i春秋Zone

转载

weixin_30701575 于 2019-09-11 14:04:00 发布 132 收藏
文章标签： php 运维
原文链接：http://www.cnblogs.com/wosun/p/11505922.html

打开网页是个简单的表单填写，

尝试注入。。。。没用

查看源码，没找到什么有用的信息

只有抓包了

发现一个cookie的login值为0，改为1试试

没什么特别的回显，但这应该就是登录与否的判定了，所以整道题都要注意login的值是否为1

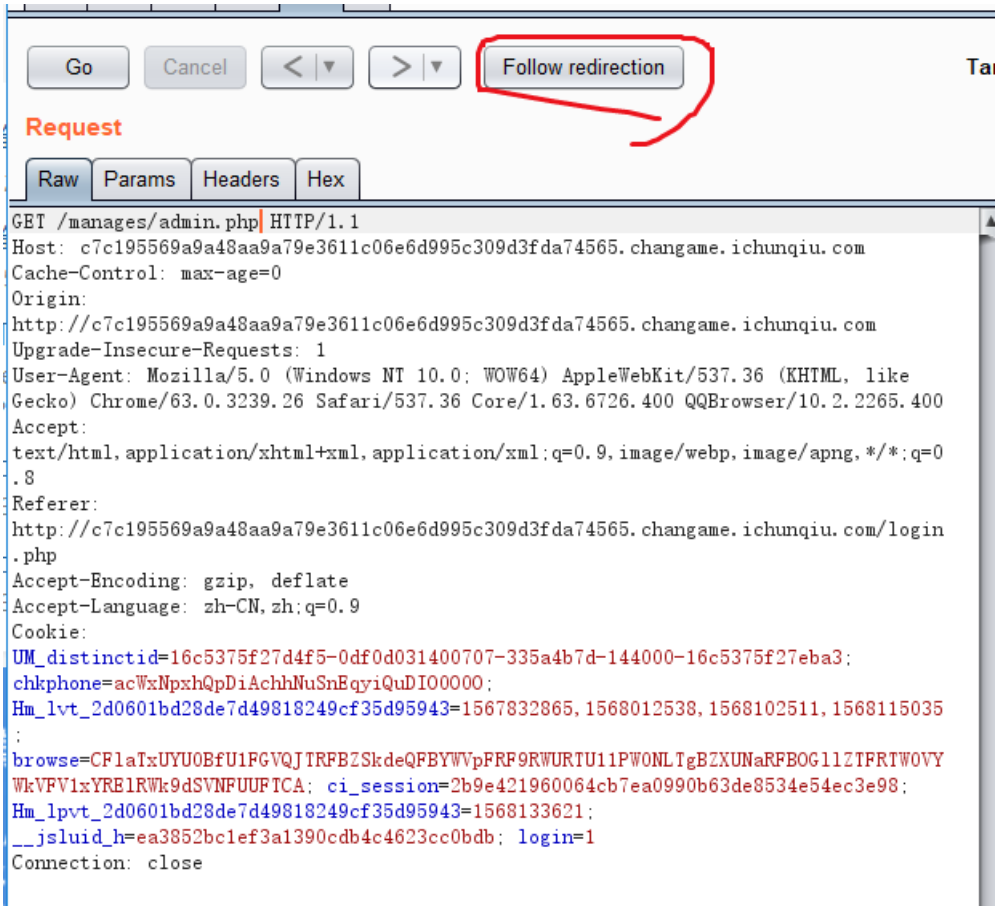
再观察request栏发现了一个/manages/admin.php

```
<div class="collapse navbar-collapse" id="bs-example-navbar-collapse-1">
    <ul class="nav navbar-nav">
        <li class="active">
            <a href="/manages/admin.php">Manage</a>
        </li>
        <li>
            <a href="/logout.php">Logout</a>
```

