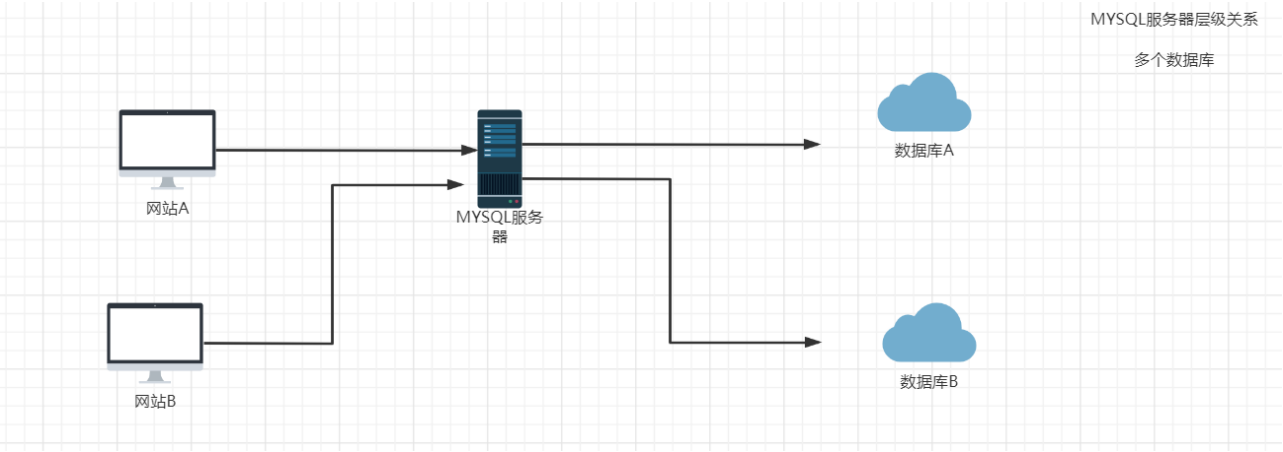
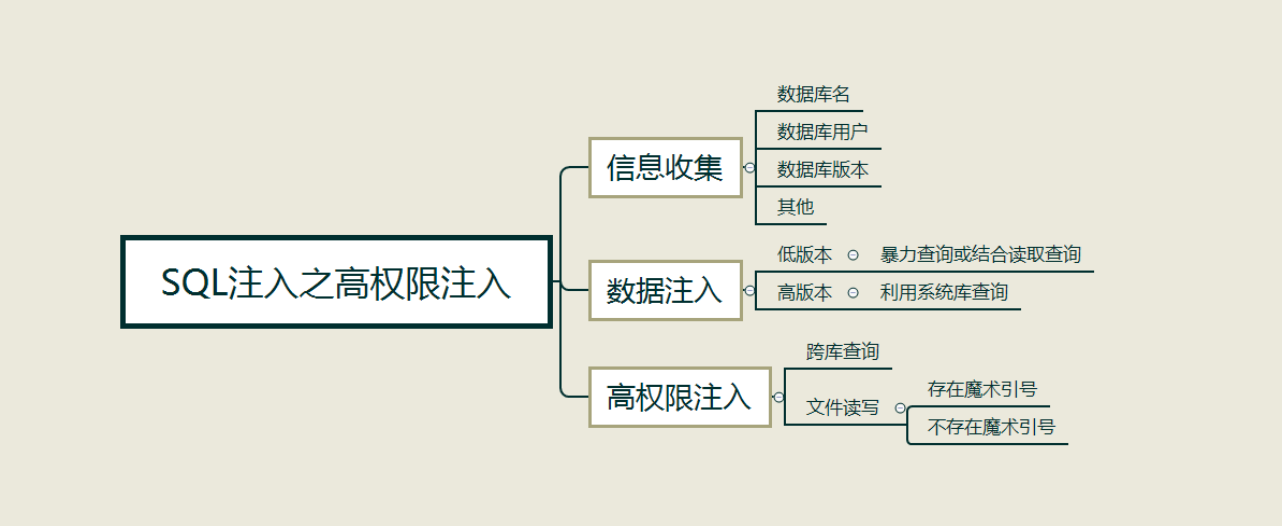
SQL注入之高权限注入

在数据库中区分有数据库系统用户与数据库普通用户,二者的划分主要体现在对一些高级函数与资源表的访问权限上。直白一些就是高权限系统用户拥有整个数据库的操作权限,而普通用户只拥有部分已配置的权限。

网站在创建的时候会调用数据库链接,会区分系统用户链接与普通用户链接;当多个网站存在一个数据库的时候,root就拥有最高权限可以对多个网站进行管辖,普通用户仅拥有当前网站和配置的部分权限。所以当我们获取到普通用户权限时,我们只拥有单个数据库权限,甚至文件读写失败;取得高权限用户权限，不仅可以查看所有数据库,还可以对服务器文件进行读写操作。

多个网站共享mysql服务器





MySQL 权限介绍

mysql中存在4个控制权限的表，分别为user表，db表，tables_priv表，columns_priv表，我当前的版本mysql 5.7.22 。

```
select * from user where user='root' and host='localhost'\G;
```

mysql权限表的验证过程为：

先从user表中的Host,User,Password这3个字段中判断连接的ip、用户名、密码是否存在，存在则通过验证。

通过身份认证后，进行权限分配，
按照user，db，tables_priv，columns_priv的顺序进行验证。
即先检查全局权限表user，如果user中对应的权限为Y，则此用户对所有数据库的权限都为Y，
将不再检查db，tables_priv,columns_priv；如果为N，则到db表中检查此用户对应的具体数据库，
并得到db中为Y的权限；如果db中为N，则检查tables_priv中此数据库对应的具体表，取得表中的权限Y，以此类推。

2.1 系统权限表
User表：存放用户账户信息以及全局级别（所有数据库）权限，决定了来自哪些主机的哪些用户可以访问数据库实例，如果有全局权限则意味着对所有数据库都有此权限
Db表：存放数据库级别的权限，决定了来自哪些主机的哪些用户可以访问此数据库
Tables_priv表：存放表级别的权限，决定了来自哪些主机的哪些用户可以访问数据库的这个表
Columns_priv表：存放列级别的权限，决定了来自哪些主机的哪些用户可以访问数据库表的这个字段
Procs_priv表：存放存储过程和函数级别的权限

2. MySQL 权限级别分为：
全局性的管理权限： 作用于整个MySQL实例级别
数据库级别的权限： 作用于某个指定的数据库上或者所有的数据库上
数据库对象级别的权限：作用于指定的数据库对象上（表、视图等）或者所有的数据库对象

3.查看mysql 有哪些用户：
mysql> select user,host from mysql.user;

4.查看用户对应权限

其中\G是把查询结果按列打印

```
select * from user where user='root' and host='localhost'\G;  #所有权限都是Y ，就是什么权限都有
```

5.创建 mysql 用户

有两种方式创建MySQL授权用户

执行create user/grant命令（推荐方式）

```
CREATE USER 'finley'@'localhost' IDENTIFIED BY 'some_pass';
```

通过insert语句直接操作MySQL系统权限表

6.只提供id查询权限

```
grant select(id) on test.temp to test1@'localhost' identified by '123456';
```

7.把普通用户变成管理员

```
GRANT ALL PRIVILEGES ON *.* TO 'test1'@'localhost' WITH GRANT OPTION;
```

8.删除用户

```
drop user finley@'localhost';
```