从 0 开始 LFI 之 2

在 **Veneno** 的 **blog** 里看到过一种 **LFI** 的思路（原帖地址：**http://www.venenof.com/index.php/archives/36/**），里面提到了一种 **php** 的正则贪婪匹配原则：

0x00.关于php的正则贪婪匹配原则：

在可配也可不配的情况下，优先匹配，直到不能匹配成功的情况下，记录备选状态，并把匹配控制交给正则表达式的下一个匹配字符，当之后的匹配失败的时候，再回溯，进行匹配。简单来说就是首次匹配的长度尽可能地长。

先尝试用 **php：//filter** 像之前的 **LFI** 题一样拿到另外的 **hint**，结果报错。

图像“http://119.29.138.57:12002/show.php?img=php://filter/read=convert.base64-encode/resource=files/images/1.jpg”因存在错误而无法显示。

尝试访问 **http://119.29.138.57:12002/show.php?img=files/flag/flag.txt**，返回“File not found.”，题目中说存在一些过滤，可能也存在一些文件名判断，于是构造新的 payload 进行贪婪匹配。

```
http://119.29.138.57:12002/show.php?img=php://filter/read=convert.base64-encode/resource=files/images/1.jpg/resource=../flag.php
```

这样访问的还是**?img=files/flag/flag.txt**，最后在源码中找到 **flag**。