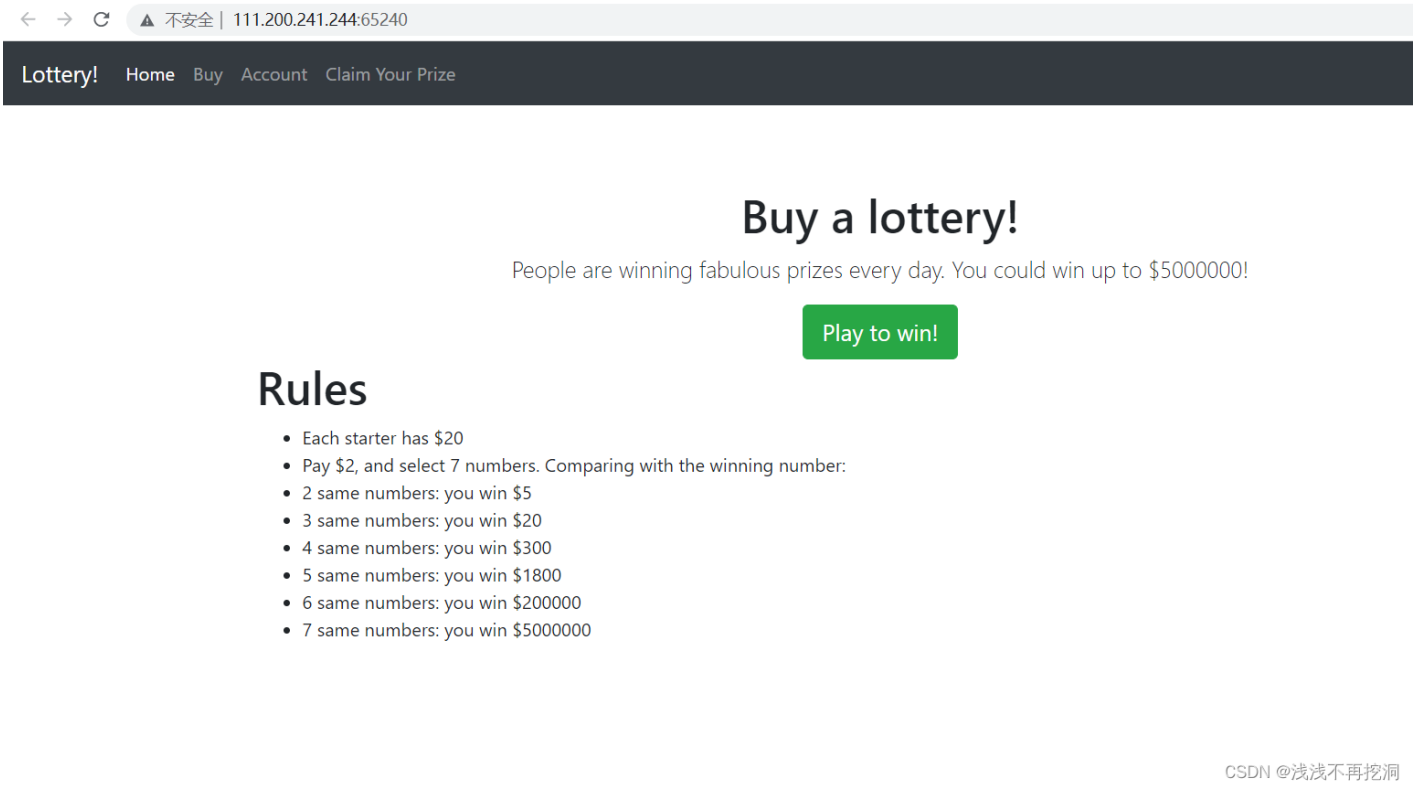
攻防世界 lottery

原创

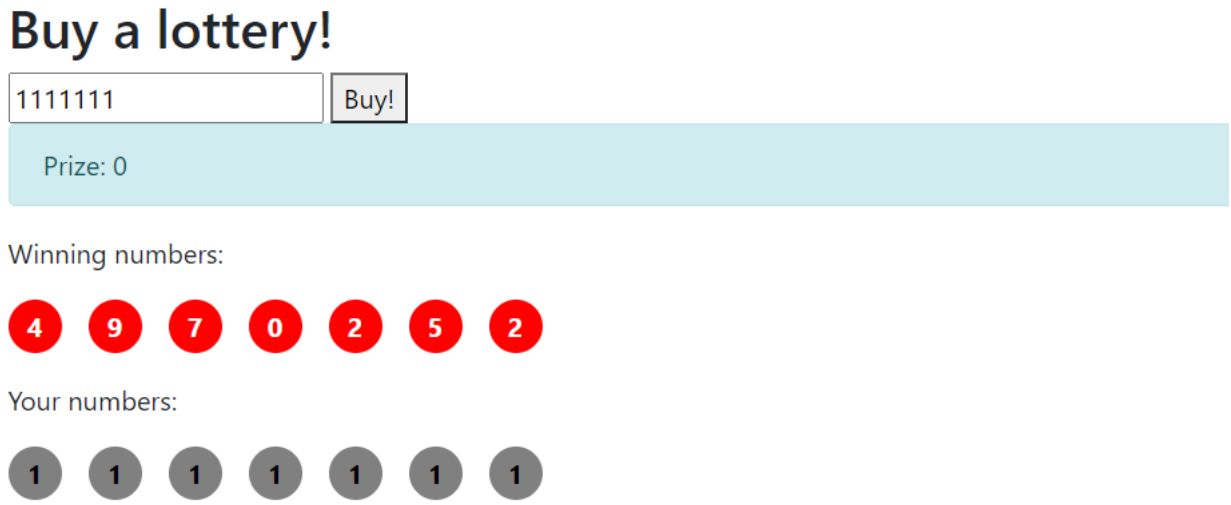
挖洞的浅浅 于 2022-03-26 21:18:52 发布 3401 收藏
