CTF-bugku-misc-[隐写3]-png高度隐写和pngCRC校验

原创

沧海一粟日尽其用 已于 2022-03-08 20:31:44 修改 143 收藏 1

文章标签： web安全 安全

于 2022-03-08 20:22:25 首次发布

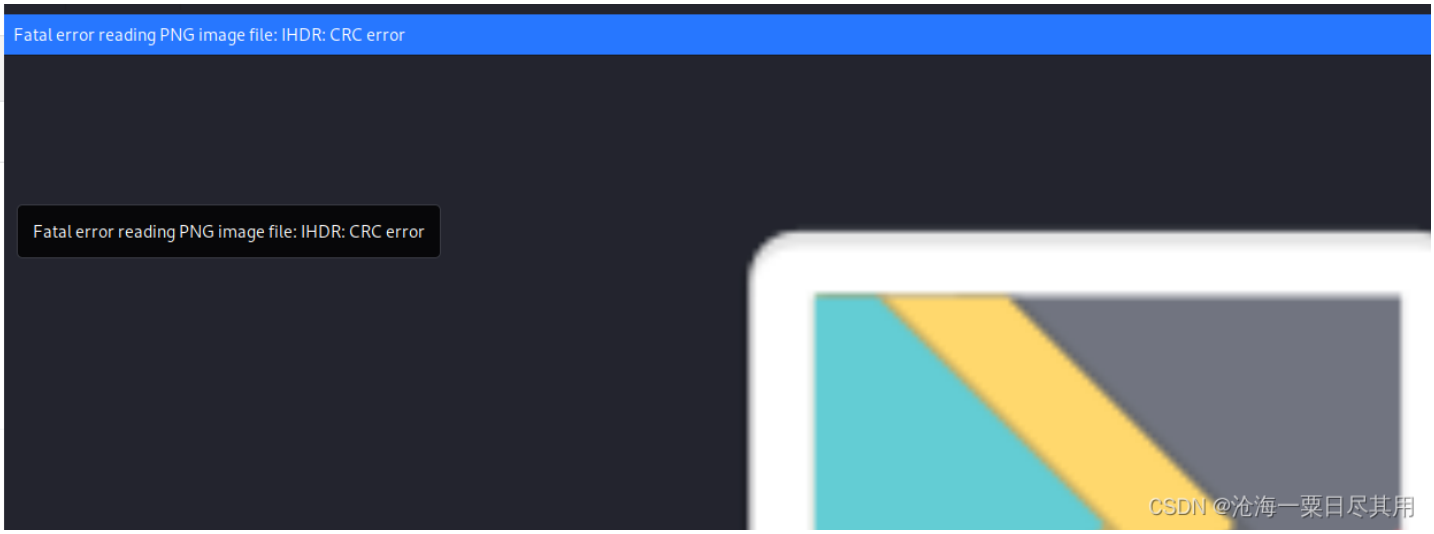
本文链接：https://blog.csdn.net/m0_43405474/article/details/123361993

