

# 攻防世界 Misc高手进阶区 6分题 Wireshark

原创

[思源湖的鱼](#) 于 2021-01-20 17:12:31 发布 332 收藏

分类专栏: [ctf](#) 文章标签: [ctf](#) [攻防世界](#) [misc](#)

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\\_44604541/article/details/112862469](https://blog.csdn.net/weixin_44604541/article/details/112862469)

版权

## CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

### 前言

继续ctf的旅程

攻防世界Misc高手进阶区的6分题

本篇是Wireshark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

得到一个流量包

打开看得眼花

先关注http

一个个追踪

先看到一个网站 [tools.jb51.net/aideddesign/img\\_add\\_info](https://tools.jb51.net/aideddesign/img_add_info)

```
GET /aideddesign/img_add_info HTTP/1.1
Host: tools.jb51.net
User-Agent: curl/7.54.0
Accept: */*
```

```
HTTP/1.1 200 OK
Date: Thu, 17 Jan 2019 03:02:06 GMT
Content-Type: text/html
Server: Microsoft-IIS/7.5
X-Powered-By: PHP/5.2.17
X-Powered-By: ASP.NET
Content-Length: 25177
Age: 1
X-Via: 1.1 PSzjlssx4gj230:4 (Cdn Cache Server V2.0), 1.1 PSzqwtxz3xa52:4 (Cdn Cache Server V2.0), 1.1 twangt84:1 (Cdn Cache Server V2.0)
Connection: keep-alive
```

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

访问发现是在线图片加密解密工具

猜测可能是一道图片解密题

The screenshot shows a network traffic analysis tool interface. The top part displays a list of network packets with columns for time, source IP, destination IP, protocol, and details. The bottom part shows a detailed view of a response packet, including headers like Content-Disposition and Content-Type, and a tree view of the PNG image data structure, including the IHDR header and ancillary chunks.

Time	Source IP	Destination IP	Protocol	Details
900	17.579157	172.25.52.32	HTTP	1226 POST / HTTP/1.1 (PNG)
960	17.877803	58.218.211.182	HTTP	656 HTTP/1.1 200 OK (json)
1008	19.053301	172.25.52.32	HTTP	891 GET /ddc891b23147ba21 HTTP/1.1
1018	19.165516	124.165.219.107	HTTP	1151 HTTP/1.1 200 OK (text/html)
1047	19.243238	172.25.52.32	HTTP	545 GET /674874/7782abccd820677fs.png HTTP/1.1
1051	19.279170	59.53.95.184	HTTP	329 HTTP/1.1 304 Not Modified
1056	19.293911	172.25.52.32	HTTP	901 POST /?c=User&a=getmessnum HTTP/1.1

Content-Disposition: form-data; name="file"; filename="upload.png"\r\n  
Content-Type: image/png\r\n\r\n\r\n  
▼ Portable Network Graphics  
  PNG Signature: 89504e470d0a1a0a  
  ▼ Image Header (IHDR)  
    Len: 13  
    Chunk: IHDR  
    ..0. .... = Ancillary: This is a CRITICAL chunk  
    .... ..0. .... = Private: This is a PUBLIC chunk  
    .... ..0. .... = Safe To Copy: This chunk is NOT safe to copy  
    Width: 1600

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

发现一个图片

导出来



[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

猜测图片隐藏了一个key或什么的

一番尝试后  
扔进winhex  
修改高度

```
00000000 | 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 | %PNG          IHDR
00000016 | 00 00 06 40 00 00 04 20 08 06 00 00 00 7B C0 AE | @             (A@
00000032 | 5A 00 00 0C 14 69 43 43 50 49 43 43 20 50 72 6F | Z             iCCPICC Pro
00000048 | 66 69 6C 65 00 00 48 89 95 57 07 58 53 C9 16 9E | file H%•W XŠÉ ž
00000064 | 5B 52 08 09 2D 10 01 29 A1 37 41 8A 74 E9 BD 08 | [R - ) ; 7AŠté%
00000080 | 48 07 1B 21 09 49 28 11 12 82 8A 1D 59 54 70 2D | H ! I( , Š YTp-
```



key:57pmYyWt

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

得到一个key: 57pmYyWt

继续翻  
又找到一个图片

3912	33.355321	124.165.219.107	172.25.52.32	HTTP	74	HTTP/1.1	200	OK	(text/html)
5227	34.540501	59.53.95.184	172.25.52.32	HTTP	1280	HTTP/1.1	200	OK	(PNG)

Portable Network Graphics  
PNG Signature: 89504e470d0a1a0a  
> Image Header (IHDR)  
> Image data chunk (IDAT)  
v Image data chunk (IDAT)  
Len: 8192  
Chunk: IDAT  
..0. .... = Ancillary: This is a CRITICAL chunk  
.... ..0. .... = Private: This is a PUBLIC chunk  
.... ....0. .... = Safe To Copy: This chunk is NOT safe to copy  
Data  
CRC: 0xc59f9a

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

导出  
去前面找到的网站解密  
这里有点坑的是  
直接导出的图片无法解密  
得扔进winhex处理下文件头和文件尾使之成为标准png

1. 从电脑中选择一张带有隐藏信息的图片:  2.png

2. 输入需要解开信息的密码 (如果没有密码可以不填):

图片中隐藏的信息为: flag+AHs-44444354467B5145576F6B63704865556F32574F6642494E37706F6749577346303469526A747D+AH0-

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

得到 flag+AHs-44444354467B5145576F6B63704865556F32574F6642494E37706F6749577346303469526A747D+AH0-

hex解码

Hex Encoding

Delimiter  
无 None

[https://blog.csdn.net/weixin\\_44604541](https://blog.csdn.net/weixin_44604541)

得到flag

## 结语

流量里注意http和图片  
图片简单长宽隐写  
图片加密