

# [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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[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

```
▶ .ichunqiu.com | Hm_lpvt_2d0601bd28de7d49818249cf35d95943
▶ .ichunqiu.com | Hm_lvt_2d0601bd28de7d49818249cf35d95943
▶ .ichunqiu.com | UM_distinctid
▶ 70f75da5d0ff4df9aad5a6bf2038c0f2d7fb595d0ea40aa.game.ichunqiu.com | rolejweb
```

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: `Zjo10iJ0aHJmZyI7`

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 `Zjo10iJucXp2YSI7`。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 are
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



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)