文章标签： web安全

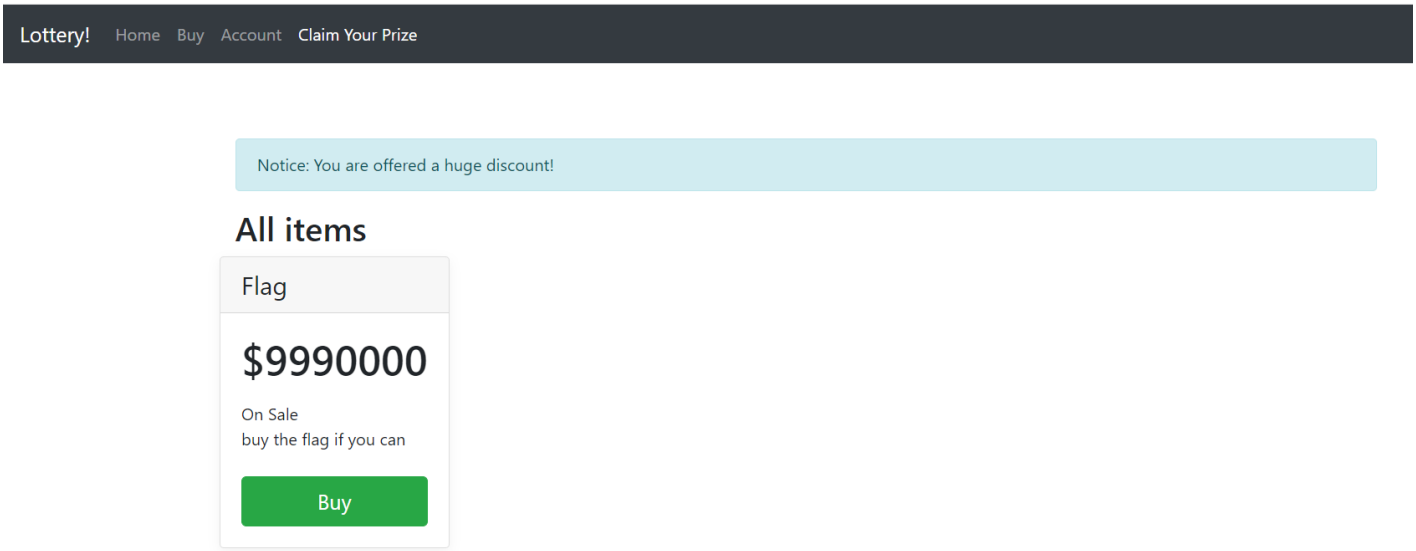
本文链接：https://blog.csdn.net/weixin_51441054/article/details/123763905

