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

本文链接：https://blog.csdn.net/gou1791241251/article/details/111059074

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

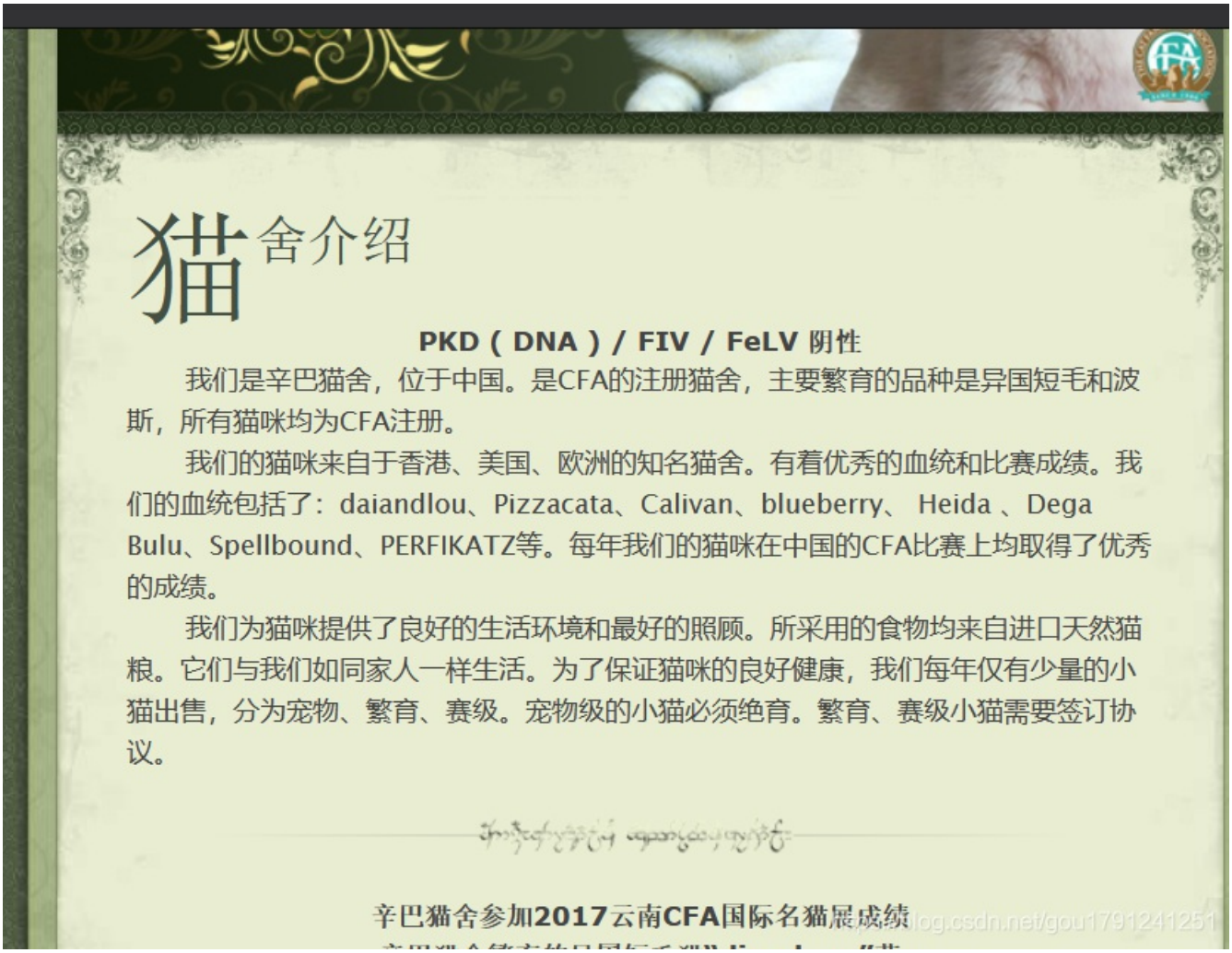
一、观察疑似可注入点

?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



