[CTF]No.0006 [强网杯] Who are you

原创

林毅洋 于 2017-09-13 20:17:44 发布 1554 收藏

分类专栏： CTF每日一题 CTF 文章标签： php rot13 base64 ctf每日一题 ctf

本文链接：https://blog.csdn.net/kajweb/article/details/77970522


CTF每日一题 同时被 2 个专栏收录

9 篇文章 0 订阅

订阅专栏


CTF

13 篇文章 0 订阅

订阅专栏

[CTF]No.0006 [强网杯] Who are you

我是谁，我在哪，我要做什么？

CTF每日一题汇总

来源：强网杯-第二届-WEB

类别：base64 rot13 php上传漏洞

来源：https://gdqwb2017.ichunqiu.com/competition/index

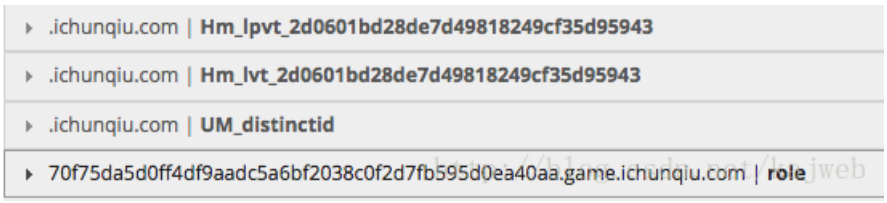
用到工具：无

尝试

进入地址，发现只显示`Sorry. You have no permissions.`

查看源码，没有收获。

接着，查看cookies



有

搜索可知，Hm_lpvt、Hm_lvt 为百度联盟推广的信息，Um_distinctid是站长统计的COOKIE，与比赛无关。剩下的是role了。

可以看到，role为：`Zjo1OiJ0aHJmZyI7`

经过base64解码得到了`f:5:"thrfg";`

紧接着，对其进行rot13得到`s:5:"guest";`，通过把guest改为admin，再逆编码得到`f:5:"nqzva";`和`Zjo1OiJucXp2YSI7`。把后者带入到role中。

上传代码

通过修改cookies后，进入页面提示：

> Hello admin, now you can upload something you are easy to forget.

证明登陆成功。

接着右键查看源码，得到

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

经过测试，filename好像没有进行过滤，但是data进行了对**<**的过滤。
会提示No No No。

经过多种途径上传失败，最后想到上传 `data[]='<?php echo "123";?>'` 数组的形式绕过过滤。
成功后执行返回的地址，得到
flag{e5f5f2cc-800c-4c35-ab59-bfb4e411aedc}

writeUp->Who are you