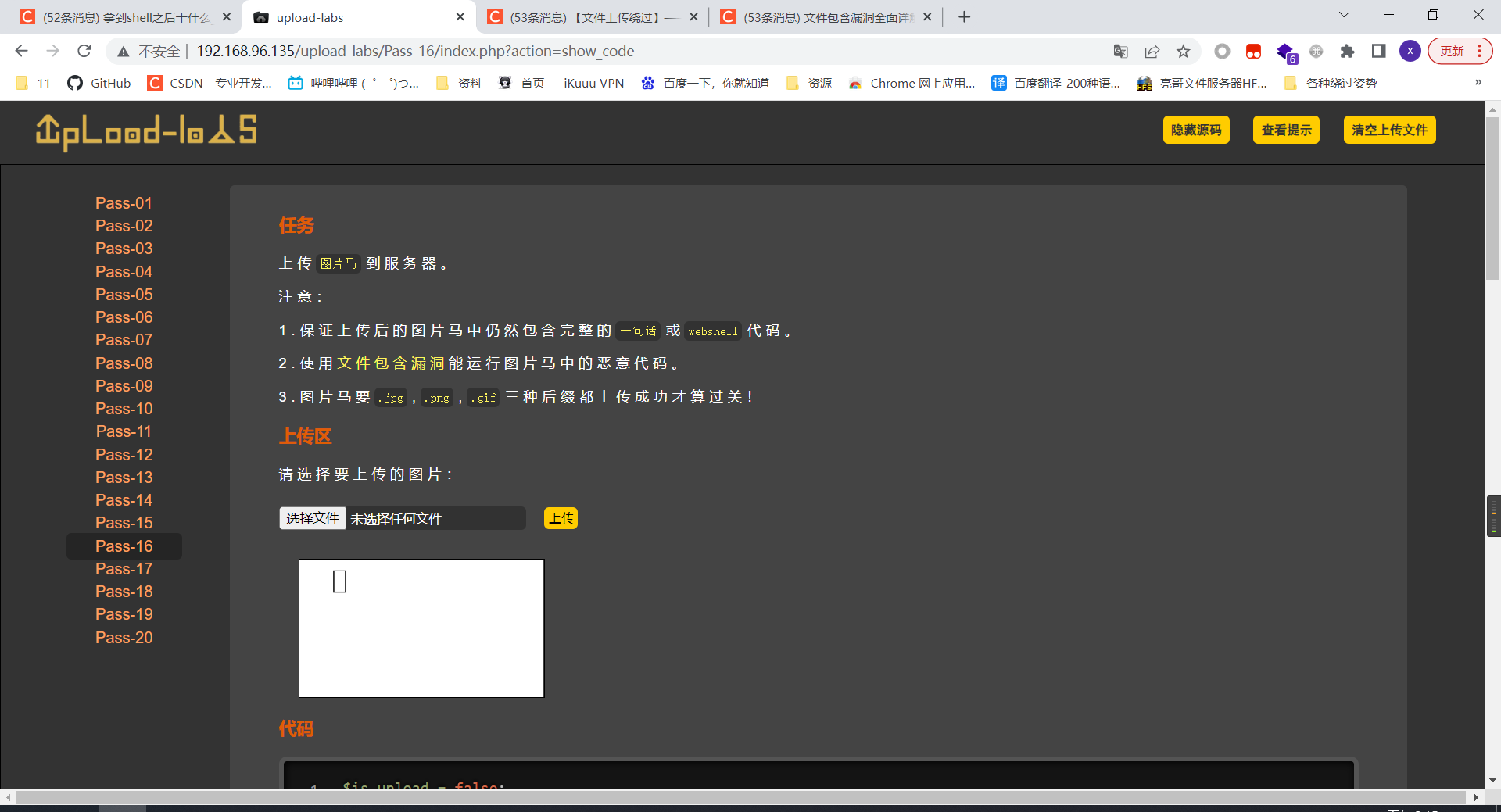
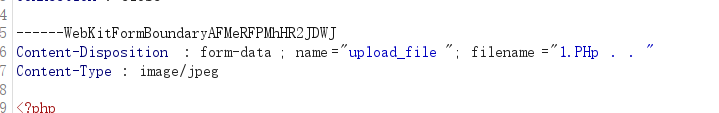
**upload-labs第16关**