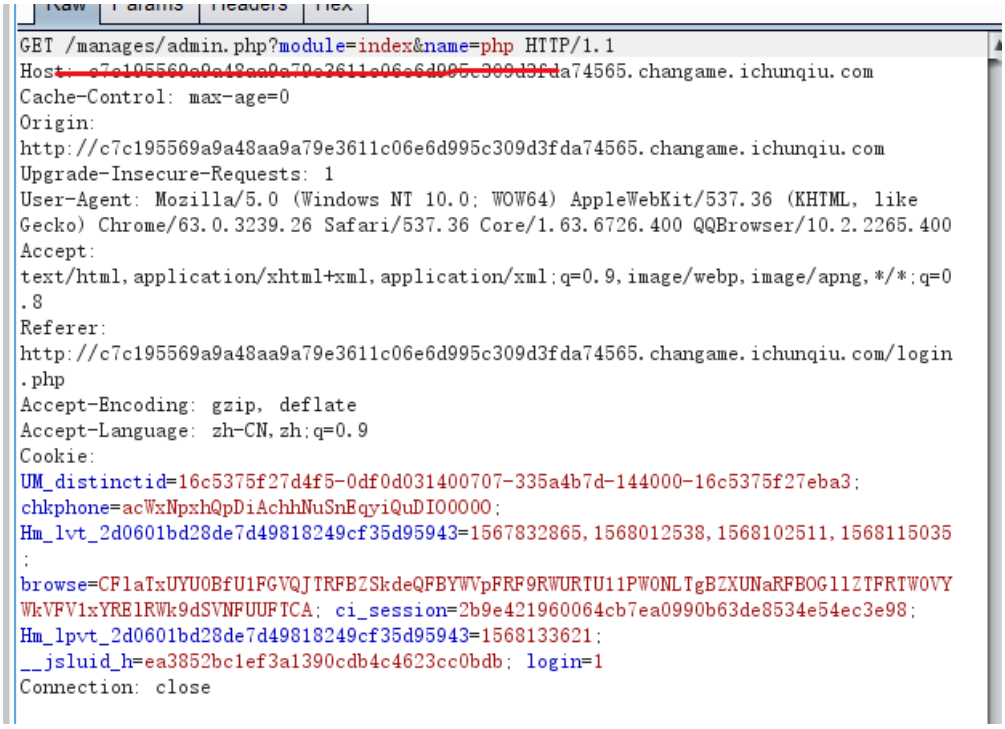
翻译

访问之

出现跳转



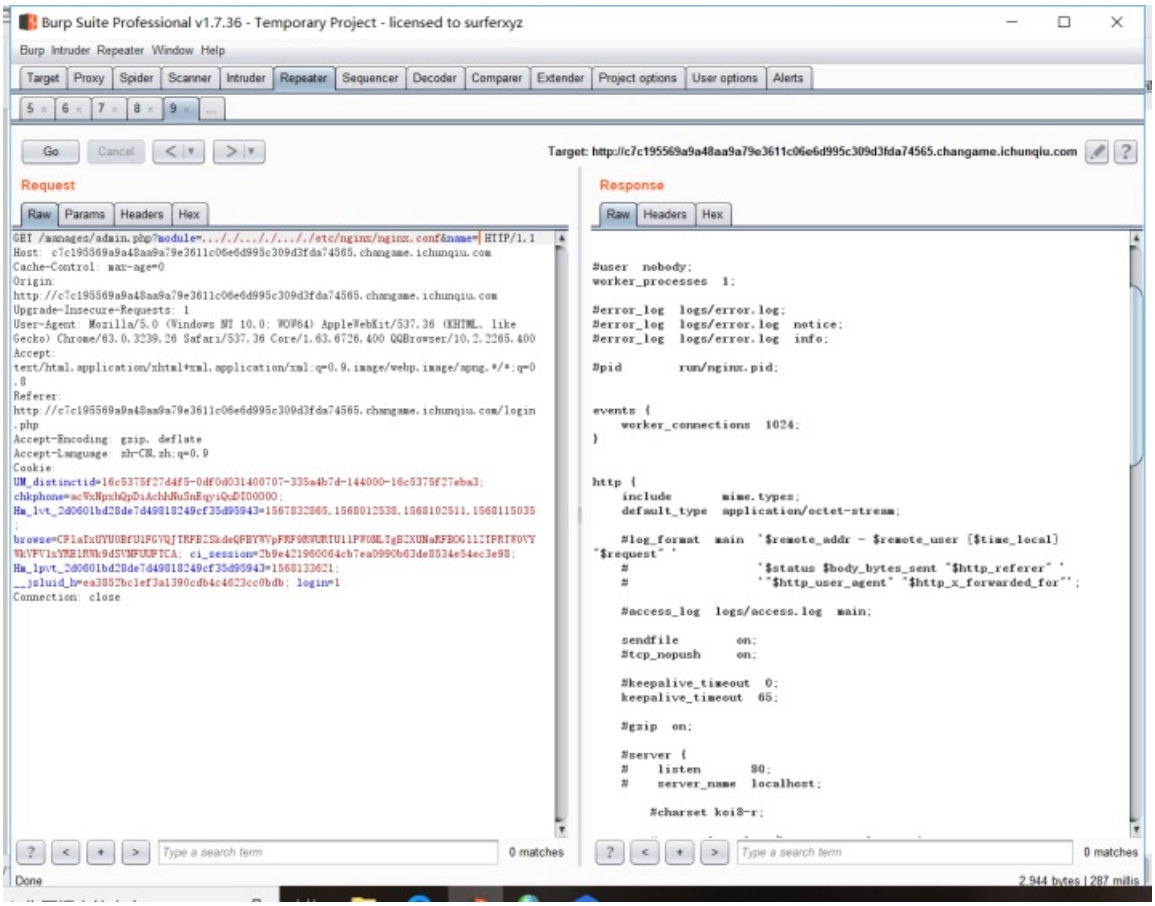
跟过去看看



发现他在GET栏进行了两个传值

试试将其修改看能否返回正常

Module后面跟..././..././..././etc/nginx/nginx.conf来查看nginx配置文件（删去name后面的值，似乎是文件类型）

