Day14　WEB漏洞–SQL注入类型及提交注入

> 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。
>
> 注：其中 SQL 语句干扰符号：',",%,),}等，具体需看写法

14.1 简要明确参数类型

- 数字：当SQL语句中出现数字时，则可以直接注入或加上引号
- 字符：当SQL语句中出现字符时，注入一定要加引号
- 搜索：当SQL语句出现 LIKE 关键字时，该SQL语句进行模糊查询，通常参数也要加引号
- JSON：当数据出现JSON时，通常为键值对，需要采用特殊一点的方法进行注入：

14.2 简要明确请求方法

- GET请求：GET请求方式在抓的数据包中会显示GET请求，该种请求方式直接在URL地址中加入注入语句

- POST请求：POST请求方式在抓的数据包中会显示POST请求，该种请求方式会将参数放到请求体中，需要在请求体中加入注入语句
- COOKIE：该请求方法在数据包中会存在一个Cookie请求头，参数会跟在Cookie头后面，需要修改Cookie头后面的信息，加入注入语句
- REQUEST：该种请求方法以GET,POST,COOKIE方式都可以提交成功，在进行注入时可以写在上述三种方式注入的位置中的任意一个位置
- HTTP头：以php为例，在php中有一个server函数，会填入指定参数获取想要的信息，当该信息结合SQL语句进行查询时，可以修改对应的HTTP头后面的参数进行SQL注入