




# bugku-点了login没反应 writeup

原创

Peithon  于 2018-04-28 12:41:13 发布  2056  收藏

分类专栏: [BugKu](#) 文章标签: [cookie](#) [bugku](#) [点了login没反应](#) [flag.php](#)

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/qq\\_39629343/article/details/80119126](https://blog.csdn.net/qq_39629343/article/details/80119126)

版权



[BugKu 专栏收录该内容](#)

9 篇文章 2 订阅

订阅专栏

## 题目 flag.php

bugku这道点了login没反应的题, 当时做的时候也是一路艰辛, 写下writeup记录解题过程

### 1.访问 <http://120.24.86.145:8002/flagphp/>

### 2.提示是hint,试试get一个hint参数, 得到源码

### 3.代码审计

```
$cookie = $_COOKIE['ISecer'];
```

若 `unserialize($cookie)` 全等于 `$KEY`, 这里注意有双引号, 大体意思是: `cookie` 的参数为 `ISecer`, 值为 `$KEY` 的序列化

之所以序列化的 `$KEY` 不为 `'ISecer:www.isecer.com'`, 由上图也是可以知晓的, 定义的 `$KEY` 在后面, 所以执行的 `$KEY` 为 `NULL`

序列化为 `s:0:""`, 用 burpsuite 抓包, 将 Cookie 改为下图所示

得到 flag: `flag{unserialize_by_virink}`