设计数据库

第一步一般都是创建数据库，除非是使用第三方的数据库服务。当创建一个数据库的时候，会指定一个所有者来执行和新建语句。通常，只有所有者（或超级用户）才有权对数据库中的对象进行任意操作。如果想让其他用户使用，就必须赋予他们权限。

应用程序永远不要使用数据库所有者或超级用户帐号来连接数据库，因为这些帐号可以执行任意的操作，比如说修改数据库结构（例如删除一个表）或者清空整个数据库的内容。

应该为程序的每个方面创建不同的数据库帐号，并赋予对数据库对象的极有限的权限。仅分配给能完成其功能所需的权限，避免同一个用户可以完成另一个用户的事情。这样即使攻击者利用程序漏洞取得了数据库的访问权限，也最多只能做到和该程序一样的影响范围。