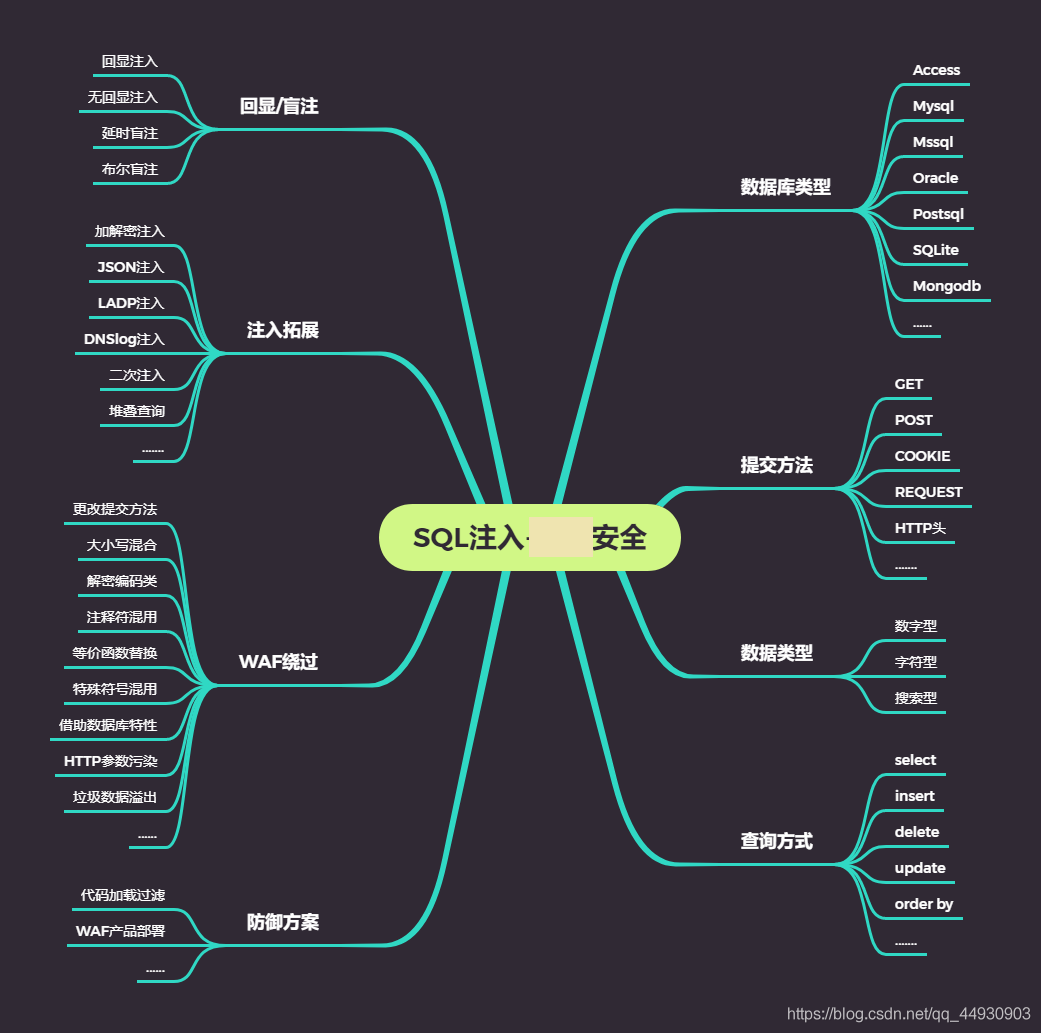
# 14 WEB漏洞-类型及提交注入



#简要明确参数类型

数字，字符，搜索，JSON等

#简要明确请求方法

GET,POST,COOKIE,REQUEST,HTTP头等

其中SQL语句干扰符号：’,",%,),}等，具体需看写法

演示案例：

✧ 参数字符型注入测试=>sqlilabs less 5 6

✧ POST数据提交注入测试=>sqlilabs less 11

✧ 参数JSON数据注入测试=>本地环境代码演示

✧ COOKIE数据提交注入测试=>sqlilabs less 20

✧ HTTP头部参数数据注入测试=>sqlilabs less 18

演示资源：

#配合sqlilabs本地数据库演示

<?php

header('content-type:text/html;charset=utf-8');

if(isset($\_POST['json'])){

$json\_str=$\_POST['json'];

$json=json\_decode($json\_str);

if(!$json){

die('JSON文档格式有误，请检查');

}

$username=$json->username;

//$passwd=$json->passwd;

$mysqli=new mysqli();

$mysqli->connect('localhost','root','root');

if($mysqli->connect\_errno){

die('数据库连接失败：'.$mysqli->connect\_error);

}

$mysqli->select\_db('security');

if($mysqli->errno){

dir('打开数据库失败：'.$mysqli->error);

}

$mysqli->set\_charset('utf-8');

$sql="SELECT \* FROM users WHERE username='{$username}'";

echo $sql;

$result=$mysqli->query($sql);

if(!$result){

die('执行SQL语句失败：'.$mysqli->error);

}else if($result->num\_rows==0){

die('查询结果为空');

}else {

$array1=$result->fetch\_all(MYSQLI\_ASSOC);

echo "用户名：{$array1[0]['username']},密码：{$array1[0]['password']}";

}

$result->free();

$mysqli->close();

}

?>