# SQL注入漏洞

base on pikachu 

# SQL Inject手动测试-基于union的信息获取

- Union联合查询、order by知识补充
- “information_schema”数据库介绍
- 基于union联合查询的信息获取（select）

# SQL Inject漏洞手动测试：基于union联合查询的信息获取

union 联合查询：可以通过联合查询来查询指定的数据

用法举例：

select username,password from user where id=1 **union** select 字段1，字段2 from 表名
联合查询的字段数需要和主查询一致！

如何确认主查询的字段数？


web安全从入门到放弃

# SQL Inject漏洞手动测试：基于union联合查询的信息获取

order by x //对查询的结果进行排序，按照第X列进行排序，默认数字0-9，字母a-z

```
mysql> select id,email from uname where username="kobe" order by 3;
ERROR 1054 (42S22): Unknown column '3' in 'order clause'
mysql> select id,email from uname where username="kobe" order by 1;
+----+--------------+
| id | email        |
+----+--------------+
|  3 | kobe@ant.com |
+----+--------------+
1 row in set (0.07 sec)
```

思路：对查询的结果使用order by按照指定的列进行排序，如果指定的列不存在，数据库会报错。

通过报错判断查询结果的列数，从而确定主查询的字段数。

# MYSQL小知识补充：

Select version(); //取的数据库版本

Select database(); //取得当前的数据库

Select user(); //取得当前登录的用户

```
mysql> select version(),database(),user();
+-----------+------------+----------------+
| version() | database() | user()         |
+-----------+------------+----------------+
| 5.6.21    | dvwa       | root@localhost |
+-----------+------------+----------------+
1 row in set (0.00 sec)
```

Select @@global.version_compile_os from mysql.user;

```
mysql> select @@global.version_compile_os from mysql.user;
+----------------------------+
| @@global.version_compile_os |
+----------------------------+
| Win32                      |
+----------------------------+
1 row in set (0.16 sec)
```

# MYSQL小知识补充：information_schema

在mysql中，自带的**information_schema**这个表里面存放了大量的重要信息。具体如下：
如果存在注入点的话，可以直接尝试对该数据库进行访问，从而获取更多的信息。

比如：
SCHEMATA表：提供了当前mysql实例中所有数据库的信息。是show databases的结果取之此表。

TABLES表：提供了关于数据库中的表的信息（包括视图）。详细表述了某个表属于哪个schema，表类型，表引擎，创建时间等信息。是show tables from schemaname的结果取之此表。

COLUMNS表：提供了表中的列信息。详细表述了某张表的所有列以及每个列的信息。是show columns from schemaname.tablename的结果取之此表。

# Sql-Inject漏洞手动测试：基于union联合查询的信息获取



web安全从入门到放弃

#具体的操作和讲解过程详见视频演示#

# 谢 谢

“听”而不思则罔，思而不“练”则殆