

2021宁波市第四届网络安全大赛——预赛

原创

base呗 于 2021-05-24 19:41:29 发布 426 收藏

分类专栏: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_52805837/article/details/117196730

版权



[CTF 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

2021宁波市第四届网络安全大赛——预赛部分wp

简单的php

找到一个flag.php

```
3.p\  
1.p\  
flag.php  
exec.php  
index.php
```

直接cat一下flag.php就可以了

```
?1=echo `cat flag.php`;
```

```
HackBar Elements Console Sources Network  
***<!--?php  
$flag="flag{e0c256f9598f72dc1e6172082173636d}";  
--> == $0  
<html>  
<head></head>
```

getflag

直接在链接后面加上 /flag.php



https://blog.csdn.net/weixin_52805837

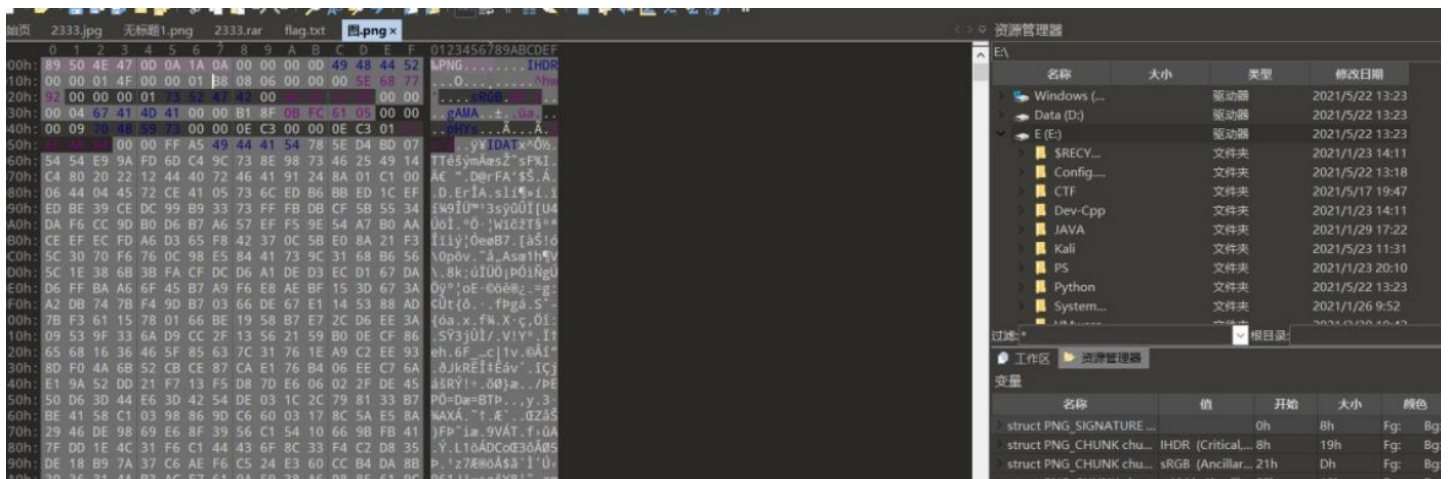
美丽的小姐

下载后得到文件
解压得到图片



https://blog.csdn.net/weixin_52805837

使用010暂无发现



Hex dump and metadata for a PNG file. The hex dump shows the signature and header bytes. The metadata table lists the structure of the PNG chunks.

名称	值	开始	大小	颜色	注释
struct PNG_SIGNATURE ...	0h	8h	Fg: Bg		
struct PNG_CHUNK chu... IHDR (Critical...	8h	19h	Fg: Bg		
struct PNG_CHUNK chu... sRGB (Ancillar...	Dh	Fg: Bg			
struct PNG_CHUNK chu... qAMA (Ancill...	10h	Fg: Bg			

https://blog.csdn.net/weixin_52805837

经过多次尝试得到结论：改高度

Hex dump showing a modified PNG header. The IHDR chunk height field is highlighted in orange (0A).

```

: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52
: 00 00 01 4F 00 00 0A B8 08 06 00 00 00 5E 68 77
: 92 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00
: 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00
: 00 09 70 48 59 73 00 00 0E C3 00 00 0E C3 01 C7
: 6F A8 64 00 00 FF A5 49 44 41 54 78 5E D4 BD 07
: 54 54 E9 9A FD 6D C4 9C 73 8E 98 73 46 25 49 14
: 64 80 20 22 12 44 40 72 46 41 81 24 8A 01 C1 00
  
