SQL 注入

很多 web 开发者没有注意到 SQL 查询是可以被篡改的，因而把 SQL 查询当作可信任的命令。殊不知道，SQL 查询可以绕开访问控制，从而绕过身份验证和权限检查。更有甚者，有可能通过 SQL 查询去运行主机操作系统级的命令。

直接 SQL 命令注入就是攻击者常用的一种创建或修改已有 SQL 语句的技术，从而达到取得隐藏数据，或覆盖关键的值，甚至执行数据库主机操作系统命令的目的。这是通过应用程序取得用户输入并与静态参数组合成 SQL 查询来实现的。下面将会给出一些真实的例子。

由于在缺乏对输入的数据进行验证，并且使用了超级用户或其它有权创建新用户的数据库帐号来连接，攻击者可以在数据库中新建一个超级用户。