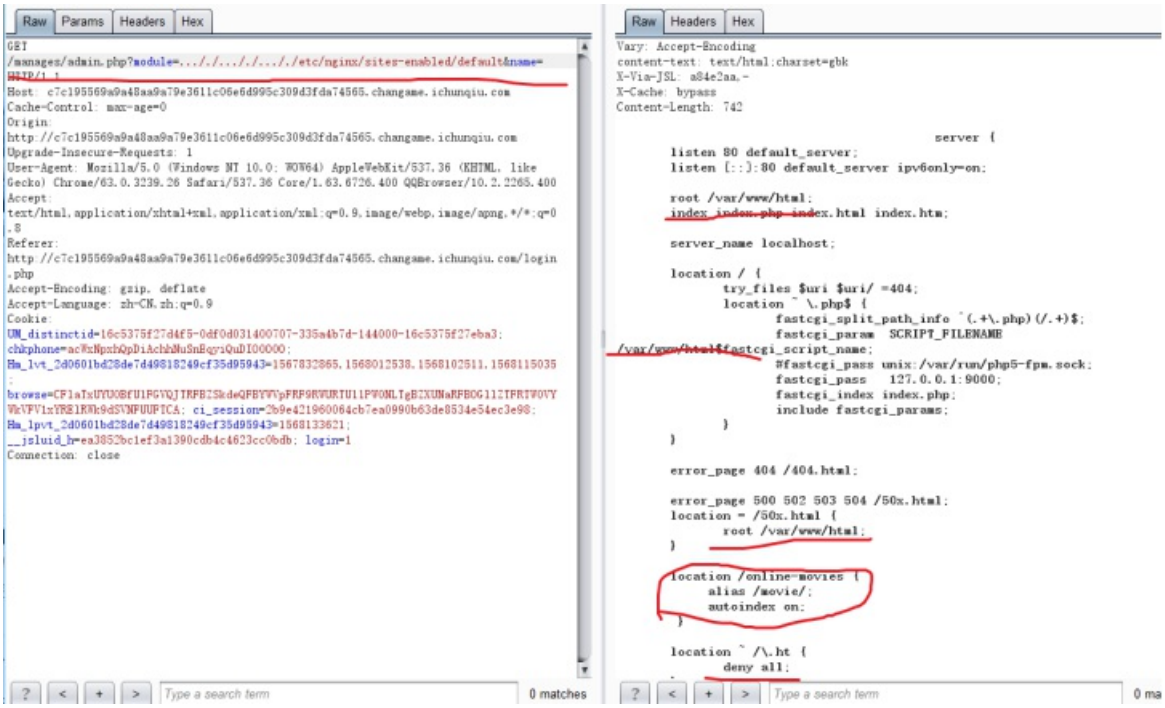


成功查看到了

```
    #    location / {
    #        root   html;
    #        index  index.html index.htm;
    #    }
    #}
    include  sites-enabled/default;
}
```