```

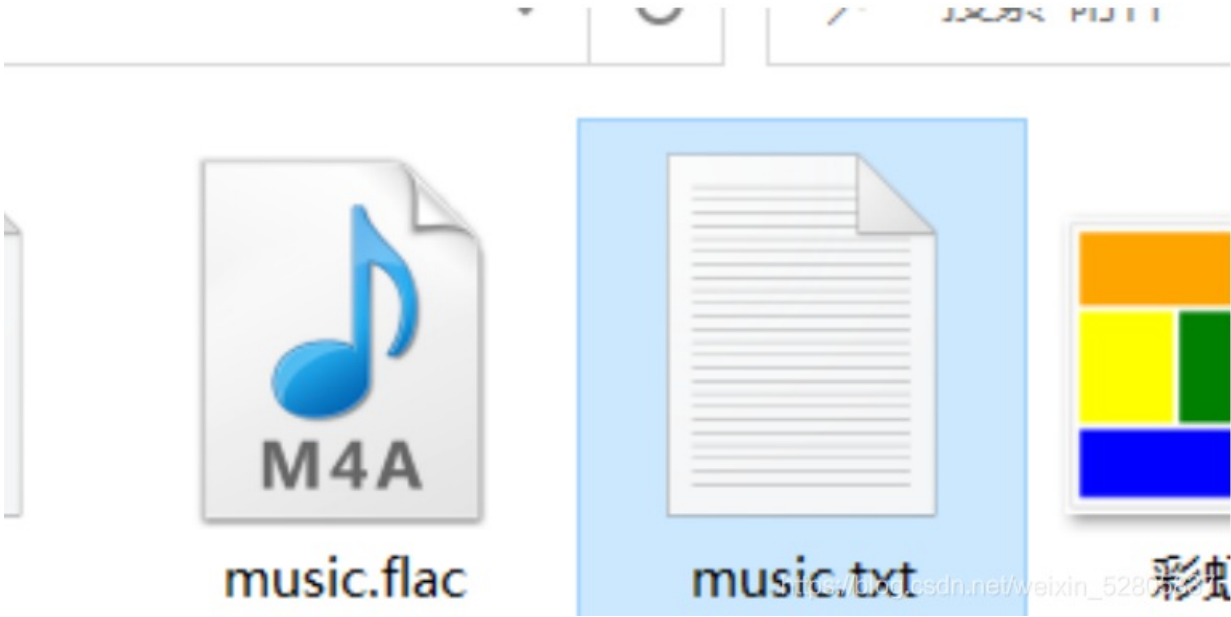
https://blog.csdn.net/weixin_52805837

另存为后得到flag

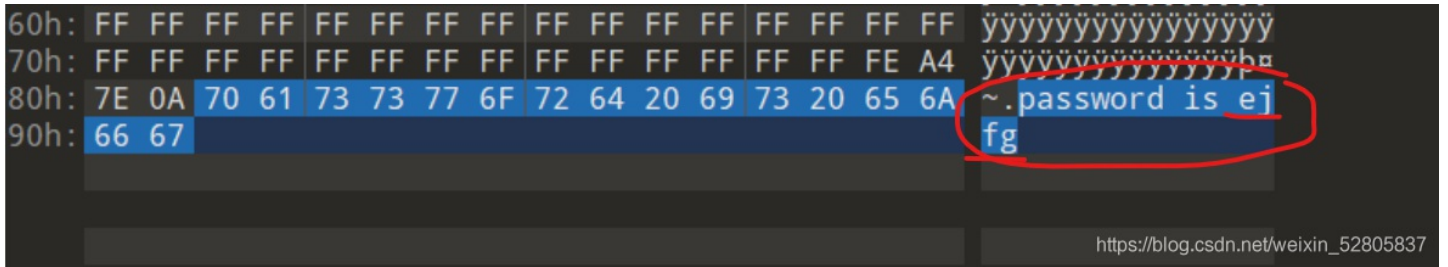


音乐和乐谱

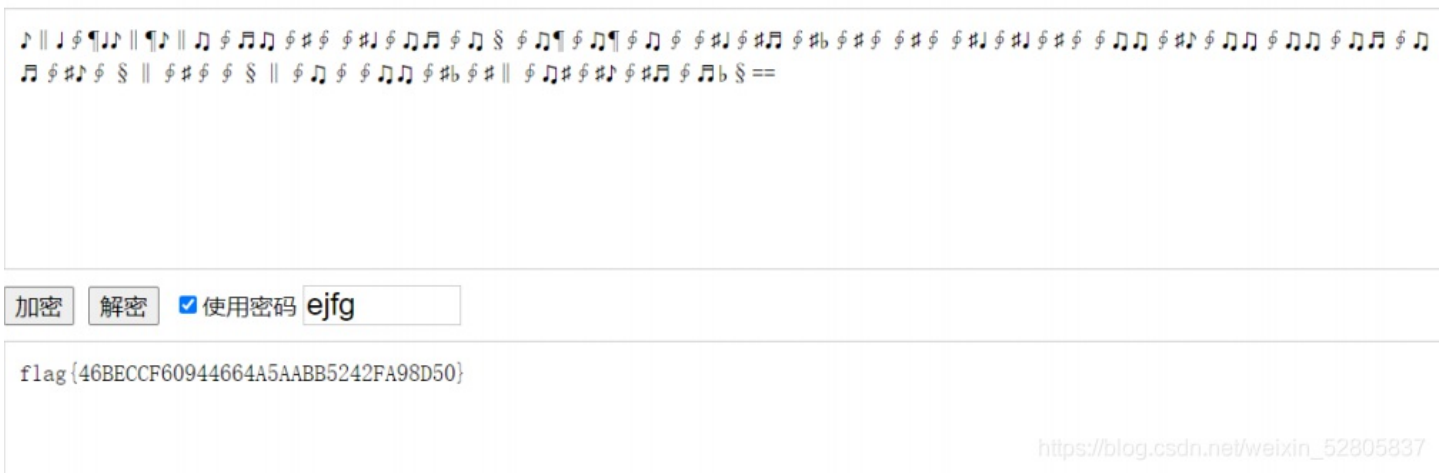
下载得到压缩包
解压得到 txt 和 flac



使用 010 查看，在 flac 末尾发现 password



Txt 中为音符加密的密文，使用发现的 password 解密，得到 flag



听雨寻知音

010看了一下又一个png头
foremost分离出一个二维码



然后ps一下，p成完整二维码之后

扫码得到

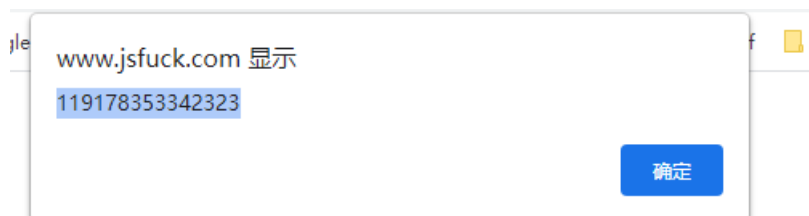
听雨寻知音
滴滴答滴滴答滴滴滴答滴答滴
