# 数据库安全

## 数据库主要威胁

数据库以数据库服务器为硬件载体，具有可远程连接性，因此数据库的主要威胁可分为硬件层面的威胁和软件层面的威胁。具体可分为以下几点。

* 1. 过载

当服务器接收到超过其处理能力的请求时，会产生请求的淤塞或者是丢失，对可用性和稳定性产生威胁。

* 1. 未授权的操作

恶意请求可能成功获得操作数据库的权限或绕过数据库对请求的检查，从而进行未授权的读写和破坏，对数据的真实性和稳定性、可用性造成威胁。主要来自于SQL注入。

* 1. 病毒入侵

处于网络环境中的数据库服务器容易受到病毒入侵。病毒对服务器数据和计算机系统都可能存在影响。

* 1. 非法接入

对服务器系统的非法接入和提权操作可能将整个服务器暴露给恶意使用者。

* 1. 数据库设计瑕疵

错误的后端逻辑和错误的数据库设计会造成在特定情况下数据库出现异常数据，影响数据真实性和可用性。

* 1. 系统崩溃

计算机系统的死机、崩溃会造成数据库服务的不可用。已经到达但未进行处理或正在处理的数据可能发生混乱。

* 1. 物理损伤

自然灾害等会对当地的服务器造成不可逆的硬件损伤，影响数据库的可用性，也可能造成数据的永久性损坏。

## 数据库安全措施

* 1. 访问控制
     1. 数据源限制

通过访问者的IP地址，拦截一部分对数据库服务器的接入请求。同时设立黑名单制度，对试图进行攻击的IP进行。

|  |  |
| --- | --- |
| 网络地址 | 权限 |
| Web内网 | 完全访问权限 |
| 开发者及开发者承认的其他地址 | 与开发相关端口的完全访问权限（如22，80，8080，3306等） |
| 普通用户、网站管理员地址 | 对外接口对应的端口（80等）的完全访问权限 |
| 黑名单 | 一段时间内禁止全部的访问 |

* + 1. 访问身份验证

采用非对称加密技术验证试图连接者的身份。使用SSL等加密协议进行连接，而不是使用HTTP等明文协议进行连接。

* 1. 密码的密文存储

用户密码在客户端进行第一次散列值计算，传输到数据库服务器之后使用密钥进行第二次散列处理，之后存储到数据库中。

* 1. 完整性控制

完整性控制依赖于事务和正确的并且最严格的约束。其中，所有的复杂过程使用事务进行处理，加入正确的并且最严格的约束。

* 1. 应用程序安全

防止SQL注入的办法一般是限制用户输入的内容，防止用于产生SQL注入的符号（如‘）进入数据库服务器。但是该方法并不能完全防止SQL注入，还需要在数据库服务器部署可检测SQL注入的中间层和防火墙。

* 1. 计算机系统安全

|  |  |
| --- | --- |
| 类型 | 策略 |
| 计算机病毒 | 对硬盘进行定时快照 |
| 提权 | 服务器运行在非root用户，且在部署之后可以删除su文件防止越权 |

* 1. 计算机硬件安全

将多个冗余备份服务器放置在地理位置相对较远的地区，防止突发事件的发生。