1. 拿到站点,测试功能点

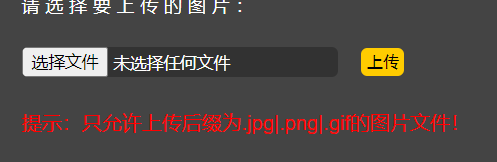


功能点正常

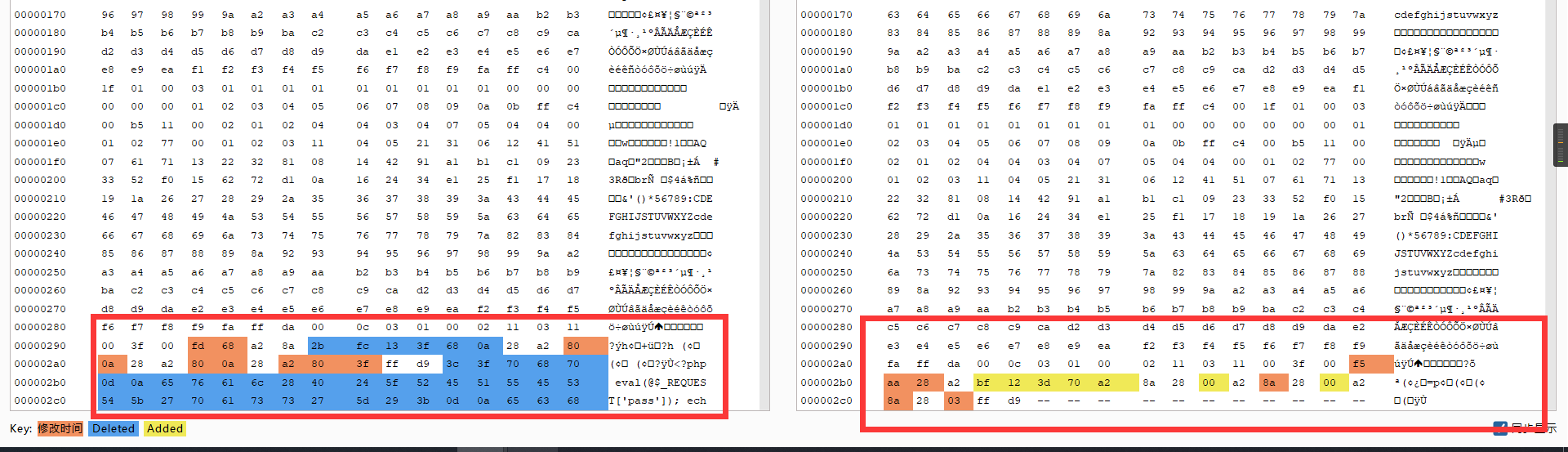
2. 尝试常规绕过方式上传php文件



发现上传点有格式限制