滴答滴滴答答滴滴滴滴滴答答答滴答
小雨落在栅栏处，只求一位有缘人

http://t.cn/RyJceglccsnei/wzalxi0_52008227

推断为摩斯密码再转栅栏解密
可是无法推断摩斯密码的空格，导致无法得出最终答案

简单编码

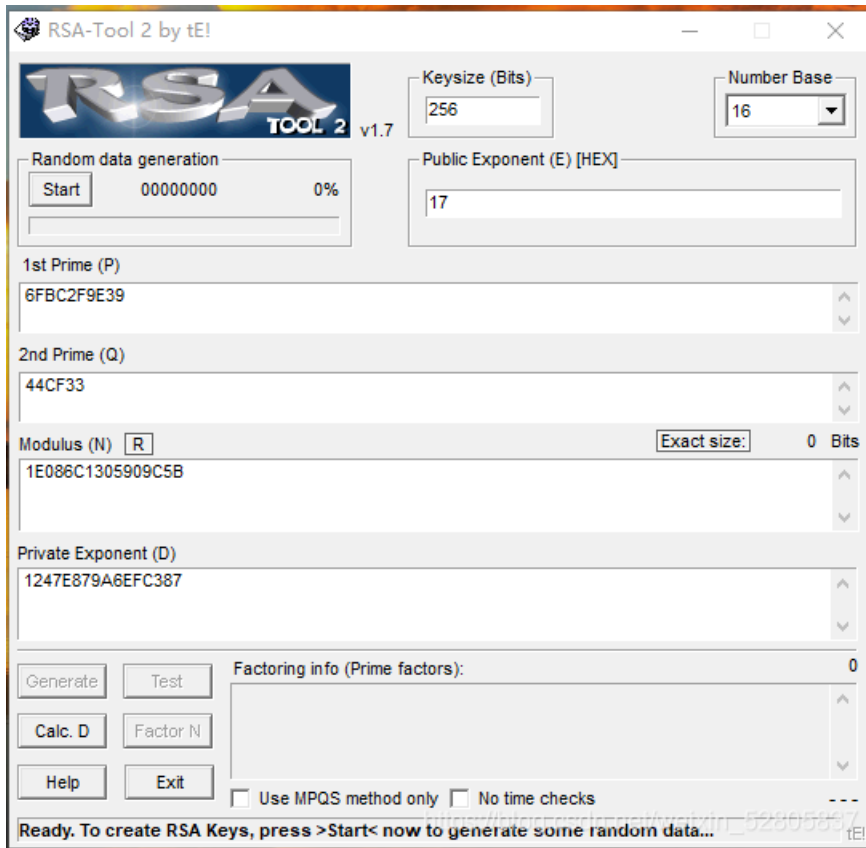
jsfuck，在火狐控制台运行一下是这个



Rsa

利用txt给的参数

使用rsa-tool



再转md5解密



MD5在线加密

要加密的字符串: 1247E879A6EFC387

加密

字符串	1247E879A6EFC387
16位 小写	2737ac1ec3640f85
16位 大写	2737AC1EC3640F85
32位 小写	479a4d532737ac1ec3640f85e375b659
32位 大写	479A4D532737AC1EC3640F85E375B659

得到flag。