WHO ARE YOU?--writeup

转载

weixin_34292287 于 2018-12-27 12:52:00 发布 45 收藏
文章标签： 前端 ViewUI
原文链接：http://www.cnblogs.com/7xiaomao/p/8411237.html

TIPS:广东强网杯线上题

总结知识点：BASE64,ROT13

0x00

Base64

> 什么是Base64?
>
> Base64编码原理
>
> 其用途

什么是Base64?

Base64是一种基于64个可打印字符来表示二进制数据的表示方法。（源于维基百科）

说白了就是一种用64个字符表示二进制数据的方法。

Base编码原理

由于 $2^6 = 64$,也就是说每6个位元为一个单元，对应某个可以打印字符。3个字节有24个位元，对应4个Base64单元，也就是可以打印4个字符。通过使用包括字母A-Z、a-z、数字0-9，这样共有62个字符，此外两个可打印符号在不同的系统中而不同。若原数据的长度为3的倍数且剩下一个输入数据则最后加两个= ；若元数据长度只剩下一个输入数据，则加一个=。

用途

本次题目结合主要利用在HTTP头部报文里，当然也有应用于邮件等。

url运用这个编码传输长数据

ROT13

> ROT13是什么？
>
> 原理

ROT13是什么？

ROT13（**迴轉13位**，**rotate by 13 places**，有時中間加了個连字符稱作**ROT-13**）是一種簡易的替換式密碼。

ROT13 也是過去在古羅馬開發的凱撒加密的一種變體。

原理描述

对任何字元x：\R_13

套用ROT13到一段文字上僅僅只需要檢查字元字母順序並取代它在13位之後的對應字母，有需要超過時則重新繞回26英文字母開頭即可[2]。 A換成N、B換成O、依此類推到M換成Z，然後序列反轉：N換成A、O換成B、最後Z換成M。只有這些出現在英文字母裡頭的字元受影響；數字、符號、空白字元以及所有其他字元都不變。因為只有在英文字母表裡頭只有26個，並且26 = 2 × 13，ROT13函數是它自己的逆反：[2]

0x01

知道了上面的知识，再来看这题：WHO ARE YOU

点进去发现：

Sorry. You have no permissions.

这时候再来看看源码，发现并没有神马提示。按照我这个小白的理解，前端没提示，多半是后台，那么考虑服务端了。于是用BP截取数据包。

诺~看http头

```
GET / HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Cookie: role=Zjo10iJ0aHJmZyI7
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

看到这行Cookie，觉得这里大有文章，于是就试了试将role的值进行了BASE64解码。得到了这个`f:5:"thrfg";`这个什么意思啊？也是思路停了好久，才知道这玩意可能是ROT13，好吧，线上解码

`s:5:"guest";`得到了这个。那么试试改成`admin`;再逆转编码，这时候就得到了`f:5:"nqzvag";`

再BASE64编码一次更改cookie值就可以得到源码提示了。

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

构造**Payload**

filename=1.php&data[]='123'

之后就得到flag文件了。

转载于:https://www.cnblogs.com/7xiaomao/p/8411237.html