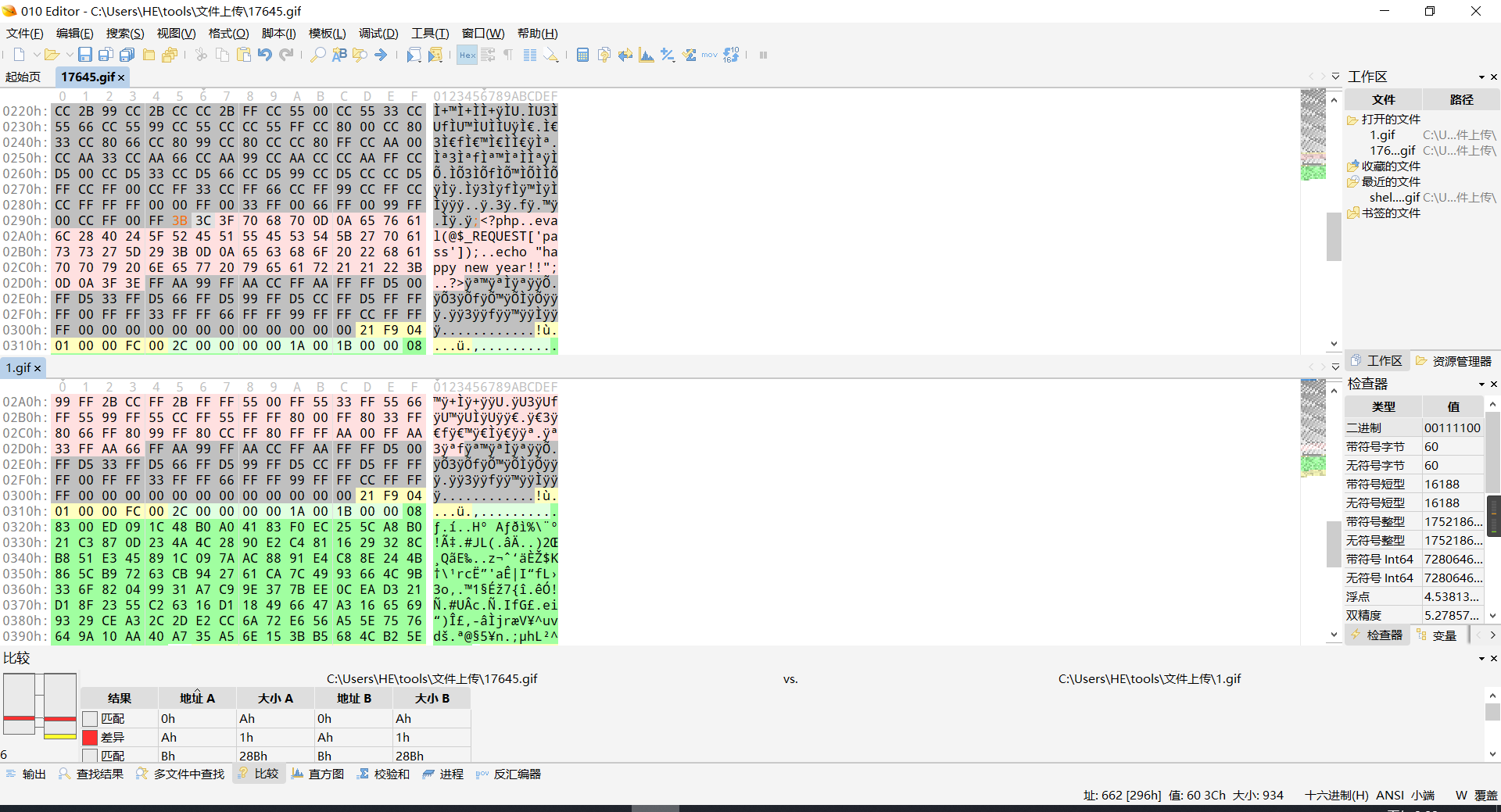
3. 上传图片马,并查看图片是否被二次渲染



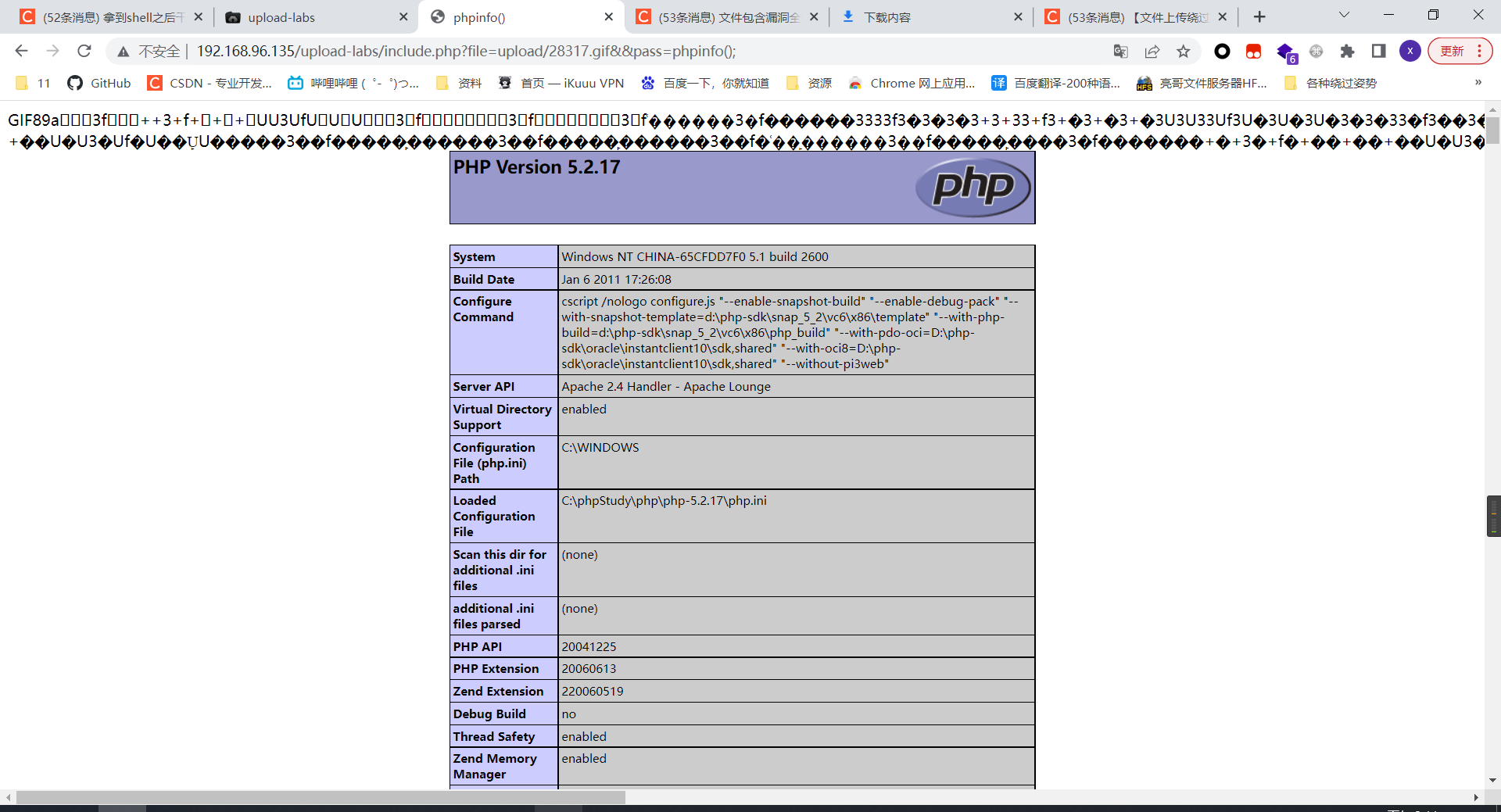
可以看出,图片被二次渲染,恶意代码被和谐

4. 制作一个不会被和谐的图片文件,再次上传

制作要点:先上传一个普通copy的图片马,然后下载被渲染的图片,与原文件进行比较,寻找两个文件相同的地方,就是二次渲染无法修改的地方,将木马写在无法二次渲染的位置,即可绕过二次渲染



5.制作防和谐的图片马后,重新上传,



绕过成功!