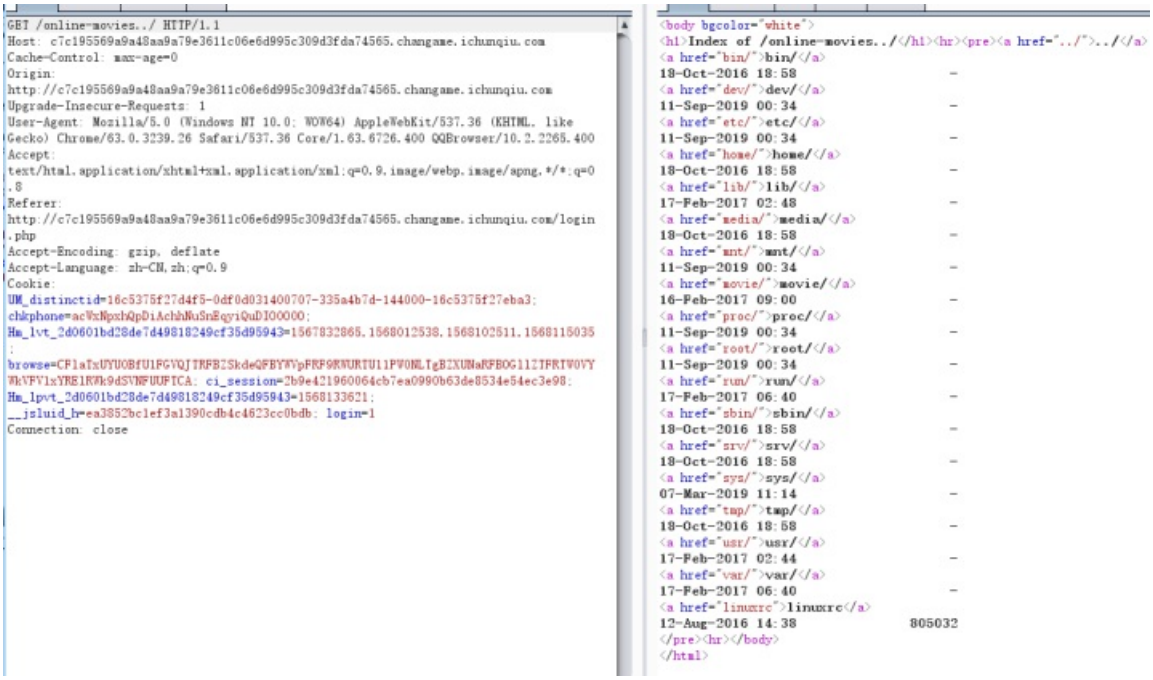
最下方又有东西

继续查看之



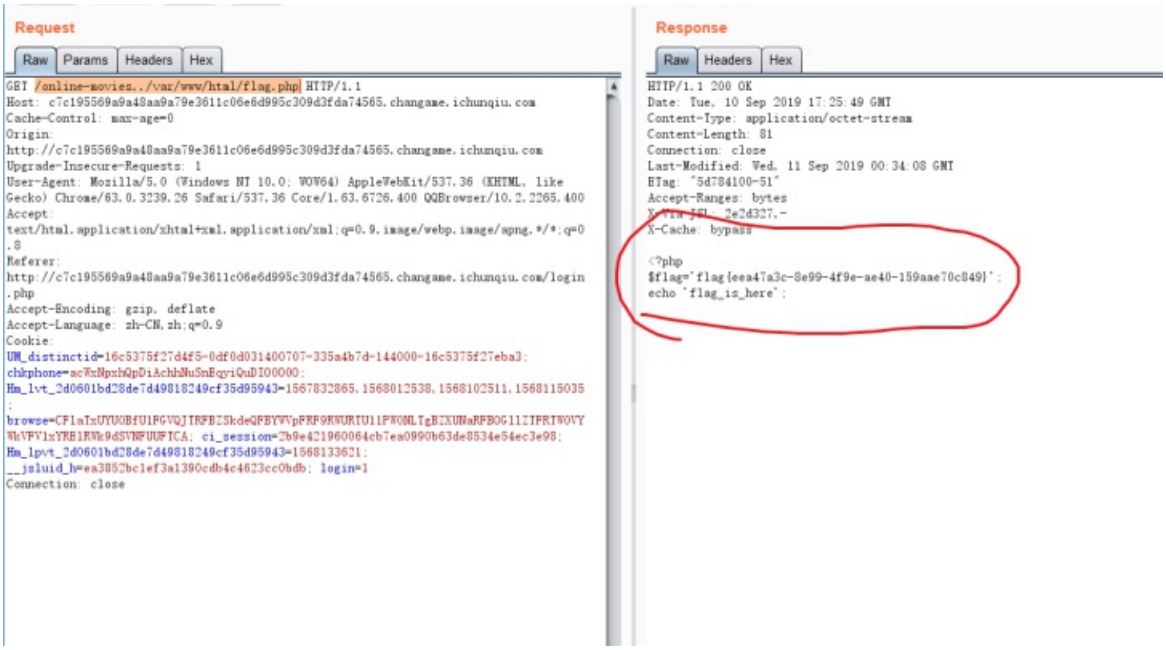
发现一个本地目录遍历/online-movies

直接尝试



然后一步步挖，最后在/var/www/html/flag.php发现flag

直接访问



获取flag

转载于:https://www.cnblogs.com/wosun/p/11505922.html