打开页面发现是个彩票页面

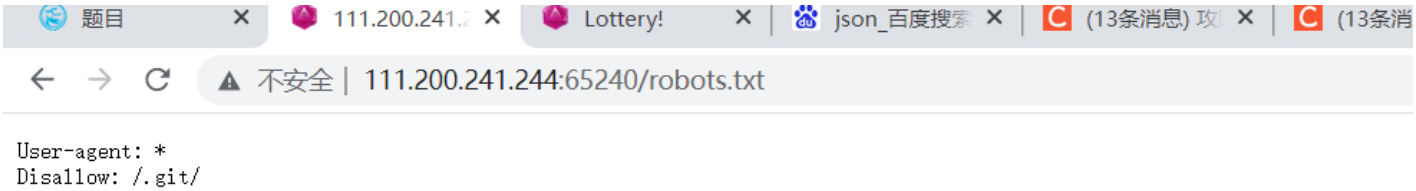


发现需要注册，然后买彩票，得到足够的钱买flag





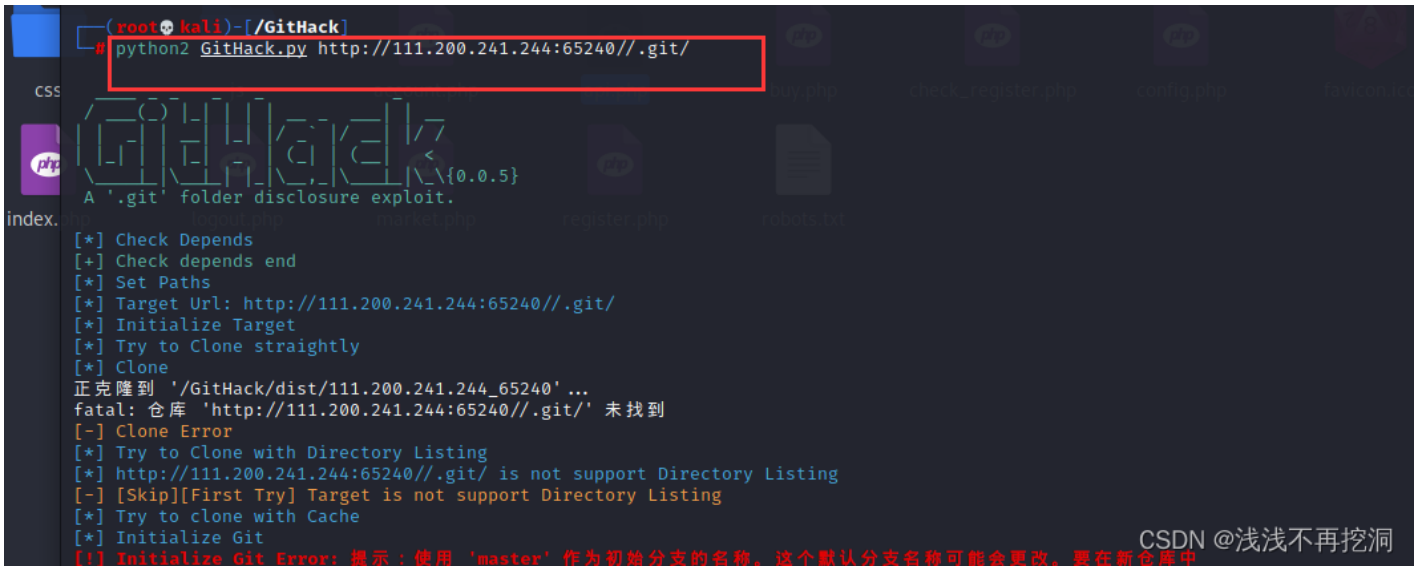
没有思路，查看robots.txt



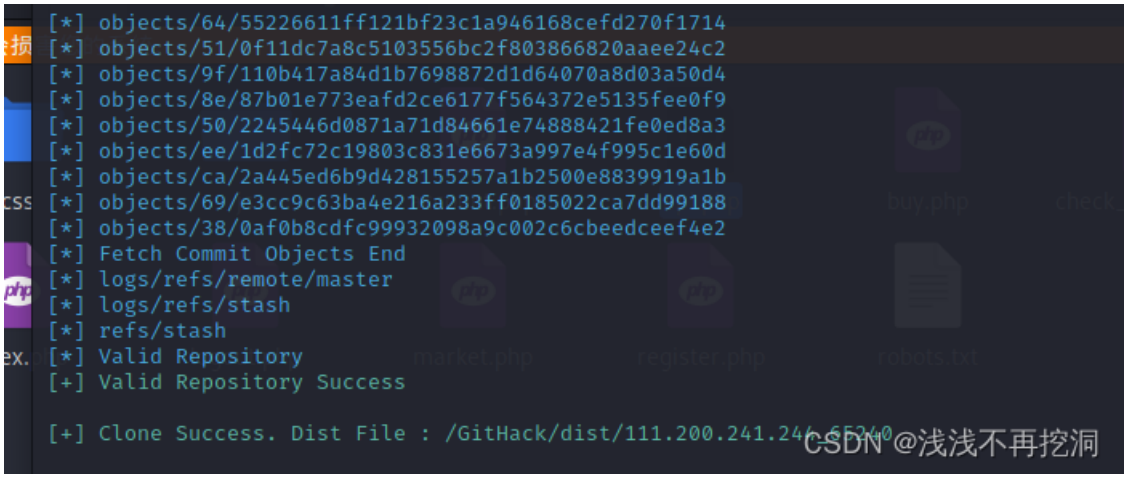

```
User-agent: *
