攻防世界 Misc高手进阶区 2分题 Ditf

原创

思源湖的鱼 于 2020-10-17 16:06:21 发布 290 收藏 1

分类专栏： ctf 文章标签： misc 攻防世界 ctf 图片隐写 网络安全

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109134244

前言

继续ctf的旅程

攻防世界Misc高手进阶区的2分题

本篇是Ditf的writeup

发现攻防世界的题目分数是动态的

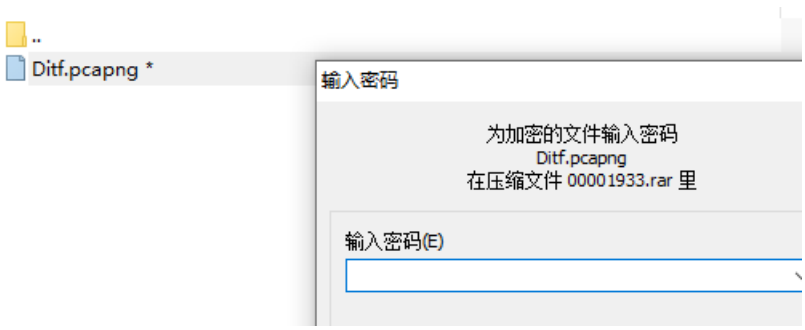
就仅以做题时的分数为准了

解题过程

下下来一个png

扔进stegsolve
没东西

foremost
得到一个rar



解压要密码
试了下不是伪加密
archpr爆破失败

那应该是要到png里去找了

查了查

- PNG文件图像头部不止是文件类型的标识；还包含了长度、高度以及校验值
- 通常情况下，一个图像的产生，就会被赋予各种文件头部信息；
- 一般情况下图像刚产生的时候，长宽高等信息会被校验，产生一个值X1
- 如果这个图象被修改了，有可能产生图像无法打开或者显示不全，校验值被修改为X2；
- 使用TWeakPNG去校验的时候，通过长宽高算出来的校验值是X1跟现在的X2不一致，产生报错。
- 高度值被修改，通过错误的长宽高，算出错误的校验值X3（Winhex 第二行前四个字节为宽度，4-7字节为高度，最后三个字节以及第三行第一字节为CRC校验值），如果计算出来的值报错，那一定是被篡改过

用TWeakPNG计算CRC值，先尝试修改图片CRC值，查看图片，如果没有出现flag，再尝试改变高度值

修改高度

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR
00000010	00	00	03	9E	00	00	05	4C	08	02	00	00	00	38	16	5A	ž L 8 Z
00000020	34	00	00	00	09	70	48	59	73	00	00	0B	13	00	00	0B	4 pHYs

StRe1izia

得到密码`StRe1izia`

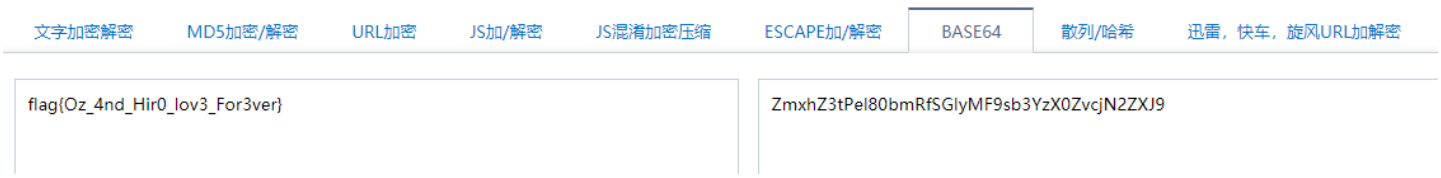
wireshark分析流量包
搜索flag无果
试试其他关键词
在搜索png时
发现kiss.png

```
Content-Encoding: gzip
Content-Length: 177
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  </head>
  <body>
        <img src="/kiss.png" />
  ZmxhZ3tPel80bmRfSGlyMF9sb3YzX0ZvcjN2ZXJ9
  </body>
</html>

GET /kiss.png HTTP/1.1
Host: 123.206.131.120
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTM
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: http://123.206.131.120/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```


得到一串字符

```
ZmxhZ3tPel80bmRfSGlyMF9sb3YzX0ZvcjN2ZXJ9
```

base64解码



得到flag

结语

知识点

- 图片隐写里修改高度
- foremost分离文件
- wireshark分析流量
- base64