# Bugku-Web-xxx二手交易市场



## 解题思路

先注册一个用户, 在用户头像出发现可以上传头像



于是上传一个图片进行抓包,发现它上传的样式是先把图片变成base64格式的

POST /user/upload HTTP/1.1 Host: 114.67.246.176:17485 Content-Length: 37739 Accept: application/json, text/javascript, \*/\*; q=0.01 X-Requested-With: XMLHttpRequest User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Origin: http://114.67.246.176:17485 Referer: http://114.67.246.176:17485/user Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Cookie: PHPSESSID=81bff69887972fafd03b90fd5b13b9ba Connection: close

#### 图片转成base64编码的格式如下:

data:image/jpeg;base64,

## 所以这里仿造一下,将文件后缀改为php,再把php使用base64进行编码



# 在上传后可以看到相应报文中有具体的绝对路径,直接使用蚁剑连接

🗅 Folders (8) <	🗅 Files (19)			^
e-to /	O New → ↑ UP 3 Refresh ★ Home ■ Bookmark → /var/www/html/ → Read			
var www html wblic public public	Name 7	Time	Size	Attr
	C application 20	021-01-13 09:41:07	149 b	0777
	C config 20	021-01-13 09:41:07	188 b	0777
	C extend 20	021-01-13 09:41:08	36 b	0777
config	🗅 public 20	021-01-13 09:41:08	21 b	0777
- extend	C route 20	021-01-13 09:41:19	23 b	0777
- route	C runtime 20	021-01-13 09:41:20	42 b	0777
- In runtime	C thinkphp 20	021-01-13 09:41:31	255 b	0777
thinkphp vendor	C vendor 20	021-01-13 09:41:31	93 b	0777
Vendor	🗋 .gitignore 20	021-01-13 09:41:01	54 b	0777
	🗋 .travis.yml 20	021-01-13 09:41:01	1.99 Kb	0777
	CHANGELOG.md 20	021-01-13 09:41:07	32.89 Kb	0777
	LICENSE.bxt 20	021-01-13 09:41:07	1.78 Kb	0777
	README.md 20	021-01-13 09:41:19	6.46 Kb	0777
	build.php 20	021-01-13 09:41:01	1.04 Kb	0777
	Composer.json 20	021-01-13 09:41:07	741 b	0777
	C composer lock 20	021-01-13 09:41:07	8.61 Kb	0777
	🗋 flag 20	021-01-18 07:04:13	39 b	0644
	d) index.php 20	020-09-22 08:25:09	17 b	0777
	think 20	021-01-13 09:41:20	823 b	0777 et/valecalida

即可得到flag