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

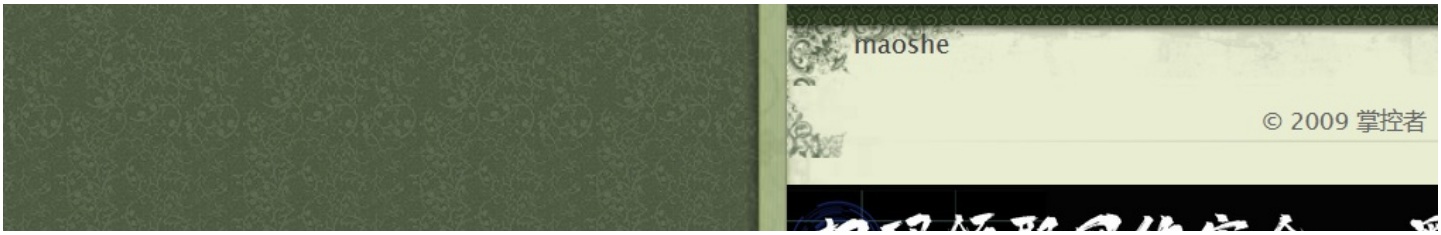
```
http://59.63.200.79:8003/
?id=1 --+
```

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

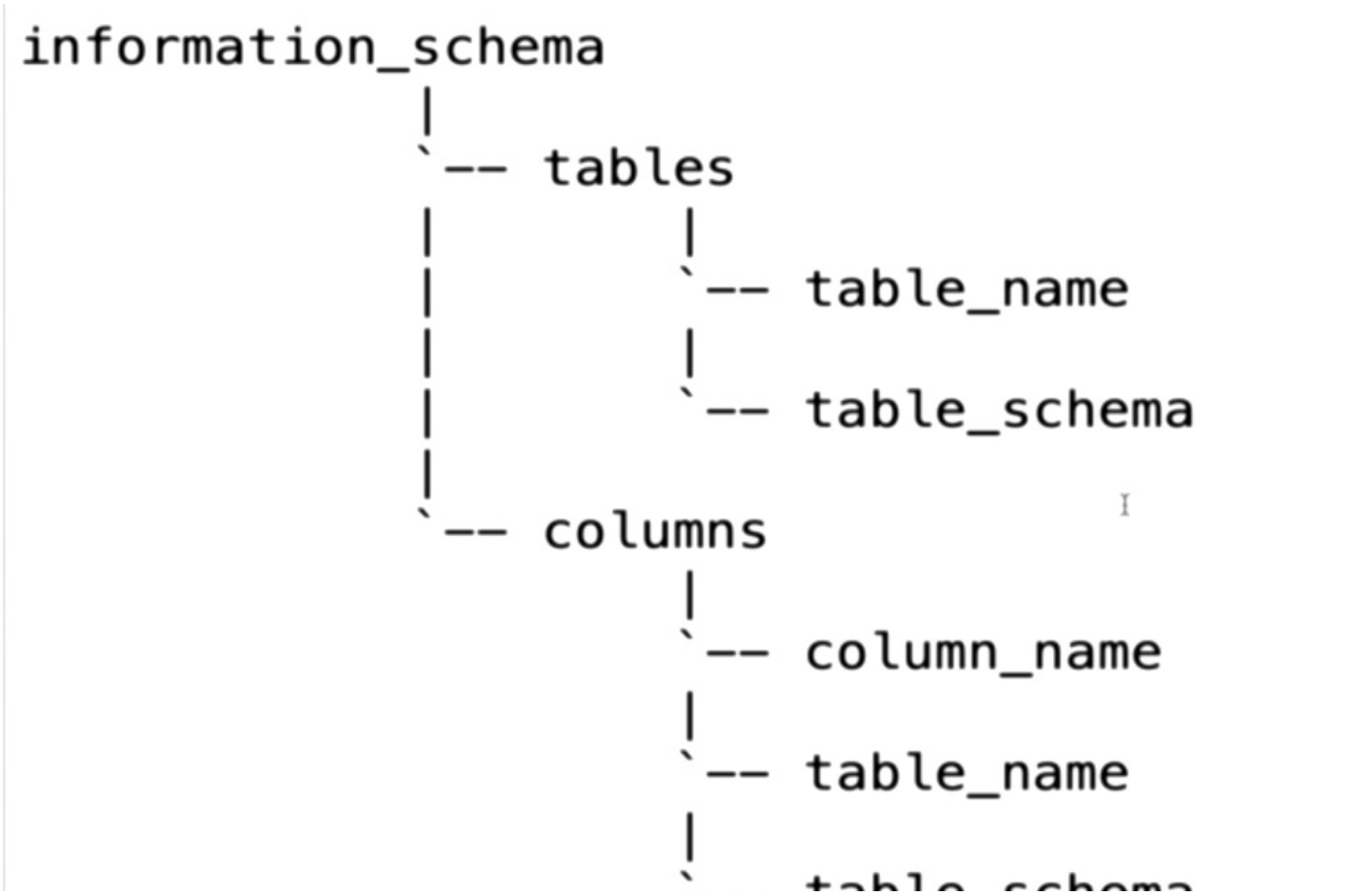
```
http://59.63.200.79:8003/
?id=1 order by 3
```

