二当家小D讲师微信：xdclass6

问题：什么是SQL注入攻击,如何避免

> 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
  - 避免将用户提供的输入直接放入SQL语句中；最好使用准备好的语句和参数化查询，这样更安全。
  - 不要将敏感数据保留在纯文本中
  - 加密存储在数据库中的私有/机密数据；这样可以提供了另一级保护，以防攻击者成功地排出敏感数据。
  - 限制数据库权限和特权
  - 将数据库用户的功能设置为最低要求；这将限制攻击者在设法获取访问权限时可以执行的操作。
  - 避免直接向用户显示数据库错误