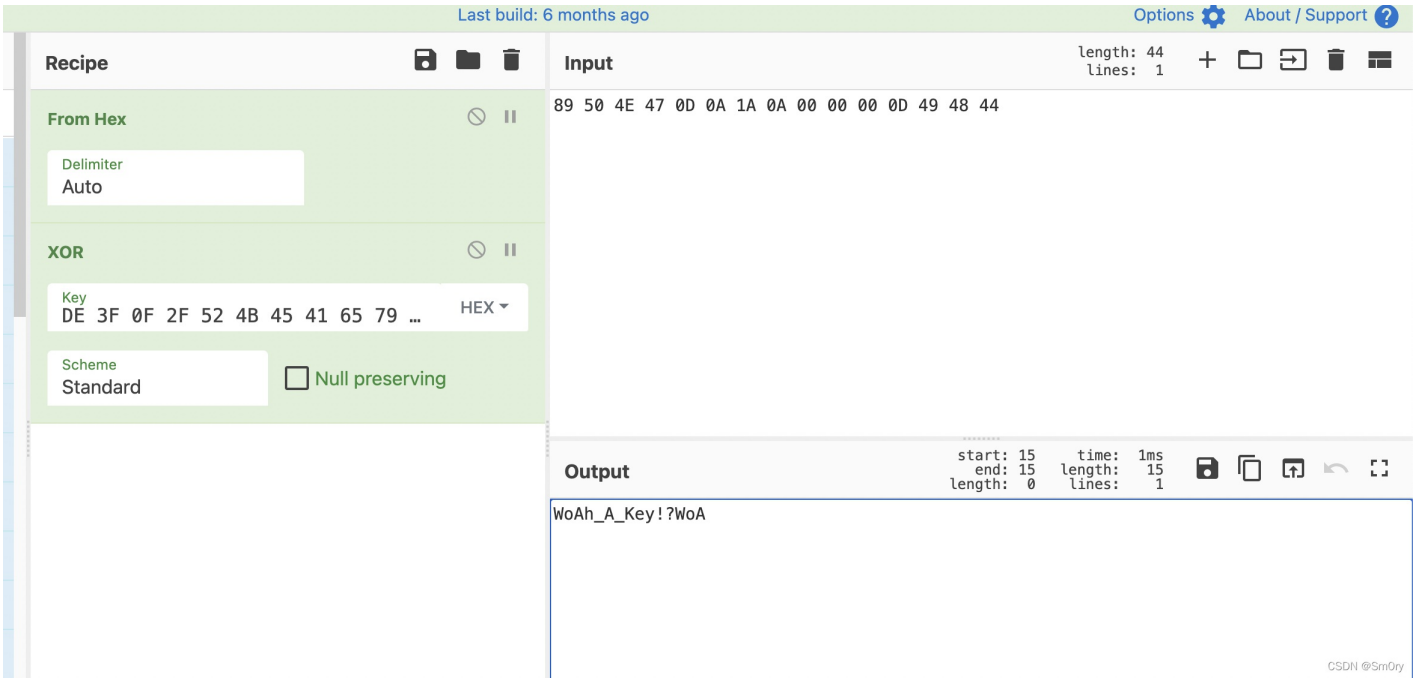


misc的题解多了应该对png头很熟悉，具体的头包含哪些内容这里就不详解释了， 感兴趣的可以搜一搜。

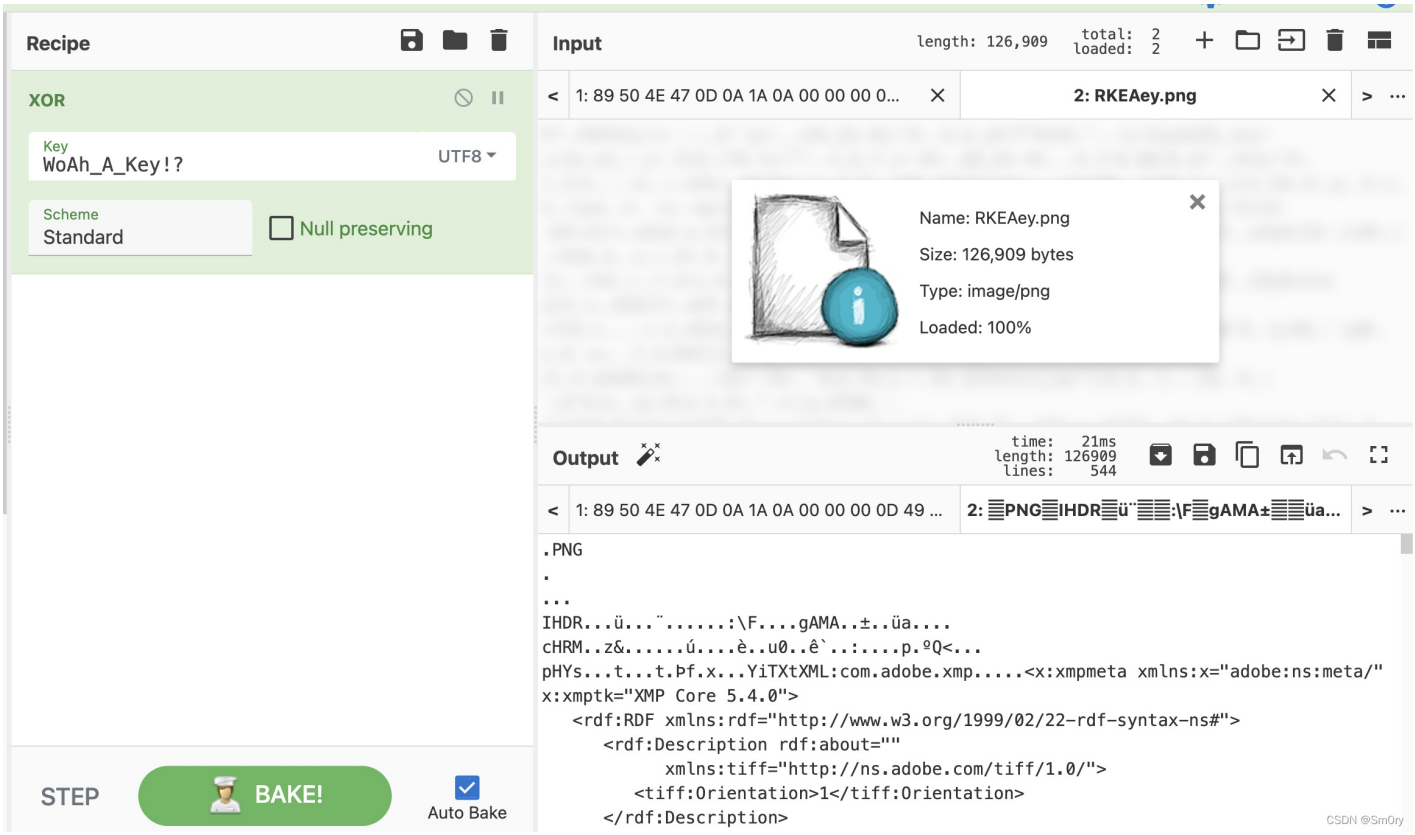
这里要说明的是png文件头的前16位是固定的 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52，那么可以根据png加密后的前16位来异或出key的值，如果key是一段有意思的字符串就很容易辨别出来。

本题png加密后的前16位为：DE 3F 0F 2F 52 4B 45 41 65 79 21 32 1E 27 05 3A

接下来就轮到神器CyberChef了，将固定长度的原文和cypher异或，就能得到key，这里我们把前16位全部放进去，input先From Hex，再XOR Cipher，就可以得到key，因为是循环xor，所以key应该是WoAh_A_Key!?，刚好12位：



