# python面试题 2

- HTTP协议通信过程
  - 1. URL自动解析
  - 2. 获取IP 建立TCP协议连接
  - 3. 客户端浏览器向服务器发出HTTP请求
  - 4. web服务器应答, 并向浏览器发送数据
  - 5. web服务器关闭TCP连接(关闭连接也可以有客户端请求)
- 为什么参数化SQL查询可以防止SQL注入? 如何彻底防范SQL注入
  - 参数化查询或者做词法分析。
    - 一个sql 是经过解析器编译并执行，注意这里是一个并字。
      - 举一个栗子,校验有没有这个用户的场景sql， select count(1) from students where name='张三'
      - 上边的数据库执行时，是直接将这句话连带 name='张三'，一起给编译了，然后执行
      - 假设注入语句是: select count(1) from students where name='张三' or '1=1'
      - 即name 参数为张三 ‘ or '1=1 ，这个参数也会被编译器一同编译。
  - 而使用预编译，数据库是怎么处理的呢？
    - 语句执行的时候 ,服务器把这个SQL发送给数据库,然后数据库将该语句编译后放入缓存池中,
    - 等到服务器execute执行的时候, 传给数据库的张三"or"1=1 并不被编译,而是找到原来的模板, 传参,执行, 所以张三"or"1=1 只会被数据库当做参数来处理

以上内容整理于 幕布