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

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}`