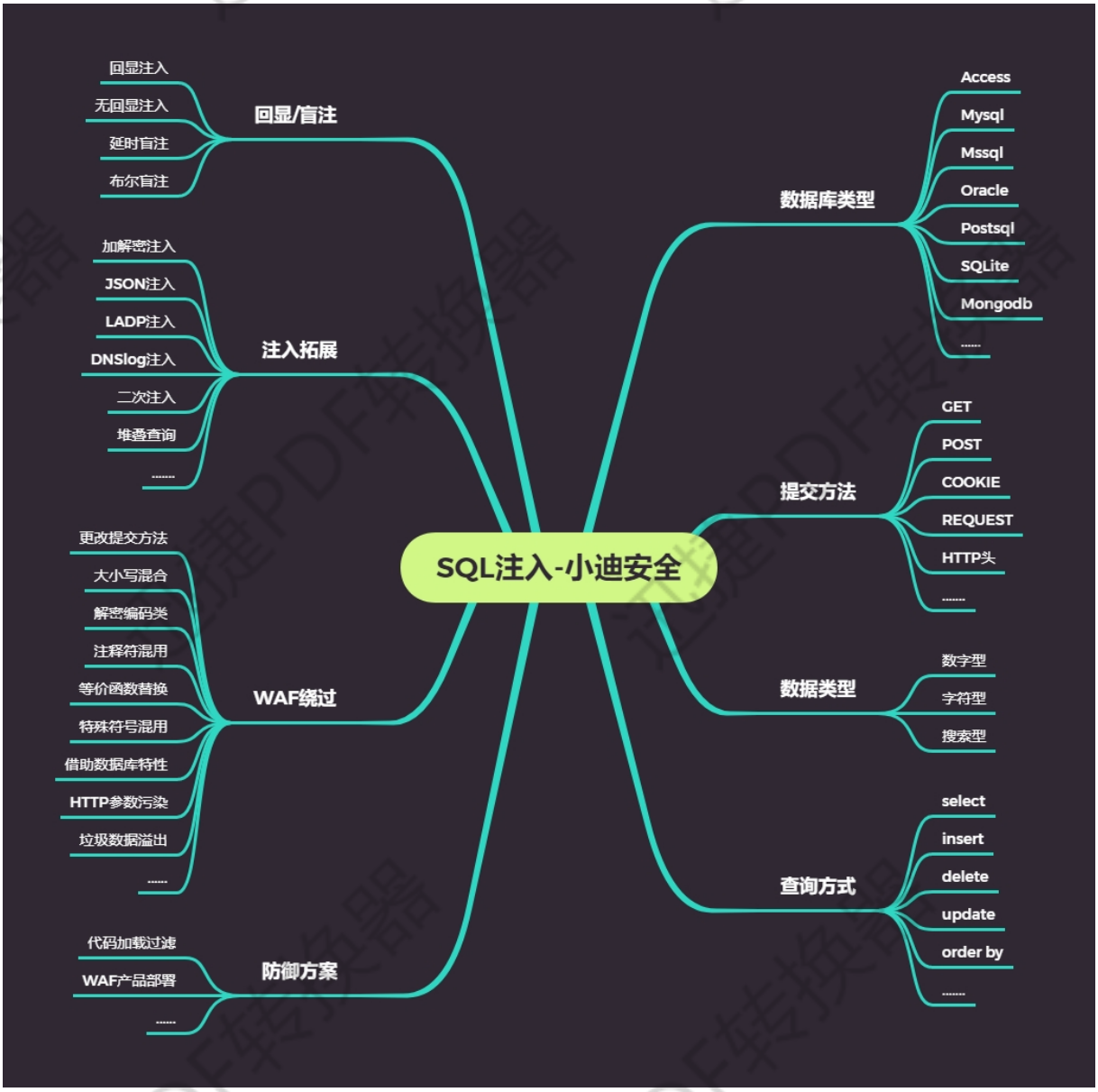
WEB 漏洞-类型及提交注入

在真实 SQL 注入安全测试中，我们一定要先明确提交数据及提交方法后再进行注入，其中提交数据类型和提交方法可以通过抓包分析获取，后续安全测试中我们也必须满足同等的操作才能进行注入。



#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();
}
?>
```
