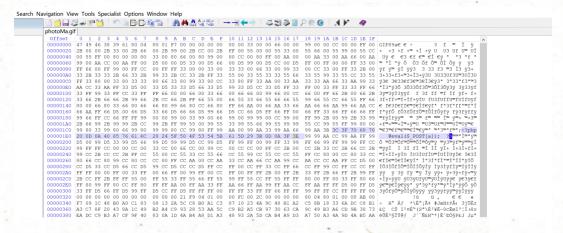
利用前几关相同的方法上传的图片马无法连接,查看代码是由于二次 渲染导致的,如果webshelll在图片中不恰当,则可能重新渲染后 wenshell会消失。

```
00000620 F7 ED F7 DF 80 07 2E F8 E0 84 17 6E F8 E1 88 27 AE F8 E2 8C 37 EE F8 E3 30 47 2E F9 E4 94 57 6E +1+9E .04, meá "$60007163 G.ùā"Mn 00000640 F9 E5 95 67 AE F9 E6 4D 76 EF F8 E7 AD 87 2E FA E8 AA 97 6E FA E9 AB A7 AE FA AC B7 EE FA E8 ùå "$60000660 AF FC E2 CC 37 EF FC E7 DF 40 AF 76 FF E7 BD 86 7A FF E0 D8 B7 AF FF E7 D8 C7 AF FF E7 FD AF FF E7 D8 C7 AF FF E7 FF D8 E7 AF FF E8 E7 AF FF E8
```

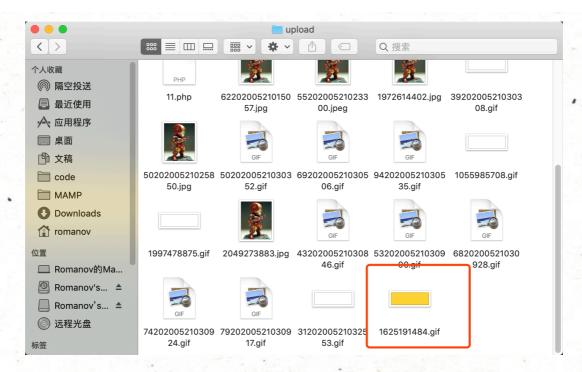
上传后的webshell不见了,这是重新渲染导致的

imagecreatefromjpeg二次渲染它相当于是把原本属于图像数据的部分抓了出来,再用自己的API 或函数进行重新渲染在这个过程中非图像数据的部分直接就隔离开了。按这个方法可以绕过https://secgeek.net/bookfresh-vulnerability/

这一个题目的思路,寻找图片被渲染后与原始图片部分对比仍然相同的数据块部分,将Webshell代码插在该部分,然后上传



手动将其插入到中间部分 之后就可以上传成功并成功访问了



上传后这个图片变黄了,应该是中间插入了一句话木马导致的解析问题