攻防世界 Crypto高手进阶区 6分题 beginners-luck

原创

思源湖的鱼 于 2021-01-23 21:15:58 发布 303 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 crypto

本文链接：https://blog.csdn.net/weixin_44604541/article/details/113051721

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的6分题

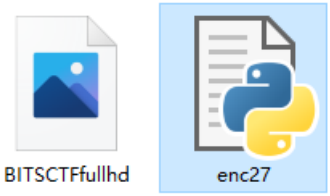
本篇是beginners-luck的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

得到一张图片和一段python



```python
#!/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)
```

用一个长度为 24 的 key 循环异或fullhd.png的字节流
进行加密得到BITSCTFfullhd.png

那就是要想办法得到key

考虑png的文件头

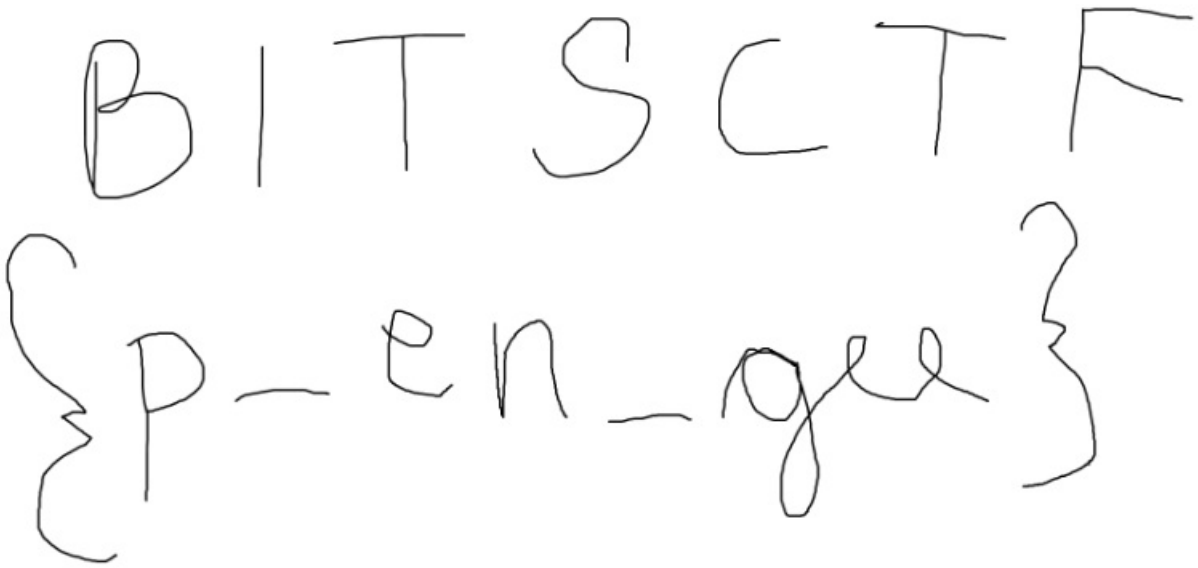
- `89 50 4e 47 0d 0a 1a 0a` 是固定文件头
- 接下来是关键数据块：`00 00 00 0d` 表示数据块长度为13，这个不会变；`49 48 44 52` 是 IHDR 标识，这个也是死的；接下来 8 位，前 4 位是宽，后 4 位是高；最后 5 位中，第一位是色深，第二位是颜色类型，接下来一般都是三个 00
- 在关键数据块后还有 4 位 CRC 校验码

可以看到，前 24 位中只有宽和高的 8 位不是死的
又长宽可以根据图片信息得到1920x1080
那就可以得到key了

脚本

```
plain ="89504E470D0A1A0A0000000D49484452000000780000000438".decode("hex")

enc = "FB3B26625C5A2E6D3026336A7D7E04662A2561A8554E2764".decode("hex")


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



key = supa_encryption(plain, enc)

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

data = add_pad(data)

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

with open('fullhd.png', 'wb') as f:
    f.write(dec_data)
```

得到图片



得到flag

结语

关键是png的文件头