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



table_schema

@ 注释

mysql 数据库的注释大概有以下几种。

#

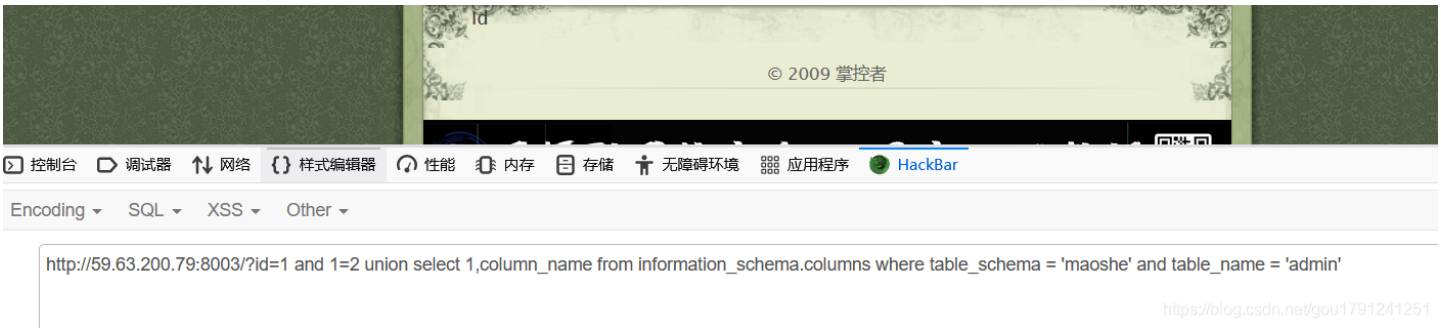
-- （杠杠空格）

/* ..... */

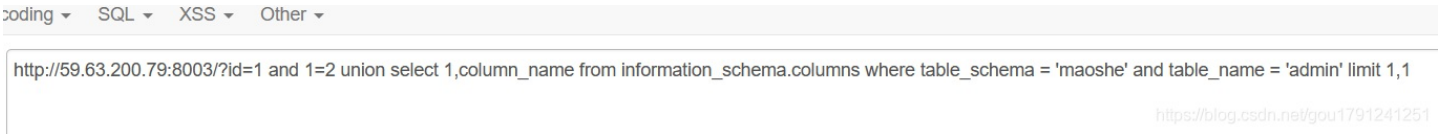
/*! .... */

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。