解到这里得出了key，再利用CyberChef对整个加密的png文件作xor，得到原文件：



惊喜，看到png的文件头了吗？保存下来就得到了flag：

第二题：攻防世界Crypto beginners-luck

题目来源： bitsctf-2017

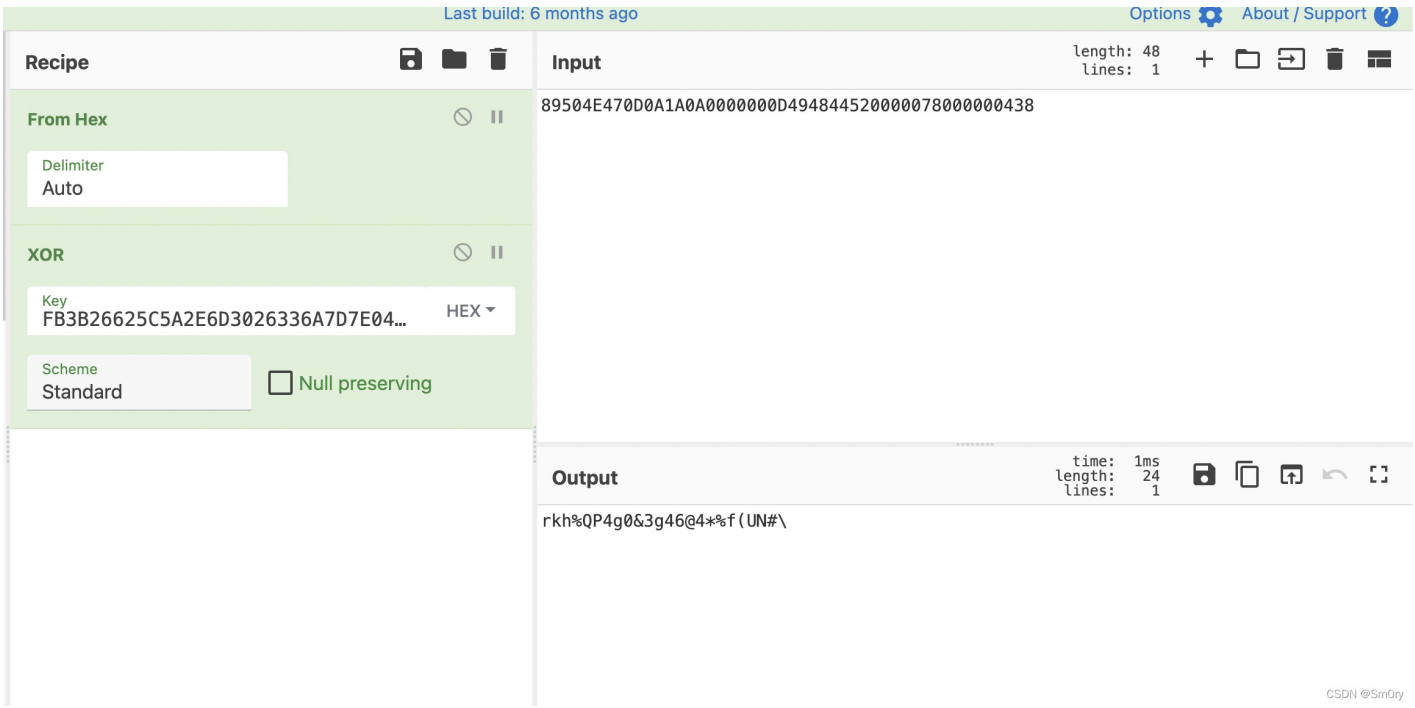
这道题跟上面这道题差不多，并给了加密png的脚本：

```
#!/usr/bin/env python

def supa_encryption(s1, s2):
    res = [chr(0)]*24
    for i in range(len(res)):
        q = ord(s1[i])
        d = ord(s2[i])
        k = q ^ d
        res[i] = chr(k)
    res = ''.join(res)
    return res

def add_pad(msg):
    L = 24 - len(msg)%24
    msg += chr(L)*L
    return msg

with open('fullhd.png','rb') as f:
    data = f.read()

data = add_pad(data)


with open('key.txt') as f:
    key = f.read()

enc_data = ''
for i in range(0, len(data), 24):
    enc = supa_encryption(data[i:i+24], key)
    enc_data += enc

with open('BITSCTFfullhd.png', 'wb') as f:
    f.write(enc_data)
```

看了脚本大概明白这题是利用一个长度为 24 的 key 循环异或原图，得到一个一堆乱码的png。上面那题的key长度是12位，这题的key是24位。

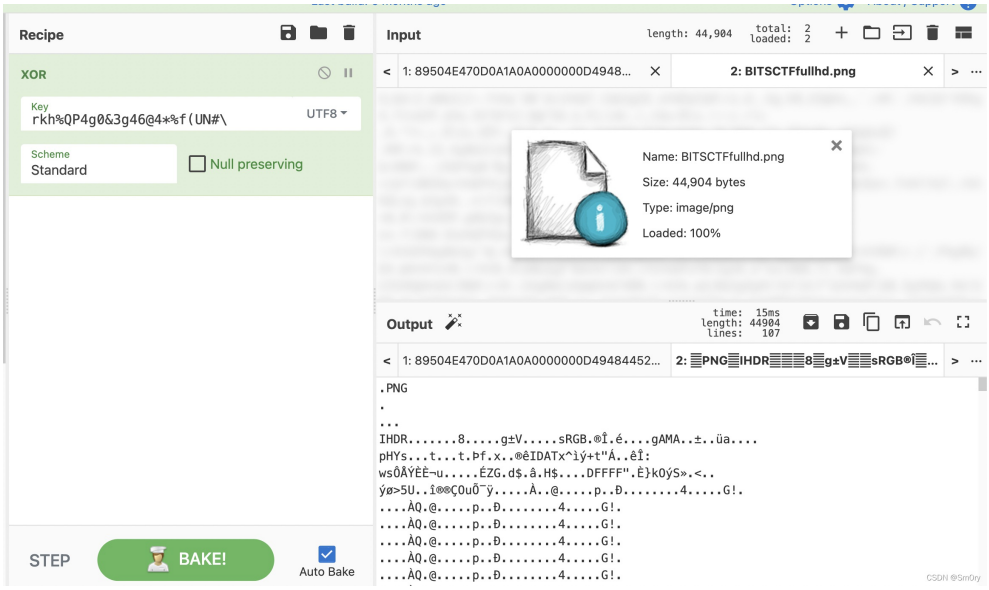
而png文件头前16位是固定的，再后面8位就是图片的长和宽，根据信息可以得到图片的尺寸是1920x1080，那么就可以得到原图的前24位固定值：89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 07 80 00 00 04 38；

BITSCTFfullhd.png也就是加密后的png前24位为：FB 3B 26 62 5C 5A 2E 6D 30 26 33 6A 7D 7E 04 66 2A 25 61 A8 55 4E 27 64；



利用 CyberChef很快得到key为：rkh%QP4g0&3g46@4*%f(UN#\

再利用key还原图片：



保存下来就是flag了：