从 0 开始 LFI 之 2

（**HeartSky** 学长说之前的思路有点问题于是再写一次吧.....)但是还是放上 **Veneno** 的一篇文章里看到过的一种 **LFI** 的思路（原帖地址：**http://www.venenof.com/index.php/archives/36/**），这里第一次看到了 **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。

当然一开始做这个题的时候并没有想到这个，先试了试用 **php** 伪协议读源码：**http://119.29.138.57:12002/show.php?img=php://filter/convert.base64-encode/resource=1.jpg**，返回的还是这张图，猜测这里做了一些过滤，不能直接像 **LFI1** 一样拿到 **base64** 加密后的码，也尝试了 **http://119.29.138.57:12002/show.php?img=../flag.php** 这种形式，返回的是“File not found.”，猜测 payload 的构造中必须包含.jpg，但是又需要读取../flag.php，这时候想到的正则贪婪匹配，之前提交的 wp 里的 payload 是直接在那篇博文中的 payload 里做了些修改后得到的，所以虽然能拿到 flag 但是思路上和本题稍有出入，于是这里放上另一种构造：
http://119.29.138.57:12002/show.php?img=php://filter/read=convert.base64-encode/resource=1.jpg/resource=../flag.php
这样的形式，既匹配到了 jpg 又可以拿到../flag.php 里的内容，最后 F12 查看源码得到 flag。