BUUCTF 2

原创

小杭 于 2021-01-15 21:41:23 发布 55 收藏
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/qq_52431855/article/details/112687460
版权

知识点：

SQL堆叠注入：在SQL中，分号（;）是用来表示一条sql语句的结束。试想一下我们在 ; 结束一个sql语句后继续构造下一条语句，会不会一起执行？因此这个想法也就造就了堆叠注入。

Tip: SQL注入中字符串要用反引号 ` ` 在sql里面这个是主要起区分作用的 如select `from` from username;在这里就是区分默认的from字符和普通字符from的 一般默认可以不加`

show

在过滤了 select 和 where 的情况下，还可以使用 show 来爆出数据库名，表名，和列名。

1. show datebases; //数据库。
2. show tables; //表名。
3. show columns from table; //字段。

alert

作用：修改已知表的列。（ 添加：add | 修改：alert，change | 撤销：drop ）

用法：

- 添加一个列：**alter table " table_name" add " column_name" type;**
- 删除一个列：**alter table " table_name" drop " column_name" type;**
- 改变列的数据类型：**alter table " table_name" alter column " column_name" type;**
- 改列名：**alter table "table_name" rename "old_column" to "new_column";**