

# i春秋CTF题库---Who are you详解

转载

[weixin\\_34279246](#) 于 2018-05-16 10:34:38 发布 917 收藏 1

文章标签: [数据结构与算法 php](#)

原文链接: <http://blog.51cto.com/12332766/2116829>

版权

1、进入链接,提示说不是管理员



@51CTO博客

我们查看源代码,也没有任何线索

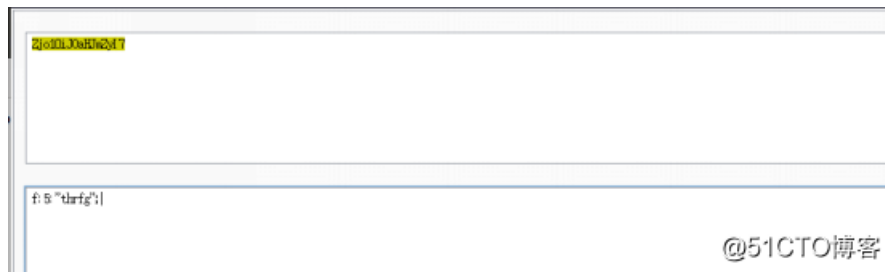
2、查看请求头

既然什么线索没有我们不妨在请求头里面找找看。接下来我们抓包看一看,



3、解码cookie

在cookie那里有一个角色的base64编码字符串,开始提示不是说没有管理员角色的凭证吗?这个应该就是喽。线索找到,我们将其解码,

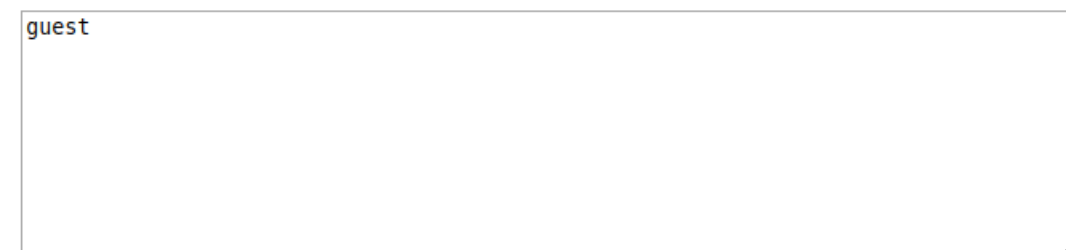


猜想thrfg是经过rot13加密过得。

Rot13加密原理:回转13位,一种简易的置换暗码。ROT13也是过去在古罗马开发的凯撒加密的一种变体。

ROT13是它自己本身的逆反;也就是说,要还原ROT13,套用加密同样的演算法即可得,故同样的操作可用再加密与解密。

我们将得到的thrfg验证后发现结果是guest。

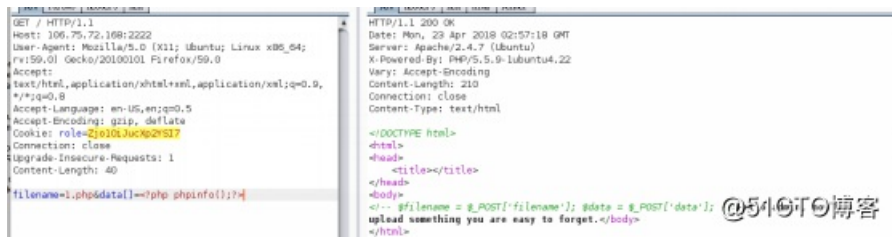


benutze ROT5  enable ROT5

rot13

@51CTO博客

win上是来宾账户，几乎没多大权限。所以我们尝试admin经过rot13加密，然后替换掉thrfg，再经过base64加密传给cookie。



```
GET / HTTP/1.1
Host: 106.75.72.108:2222
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: role=210101uc%2S17
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 40
filename=1.php&data[]=?php:phpinfo();?

HTTP/1.1 200 OK
Date: Mon, 23 Apr 2018 02:57:18 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'];
upload something you are easy to forget.</body>
</html>
```

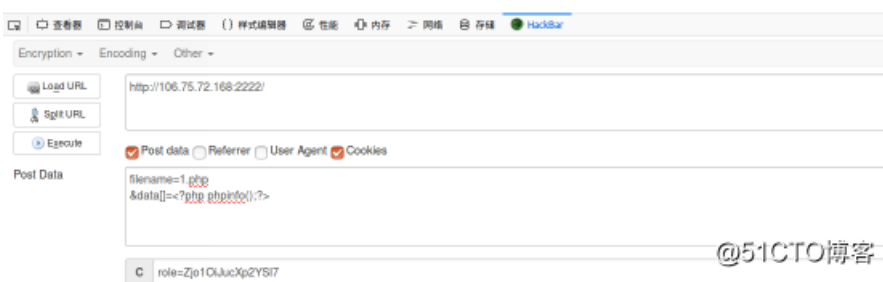
我们得到一串源吗的提示，需要post上传两个文件。并且我们现在拥有了管理员的权限。

#### 4、构造上传语句

试试直接上传php\*\*\*。这时提示nonono:



说明在写入数据的时候应该触发了什么鬼。既然是上传文件，后台处理的时候肯定利用了函数写入。在上传时写入文需要有fopen fwrite fclose等等系列函数，还有一种file\_put\_contents()函数，它与依次调用上面三个函数功能一样，并且还这个可以允许数组。我们这里暂时不知道他们用的那个函数。所以我们应该将可上传的数据类型都尝试一下，所以我们再来尝试上传一个数组，可以将绕过语句改为  
Filename=1.php&data[]=<?php phpinfo();?>



可以看到，页面返回给我们了文件上传后的路径，证明利用的file\_put\_contents()函数写入的文件。

### 5、获得flag

这时我们去访问得到的文件路径就可以看到flag



自我感觉此题难点有三：

- (1) 当我们打开题目时，不知道去干什么。这时应该尝试抓包查看头部信息，否则想破头（如此题）
- (2) 当我们得到base64解密后的字符串时，不知道代表着什么。这里需要对密码有着充足的理解。特别是不知道rot13的，容易想破头。
- (3) 在我们得知能够上传文件的时候，不知道该如何正确的去上传。这里需要明白上传写入的函数。可能大多都对上传数据写入的函数fopen(),fwrite(),fclose()函数比较熟，但是不知file\_put\_contents()函数，此题你就会想破头。

总结：积累很重要啊

转载于:<https://blog.51cto.com/12332766/2116829>