10 大最常见的数据库安全问题

数据库作为非常重要的存储工具，里面往往会存放着大量有价值或敏感信息， 这些信息包括金融财政、知识产权、企业数据等方方面面的内容。因此，数据库往往会成为黑客们的主要攻击对象。网络黑客们会利用各种途径来获取他们想要的信息，因此，保证数据库安全变得尤为重要。

尽管意识到数据库安全的重要性，但开发者在集成应用程序或修补漏洞、更新数据库的时候仍然会犯一些错误，让黑客们乘虚而入。本文列出了数据库系统 10 个最常见的安全问题。

1.错误地部署

开发者在部署过程中的粗心大意会很容易让数据库陷入危难之中。在现实中，有些公司会意识到优化搜索引擎对于业务取得成功的重要性，但只有对数据库进行排 序，SEO 才可以很好地对其优化。尽管功能性测试对性能有一定的保证，但测试并不能预料数据库会发生的一切。因此，在进行完全部署之前，对数据库进行全面 的检查是非常有必要的。

2.数据泄露

你可以把数据库当做后端设置的一部分，并将焦点转移到保护互联网安全上面，黑客很容易操纵数据库中的网络接口的，所以，为了避免这种现象发生，工程师在进行数据库开发时，使用 TLS 或 SSL 加密通信平台变的尤为重要。

3.数据库维护

你是否还记得 2003 年的 SQL Slammer 蠕虫病毒，该病毒利用 SQL Server 的漏洞进行传播，导致全球范围内的互联网瘫痪，中国也有 80%以上网民受到

影响。该蠕虫的成功充分说明了保护数据库安全是多么的重要。不幸的 是，现实中很少有公司对他们的系统提供常规的补丁，因此，他们很容易遭受蠕虫攻击。

4.数据库备份信息被盗

通常，数据库备份信息外泄一般会来自两种途径，一个是外部，一个是内部的。这是许多企业会经常遇到的问题，而解决这种问题的唯一方法是对档案进行加密。

5.滥用数据库特性

据专家称，每一个被黑客攻击的数据库都会滥用数据库特性。例如，黑客可以在系统没有执行的情况下随意进入系统。解决这种问题的方法是移除不必要的工具。

6.基础设施薄弱

黑客一般不会马上控制整个数据库，相反(+本站微信 networkworldweixin)，他们会选择玩跳房子游戏来发现基础架构中薄弱的地方，然后再利用该地方的优势来发动字符串攻击，直到抵达后端。

7.缺乏隔离

给管理员和用户进行职责划分，如果他们试图盗取数据，那么内部员工将会面临更多的困难。所以，限制用户数量，这样黑客想控制整个数据库就会有一定的挑战。

8.SQL 注入

一旦应用程序被注入恶意的字符串来欺骗服务器执行命令，那么管理员不得不收拾残局，在保护数据库上，这是一个主要问题。目前最佳的解决方案就是使用防火墙来保护数据库网络。

9.密钥管理不当

保证密钥安全是非常重要的，但是加密密钥通常存储在公司的磁盘驱动器上，如果无人防守，那么您的系统会很容易遭受黑客攻击。

10.违法操作

开发人员可以利用追踪信息/日志文本来查询和解决此类问题。