day1-SQL注入基础

课前回顾

增删改查

union，正则，聚合函数，排序order by

 常见的数据库已经对应的端口初试sql注入

什么是sql注入

所谓SQL注入，就是通过把SQL命令插入到Web表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意SQL命令目的的入侵行为。

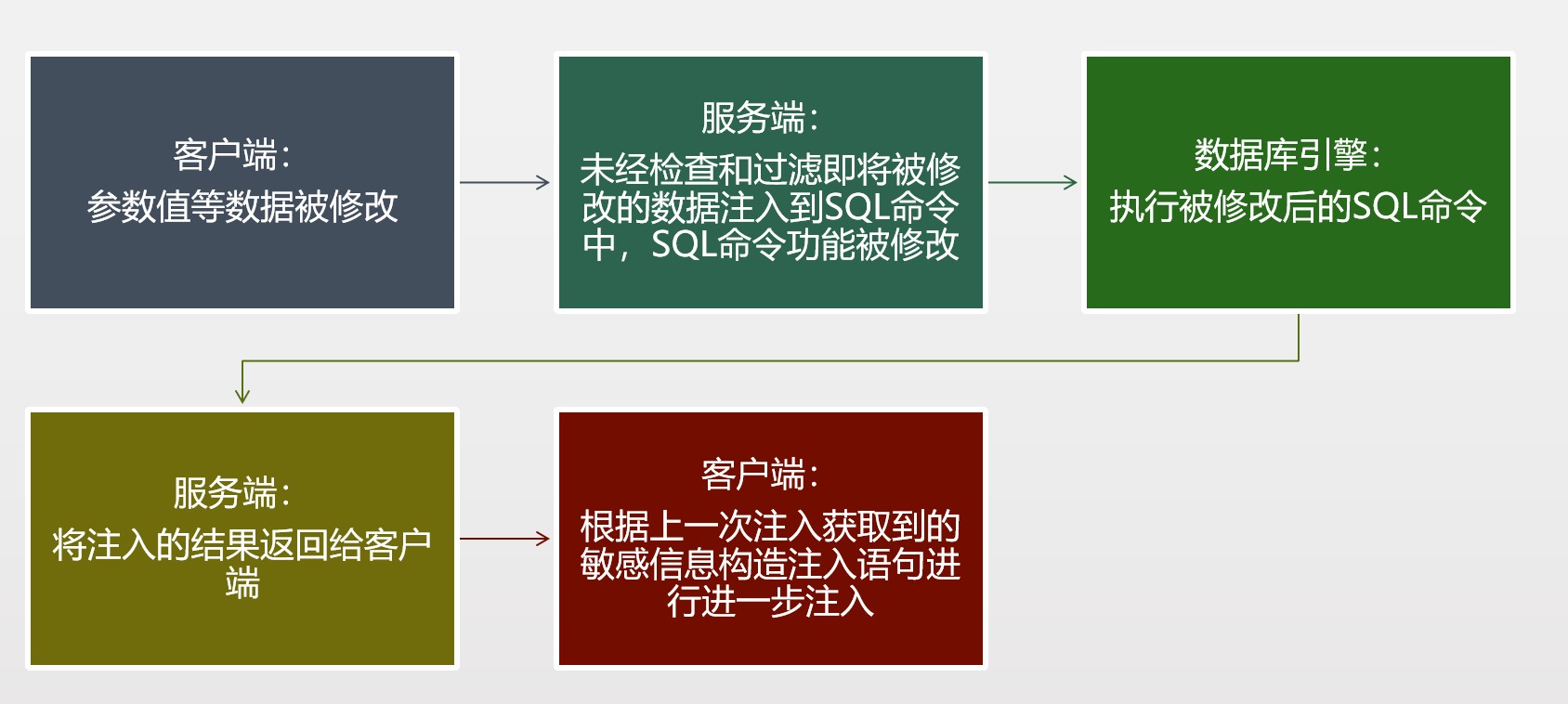
SQL注入是怎么形成的 sql注入产生的原因

没有对**用户的输入数据**或者是页面中所携带的信息进行必要的合法性判断，

sql注入的危害数据泄露网页

权限案列讲解

如何挖掘sql注入

sql注入的流程

select \* from user where id=1 order by name; id=1

name

\* user

sql注入的分类

数据类型

数字型 ——数字直接识别 算术

id=1 and 1=1 正常

id=1 and 1=2 报错算术 四则运算

字符型 —— 字符串需要引号ʼ “ ʻ ” ） 等ʼ） “）

闭合问题返回结果

报错注入——报错内容直接返回到客户端盲注——

select \* from user where id=1;

输入id=1 and 1=1 页面正常

输入id=1 and 1=2 页面不显示内容如何寻找注入点

登录框、搜索框参数名、参数值 cookie

文件名

ua头

。。。。。。任何你觉得跟数据库有交互的地方都可能存在注入如何判断存在sql注入

依据

根据页面的回显判断我们的测试语句是否呗数据库执行构造测试语句

四则运算闭合

根据业务功能考虑它的sql语句，构造能够呗执行的语句—— select \* from user where id=1 order by name; (数字型)

id=1 // 1 and 1=1

name //if(1=1,exp(999),1)

\* // user()--+

user // user where 1=1--+

自己复习一下数据库的内容

以上内容整理于 [幕布文档](https://mubu.com/)