**陈中原：**

**什么是SQL注入？**

SQL注入（SQLi）是一种注入攻击，，可以执行恶意SQL语句。它通过将任意SQL代码插入数据库查询，使攻击者能够完全控制Web应用程序后面的数据库服务器。攻击者可以使用SQL注入漏洞绕过应用程序安全措施；可以绕过网页或Web应用程序的身份验证和授权，并检索整个SQL数据库的内容；还可以使用SQL注入来添加，修改和删除数据库中的记录

**如何防止SQL注入攻击？**

**不要使用动态SQL**

**不要将敏感数据保留在纯文本中**

**限制数据库权限和特权**

**我来单独解释一波我的理解：**

**select \* from 表名 where id=1 or 1=1**

**那么这条sql 就是查全表了。**

**sql 语句的预处理是可以解决sql 注入的。**

**where 条件的强制类型转换，也是可以的。**

**苏建飞：**

javascript:document.body.contentEditable='true';

document.designMode='on';void0

打开网页 F12

console

整个网页就可以随便编辑了

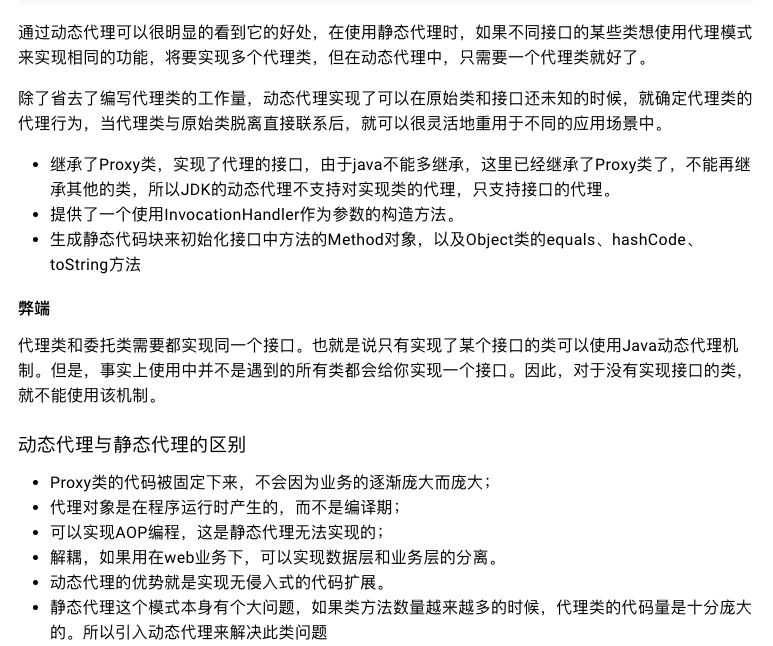
丁昌茂：

****

****

**王福成：**

****

****