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

本文链接：https://blog.csdn.net/weixin_44604541/article/details/112862469

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

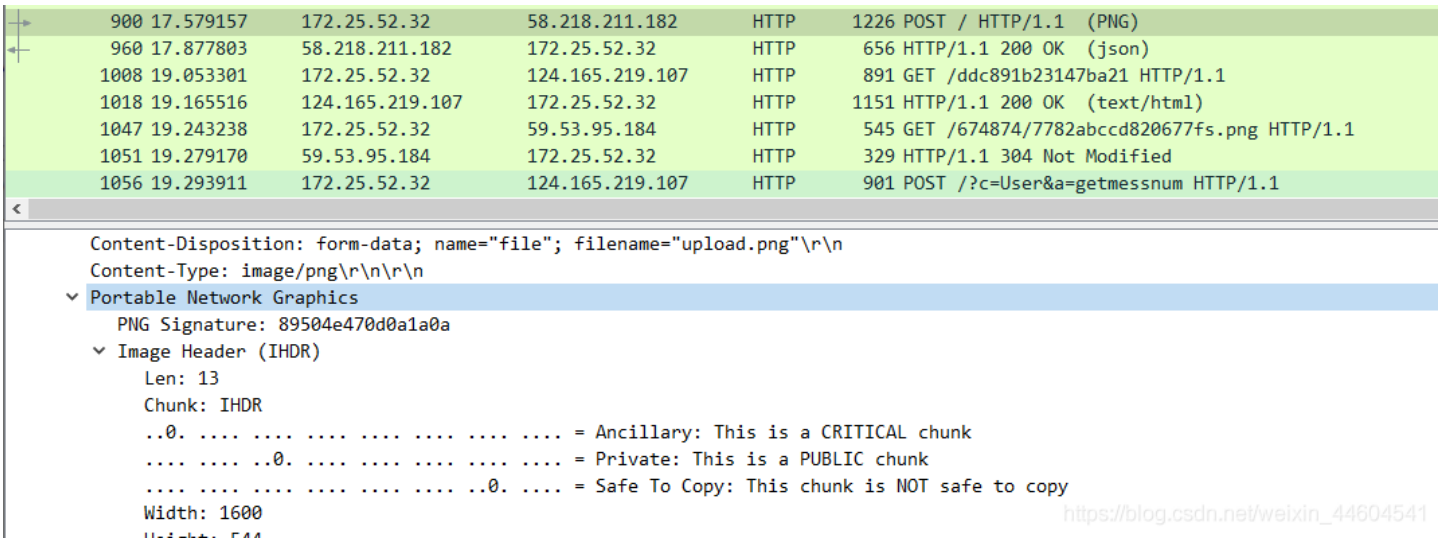
一个个追踪

先看到一个网站`tools.jb51.net/aideddesign/img_add_info`

```
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
```


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



发现一个图片
导出来

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	@ {À®
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 XSÉ ž
00000064	5B	52	08	09	2D	10	01	29	A1	37	41	8A	74	E9	BD	08	[R -)¡7AŠté½
00000080	48	07	1B	21	09	49	28	11	12	82	8A	1D	59	54	70	2D	H ! I(‚Š YTp-

key:57pmYyWt

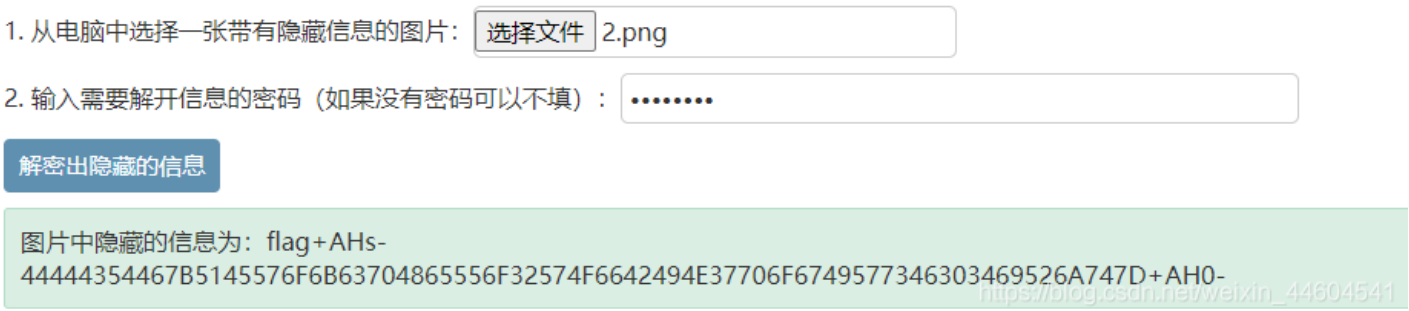
得到一个key：`57pmYyWt`

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: 0xcdc59f9a
```


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



得到`flag+AHs-44444354467B5145576F6B63704865556F32574F6642494E37706F6749577346303469526A747D+AH0-`

hex解码

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