CTF-bugku-misc-[隐写3]-png高度隐写和pngCRC校验

看很多教程都教直接改高度恢复图片拿到flag，但是我尝试了很久，并不奏效。
特定记录了一下自己探索的过程。

1.题目

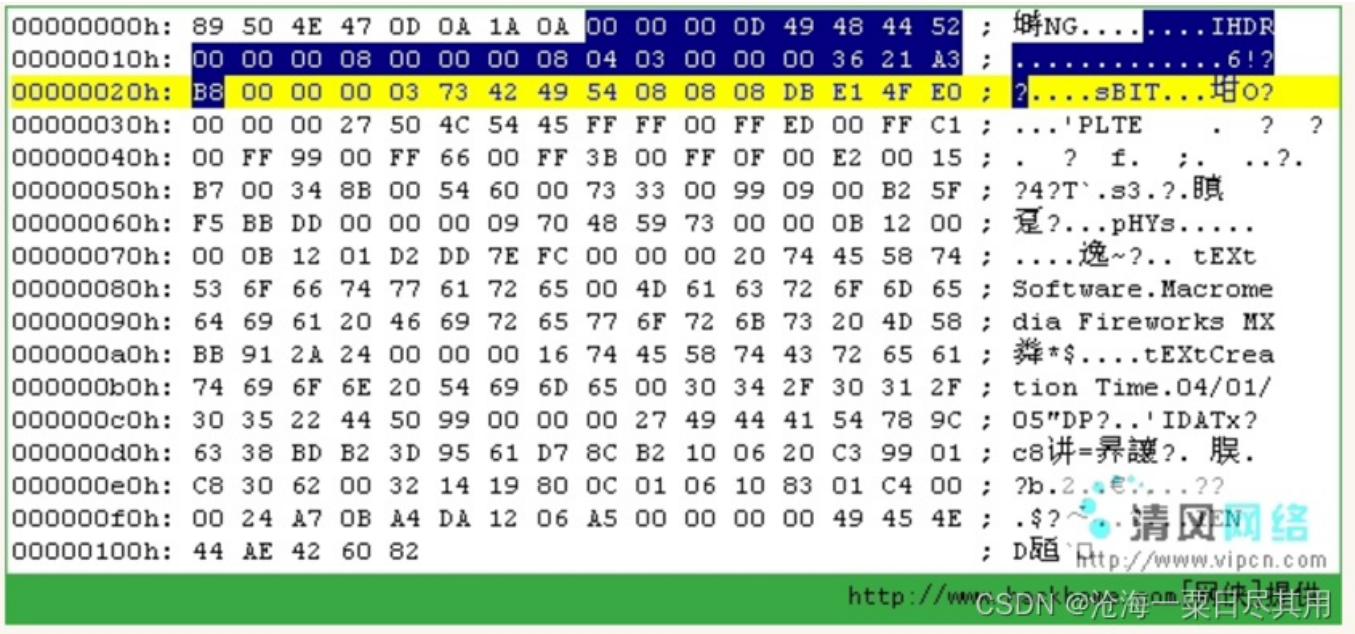
一张名为dabai的png图片，但是不能正常打开。
打开的时候提示CRC校验错误：



思路：恢复图片拿到flag

2.png文件结构分析

首先来详细的分析一下png的存储结构主要关注头部。



(1). png的文件头：8个字节 89 50 4E 47 0D 0A 1A 0A 为 png的文件头(固定)

(2). 4个字节 00 00 00 0D (即为十进制的13)代表头部数据块的长度为13(固定)

(3). 4个字节 49 48 44 52 (即为ASCII码的IHDR)是文件头数据块的标示(IDCH)(固定)

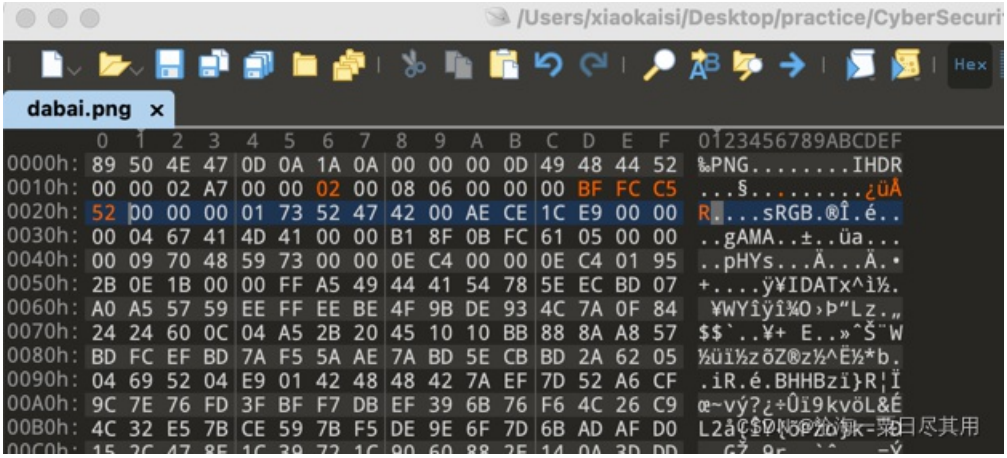
(4). 13位数据块(IHDR)
前四个字节代表该图片的宽 00 00 00 08
后四个字节代表该图片的高 00 00 00 08
后五个字节依次为: Bit depth、ColorType、 Compression method、 Filter method、Interlace method
(可变)

(5). 剩余四字节为该png的CRC检验码 36 21 A3 B8，由从IDCH到THDR的十七位字节进行crc计算得到。(可变)

3.改变图片的高度+CRC校验

这里打开图片的时候CRC校验不过的话，多半是头部出了问题，CRC是由49 48 44 52 + 后面的13个字节共17个字节做CRC校验得到的。改变高度还不行，因为CRC校验依然不正确。

改完高度之后，要重新计算CRC校验码：
http://www.ip33.com/crc.html【工具网址】



总之，高度可以改到足够显示出flag为止，没有固定值，只要保证你改完之后，把相应的CRC值计算出来，填在相应的位置上即可。

4.修复图片获得flag

flag{He1l0_d4_ba1}