Disallow: /.git/
```


发现git，怀疑是git泄密

利用githack将源文件下载下来



下载成功了，果然存在git泄密



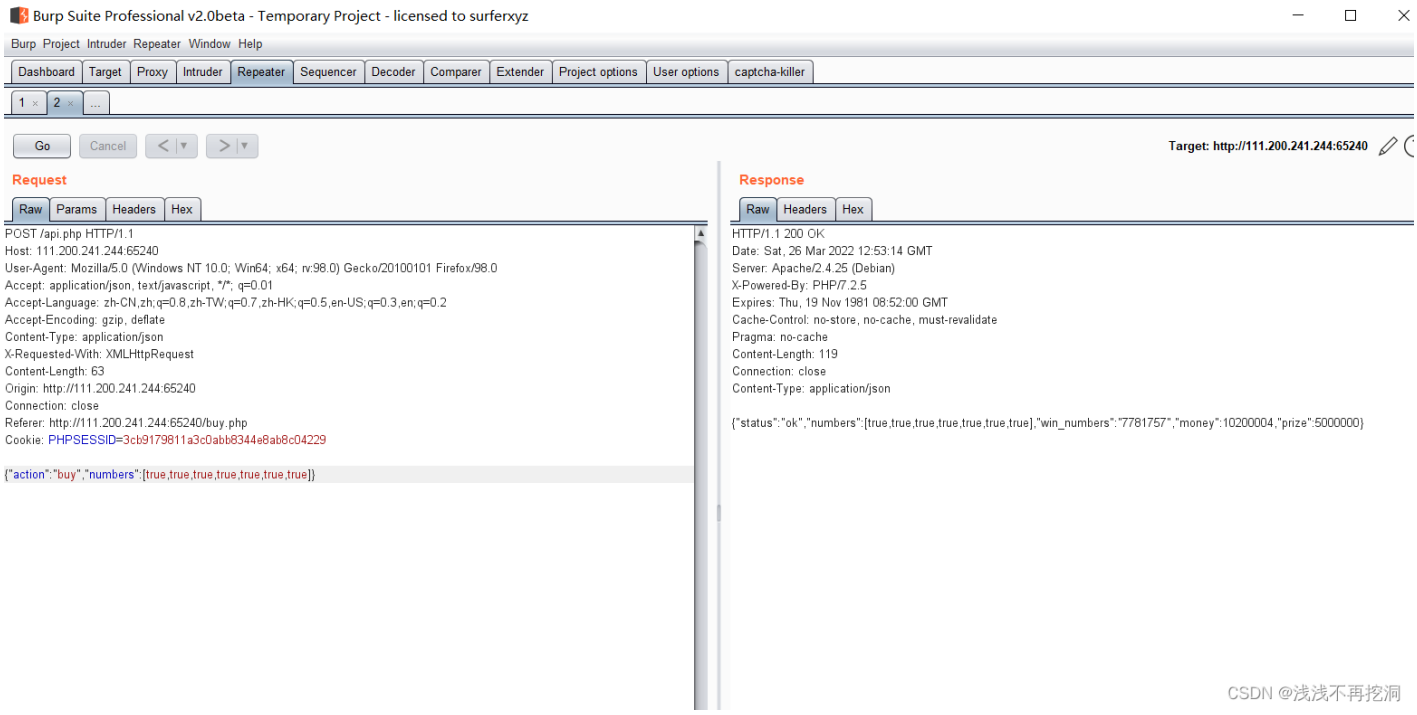
查看代码，发现api.php中有一行代码存在问题

requests是json格式的

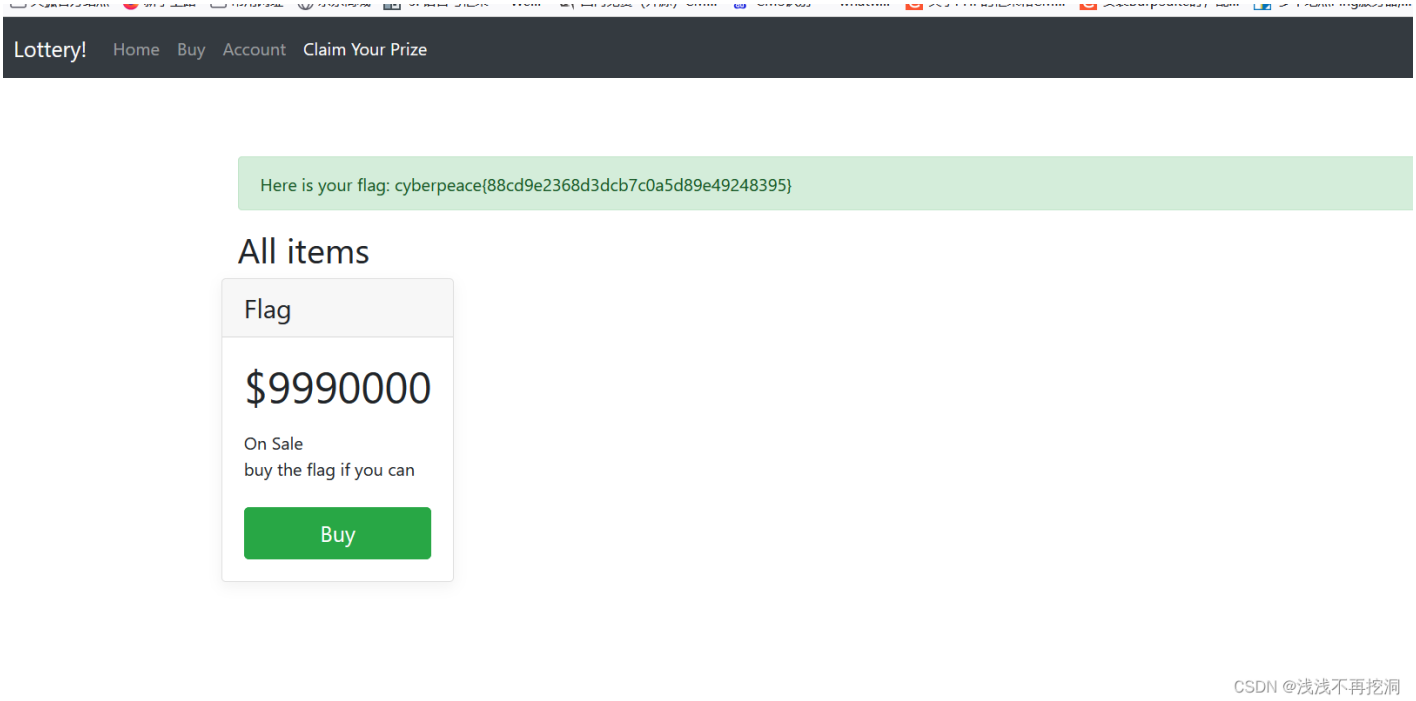
比较彩票数字与用户数字采用==弱比较

而且是一位一位的比较的

由于使用的是PHP 弱类型比较，TRUE,1,"1"都相等相等，即true与字符串和数字都是弱相等的。而且，由于 json 支持布尔型数据，那么就可以构造一串数组[true,true,true,true,true,true,true]传入了。



抓包两次即可得到flag



补：- -后面发现题目已经给出附件，可以直接下载源码。